Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FORENSIC ANALYSIS AND PREVENT OF CROSS SITE SCRIPTING IN SINGLE VICTIM ATTACK USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP) FRAMEWORK

[1]ADE KURNIAWAN, [2]IMAM RIADI, [3]AHMAD LUTHFI

[1,3]Department of Informatics Engineering, University Islam of Indonesia,Yogyakarta, Indonesia

[2]Department of Information System, Ahmad Dahlan University, Yogyakarta, Indonesia

E-mail: [1]adekurniawanrusdy@gmail.com, [2]imam.riadi@is.uad.ac.id [3]ahmad.luthfi@uii.ac.id

ABSTRACT 1

Internet has changed the world, today almost everyone connected to the Internet indicated the percentage of penetration of internet users in the world is increasing which caused the change in targeted cyberattacks to individual targets. Reported eight of the top ten websites in the world are at a critical point of vulnerability from attacks by injection methods such as Cross Site Scripting and SQL Injection that can be used by certain parties to steal information or for a particular purpose. In this paper the research conducted by three key stages: first Attacking (Single Victim Attack: Information Gathering, Live Webcams Screenshot, Keyloggers and Download Spoofer), second stage Analysis (Digital Forensic: Live Forensic and Analysis Evidence) and third stage to Prevent (Patching). Contribution of this study offers a method of protection solutions to users in the browser application to be filtered, disable the plugin, notifying, blocking, and reducing Cross Site Scripting attacks.

Keywords: *Live Forensic, Cross Site Scripting, OWASP, Xenotix,*

1. INTRODUCTION

Penetration of Internet users in 1995 only 1 percent of the world population and in 2014 the figure had reached 40 percent or 3 billion users, 1 billion websites and the increasing. Alarming number of Cyberattacks to a target individual that continues to grow each year [1]. Symantec Reports [2] entitled Internet Security Threat Report 2015 says the average attack in 2013 reached 568 734 and 496 697 per day in 2014.

Heightened attacks and Cybercrime have finally been made a loss in the business sector, government, communities and individual targets that caused the issue becomes serious attention from Governments, corporations, and the research community [3]. Research results OWASP Top Ten 2013 Most Dangerous Web Vulnerabilities [4] mentions XSS Cross Site Scripting put in third place while the report OWASP 2015 [5] reported a 77 percent vulnerable and 16 percent were classified with a critical point, and according to reports Web Application Security Statistics Report 2016 [6] [7] XSS ranked third.

Cross-site scripting attack is a type of injection attack and a very specific types of attacks against web applications and become the most critical vulnerabilities in web applications today[8] [9]. An attacker injects malicious scripts into web pages trusted as Web applications do not check and filter user input efficiently. When a trusted web page displayed on the user's browser, malicious script is run and steal sensitive user information [10].

Malicious scripts, loss of privacy and theft of sensitive information to the individual targets or certain parties becoming a trend in the Cyber world today, marked with in its release of the OWASP report as has been mentioned above. OWASP Framework is a non-profit institution research community category 501c, OWASP membership comes from the scientists, researchers and the private sector which will issue a report articles, tool / equipment and documents that is Open Source. Using tool OWASP Framework by the security researchers, fueled by the software is open source in comparison with the tools in the market is still

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

relatively expensive, has problems in its use, is not secured with a security system with the latest technology and must specify the XSS payload manually to search vulnerability, exploit an XSS attack site or to a specific target or with the terms Single Victim Attack [11][12].

Single Attack Victim in this study took several methods of attack include: Information Gathering, Live webcams Screenshot, Keylogger, Download spoofer. Single-Victim-Attack can happen to anybody; victims include a President, former chairman of the Joint Chiefs of Staff, celebrities, corporate CEOs [13].

In Single Victim Attack we assuming the victim used Browser Firefox Mozzilla with a social engineering attack method by sending an email phishing. Tool used in performing Single Attack Victim using OWASP Xenotix XSS Exploit Framework v6.2 and for the capture, extraction and analysis of packet traffic using Live Forensic using Wireshark tool and Live HTTP Headers. While on stage Prevent solution, approach is done by make Patching Stages Prevent done by making patching Mozilla Firefox browser in the form of add-on extension with the name XSSFilterAde by providing early warning function, the plugin switched off, restricting, allowing payload / script to the victim when it will open a website address.

2. BASIC THEORY

2.1 Forensics

Forensic meaning of the word is "presenting to the court" while the term "forensics" is derived from the Latin word relating to the law or apply scientific analysis in the context of the law. Digital Forensics is a scientific process or a scientific effort that is based on the science of collecting, analyzing and presenting evidence in a court proceeding to assist the disclosure of a crime through disclosure of evidence authorized by the laws and regulations[4]

Network forensics is a scientific process to identify, analyze and reconstruct the events based on digital evidence from log network [14]. Quality tools, techniques and skills Network Forensics investigator is required due to Cybercrime is increasing and more sophisticated [15]. Network Analyzer tool used by investigators in the search for, identify and analyze the evidence log is Wireshark, Tcpdump and NetworkMiner

2.2 Cross Site Scripting

Cross Site Scripting on show in Figure 1 is one type of injection attack code (code injection attack) carried out by an attacker by entering client code HTML or script code to be loaded into a site [16]. This attack as if it came from the site, as a result of this attack, among others, the attacker can bypass the security on the client side, get sensitive information, or save malicious applications [17].

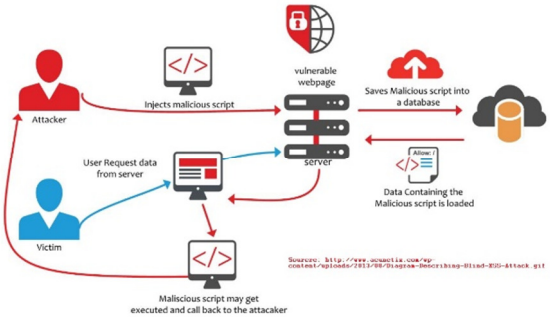

Figure 1 Cross Site Scripting Attacks

Cross-site Scripting can be classified into three main categories:

a. Stored Cross Site Scripting (Persistent). Cross Site Scripting attacks involve an attacker to inject script stored (referred to as payload) are stored permanently (remain) in the target application (eg in a database or web browser). The classic example is stored XSS is a malicious script inserted by an attacker in the comment field on a blog or in a forum post
b. Reflected Cross Site Scripting is an attack by an attacker to send a payload scripts that are part of the request and sent to the Web server and then reflected in such a way that the HTTP response including the payload of an HTTP request.
c. DOM-based Cross Site Scripting. DOM-based Cross Site Scripting is an advanced type of Cross Site Scripting attacks are possible when a Web application from a client-side script to write the user to provide data to the Document Object Model (DOM).

2.3 Single Victim Attack

Single Victim Attack is an attack using social engineering methods that target to a system, device or victim by exploiting the weakness and vulnerability of a system or user devices. Here are four attacks in Single Attack Victim:

1. Information Gathering.
   Information Gathering is to seek, find, collect and utilize the protocol services and critical information used by the victim that one of its firewall, IP, ISP, and the location contained on the target device.[5]
2. Keylogger.
   Keylogger is one kind of spywares, keyloggers functioning steal user information, keeping

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

track of every keystroke keyboard user, and stored in the form of log files. [18]

3. Download Spoofer.
   Download spoofer is an attack in which the attacker pretends to be an authorized service by sending an address to download a file to the victim previously had been infiltrated by malware.
4. Live Webcams Screenshoot.
   Live Webcams Screenshot is an attack in which the attacker take pictures or videos by recording the activity of camera unnoticed by the victim.

2.4 Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) is a non-profit organization that aims to help organizations to develop, purchase, and maintain software applications that can be trusted [19]. OWASP is an open source, has been recognized in various forums where information technology professionals and a network that can build up expertise.

Xenotix OWASP XSS Exploit Framework is an application created by Ajin Abraham for penetration testing, detecting and exploiting Cross Site Scripting vulnerabilities in Web applications [11]. Ajin Abraham build a database of over 5000 payload XSS Cross Site Scripting and apply in VB.NET.

3. METHODOLOGY

Preparation stage starts with the setup of hardware and software that will be used in this study. hardware used in this study is a notebook Processor: Intel (R) Core (TM) i7-6500U CPU @ 2.30GHz, 8GB RAM, 250GB SSD, Intel 530 Graphics Card and application virtual machine (VMware workstation 12) to run the device attacker and server. The operating system used by the attackers was Windows 8.1 and applications to perform Single-Victim -Attack is Xenotix OWASP XSS Exploit Framework v6.2. The operating system used by Victim is Windows 10 and applications for the browser is Mozilla Firefox v49 while for Server using the Windows 8.1 operating system and to run the localhost place to store website and backdoor file is to use XAMPP software v5.6.

Illustration of the Methodology is shown in Figure 2

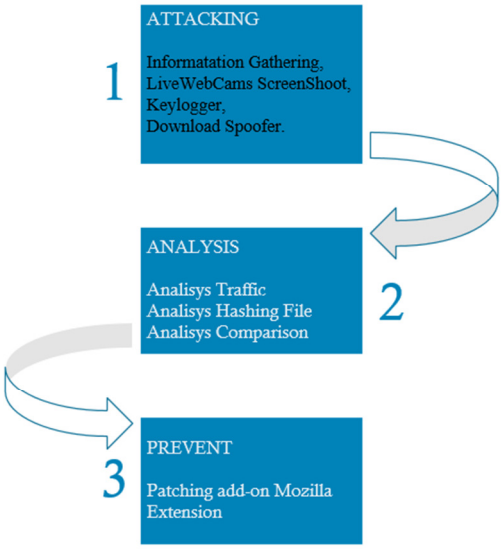

Figure 2. Methodology

Explanation of figure 2 as follows:

3.1 Attacking

Single Attack Victim is a single attack or attacks on various targets in a planned and structured. At Attack Victim single simulation will only be exploited on the Victim with a variety of attack methods including Information Gathering, Live webcams Screenshot, Keylogger, Download spoofer

Stage an attack starts with the preparation stages. Stages of preparation begins with vulnerability scanner, email phishing and Single Attack Victim.

1. Vulnerability Scanner
   Vulnerability is a weakness that can lead to machine can be stopped, modified or taken over by a third party. Vulnerability scanner is the art of using a computer to search for weaknesses in computer security other which allows an attacker to reduce a system's information [20]. Process Vulnerability Scanner is a step process to search, find and exploit weaknesses of a web application by using a particular technique or tool. Tool used in this study using OWASP Xenotix v6, the process of the stages is to inject a Cross Site Scripting Script Payload in a search box on a web.
2. Sending Emails Phishing
   Email Phishing is a form of online identity theft that aims to steal sensitive information such as passwords, credit card information and

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the user's operating system by way of impersonating a legitimate entity [21]. The process of sending phishing emails to the Victim of attackers using social engineering techniques to take advantage of the carelessness that the victim has to get a free quote by clicking a link to the registration offers.

3. Single Victim Attack
   Single Attack Victim process launched by the method of sending malicious payload script. Payload Script used to conduct the attack Single Attack Victim Information Gathering, Keylogger, Download spoofer and Live Webcams Screenshoot generally uses javascript..

3.2 Analysis.

The integrity of digital evidence plays an important role in the process of forensic investigation [22], starting with the appropriate procedures of the stages of how digital evidence is collected, extracted, analyzed, preserved, and presenting to the court. Digital Evidence is some or something extraction of data from electronic evidence became proof digital information with the scientific method, in binary form either stored or sent [23]

Source of digital evidence obtained using Wireshark, HashMyFile and Mozilla extension Live HTTP Headers. Analysis process is divided into three different stages according to the source of digital evidence. The three stages are: Traffic analysis, hashing file Analysis and Comparative Analysis

1. Traffic Analysis.
   Network traffic analysis is the process of recording, reviewing and analyzing network traffic to assess network performance in general and security. Sources in the analysis of digital evidence obtained from traffic header by using Wireshark, add-on extension Live HTTP Headers and for data communication to requests from the attacker, the victim and the server using Wireshark to capture, extraction and analysis
2. Analysis File Hashing
   Source of digital evidence obtained from backdoor-master.zip file downloaded by the victim in the attack and the spoofer Download backdoor.exe file on the server machine.

3.3 Prevent

Prevention solution in the Single Victim Attack on Cross Site Scripting are patching to create an add-on extensions in Mozilla Firefox browser. Patching add-on to Prevent step is providing early warning, disable the plugin, restrict, allow payload / script to the victim when it will open the website address

Mozilla Firefox extension named by XSSFilterAde with three main features. The first feature that allowed while all these pages, a feature that both allow all these pages and features that allow scripts third globally.

4 RESULT

4.1 Simulation Single Victim Attack

In this study we assume the attacker has to know the email of the victim and are in the same network. Simulation of this case is shown in Figure 3 identifies that the attackers IP 192.168.2.245 by email at korbantesis@gmail.com connect in a network shared public place and send a phishing email that has been injected XSS payload using the tool OWASP Xenotix email to victim in adekurniawanrusdy@gmail.com on IP 192.168.2.246.

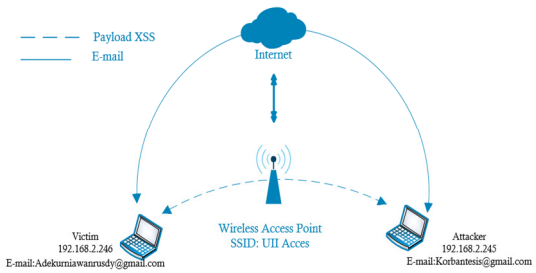

Figure 3. Single Victim Attack Diagram Flow

After the victim received the email and click the link that has been injected with a payload by attackers later stage the attacker attack as shown in Figure 4.

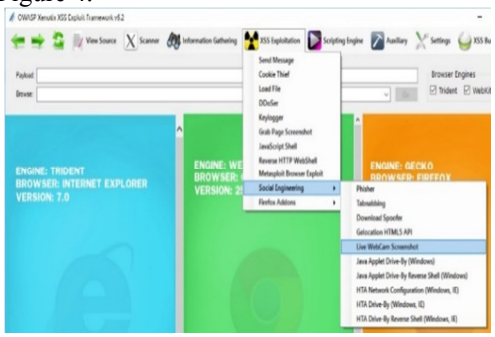

Figure 4. OWASP Xenotix XSS Exploitation

The next steps attacker perform Single Victim Attack with techniques of social

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

engineering, first of all carry out attacks Information Gathering with the intent to steal important information from the victim, and then performed Keylogger by recording every beats keyboard of each input, then launch an attack Download spoofer to the victim for the purpose of downloading a malware and attacks in the last stage is live Webcam Screenshoot which aims to record the activity the victim live streaming. During the attack process traffic data and browsing activities of victims recorded by using Wireshark and Live HTTP Headers.

During the attack process traffic data and browsing activities of victims recorded by using Wireshark and Live HTTP Headers. In Figure 5 shows the result of the Single Victim Attack on show Visitor Information Gathering, Country Code, and State IP, Public IP and ISP.

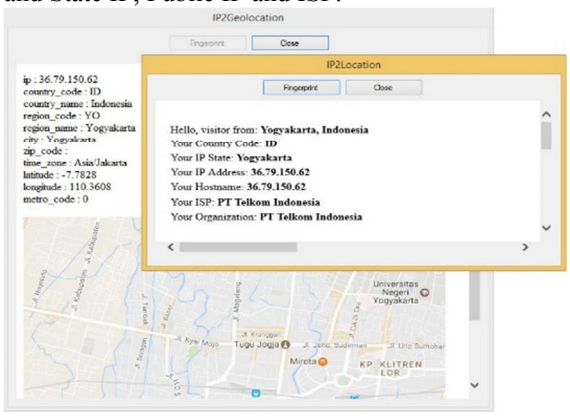

Figure 5. Information Gathering

In Figure 6 shows the result of the Single Victim Attack on the victim showed Keylogger Victim wrote adekurniawanrusdy@gmail.com to log in on Facebook.com and other side of figure 6 as the results of XSS Keylogger.

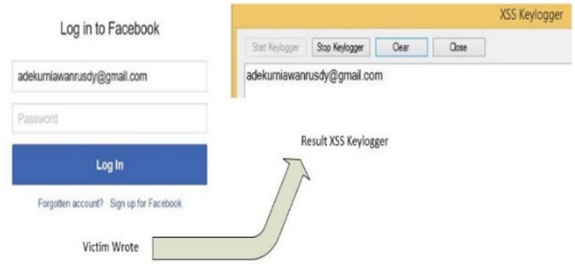

Figure 6. XSS Keylogger

In figure 7 shows the result of the Single Victim Attack on spoofer Download showed the victim to download a file with the name backdoor-master.zip

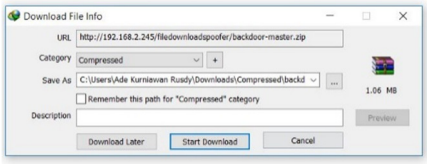

Figure 7. Download Spoofer

In Figure 8 shows the result of the Single Victim Attack on Live Webcam screenshot shows the video of the victim being active.

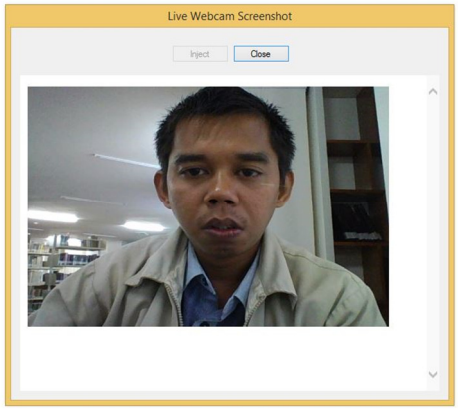

Figure 8. Live Webcam Screenshoot

4.2 Analysis Single Victim Attack

Network Analysis in Information gathering attacks using the Wireshark frame packet 299 and packet frame 373 the packet data traffic sent from Victim to the attacker and the results of the Information Gathering as shown in Figure 9 shows the results that the payload script used by the attacker had made it known. The payload script to force the victim to open a website that is http://freegeoip.net/ with the intention of the attacker will be able to know all the important information from the victim: Public IP, Country, Region, City Zip / Postal cod, Lat / Long, Metro code, Time zone.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

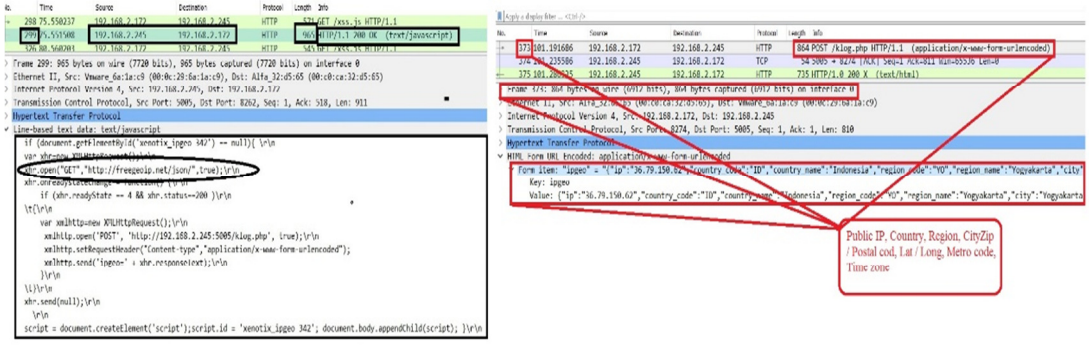

Figure 9. Payload Script Information Gathering and Public IP, Country, Region, CityZip / Postal cod, Lat / Long, Metro code, Time zone

Analysis of the results showed that the payload Keylogger is sent by an attacker with Live Forensics method successfully capture, extract and analysis by Wireshark. Packet Analysis 580 in figure 10 shows the payload sent by an attacker with a file extension HTML5v3.xpi and on the frame packet 311 up to 641 frames of data traffic using the TCP protocol and packet length 60, with a network forensic analysis captured input keys of the victim who wrote "adekurniawanrusdy@gmail.com

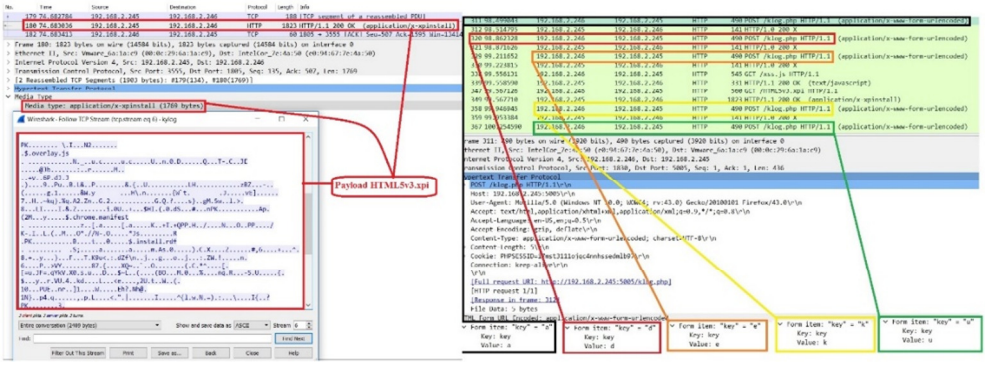

Figure 10. Payload HTML5v3.xpi

Analysis of the results showed that the spoofer Download payload script that is sent by the attacker succeeded in the capture, extract and analysis by Wireshark with Live Forensic methods.

```
Line-based text data: text/javascript
  if (document.getElementById('xenotix_spf 1129') == null){ \r\n
  var w;\r\n
  var or='http://192.168.2.245/filedownloadspoofer/backdoor-master.zip';\r\n
  var fak='http://2.bp.blogspot.com/-Fsxc1F3aIE0/VKkUCWsan-I/AAAAAAAAFqI/1fdqFMGdbYM/s1600/gambar%201ucu%20banget5.gif';\r\n
  function dostuff() {\r\n
    w = window.open(or, 'target');\r\n
    setTimeout(dostuff2, 3500);\r\n
  }\r\n
  function dostuff2() {\r\n
     w.location.replace(fak);\r\n
  }\r\n
  dostuff();\r\n
  script = document.createElement('script');script.id = 'xenotix_spf 1129'; document.body.appendChild(script); }\r\n
```

Figure 11. Two link addresses to trick the victim

Wireshark made the results as shown in Figure 11 describes the attacker used to see the script and two link addresses to trick the victim is fake and the original link link to download the file backdoor-master.zip

Extraction, analysis, and all so Test Data Integrity of file downloads by Wireshark seen in Figure 12 are in the circle with a red square is a stage Backdoor file extraction and yellow circles are comparing the value of the second hash files between files that have been downloaded by Victim with Wireshark file extraction.

Test data integrity of files that have been downloaded by the victim with the files stored on the server is very important done by the digital investigator due to test that the file is authentic. application used to perform hashing file is HashMyfile with MD5 and SHA1 algorithms and used file consists of three files from the file

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

extraction Wireshark, Victim downloaded files and files stored on the server.

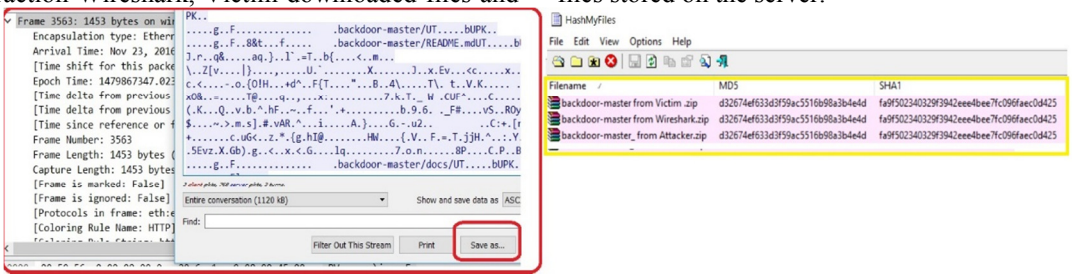

Figure12. Extraction and Hashing of File

Analysis on Live Webcam Screenshot showing the results that the payload that is sent by the attacker succeeded in the capture, extract and analysis by Wireshark with Live Forensics methods. Extraction and analysis using the PCAP file Wireshark which is the show in Figure 13 shows the results that the victim received a packet payload 350 and a script to conduct attacks Live Webcam Screenshoot.

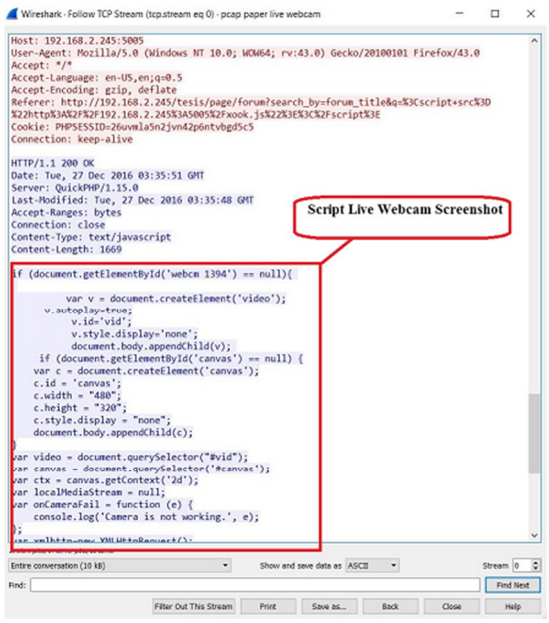

Figure13. Payload Script Live Webcam Screenshoot..

In Figure 13, Wireshark shows the results of analysis of packet 903 describes the payload used by the attackers to attack Live Webcam Screenshoot to take advantage of lax from the victim to click on a link which could consequently activate the camera from the Victim, while in figure 14 describes the data flow results live streaming webcam from the victim to the attacker.

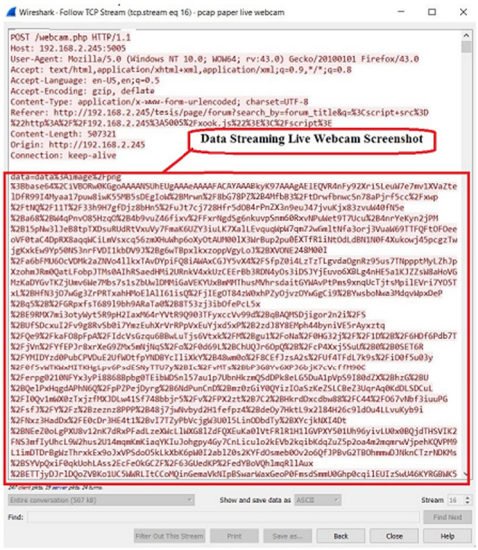

Figure14. Extraction Live Webcam Screenshot.

4.3 Prevent and Patching

Figure 15 shows the display *Tentang*/About XSSFilterAde and *Pengaturan*/ Setting XSSFilter on Mozilla Firefox browser. On the menu *Pengaturan*/Settings XSSFilter divided into sub menu Setting general, Whitelist, Embandings, Appearance, and Advanced Notification.

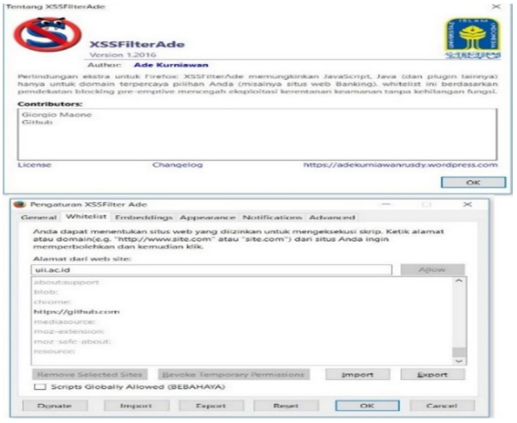

Figure15. About (Tentang) and Setting (Pengaturan) XSSFilterAde

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

General menu make arrangements in general to add-on, the sub menu whitelists make arrangements at the sites of trusted, Sub menu Embeddings perform plugin settings (such as Java, Adobe Flash and Microsoft Silverlight) which may in turn, sub menu appearance make the adjustment to the notification in sidebar menu, Sub menu Notification make arrangements notifications will be displayed if no payload or a script that found the script Cross Site scripting and Sub menu Advanced undertake additional settings to plugins and others.

Figure16. Main Feature XSSFilterAde

XSSFilterAde on the setting in the address bar has three main functions as shown in figure 16. The three main functions that give privileges to users to perform the setting for each website visit as shown in the red box the arrangements 1 to give privileges to the browser Temporarily allow all this page, setting the 2 privileges the browser Allow all this page and setting 3 privileges the browser Allow Scripts Globally (dangerous).

Shown in Figure 17 XSSFilterAde successfully detect, filter, block and notifies the Cross Site Scripting attacks and payload script that has been injected into an email by an attacker with a hook script to the user's browser.

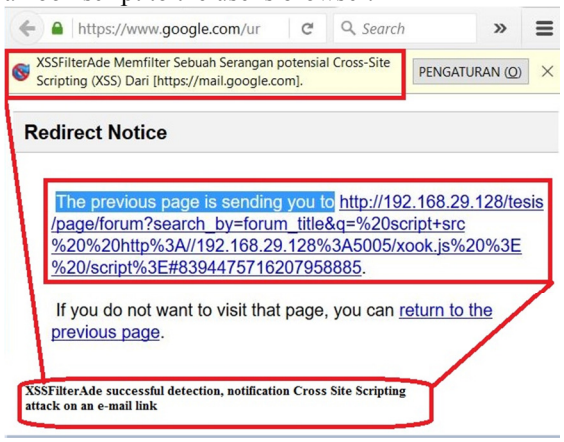

Figure17. Success Result XSSFilterAde email phishing

Shown in Figure 18 XSSFilterAde successfully detect, filter, block and notifies the user so that the victim be more watchful if you're browsing that there has been a payload that has been injected by the attacker into a website with a hook script form of Cross Site Scripting

Figure18.Success Result XSSFilterAde

The weak points in our research is on the network side, where the victim and the attacker still in the same network, for the future work of victims and attackers separated networks with two different public IP address.

5. CONCLUSION

Forensic Analysis and Prevent of Cross Site Scripting Using the Open Web Application Project (OWASP) Framework covers three important stages, namely: Attacking stages, Analysis, and Patching. Stages Attacking is doing activities with Single-Victim-method using the OWASP Xenotix XSS Attack Exploit Framework v6.2 to include attacks Information Gathering, Keylogger, Download spoofer and Live webcams screenshot to the victim through the Mozilla Firefox browser. Stages Analysis was conducted using Live Forensic by Wireshark, live HTTP Header and Tcpdump. The use of live forensic methods enabled to capture all kinds of activities going on such a request, the payload, and the script. the results of the analysis stage and how the script file. some files in the test hash value with application to use it to compare the value of the integrity of the files that have been downloaded by the victim premises files stored on the server. Prevent the last stage is the process by making patching on the user side by installing extensions add-ons in the Mozilla Firefox browser with the extension name XSSFilterAde.

XSSFilter outline is providing early warning, disable the plugin, restrict, allow payload /

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

script to the victim when it will open a website address. Three main setting in XSSFilerAde is Temporarily allow all this page, Allow all this page and Allow Scripts Globally (dangerous).

REFERENCES:

[1] Microsoft, "Microsoft Security Intelligence Report," vol. 21, pp. 7–8, 2016.

[2] Symantec, "015 Internet Security Threat Report," *Internet Secur. Threat Rep.*, vol. 20, no. April, p. 119, 2015.

[3] J. Fonseca, N. Seixas, M. Vieira, and H. Madeira, "Analysis of Field Data on Web Security Vulnerabilities," *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 2, pp. 89–100, 2014.

[4] M. N. Al-Azhar, "Digital Forensic: A Practical Guide Computer Investigation." Salemba Infotek, p. 236, 2012.

[5] M. Meucci and A. Muller, "Testing Guide 4.0," no. Cc, 2014.

[6] WhiteHat Security, "Web applications security statistics report 2016," 2016.

[7] Acunetix, "Web Application Vulnerability Report," 2015.

[8] M. Parvez, P. Zavarsky, and N. Khoury, "Analysis of effectiveness of black-box web application scanners in detection of stored SQL injection and stored XSS vulnerabilities," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 186–191, 2016.

[9] X. Guo, S. Jin, and Y. Zhang, "XSS Vulnerability Detection Using Optimized Attack Vector Repertory," *Proc. - 2015 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2015*, pp. 29–36, 2015.

[10] G. Dong, Y. Zhang, X. Wang, P. Wang, and L. Liu, "Detecting cross site scripting vulnerabilities introduced by HTML5," *2014 11th Int. Jt. Conf. Comput. Sci. Softw. Eng. "Human Factors Comput. Sci. Softw. Eng. - e-Science High Perform. Comput. eHPC, JCSSE 2014*, pp. 319–323, 2014.

[11] A. Abraham, "Detecting and Exploiting XSS With OWASP Xenotix XSS Exploit Framework v3," 2013.

[12] R. Vibhandik. and A. kumar Bose, "Vulnerability Assesment of Web Applications A Testing Approach," pp. 16–21, 2015.

[13] H. Depot and S. Pictures, "Identity Theft 2016 : An Ounce of Prevention is Worth a Pound of Cure," no. September, pp. 1–10, 2016.

[14] R. U. Putri and J. E. Istiyanto, "Network Forensic Analysis Case Studies SQL Injection Attacks on Server Universitas Gadjah Mada," *Indones. J. Comput. Cybern. Syst.*, vol. 6, no. 2, 2012.

[15] Imam Riadi. Jazi Eko Istiyanto, "Network Forensics Log Analysis Techniques using Clustering in Network Forensics," no. August 2016, 2013.

[16] P. A. Sonewar and N. A. Mhetre, "A novel approach for detection of SQL injection and cross site scripting attacks," *Pervasive Comput. (ICPC), 2015 Int. Conf.*, vol. 0, no. c, pp. 1–4, 2015.

[17] S. Fogie, J. Grossman, R. Hansen, a. Rager, and P. D. Petkov, *XSS Attacks: Cross Site Scripting Exploits and Defense*. 2007.

[18] T. O. M. Ali, O. S. A. Awadelseed, and A. E. W. Eldewahi, "Random Multiple Layouts," pp. 1–5, 2016.

[19] D. Wichers, "OWASP Top-10 2013," 2013.

[20] B. Wikipedians and R. Creutzburg, "Handbook of Computer Security and Digital Forensics 2016 Part I – Computer Security," no. April, 2016.

[21] L. Wu, X. Du, and J. Wu, "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6678–6691, 2016.

[22] M. Baca, J. Cosic, and Z. Cosic, "Forensic analysis of social networks (case study)," *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, pp. 219–223, 2013.

[23] Eoghan Casey, *Digital Evidence and Computer Crime*. 2015.