

**SECURITY TESTING OF ETHIOPIAN  
E-GOVERNMENTAL WEBSITES USING  
PENETRATION TESTING TOOLS**

**A THESIS SUBMITTED TO THE GRADUATE  
SCHOOL OF APPLIED SCIENCES  
OF  
NEAR EAST UNIVERSITY**

**By  
HABTAMU GIRMA DEBEBE**

**In Partial Fulfillment of the Requirements for  
the Degree of Master of Sciences  
in  
Software Engineering**

**NICOSIA, 2019**

**HABTAMU GIRMA**

**DEBEBE**

**SECURITY TESTING OF ETHIOPIAN E-GOVERNMENTAL  
WEBSITES USING PENETRATION TESTING TOOLS**

**NEU**

**2019**

**SECURITY TESTING OF ETHIOPIAN  
E-GOVERNMENTAL WEBSITES USING  
PENETRATION TESTING TOOLS**

**A THESIS SUBMITTED TO THE GRADUATE  
SCHOOL OF APPLIED SCIENCES  
OF  
NEAR EAST UNIVERSITY**

**By  
HABTAMU GIRMA DEBEBE**

**In Partial Fulfillment of the Requirements for  
the Degree of Master of Sciences  
in  
Software Engineering**

**NICOSIA, 2019**

**Habtamu Girma DEBEBE: SECURITY TESTING OF ETHIOPIAN E-  
GOVERNMENTAL WEBSITES USING PENETRATION TESTING TOOLS**

**Approval of Director of Graduate School of  
Applied Sciences**

**Prof.Dr.Nadire CAVUS**

**We certify this thesis is satisfactory for the award of the degree of Master of Sciences  
in Software Engineering**

**Examine committee in charge:**

Assist. Prof. Dr. Boran ŞEKEROĞLU

Department of Information Systems  
Engineering, NEU

Assoc. Prof. Dr. Kamil DIMİLİLER

Department of Automotive Engineering, NEU

Assoc. Prof. Dr. Yoney Kirsal-Ever

Supervisor, Department of Software  
Engineering, NEU

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original of this work.

Name, Last name: Habtamu Girma Debebe

Signature:

Date:

## **ACKNOWLEDGMENT**

I would like to thank my thesis advisor Assoc. Prof. Dr. Yoney Kirsal-Ever, for her major advice, motivation and different valuable comments which helps me to understand problems in easy ways. The role of Assoc. Prof. Dr. Yoney Kirsal-Ever in this thesis is not only commenting on the paper rather it is more supportive. And she was loyal to me, whenever I go to her office she never hesitated to help. So, I would like to express my appreciation to her and it was a pleasure that she was my advisor. Next to this, I want to thank my course advisor Assist. Prof. Dr. Boran for his kindness and his positive thinking.

Lastly, I would like to thank my parents, my father Girma Debebe, my mother Mulu Tesfa and my three sisters (Yetnayet, Sossina and Meskerem) , who are helping me to do this thesis and gives me advice to stand here. And I want to thank egziabher, he is everything for me, he provides whatever I ask. Am happy knowing him and to have him. This work is not only mine, all of them were behind this, and they will be behind me whenever I need them because I couldn't make it alone.

## ABSTRACT

In recent days, there is nothing which can be done without the involvement of technology. Because, technology is not an option on this days, rather it is a necessity in order to walk on with the rest of the world. Websites for Governments are one of word's best technology, which allows consumers and the government to execute tasks in easy and faster way. Governmental websites reduces the effort and the time wastage of consumers because most governmental organizations or sectors works manually. As websites are working automatically, they are feasible and better than manual way of providing services. In Ethiopia, there are a number of Governmental websites which provides effective and efficient services for their respected citizens. In order to serve the citizen of the country, those websites should be secured. So that citizens will have faith or trust on their governmental services. To insure or evaluate their security, we select 11 Ethiopian websites. By using three penetration testing tools, we test the security of websites. We use Acunetix, Vega and NetSparker VAPT to assess or evaluate the vulnerabilities that the websites are exploited. This thesis focuses on the security of Ethiopian governmental websites using the three well-known scanner tools. We compare the security of my country to Turkish governmental and websites. And the result shows that Turkish websites are much more secured than Ethiopian websites. Based on the final result, we conclude that almost all Ethiopian websites are vulnerable for different vulnerabilities. Most websites are vulnerable for SQL Injection and XSS (high severity vulnerabilities). When we compare scanning tools based on their result, Vega web vulnerable scanner was the best one. It detects maximum number of high severity vulnerabilities from Ethiopian governmental websites than the other tools.

**Keywords:** Vulnerabilities; Website Security; governmental websites; Vulnerability Assessment and Penetration testing tools

## ÖZET

Son günlerde, teknolojinin katılımı olmadan yapılabilecek hiçbir şey yoktur. Çünkü teknoloji bugünlerde bir seçenek değil, dünyanın geri kalanıyla birlikte devam etmek için bir zorunluluktur. Hükümetler için web siteleri, tüketicilerin ve hükümetin işleri kolay ve daha hızlı bir şekilde yerine getirmelerini sağlayan, kelimenin en iyi teknolojilerinden biridir. Hükümet web siteleri, çoğu devlet kuruluşu veya sektörü manuel olarak çalıştığı için tüketicilerin çabalarını ve zaman kaybını azaltır. Web siteleri otomatik olarak çalıştığı için, hizmet sunmanın manuel yolundan daha uygun ve daha iyidirler. Etiyopya'da, saygın vatandaşlarına etkili ve verimli hizmetler sunan bir dizi Hükümet web sitesi vardır. Ülke vatandaşına hizmet etmek için bu web sitelerinin güvenceye alınması gerekir. Böylece vatandaşlar devlet hizmetlerine güvenecek veya güveneceklerdir. Güvenliklerini güvence altına almak veya değerlendirmek için 11 Etiyopya web sitesi seçiyoruz. Üç penetrasyon test aracı kullanarak, web sitelerinin güvenliğini test ediyoruz. Web sitelerinin sömürüldüğü güvenlik açıklarını değerlendirmek veya değerlendirmek için Acunetix, Vega ve NetSparker VAPT kullanıyoruz. Bu tez, iyi bilinen üç tarayıcı aracını kullanarak Etiyopya hükümetinin web sitelerinin güvenliğine odaklanmaktadır. Ülkemin güvenliğini Türkiye'deki resmi web siteleriyle karşılaştırıyoruz. Sonuçta, Türk web sitelerinin Etiyopya web sitelerine göre çok daha güvenli olduğunu gösteriyor. Nihai sonuçlara göre, neredeyse tüm Etiyopya web sitelerinin farklı güvenlik açıklarına açık olduğu sonucuna vardık. Web sitelerinin çoğu, SQL Injection ve XSS'den (yüksek önem açıkları) korunmasızdır. Tarama araçlarını sonuçlarına göre karşılaştırdığımızda, Vega web savunmasız tarayıcı en iyisiydi. Etiyopya resmi web sitelerinde diğer araçlara göre azami derecede yüksek güvenlik açığı tespit ediyor.

**Anahtar Kelimeler:** Güvenlik Açıkları; Web Sitesi Güvenliği; resmi web siteleri; Güvenlik Açığı Değerlendirmesi ve Penetrasyon testi araçları

## TABLE OF CONTENTS

<b>ACKNOWLEDGMENT.....</b>	<b>ii</b>
<b>ABSTRACT .....</b>	<b>iii</b>
<b>ÖZET.....</b>	<b>iv</b>
<b>TABLE OF CONTENTS .....</b>	<b>v</b>
<b>LIST OF TABLES .....</b>	<b>viii</b>
<b>LIST OF FIGURES .....</b>	<b>ix</b>
<b>LIST OF ABBREVIATIONS .....</b>	<b>x</b>

### CHAPTER 1: INTRODUCTION

1.1. Background .....	2
1.1.1. Country profile .....	3
1.2. Overview of Website Security .....	4
1.2.1. Types of website attacks .....	4
1.2.2. Why website security? .....	5
1.2.3. Website security using SSL .....	6
1.2.4. Vulnerability assessment and penetration testing .....	6
1.3. Statement of the problem .....	7
1.4. Research Questions .....	8
1.5. Objectives .....	8
1.5.1. General objectives .....	8
1.5.2. Specific objectives .....	8
1.6. Motivation .....	9
1.7. Scope and Limitation .....	9
1.8. Significance of the Research .....	9
1.9. Methodology and Tools of the Research .....	9
1.10. Pros and Cons of E-Government .....	10
1.11. Organization of the research .....	11

### CHAPTER 2: LITERATURE REVIEW

2.1. E-Government .....	12
-------------------------	----



2.2. E-Government in Ethiopia .....	13
2.2.1.Ethiopia E-Government websites, e-Services and applications .....	13
2.3. E-Government Delivery Models and Activities.....	13
2.4. Manual vs Automated Penetration Testing.....	14
2.5. Web Services Security .....	15
2.6. Using of Website Scanners to Detect Vulnerabilities .....	16
2.7. Overview of Literature Review.....	20

### **CHAPTER 3: ANALYZING OF EXISTING WORKS**

3.1. Accessibility and Usability of Ethiopian E-Governmental Websites.....	21
3.2. Security Evaluation of Ethiopian Governmental Universities .....	22
3.3. E-Government Website Evaluation for Jordan .....	23
3.4. Website Security a Survey of Government Websites in Kyrgyz Republic .....	25
3.5. Penetration Testing for Libyan Governmental Website .....	26
3.6. Security Analysis of Mozambique’s Web Servers.....	28

### **CHAPTER 4: RESEARCH METHODOLOGY**

4.1. Research Methodology .....	29
4.1.1.Literature review .....	30
4.1.2.Development tools .....	30
4.2. Research Approach.....	30
4.3. Research Strategy .....	31
4.4. Assessing Websites .....	31
4.5. Tool Selection .....	31
4.5.1.NetSparker .....	32
4.5.2.Acunetix .....	32
4.5.3.Vega .....	33
4.6. Sampling Design .....	34

### **CHAPTER 5: WEBSITE EVALUATION AND RESULTS**

5.1. Procedures of Web Security Evaluation .....	36
5.2. Result on NetSparker.....	37
5.3. Result on Acunetix scanner .....	42

5.4. Result on Vega Scanner .....	47
5.5. Result of Some Turkish Websites .....	52
5.6. Tool Comparison.....	52
 <b>CHAPTER 6: CONCLUSION AND FUTURE WORKS</b>	
6.1. Conclusion .....	53
6.2. Future Works.....	54
 <b>REFERENCES</b> .....	55
 <b>APPENDICES</b> .....	58
<b>APPENDIX 1:</b> Screen shots of vega web vulnerability scanner.....	59
<b>APPENDIX 2:</b> Screen shots of acunetix web vulnerability scanner .....	62
<b>APPENDIX 3:</b> Screen shots of netsparker web vulnerability scanner .....	65

## LIST OF TABLES

<b>Table 4.1:</b> Name of the organization with their URL .....	35
<b>Table 5.2:</b> Result of NetSparker VAPT for Ethiopian websites .....	37
<b>Table 5.3:</b> Result of Acunetix VAPT for Ethiopian websites .....	42
<b>Table 5.4:</b> Comparing Scanners based on number of high severity vulnerabilities.....	52

## LIST OF FIGURES

<b>Figure 5.1:</b> Result of Net Sparker VAPT for Ethiopian websites .....	38
<b>Figure 5.2:</b> Important severity of Ethiopian websites .....	39
<b>Figure 5.3:</b> Medium Severity of Ethiopian websites.....	40
<b>Figure 5.4:</b> Low Severity by NetSparker VAPT.....	41
<b>Figure 5.5:</b> Result of Acunetix VAPT for Ethiopian websites .....	43
<b>Figure 5.6:</b> High Severity of Ethiopian Websites .....	44
<b>Figure 5.7:</b> Medium severity by Acunetix .....	45
<b>Figure 5.8:</b> Low Severity by Acunetix VAPT .....	46
<b>Figure 5.9</b> Vega result of Ethiopian E-Governmental Websites .....	48
<b>Figure 5.10:</b> Vega High Severity of Ethiopian E-Governmental Websites .....	49
<b>Figure 5.11:</b> Vega Medium Severity of Ethiopian E-Governmental Websites .....	50
<b>Figure 5.12:</b> Low Severity by Vega VAPT .....	51
<b>Figure A1.1:</b> Vega Result for Bahrdar University.....	59
<b>Figure A1.2:</b> Development Bank of Ethiopia.....	59
<b>Figure A1.3:</b> National Bank of Ethiopia .....	60
<b>Figure A1.4:</b> National Educational Assessment and examination agency.....	60
<b>Figure A1.5:</b> Ministry Of Science and Technology.....	61
<b>Figure A2.1:</b> Addis Ababa University .....	62
<b>Figure A2.2:</b> Ethiopian Telecommunication.....	62
<b>Figure A2.3:</b> National Bank of Ethiopia .....	63
<b>Figure A2.4:</b> Bahrdar University .....	63
<b>Figure A2.5:</b> Development Bank of Ethiopia.....	64
<b>Figure A3.1:</b> Addis Ababa University .....	65
<b>Figure A3.2:</b> Ministry of Education.....	65
<b>Figure A3.3:</b> National Bank of Ethiopia .....	66
<b>Figure A3.4:</b> National Educational Assessment and Examination Agency .....	66
<b>Figure A3.5:</b> Ethiopian Telecommunication .....	67

## LIST OF ABBREVIATIONS

<b>E-Government</b>	Electronic Government
<b>SQL Injection:</b>	Structured Query Language Injection
<b>XSS:</b>	Cross Site Scripting
<b>VAPT:</b>	Vulnerability Assessment and Penetration Tool
<b>SSL:</b>	Secured Socket Layer
<b>Vs:</b>	Versus
<b>HTML:</b>	Hypertext Markup Language
<b>HTTP</b>	Hyper Text Transfer Protocol
<b>URL:</b>	Uniform Resource Locator
<b>W3C:</b>	World Wide Web Consortium
<b>WAVE:</b>	Web Accessibility Evaluation Tool
<b>WCAG:</b>	Web Content Accessibility Guidelines

## **CHAPTER 1**

### **INTRODUCTION**

In this modern world, everything is performed or executed in automated or computerized way. This world is full of technology, E-Government is one of those technologies that this world have created (Zhiyuan, 2002). (Abdullah, 2011) The idea or concept of E-Government is providing access to citizens without any limit or boundary. It has aim of bringing high quality services to the consumers and creating a good relationship between the government with government and government with citizen.

Now a day's security is considered as the big issue to design or develop a certain application or system. The first question that comes from the user before buying an application is that "is the application secure?" they ask this question because, everyone wants security. No one wants to be threatened, they want to be free from any danger or risk.

Website is a collection of related web pages which are located or found under the same domain, which provides an interface between the server and the client in order to communicate. The data is transmitted from the client to the server and from the server to the client in the form of HTML pages through the standard protocol which is called HTTP protocol.

At the same time, websites are vulnerable for security problems. Because of the nature of the hostile environment they are exposed to security problems. Most websites which are developed in Ethiopia do not concern about the security of the website instead they give an emphasis about the availability or the accessibility of the website. Website users do not feel comfort by using this website. Because their browser shows that the website that they are using is not secured.

Security testing is a form of non-functional testing which is executed to make sure that, whether the developed software is secured or not. Is the developed website vulnerable to attacks or not. Those questions are answered by the help of security testing. The public key

infrastructure must be applied during the development of any types of applications or websites.

The main goals of security (Rahman and Eyimaya, n.d.) is preserving Availability, Integrity and Confidentiality. Confidentiality means keeping the information secret or private. Integrity means prevent unauthorized writing or modification of the original information; everything is as expected to be. Availability means the information should be accessible and usable.

There are common words we used more frequently when we talk about security. Let's list and describe some of them.

- ✓ Vulnerability- Is a fault or a weakness which exposes information to attacks or to bring some damage on the system. It can be server side vulnerability or client side vulnerability.
- ✓ Threat- Are circumstances that bring a possible danger through unauthorized access, denial of service or disclosure. Threats can be either human or Natural. Human threats are Hackers, Virtual theft, Internet scams or viruses, worms and Trojan horses. Whereas Natural threats are Natural disaster, Fire, Voltage problems, etc.
- ✓ Attack- is an attempt to gain access or causing a damage to the system. There are three types of attacks passive, active attacks and unintentional attack. Security attacks are Interruption, Interception, Modification and fabrication.

### **1.1.Background**

Before recent times, most website holders were not afraid or worry about the security of their webpages. Except the website is conducting commercial services like Amazon, e-bay, or banking systems. But currently, everything has changed and most websites takes the security of their website under consideration. Because every visitor expects a security of the website because it is a common practice for all companies or organizations.

Being frequently accessible is not mean that the website is secured. But at the same time the website which is accessed frequently is doesn't make the website secured over others. Rather it should have been tested frequently in order not to open for vulnerability. In addition to that it makes the website secured and strong.

After a system is developed, the testing team is responsible to test the security of the developed software. There are different types of testing like usability testing, accessibility testing, security testing and etc. This document describes security testing for Ethiopian governmental websites.

(Kumar et al., 2007) E- Governance (electronic governance) is an application of information and technology for delivering government services between Government to citizens, Government to business and Government to Government. This makes services efficient and convenient for citizens.

Furthermore, E-Governance consists that comprises functions, processes, practices, and actions through digital means. It is a public sector use of information and communication in the aim of improving service delivery, to make the government accountable, effective and efficient.

In simple word, E-Government is the use of technology to deliver the services of governments to their citizens and their employees. It is about construct cooperation between the governments and citizens who are benefited by gaining accesses from their services.

But, there are security problems on those Ethiopian governmental websites. So how those websites will be secured? This document is proposed to test and compare which website is better than the other? How and why?

#### **1.1.1. Country profile**

Ethiopia is located in eastern part of Africa, boarded by Eritrea to the north, Somalia to the east, Sudan to the west and Kenya to the south. Its capital city is called Addis Ababa. Ethiopia is the second populous country in African continent nest to Sudan which covers 1,100,000 square kilometers. Unlike other African countries, Ethiopia never colonized by European countries during the colonization period. More than 100 million people lives in this African developing country. Ethiopian uses Ge'ez alphabet which any other countries never knows. At the same time Ethiopia uses a calendar which is seven years and three months behind the calendar of Gregorian.



According to world internet statistics, in Ethiopia 16,437,811 people uses internet, which is almost 15.3 % of the population. And more than 4 million people uses face book 4.2% of the whole population who lives in this country.

## **1.2.Overview of Website Security**

Web security is a mechanism to protect both websites and users (visitors) from cyber threats and unauthorized access of their information. Those malwares are able to slow the speed of the website, steal confidential secretes like credit numbers and they are also able to remove websites from search engines once and for all. There are different effective web security techniques that helps to prevent those threats (Grossman, 2012). So, in order to secure websites, there are website scanner tools. Website scanners are tools which notifies companies whether they are exposed to vulnerability or not. This helps website owners to take a decision of what has happened on their website.

Websites can be affected by several vulnerabilities. This vulnerability can be logical or technical. Some examples of technical vulnerabilities are SQL injection, local inclusion, cross site encrypting and remote file inclusion. These technical vulnerabilities can affect website security. There are different reasons about the occurrence of vulnerability on websites. Some reasons are vulnerabilities are happened because of poor programming or the outdated of the system.

Even if, websites can be secured using different security mechanisms. There are approaches which are available in the websites starting from development up to the deployment. Those are web application firewall, practicing of source coding and code reviewing. The other approach which helps websites secured is that Vulnerability Assessment and Penetration Tool (VAPT). VAPT is a particular testing which provides a detail assessment for the whole system. It also provides risk level for a web applications.

### **1.2.1. Types of website attacks**

- ✓ SQLi- Stands for Structured Query Language Injection. The website attacker could be able to control websites by changing commands which are inserted to the webpages. The attacker enters SQL commands which are malicious queries, and those commands are executed at the backend of the database and it results annoying

or unwanted results. (Hasan et al., 2017) The attacker must have a knowledge about database so the attacker can apply different queries by using different strings. This allows the attacker to login to the web application even without knowing the system and they are able to change data and even they can erase all data (OWASP, 2016).

- ✓ Cross Site Scripting (XSS) - By the help of XSS, attackers can alter or modify the webpages that other users can see. Attacker will modify information either to steal sensitive information like passwords and credit cards, or executing malicious scripts in the browser. Attacker injects client-side scripts into webpages and dynamically generates vulnerable into generated webpages. This attack can hijacked sessions and redirect the webpages into another websites (OWASP Testing Guide v2, n.d.).
- ✓ Broken Access Control- Most websites limit accesses on what users can see and what they are operating or perform. Though, Attackers can avoid such access limiting mechanisms or controllers to access unauthorized functionality. These includes accessing accounts of users, (view and modify sensitive files). Even attackers can apply this attack on administrative actions (OWASP, 2016).

The above types of attacks are not the only types. There are different types of web application attacks. However, all attacking types have their own preventing mechanisms. And by using vulnerable scanning tools, we can identify the types of problems that the website is suffering.

### **1.2.2. Why website security?**

There are common and main reasons why websites needs security. Some of them are:

- ✓ Websites which are hacked targets visitors- By using automated hacking tools, malicious software can affect websites in many different ways. And this allows attackers to gain access from the website and they are able to redirect traffic and infect website users. Summerfield, J. (n.d.) Web security is important to provide secure communication with the website visitors and the server.
- ✓ Internet is a dangerous place- Hackers frequently checks the websites for vulnerable systems. And hackers use internet to crack a certain website. Due to this, websites should be secured because websites uses internet for accessing and provide their services.

### **1.2.3. Website security using SSL**

Covering the security of the website has many areas. Let's take an example of using SSL (Secure Socket Layer). (Summerfield, J. n.d.) SSL is a security technology which creates an encrypted connection with the browser and the server; by using the prefix 'https', instead of the unsecured standard protocol 'http'. Some browsers like chrome, shows a lock symbol or icon if the website is secured by https. Websites which do not have a lock icon or websites which do not use SSL, they are considered as unsecured. The message which is sending through http protocol can be exposed by attackers. And attackers are able to delete or modify user's message. But in case of https, the messages are encrypted so that an attacker is not able to access the message. Even if the attacker intercepted the message, they are unable to read, edit or delete the message. Amazingly, we can say almost all of Ethiopian websites do not use this SSL security standard to make an encrypted connection between their server and their users' browser. While SSL is a finest standard for all types of websites. Even the rest of the world uses this standard while they do not process a complex or sensitive data.

According to HubSpot research, Chrome has 47% share of the market, and 82% of respondents. Those respondents said that they will leave the website which is not secured. Which means, if the website is not secured with SSL, from ten users 8 will leave this site. Because it is difficult to browse this website while the browser indicates it is not secured (Summerfield, n.d).

### **1.2.4. Vulnerability assessment and penetration testing**

Vulnerability assessment and Penetration testing have similar concept or we can use them interchangeably. Penetration testing is also known as Pen test. It is a testing mechanism which checks the existence or availability of vulnerabilities on websites. (Hasan et al., 2017) As we described before, websites are tested using penetration testing techniques. And these techniques are Black box testing, White box testing and gray box testing. Black box testing is a testing mechanism in which the internal structure that is going to be tested is not known by the tester. The knowledge of programming is not expected from testers. Whereas white box testing requires knowledge of programming from testers. The system which is going to be tested is known by the tester. And the combination of the two is called grey box testing (Hasan et al., 2017).

### **1.3.Statement of the problem**

Unlike the developed countries, information is spreading out gradually in the developing countries. For this reason governments of developing country uses e-Governance as a mechanism to communicate with their citizens in order to maximize the efficiency and effectiveness of their services. Ethiopian Government spends lots of budget for the development of e-Governance through the ministry of communication and Information Technology. The success or the failure of the security of the website affects E-Government either in positive or negative ways. E-Government still faces some big challenges when considering their interaction with users, due to their problem of usability, Accessibility and security.

As we know, website is an essential for company in order to communicate with customers or users. Because it is the best way to promote their products for their users. For example in Ethiopian airlines, the user can book a ticket online by the help of banking system. And most universities in my country Ethiopia, allows their students to see their dormitory placement and grades online. This makes their websites exposed to attacks because of its security weakness.

However, such kinds of vulnerabilities should be fixed before unethical hackers use this kinds of situation. This document is required to test those websites in ethical way. Websites are tested before they are deployed, but the testing is not executed carefully because of the testers. Testers will test only the technical part. This paper tests some websites by penetration testing to scanning their URL and reach on conclusion why they are not secured and how could they be secured for the future. We will have the complete test on those governmental websites and we compare results.

This research assesses the security of websites. In addition this research has an aim to answer the following questions:

- ✓ What kinds of security problems are exist in Ethiopian E-Governmental websites which makes the website more exposed to vulnerable?
- ✓ What kind of security mechanism is suitable for Ethiopian websites?
- ✓ How can we make a secured Ethiopian E-Governmental websites?

#### **1.4.Research Questions**

According to the problem statement which is described above, the following research questions are developed or constructed.

- ✓ What are limitations or drawbacks of the current security of Ethiopian E-Governmental websites?
- ✓ What are techniques and tools that we are going to use during the security testing?
- ✓ How can we evaluate the security of E-Governmental websites?

#### **1.5.Objectives**

##### **1.5.1. General objectives**

The general objective of this research is testing the security of Ethiopian websites using vulnerability assessment and penetration testing tools.

##### **1.5.2. Specific objectives**

There are specific objectives which helps to satisfy the general objective this research.

- ✓ Identify websites which are going to be tested.
- ✓ To improve the security of E-Government websites.
- ✓ Understanding and describing briefly about the security status of Ethiopian E-Governmental websites.
- ✓ Review literatures which are related with website penetration test and black box testing.
- ✓ Scan URL of the websites to detect the vulnerability.
- ✓ Determine or state hypothesis about the security of the websites.
- ✓ Prepare a research design.
- ✓ Test the security of websites and compare results of websites one with the other.

## **1.6.Motivation**

If somebody makes himself ready to do a specific research, he must have an inspiration. So that he works his research in a good manner. Here, there are some motivations which makes me to select this topic.

- ✓ Currently there is a development of hosting a website for governmental sectors. But there is a question about how much they are secured.
- ✓ Most websites are exposed to vulnerability. So to remove those vulnerable this document is prepared. That is how security testing works remove vulnerable.

## **1.7.Scope and Limitation**

The scope or the boundary of this research is to identify e-governmental websites which are going to be tested, test the security of those websites and report those results. Finally reach on conclusion whether Ethiopian governmental websites are secured or not. In addition to this we are going to compare and contrast web vulnerability scanners based on the results that every scanners provide. Here, in this paper we used two well-known vulnerable scanners and we will conclude which website is secured and which scanner provides better result. Most universities in Ethiopia are governmental, so some university websites are going to be tested. The limitation of this research is that, it uses tools to test the security of the website instead of designing web testing methodologies.

## **1.8.Significance of the Research**

This research is significant or important to those e- governmental companies and universities by identifying the security problems and by remove those vulnerabilities before unethical hackers bring some damage on their websites. This research tests at most 15 governmental websites. This will be a motivation for the rest of companies in order to secure their companies website before they suffer any damage. This research is completely advantageous for all of governmental companies which are found in Ethiopia because, it identifies critical vulnerabilities of their websites.

## **1.9.Methodology and Tools of the Research**

Methodologies and tools that are included in developing this research are:

- ✓ Literature review- Literatures which have relations with website or web application are going to be conducted. There are various literatures which deals about web application security and their testing tools. So, most researches will be reviewed
- ✓ Automated web application testing or scanner tools- Are both desktop and online website scanner tools. Tools take the URL and scan the address after that, report the level of the security of the websites as a result.

### **1.10. Pros and Cons of E-Government**

As we know, everything in this world has advantage and disadvantage. Here we are going to see the pros and cons of E-Governments as a whole (E-Spin, 2018, October 24). Here we are going to see some advantages and disadvantages of E-Government according to (Joseph, 2015).

#### **Advantages of E-Government**

- ✓ The main advantage of E-Government is improving the efficiency of the current system of the government. The current system will be paper based or it works manually.
- ✓ The goal of E-Government is able to offer services to citizens in an efficient and effective way to increase the public services.
- ✓ It also helps for the improvement of accessibility of the public services and make it accountable (E-Spin. (2018, October 24).
- ✓ It is also advantageous to reduction of costs and better for savings.
- ✓ It provides online accesses for visitors.
- ✓ And it is also transparent and less bureaucracy.

#### **Disadvantage of E-Government**

- ✓ (Alshehri and Drew, 2011) The disadvantage of E-Government is the deficiency of reliability of the information on websites.
- ✓ They are vulnerable to cyber-attacks. There is a security problem because internet is vulnerable for cyber-attacks. It results lack of trust from visitors of the sites.
- ✓ Somehow, there is an accessibility problem. It will not be accessible for disable persons (E-Spin, 2018, October 24).

- ✓ It costs too much for the development and the implementation of E-Governments.

### **1.11. Organization of the research**

In this research paper, we will have six chapters to make the paper complete. The first chapter is going to be an introduction of the research and it includes background of the research, overview of website security, statement of the problem, research questions, objective of the research: this includes specific and general objectives of the research, motivation of the research, scope and limitation of the research, significance of the research, methodologies that are using during developing this paper and the last part of this chapter is that, pros and cons of E-Governments.

The second chapter is named as Literature review. In this chapter, some literatures which talks about E-Government and their security are reviewed. Here, we will see literatures that are wrote about the websites of E-Governments in different perspectives.

The third chapter is Research methodology. In this chapter we will see research methods that this paper uses, the research approaches or data gathering techniques. Tools that are used to test the security of the website is selected in this chapter. Tools are not selected randomly. There are lots of website vulnerability scanners, among them we select two scanners. Why we choose those two over the others will be answered in this chapter.

The fourth chapter includes related works which have done before. The name for this chapter is related works. This chapter describes, the number of websites that are tested, the scanner tools that the researcher used to test those websites, the final result from the generated result and finally the best scanner over the others that the researcher used will be selected. The conclusion will then followed.

The fifth chapter is evaluation of websites, the description of sample websites that are going to be tested. This chapter includes testing website, reporting final result, comparing scanners and selecting the better scanner. At the same time which website has better security and which website has the high security risk.

The sixth chapter is conclusion and future work of website security. It also includes recommendation for Ethiopian E-Governmental websites.



## **CHAPTER 2**

### **LITERATURE REVIEW**

Literature review is not a quote and summary of other documents which are gathered from different sources. It is one of the methodologies which helps to gather or collect data for the research which is going to be prepared. The researcher could refer websites, books, articles or journals to collect documents about the subject or topic that the researcher are doing the paper. The readers of this paper will understand that the researcher has a detail knowledge about what he is written. In another words, literature review is a measure or an indicator of how much the researcher has a detail information about what is developed. In simple word, literature review is a search and evaluation of available documents which have related or similar idea with the selected topic.

#### **2.1.E-Government**

According to (Lessa, 2015, December), E-Government is a project in a national level that provides the information and its services all over the internet for public services. So that citizens are able to ask governmental related services without the physical interactions of both the government and the citizens.

And in the assumption of (Ihmouda and Alwi, 2014) E-Government is an effective government which uses modernized technology in order to provide efficient and effective services to citizens and business areas.

(Ndou, 2004), defines E-Government as, it is the means of using networks and computers in order to improve the structure of the governments and the way of working mechanisms. This helps the government the process of doing any tasks easy or simple and suitable when we

compare in the meaning of time. The separation of departments offers the extraordinary quality and consistent management to the citizen's service.

## **2.2.E-Government in Ethiopia**

There is one sector which controls the E-Government of Ethiopia and it is called Ministry of Communication and Information Technology or MCIT in short form. According to (MCIT-eGovernment, 2011) and (MCIT-eGovernment, 2016), the strategy and the implementation plan of Ethiopian E-Government has four vital aims or objectives.

The first one is bring the people and the governments much closer. Which means, as the closeness of the two increases, the deliverance of the services becomes too much effective. The second objective is the implementation of effective governance. Being effective in governance needs best implementation in real life, so that, the way we implement the governance really matters. The third is, improve service delivery. As its name suggests, the deliverance of the products should be in a civilized way. The fourth objective is that, the deployment of those resources and being competence in the outside world.

### **2.2.1. Ethiopia E-Government websites, e-Services and applications**

According to Ethiopian National Growth and Transformation Plan (FDRE, GTPII, 2011) and (FDRE, GTPII, 2016) report, there are about 126 informational services and 164 transactional electronics services have been developed by Ministry of Communication and Information Technology. Similarly, vast application of E-Government, e-learning, e-library, mobile banking and others enables to increase the effectiveness, efficiency and quality of both private and public facilities. Those services are delivered to the citizen of Ethiopia.

## **2.3.E-Government Delivery Models and Activities**

According to (Mohammed and Steve, 2010) and (Pulinat, 2011), the deliverance of the activities of the government to its customers have the following groups.

### **i. Government-to-Citizen**

Government-to-Citizen (G2C) lets consumers or citizen to interact with the government by using just one window. Ethiopian government applies this deliverance way to evaluate such kinds of websites.

ii. Government-to-business

Government-to-business (G2B) implies the relationship between the government and the individual sectors. Those individual sectors or non-governmental organizations are the corporate bodies for the government. As a general truth, it makes the government more profitable in working with individual or non-governmental sectors. This deliverance makes the relationship strong and efficient.

iii. Government-to-Government

Government-to-Government (G2G) is referred as the milestone or the backbone of the E-Government. This sector believes in Modernizing their own internal systems and procedures before commencing electronic transactions with citizens and businesses. This sector involves sharing of data and improving collaboration between central and local governments. This type of delivery mechanism is mostly applied on countries which follows federalism structure. This allows the regional and the federal governments to exchange or share data or information.

iv. Government-to-Employees

Government-to-Employee (G2E) is training the employee of the government to support or help the citizen in different and fastest way. This will make the government websites easy to use and easy to understand.

## **2.4.Manual vs Automated Penetration Testing**

According to (Abu-Dabaseh and Alshammari, 2018), the aim for this paper is that the comparison of Manual and Automated web site penetration testing. Currently there are different penetration testing tools which helps to identify and fix vulnerabilities that the website is suffering. In addition this article compares the methodologies that the current automated testing tools are using. Penetration testing is necessary for all companies or organizations because, it is used to discover vulnerabilities that the system have suffered. During the penetration test, the tester uses one of the approaches: either manual or automated way.

As (Abu-Dabaseh, and Alshammari, 2018) states, Automated penetration test is the easiest and the simple way to find available vulnerabilities in the system or in the website with the

help of tools. Whereas, manual penetration testing is find and fix every vulnerabilities in the system and differentiate the unusual. The comparison of the two approaches seems like the following:

The testing process for automated testing is fast, easily repeatable test, and standard process. But in the manual side, the testing process is, high cost of customization, manual and it is not standard process. Vulnerability management of automated test is, attacked database is maintained automatically because codes are written in for many platforms. Whereas manual is, maintenance of the database is done manually. The final report is made automatically for automated test and manual test requires the collecting of data. Training for automated tools is easier than that of manual testing. For the manual testing, testers should learn nonstandard testing mechanisms. Based on the above comparisons, the researcher concludes that, penetration testing is the most important test to make the company's website secure. Finally, automated penetration testing approach is selected as the best testing method.

## **2.5.Web Services Security**

According to (Hasan et al, 2017), hackers uses vulnerabilities to steal data or information from the center. VAPT is a short form of Vulnerability Assessment and Penetration Testing allows to avoid such kinds of dangers from the websites. This paper focuses on the highest vulnerabilities that are happened more frequently than the others. Those vulnerable are SQL Injection, Cross Site Scripting Local File Inclusion and Remote File Inclusion and applies VAPT processes. VAPT tools includes, w3af, Havij, Fimap, Metasploit, Acunetix and Nexpose are the listed VAPT tools.

There are various approaches available to resolve the vulnerability, which may be available in the web application such as code review, secure coding practices, web application firewall. All these techniques are providing an option to secure the web application at each phrase since the development to deployment of web application. VAPT is also a dedicated mechanism which provides the highest security support for web services. Finally, this paper concludes that, VAPT is very important process helps in identifying security defects. Many repositories inform of tools, methods and mechanics available to support VAPT.

## **2.6.Using of Website Scanners to Detect Vulnerabilities**

(Vieira et al., 2009) Web services are used as a critical for business components. However, those websites are deployed with serious bugs which can be explored in malicious way. Due to this, web vulnerability scanners are developed to detect security vulnerabilities in web services. Even though, depend on the types of vulnerability scanners, there is different result after testing the security of the websites. Here, this article tests publically available websites with four well known vulnerability scanner tools. And during the test, large amount of vulnerabilities have been detected. Around 177 vulnerabilities are detected, as a result, this is a guide to conclude that web services are not tested before deploying. There is also a limitation on web scanners on detecting vulnerabilities from the web services. Vulnerability scanners that this paper used are: i) HP WebInspect, which is a commercial web scanner and used as an assessment for complex web services. ii) IBM Rational AppScan, is website security scanner tool for common vulnerabilities. iii) Acunetix Web vulnerability scanner is automated vulnerability scanner tool which audits or checks web services to detect and report vulnerabilities that are existed on the website. By the help of those scanner tools reports have been made according to results. For the presentation of the results, the researchers decided not to describe the brand of the scanners in order to be neutral. Because the license of the commercials do not allow evaluation of tools. So they are described in VS1.1, VS1.2, VS2 and VS3 without any order. And the overall result for those vulnerability scanners and their vulnerable have the following output or result.

The vulnerabilities that concerned are SQL Injection, XPath Injection, Code execution, Possible Parameter Based Buffer Overflow, Possible Username and Password Disclosure and possible Server Path disclosure. According to this paper's result, the first vulnerability scanner detects 217 SQL injection vulnerabilities from 38 web services, 10 XPath Injection 10 from 1 web service and 1 code execution from one web service. But, the rest three vulnerabilities can't be detected by this scanner.

The second scanner detects 225 SQL Injection vulnerabilities from 38 web services, 10 XPath Injection from one web service and one code execution. But, the rest three vulnerabilities can't be detected by this scanner. The third scanner detects 25 SQL Injection from 5 web services and can't detect the rest five vulnerabilities. Finally, the fourth scanner detects 35 vulnerabilities from 11 web services, 4 Possible Parameter Based Buffer Overflow

vulnerabilities from 3 web services, 47 Possible Username or Password Disclosure vulnerabilities from 3 web services and 17 Possible Server Path Disclosure from 5 web services.

Based on the generated reports, the result for each scanner with correspond to their vulnerability seems the first two scanners that are VS1.1 and VS1.2 provides good result whereas the other two scanners shows low coverage for SQL injection.

Finally, this paper concludes that, selecting tools for scanning vulnerabilities of web services is the most difficult job. Because, as we change the scanners, the result changes at the same time. In addition to this, the amount of false positive results is too high, which reduces the accuracy of vulnerabilities that are detected. And at last, many vulnerabilities will not be discovered or detected. Prevalent.

However, the two scanners from the same brand detects more vulnerabilities than the other two different vulnerability scanners. The VS1.1 and VS1.2 are the only scanners that detect code execution and XPath vulnerabilities. As discussed before it is difficult to select scanner tools due to the license of the commercial scanners. But the scanners that are in the same brand are better than the other scanners. There is a final statement about SQL injection, they are dominant in the tested as they symbolize 84% of all vulnerabilities detected.

(Fonseca et al., 2007), the researcher chooses two vulnerabilities that are faced more frequently than the other types of vulnerabilities. Those vulnerabilities or threats are SQL Injection and Cross Site Scripting (XSS). The writer chooses those two vulnerable over others, because they are the most widespread and hazardous vulnerable that can spread and damage the websites easily. And at the same time it is important to trust the results that the scanning tools generated.

Here, three leading commercial web vulnerability scanners are applied and their results are compared by coverage analysis of detected vulnerabilities and false positives that are existed in the result. Depend on the results that the scanners generate, it is easy to select the best scanner from the above three vulnerability scanners. Here. Like the above articles or papers, this researcher do not decide to select the better scanner due to commercial problem. They used three commercial web scanners to test two web applications. The first web application is named by MyReference and it is used to manage information which are related with

personal. The second web application is called BookStore web application. According to (Fonseca et al., 2007), the number of vulnerable or faults which are detected were 659. Whereas, in the BookStore application 327 faults were detected. All faults were results XSS and SQL Injection.

And they develop bench mark for web vulnerability scanners. And the approach is based on one fault at each time. That means, once scanners supposed to detect vulnerabilities, then the researcher provides an input to handle those vulnerabilities. This was the benchmark which the researcher proposed. According to (Fonseca et al., 2007), Number of false positives for BookStore web application are as follows: scanner 1 detects 6 false positive vulnerabilities and it is 38% in percentage, scanner 3 detects 36 false positive vulnerabilities. Number of false positives for MyReference web application is: 13 false positive vulnerabilities are detected from the scanner1 it is almost 20% in percentage, scanner 2 detects 43 vulnerabilities and it is 62%, scanner 3 detects 45 vulnerabilities which is 38% in percentage. When we see SQL Injection and XSS coverage of BookStore web application, it seems: 19 XSS and 3 SQL Injection are found by scanner 1, scanner 3 detects 29 XSS vulnerabilities and 5 SQL Injection results have been detected. And finally the researcher chooses scanner 3 as a best scanner when compared to the others. The conclusion shows that, different scanners provides different results and they report number faults they are detected, false positives in percentage. Besides, it also concludes the scanner that detects more XSS will not be the same for SQL Injection. Because vulnerabilities are not proportional.

(Bau et al., (2010), black-box scanners are automated tools that are used to analyze or examine the security of web services. This paper accesses eight well known scanners and applies the following studies. The class of the vulnerability that scanner tested, scanners effectiveness towards the vulnerabilities and the importance of vulnerabilities to be found. This paper asks the following questions. The types of vulnerabilities which are going to be tested and the effectiveness of the scanners. The aim of this paper is not comparing those scanners, rather detecting the vulnerabilities and determine the effectiveness of the scanners.

(Bau et al., (2010), the most common web vulnerabilities are cross site scripting, SQL Injection, information disclosure and other cross channel scripting .studied the vulnerabilities. In addition to this, this article states that black box web application

vulnerability scanners are good to detect SQL Injection and XSS vulnerabilities. This paper concludes that black box scanners are better scanners to scan and detect the most dangerous vulnerabilities that will harm the website. If someone wants to scan the vulnerabilities of a certain website, this paper advises to use black-box scanners.

Grossman, J. (2012), more than 8,000 websites have been tested. And this paper provides a better way for the improvement of the company's website security. This paper makes average number of vulnerabilities starting from 2007 to 2011. In 2007, 1,111 vulnerabilities were detected per website. In 2008, 795 vulnerabilities were found per website, 480 web vulnerabilities were detected per website in 2009. In 2010, 230 vulnerabilities were detected and 79 vulnerabilities detected. A serious problems have decreased from year to year per websites. This paper prepares the average number of dangerous vulnerabilities per website in 2011. For banking websites 17 vulnerabilities, 53 for Educational websites, or health care websites 48, or IT 85 vulnerabilities, 52 average vulnerabilities for telecom, 67 for financial services, 92 vulnerabilities for insurance websites, manufacturing has 30 average vulnerabilities, 31 for social networking websites, 37 for nonprofit websites and 31 average web vulnerability for energy websites. But, it takes much to fix those vulnerabilities. According to this article, the minimum day to fix those serious vulnerabilities is 4 days and the maximum day is 80 days. This paper concludes, to minimize the average number of vulnerabilities in each websites, it is better to teach the right person and test the security of websites before they are launched. This approach is able to remove vulnerabilities and ensures the security of websites. The company should test its security of the network before launching and at the same time, if the company designs a web services, they must have test the security of their web services before launching it.

(Antunes and Vieira, 2014), most of the time, web services are deployed with different malicious or vulnerabilities. This paper uses automated web vulnerable tools to avoid such malicious attacks from the websites. (Antunes and Vieira, 2014), uses Black-box scanners to detect different kinds of vulnerabilities and uses four different scanners to check the security of websites. 25 different web services have been tested in this paper. According to this paper, the overall result for the scanners and their corresponding result is listed as follow: four vulnerability have named as VS1, VS2, VS3, and VS4. VS1 detects 62 SQL Injection and 2 XPath Injection vulnerabilities, VS2 discovers 42 SQL Injection and 0 XPath Injection



vulnerabilities, the third scanner VS3 founds 6 SQL Injection and zero XPath Injection and VS4 which is the fourth scanner detects 47 SQL Injections and 1 XPath Injections.

The two scanners which are VS2 and VS3 can't detect XPath selection but they discover SQL Injection vulnerabilities. When we compare all four tools, the first and the fourth scanners detect both types of vulnerabilities. The false positives which are generated as an overall result indicate that, VS1, VS2 and VS4 have high percentages. Whereas, the VS3 scanner reports no false positives. The paper concludes that VS1 has a better coverage than the others and VS3 does not cover like the rest two scanners. This indicates that, VS1 is a better scanner than the others even though, it is better when compared with the others but it has some limitation.

## **2.7.Overview of Literature Review**

As a summary, here we are going to recap the concept of the articles which are discussed in this chapter. Most articles have the same concept which is selecting a website which is going to be tested and select a good vulnerable scanner to detect vulnerabilities without the knowledge of the website owners. The researchers test the selected websites with the selected scanners and report the overall result. Based on the final result the researchers selected the preferable scanner and conclude whether the websites are vulnerable to threats or not. Which type of vulnerability is challenging the website and which website is easy to attackers for hacking and cracking. But, researchers are not volunteer to tell the selected scanner because of the commercial license. But most researchers use Acunetix and NetSparker web vulnerability scanners to detect the available web scanners. They chose those scanners because such kinds of scanners are good at detecting the most well-known vulnerabilities like SQL Injection and Cross Site Scripting.

## **CHAPTER 3**

### **ANALYZING OF EXISTING WORKS**

This chapter describes some works which are related with the topic or the business idea of the thesis. For this paper there are related papers on e-government websites, the accessibility and usability of e-Governmental websites and security of e-Governance websites. Here we are going to review some related documents. Some of them are accessibility, usability and security of the e-governmental websites for my own country (Ethiopia) and for other countries.

#### **3.1. Accessibility and Usability of Ethiopian E-Governmental Websites**

This article was made for the partial fulfillment of master's degree in Ethiopia in a well-known university which is called Addis Ababa University. The vital goal of this paper is to create accessible and usable Ethiopian e-Governmental through the proposed model. The accessibility of those websites is tested by using automated tool which is WAVE accessibility assessment tool. The usability testing uses data collection and analyzing methodology to identify the usability problems of Ethiopian e-Governmental websites. This paper was prepared to improve the accessibility and usability of Ethiopian websites in users and manager's perspective.

According to (Yosef, 2018), there are defined challenges for making websites usable. Some of them are shortage or lack of awareness of usability, deficiency of end users to send feedback, problems of managing and lack of budget. But, the main challenge were lack of awareness, standards and guidelines for usability. The researcher prepares questionnaire for citizens and managers of Ethiopian websites to assess the usability.

The accessibility testing is executed by the help of WAVE accessibility tools. Those tools are web services and browser extensions to evaluate the content of the testing website. Let's take an example to see a web accessibility summary report for Ethiopian government portal. It has 50 features, 93 HTML5 and ARIA, 23 alerts for system design, 3 errors in a link and

287 contrast errors. Other reports have been summarized, this is taken to see how Ethiopian e-Governmental websites are accessible.

(Yosef, 2018) concludes that, Ethiopian e-Governmental websites have more usability and accessibility errors. Ethiopian e-Governmental websites violates or disrespects the guidelines and standards of W3C and WCAG 2.0. Usability is the vital to fulfill users need over Ethiopian e-Governmental websites. If the website is not usable, the users will go away to use such kinds of websites. To make users satisfy, there should be an effective way to make the available websites more usable and accessible. As a result, they are poor on usability and accessibility.

### **3.2. Security Evaluation of Ethiopian Governmental Universities**

Like the first paper, this article was made for the partial fulfilment of master's degree in Addis Ababa University. (Gebrekidan, 2015), states that attackers can easily attack Ethiopian university websites in order to post unwanted or false information which invites to the Ethiopian communities to start a civil war between Ethiopian communities. Before those results occurred, the Ethiopian university websites must be secured by the help of different web security mechanisms. The preventive mechanism is identifying vulnerabilities by using black-box penetration testing to exploit the available vulnerabilities. Ethiopian universities that this paper tested are, Wollo University, Addis Ababa University, Diredewa University and Assosa University. The researcher uses three scanners namely Qualysguard, Nessus and Nexpose web vulnerability scanners.

The researcher tests 4 universities that are described above and here we are going to see the result of Assosa University. And this university is vulnerable for the following vulnerabilities by the three scanners. Here we are listed some vulnerabilities from the overall result.

- ✓ Qualysguard Scanner- Assosa University is vulnerable to: Joomla! Cross-Site Scripting and Unauthorized Gmail Login Vulnerabilities (port 80/tcp), HTTP TRACE / TRACK Methods Enabled (port 80/tcp), Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability and web links-categories SQL Injection Vulnerability

- ✓ Nexpose Scanner- Apache HTTPD: insecure LD\_LIBRARY\_PATH handling, Apache HTTPD: mod\_status buffer overflow, Joomla!: [20131101] Core XSS Vulnerability (joomla-20131101-core-xss) and HTTP TRACE Method Enabled (http-trace-method-enabled)

Nessus Scanner- Apache 2.2 < 2.2.24 Multiple XSS Vulnerabilities, PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities, PHP 5.3.x < 5.3.23 Information Disclosure, Web Server Allows Password Auto-Completion and HTTP TRACE / TRACK Methods Allowed are detected from this scanner.

The comparison of the vulnerabilities of the scanners is that, most vulnerabilities that are detected by the three scanners are common and similar. The difference is that the naming of those vulnerabilities due to the nature of the scanner. The three scanners detected the most common vulnerabilities like SQL Injection and XSS vulnerabilities.

Finally (Gebrekidan, 2015) concludes that Ethiopian universities are vulnerable to the most critical vulnerabilities such as Cross Site Scripting (XSS), SQL Injection and other web attacks. Especially Dire Dawa University and Hawassa University are the most vulnerable universities. If all Ethiopian Universities continues in this way, they will be exposed to more attacks and vulnerabilities. Information of students that those universities stored are going to be traced and modified or changed maybe deleted by those unauthorized attackers. Thus, critical information is going to be exposed for crackers. If such kinds of website assessment applies on the other University websites, there is a high probability to detect more vulnerabilities than those four Universities. Before attacking, it is better if all universities assesses their websites for their own safety.

### **3.3. E-Government Website Evaluation for Jordan**

It is clear that if any researcher tries to do a research on a certain area, there is a motivation or a reason behind this. (Alsmadi and Shanab, 2016), they were motivated to do this work because, when they writes “inurl:/tabid/36/language/en-US/default.aspx” in the searching box, the browser displays the websites of the Jordan’s e-Governmental websites. Due to this, the researchers prepares this paper. This work focuses on the security testing or ethical hacking on e-Governmental websites of Jordan. It uses different web penetration testing

tools like rapid 7, Nessus and Acunetix vulnerability scanners and most frequently vulnerabilities have been detected. Most websites are vulnerable for those vulnerabilities. The researcher uses different websites to identify the possible problems that the websites faced. At the same time this paper assures that almost all types of vulnerabilities have been occurred on some e-Governmental websites. Securing e-Governmental websites means securing information of the citizens of the government. Securing citizen's information includes, the protection of deletion or modification of those information without the permission of the authenticated citizen. Based on the result of this paper, the websites that are more vulnerable for more exploits or vulnerabilities are listed below as follow.

Moj.gov.jo- Minister of Jordan. The types of operating system that this site using is Linksys Embedded. The number Exploits is 23 and the number of vulnerabilities that the scanner detected is 122.

Pm.gov.jo- Prime ministry. Linksys is the type of operating system that this website is using and there are 23 Exploits and 85 vulnerabilities have been detected.

Moh.gov.jo- Ministry of health. The type of operating system that this site using is Microsoft Windows NT 4.0. Eight vulnerabilities have been detected and 1 exploit.

Moe.gov.jo- Ministry of Education. Microsoft Windows Server 2003 is the operating system that the website uses. Two vulnerabilities have been detected and one exploit.

Moi.gv.jo- Ministry of Industry. Microsoft Windows is the operating system that the ministry of industry uses. Three vulnerabilities have been discovered and two exploits from this site.

The tools that detects different critical and the severe security problems of the Jordan websites are listed and descried below. The result is combined for all tested websites.

NT IIS Malformed HTTP Request Header DoS Vulnerability occurs 12 times, Microsoft IIS Unprotected CNF Files Information Disclosure exists 9 times, ISC BIND dos attack happens 4 times and Microsoft IIS search DoS attack occurs 6 times. The severity or brutality of those vulnerabilities are categorized under severe.

The vulnerabilities which are categorized under moderate are the following exploits. ISC BIND catch update occurs 4 times and DNS Traffic Amplification happens 4 times from the selected websites of Jordan's e-Governmental websites that the researcher tested.

There are vulnerabilities that are categorized under critical state. ISC BIND installation have four occurrences and handling of zero data occurs four times. These are the critical vulnerabilities that Jordan' e-Governmental websites.

(Alsmadi, I., 2016) concludes that security for e-Governmental websites do not considered as an option rather it is the core for the success of the survival of those websites. Therefore all websites should be tested more frequently to make websites free from existed vulnerabilities by the help of vulnerability assessment and scanning tools.

According to the results which are recorded Ministry of Education (moe.gov.jo) was registered as the top vulnerable websites. This result leads that, citizens are exposed to security problems and this site will lost the trustiness of its consumers. It must be secured, because it's a website for higher educational information in a national level. So, there will be a fear of using this site. Finally this paper reminds Jordanian e-Governmental websites should provide high protection mechanism to protect their websites for attacks from attackers and must eliminate more risks.

As a recommendation, those websites should be tested and the developers have to identify the existed vulnerabilities before the developed website is deployed. This will make the websites secure and at the same time this leads a better interaction between the government and their consumers. Because, customers need a secured service in order to be free from any threat and risk. So for the future, testing a website before deploying should be considered as an obligation.

### **3.4. Website Security a Survey of Government Websites in Kyrgyz Republic**

Before defining and reviewing the final result of the Kyrgyz's websites, let us say something about Kyrgyz. Kyrgyz republic is located in the central Asia and the nearest country for Kyrgyz is Uzbekistan. The Kyrgyzstan researcher studies this study to analyze the security of the countries website.

The vital aim or objective of (Ismailova, 2015) is that, inspecting or investigating the usability, accessibility and security of e-Governmental websites which are found in Kyrgyz Republic. Fifty five websites have been selected for usability, accessibility and security testing. The analysis of those websites is conducted using automated tools. The results indicated that Kyrgyz Republic websites have 46.3% error rate in usability and 69.38% error rate in accessibility. The study shows that those websites have different security vulnerabilities. Tools that the researcher uses are: for testing the usability WebSiteOptimization online tool is used. For testing the accessibility EvalAccess 2.0 is used. When we come to the tools that the researcher uses to test the security of the website, there is an extension which chrome browser uses. And also there is a web vulnerability scanner Net Sparker. Which helps to detect SQL Injection and XSS vulnerabilities of websites. Net Sparker provides a report that, how many website vulnerabilities have been detected in a certain website. The researcher describes that Net Sparker is preferable to scan the SQL Injection and XSS vulnerabilities. Because, it reports which vulnerabilities are critical, which are important and which are low.

Finally (Rita, 2015) concludes that, the priority which the government gives for usability is too low. About 44.23% of websites have links which is broken. At the same time more than 70% of websites failed during the accessibility test. Those results lead to conclude, Kyrgyz e-Governmental websites exploit WCAG 1.0 to make their websites accessible. The security problem was that 55% of Kyrgyz e-Governmental websites use the old version of Content Management System (CMS). As a final word, the websites give low priority for the security of their websites. The number of attacks on websites is increased from year to year, due to this, Kyrgyz e-Governmental websites should give an emphasis about the security of their company. As e-Governance provides services to the citizens, citizens should not have been afraid of their privacy. To make the citizens' information confidential, all e-Governmental websites should be secured. They have to be tested before they are launched.

### **3.5. Penetration Testing for Libyan Governmental Website**

Libya is a developing country which is located in the northern part of Africa. The Libyan researcher selects this topic, to know whether the Libyan governmental websites are secured or not. The main objective of making research is that to assess the vulnerabilities that

websites faced and evaluate the weakness of the different e-Governmental websites of Libyan government. (Ihmouda and Alwi, 2014) uses three different web vulnerable scanners to assess and evaluate the security of the websites. Websites that this paper tested are Prime minister's office, Ministry of Defense, Ministry of Transportation.

Web vulnerability scanner that this study uses are NStalker, Acunetix and Nessus vulnerability scanners. All of the tools start scanning after the URL of the websites which are going to be tested are typed. Finally the results have been reported.

The result that N-Stalker scanner results. The result seems: prime minister's office have 16 high severity risks, 5 moderate severity risks and 0 low risks. Ministry of defense have 8 high severity risks, 4 moderate severity risks and 10 low severity risks. Ministry of Transportation have 6 high severity risks, 8 moderate severity risks and 11 low severity risks.

Acunetix scanner has the following result. Prime minister's office have 22 high severity risks, 11 moderate risks and 1 low severity risks. Ministry of defense have 0 high severity risks, 1 moderate severity risks and 7 low severity risks. Ministry of Transportation have 9 high severity risk, 4 moderate severity risk and 6 low severity risk.

The third scanner Nessus produces the following result. Prime minister office have 5 high severity risks, 0 moderate severity risks and 4 low severity risks. Ministry of defense have 2 high severity risks, 1 moderate risk and 7 low severity risk. Ministry of Transportation have 0 high severity risk, 1 moderate severity risk and 2 low severity risks have been detected.

Finally (Rabia and Najwa, 2013) concludes that, e-Governmental websites of the Libyan government are in a very high severity risk. Almost all of Libyan websites are vulnerable for most well-known vulnerabilities. Among the three websites, Prime Minister Office's is the more vulnerable website in both high and moderate severity risks. Security is not only Libyan problem but also, the other Arab countries' website are most vulnerable for the vulnerabilities. The researcher explained that Libyan governmental websites are vulnerable, so assess and evaluate them before the citizen of the government attacked by attackers and hackers. And finally the researcher reminds hosting a website is not feasible if, the website is vulnerable for many security risks.



### **3.6. Security Analysis of Mozambique's Web Servers**

Before writing about Mozambique's website, it is better to say something about the country. It is found or located in the southeastern part of Africa. Now we can see the security of their websites according to the paper. The paper (Vumo et al., 2017) is made to evaluate the exposure of Mozambican web servers. The vital goal or aim of this study is to analyze the security of Mozambique's website and to identify how many Mozambican websites use a security mechanism to make their website and their consumers secured. And to examine or measure the security of the number of Mozambican websites which are existed by applying HTTPS header. And this paper ensures the significance of using high security mechanisms to keep the websites and their respected customers secured. According to the researcher, security of Mozambican websites should not be a choice rather it is a must or a necessity.

The researcher evaluates the following websites in both in the Government and a non-Government ways websites. Those are: Bank, Telecommunication and Medias. According to the researcher, none of those websites are configured in order to use HTTP headers. This paper mainly focuses or tests the ssl of the selected websites of the privates and the governments. Focuses on implementations of HTTP security headers and the testing of those HTTP security headers.

The paper concludes that from the tested Government websites only 2% are implemented using HTTP security headers. Most of the certificates of those HTTP headers are expired, this leads the governmental websites of Mozambican to be in secured and vulnerable for attacks. This means, from the tested of Governmental websites only four of them are using HTTP security headers. This result is an indicator to conclude that, the Government of Mozambican do not give a big emphasis on their websites security in a national level. And the researcher stated that this happens because they don't have enough knowledge to make their websites secured. So, the researcher believed that carelessness and the lack of knowledge in Mozambican government makes their websites vulnerable for attacks.

And finally the researcher recommends that it should be an obligation to push both the Governmental and non-Governmental sectors to apply the security mechanisms which leads to reduce the risk that their website is faced or suffered. In addition, the researcher recommends the organization should test their websites before it is deployed by using

different vulnerability scanning tools. This is another way to keep the websites secured and confidential. Because, the organizations will know their problem and will take a measurement to fix those vulnerabilities before they bring some damages to both the organization and their respected users.

So as a future work, if those organizations apply the above recommendations, there will be a clear improvement on the security of their websites. If their website is secured there will be a satisfaction from their consumers. And this leads a better interaction between the suppliers and the producers.

## **CHAPTER 4**

### **RESEARCH METHODOLOGY**

This chapter aims to present methodologies which help to achieve the objectives of our study. First we are going to see the research methodologies which help to gather preferable documents which have a common idea or concept about website testing and e-Governmental aspects. Then research approaches and strategy that this paper uses will be described. At the same time tools which test the selected websites are selected in this chapter. Also the data analysis upholds in research methodology part of the paper.

#### **4.1. Research Methodology**

In this study, quantitative research methodology is applied to identify the basic security issues of Ethiopian e-governmental websites to find a security problem of those e-Governmental websites. As we discussed before, the research method that this paper used is surveying or reviewing literatures which have the same concept about e-government, accessibility and usability testing of a certain country's website and security testing of e-Government websites. In general we review literatures which talk about testing of websites. The results are expressed in numbering format. Which means results are stated in table form to show the types of vulnerabilities that the website faced and the frequency of those vulnerabilities in websites.

#### **4.1.1. Literature review**

As the name indicates, different papers (articles) and books are reviewed which have the same concept with the study. In this paper, we review documents which are related with testing. It can be E-Government website accessibility testing, usability and security testing. Those helps to collect more information about vulnerability assessment and penetration testing. Mostly developing countries are vulnerable to those vulnerabilities. Due to this, papers which we reviewed are from those developing countries like Jordan, Libya and Kyrgyz Republic. We reviewed those articles because we are going to test the same developing country (Ethiopia) The reviewing includes identify websites which are going to tested, the type of vulnerability that the website is exploited, the conclusion and recommendation that the researcher stated.

#### **4.1.2. Development tools**

During the development of this study, we use different tools to prepare this document. So, tools that we used are: Microsoft office word 2013 for documenting the entire study, vulnerability assessment and penetration testing tools to test and notify what type of web vulnerabilities are the website faced. In addition, the scanner tools helps to identify vulnerabilities based on their security level. The third tool is snipping tool, which helps to screenshot the results that the scanners provides. The development environment is windows eight operating system. Scanners are developed both in Linux and windows operating systems. We will see in details about the scanners or security testing tools.

#### **4.2. Research Approach**

Based on the aim or objective of the research, the types of approach that we are going to use exploratory type of research approach. Because the result of the website should be explained briefly. In this document we are going to list the exploits which makes the websites unsecured and what type of security mechanism is good to protect those exploits. In addition to the exploratory approach, we can have a case study as a second approach. According to the results which are reported by the web vulnerability scanners, we are defining the corresponding problems which are open for the attackers.

### **4.3. Research Strategy**

In order to address the aim of this research, the researcher uses different sides in order to obtain issues of security. There are different strategies which help to satisfy the objective of our study. The security evaluation of e-Governmental websites performed by automated tools. So the main research strategy is carry out vulnerability assessment tools to find the real picture of the existing security level of e-Government websites. The results which are produced by the automated tools are accurate. This leads us to reach on the correct conclusion. So, for this study the experimental research strategy is applied.

### **4.4. Assessing Websites**

As we defined before, the vital objective of this paper is, to assess or evaluate the security of the Ethiopian e-Governmental websites. While the assessment is performing using automatic security testing tools, sometimes they are called vulnerability assessment and penetration testing tools. At the same time we test two Turkish websites so that we can compare the security strength of the Turkish along with the developing country (Ethiopian) websites. In addition, we are going to compare the tools or scanners based on their scanning result.

According to the methodology that we used, we will summarize the results in both table and graph form. Because the research methodology for this study is quantitative research approach.

### **4.5. Tool Selection**

Testing can be executed by both manually and automatically. Now, the next task that we are going to do is, selecting automated web vulnerability scanner which helps to detect available vulnerabilities from the tested website. There are different both commercial and open source web vulnerable scanners that allow to detect vulnerabilities. Here we use both of them and the commercial scanners have trial version. So by taking this trial as an advantage, we are going to test the selected websites automatically.

The tools that we are going to use for the testing are: Acunetix web vulnerability scanner, Vega scanner and NetSparker web vulnerability scanners. Both Acunetix and Net Sparker

scanners are commercial web vulnerable scanners and we are using the trial versions for those two scanners. The reason why we choose those scanners is that they are preferable to detect the most widely available vulnerabilities like SQL Injection and cross site scripting vulnerabilities. Those vulnerabilities are the most important attacks for hackers to crack the website easily. Vega web vulnerable scanner is a free or pen software which helps to detect the most known web vulnerabilities. It is one of the web penetration testing tool and it provides graphical user interface (GUI) for testers.

#### **4.5.1. NetSparker**

NetSparker vulnerability assessment tool is the world's best scanner which detects more vulnerabilities including SQL Injection and XSS. It is an automated commercial vulnerability scanner, which is configured fully and provides a trial version. In addition, it affords the results in read only format so that the exploits will be registered safely.

NetSparker has GUI which helps the testers to interact easily. Allows the users to import and export saved scanning results. At the same time it can work with other website security scanning tools. This scanner identifies vulnerabilities like Local SQL Injection, XSS, File Inclusion and Command or Shell Injection. Based on the damage they bring and their urgency of fixing, vulnerabilities are assigned for a specific level or severity. There are three vulnerability severities or levels, important or critical, medium and low level vulnerabilities. SQL Injection and XSS are categorized under important or critical level or severity.

According to the owner of NetSparker, the scanner is developed to help web designers to develop a secure website and helps them not to worry about the safety after the developed website is deployed. So, the main aim of NetSparker is helping the website developers to secure their websites before and after the deployment. Because, it can scan any types of web applications or services in accurate and precise way.

#### **4.5.2. Acunetix**

Acunetix vulnerability scanner is a commercial web vulnerability scanner. It is mostly known by detecting SQL Injection, XSS and most well-known website vulnerabilities. Like NetSparker, Acunetix is an automated web vulnerability scanner, which provides GUI to make the interaction too simple and easy. It provides vulnerabilities as the final results in

pdf format with their level or severity. It affords a trial version with almost full configuration and application.

It is helpful for website developers and the owner of the websites, because like NetSparker it allows to identify the existing vulnerabilities before deploying them. It reduces the risk for the developer, the owner and the user of the websites. This is why the company develops Acunetix.

There is a space which allows testers to put the URL of the website that they want to test, then the scanner starts scanning and provides the result in pdf format. So that the tester will understand what is happening on the website. Based on the result, the tester improves the security of the website. Like NetSparker, Acunetix identifies and categorizes vulnerabilities in different severities or levels. There are three severities, High, Medium and Low severity vulnerabilities.

#### **4.5.3. Vega**

Vega is a well-known web vulnerability scanner, which is free and open source. Unlike the first two web vulnerable scanners, Vega is a non-commercial penetrating testing tool. In addition to this, it is an automated testing tool that searches and finds vulnerabilities in each page of the website.

Like the above two vulnerability scanners, Vega identifies and categorizes the vulnerabilities in various severities or levels. They are, High, Medium and Low severity vulnerabilities. SQL Injection and XSS are categorized under the high level or severity. The scanner detects common OWSAP vulnerabilities that websites will be exploited.

Unlike the first two scanners, Vega do not provide results in pdf format rather the tester uses a snipping tool to screenshot the final result. Vega stores all information which is scanned before or which is scanning currently in workspaces. The way to scan a website is similar to that of the first two scanners. There is a space which allows the tester to insert the URL of the website which is going to be tested.

#### **4.6.Sampling Design**

We try to say something about Ethiopia in the first chapter. Though, here we are going to describe Ethiopia in some details. My country Ethiopia is found in the eastern part of Africa. Ethiopia is the only country which have never been colonized during the period of colonization. All African countries represents Ethiopia as a “symbol of freedom”. The first battle was held in northern part of Ethiopia which is called “Adwa”. After defeating Italy, most African countries copies the flag of Ethiopia. Some countries which uses Ethiopian flag in a little modification are Senegal, Ghana and Zimbabwe.

Ethiopia is well-known in the export of coffee and flower to the rest of the world. The country’s foreign income is from coffee. Next to Brazil, Ethiopia is the country which sells coffee in an international level with a high quality and quantity. This makes Ethiopia different from other African countries.

Now a days, Ethiopia is structured in the federal and regional level because, Ethiopia is governed in federalism structure. To make the administrating system simple, politicians choses a federalism structure. Due to this type of structure, there are about sixty (60) websites

in Ethiopia, both in federal and regional level. But, most of the websites are not working properly inline for different network or server problems. So for this study, about 11 e-Governmental websites are tested and their result is expressed in terms of table and chart. Here we use the non-probability sampling technique to select the working websites. On this research the number of sample size is 14 e-Governmental websites.

In Ethiopia, universities are belongs to the Ethiopian government. From those, we select the three the most well-known big universities. We select the three universities because, if they are not secured, then we can concludes that the whole universities are not secured. Because, like the other universities those universities allows students to see their grades online. In addition the layout and the design of universities website is almost the same.

**Table 4.1:** Name of the organization with their URL

<b>No.</b>	<b>Name of Ethiopian and Tukey websites</b>	<b>Company Name</b>
<b>1</b>	moe.gov.et	Ministry of education
<b>2</b>	moh.gov.et	Ministry of health
<b>3</b>	neaea.gov.et	National Educational Assessment and Evaluation Agency
<b>4</b>	ethiopianairlines.com	Ethiopian Airlines
<b>5</b>	ethiotelecom.et	Ethiopian Telecommunication
<b>6</b>	most.gov.et	Ministry of Science and Technology
<b>7</b>	nbe.gov.et	National Bank of Ethiopia



<b>8</b>	dbe.gov.et	Development Bank of Ethiopia
<b>9</b>	aaau.edu.et	Addis Ababa university
<b>10</b>	bdu.aau.edu.et	Bahir dar University
<b>11</b>	ddu.edu.et	Dire dawa University
<b>12</b>	tuba.gov.tr	Turkish Academy of Science
<b>13</b>	meb.gov.tr	Ministry of National Education
<b>14</b>	mfa.gov.tr	Ministry of Foreign Affairs

---

## **CHAPTER 5**

### **WEBSITE EVALUATION AND RESULTS**

As its name indicates, this chapter includes the way how the evaluation or the testing of Ethiopian e-governmental websites executed and what the final result is going to be. As we describe about the tools which we are selected, we used those tools to measure the security of the Ethiopian e-Governmental websites. The scanners displays the final report of my country websites and turkey websites. Whatever the level of the vulnerabilities differs, most websites are vulnerable for different vulnerabilities.

#### **5.1.Procedures of Web Security Evaluation**

The testing of a website starts with the functional testing of the website. This is the first step during the testing process. The second testing process is usability testing of the website. And then interface testing, compatibility testing and performance testing. Finally, security testing

is taking place. The website is deployed after passing those steps. But, there is still a security problem. The scanning will take more than a day, based on the number of pages in the website.

The procedures to test the security of a certain website is, selecting scanner from the globe which can detect more vulnerabilities. Next, choose the website to be tested. After selecting the websites which are going to be tested, write the URL of the site in the space provided. The next task is given to the scanner, it detects vulnerabilities that the website faced or exploited. After the testing completed, the scanner allows to download the final result. This is the procedure to test the secureness of the website.

## 5.2. Result on NetSparker

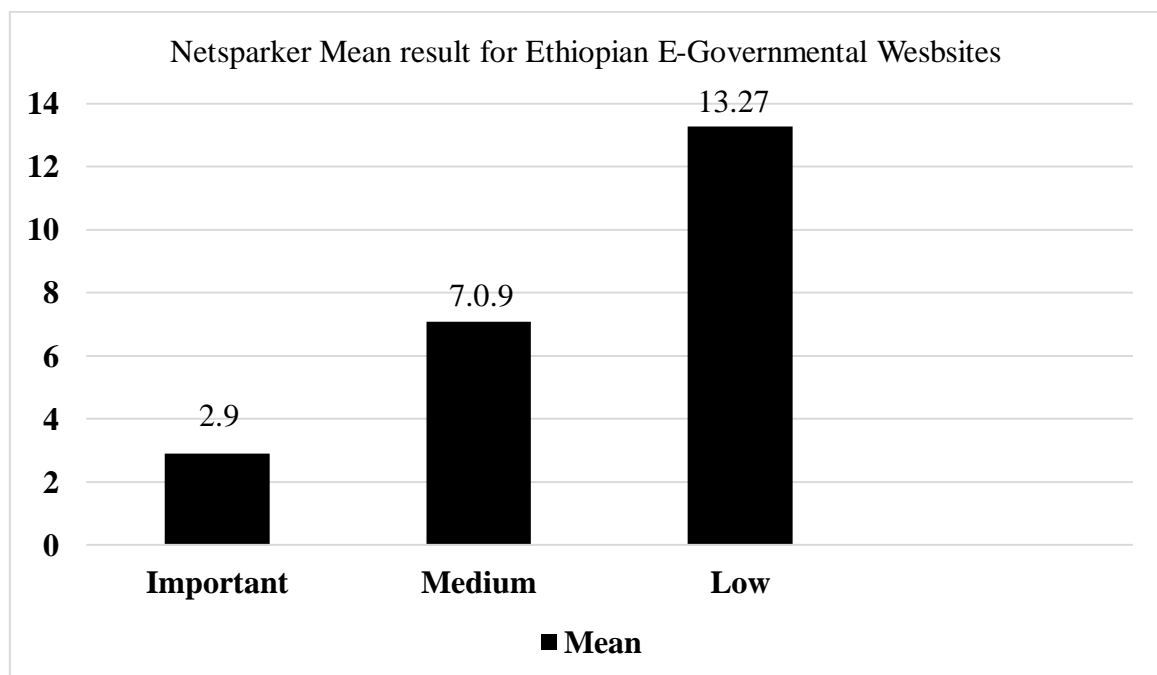
According to NetSparker, the following results have been reported and presented in the form of table.

**Table 5.2:** Result of NetSparker VAPT for Ethiopian websites

No.	Address of the website	Total number of severity risks			
		Important	Medium	Low	Average
1	Moe.gov.et	1	9	12	7.33
2	Moh.gov.et	1	7	53	20.33
3	nbe.gov.et	15	1	12	9.33
4	Ethiopianairlines.com	0	0	4	1.33
5	Ethiotelecom.et	0	4	10	4.67
6	Most.gov.et	1	3	8	4
7	dbe.gov.et	3	6	15	8
8	Aau.edu.et	3	2	9	4.67

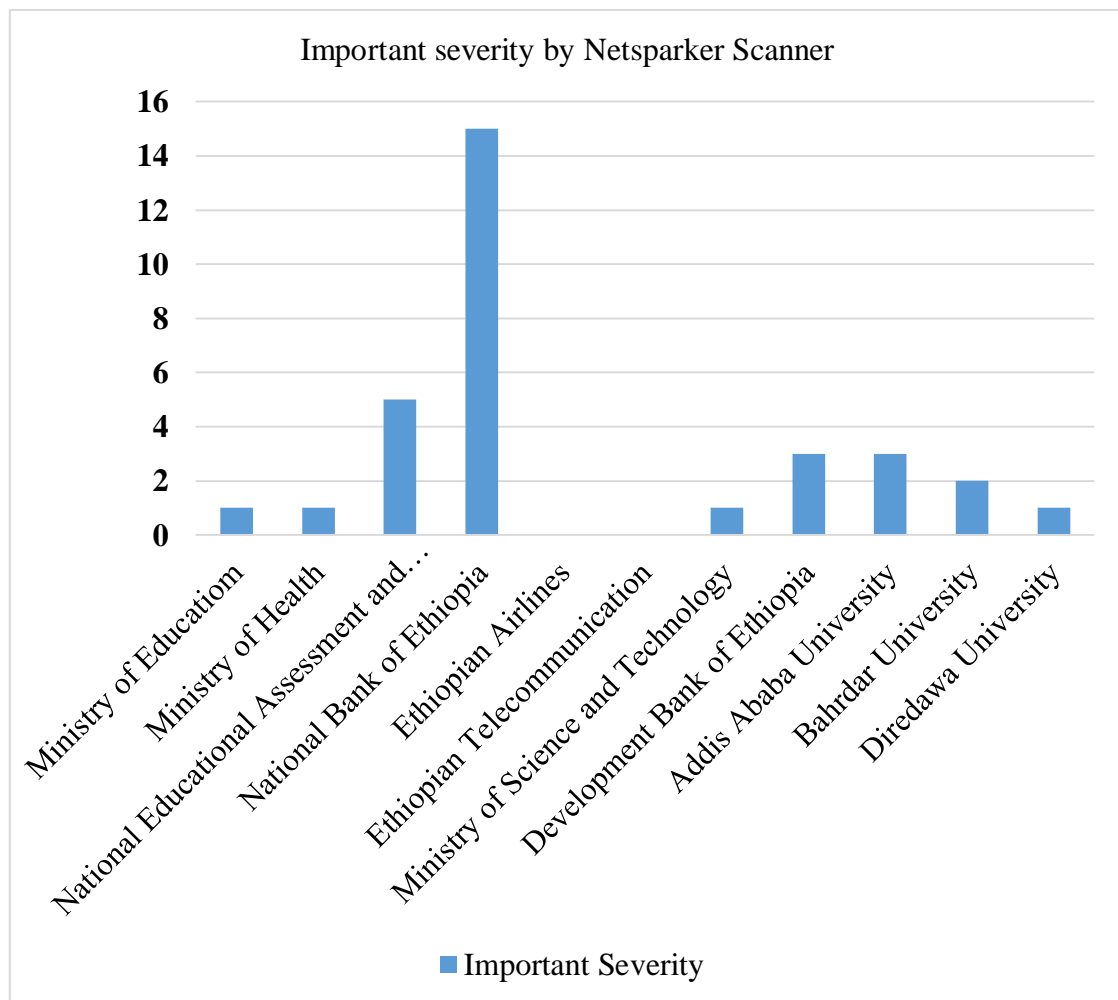
9	Bdu.edu.et	2	2	12	5.33
10	Ddu.edu.et	1	0	3	1.33
11	neaea.gov.et	5	44	8	19
<b>Total</b>		<b>32</b>	<b>78</b>	<b>146</b>	
<b>Mean</b>		<b>2.9</b>	<b>7.09</b>	<b>13.27</b>	

Important Vulnerabilities are vulnerabilities which the organization should fix immediately. Because the attacker could use those vulnerabilities to attack the website. So, those vulnerabilities should be eliminated from the website. To check whether they are eliminated, there will be a rescan so that, websites will be free from any danger. Medium vulnerabilities are bad, but they are not bad as the important one. Like important vulnerabilities, medium vulnerabilities should fix as soon as possible. Because, attackers can use this opportunity to bring some danger to the website. Low vulnerabilities are vulnerabilities which helps attackers to know about user's username, password and credit cards by the autocomplete of the browsers.



**Figure 5.1:** Result of Net Sparker VAPT for Ethiopian websites

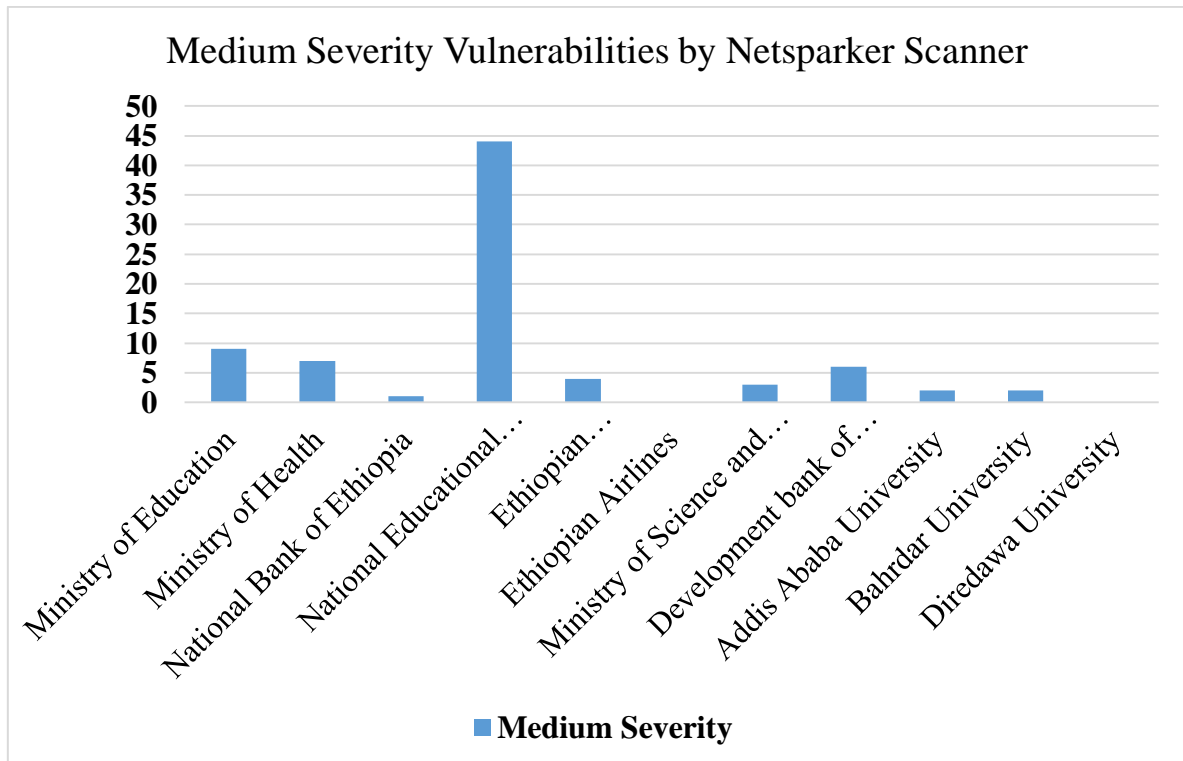
According to the mean result of the websites, almost all of websites are vulnerable to attacks. Except Ethiopian Airlines and Ethiopian Telecommunication. When we compare the security of websites based on the existence of important severity, national bank of Ethiopia is the weaker website. But, it doesn't mean that others are not weak. Based on NetSparker, National bank of Ethiopia is the weakest from others based on numbers of vulnerabilities.



**Figure 5.2:** Important severity of Ethiopian websites

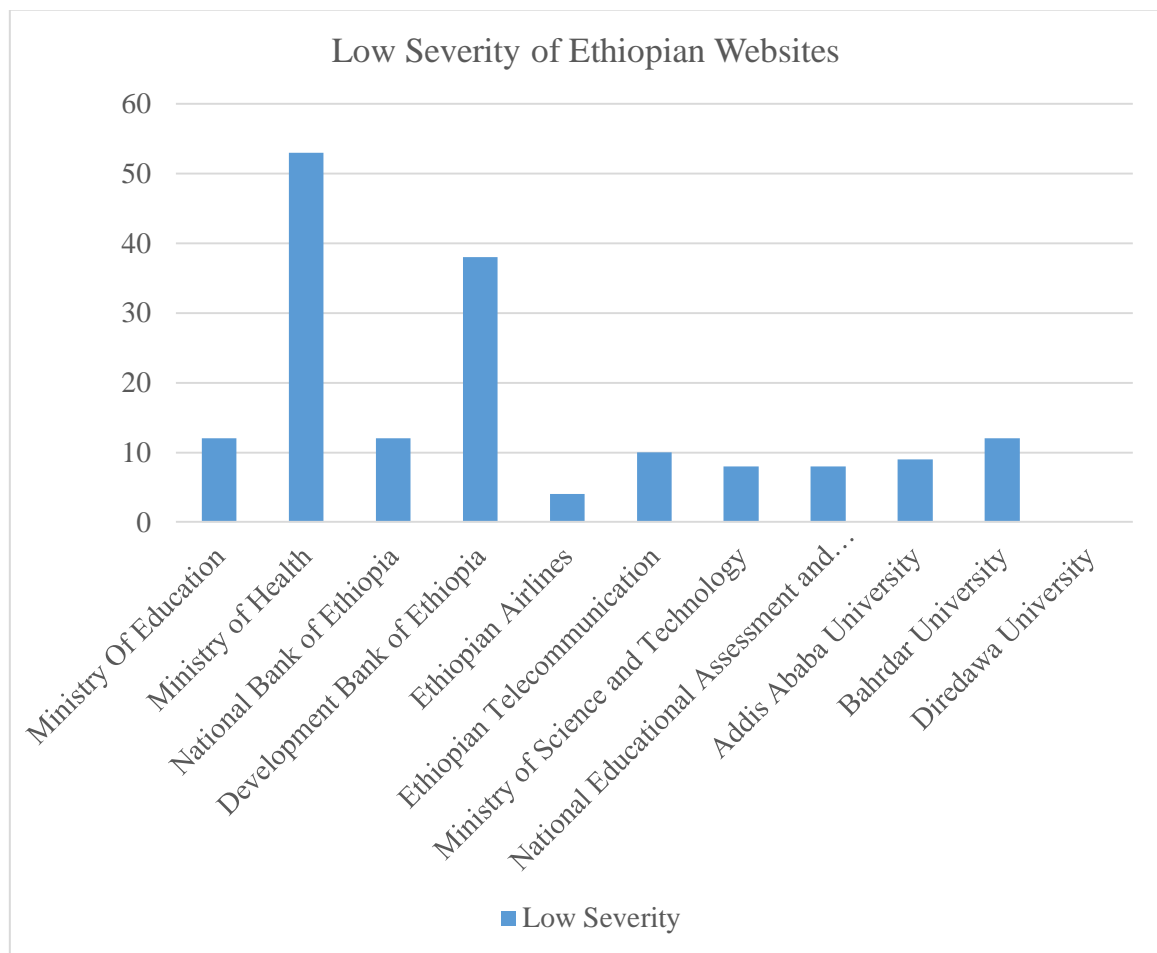
Those vulnerabilities which are categorized under the important level are vulnerabilities, which brings damage to the website in different ways. Those are SQL Injection, XSS, Basic Authorization over HTTP and Password Transmitted over HTTP. According to NetSparker, SQL Injection exists once in Ministry of Education and National Bank of Ethiopia. XSS exists 2 times in National Bank of Ethiopia, once in Addis Ababa University. Password Transmitted over HTTP exists almost all websites except Ethiopian Telecommunication and

Ethiopian Airlines. Basic Authorization over HTTP exists in National Bank of Ethiopia. Out of date version (open SSL) exists in Development bank of Ethiopia. Based on the final result of NetSparker, National Bank of Ethiopia and National Educational Assessment and Examination Agency are more vulnerable for important or high severity vulnerabilities.



**Figure 5.3:** Medium Severity of Ethiopian websites

Those vulnerabilities which are categorized under the medium level are vulnerabilities, which brings damage to the website in different ways. Those vulnerabilities are Possible Source Code Disclosure, Unsecure Transportation Security Protocol Supported (SSLV3), out-of-date version (PHP), out-of-date version (Apache), Weak Ciphers Enabled and Open Redirection. Except Diredawa University and Ethiopian Airlines, all are vulnerable for medium severity vulnerabilities. National Educational Assessment and Examination is vulnerable for such kinds of vulnerabilities.



**Figure 5.4:** Low Severity by NetSparker VAPT

Vulnerabilities which are classified under Low severity are OPTIONS Methods Enabled, Autocomplete, Internal Server Error, Disclosure of Versions (openssl), Version Disclosure (PHP) and TRACE/TRACK Method Enabled. Here, all websites are open for those vulnerabilities. An attacker can use those vulnerabilities to hack and get unauthorized access from those websites.

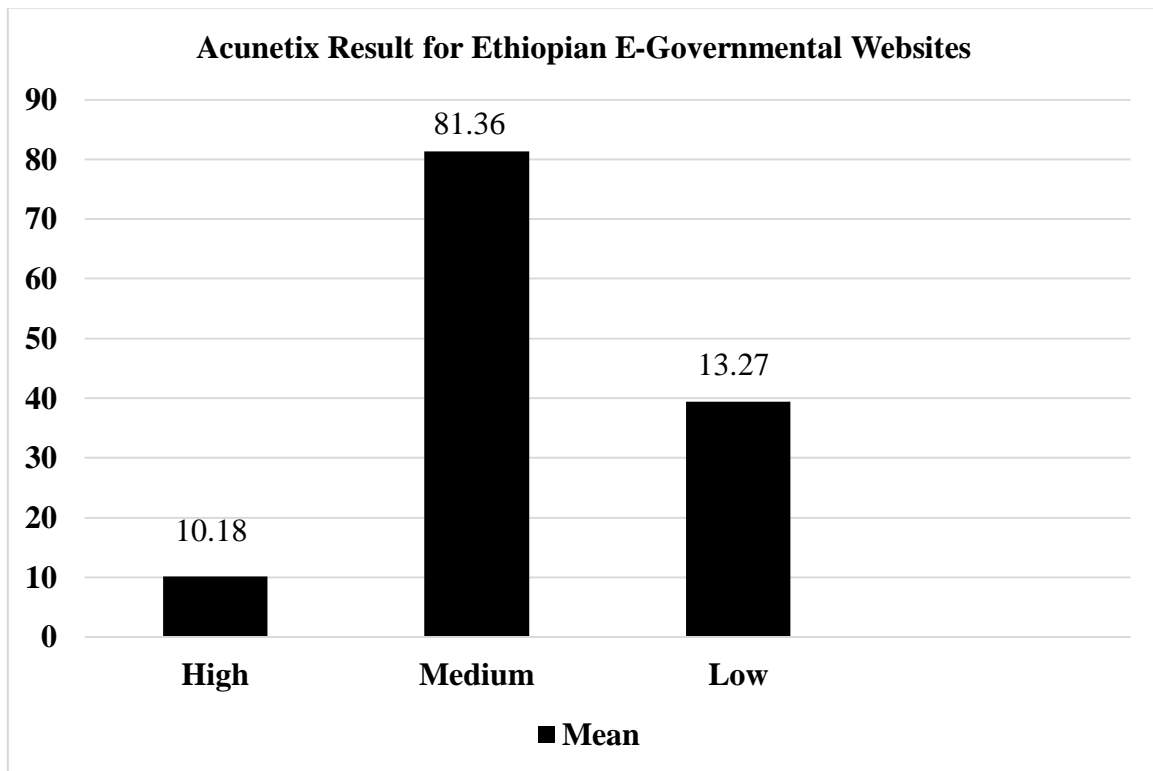
### 5.3.Result on Acunetix scanner

Based on the results of Acunetix web vulnerable scanner, the following results have been produced.

**Table 5.3:** Result of Acunetix VAPT for Ethiopian websites

No.	Name of Website	Total number of severity risks			
		High	Medium	Low	Average
1	moe.gov.et	8	3	7	6
2	moh.gov.et	26	15	4	15
3	neaea.gov.et	3	10	29	22.67
4	nbe.gov.et	1	371	67	146.33
5	ethiopianairlines.com	0	2	3	1.67
6	ethiotelecom.et	9	318	201	176
7	most.gov.et	1	6	13	6.67
8	dbe.gov.et	31	65	38	113.33
9	aau.edu.et	32	1	46	43.67
10	bdu.edu.et	1	3	24	9.33
11	ddu.edu.et	0	1	2	1.67
	<b>Total</b>	<b>112</b>	<b>895</b>	<b>434</b>	
	<b>Mean</b>	<b>10.18</b>	<b>81.36</b>	<b>39.45</b>	

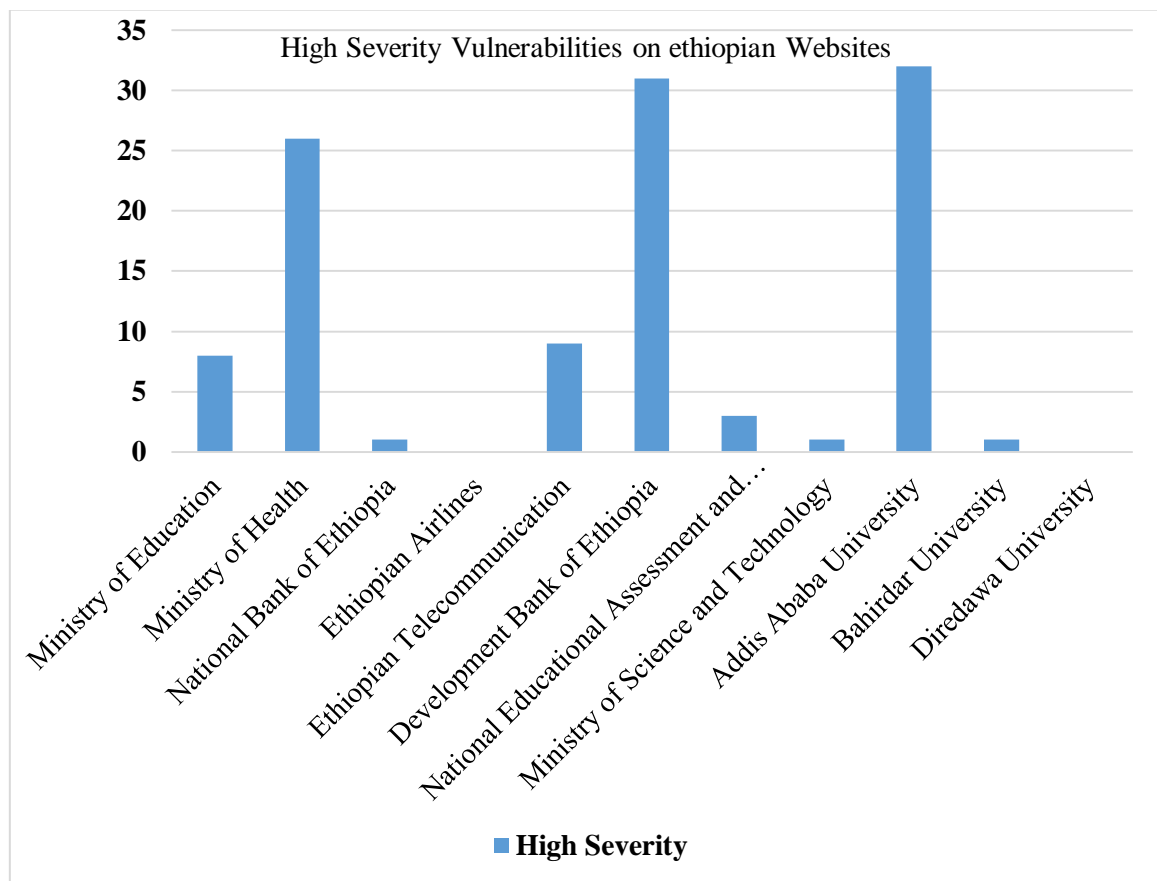
According to Acunetix, High vulnerabilities means the attacker attacks the entire system like the confidentiality, integrity and availability of the website. If the website is vulnerable to those severities, then it is in a big risk or danger. Medium Severities are vulnerabilities that the attacker attacks the website partially. In low severity vulnerabilities, the attackers have a limited effect on the safety of the website.



**Figure 5.5:** Result of Acunetix VAPT for Ethiopian websites

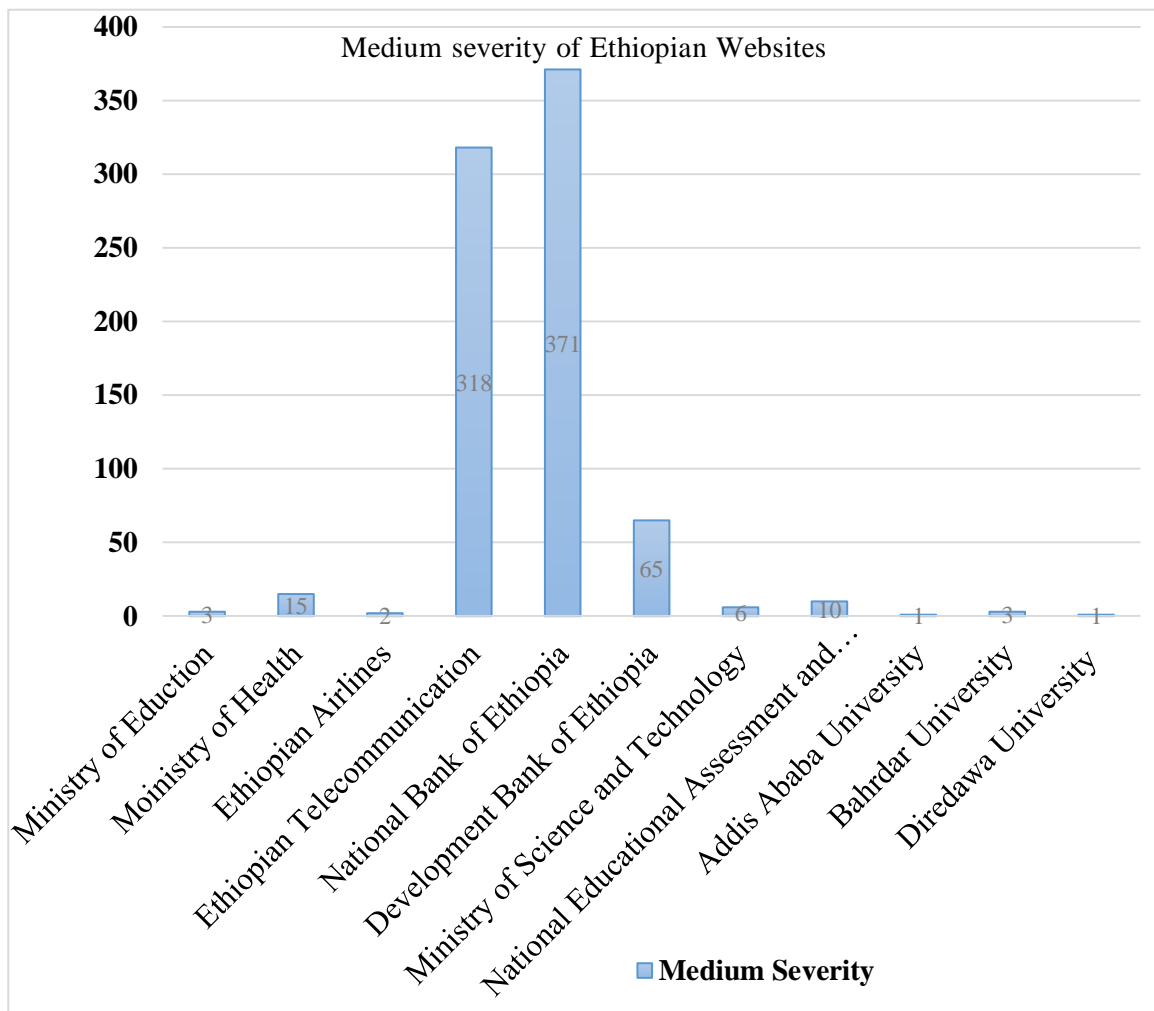
The mean result of Ethiopian websites indicates that, all websites are vulnerable to high, medium and low severity type of vulnerabilities. According to the scanner, Dire Dawa University is the only website which is free from high severity vulnerabilities like XSS and SQL Injection. When comparing most websites are vulnerable to medium severity vulnerabilities. Medium severity vulnerabilities helps attackers to hack and crack the website. Based on the mean result of Acunetix, Ethiopian websites are not safe which means they need an immediate fixing.





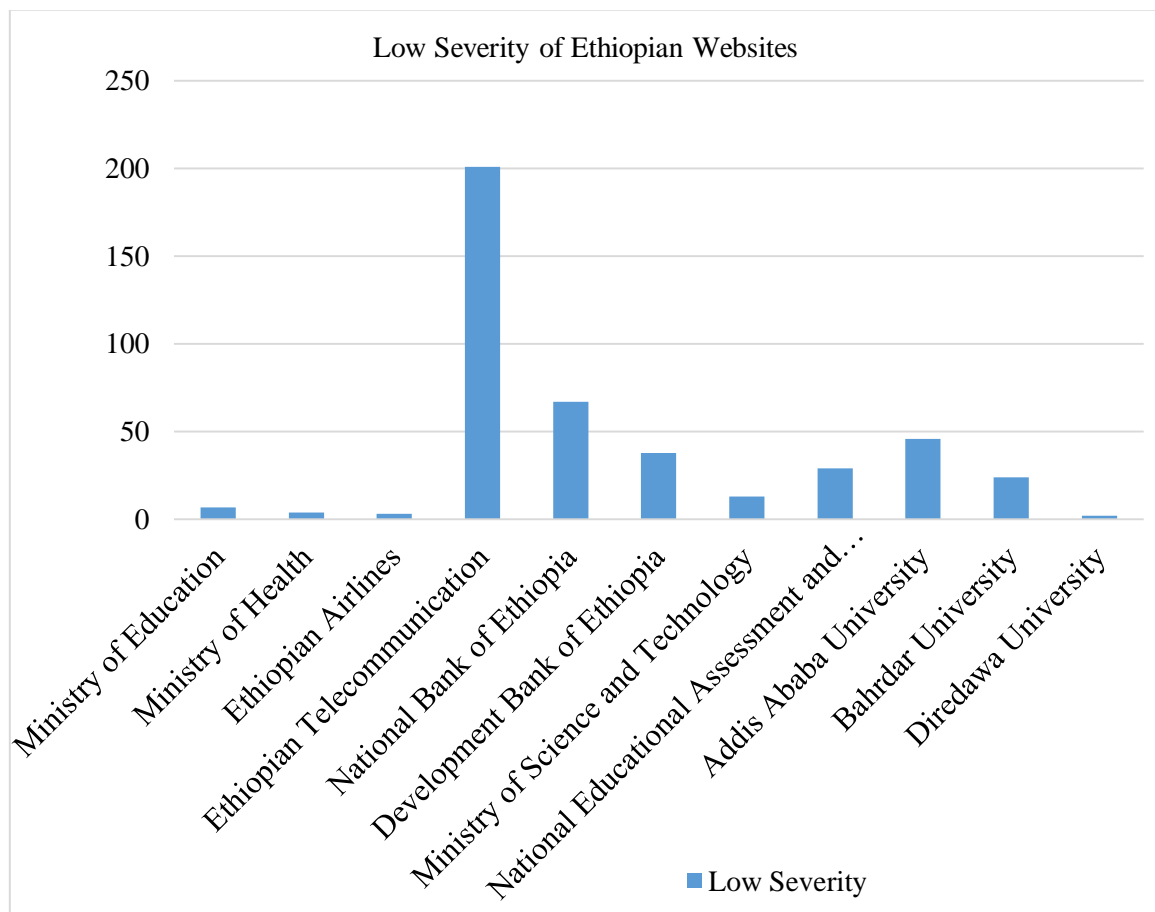
**Figure 5.6:** High Severity of Ethiopian Websites

Vulnerabilities which are classified under high severity vulnerability according to Acunetix are described below. Apache Struts2 Remote Command Execution (S2-052), Session Fixation, XSS, SQL Injection, WordPress 4.9.x Multiple Vulnerabilities (4.9 - 4.9.8), WordPress Plugin Smush Image Compression and Optimization Multiple Vulnerabilities (2.9.1), WordPress Plugin Yoast SEO Possible Remote Code Execution (9.1.0), WordPress Directory Traversal (3.7 - 5.0.3), WordPress 5.0.x Cross-Site Request Forgery (5.0 - 5.0.3). If the website is vulnerable one of those vulnerabilities, then this website is open for attackers. The website needs an immediate fixing in order to be not harmed. The scanner detects 30 XSS vulnerabilities from Addis Ababa University and it is the most XSS vulnerability from the other websites. SQL Injection results detected by the scanner are: 1 from National Bank of Ethiopia, 3 from Development bank of Ethiopia.



**Figure 5.7:** Medium severity by Acunetix

Vulnerabilities which are categorized under Medium severity are: HTML form without CSRF protection, Error message on page, Basic Authentication over HTTP, WordPress XML-RPC authentication brute force, the shifting from HTTP to HTTPS is not fully secured, the identification or identity of the users are transferred as a normal text. All websites are vulnerable for each medium exploits according to the scanner. 318 medium vulnerabilities are detected by the scanner from Ethiopian Telecommunication. The scanner detects



**Figure 5.8:** Low Severity by Acunetix VAPT

Vulnerabilities that are categorized under Low level or low severity are those which have a little impact on the security of the website. These vulnerabilities helps attackers in one or another way to crack or hack websites. All websites which are tested or scanned by this scanner has one or more low severity vulnerabilities. Those vulnerabilities are TRACE Method Enabled, Cookie without secure flag, Possible Sensitive Directories, OPTIONS Method Enabled, Possible Sensitive Files and Documentation File. According to Acunetix web vulnerable scanner, all websites are vulnerable for low severity vulnerabilities. Based on the result that we gathered, Ethiopian Telecommunication is vulnerable for those exploits, more than 148 Documentation File have been detected. All websites are vulnerable for Possible Sensitive Directories.

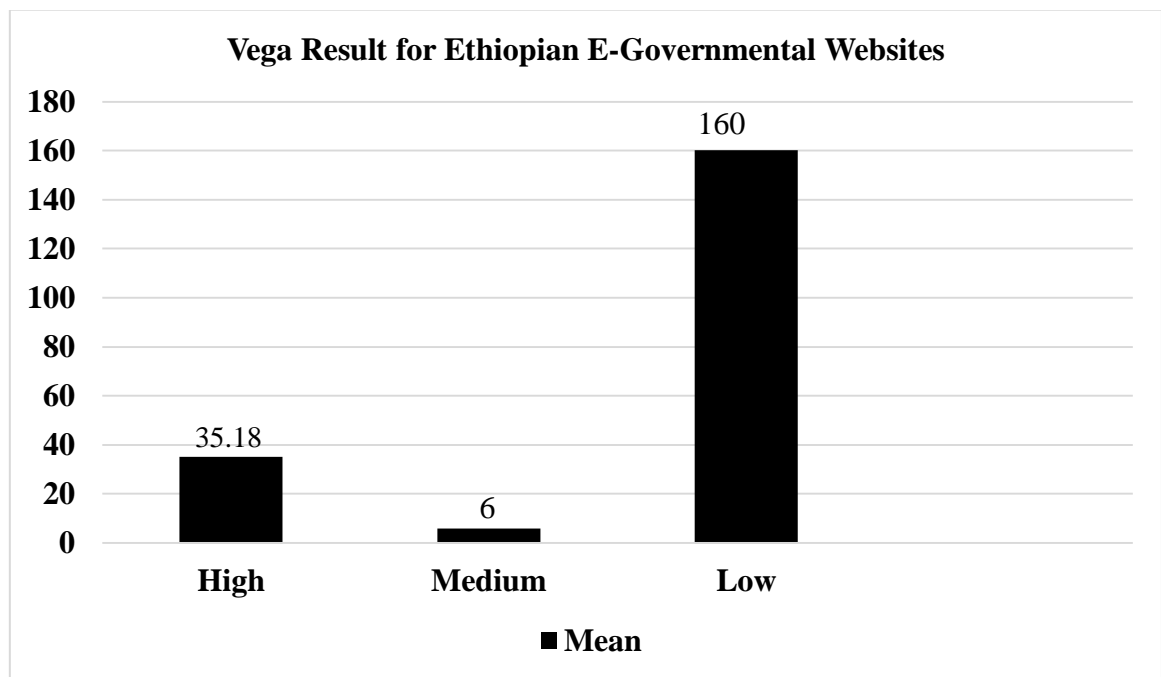
#### 5.4.Result on Vega Scanner

The following results have been prepared based on the reports of Vega scanner. The number of vulnerabilities which are detected on the websites have been expressed as follows.

**Table 5.3:** Result of Vega scanner with the mean of the websites

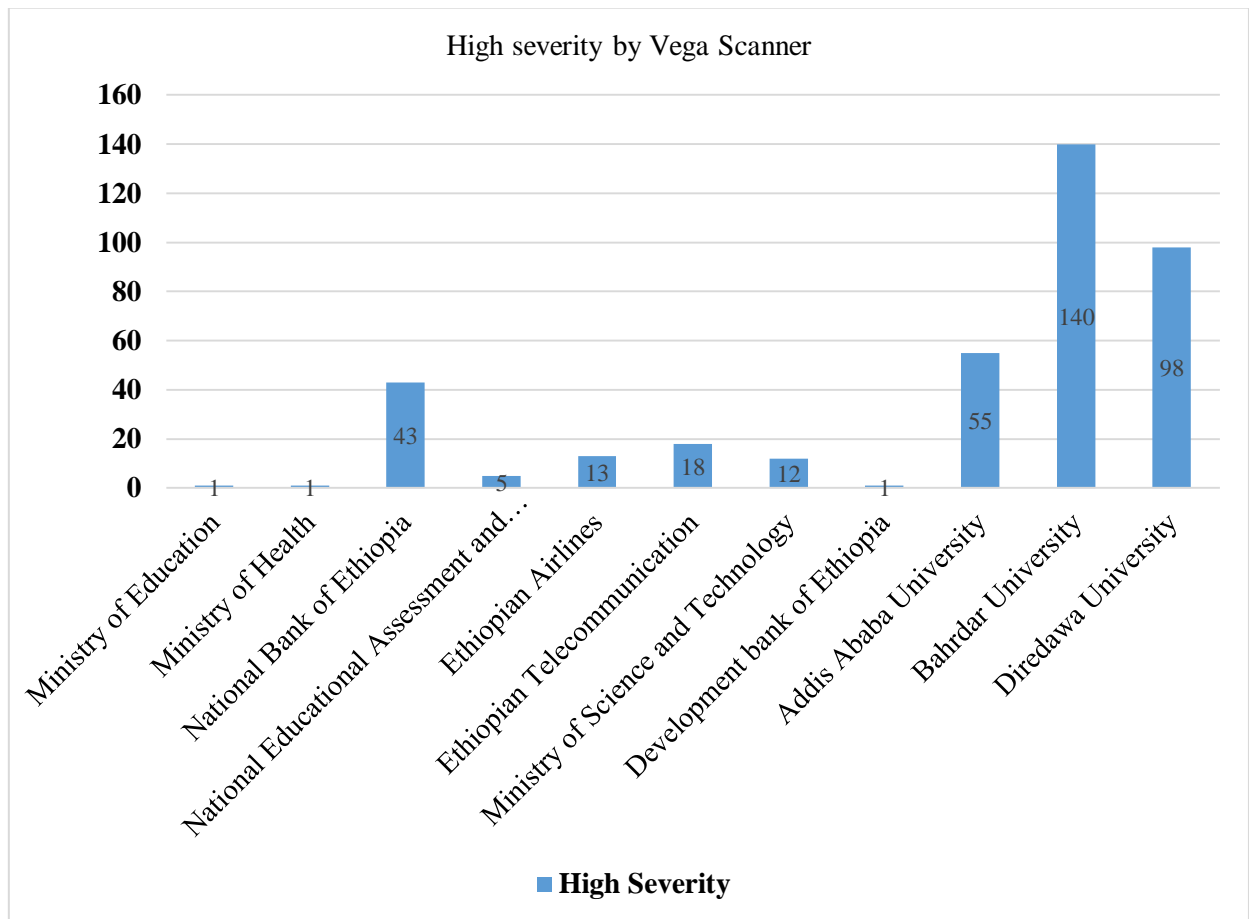
No.	Address of the website	Total number of severity risks			
		High	Medium	Low	Average
1	moe.gov.et	1	0	0	0.33
2	moh.gov.et	1	0	0	0.33
3	dbe.gov.et	1	23	391	415
4	ethiopianairlines.com	13	4	66	83
5	ethiotelecom.et	18	5	87	110
6	most.gov.et	12	6	24	42
7	nbe.gov.et	43	5	204	252
8	neaea.gov.et	5	4	20	8.67
9	aaau.edu.et	55	13	236	304
10	bdu.edu.et	140	3	706	849
11	ddu.edu.et	98	3	29	130
	<b>Total</b>	<b>387</b>	<b>66</b>	<b>1763</b>	
	<b>Mean</b>	<b>35.18</b>	<b>6</b>	<b>160.2</b>	

The above table includes the number of vulnerabilities that are exist in the website, their average and the mean result of Ethiopian E-Governmental websites. According to Vega scanner, High severity vulnerabilities are vulnerabilities which allows attackers to crack the websites easily. Medium severity vulnerabilities are helpful for attackers, guides how to crack the website. But, they are not as dangerous as high severities. Low severity vulnerabilities have an impact on the security of the website but the hardness decreases as we go from high level to low level.



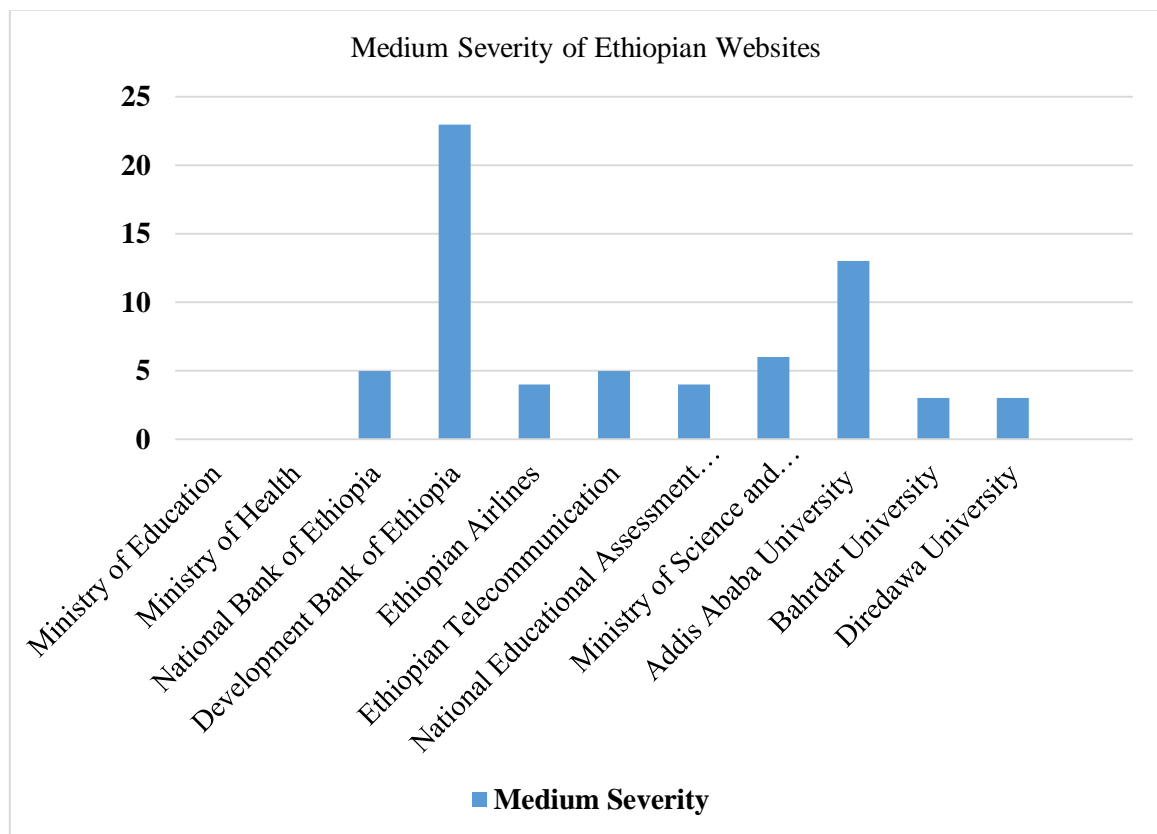
**Figure 5.9:** Vega result of Ethiopian E-Governmental Websites

Based on the mean result of the websites, the above chart have been produced. As we see, Vega vulnerability scanner detects too many high severity vulnerabilities than the other scanners. The scanner detects 160 low severity vulnerabilities, 6 medium severity vulnerability and 35.18 Severity vulnerability of each websites. This result is the best result than the above two scanners. Because it detects more high level severity vulnerabilities.



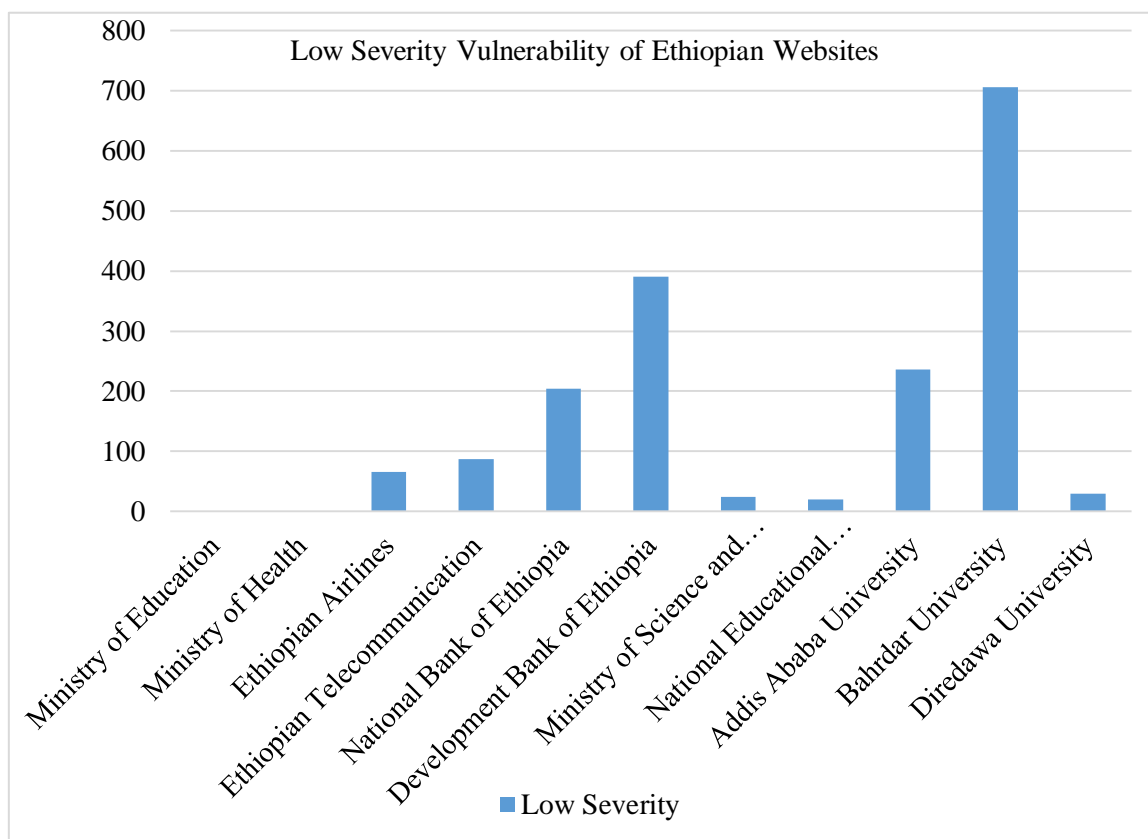
**Figure 5.10:** Vega High Severity of Ethiopian E-Governmental Websites

Vulnerabilities which are categorized under high severity based on Vega scanner are described below. SQL Injection, XSS, cleartext Password over HTTP, the cookie is available without its flag of security, shell injection and HTTP Authentication Over unencrypted HTTP. According to Vega, every websites are vulnerable to the above vulnerabilities. The scanner detects 32 XSS vulnerabilities from National Bank of Ethiopia, 1 XSS from Development bank of Ethiopia, 3 from Ethiopian Airlines, 6 XSS from Addis Ababa University, 5 from Diredawa University. The scanner detects SQL Injection vulnerabilities, 1 from National Bank of Ethiopia, 1 from Development bank of Ethiopia, 5 from Ministry of Science and Technology, 3 from National Educational Assessment and Examination Agency, 9 from Ethiopian Telecommunication, 4 from Addis Ababa University and 11 from Diredawa University



**Figure 5.11:** Vega Medium Severity of Ethiopian E-Governmental Websites

Vulnerabilities which are classified as medium severities are listed below with their corresponding number of Occurrence. Local Filesystem Path Found, HTTP Trace Support Detected, Java Debug Output Detected and Possible HTTP Put File upload. Vega detects Local Filesystem Paths from National Bank of Ethiopia, Bahrdar University, Addis Ababa University, Ethiopian Telecommunication, Development Bank of Ethiopia, Ministry of Science and Technology, National Educational Assessment and Examination Agency. In addition scanner detects HTTP Trace support from Bahrdar University, Development Bank of Ethiopia, Ethiopian Telecommunication, Ethiopian Airlines, National Educational Assessment and Examination Agency, Development Bank of Ethiopia and Diredawa University. Except Ministry of Education and Ministry of Health are free from medium severity vulnerabilities.



**Figure 5.12:** Low Severity by Vega VAPT

Type of vulnerabilities which are categorized under low level severity are explained here. Low severities Vega detects are Form Password Field with Autocomplete Enabled, Internal Address Found and Directory Listing Enabled. Almost All Ethiopian Governmental Websites are vulnerable to all Low level vulnerabilities except Ministry of Education and Ministry of Health. The scanner detects 391 low severity vulnerabilities from National Bank of Ethiopia, 391 from Development Bank of Ethiopia, 236 from Addis Ababa University and 706 from Bahrdar University.



### 5.5.Result of Some Turkish Websites

We select five Turkish governmental and non-governmental websites to check the security and at the same time we are going to compare Ethiopian websites with those Turkish websites. Ministry of National Education, Turkish Academy of Science, Near East University, Near East Bank and Ministry of Foreign Affairs which are tested to know the vulnerabilities that those websites suffered or faced. The five Turkish websites have been scanned by the three scanners. But only Ministry of National Education was vulnerable for low severity vulnerability (Directory Listing Enabled) by Vega scanner. May be other websites will be vulnerable for some vulnerabilities. But those websites are not vulnerable by those three selected scanners. So here, we conclude that Turkish E-Governmental websites are much better than my country (Ethiopia). My country government should work more on security of their websites to make the customer's information safe.

### 5.6.Tool Comparison

As we have seen before, we use three world's best scanners. Namely Acunetix, NetSparker and Vega VAPT. Based on the results that the scanner produces, we are going to select which scanner is good or which one is bad. SQL Injection and XSS vulnerabilities are the most critical vulnerabilities, so we are going to compare scanners based on tools which detects those vulnerabilities more frequently than the others.

**Table 5.4:** Comparing Scanners based on number of high severity vulnerabilities

Scanner Name	SQL Injection	XSS
NetSparker	5	8
Acunetix	22	42
Vega	25	47

## **CHAPTER 6**

### **CONCLUSION AND FUTURE WORKS**

This chapter describes the decision that the researcher reaches on and some recommendations which should be done in the future in order to reduce the available risks and challenges. Here, the decisions or the conclusions which are made on this paper and their future work are described below in simple and precise words.

#### **6.1.Conclusion**

In this research, we tried to select Ethiopian e-Governmental websites to test their security using vulnerability assessment and penetration. We choose 11 Ethiopian e-Governmental websites and 3 Turkish websites. We use the Turkish websites in order to compare the security result of my country websites with these websites. We use three web vulnerable scanners to test the security of both countries websites; NetSparker, Acunetix and Vega.

Depend on the type of the web vulnerable scanners, the final result is different from one scanner to the other. Due to this, the best scanner which detects more vulnerabilities from Ethiopian websites is Vega vulnerability assessment and penetrating testing tool. Whereas the rest two scanners detect vulnerabilities, but, Vega's final result is best. So, on this research we conclude that Vega's result is good and it is the best scanner.

When we come to the websites, the security of Turkish websites are much better than my country websites. All Ethiopian websites are vulnerable to XSS and SQL Injection vulnerabilities. But, the most vulnerable website is Bahrdar University's website, about 140 high severity vulnerabilities are detected according to the scanner.

Finally, according to the final result of the scanners, we conclude that Ethiopian Governmental companies deployed their websites before they test its security. Due to this, Ethiopian e-Governmental websites are vulnerable for attacks and loss of consumer's information. All of websites should fix their websites as soon as possible. Because, they are at a very high risk.

## **6.2.Future Works**

If Ethiopian websites continues in this situation, it is difficult to get enough number of consumers. Because, consumers needs good security to keep their information in a confidential way. There will not be a continuity for Ethiopian e-Governmental websites. So we recommends the following ideas to make Ethiopian e-Governmental websites secured.

As Ethiopian websites deployed before testing their performance of security, it leads them to different vulnerability problems and they are exposed to attacks. Thus, the recommendation for the future works are; testing the security of the website before deployment should be a necessity or a duty to all of Ethiopian e-Governmental websites. So that, they will be afraid of the punishment and they will test their websites with the available penetration testing scanners. In addition to that, for the future, websites should be developed by a developers who have enough knowledge about securing of websites. If the developers do not have enough knowledge of security, the company must search an expert who have enough or efficient knowledge of securing websites.

## REFERENCES

- Abdullah, H. A.-N. (2011). An Evaluation Framework for Saudi E-Government
- Abu-Dabaseh, F., & Alshammari, E. (2018). Automated Penetration Testing : An Overview. *Computer Science & Information Technology*. doi:10.5121/csit.2018.80610
- Alshehri, M., & Drew, S. (2011). E-government principles: Implementation, advantages and challenges. *International Journal of Electronic Business*, 9(3), 255.doi: 10.1504 /ijeb. 2011. 042545.
- Alsmadi, I., & Shanab, E. A. (2016). E-Government website security concerns and citizens adoption. *Electronic Government, an International Journal*,12(3), 243. doi:10.1504/eg.2016.078417
- Antunes, N., & Vieira, M. (2014). Penetration Testing for Web Services. *Computer*,47(2), 30-36. doi:10.1109/mc.2013.409
- Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010). State of the Art: Automated Black-Box Web Application Vulnerability Testing. *2010 IEEE Symposium on Security and Privacy*. doi:10.1109/sp.2010.27
- E-Spin. (2018, October 24). The Advantages and Disadvantages of E-Government. Retrieved from <https://www.e-spincorp.com/the-advantages-and-disadvantages-of-e-government/>
- FDRE, GTPII. (2011). FDRE, Growth and Transformation Plan I. Addis Ababa, Ethiopia.
- FDRE, GTPII. (2016). FDRE, Growth and Transformation Plan II. Addis Ababa, Ethiopia.
- Fonseca, J., Vieira, M., & Madeira, H. (2007). Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks. *13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*. doi:10.1109/prdc.2007.55
- Gebremedhn, G. (2015). Developing Black Box Web Application Penetration Testing Methodology Using Comparative Criteria. *Universal Access in the Information Society*,1-138. doi:10.1007/s10209-015-0446-8
- Grossman, J. (2012). The State of Website Security. *IEEE Security & Privacy*,10(4), 91-93. doi:10.1109/msp.2012.111

- Hasan, A. M., Meva, D. T., Roy, A. K., & Doshi, J. (2017). Perusal of web application security approach. *2017 International Conference on Intelligent Communication and Computational Techniques (ICCT)*. doi:10.1109/intelcct.2017.8324026
- Ihmouda, R., & Alwi, N. H. (2014). A Comparative Analysis of e-government security frameworks Social-Technical Security Aspect. *International Journal Of Management & Information Technology*, 9(3), 1736-1747. doi:10.24297/ijmit.v9i3.662
- Ismailova, R. (2015). Web site accessibility, usability and security: A survey of government web sites in Kyrgyz Republic. *Universal Access in the Information Society*, 16(1), 257-264. doi:10.1007/s10209-015-0446-8
- Joseph, S. R. (2015). Advantages and disadvantages of E-government implementation: Literature review. Retrieved from [https://www.academia.edu/15331532/Advantages\\_and\\_disadvantages\\_of\\_E-government\\_implementation\\_literature\\_review](https://www.academia.edu/15331532/Advantages_and_disadvantages_of_E-government_implementation_literature_review)
- Kumar, v., Mukerji, B., Butt, I., & Persaud, A. (2007). Factors for Successful E-Government Adoption: a Conceptual Framework
- Lessa, L. (2015, December). Sustainability Framework for E-Government Success: Case of Woredanet Services in Ethiopia. Addis Ababa, Ethiopia
- MCIT-eGovernment. (2011). Ethiopian E-Government Strategy and Implementation Plan. Addis Ababa, Ethiopia
- MCIT-eGovernment. (2016). *Ethiopian E-Government Strategy and Implementation Plan* . Addis Ababa, Ethiopia.
- Mohammed, A and Steve. D, (2010).E-government fundamentals. *IADIS International Conference ICT, Society and Human Beings*.
- Ndou, V. (2004). E-government for developing countries: opportunities and challenges. *The Electronic Journal on Information Systems in Developing Countries* , 1-24.
- OWASP Testing Guide v2. (n.d.). *Testing for Cross site scripting*. Retrieved May 5, 2017, from [https://www.owasp.org/index.php/Testing\\_for\\_Cross\\_site\\_scripting](https://www.owasp.org/index.php/Testing_for_Cross_site_scripting)

- OWASP. (2016, April 26). *Testing for SQL Injection (OTG-INPVAL-005)*. (OWASP Foundation Inc) Retrieved Jun 6, 2017, from [https://www.owasp.org/index.php/Testing\\_for\\_SQL\\_Injection\\_\(OTG-INPVAL-005\)](https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005))
- Pulinat, B. (2011). Delivery models of E-Government.
- Rahman, N., & Eyimaya, E. (n.d.). Home. Retrieved from <http://tryqa.com/what-is-security-testing-in-software/>
- Summerfield, J. (n.d.). Why You Need to Secure Your Website with HTTPS and SSL. Retrieved from <https://www.hsolutions.com/resources/why-you-need-to-secure-your-website/>
- Vieira, M., Antunes, N., & Madeira, H. (2009). Using web security scanners to detect vulnerabilities in web services. *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. doi:10.1109/dsn.2009.5270294
- Vumo, A. P., Spillner, J., & Kopsell, S. (2017). Analysis of Mozambican websites: How do they protect their users? *2017 Information Security for South Africa (ISSA)*. doi:10.1109/issa.2017.8251780
- Yosef, Z. (2018). Usability and Accessibility Model for E-Government Websites in Ethiopia.
- Zhiyuan, F. (2002). E-Government in Digital era: Concept, Practice, and Development. *International Journal of the Computer, the Internet and Management* vol.10, no, 2, 2002, p1-22.

## **APPENDICES**


## APPENDIX 1

### SCREEN SHOTS OF VEGA WEB VULNERABILITY SCANNER

#### Scan Alert Summary

<b>High</b>		(128 found)
Cleartext Password over HTTP	128	
<b>Medium</b>		(3 found)
HTTP Trace Support Detected	1	
Local Filesystem Paths Found	2	
<b>Low</b>		(692 found)
Internal Addresses Found	561	
Form Password Field with Autocomplete Enabled	128	
Directory Listing Detected	3	

**Figure A1.1:** Vega Result for Bahrdar University

Scan Info		
		
Scan Alert Summary		
<b>High</b>		(1 found)
SQL Injection	1	
<b>Medium</b>		(23 found)
HTTP Trace Support Detected	1	
Local Filesystem Paths Found	18	
Possible HTTP PUT File Upload	4	
<b>Low</b>		(498 found)
Internal Addresses Found	458	
Directory Listing Detected	40	

**Figure A1.2:** Development Bank of Ethiopia





### Scan Alert Summary

<b>High</b>		(43 found)
Session Cookie Without Secure Flag	1	
Session Cookie Without HttpOnly Flag	1	
Cleartext Password over HTTP	4	
HTTP Authentication over Unencrypted HTTP	4	
MySQL Error Detected - Possible SQL Injection	1	
Cross Site Scripting	32	
<b>Medium</b>		(5 found)
Local Filesystem Paths Found	4	
Possible Source Code Disclosure	1	
<b>Low</b>		(204 found)
Directory Listing Detected	200	
Form Password Field with Autocomplete Enabled	4	

Figure A1.3: National Bank of Ethiopia






### Scan Alert Summary

<b>High</b>		(5 found)
Session Cookie Without Secure Flag	1	
Session Cookie Without HttpOnly Flag	1	
SQL Injection	3	
<b>Medium</b>		(4 found)
HTTP Trace Support Detected	1	
Local Filesystem Paths Found	3	
<b>Low</b>		(20 found)
Directory Listing Detected	20	

Figure A1.4: National Educational Assessment and examination agency

## Scan Alert Summary

 <b>High</b>	(12 found)
Session Cookie Without Secure Flag	4
SQL Injection	5
Cleartext Password over HTTP	1
Shell Injection	2
 <b>Medium</b>	(6 found)
Local Filesystem Paths Found	5
Java Debug Output Detected	1
 <b>Low</b>	(24 found)
Directory Listing Detected	23
Form Password Field with Autocomplete Enabled	1

**Figure A1.5:** Ministry Of Science and Technology

## APPENDIX 2

### SCREEN SHOTS OF ACUNETIX WEB VULNERABILITY SCANNER

Alert group	Severity	Alert count
Cross site scripting	High	30
WordPress 5.0.x Cross-Site Request Forgery (5.0 - 5.0.3)	High	1
WordPress Directory Traversal (3.7 - 5.0.3)	High	1
HTML form without CSRF protection	Medium	281
Directory listing	Medium	4
Possible sensitive directories	Low	163
Documentation file	Low	3
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Cookie(s) without Secure flag set	Low	1
Login page password-guessing attack	Low	1

**Figure A2.1: Addis Ababa University**

Alert group	Severity	Alert count
WordPress 4.9.x Multiple Vulnerabilities (4.9 - 4.9.8)	High	1
WordPress Plugin Duplicator-WordPress Migration Remote Code Execution (1.2.40)	High	1
WordPress Plugin Smush Image Compression and Optimization Multiple Vulnerabilities (2.9.1)	High	1
WordPress Plugin Yoast SEO Possible Remote Code Execution (9.1.0)	High	1
Directory listing	Medium	2
Credit card number disclosed	Medium	1
HTML form without CSRF protection	Medium	1
Possible sensitive directories	Low	150
Clickjacking: X-Frame-Options header missing	Low	1
OPTIONS method is enabled	Low	1

**Figure A2.2: Ethiopian Telecommunication**

Alert group	Severity	Alert count
SQL injection	High	1
HTML form without CSRF protection	Medium	238
Directory listing	Medium	85
Insecure transition from HTTP to HTTPS in form post	Medium	26
Basic authentication over HTTP	Medium	10
User credentials are sent in clear text	Medium	5
Vulnerable Javascript library	Medium	4
Application error message	Medium	1
Backup files	Medium	1
WordPress XML-RPC authentication brute force	Medium	1
Possible relative path overwrite	Low	30
Possible sensitive directories	Low	23
Possible sensitive files	Low	8
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Cookie(s) without Secure flag set	Low	1
Login page password-guessing attack	Low	1
Possible virtual host found	Low	1
WordPress REST API User Enumeration	Low	1

**Figure A2.3:** National Bank of Ethiopia

Alert group	Severity	Alert count
Drupal Core 7.x Multiple Vulnerabilities (7.0 - 7.61)	High	1
Error message on page	Medium	1
HTML form without CSRF protection	Medium	1
Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28	Medium	1
Documentation file	Low	11
Possible sensitive files	Low	11
Possible virtual host found	Low	1
TRACE method is enabled	Low	1













**Figure A2.4:** Bahrdar University

Total alerts found	189
 High	31
 Medium	65
 Low	38
 Informational	55











**Figure A2.5:** Development Bank of Ethiopia

### APPENDIX 3



















#### SCREEN SHOTS OF NETSPARKER WEB VULNERABILITY SCANNER

Vulnerability	Suggested Action
 Cross-site Scripting	<b>Fix immediately:</b> An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
 Out-of-date Version (Apache)	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.  <b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 [Possible] Source Code Disclosure (PHP)	
 [Possible] Insecure JSONP Endpoint	
 Internal Server Error	
 Missing X-Frame-Options Header	
 OPTIONS Method Enabled	
 [Possible] Cross-site Request Forgery Detected	
 Missing Content-Type Header	
 Version Disclosure (Apache)	
 Cookie Not Marked as HttpOnly	
 [Possible] Internal IP Address Disclosure	










**Figure A3.1:** Addis Ababa University

Vulnerability	Suggested Action
 Password Transmitted over HTTP	<b>Fix immediately:</b> An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
 Version Disclosure (SharePoint)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 [Possible] Cross-site Request Forgery Detected	
 Autocomplete Enabled	
 Missing Content-Type Header	
 [Possible] Internal IP Address Disclosure	
 OPTIONS Method Enabled	
 Internal Server Error	
 Missing X-Frame-Options Header	
 Insecure Frame (External)	






**Figure A3.2:** Ministry of Education

Vulnerability	Suggested Action
 [Probable] SQL Injection	<b>Fix immediately:</b> With these vulnerabilities your website could be hacked right now. You should make it your highest priority to fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
 Permanent Cross-site Scripting	
 Cross-site Scripting	
 Basic Authorization over HTTP	
 Password Transmitted over HTTP	<b>Fix immediately:</b> An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
 Out-of-date Version (jQuery)	
 [Possible] Cross-site Request Forgery Detected	
 Missing X-Frame-Options Header	
 Database Error Message Disclosure	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Cookie Not Marked as HttpOnly	
 OPTIONS Method Enabled	
 [Possible] Backup File Disclosure	
 [Possible] Cross-site Request Forgery in Login Form Detected	
 Insecure Frame (External)	
 Missing Content-Type Header	
 Version Disclosure (PHP)	
 ...	
 ...	

**Figure A3.3:** National Bank of Ethiopia

Vulnerability	Suggested Action
 [Possible] Source Code Disclosure (Generic)	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 OPTIONS Method Enabled	
 TRACE/TRACK Method Detected	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Apache)	
 Missing Content-Type Header	
 [Possible] Cross-site Request Forgery Detected	
 Insecure Frame (External)	
 Version Disclosure (PHP)	
 Missing X-Frame-Options Header	

**Figure N3.4:** National Educational Assessment and Examination Agency

Vulnerability	Suggested Action
 [Possible] Source Code Disclosure (Generic)	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Internal Server Error	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 OPTIONS Method Enabled	
 [Possible] Cross-site Request Forgery Detected	
 [Possible] Internal IP Address Disclosure	

**Figure N3.5:** Ethiopian Telecommunication