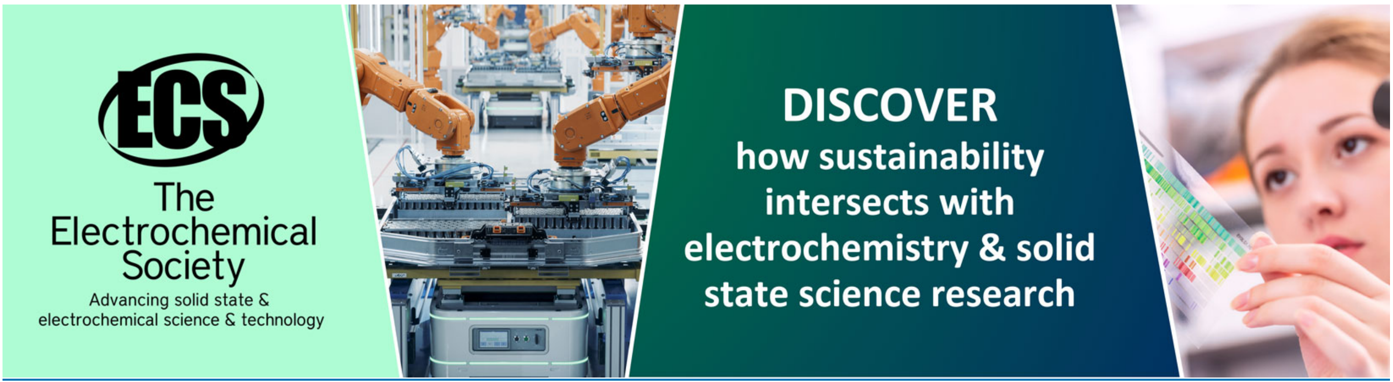
Web vulnerability analysis and implementation

To cite this article: E B Setiawan and A Setiyadi 2018 *IOP Conf. Ser.: Mater. Sci. Eng.* **407** 012081


ECS
The Electrochemical Society
Advancing solid state & electrochemical science & technology
DISCOVER
how sustainability intersects with electrochemistry & solid state science research

Web vulnerability analysis and implementation

E B Setiawan*, A Setiyadi

Universitas Komputer Indonesia, Jl. Dipatiukur 102-116 Bandung, West Java, Indonesia, 40132

*eko@email.unikom.ac.id

Abstract. Data security on the internet is synonymous with a website and a computer network that connects to one another. In the context of computer networks, any existing data on a computer that is connected to another computer, is unsafe, so need to do some way to secure the data so that cannot be accessed by another computer. Each website is created using a series of codes to be able to display data that is public and accessible or accessible to everyone. However, usually on the server computer where the website is stored, there are also data that are confidential or private, so it is not allowed to be accessed by the public. This research is conducted to analyze various techniques and ways of attack that usually done on the internet website, in order to implement various ways of handling so that the existing website can be more secure against the attack so that the data contained in the server. The results have been obtained that is known some weaknesses and attacks that occur on a website. This research used htaccess technique and website script for security improvement. But, the improvements that have been done still cannot guarantee the website 100% safe, it is because that in the world of data security in addition to the web and server side is fixed, must also be viewed from the network security.

1. Introduction

Development of technology has been very rapid, especially in the field of Internet development. Traffic data communication and information in the virtual world has become commonplace. All sorts of data can be found on the internet easily. In fact, up to the data that should be confidential or private, with various techniques on the internet data can be obtained.

Data security on the internet is synonymous with a website and a computer network that connects to one another. In the context of computer networks, any existing data on a computer that is connected to another computer, is unsafe, so need to do some way to secure the data so that cannot be accessed by another computer. Many of the problems that make data security a very important topic in the world of cloud computing [1]. Sabahi [2] points out that the issues that need to be considered for data security are the reliabilty and availability of the system. Some system security tests need to be done to ensure that the data stored on the server remains secure. Security testing of the website system using OSSTM and got the result that its security only gets 74,5% value from maximal value is 100% secure level [3]. In addition, other methods that can be used are NIST and ISSAF [4], but the results are not as good as the OSSTM method [5] [6].

When talking about the internet, not be separated from the term website, client and server. Someone who accesses a URL address through a browser is named as a client who is accessing an application or system contained on the server through the website. The website is actually an intermediary to display the existing data on the server but displayed in the form of websites and views that suit the needs of users. Each website is created using a series of codes to be able to display data that is public and accessible or accessible to everyone. However, usually on the server computer where the website is stored, there are also data that are confidential or private so it is not allowed to be accessed by the public. According to Pratama [7] a cyber-security expert from Communication & Information System Security Research Centre (CISSReC) mentions that in every minute, there are 100 "Cyber Attacks" conducted to websites especially in Indonesia. Even for the size of the world, there are 20,000 malware-infected websites, as well as 50,000 websites affected by phishing attacks in just a week [8].

Computer security system can be said an attempt made to secure the function, data, performance or process that exist on a computer system. The security system on the computer is required to maintain and guarantee the existing resources on the system inside the computer be it hardware, software or data from irresponsible parties so unused or modified person or party is not authorized. The criminals in the cyber world called cracker or attacker. Lots of techniques and ways that the cracker to enter into a server system on a website. One way is to know the gaps that are still less secure security on the website commonly referred to as vulnerability. This research analyzes the security of the vulnerability of a website and directly implement the way of handling it or improvements into the website so that techniques that are often used to attack the server or website, can be addressed or anticipated as possible. Testing in this research should be done because to know whether the web server is safe or not from some criminal actions committed by an attacker [9].

The notion of computer security is diverse, for example, we can see some definitions of computer security according to the experts, among others: According to John D [10] and the Zonggonau [11] states that computer security is a precautionary measure against computer users or irresponsible network users.

Computer security is concerned with self-prevention and detection of unknown intruders in computer systems [12]. Spoofing is a technique used to gain unauthorized access to a computer or information, in which attackers deal with users by pretending to falsify that they are trustworthy hosts. This is usually done by a hacker/cracker by falsifying the identity of the user so that the attacker can log into a computer network illegally. Spoofing consists of several kinds, namely IP spoofing, DNS spoofing and ARP spoofing and email spoofing [13].

DOS attacks (Denial-Of-Service attacks) is a type of attack on a computer or server in the Internet network by spending resources (resources) owned by the computer until the computer cannot perform its function properly so that indirectly prevent the user to gain access to services from a computer that is attacked by DOS. The main target of a denial of service is to damage the services provided so that it becomes unavailable [14].

SQL Injection has a meaning and meaning that is a technique that misuses a security hole that occurs in the database layer of an application. This gap can occur when a programmer who creates code or script does not filter correctly from special characters used in the input data. SQL Injection is a hacking action on computer security where an attacker can gain access to the database within the server. When a website application fails to perform parameter filtering into the database, the SQL command entered in the website address executed so that the attacker can get structure from the database [15].

SQL Injection is currently one of the most serious threats to web applications. On a website that has a SQL Injection slot, it allows an attacker to access the entire database on the website [16]. The cause of the occurrence of SQL Injection is the absence of handling of special sign characters, such as single quotes (') or double minus (-) characters that can cause an application to be inserted with SQL commands, so an attacker can insert SQL commands into a parameter or form.

Cross Site Scripting / XSS is a vulnerability that can cause an attacker to send malicious code to other users. XSS can also be interpreted as a weakness that occurs because the web server cannot validate the input data provided by the user [17]. With the XSS then a web page is displayed the actual commands should not be displayed. XSS is one of the weaknesses that is often exploited by the attacker, but many service providers who do not recognize the weakness.

For a website that has implemented a security system, vuln vulnerability can still occur because there is the possibility missed in one side of the security of the web not previously considered during the design or construction of the system, or also because of the ability of hackers or crackers ability increases. Stages of a hacker attack system can be seen in the following figure 1:

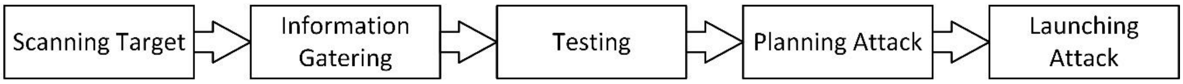


Figure 1. Stages of web attack system, start from scanning process until launching the attack by the attacker.

In general times Linux has a variety of tools that can be divided into several classifications based on its main functions are:

- Information gathering is used to gather information from a system
- Reverse engineering is used to analyze a system through the identification of its components and the interrelationship between the components then create abstraction and design information of the analyzed system [18].

Website defacement is an attack on the website by changing the content or appearance on the website [19]. This attack is generally the result of the act of attackers who enter into the web server and replace the website in the web server with the appropriate display they want. The workings of web deface is to make changes to the website on the website [20]. This research is done because the current attack on a website is very much and theft of data on the internet is very high. Thus, after this research is expected to provide knowledge to improve the security of a website so that the action of data theft on the internet can decrease.

2. Experimental method

Stages of research conducted in this study are :

2.1. Determine the formulation

Research is a way to answer from a problem. To determine the problem in this study, the researcher conducted a preliminary study of empirical facts obtained from references in the form of relevant concepts and theories, as well as previous research related to the research undertaken.

In order for the problems in this research is clear and does not cause the doubt to be answered well, then needed a problem formulation. Problem formulation is a question searched for answers through data collection. Problem formulation is used as the basis of a theoretical submission, a method of analysis and conclusion.

2.2. Data collection

This section explains the stages of data collection, which consists of literature studies and analysis of frequent attacks. The data collected in this study refers to the website and server that exist on the address http://ekobudisetiawan.com, http://if.unikom.ac.id com which is the website of the study program at the university computer Indonesia where the researchers work and the last from http://umkmbandung.com.

2.3. Analysis stage, improvement and test implementation

At this stage performed stages of analysis to determine the part of a web that has vuln. This analysis is done by using the initial tool to check the vulnerability of a website. After getting some information about security holes that exist in a website, the next step is to fix the existing security gaps, both from the side of the server side or from the web side scripting. Repairs are done is add a script especially in the htaccess file on the server. After improvements, the researchers test the improvements that have been done, so it is known whether the fix can cover the previous security hole. This test is done by penetration testing of a website.

2.4. Phase analysis of improvement results and implementation results

This stage is performed after testing the improvement with penetration testing. Analysis of the results of improvements and implementation results conducted to determine how much success rate improvement has been done.

2.5. Determining conclusions and suggestions

This stage is done after all stages of research is completed. The conclusion that taken is the result of research that has been done, then provide some suggestions that can be done for further research.

3. Result and Discussion

This study was conducted and implemented on three websites that can be accessed by researchers from the server side. The specification of each website server can be seen in table 1.

Table 1. Specification for each server website.

Status	**Website**		
	ekobudisetiawan.com	**if.unikom.ac.id**	**umkmbandung.com**
Cpanel Version	68.0 (build 37)	56.0 (build 52)	68.0 (build 37)
Web Server Version	Apache 2.4.33	Apache 2.2.31	Apache 2.4.33
PHP Version	5.6.35	5.4.45	5.6.35
MySQL Version	10.1.32-MariaDB	5.1.73-cll	10.0.34-MariaDB
Architecture	x86_64	i686	x86_64
Operationg System	linux	linux	linux

Based on the results of observations and research conducted, obtained information that the analysis of attacks that often occur on the website used as the object of this research is web defacement and SQL injection. To perform vulnerability analysis process to a website in this research use some tools, that is ZenMap, XSS Tools Nikto, Owasp Dir Buster and ViSQL Tools.

3.1. Scanning information using zenmap tools

Zenmap is an open source GUI application for network exploration and security auditing. Based on the scanning results there are 10 ports on the open website server such as port 21, port 22, port 53, port 80, port 110, port 143, port 443, port 465, port 587, port 993, port 1433, port 8080 and operating system used is Linux. Figure 2(a) is the view of the scanning results using Zenmap tools.

3.2. Scanning vulnerability using Nikto XSS tools

Nikto is an open source application used to test vulnerabilities in a website. The command typed to test the XSS vulnerability inside a website is nikto -h url_target -Tuning 4. This command scans the target with scan option 4 i.e. injection (XSS / Script / HTML). Figure 2(b) is the output screen display from typing a command on terminal Nikto -h url_target -Tuning 4.

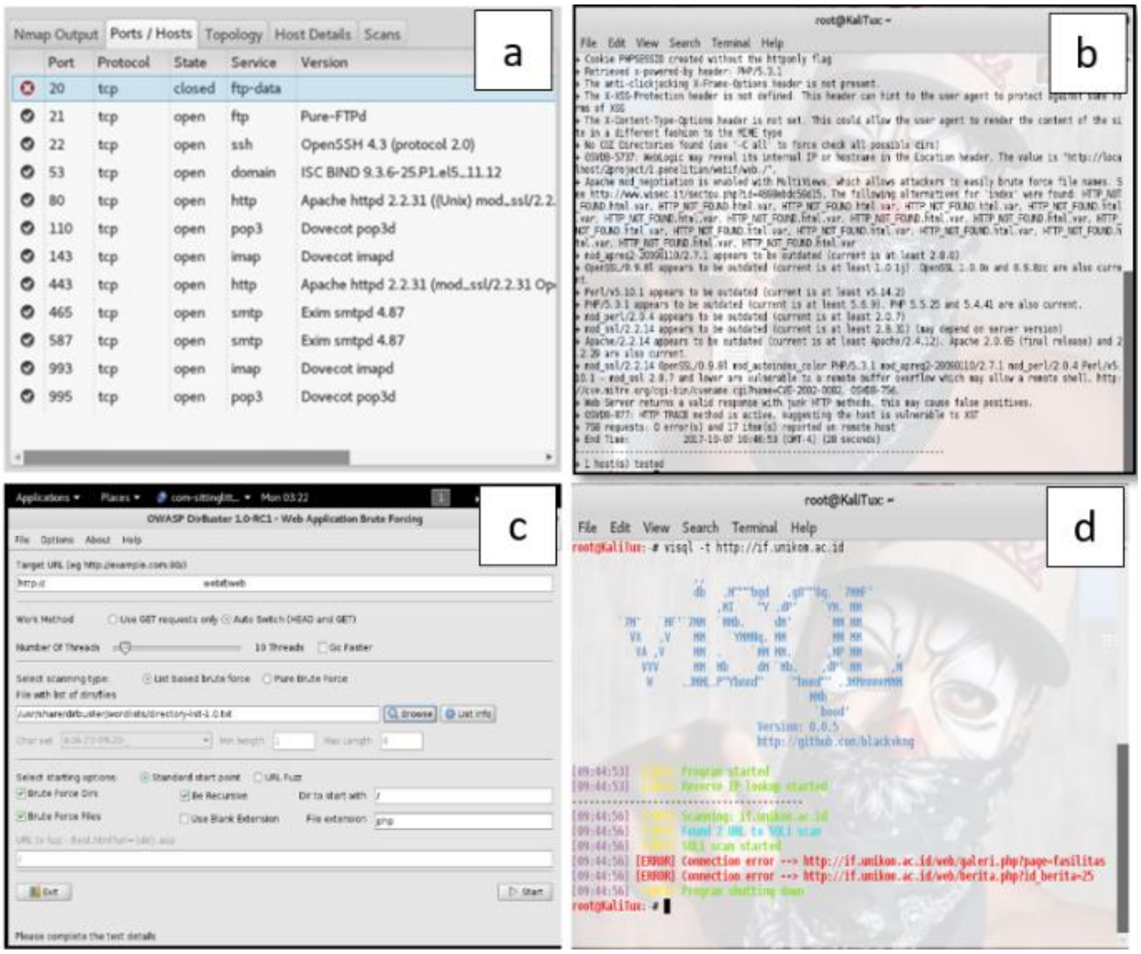
Based on figure 2 (b) there are vulnerabilities of the website of the research object such as OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to Cross Site Tracing (XST), the result shows the active trace method that can cause XST. XST is one of the web security bypass techniques by combining XSS bugs and request method TRACE in HTTP protocol.

3.3. Scanning vulnerability using the Owasp Dir buster tools

Owasp Dir Buster is an application created by OWASP (Open Site Application Security Project) and is designed for brute force directories and on web/application servers. Figure 2(c) is the result of scanning and report analysis using tools Owasp Dir Buster with the directory used is directory-list-1.0.txt.

3.4. Scanning vulnerability using ViSQL tools scanning vulnerability

Visql is a tool used to scan SQL vulnerabilities on a site on the server. The typed command to scan an SQL vulnerability on a site on the server is Visql -t target. Figure 2(d) is the output screen of scanning vulnerability using Visql tools (See Figure 2).



	Port	Protocol	State	Service	Version
⊗	20	tcp	closed	ftp-data	
✔	21	tcp	open	ftp	Pure-FTPd
✔	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
✔	53	tcp	open	domain	ISC BIND 9.3.6-25.P1.el5_11.12
✔	80	tcp	open	http	Apache httpd 2.2.31 ((Unix) mod_ssl/2.2.
✔	110	tcp	open	pop3	Dovecot pop3d
✔	143	tcp	open	imap	Dovecot imapd
✔	443	tcp	open	http	Apache httpd 2.2.31 (mod_ssl/2.2.31 Op
✔	465	tcp	open	smtp	Exim smtpd 4.87
✔	587	tcp	open	smtp	Exim smtpd 4.87
✔	993	tcp	open	imap	Dovecot imapd
✔	995	tcp	open	pop3	Dovecot pop3d

```
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some fo
rms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the si
te in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location header. The value is "http://loca
lhost/2project/1.penelitian/webif/web./".
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. S
ee http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP_NOT
_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html
.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_
NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.h
tml.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ mod_apreq2-20090110/2.7.1 appears to be outdated (current is at least 2.8.0)
+ OpenSSL/0.9.8l appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also curre
nt.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ PHP/5.3.1 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2
.2.29 are also current.
+ mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.
10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http:
//cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 756 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2017-10-07 10:46:53 (GMT-4) (28 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Target URL (eg http://example.com:80/)
http://   webif/web

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-1.0.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /
☑ Brute Force Files □ Use Blank Extension File extension php
URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

```
root@KaliTux:~# visql -t http://if.unikom.ac.id

                Version: 0.0.5
                http://github.com/blackvkng

[09:44:53] [INFO] Program started
[09:44:53] [INFO] Reverse IP lookup started
**********************************
[09:44:56] [INFO] Scanning: if.unikom.ac.id
[09:44:56] [INFO] Found 2 URL to SQLi scan
[09:44:56] [INFO] SQLi scan started
[09:44:56] [ERROR] Connection error --> http://if.unikom.ac.id/web/galeri.php?page=fasilitas
[09:44:56] [ERROR] Connection error --> http://if.unikom.ac.id/web/berita.php?id_berita=25
[09:44:56] [INFO] Program shutting down
root@KaliTux:~#
```

Figure 2. Result scanning using ZenMap, XSS Tools Nikto, Owasp Dir Buster and ViSQL Tools.

The four tools are implemented for each website that made the object of research. Differences results obtained because each server and website have different server types and settings. The results of scanning for all websites can be seen in table 2.

Table 2. Specification for each server website.

Scanning Tools	Vulnerability Website Status		
	ekobudisetiawan.com	**if.unikom.ac.id**	**umkmbandung.com**
ZenMap	port 21, port 22, port 53, port 80, port 110, port 143, port 443, port 465, port 587, port 993, port 995 status : vuln	port 21, port 22, port 53, port 80, port 110,113, port 143, port 443, port 465, port 587, port 993, port 1433, port 8080 status : vuln	port 20, port 21, port 22, port 53, port 80, port 110, port 143, port 443, port 465 status : vuln
Nikto XSS	HTTP TRACE active, status : not vuln	HTTP TRACE active, Cross Site Tracing, XSS Bugs status : vuln	HTTP TRACE active, Cross Site Tracing, XSS Bugs status : vuln
Owasp Dir Buster	directory-list not found status : not vuln	directory-list found status : vuln	directory-list found status : vuln
ViSQL	SQL Injection : not found Status : not vuln	SQL Injection found status : vuln	SQL Injection found status : vuln

3.5. Website improvement implementation

Improved website implemented to fix the gap of a security hole, bugs and to improve the performance of a website. Based on penetration testing then found a security gap where users/visitors can download files or documents that are not allowed. The following in figure 3 are the steps to fix the security flaw by adding the htaccess file to the root folder in a server (See Figure 3).

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK|DEBUG) [NC]
RewriteRule ^(.*)$ - [F,L]
RewriteCond %{REQUEST_URI} (timthumb\.php|phpthumb\.php|thumb\.php|thumbs\.php) [NC]
RewriteRule . - [S=1]
RewriteCond %{HTTP_USER_AGENT} (libwww-
perl|wget|python|nikto|curl|scan|java|winhttp|clshttp|loader) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (<|>|'|%0A|%0D|%27|%3C|%3E|%00) [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
(;|<|>|'|"|\)|\(|%0A|%0D|%22|%27|%28|%3C|%3E|%00).*(libwww-
perl|wget|python|nikto|curl|scan|java|winhttp|HTTrack|clshttp|archiver|loader|email|harvest|extract|
grab|miner) [NC,OR]
RewriteCond %{THE_REQUEST} \?\ HTTP/ [NC,OR]
RewriteCond %{THE_REQUEST} \/\*\ HTTP/ [NC,OR]
RewriteCond %{THE_REQUEST} etc/passwd [NC,OR]
RewriteCond %{THE_REQUEST} cgi-bin [NC,OR]
```

Figure 3. Improvement website security hole via htaccess method.

The result of this research after improvement can show in table 3.

Table 3. Status result after improvement website security.

Vulnerability	Status After Improvement
SQL Injection	not vuln
Port Status	not vuln
XSS / Script / HTML Injection	not vuln
Directory List	not vuln

It can be seen that after doing website repair with htaccess and fix scripting method, the status of each website that becomes the object of research is no longer vuln again. However, even if it is considered secure, it does not guarantee that the website free from attack. This is because when talking about the website technology will certainly continue to grow. For example, the format of the script in PHP 5 is no different from the script in PHP 7 so that improvements made now for the future must be done back in accordance with technological developments. In addition, researchers believe that when we are connected to the internet, it is very difficult to get 100% security level, because data security not separated from the software security, hardware security and network security itself.

4. Conclusion

As for some conclusions obtained are there has been some kind of attack that usually happens on a website and has been some improvements to the weaknesses, so as to improve the security of a website from various parties who do not have privileged. Some types of vulnerability that usually become the main door of the cyber criminals actually exist on the weaknesses that exist on the software side, namely the understanding in the creation of a safe script is very low. Although already using security in terms of hardware such as the use of a firewall engine on the server, still not be safe if not accompanied by the ability to understanding related data security by each stakeholder.

Acknowledgments

Authors wishing acknowledge to UNIKOM and KEMENRISTEKDIKTI for help and support this research using grant Penelitian Strategis Nasional Institusi (PSN Institusi) 2018.

References

[1] Chen D and Zhao H 2012 *Proc. Int. Conf on International Conference In Computer Science and Electronics Engineering (ICCSEE)* **1** (IEEE) p 647-651

[2] Sabahi F 2011 *Proc. Int. Conf In Communication Software and Networks (ICCSN)* **3** (IEEE) p 245-249

[3] Fernando Y I and Abdillah R 2016 Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM) *Jurnal CoreIT* **2** 1 p 33-40

[4] Corral G 2005 *Proc. Int. Conf on First International Conference (IEEE)* p 86-93

[5] Herzog P 2003 Open-source security testing methodology manual *Institute for Security and Open Methodologies (ISECOM)*

[6] Prandini M and Ramilli M 2010 *Proc. Int. Symp. Computers and Communications (ISCC)* (IEEE) p 320-325

[7] Kontan and Ihsan A 2015 *Tiap Menit, 100 Serangan "Cyber" Incar Indonesia* http://tekno.kompas.com/read/2015/01/21/11231777/Tiap.Menit.100.Serangan.Cyber.Incar.Indonesia [Accessed : January 21, 2017]

[8] Mohammed T 2017 Grandon. com Got Hacked! *Journal of Information Technology Education: Discussion Cases* **6** 1 p 1-25

[9] Sasongko A 2011 *Panduan Keamanan Web Server* (Jakarta: Informatika)

[10] John H and Weaver G 1995 *An Analysis of Security Incidents on the Internet* (Software Engineering Institute)

[11] Zonggonau K and Sajati H 2015 Membangun Sistem Keamanan ARP Spoofing Memanfaatkan ARP Watch dan Addons Firefox *Jurnal Compiler* **1** 4 pp 49-57
[12] Gollman D 2011 Computer Security (New York: John Wiley & Sons, Inc)
[13] Hoiriyah 2016 Investigasi Forensik Pada Email Spoofing Menggunakan Metode Header Analysis *Jurnal Ilmiah Data Manajemen dan Teknologi Informasi* **17** 4 p 20-25
[14] Rudi H 2015 Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service (DOS) *Jurnal Faktor Exacta* **5** 1 p 1-14
[15] Clarke 2009 *SQL Injection Attacks and Defense* (Burlington: Syngress)
[16] Halfond 2006 *Proc. Int. Symp. Secure Software Engineering* (IEEE)
[17] Tolle H 2008 Peningkatan Keamanan Web Terhadap Serangan Cross Site Scripting (XSS) *Jurnal Tekno* **9** p 52-61
[18] Setiyadi A 2017 *Proc. Seminar Nasional Komputer dan Informatika* p 113-119
[19] Kanti TV 2011 Implementing a Web browser with Web defacement detection techniques *World of Computer Science and Information Technology Journal (WCSIT)* **1** 7 p 307-310
[20] Rialda A 2012 Security System Layanan Internet Banking PT BANK MANDIRI (Persero) Tbk *Jurnal Sistem Komputer* **2** 2 p 54-60