

PENCEGAHAN SERANGAN JUDI ONLINE PADA WEBSITE PEMERINTAHAN

**DINAS KOMUNIKASI, INFORMATIKA
DAN STATISTIK KOTA CIREBON**

**Di susun oleh :
AKBAR HARIWIBOWO
YONO SURYONO**



Tujuan Paparan

- Mengidentifikasi Penyebab: Menjelaskan faktor-faktor yang menyebabkan serangan judi online pada website pemerintahan.
- Strategi Pencegahan: Mempresentasikan langkah-langkah konkret yang dapat diambil untuk mencegah serangan dan melindungi integritas website pemerintah.

Penyebab (Dugaan)

Penyebab Umum:

- Kurangnya sistem keamanan yang memadai
- Ketidakpahaman pengguna mengenai risiko online
- Penggunaan platform dan software yang rentan

Faktor Eksternal:

- Meningkatnya serangan siber dari kelompok kriminal
- Penyebaran informasi yang tidak benar tentang perjudian online

Tindak Lanjut (Respons terhadap Serangan)

a)

Identifikasi dan Analisis Insiden:

- Proses pengumpulan data
- Analisis jenis serangan

b)

Penanggulangan Segera:

- Memperbaiki kerentanan yang ditemukan
- Pemantauan aktif terhadap website

**https://kellemahwungkuk.cirebonko
ta.go.id/author/?
kocok=situs+slot+dana**

TEMUAN LOG -> [19/Oct/2024:10:26:14 +0700] "GET /images/b374k-mini-shell.php HTTP/2" 404 708

"http://kellemahwungkuk.cirebonkota.go.id/images/b374k-mini-shell.php"

"Go-http-client/2.0"

https://rsdgunungjati.cirebonkota.go.id/royal/

rsdgunungjati.cirebonkota.go.id-ssl_log-Oct-2024 X

C: > Users > egovk > AppData > Local > Temp > 47986277-9c8c-44ee-b1b7-924eda29a60b_rsdgunungjati.cirebonkota.go.id-ssl_log-Oct-2024.gz.60b > rsdgunungjati.cirebonkota.go.id-ssl_log-Oct-2024

```
251401 152.42.234.184 - - [16/Oct/2024:17:26:12 +0700] "POST //wp-login.php HTTP/1.1" 200 6173 "https://rsdgunungjati.cirebonkota.go.id/royal/" "Mozilla/5.0"
251402 72.14.201.146 - - [16/Oct/2024:17:27:08 +0700] "GET / HTTP/2" 200 28666 "https://www.google.com/" "Mozilla/5.0"
251403 46.248.185.247 - - [16/Oct/2024:17:30:55 +0700] "GET / HTTP/1.1" 200 258587 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0"
251404 85.208.96.211 - - [16/Oct/2024:17:31:26 +0700] "GET /robots.txt HTTP/1.1" 200 140 "-" "Mozilla/5.0 (compatible; SemrushBot/7~bl; +http://www.semrush.com/bot.html)"
251405 103.105.142.195 - - [16/Oct/2024:17:37:36 +0700] "GET / HTTP/1.1" 200 36152 "-" "Python/3.11 aiohttp/3.9.2"
251406 164.90.157.94 - - [16/Oct/2024:17:38:23 +0700] "GET / HTTP/2" 200 258587 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/121.0"
251407 180.245.222.176 - - [16/Oct/2024:17:29:05 +0700] "GET /wp-content/plugins/apex-notification-bar-lite/css/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/2" 200 77160 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251408 180.245.222.176 - - [16/Oct/2024:17:29:02 +0700] "GET /wp-content/uploads/2021/10/logorsgj-removebg-preview.png HTTP/2" 200 34809 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251409 180.245.222.176 - - [16/Oct/2024:17:29:00 +0700] "GET /wp-content/uploads/2022/03/Sequence-03.gif HTTP/2" 200 682000 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251410 180.245.222.176 - - [16/Oct/2024:17:29:09 +0700] "GET /wp-content/uploads/2022/03/cropped-Sequence-03-192x192.gif HTTP/2" 200 16261 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251411 180.245.222.176 - - [16/Oct/2024:17:29:09 +0700] "GET /wp-content/uploads/2022/03/cropped-Sequence-03-32x32.gif HTTP/2" 200 1595 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251412 193.186.4.176 - - [16/Oct/2024:17:30:35 +0700] "GET / HTTP/2" 200 28666 "https://www.google.com/" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0"
251413 85.208.96.207 - - [16/Oct/2024:17:31:28 +0700] "GET /rumah-sakit-daerah-gunung-jati-kota-cirebon-berpartisipasi-pemeriksaan-kesehatan-gratis-dalam-kegiatan-karnaval-sc HTTP/2" 200 28666 "https://www.google.com/"
251414 202.46.68.120 - - [16/Oct/2024:17:45:22 +0700] "GET /jadwal-dokter HTTP/1.1" 301 0 "-" "WhatsApp/2.23.20.0"
251415 202.46.68.120 - - [16/Oct/2024:17:45:22 +0700] "GET /jadwal-dokter/ HTTP/1.1" 200 17629 "-" "WhatsApp/2.23.20.0"
251416 202.46.68.120 - - [16/Oct/2024:17:45:22 +0700] "GET /jadwal-dokter/ HTTP/1.1" 200 17629 "-" "WhatsApp/2.23.20.0"
251417 202.46.68.120 - - [16/Oct/2024:17:45:22 +0700] "GET /wp-content/uploads/2021/10/cropped-logorsgj-removebg-preview.png HTTP/1.1" 200 29836 "-" "WhatsApp/2.23.20.0"
251418 103.105.142.195 - - [16/Oct/2024:17:45:24 +0700] "POST /wp-cron.php?doing_wp_cron=1729075524.3665339946746826171875 HTTP/1.1" 200 0 "-" "WordPress/6.6.2; https://rsdgunungjati.cirebonkota.go.id/royal/"
251419 66.249.69.104 - - [16/Oct/2024:17:45:23 +0700] "GET /slot-thailand/sitemap.xml HTTP/1.1" 404 15338 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
251420 103.105.142.195 - - [16/Oct/2024:17:45:25 +0700] "POST /wp-admin/admin-ajax.php?action=async_litespeed&nonce=5wsi8CYH5IiIALBbsGZflKwlvmoJvYRI&litespeed_type=imgoptm HTTP/2" 200 0 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251421 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/plugins/float-menu/public/assets/css/style.min.css?ver=6.0.4 HTTP/2" 200 2008 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251422 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/plugins/recent-posts-widget-with-thumbnails/public.css?ver=7.1.1 HTTP/2" 200 400 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251423 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/themes/popularfx/sidebar.css?ver=1.2.5 HTTP/2" 200 2079 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251424 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-includes/css/dist/block-library/style.min.css?ver=6.6.2 HTTP/2" 200 13903 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251425 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/uploads/popularfx-templates/eduhub/style.css?ver=1.2.5 HTTP/2" 200 989 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251426 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/plugins/float-menu/vendors/fontawesome/css/all.min.css?ver=6.6 HTTP/2" 200 21821 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251427 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/plugins/apex-notification-bar-lite/css/frontend/responsive.css?ver=6.6.2 HTTP/2" 200 5925 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251428 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1 HTTP/2" 200 4678 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251429 202.46.68.120 - - [16/Oct/2024:17:45:32 +0700] "GET /wp-content/plugins/apex-notification-bar-lite/js/frontend/jquery.scroller.js?ver=2 HTTP/2" 200 4142 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251430 202.46.68.120 - - [16/Oct/2024:17:45:31 +0700] "GET /jadwal-dokter/ HTTP/2" 200 15028 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0"
251431 114.5.212.115 - - [16/Oct/2024:17:45:31 +0700] "GET /wp-content/uploads/2022/06/9777_ELSHINTADOTCOM_20210827_485.png HTTP/2" 200 392532 "https://www.google.com/" "Mozilla/5.0"
251432 103.105.142.195 - - [16/Oct/2024:17:45:26 +0700] "POST /wp-admin/admin-ajax.php?action=as_async_request_queue_runner&nonce=40b4023cac HTTP/1.1" 200 0 "-" "WordPress/6.6.2"
251433 202.46.68.120 - - [16/Oct/2024:17:45:33 +0700] "GET /wp-content/uploads/2021/10/logorsgj-removebg-preview.png HTTP/2" 200 34809 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251434 202.46.68.120 - - [16/Oct/2024:17:45:33 +0700] "GET /wp-content/uploads/2021/10/rshitam.png HTTP/2" 200 1243 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251435 202.46.68.120 - - [16/Oct/2024:17:45:34 +0700] "GET /wp-content/plugins/float-menu/public/assets/js/velocity.min.js?ver=6.0.4 HTTP/2" 200 15569 "https://rsdgunungjati.cirebonkota.go.id/royal/"
251436 202.46.68.120 - - [16/Oct/2024:17:45:34 +0700] "GET /wp-content/plugins/float-menu/public/assets/js/floatMenu.min.js?ver=6.0.4 HTTP/2" 200 6350 "https://rsdgunungjati.cirebonkota.go.id/royal/"
```

https://rsdgunungjati.cirebonkota.go.id/royal/

Warning 3

Sep 24 05:45:28 I LAPTOP-39N5PT0P/192.168.175.206

MODULE: Filescan

MESSAGE: Malware file found

SCORE: 84

FILE: D:\DKIS Kota Cirebon\Backup Website 23 September 2024\Backup 19 September 2024\rsudgj_crb\public_html\wp-admin\user\about\index.php

EXT: .php

TYPE: UNKNOWN

SIZE: 80292

MD5: c1da27185684c7d50adab602c2ed6b4a

SHA1: 35840532078283c4fdf466c46b1ac09f21e9788f

SHA256: 318dc4f1630bf237b52763f74479f8b418aaa6fcd67b0c8ee0a243e1cdaa50fe

FIRSTBYTES: 3c21646f63747970652068746d6c3e0a3c68746d / <!doctype html> <htm

CREATED: Mon Sep 23 16:17:09.195 2024

MODIFIED: Fri Mar 29 15:45:45.000 2024

ACCESSED: Mon Sep 23 16:17:09.195 2024

PERMISSIONS: BUILTIN\Administrators:F / BUILTIN\Users:R / NT AUTHORITY\Authenticated Users:C / NT AUTHORITY\SYSTEM:F

OWNER: LAPTOP-39N5PT0P\egovk

REASON_1: YARA rule Shell_IndoXploit / Detects IndoXploit webshell and related exploits

SUBSCORE_1: 75

REF_1: not set

SIGTYPE_1: internal

SIGCLASS_1: YARA Rule

MATCHED_1

- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"
- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"
- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"

RULEDATE_1: 2024-08-08

RULENAME_1: [Shell_IndoXploit](#)

AUTHOR_1: Suharyanto

REASON_2: YARA rule Shell_IndoXploit / Detects IndoXploit webshell and related exploits

SUBSCORE_2: 75

REF_2: not set

SIGTYPE_2: custom

SIGCLASS_2: YARA Rule

MATCHED_2

- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"
- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"
- **gacor** at 0x8b2in
"er luar negeri dan menjadi salah satu situs paling **gacor** sedunia." />\x0a <meta itemprop="thumbnailUrl" co"

RULEDATE_2: 2024-08-08

RULENAME_2: [Shell_IndoXploit](#)

<http://simenor.appdevel.cirebonkota.go.id/upload/site/?colamut=77slot>

Sudah di nonaktifkan 11 Juni 2024

Upaya Pencegahan

Sistem Keamanan yang Diperkuat:

- Implementasi firewall dan antivirus
- Pembaruan rutin perangkat lunak

Pendidikan dan Pelatihan:

- Pelatihan untuk staf mengenai keamanan siber
- Sosialisasi kepada masyarakat tentang bahaya judi online

Upaya Pencegahan

- Defender Masking URL Slug Login (Halaman Login) Plugin
- Tambahkan kode berikut di wp-config.php:
`define('DISALLOW_FILE_EDIT', true);`
- Instal plugin : Wordfence , Limit login Attempts

Upaya Pencegahan

Disabled XMLRPC

Tambahkan
berikut
.htaccess :

kode
pada
file

```
<Files xmlrpc.php>  
order deny,allow  
deny from all  
</Files>
```

Upaya Pencegahan

Blocking .php
.htacces /wp-
content/upload

/

Tambahkan file .htaccess
pada wp-
content/upload/. dengan
perintah berikut :

```
<Files *.php>  
deny from all  
</Files>
```

TERIMA KASIH

"Keamanan situs adalah investasi terpenting; lakukan pembaruan rutin, gunakan password yang kuat, dan selalu buat cadangan—lindungi harta digital Anda seperti yang Anda lakukan untuk kehidupan nyata."