Computer Engineering and Applications Vol. 5, No. 1, February 2016

An Analysis of Vulnerability Web Against Attack Unrestricted Image File Upload

Imam Riadi[1], Eddy Irawan Aristianto[2]

Departement of Information Systems, Universitas Ahmad Dahlan[1]
Departement of Information Systems, Universitas Ahmad Dahlan[2]
imam.riadi@is.uad.ac.id, eddy@uad.ac.id

ABSTRACT

The development of computer security technology is very rapidly. Web security is one of the areas that require particular attention related to the abundance of digital crimes conducted over the web. Unrestricted file upload image is a condition in the process of uploading pictures is not restricted. This can be used to make the attacker retrieve the information that is contained in a system. This research developed with several stages, such as, data collection, analysis of the current conditions, designing improvements to the program code, testing and implementation of the results of patch. Security testing is performed to find out the difference between before and after conditions applied patch unrestricted image file upload. Based on the results of testing done by the method of penetration testing results obtained before the application of patch unrestricted image file upload results respondents said 15% strongly disagree, 85% did not agree. Testing after applying patch unrestricted image file upload results respondents said 7.5% strongly agree, 92.5% agree, so it can be concluded that the development of the patch that has been done has been running smoothly as expected.

Keywords: Vulnerability, Web, Attack Unrestricted, Image, File, Upload.

1. INTRODUCTION

The development of technology and information increasing rapidly So that it directly influence the needs of the society toward information and communication. The website is the most effective media to be used as a storange media. Website service that provides a graphical and textbased information allows anyone to access them for 24 hours with internet availability requirements. Related with this development, so that web security began to become an important issue, since hacking events often occur in an interconnected world. A vulnerability in a web application can be opening way for an attack in the whole information system and does not close the possibility for the control server.

Oscommerce is an opensource program to manage web-based online shop. Oscommerce can be used in various web server that already installed php and a database MySQL. Oscommerce used freely under GNU General Public License. Oscommerce is a solution to build online based small scale trading business to big scale trading business. Web hosting that uses control panel cpanel / whm can install oscommerce more easily because fantastico has provided cms Oscommerce.
Oscommerce chosen because more easily in the installation and use. However oscommerce has security gap in the form of unrestricted upload image file. So this

constituted patches should be done to ensure that online stores that managed can be protected from the attack by attackers.

Based on the description above shows that it needs a patch that can be able to counteract the weakness in the form of unrestricted upload image file, so that a web application can be spared from attack unrestricted upload image file. Patches can be made by identify the code program. The result of the identification code program will be used to make improvements or patch code against lines that cause the image attack unrestricted file upload. Improvement program code expected to minimize attacks unrestricted upload image file so that the information on the website is secured.

2. METHODS

The site of security gap collection Exploit database in 2011, releasing information about security gab in Oscommerce. Slit discovered by indoushka, a developer of information security system. Slit on oscommerce of remote file upload and files disclosures vulnerabilites.Gap security found has been diekspose in website exploit database. Gap security remote file upload can be used to do upload file backdoor into a system. The uploaded backdoor can be used by uploader to get access to system directly by doing authentication Next the uploader can read the secret information of files configuration that can be used to access to manage the database, load data, or even enable the master server [1]. OWASP is stand for Open Web Application Security Project, an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. OWASP was started on September 9, 2001 by Mark Curphey and Dennis Groves. Since late 2003, Jeff Williams has served as Chairman of the volunteers from the OWASP [2].

Header content-type determines content type of data attachment whether the text, audio, data binary, or others. In an optional manner this header is also able to application which is used to make the data. For example, spreadsheets may be made using microsoft excel. Header can be used for determining program what can be used to open the file. Two of the first part separated by slashes, in an optional manner followed by a set of parameter to give you some extra information. Top level type media determines general type of the data, while subtype determines the special format for typing the data. For example, 'image / gif' announced on program client that this data is the image, and in particular that file the image in window GIF [3]. Vulnerability prediction is an important task in securing the web applications before their release. Insecure web applications may cause of stealing personal and crucial user information. Experimental results showed that by considering the context of the user-input significantly improved the performance of the vulnerability prediction model [4]

In the area of PHP source code audit, no matter dynamic analysis or static analysis, each one has great defect that can`t be solved perfectly right now. While until now, what related works do is just to repair the defect of the two, but not propose a new method or thinking [5]. Providing a description of mapping study for synthesizing the reported empirical research in the area of web applications security vulnerabilities detection approaches. The proposed solutions are mapped against the software development stages for which the solution has been proposed and the web application vulnerabilities mapping according to OWASP Top 10 security vulnerabilities [6]

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Web services work over dynamic connections among distributed systems. This technology was specifically designed to easily pass SOAP message through firewalls using open ports. These benefits involve a number of security challenges, such as Injection Attacks, phishing, Denial of Services (DoS) attacks, and so on. The difficulty to detect vulnerabilities before they are exploited encourages developers to use security testing like penetration testing to reduce the potential attacks [7]. Hacker forums, IRC channels, and carding shops all appear to contain a variety of contents relevant to discovering current and emerging cyber threats. There are several examples of evidence related to threats against financial institutions and government [8].

Oscommerce is developed and tested by a team whick is dedicated and focus on core features, community of shop owners online that active, and the developer focusing on features of additional. Community Oscommerce has produced more than 7000 additional features in Oscommerce available for free. Growth community Oscommerce it was recorded more than 260.000 shop owners online, developer and service providers that focuses in a shop online and business. OsCommerce made using PHP, a programming language tough and use mysql as server database to store data. The combination of php and MySQL allows oscommerce to run some web server that supports PHP and MySQL as linux, solaris, BSD, Mac OS X and Microsoft Windows [9].

2.1. Literature study

Literature study done by reading books commercial about web security, the articles and e-book about web hacking in the internet.

2.2. Experiments

In this research needs experiment by onducting assault trials and testing the security of the system that will be implemented using a virtual web server.

2.3. Testing Oscommerce design

Testing application osCommerce use computers virtual Metasploitable installed at virtualbox as server, while computer attackers use times linux. Figure 1. is a description computer of the assailants and computer server

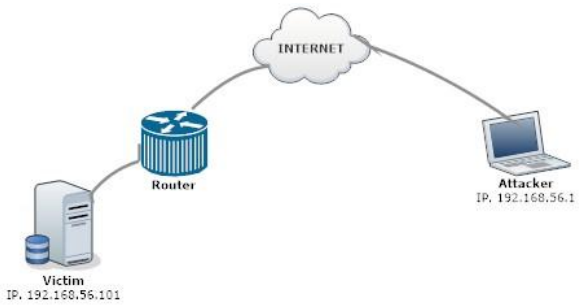

FIGURE 1. Attackers computer and computer servers.

Attackers connected to a computer server using port 80 or via web oscommerce. The steps that must be done by attacker is by doing brute force in the login page which is

owned by Oscommerce. Figure 2 is a method of brute force used for access to page administrator and then upload php shell.

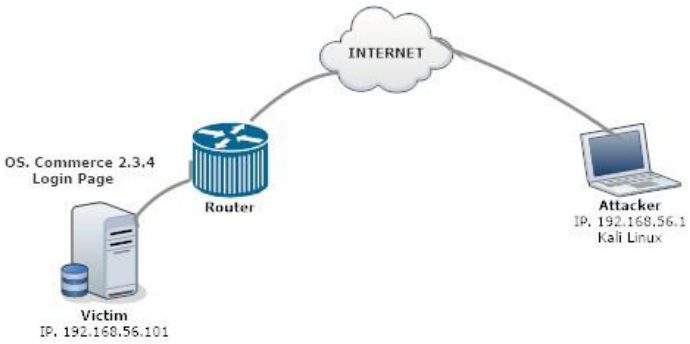

FIGURE 2. The process attackers perpetrated brute force.

Attackers try to do brute force on the login page using tool that has been made in accordance with their needs. Oscommerce by default will disable login when the user doing mistaken in entering the username and password more than three times. Tools designed to be able to detect if login disbale so that the process brute force was halted for while and will be continued if page login no longer disabled. After getting username and the passwords that valid from the brute force, so the attackers can be immediately upload php shell by using upload banner features. PHP shell will were uploaded made pure of plaintext without crafted process was completed.

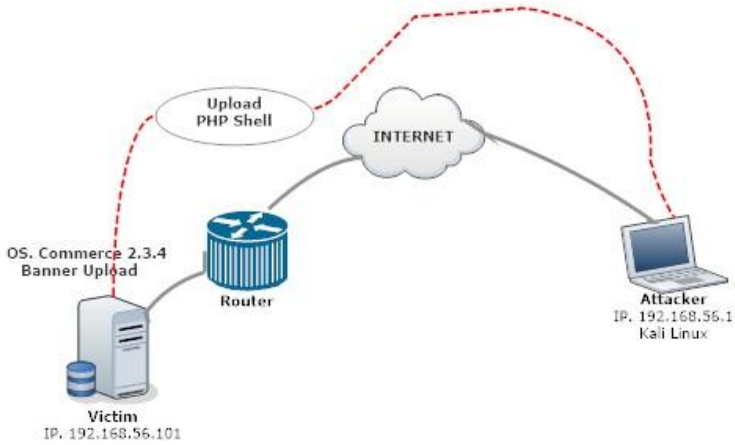

FIGURE 3. The process of uploading PHP shell.

Figure 3. shows the process of php upload shell by using banner upload feature. In uploading image by osCommerce not using osCommerce files uploaded so that the attacker can upload a PHP file shell. Oscommerce proved can be able to release uploading non banner upload module image. The next process is to create a filter on the banner upload module. The filters are made to detect the file type uploaded, so that only the image files can be uploaded in modules upload banner.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

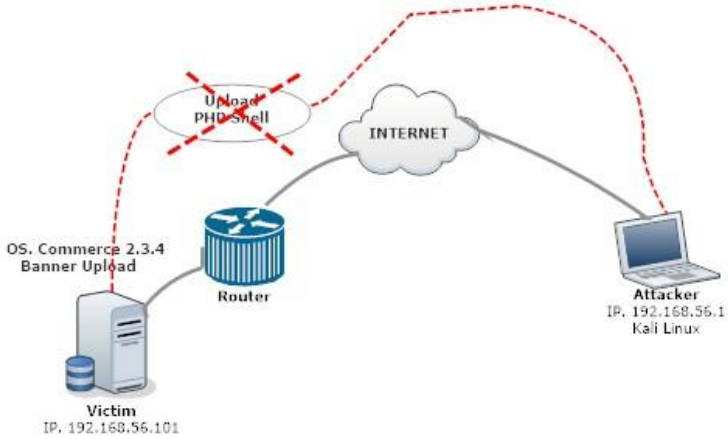

FIGURE 4. The process filter successfully.

Figure 4. Shows that the filter process in uploading file in the banner upload module is success. The attacker only allowed to upload image file type.

3. RESULT AND DISCUSSION

In analyzing the program would be conducted using a debug source programming language PHP process to exploited the security gap Unrestricted Image File Upload in oscommerce-2.3.4.zip. The phases of exploitation process has three phases started from:

1. Access the admin page
2. Do brute force in the login form.
3. Upload php shell then tries to follow unix on the server.

After pass the exploitation process so continued with a groove the process patching that has 8 phase started from :

1. Checking a picture file from the client.
2. Checking the size of the picture file.
3. Checking the extension based on whitelist.
4. Checking based on blacklist.
5. Checking based on content-type.
6. Checking based on an attribute picture file.
7. Checking based on storage location.
8. Checking based on all the content of a picture file.

The next step is to run a test against the patches that made in stage process of patching . The phases of testing process has same 8 phases like patching process grove, such as :

1. Testing of checking client side.
2. Testing of checking size a picture file.
3. Testing of checking extension whitelist.
4. Testing of checking the blacklist extension.

5. Testing of checking content-type.
6. Testing of checking picture attribute.
7. Testing of checking storage location.
8. Testing checking content a picture file.

Three phases mentioned will show how exploitation, repair a program code and testing to a program code that had been repaired. The less filtering the file images that will be upload can cause application and system exploited. Eight phases that used in filtering used to minimize attacks from the attacker. Every filter is a forms of attack that used by attacker based on the OWASP.

3.1. Checking and testing use javascript.

Javascript used to detect file images extension that will be upload. When a picture had been selected, so that javascript will be active and scan the extension from the selected file. Javascript will give warning when extension picture were uploaded not allowed and off the buttons up.

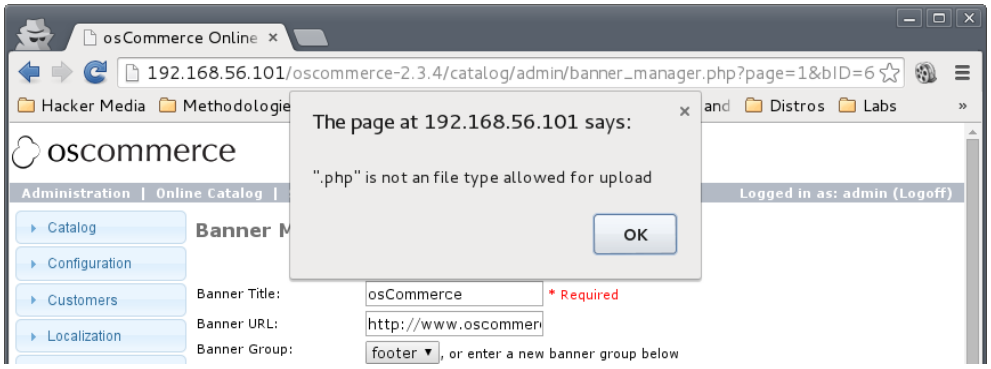

FIGURE 5. Alert javascript.

Figure 5. Shows that uploaded extension picture unsuitable and will give warn to the users.

3.2. Checking and testing picture size

Checking will limit uploaded file with maximum size 1 megabytes. If file that uploaded greater than the maximum size that has been fixed it would be rejected and would not be uploaded. Restrictions the file size used to avoid an attacker who will use a storage media on a hosting or a server.

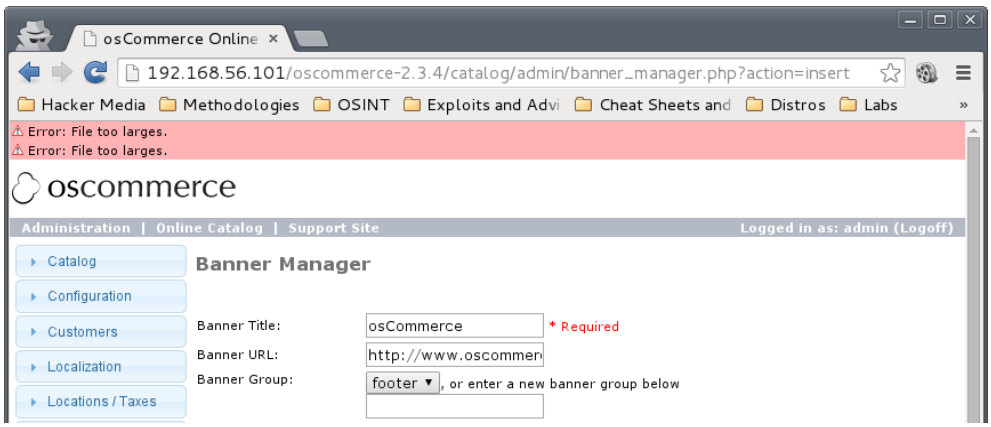

FIGURE 6. Warning file too large.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Figure 6. display a warning that uploaded file too large and not allowed by the application. The warning will not appear when file size who were uploaded does not exceed of the certain limitation.

3.3. Checks and blacklist extension testing

Restrictions extension file that uploaded with blacklist methods used by limit dangerous extention. Dangerous extensions can be php, php3, php4, phtml, exe, jsp, asp, txt, htaccess, this, vbs, htpasswd extension. When file that uploaded use extension in the list it will automatically rejected by the applications and failed to upload.

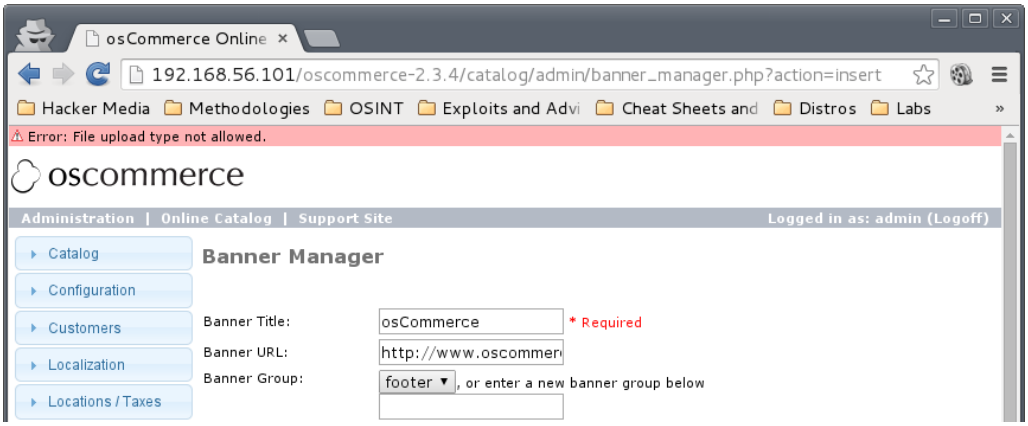

FIGURE 7. Warning file type not allowed.

Figure 7. show a warning that given by the application if an extension that uploaded are mentioned in the black list.

3.4. Checking and whitelist extension testing

In Checking the whitelist used by define extension that allowed to upload, for example allowed extension are jpeg, jpg, png and gif. File were uploaded must be in accordance with extension in the list of whitelist, if can not be found it would be rejected.

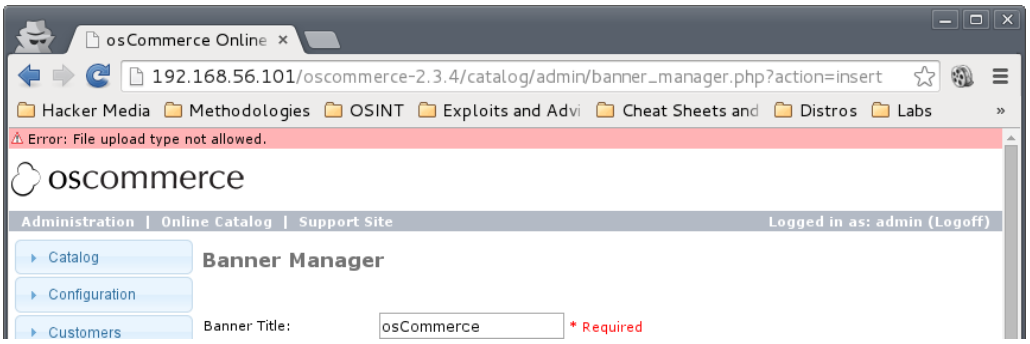

FIGURE 8. Warning file type not allowed.

Figure 8. shows a warning that a file that is diupload failed because extension that used not allowed by the application.

3.5. Checking and content-type testing

File that will be uploaded will be tested in content-type. Information about content-type obtained from HTTP header when sending process. Content-type in HTTP header sent by browser when sending the data use post method

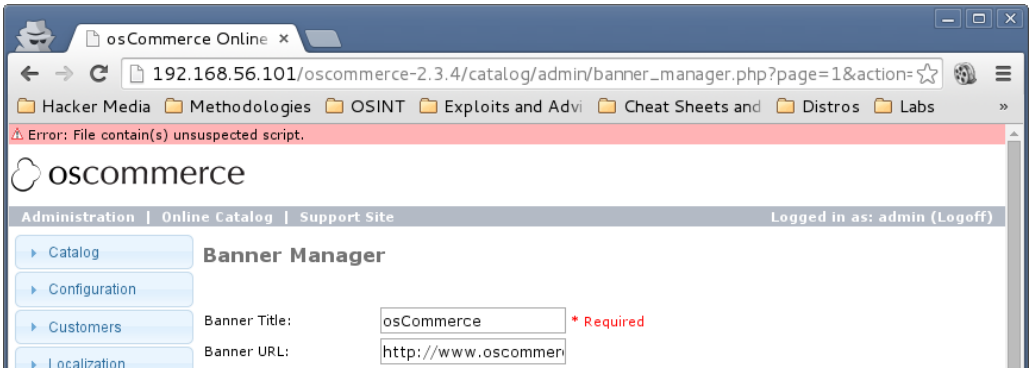

FIGURE 9. Warning content-type.

Figure 9. Showed a rejection of file were uploaded because detected the content-type who do not the suit that has been set.

3.6. Checking and testing attribute picture

Checking the drawing attribute that done by analyzing attribute file that uploaded. The temporary file that has been uploaded and then it checking the image attribute like height and wide picture.

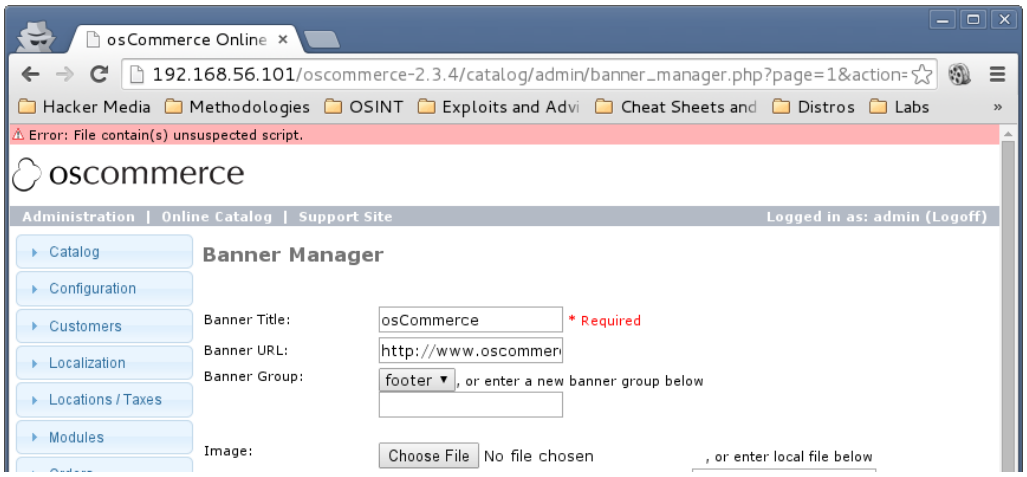

FIGURE 10. Warning failed upload.

Figure 10. Show the failed picture upload because file that uploaded has not high attributes of high and wide image.

3.7. Checks and testing picture path

Checking done by detect in path storage .Path on the application Oscommerce can be determined by user as desired. Storage location supposed to be in the image folders and subfolders, but the attacker can change by a way of adding a

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

double dot (.) to direct into another folder. Double dot who entered has to be filtered to prevent storage out of image folder.

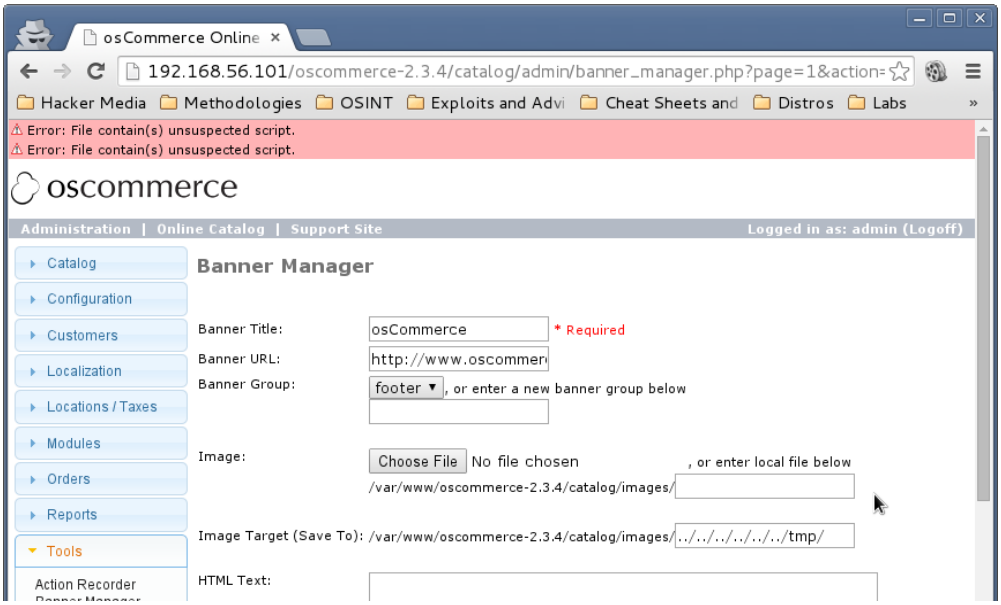

FIGURE 11. Warning input double dot

Figure 11. Show disapproval application to inputan the path command of user because it contains double dot.

3.8 Checking and testing picture content

Checking done by read content in the picture file that has been crafted upholstering PHP shell. Picture file that has been crafted in the content that contain the scripts php shell so that must be rejected.

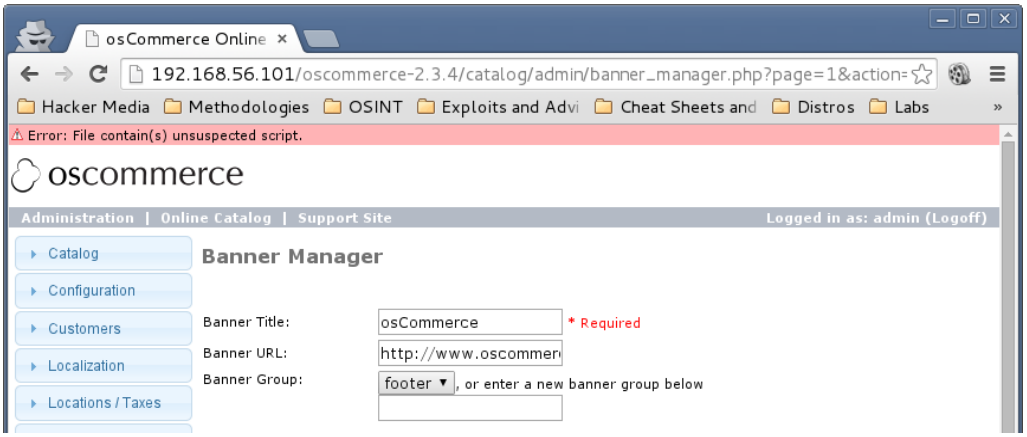

FIGURE 12. Warning file contain unsuspected script.

Figure 12. Shows that application rejected a picture file that is uploaded because it contains the script php shell.

Testing conducted by test security test between before and after use patches unrestricted image file upload. The results of testing before applied patches

unrestricted image file upload was 85% of respondents state not agree if the implementation of security image file upload in Oscommerce are safe, so it can be concluded that the implementation of security image file upload in Oscommerce has not safe yet. Testing of security test after applying patches unrestricted image file upload the results 7.5% totally agree, 92.5% agree, so as to from data testing can be concluded that the implementation of patches unrestricted image file upload in CMS Oscommerce can improve image file upload security.

4. CONCLUSION

The results of testing in security tested methods obtained before the application of patches unrestricted image file upload the results of respondents said 15% strongly disagree, 85% did not agree. Testing after the application of patches unrestricted image file upload the results of respondents said 7.5% totally agree, 92.5% agree, that the implementation of unrestricted image file upload security run as expected. This research can be concluded that making patches to application Oscommerce that is vulnerable to be attacked by unrestricted image file upload, has been successfully made in accordance with the purpose of this research. Patch that made can be used to increase application security that needs validation upload file process.

REFERENCES

[1] Exploit Database. "*Oscommerce Remote File Upload and File Disclosure Vulnerabilities*", [online] 2011, https://www.exploit-db.com/exploits/36248/ (Accessed : 10 January 2015)

[2] OWASP. "*Top Ten OWASP 2007*", [online] 2007, https://www.owasp.org/index.php/Top_10_2007 (Accessed: 11 Januari 2015)

[3] Mansfield, N. Practical TCP/IP in Linux and Windows. Yogyakarta: Andi Publisher, 2004.

[4] Gapta, K, Govil, M., Singh, G., "*Rational Unified Treatment for Web Application Vulnerability*" in 12th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2015.

[5] Zao, J., Gong R, "*A New Framework of Security Vulnerabilities Detection in PHP Web Application*", in 9th International Conference on Innovative Mobile and Internet Services ini Ubiquitous Computing, 2015, pp.271-276.

[6] Rafique, S., Humayun, M., Hamid B., Abbas, A, Akhtar, M., Iqbal, K., "*Web Application Security Vulnerabilities Detection Approaches: a Systematic Mapping Study"*, in Proceeding IEEE SNPD, Takamatsu, Japan, 2015, pp 1-6.

[7] Salas, M.I.P., Martins, E., "*A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing*", in proceedings on IEEE Latin America Transaction, Vol. 13, No. 3, 2015, pp 707-712.

[8] Benjamin, V., Li, W., Holt, T., Chen, H., "*Exploring Threats and Vulnerabilities in Hacker Web: Forums, IRC and Carding Shops*" in proceedings IEEE, Intelligence and Security Informatics (ISI) 2015, pp. 85-90.

[9] Oscommerce. "*Official osCommerce Site*", [online] 2015, http://oscommerce.com, (Accessed: 14 Januari 2015)

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)