International Journal on Advanced Science Engineering Information Technology

Vol.10 (2020) No. 5
ISSN: 2088-5334

Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website

Ahmad Almaarif[a,1], Muharman Lubis[a,2]

[a]School of Industrial Engineering, Telkom University, Jalan Telekomunikasi No. 1, Bandung, 40257, Indonesia
E-mail: [1]ahmadalmaarif@telkomuniversity.ac.id; [2]muharmanlubis@telkomuniversity.ac.id

***Abstract*—Information security often neglected by individual or employee or even by the enterprise, with there is no proper strategy to raise awareness, promote consistency and maintain performance regarding protect sensitive, confidential, and critical data. One of the common techniques used is a vulnerability assessment and penetration testing (VAPT) to assure the security strategy has been implemented into the computer system by analyzing both its strength and weakness. SQL plays an essential role in the Relation Database Management System (RDBMS) and its relationship to the existence of a website and its flexible operation because of its simplicity and integrity. To anticipate these types of threats or other Internet attacks, a goal-oriented penetration test that has a framework is recommended to identify specific types of vulnerabilities that lead to business concessions and to avoid the risks that adversely affect the enterprise Thus. This study conducts VAPT to uncover the possibility of threats and evaluate the potential impact to be reported to the system owner through a proper engagement framework that allows systematic measurement. Government websites have been identified for this purpose of the research to show the current trend that occurred in cyber communities, especially in Indonesia. This study has found various vulnerabilities lies in the directory listing, full path disclosure, PHP info disclosure, folder webserver disclosure, and other potential threats, which present 2 (two) critical, 6 (six) medium, and 2 (two) low level of risk.**

***Keywords*— vulnerability; threat; pen test; network security; assessment.**

I. Introduction

Indonesia, as a country, has a critical note to take into consideration indicated by huge cases in cybercrime by Symantec 2018 [1] that recorded the number of cybercrimes experienced at 59.45 million, which hold the fifth position below China, India, United States of America, and Brazil. Unfortunately, Global Security Index 2017 by ITU-D presented a low maturity score of 0.424 above Sri Lanka and below Pakistan, which holds Indonesia in the rank of 70 out of 193 in terms of cybercrime strategy. It involves several criteria for the assessment, namely the establishment of cybercrime legislation, cybersecurity regulation and training, the existence of technical institution (national CERT/CIRT/CSIRT), implementation standard framework for organization, child online protection, public consultation, cybersecurity metrics, public awareness campaign, incentive mechanism, academic curricula, bilateral and multilateral agreements, or interagency partnership [2]. This condition can be interpreted that predominantly, the legislative, executive, or judicative, or even mostly the citizen are not aware of the crucial implication of cybercrime to society in the long run. Sadly, Indonesia also becomes the top 10 (ten) for most country that has the most victim lost at $ 3.2 billion annually [3], while China has experienced the greatest loss with $ 66.3 billion. On the other hand, memory dumper/memory scrapper (16%), downloader (14%), remote administration tool (RAT) (9%), the injector (9%), keystroke logger (8%) and bot (7%) become the most encountered type of malware in industrial cyberattacks worldwide in 2017 [3].

Historically, ID SIRTII (Indonesia Security Incident Response Team of Internet Infrastructure) mentioned that at the external side, 1.1 million attacked occurred against Indonesia Internet Infrastructure every day, which mostly comes from China. On the other hand, 3 (three) million attacks against foreign Internet Infrastructure, mostly to Malaysia, come from Indonesian users. Also, from 1998 to 2009, there were around 5.239 attacks against Indonesia websites (domain id: go.id, co.id, or.id, and ac.id), which some practitioner assumed that those activities are in line with the distribution of 48 (forty-eight) books related to hacking activities of a module that encourage the common user to execute the code on practice either based on entertainment or economic benefits [4, 18]. Unfortunately, the type of cyber case has been handled are quite varied, which cover several types of cybercrime domain such as deface, cyber gambling, cyber pornography, cyber prostitution, child prostitution, cyber fraud case, cyberterrorism, cyberbullying, cyberstalking, denial of service, ransomware, and privacy infringement.

Commonly, the application or the website will be tested thoroughly before launching or go live to identify the potentiality of vulnerability, the functionality of the features, and the acceptance of the users. Thus, network penetration testing as one common method of assessment becomes critical to anticipating the risk of security exposures when cyber-attacks are launched at a sudden moment. The security assessments also help the organization to assure the important program become protected from exploitation, which can be elaborated further by comparing specific best practice or benchmarking with the current implementation. However, the general criteria, indicator, and category of network vulnerabilities can embody polar differences depend on the context, configuration, and standard. This may be different from the penetration of word systems, remote passwords, web servers, databases, network services, network devices, directories, disclosure of information, and encryption.

Importantly, the prioritization of vulnerabilities identification drives essential requirements for the overall penetration testing process. Also, the reasons for intense pressure on pen test requirements include concerns such as threat identification, perimeter security assessment, industrial regulatory certification, IT security cost control, vulnerability control solutions, legal compliance, security check, verification, authentication, and justification for the return of security investments. Currently, this type of testing becomes a general phenomenon to improve the operational efficiency of IT security, while others are used to address different kinds of problems.

Domain selection is one of the essential components of penetration testing, but it is also one of the most overlooked components. Unfortunately, much of the article volume has been written about various tools and techniques that can be used to access the network, but the pre-hacking topic got neglected, which is the preparation phase. Ignoring the completion properly of pre-engagement activities could open a penetration test by potential hackers to many complex problems, including crawling scopes, unsatisfied customers, and even legal issues. Thus, identifying the scope of the project precisely and determines what will be tested can be extremely useful in the process of security assessment, mainly to conduct penetration testing as the preliminary phase in identifying vulnerabilities of a specific website. Enterprises spend millions of dollars recovering from security breaches due to notification fees, remedial efforts, low productivity, and loss of income, which estimates that recovery efforts alone will be at around US $ 167 thousand per incident [5]. Thus, from a business perspective, penetration testing can protect the organization against failure by preventing financial losses, able to raise popularity through demonstrating due diligence and compliance with industry organizations, customers, and shareholders as well maintaining the corporate image with streamlining information security investments.

II. Material and Method

A. Material Review

There are various tools to conduct pen test, such as [5]:

- Nmap to find a web server.
- Fiddler for web debugging proxy.
- Nikto to identify web server type, version, add on, configuration, and other interesting files.
- WebScarab as an interceptor for identifying new URLs on the test target, the session ID analyzer, and the parameter fuzzer.
- w3af for vulnerability tester.
- Firefox extension, named firebug for inline editing, breaking forms, messing with JavaScript, making rogue sites, and man-in-the-middle component.
- Cenzic Hailstorm as a web vulnerability scanner.
- Core Impact to identify, validate and exploit vulnerabilities in Reflective/XSS, Blind SQL/ Injection and Remote File Inclusion for PHP application.
- Nessus 4 to detect remote cracker that can control or access sensitive data, misconfiguration, and default password.
- DOS, lastly, Metasploit Framework to develop and execute exploit code against a remote target machine.

The penetration test can be performed in two models, both external and internal [6]. The penetration test for external networks has a function to show that there are known security vulnerabilities that can be exploited by attackers when they appear outside the network's boundaries, usually from the Internet. It includes the analysis of information available to the public, the network enumeration stages, and the behavior of the security agencies analyzed, which can be categorized as a traditional approach because related to server evaluation, technical infrastructure, and core software and without prior knowledge of the target environment. All web servers, mail servers, firewalls, routers, IDPs, and others must be subject to intrusion testing activities to assess security positions. On the other hand, the intrusion penetration test reveals a comprehensive view of the organization's security situation, which quite like the external evaluation. The test will be conducted through several network access points, representing each logical and physical network segment. It is used to determine whether an internal employee of an unsatisfied organization can break into the internal network with the amount of knowledge he/she has in the IT field. Commonly, it can occur through exposing the poor level of security or control in the environment for stealing sensitive information.

SQL plays an essential role in the Relation Database Management System (RDBMS) and its relationship to the existence of a website and its flexible operation because of its simplicity and integrity. Problems such as SQL injection can occur when an attacker injects SQL queries with new parameters in the input values to access the information within the database. Meanwhile, Cross-Site Scripting (XSS) can occur when embedding JavaScript, VBScript, ActiveX, Flash, or HTML with malicious XSS links to obtain root privileges and all sensitive data [7]. This technique is quite common to be used by hackers to have the privilege to control or looking at specific data within the system for various types of purposes such as wealth, desire, fame, or other internal or external motivation. To anticipate these types of threats or other Internet attacks, a goal-oriented penetration test that has a framework is recommended to identify specific types of vulnerabilities that lead to business concessions and to avoid the risks that adversely affect the enterprise [8]. Of course, it should not be driven by compliance because some different reasoning influences the culture and work pattern to implement specific security strategy within an organization.

Before conducting the penetration test, it is good to determine the maturity level of the client's security location and establish the line of communication with the customers in terms of the incident reporting process, status report frequency, legal considerations, and others. For customers with immature security software, it is often useful to conduct a gap analysis first before jumping to penetration testing or conduct vulnerability assessment VA [8, 9]. Therefore, each vulnerability or risk identified should be labeled and categorized as extreme (catastrophic), high (significant), elevated (material), moderate (limited), and low (measurable), which are defined based on the security controls being compromised with several types of the possibility that impact reputational, financial, physical, or other resources in the organization [10]. To prevent security breaches and loss of important business data, a person must identify and categorize security gaps in its network. Thus, penetration testing has benefits to increase awareness of highly-exposed systems, demonstrate compliance with industry standards and regulation, measure security effectiveness based on own security perimeter security investment, reduce risk by following expert remediation guidance and demonstrate impact to executive leadership with concrete proof to the business [11]. However, the threats usually come from the weakest link in the organization, which is human beings concerning their attitudes, behaviors, or responsibilities at a certain level through the exploitation of their habits or patterns. For example, through e-mail phishing, telephone pretexting, physical vector, or any type of social engineering technique to elicit information or manipulate an employee into performing actions that may aid in an attack later [12].

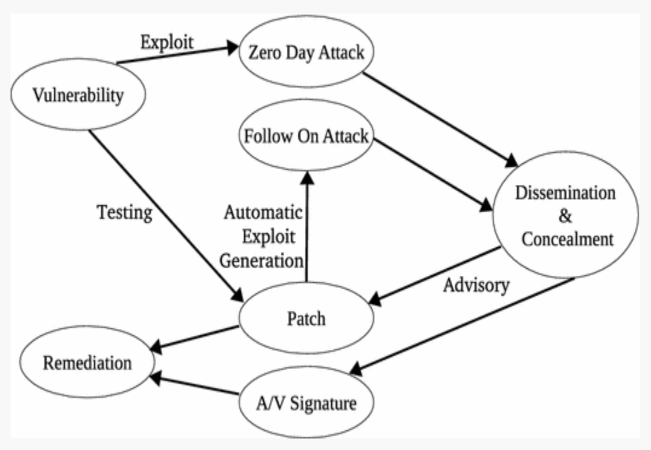


Fig. 1 Life Cycle Vulnerabilities [15]

Penetration tests on companies can be classified into three types, which are grey hats, white hats, and black hats. In the white hat, the laboratory is a moral breach that respects the regulations, and staff can assist in testing. In the meantime, a black hat is used primarily to see how employees interact with unwanted attacks. Meanwhile, in grey hats, certain techniques have not reported for several reasons when conducting the test [13]. Security threats arise when there are opportunities, motivations, and technical means from the intended person to attack a specific system based on certain circumstances regarding when, why, and how. Therefore, the penetration test only addresses the dimensions of "how" the threats can be conducted with understanding its step-by-step mechanism [14]. Vulnerability assessment, including the use of various automated tools and manual testing techniques, is used to determine the security situation of the target system. In this step, all the breakpoints and gaps are found. This point of violation or vulnerability, if detected by an attacker, can cause significant data loss and deceptive intrusion activities. In the penetration test, the laboratory simulates the activity of a malicious attacker trying to exploit the target system vulnerability. In this step, the set of gaps identified in the VA are used as input domains. This VAPT process helps assess the effectiveness of security measures in the target system [15].

Essentially, hackers, after compromising the host, need to obtain information about the host's location and functions in the intranet, which will include the hostname, interface, direction, and service that our host listens to. The more host gets used to the operating system, the more reliable it is [16]. It should take note that current techniques in the VAPT can be obsolete due to the improvement of the operating system or platform as the frequent attempts to commemorate a new generation of technology advancement such as Google Hacking [17]. Once the service provider or the system owner realizes and aware of the importance of security strategy and routine check-up over the system, which has been formulated into employees' work practice, the objective of protecting resources and assets can be optimized [19-20]. Usually, the reconnaissance type of network attacks has been occurring in the majority list of security logs with a percentage of around 90-95%, with the rest left for access and denial of service attacks [21]. Furthermore, it is recommended to perform intelligence gathering that deals with foot printing, scanning, and enumerating, as well as to establish threat modeling consist of attacker-centric, software-centric, and asset-centric [22]. VAPT activities are simply reconnaissance (mapping), enumeration (picture) and exploitation (execution) [23].

B. Research Methodology

In this study, the researchers employed qualitative methodology, which is an experiment by developing a framework to conduct VAPT systematically. The consideration in the experimental design is related to the variable that influences another called effect. It has the strength calculation to define significance and classification based on the industrial standard, benchmark, or matrix [24], [25]. There are still differences in the definition of the VAPT testing with the risk assessment, black-box evaluation, and performance measurement. Moreover, assessment emphasized the value or quality of something through the strict procedure while evaluation focused on the effectiveness or performance of certain activities. On the other hand, measurement prioritizes on the level of hierarchy by labeling the useful detail before the process. In this case, the researchers describe VAPT as the documentation process to retrieve evidence through experimentation towards a specific object or product based on certain objectives. One of them is related to the identification of the possibility of exploitation within the system. This research also has several drivers, namely understanding the way of business process is organized and operated, locating the application and data that are used, searching for hidden data sources that may allow access to secure information and identifying both virtual and physical servers that run application necessary for business operation. The VAPT also can keep track of what security measures are already in place and scan the network for vulnerability based on goal-oriented. In this study's framework, which derived from literature analysis; there are 8 (eight) linear steps that should be considered for a complete process of VAPT. As can be seen from the figure. 2, the discovery analysis has five domains, which are Directory Listing, User Information Disclosure, PHPInfo Disclosure, Folder Webserver Disclosure and Potential Vulnerability. Meanwhile, in the detection test, there are two domains involve description & analysis as well as recommended remediation.

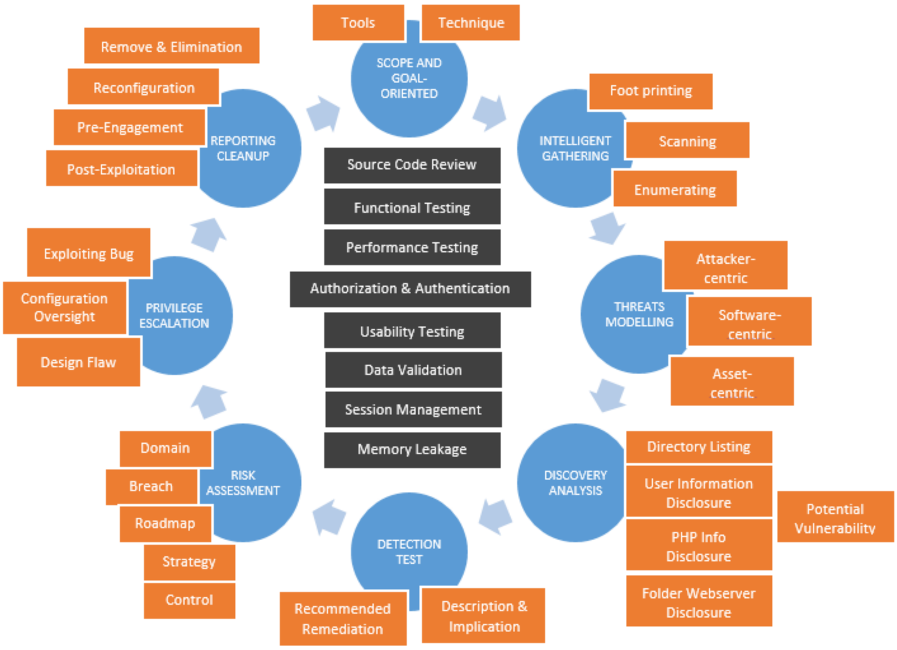
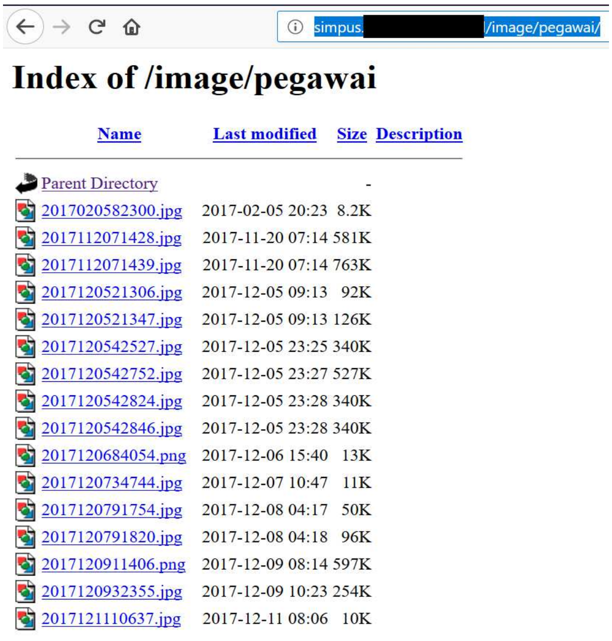


Fig. 2 VAPT Framework

III. Results and Discussion

A. Directory Listing



simpus.[redacted]/image/pegawai/

Index of /image/pegawai

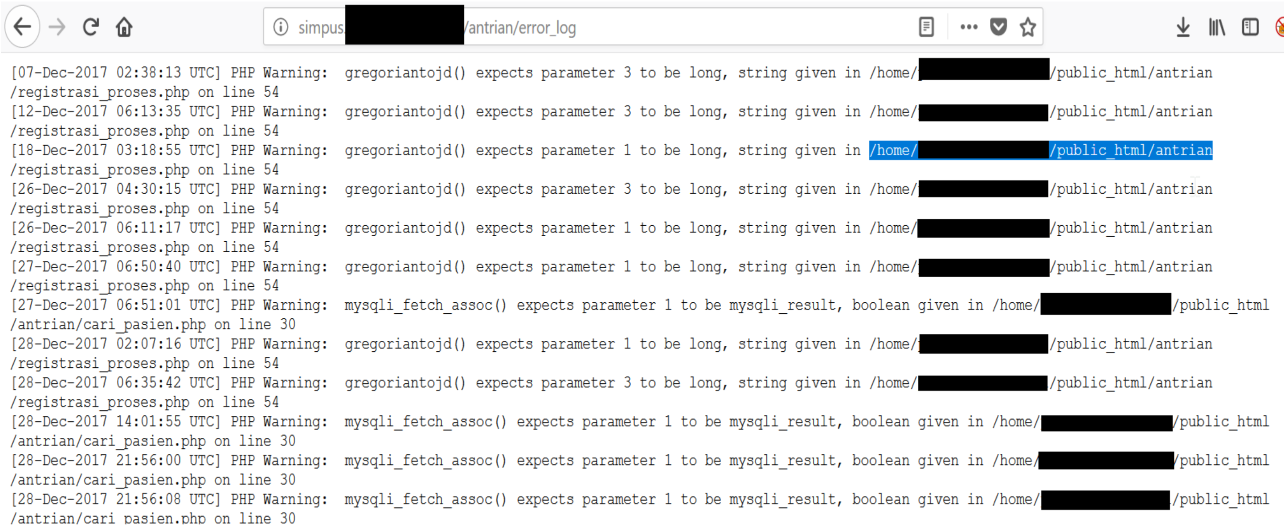
Name	Last modified	Size	Description
Parent Directory		-	
2017020582300.jpg	2017-02-05 20:23	8.2K	
2017112071428.jpg	2017-11-20 07:14	581K	
2017112071439.jpg	2017-11-20 07:14	763K	
2017120521306.jpg	2017-12-05 09:13	92K	
2017120521347.jpg	2017-12-05 09:13	126K	
2017120542527.jpg	2017-12-05 23:25	340K	
2017120542752.jpg	2017-12-05 23:27	527K	
2017120542824.jpg	2017-12-05 23:28	340K	
2017120542846.jpg	2017-12-05 23:28	340K	
2017120684054.png	2017-12-06 15:40	13K	
2017120734744.jpg	2017-12-07 10:47	11K	
2017120791754.jpg	2017-12-08 04:17	50K	
2017120791820.jpg	2017-12-08 04:18	96K	
2017120911406.png	2017-12-09 08:14	597K	
2017120932355.jpg	2017-12-09 10:23	254K	
2017121110637.jpg	2017-12-11 08:06	10K	

Fig. 3 Screenshot of Directory Listing

Penetration testing related to a simulation of the hacking process to identify security threats, which can be called ethical hacking. Importantly, there are specific points to be considered before conducting the testing, such as understanding the consequences of the risk related to the data stored and the test coverage to align with goal-oriented. In this VAPT, it is found that the folder in the Simpus application is not protected so that the attacker can view the contents of files from several folders such as /image/ and /assets/. The attacker also can see the contents of files contained in certain folders, so it is dangerous if the folder on the website has several confidential data such as databases and user passwords. This type of threats has a severity level of low, so the recommendations can be given by adding empty index.htm files to each folder.

B. Full Path Disclosure

Full path disclosure vulnerabilities allow the attacker to know the information of the web path. This information will reveal a full error message to the attacker. By knowing the full error message, the attacker can predict the directory listed on that website. The attacker can also conduct direct access to the specific files on a directory. Another use of this full path this closure is predicting the directory of user information. The user information plays a critical role within companies, so the protection of personal data should be prioritized over the others. Unfortunately, Indonesia does not have specific legislation to administer and control personal data protection within an organization under government or private institution [26]. This type of threat can be overcome by hiding error message with a certain code of error message, for example, by displaying Error 404.



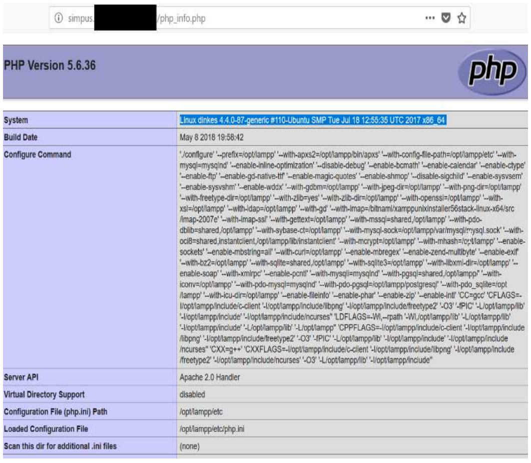
simpus[redacted]/antrian/error_log

```
[07-Dec-2017 02:38:13 UTC] PHP Warning:  gregoriantojd() expects parameter 3 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[12-Dec-2017 06:13:35 UTC] PHP Warning:  gregoriantojd() expects parameter 3 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[18-Dec-2017 03:18:55 UTC] PHP Warning:  gregoriantojd() expects parameter 1 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[26-Dec-2017 04:30:15 UTC] PHP Warning:  gregoriantojd() expects parameter 3 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[26-Dec-2017 06:11:17 UTC] PHP Warning:  gregoriantojd() expects parameter 1 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[27-Dec-2017 06:50:40 UTC] PHP Warning:  gregoriantojd() expects parameter 1 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[27-Dec-2017 06:51:01 UTC] PHP Warning:  mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in /home/[redacted]/public_html
/antrian/cari_pasien.php on line 30
[28-Dec-2017 02:07:16 UTC] PHP Warning:  gregoriantojd() expects parameter 1 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[28-Dec-2017 06:35:42 UTC] PHP Warning:  gregoriantojd() expects parameter 3 to be long, string given in /home/[redacted]/public_html/antrian
/registrasi_proses.php on line 54
[28-Dec-2017 14:01:55 UTC] PHP Warning:  mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in /home/[redacted]/public_html
/antrian/cari_pasien.php on line 30
[28-Dec-2017 21:56:00 UTC] PHP Warning:  mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in /home/[redacted]/public_html
/antrian/cari_pasien.php on line 30
[28-Dec-2017 21:56:08 UTC] PHP Warning:  mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in /home/[redacted]/public_html
/antrian/cari_pasien.php on line 30
```

Fig. 4 Screenshot of Full Path Disclosure

C. PHPInfo Disclosure

PHPInfo is valuable to explain the compiled information about the server's environment, which controls processing information such as cookie, server, GET, POST, and others. In this vulnerability, there is a phpinfo.php file that can be accessed by everyone. This file is dangerous because it contains detailed information about the webserver. An attacker can find out any information about the webserver, such as the type of web server is used, the version, and the information in it. This type of threats has a severity level of medium, so the recommendation that can be given is to delete the phpinfo.php file. Commonly, unauthorized parties after finding certain exploitable weaknesses within the system, they will design and testing the performance of the attack within their system that has a similar attribute. Then, they will try to secure the line to obtain full access, and privilege together eliminates the possibility to track the source before conducting a cyber-attack and delete the recovery process.

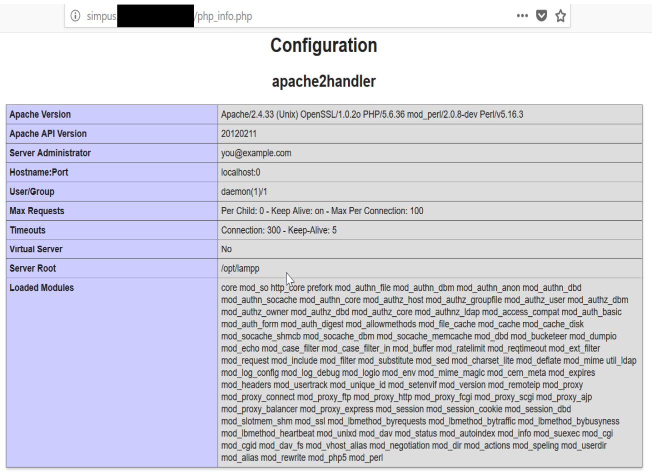


simpus[redacted]/php_info.php

PHP Version 5.6.36

System	Linux dinkes 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_64
Build Date	May 8 2018 19:58:42
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap=/bitnami/xamppunixinstaller56stack-linux-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/opt/lampp' '--with-mssql=shared,/opt/lampp' '--with-pdo-dblib=shared,/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/opt/lampp/' '--with-iconv=/opt/lampp' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo_sqlite=/opt/lampp' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar' '--enable-zip' '--enable-intl' 'CC=gcc' 'CFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'LDFLAGS=-Wl,--rpath '-Wl,/opt/lampp/lib' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-L/opt/lampp/lib' '-L/opt/lampp'' 'CPPFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'CXX=g++' 'CXXFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-I/opt/lampp/include/ncurses' '-O3' '-L/opt/lampp/lib' '-I/opt/lampp/include''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)

Fig. 5 Screenshot of PHPInfo (1)



simpus[redacted]/php_info.php

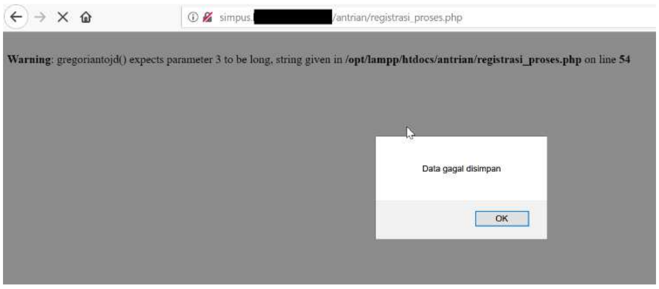
Configuration

apache2handler

Apache Version	Apache/2.4.33 (Unix) OpenSSL/1.0.2o PHP/5.6.36 mod_perl/2.0.8-dev Perl/v5.16.3
Apache API Version	20120211
Server Administrator	you@example.com
Hostname:Port	localhost:0
User/Group	daemon(1)/1
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	No
Server Root	/opt/lampp
Loaded Modules	core mod_so http_core prefork mod_authn_file mod_authn_dbm mod_authn_anon mod_authn_dbd mod_authn_socache mod_authn_core mod_authz_host mod_authz_groupfile mod_authz_user mod_authz_dbm mod_authz_owner mod_authz_dbd mod_authz_core mod_authnz_ldap mod_access_compat mod_auth_basic mod_auth_form mod_auth_digest mod_allowmethods mod_file_cache mod_cache mod_cache_disk mod_socache_shmcb mod_socache_dbm mod_socache_memcache mod_dbd mod_bucketeer mod_dumpio mod_echo mod_case_filter mod_case_filter_in mod_buffer mod_ratelimit mod_reqtimeout mod_ext_filter mod_request mod_include mod_filter mod_substitute mod_sed mod_charset_lite mod_deflate mod_mime util_ldap mod_log_config mod_log_debug mod_logio mod_env mod_mime_magic mod_cern_meta mod_expires mod_headers mod_usertrack mod_unique_id mod_setenvif mod_version mod_remoteip mod_proxy mod_proxy_connect mod_proxy_ftp mod_proxy_http mod_proxy_fcgi mod_proxy_scgi mod_proxy_ajp mod_proxy_balancer mod_proxy_express mod_session mod_session_cookie mod_session_dbd mod_slotmem_shm mod_ssl mod_lbmethod_byrequests mod_lbmethod_bytraffic mod_lbmethod_bybusyness mod_lbmethod_heartbeat mod_unixd mod_dav mod_status mod_autoindex mod_info mod_suexec mod_cgi mod_cgid mod_dav_fs mod_vhost_alias mod_negotiation mod_dir mod_actions mod_speling mod_userdir mod_alias mod_rewrite mod_php5 mod_perl

Fig. 6 Screenshot of PHPInfo (2)

D. Folder Webserver Disclosure



simpus[redacted]/antrian/registrasi_proses.php

Warning: gregoriantojd() expects parameter 3 to be long, string given in **/opt/lampp/htdocs/antrian/registrasi_proses.php** on line **54**

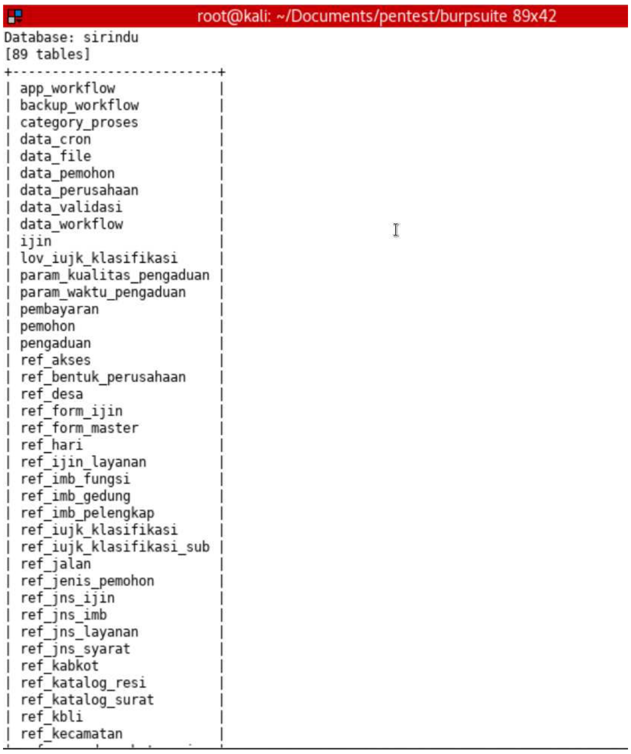
Data gagal disimpan

Fig. 7 Screenshot of Folder Webserver

When an HTTP client of web browser requests a URL that wants to access targeted sites within directory structure instead of the actual webpage in the directory, the web server generally serves the default page, often called as main or index, that offers content to the www. and have dedicated software and hardware to conduct its function. In this VA, it was found many errors in the application that raises sensitive information such as the folder's location from the webserver. When accessing the URL below, as the location of the folder used is /opt/lamp/htdocs/. There will be an error that raises the information. As a result of the ability to access this, the attacker can find out the location information of the webserver folder used. This type of threats has a severity level of medium, so the recommendation given is to make improvements on the coding side so that it does not cause errors.

E. Potential Vulnerability

In the process of penetration testing, there are fully identified threats that can be verified and confirmed positively based on experiment and monitoring process, but there are also cases, in a certain condition where they cannot be fully explained. It is recommended to establish a further step to determine whether they exist or not when the authentication mechanism or trusted scanner can reveal the location or their cause. In this, VAPT found a blind SQL injection gap in the licensing file monitoring function. SQL injection occurs because there is no filter from user input so that it can perform database query injection. An attacker can see all the contents of the database from the website dpmptsp where the database contains confidential data in the form of usernames, passwords, employee data and permitted community data, and others. This kind of threats has a severity of critical while the recommendation that can be given is to use the filter function mysql_real_escape () on the parameter/variable that captures input from the user. This taken picture is the result of a dump database from the website dpmptsp, where the name of the database used is Sirindu. There are 89 tables in the *sirindu* database, which contain all confidential data such as users, passwords, permission data, complaint data and more.



```
Database: sirindu
[89 tables]
+---------------------------+
| app_workflow              |
| backup_workflow           |
| category_proses           |
| data_cron                 |
| data_file                 |
| data_pemohon              |
| data_perusahaan           |
| data_validasi             |
| data_workflow             |
| ijin                      |
| lov_iujk_klasifikasi      |
| param_kualitas_pengaduan  |
| param_waktu_pengaduan     |
| pembayaran                |
| pemohon                   |
| pengaduan                 |
| ref_akses                 |
| ref_bentuk_perusahaan     |
| ref_desa                  |
| ref_form_ijin             |
| ref_form_master           |
| ref_hari                  |
| ref_ijin_layanan          |
| ref_imb_fungsi            |
| ref_imb_gedung            |
| ref_imb_pelengkap         |
| ref_iujk_klasifikasi      |
| ref_iujk_klasifikasi_sub  |
| ref_jalan                 |
| ref_jenis_pemohon         |
| ref_jns_ijin              |
| ref_jns_imb               |
| ref_jns_layanan           |
| ref_jns_syarat            |
| ref_kabkot                |
| ref_katalog_resi          |
| ref_katalog_surat         |
| ref_kbli                  |
| ref_kecamatan             |
```

Fig. 8 Example of an unacceptable low-resolution image

After conducting the VAPT, as it can be seen in table 1 about risk rating, which is defined four levels of categories: Critical, High, Medium, and Low, then this study identified five threats within three targets. In this case, critical level means an attack is expected that can endanger the resources and assets of the organization, while high level means an attack might disrupt the business process and operation, even the popularity. On the other hand, medium level defines that an attack is possible that can present certain profit loss while low level points out that an attack is unlikely but possible, which can reveal procedure about a specific project.

TABLE I
RISK RATING

	Risk Rating				
Target	Critical	High	Medium	Low	Total
xxx.go.id	-	-	-	-	0
Simpus.xxx.go.id	-	-	3	1	4
Dpmptsp.xxx.go.id	1	-	-	-	1
Total	1	-	3	1	5

IV. CONCLUSION

VAPT is a systematic process of deciding the weaknesses of an application that become popular and critical to promote security, reliability, and integrity. In the era of the technology advancement, which hacking become the trend among a society that threaten and endanger the harmony and business flow of a company, it is necessary to have standard to minimize risks and mitigate dangers. This study offers the developed framework to conduct VAPT to reduce the cost incurred and having a broad range of security measure and strategy for diverse application and IT resource, as well as to have a holistic view of the possibility of danger because of threats encountered within networks.

REFERENCES

[1] Symantec Corporation. *2017 Norton Cyber Security Insight Report Global Results.* Retrieved at January 2019 from: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[2] ITU-D. *Global Cybersecurity Index (GCI) 2017.* Retrieved at January 2019 from: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

[3] Statista. *Consumer Loss Through Cyber Crime Worldwide in 2017, by Victim Country (in billion US dollars).* Retrieved January 2019 from: https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/

[4] R. Kuncoro. Current State of Cybersecurity Readiness and Cybercrime Enforcement Capability in Indonesia. *Cybercrime Capacity Building Conference*, 27-28 April 2010. Indonesiaan National Police.

[5] A.G. Bacudio, X. Yuan, B.T.B.Chu and M. Jones. An Overview of Penetration Testing. Int. Journal of Network Security & Its Applications 3(6), pp. 19-38, 2011.

[6] K. Palanisamy. *Network Penetration Testing*. White Paper: Happiest People Happiest Customer, 2014.

[7] T.S. Gunawan, M.K. Lim, M. Kartiwi, N.A. Malik and N. Ismail. Penetration Testing using Kali Linux: SQL Injection, XSS, Wordpress and WPA2 Attacks. *Indonesian J. of Electrical Engineering and Com. Science*, vol. 12(2), Nov., pp. 729-737, 2018.

[8] PTES Team. *The Penetration Testing Execution Standard Documentation: Release 1.1 (February 8th, 2017).* Retrieved at January 2019 from: https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf

[9] KSM Consulting. *Cybersecurity Guide: Vulnerability Assessments and Penetration Testing.* Retrieved at January 2019 from: https://www.ksmconsulting.com/wp-content/uploads/2017/10/CS-Guide_Vulnerability-Assessment-and-Penetration-Testing.pdf

[10] S. Marsiske, A. Mishra, M. Saptarshi and P. Piolon. *Penetration Test Report v.1.0*. Open Tech Fund, 2018.

[11] Cisco. Cisco Network Penetration Testing. Retrieved at January 2019 from:https://www.cisco.com/c/dam/en/us/services/collateral/se/NetPenTest-AAG.pdf

[12] R. Ackroyd, A. Mason and G. Watson. *Social Engineering Penetration Testing*. Syngress, April 2014.

[13] F. Abu-Dabaseh and E. Alshammari. Automated Penetration Testing: An Overview. 4th *Inter. Conference on Natural Languange Computing (NATL)* 2018.

[14] C. Weissman. *Handbook for the Computer Security Certification of Trusted Systems*. IATAC (Inf. Assurance Tech. Analysis Center), DTIC (Defense Technical Inf. Center), 1996.

[15] S. Shah and B.M. Mehtre. An Overview of Vulnerability Assessment and Penetration Testing Techniques. *Journal of Computer Virology and Hacking Techniques*, vol. 11(1), pp. 27-49, 2015.

[16] R. Baloch. *Ethical Hacking and Penetration Testing Guide*. CRC Press: Taylor & Francis Group, 2015.

[17] M. Lubis, N.I. Yaacob, H. Reh and M. Ambag. Study on Implementation and Impact of Google Hacking in Internet Security. *Proc. of Regional Con. on Knowledge Integration in ICT*, 2010.

[18] M. Lubis, M. Kartiwi and S. Zulhuda. Election Fraud and Privacy Related Issues: Addressing Electoral Integrity. *Int. Con. on Informatics and Computing (ICIC)*, 2016.

[19] AR Ahlan and M. Lubis. Information Security Awareness in University: Maintaining Learnability, Performance and Adapability through Roles of Responsibility. *Information Assurance and Security (IAS)*, 2011.

[20] AR Ahlan, M. Lubis and A.R. Lubis. Information Security Awareness at Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science* 72, 361-373, 2015.

[21] A.R. Lubis, F. Fachrizal, M. Lubis and H.M. Tahir. Wireless Service at Public University: A Survey of Users Perception on Security Aspects. *Proc. of Int. Conf. on Inf. and Communications Technology (ICOIACT)* 2018.

[22] S.K. Lamichhane. *Penetration Testing in Wireless Networks*. Bachelor Thesis, Helsinki Metropolia University of Applied Sciences, 2016.

[23] C.T. Phong. *A Study of Penetration Testing Tools and Approaches*. Master Thesis, Auckland University of Technology, 2014.

[24] K. Leiviska. *Introduction to Experiment Design*. University of Oulu, Control Engineering Laboratory, 2013.

[25] W.J. Diamond. *Practical Experiment Design for Engineers and Scientiests*. Lifetime Learning Publications, 1981.

[26] M. Lubis, M. Kartiwi and S. Zulhuda. Current State of Personal Data Protection in Electronic Voting: Criteria and Indicator for Effective Implementation. *Telkomnika*, vol. 16(1), pp. 290-301, 2018.