

P R E S E N T A T I O N

CYBER ATTACK

Start



CYBER ATTACK ?

- Cyber attack merupakan tindak kejahatan yang dilakukan oleh para peretas dengan tujuan untuk merusak jaringan atau sistem komputer. Selain menimbulkan berbagai kerusakan, cyber attack biasanya juga dilakukan untuk mencuri data penting yang tersimpan di dalam server.

JENIS CYBER ATTACK ?



MALWARE

Malware merupakan virus yang dikirim ke dalam komputer atau sistem. Virus ini dapat menghilangkan dokumen penting yang tersimpan di dalam database atau bahkan dicuri. Serangan dapat terjadi apabila Anda mengakses website yang memiliki tanda "not secure" pada bagian atasnya berarti belum diperkuat sistem keamanan yang baik sehingga hal ini dapat menjadi kesempatan bagi para pelaku cyber attack untuk menyebarkan virus malware.

SQL INJECTION

SQL merupakan singkatan dari Structured Query Language. SQL ini termasuk ke dalam bahasa pemrograman yang ditujukan untuk segala kebutuhan yang berkaitan dengan database. Pemrograman SQL dengan sistem keamanan yang lemah atau penggunaan bahasa program yang kurang baik dapat menjadi sasaran empuk para pelaku cyber attack untuk meluncurkan serangan SQL Injection. Hacker dapat melakukan manipulasi database melalui serangan ini.

DDOS

DDoS atau Distributed Denial of Service merupakan serangan cyber yang sering dialami oleh para pemilik website bisnis. Serangan ini mampu memperlambat kecepatan suatu website sehingga pengunjungnya akan langsung meninggalkan website tersebut.

PHISHING

Anda mungkin sering mendengar istilah phishing dalam kasus penipuan uang melalui telepon yang sering disebut dengan voice phishing. Lain halnya di dalam dunia bisnis, kejahatan phishing yang terjadi termasuk ke dalam cyber attack di mana pelakunya dapat melakukan pencurian data melalui jenis serangan ini.



C Y B E R A T T A C K

**TERJADI DI PEMKAB SOLOK
SELATAN**

DAFTAR 1

DAFTAR 2

SLOT GACOR TERBARU 2022



STEP 1

Daftar untuk
mendapatkan
User ID



STEP 2

Deposit ke
rekening
tujuan
yang telah
diberikan



STEP 3

Mainkan
berbagai
permainan
menarik kami
dan semoga
beruntung



STEP 4

Menangkan
dan withdraw
kemenangan
anda



SLOT ONLINE

SLOT GACOR 2022

P E N A N G A N A N

CYBER ATTACK DI PEMKAB SOLOK SELATAN

Malware scanner

USERS MALICIOUS SCAN HISTORY 29 IGNORE LIST

Malicious (13)

Malware detected by imunifyAV

Clean up all

Timeframe

Status

Search

Your server is infected. Do you want to **clean it up** ?

	Scan date	Type	Username	Malicious	Reason	Status	Actions
	November 21, 2022 9:35 PM		homes6668	/home/home.solselkab.go.id/public_html/public/filesystem.php	SMW-BLKH-1311081-php.bkdr.aut o244	Infected	
	November 21, 2022 8:17 PM		tests8254	/home/test.solselkab.go.id/public_html/public/deploy/js/cmapi/logs.php	SMW-BLKH-1754557-php.bkdr.ws hll	Infected	
	November 21, 2022 9:35 PM		homes6668	/home/home.solselkab.go.id/public_html/index.php	SMW-INJ-20917-php.bkdr.oneliner -0	Infected	
	November 21, 2022 9:35 PM		homes6668	/home/home.solselkab.go.id/public_html/info.php	SMW-INJ-20917-php.bkdr.oneliner -0	Infected	
	November 21, 2022 9:35 PM		homes6668	/home/home.solselkab.go.id/public_html/public/index.php	SMW-INJ-20917-php.bkdr.oneliner -0	Infected	
	November 21, 2022 4:39 PM		helpd5238	/home/helpdesk.solselkab.go.id/public_html/tunnel.php	SMW-SA-04684-php.tool.db-2	Infected	

> localhost > Downloads > home.solselkab.go.id.access_log

```
6.67.234.41 - - [15/Nov/2022:21:53:23 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/uploads HTTP/2" 200 38752 "https://home.solselkab
6.67.234.41 - - [15/Nov/2022:21:53:25 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html HTTP/2" 200 37969 "https://home.solselkab.go.id/u
6.67.234.41 - - [15/Nov/2022:21:53:26 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor HTTP/2" 200 37732 "https://home.solselkab.
6.67.234.41 - - [15/Nov/2022:21:53:28 +0700] "GET /guestbook HTTP/1.1" 200 9746 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0; +http:/
6.67.234.41 - - [15/Nov/2022:21:53:31 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor/guzzlehttp HTTP/2" 200 37630 "https://home
6.67.234.41 - - [15/Nov/2022:21:53:33 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor/guzzlehttp/promises HTTP/2" 200 37731 "htt
6.67.234.41 - - [15/Nov/2022:21:53:35 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor/guzzlehttp/promises/src HTTP/2" 200 38152
6.67.234.41 - - [15/Nov/2022:21:53:39 +0700] "POST /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor/guzzlehttp/promises/src HTTP/2" 200 38225
6.67.234.41 - - [15/Nov/2022:21:53:46 +0700] "GET /assets/plugins/font-awesome/fonts/fontawesome-webfont.woff?v=4.2.0 HTTP/1.1" 200 65452 "-" "Mozilla/5.0 AppleWebKit/5
6.67.234.41 - - [15/Nov/2022:21:53:58 +0700] "GET /vendor/guzzlehttp/promises/src/ddwwqq.php HTTP/2" 200 381 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
6.67.234.41 - - [15/Nov/2022:21:54:01 +0700] "POST /vendor/guzzlehttp/promises/src/ddwwqq.php HTTP/2" 200 38189 "https://home.solselkab.go.id/vendor/guzzlehttp/promises
6.67.234.41 - - [15/Nov/2022:21:54:07 +0700] "GET /cms/Slideshow/delete_data/27/1 HTTP/2" 307 0 "https://home.solselkab.go.id/cms/Slideshow" "Mozilla/5.0 (Windows NT 10
6.67.234.41 - - [15/Nov/2022:21:54:07 +0700] "GET /cms/Slideshow HTTP/2" 200 6578 "https://home.solselkab.go.id/cms/Slideshow" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
6.67.234.41 - - [15/Nov/2022:21:54:07 +0700] "GET /assets/plugins/fancybox/source/jquery.fancybox.css?v=2.1.5 HTTP/2" 404 565 "https://home.solselkab.go.id/cms/Slidesho
6.67.234.41 - - [15/Nov/2022:21:54:07 +0700] "GET /assets/plugins/fancybox/lib/jquery.mousewheel-3.0.6.pack.js HTTP/2" 404 565 "https://home.solselkab.go.id/cms/Slidesh
6.67.234.41 - - [15/Nov/2022:21:54:07 +0700] "GET /assets/plugins/fancybox/source/jquery.fancybox.js?v=2.1.5 HTTP/2" 404 565 "https://home.solselkab.go.id/cms/Slideshow
6.67.234.41 - - [15/Nov/2022:21:54:11 +0700] "GET /uploads/file/ddwwqq.php?path=/home/home.solselkab.go.id/public_html/vendor/guzzlehttp/promises/src HTTP/2" 200 38189
6.67.234.41 - - [15/Nov/2022:21:54:16 +0700] "GET /uploads/file/ddwwqq.php HTTP/2" 200 41376 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
6.67.234.41 - - [15/Nov/2022:21:54:16 +0700] "GET /assets/front/css/bootstrap.min.css HTTP/1.1" 200 9426 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com
6.67.234.41 - - [15/Nov/2022:21:54:18 +0700] "GET /uploads/file/ HTTP/2" 404 705 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
6.67.234.41 - - [15/Nov/2022:21:54:20 +0700] "GET /uploads/file/ddwwqq.php HTTP/2" 200 41362 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
6.67.234.41 - - [15/Nov/2022:21:54:32 +0700] "POST /uploads/file/ddwwqq.php?option&path=/home/home.solselkab.go.id/public_html/uploads/file HTTP/2" 200 41352 "https://h
6.67.234.41 - - [15/Nov/2022:21:54:36 +0700] "GET /uploads/file/ddwwqq.php HTTP/2" 404 565 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
6.67.234.41 - - [15/Nov/2022:21:10:11 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 36526600 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64;
6.67.234.41 - - [15/Nov/2022:21:09:33 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 36960776 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64;
6.67.234.41 - - [15/Nov/2022:21:14:12 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 35274752 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64;
6.67.234.41 - - [15/Nov/2022:21:55:16 +0700] "GET /home/akun/cms?_id=1668524047755 HTTP/2" 200 1500 "https://home.solselkab.go.id/cms/Slideshow" "Mozilla/5.0 (Windows NT
6.67.234.41 - - [15/Nov/2022:21:55:23 +0700] "GET /uploads/kepegawaian/pasfoto/ HTTP/2" 404 705 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
6.67.234.41 - - [15/Nov/2022:21:55:05 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 757028 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
6.67.234.41 - - [15/Nov/2022:21:55:31 +0700] "GET /halaman/pariwisata_kebudayaan HTTP/1.1" 200 397116 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.c
6.67.234.41 - - [15/Nov/2022:21:55:00 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 892165 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
6.67.234.41 - - [15/Nov/2022:21:51:45 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 4833280 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x
6.67.234.41 - - [15/Nov/2022:21:55:22 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 367908 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
6.67.234.41 - - [15/Nov/2022:21:55:37 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 114354 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
6.67.234.41 - - [15/Nov/2022:21:55:39 +0700] "GET / HTTP/1.1" 200 1369 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.10) Gecko/20060927 Firefox/1.0.4 (Debian pack
6.67.234.41 - - [15/Nov/2022:21:55:40 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 57209 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
6.67.234.41 - - [15/Nov/2022:21:52:34 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 5455872 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x
6.67.234.41 - - [15/Nov/2022:21:55:37 +0700] "GET /assets/video/portal.mp4 HTTP/1.1" 206 196608 "https://home.solselkab.go.id/" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
```





























AnonSecTeam

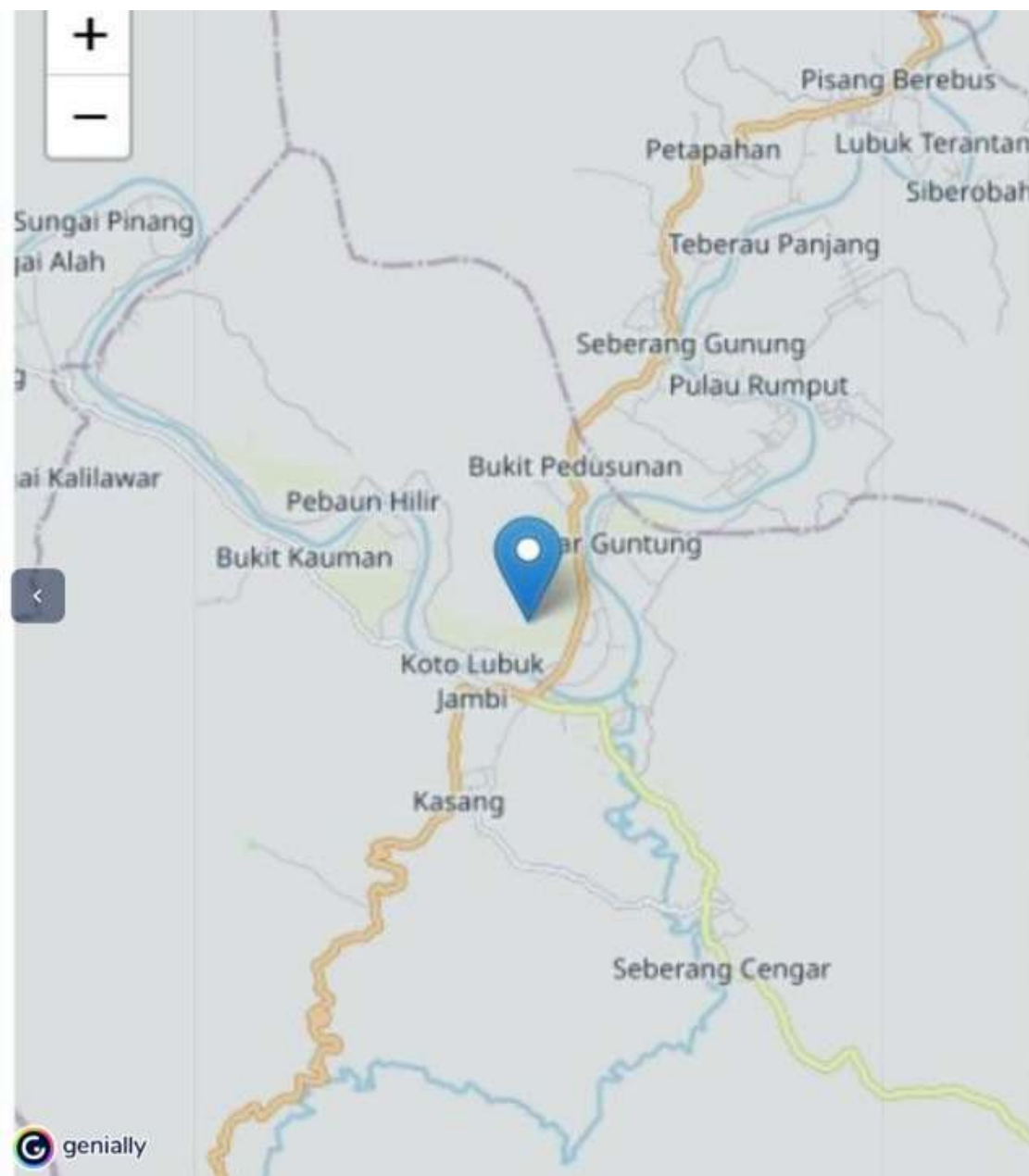
Path: /home/test.wolseikab.go.id/public_html/
[Home]

Pilih File

Tidak ada file yang dipilih

Upload

Name	Size	Permissions	Last Update	Options
[D] app	--	drwxr-xr-x	11-Jul-2022 13:24	 
[D] logs	--	drwxr-xr-x	21-Nov-2022 14:38	 
[D] public	--	drwxr-xr-x	11-Jul-2022 13:21	 
[D] tests	--	drwxr-xr-x	28-Aug-2022 13:15	 
[D] vendor	--	drwxr-xr-x	11-Jul-2022 13:23	 
< [D] writable	--	drwxr-xr-x	11-Jul-2022 13:23	 
[F] .env	4.418 KB	-rw-r--r--	25-Aug-2022 05:41	 
[F] .gitignore	1.816 KB	-rw-r--r--	23-Mar-2022 02:48	 
[F] .htaccess	1.737 KB	-rw-r--r--	02-Oct-2021 19:36	 
[F] LICENSE	1.132 KB	-rw-r--r--	23-Mar-2022 02:48	 
[F] README.md	2.66 KB	-rw-r--r--	23-Mar-2022 02:48	 
[F] builds	3.811 KB	-rw-r--r--	23-Mar-2022 02:48	 
[F] composer.json	1.024 KB	-rw-r--r--	23-Mar-2022 02:48	 
[F] composer.lock	91.3 KB	-rw-r--r--	23-Mar-2022 02:48	 



useragent	Mozilla/5.0 (Linux; Android 12; CPH2127) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36
ip	114.125.28.206
country	Indonesia
city	Lubuk Jambi
state	Riau
referrer	https://home.solselkab.go.id/
bot	Not
latitude	-0.651700000000000010
longitude	101.468000000000000000

THANKS!

