Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Web Server Security Analysis Using The OWASP Mantra Method

Bambang Subana[1], Abdul Fadlil[2], Sunardi[3]

[1,2,3]Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta

Email: bsubanaafandi@yahoo.com[1], fadlil@mti.uad.ac.id[2], sunardidi@mti.uad.ac.id[3]

ARTICLE INFO

Article history:
Received: 02/03/2020
Revised: 26/03/2020
Accepted: 01/05/2020

Keywords:
Security, DDNS, DDoS, Fail2ban

ABSTRACT

Higher Education has been using web-based academic information system, for all academic administration process in this academic system such as study plan, academic transcipt, lecturers and Curriculum and student data. So that required maintenance in database and system management whith well-maintained and scheduled. It is necessary to apply the system to determine the level of vulnerability in order to avoid attacks from irresponsible parties. OWASP (Open Web Application Security Project) is one of the methods for testing the web-based applications released by owasp.org. Using OWASP may indicate that authentication management, authorization and session management.The STMIK Jakarta website often has problems on the web and the loss of some important data that interferes with lectures. At the end of 2016, around September when preparing for the first semester of the Study Plan, the website experienced programmed data loss, consequently the academic system was disrupted. The STMIK Jakarta has used a web-based academic information system, for all academic administrative processes such as study plans, academic transcripts, lecturers, curriculum and student data.This system requires data base and system management. It is important to implement a security system to determine the level of vulnerability to avoid attacks from irresponsible parties. OWASP (Open Web Application Security Project) is one method for testing web-based applications released by owasp.org. The results of the research have been carried out with the results reaching around 90% management authentication, authorization, and session management not being implemented properly.

1. Introduction

Web-based applications have developed both in terms of features and data stored. Most of the business and education world uses web-based systems, in addition to promoting the type of business or service to the community in general, web applications can be accessed anywhere without being limited by time and space. Web application data is usually stored on the My Sql or SQL Server database on the web server. Given the importance of the stored data it is necessary to apply security testing of web-based applications. The safety test is carried out to determine the level vulnerability to avoid attacks from irresponsible parties [7,9]. One method for testing web-based applications is the OWASP (Open Web Application Security Project) version 4 method released by owasp.org, a non-profit organization dedicated to the security of web-based applications[1,8]. This method is free to use for anyone who wants to know the vulnerability of a web application. From the explanation in the background above, a study was carried out to implement the security testing of a Web-based application using the OWASP Mantra method to determine the level of vulnerability.

2. Research Methods

This research method was completed with the activity stages in Figure 1.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

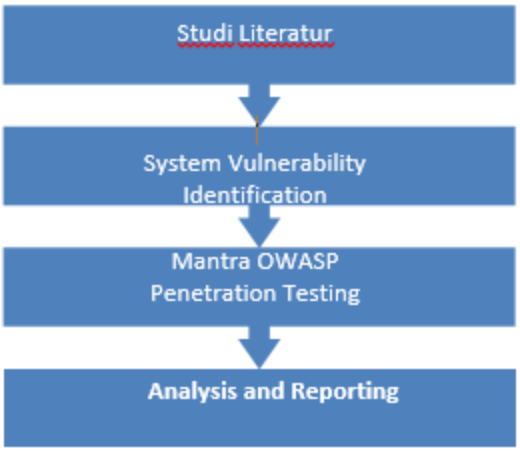

Figure 1 Research Stages

a. Study of literature
In this study conducted by reading books, journals, research report articles, and sites on the internet.
b. System Vulnerability Identification
Identification of vulnerabilities in the STMIK Muhammadiyah Jakarta e-learning web server model using PHP and Moodle applications.
c. Implementation of Mantra OWAPS Testing
OWASP is a charitable non-profit organization in the United States founded on April 21, 2004 dedicated to creating a security testing framework that is free to use by anyone.
The framework used in the OWASP Mantra is as follows:
a. Authentication Testing
Authentication is a constructive action and confirms something that the claim made is true. Authentication of an object can mean confirming its source, whereas someone's authentication often consists of verifying his identity. Authentication depends on one or more authentication factors[6].
In computer security, authentication is the process of trying to verify the digital identity of a communication sender. A common example of the process is the process log. Testing an authentication scheme means understanding how the authentication process works and using that information to circumvent the authentication mechanism[4-5].
b. Authorization Testing
Authorization is a concept that allows access to resources for those who are allowed to use it. Testing for authorization means understanding how the authorization process works, and using that information to circumvent the authorization mechanism.
Authorization is a process that comes after successful authentication, so the tester will verify this point after he holds a valid identity. During this type of assessment, it must be verified whether it is possible to bypass authorization schemes, find traversal pathways, or find ways to increase the privileges assigned to the tester.
c. Session Management Testing
Session Management is defined as a set of all controls that govern full state interactions between users and web-based applications (Matteo Meucci and Friends: 2014). This broadly covers anything from how user authentication is performed, how they are logged out.
Popular web application environments, such as ASP and PHP, provide developers with built-in session handling routines. Some type of token identification will usually be issued, which will be referred to as "Session ID" or Cookie.

3. Result

a. Vulnerability Identification

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Vulnerability identification in this study uses the Acunetix application to determine the level of vulnerability that exists. Here are the results of the Acunetix scan:

Scan of 192.168.0.200

Scan details

Scan information	
Starttime	07/07/2015 8:57:45
Finish time	07/07/2015 9:02:52
Scan time	5 minutes, 7 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1
Server OS	Windows
Server technologies	PHP,mod_ssl,mod_perl,OpenSSL,Perl

Threat level

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or

Alerts Distribution	
Total alerts found 316	
High 3	
Medium 144	
Low 12	
International 157	

Executive summary

Alert group	Severity
Cross Site Scripting	High
Apache httpd Remote Denial of Service	Medium
Application error message	Medium
Backup files	Medium
Directory Listing	Medium
Error message on page	Medium
PHP hangs on parsing particular strings as floating point number	Medium
Login page password-guessing attack	Low

Session Cookie without HttpOnly flag set	Low
Session Cookie without Secure flag set	Low

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

TRACE method is enabled	Low
TRACK method is enabled	Low
User credentials are sent in clear text	Low
Broken links	Informational
Email address found	Informational
GHDB	Informational
Password type input with autocomplete enabled	Informational
Possible internal IP address disclosure	Informational
Possible username or password disclosure	Informational

Based on the information above can be identified vulnerabilities from Web-Based Applications have a high level of vulnerability. With the high level of vulnerability, further testing is done using OWASP Mantra.

b. OWASP Penetration Mantra

In this test, testing is done at the address 192.168.0.xxx/pmb, this is done because this research is focused on the use of lecturers such as seen in table 1 OWASP Mantra Test Results

Tahapan	Tool	H	Status
Testing for Credentials Transporte d over an Encrypted Channel (OTG-AUTHN-001)	WebScar Ab	POST /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123	X
Testing for default credentials (OTG-AUTHN-002)	Brutus	Proses brute force selama 7 jam tidak berhasil	OK
Testing for Weak lock out mechanism (OTG-AUTHN-003)	Browser Mozilla Firefox	Tidak ada mekanisme penguncian	X
Testing for bypassing	WebScar Ab	---- Scanning URL: http://192.168.0.200/ ---- FOUND: http://192.168.0.200/ [STATE: 403 - 296]	X

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Tahapan	Tool	H	Status
authenticati on schema (OTG-AUTHN-004)		(*) DIRECTORY: http://192.168.0.200/css (*) DIRECTORY: http://192.168.0.200/foto (*) DIRECTORY: http://192.168.0.200/images (*) DIRECTORY: http://192.168.0.200/img (*) DIRECTORY: http://192.168.0.200/js	
Test remember password functionality (OTG-AUTHN-005)	WebScar ab	POST /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123	X
Testing for Browser cache weakness (OTG-AUTHN-006)	Browser Mozilla Firefox	POST /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123	X
Testing for Weak password policy (OTG-AUTHN-007)	Brutus	Proses brute force selama 5 jam tidak berhasil	OK
Testing for Weak security question/an swer (OTG-AUTHN-008)	-	Fitur lupa password tidak ada, apabila user lupa password langsung menghubungi admin	OK

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Testing for weak password change or reset functionalities (OTG-	-	Tidak ada fitur reset password	OK

Tahapan	Tool	H	Status
AUTHN-009)			
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)	-	Tidak ada akses lain selain website utama	OK
Testing Directory traversal/file include (OTG-AUTHZ-001)	WFuzz	Tidak berhasil menemukan dokumen root maupun root *Directory*	OK
Testing for bypassing authorization schema (OTG-AUTHZ-002)	Dirb	---- Scanning URL: http://192.168.0.200/ ---- FOUND: http://192.168.0.200/ [STATE: 403 - 296] (*) DIRECTORY: http://192.168.0.200/css (*) DIRECTORY: http://192.168.0.200/foto (*) DIRECTORY: http://192.168.0.200/images (*) DIRECTORY: http://192.168.0.200/img (*) DIRECTORY: http://192.168.0.200/js	X
Testing for Privilege Escalation (OTG-AUTHZ-003)	WebScarab	Tidak ada	OK
Testing for Insecure Direct Object References (OTG-AUTHZ-004)	Browser Mozilla Firefox		X
Testing for Bypassing Session Management Schema (OTG- SESS-001)	Dirb	---- Scanning URL: http://192.168.0.200/ ---- FOUND: http://192.168.0.200/ [STATE: 403 - 296] (*) DIRECTORY: http://192.168.0.200/css (*) DIRECTORY: http://192.168.0.200/foto (*) DIRECTORY: http://192.168.0.200/images (*) DIRECTORY: http://192.168.0.200/img (*) DIRECTORY: http://192.168.0.200/js	X
Testing for Cookies	Zed Attack	POST /dosen HTTP/1.1 Host: 192.168.0.200	OK

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Tahapan	Tool	H	Status
attributes (OTG- SESS-002)	Proxy	User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123 GET /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive	
Testing for Session Fixation (OTG- SESS-003)	Zed Attack Proxy	POST /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123 GET /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive	OK

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Testing for Exposed	Zed Attack	POST /pmb HTTP/1.1 Host: 192.168.0.200	OK

Tahapan	Tool	Hasil	Status
Session Variables (OTG- SESS-004)	Proxy	User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123 GET /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0	
Test Session Timeout (OTG- SESS-007)	Browser Mozilla Firefox	Tidak ada session timeout	X

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Tahapan	Tool	Hasil	Status
Testing for Session puzzling (OTG-SESS-008)	Zed Attack Proxy	POST /pmb HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 29 kode=999999&password=dload123 GET /dosen HTTP/1.1 Host: 192.168.0.200 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.0.200/pmb Cookie: PHPSESSID=4jv3pbgms1d0l7o0rcnt6al0h7 Connection: keep-alive	X

From table 1 it can be seen that in the authentication process there are vulnerabilities, namely in the OTG-AUTHN-001 test, OTG-AUTHN-003, OTG-AUTHN-004, OTG-AUTHN-005, OTG-AUTHN-006 so this process needs improvement. In the authorization testing process there is a vulnerability in OTG-AUTHZ-002, OTG-AUTHZ-004, but after checking above the results are false alarms so that the authorization process is running well, while in session management there is a vulnerability in OTG-SESS-001, OTG -SESS-005, OTG-SESS-007, OTG-SESS-008. The absence of session timeouts allows users who leave the computer to be used by other unauthorized users. On OTG-SESS-008, this application uses same session variable for more than one purpose so that attackers can access pages randomly.

4. Conclusion

The results of testing using OWASP Mantra show that authentication management, authorization and session management have not been implemented properly so that further improvements need to be made by the stakeholders

5. References

[1] Alfred Basta, W. H. (2008). *Computer Security and Penetration Testing.*
[2] Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing for it Security Teams. Assosiasi Penyelenggara Jasa Internet Indoneisa*. (2012). Retrieved May 17, 2014, from http://www.apjii.or.id/v2/read/page/hal aman-data/9/statistik.html
[3] Chow, E. (2011). *Ethical Hacking & Penetration Testing.* Friends, N. N. (2009). *Penetration Testing A Roadmap to Network.* J Thomson, F. (2013, Desember). *Akamai*.Retrieved Mei 19, 2014, from http://www.akamai.com/dl/akamai/ak a mai-soti- q413.pdf?WT.mc_id=soti_Q413

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 107-116 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

[4] Resti Journal (Systems Engineering and Information Technology) (2017) Security of Data Package Traffic on Ubuntu Using the Attack Centric Method. http://jurnal.iaii.or.id. (2017)
[5] Jurnal Ilmiah Nero Volume 3 1 (2015)Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server
[6] Ritzkal, Manajemen Jaringan Untuk Pemula, Bogor:UIKA Press,2018.
[7] Ritzkal, Keamanan Jaringan Cyber, Bogor:UIKA PRESS,2019.
[8] Ritzkal R, Goeritno A, Hendrawan AHH. 2016. Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor. Seminar Nasional Sains dan Teknologi 2016.
[9] Intan Kamilah, Ritzkal R, Ade Hendri Hendrawan. 2019. A nalisis Keamanan Vulnerability p ada Server Absensi Kehadiran L aboratorium di Program Studi Teknik Informatika.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.