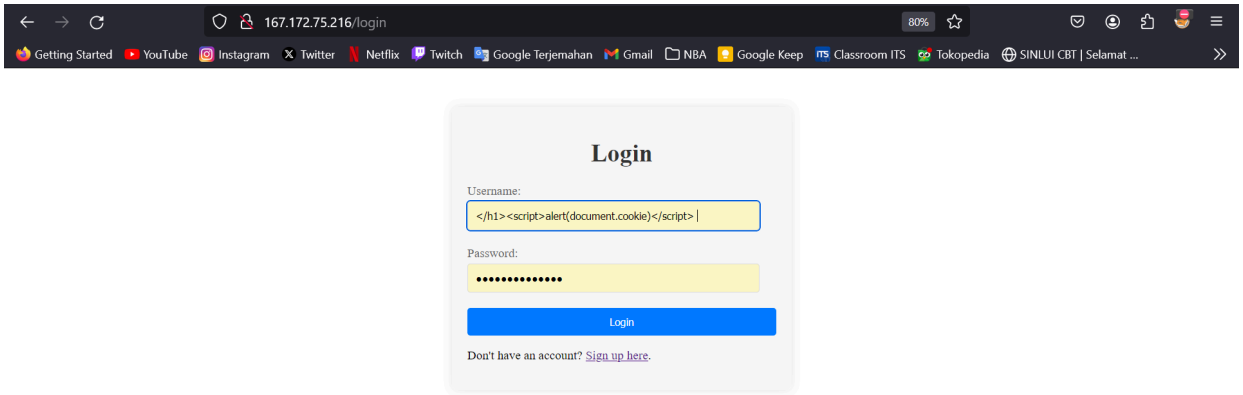
Nicholas Marco Weinandra
5027221042

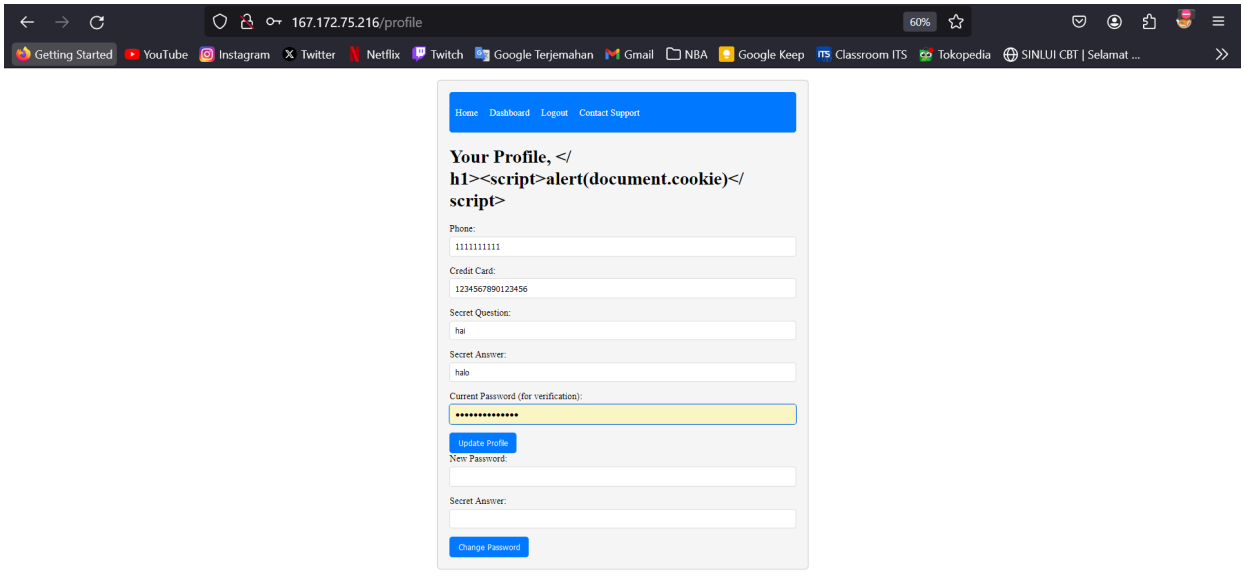
XSS Vulnerability pada form kolom Username

---

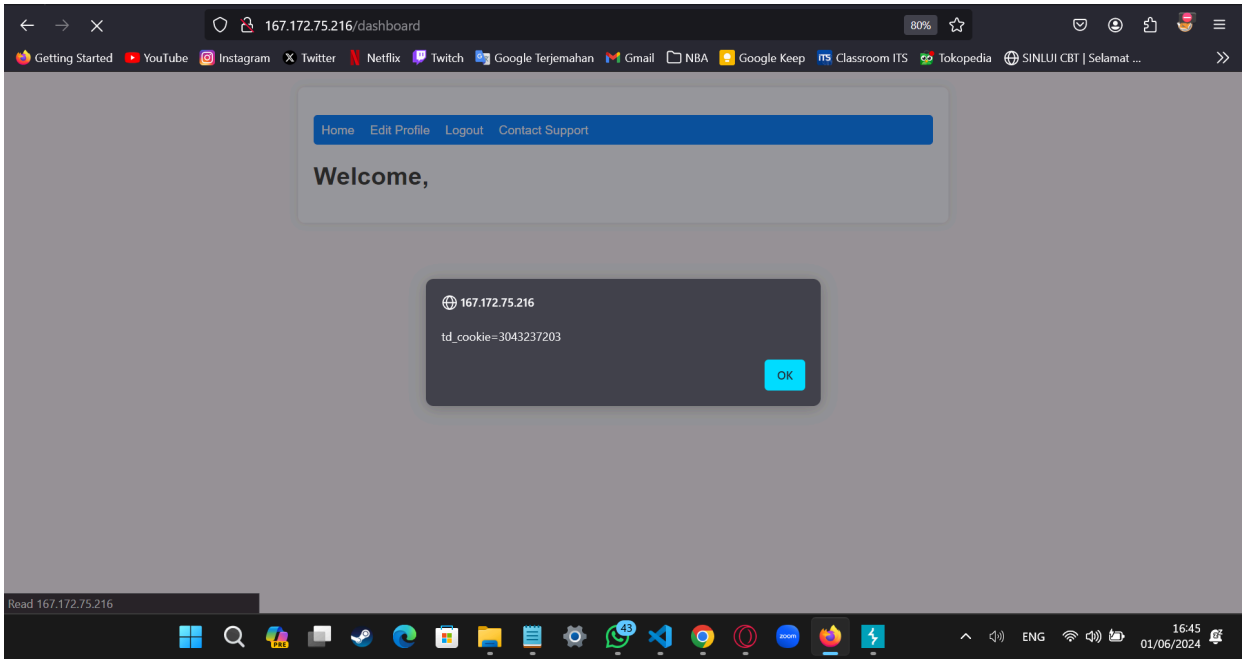
1. Register dengan menggunakan script pada username.



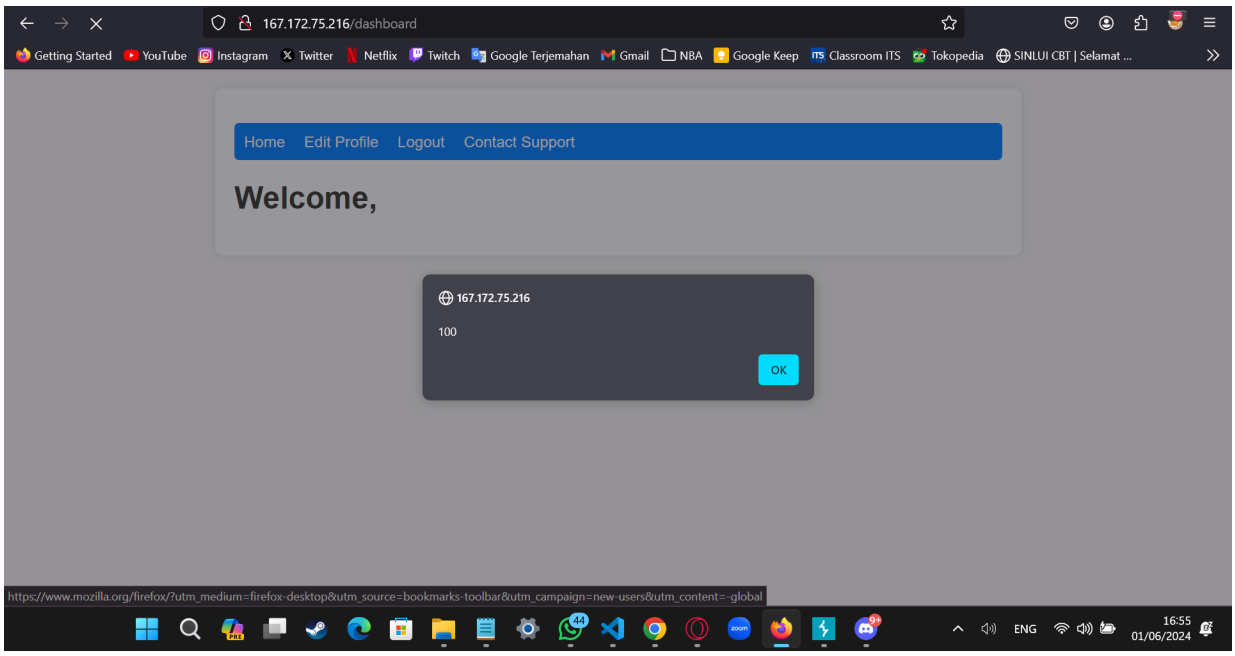
2. Setelah kita register dan login, script belum berjalan. Maka kita tambahkan dulu data dengan edit profile



3. Lalu Logout dan login kembali. Script telah berjalan dan bisa mendapat session cookie kita.

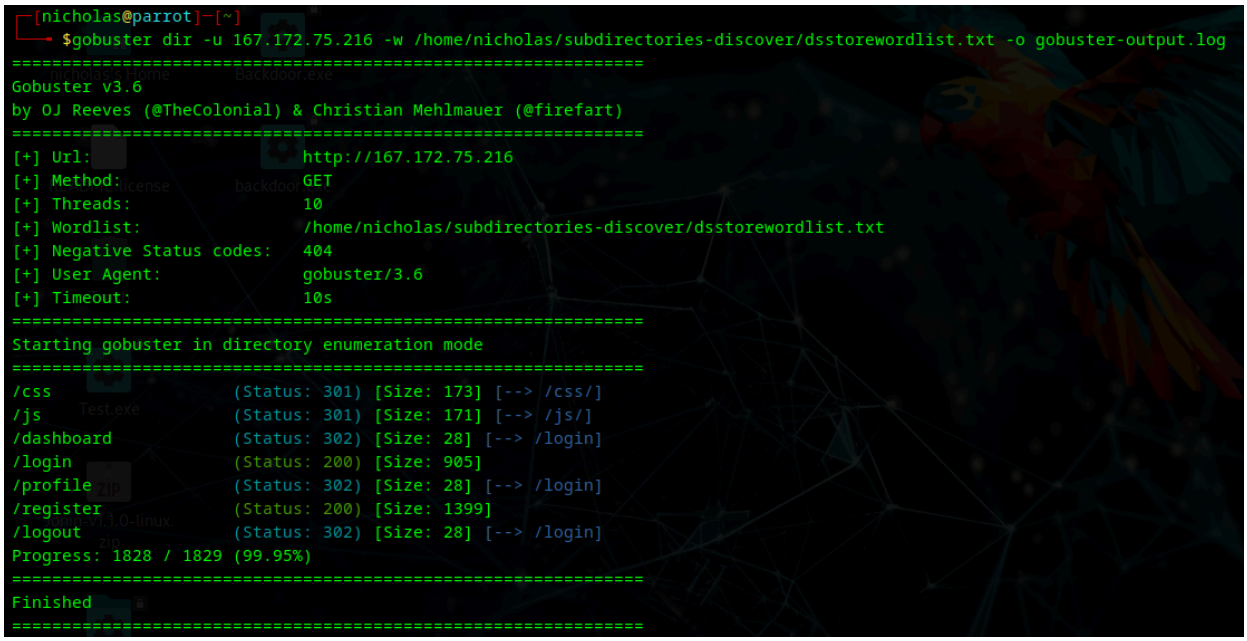


Contoh lain:



Gobuster

1. Menggunakan command
   gobuster dir -u 167.172.75.216 -w /home/nicholas/subdirectories-discover/dsstorewordlist.txt -o gobuster-output.log untuk mencari semua subdirectories yang ada di domain tersebut.



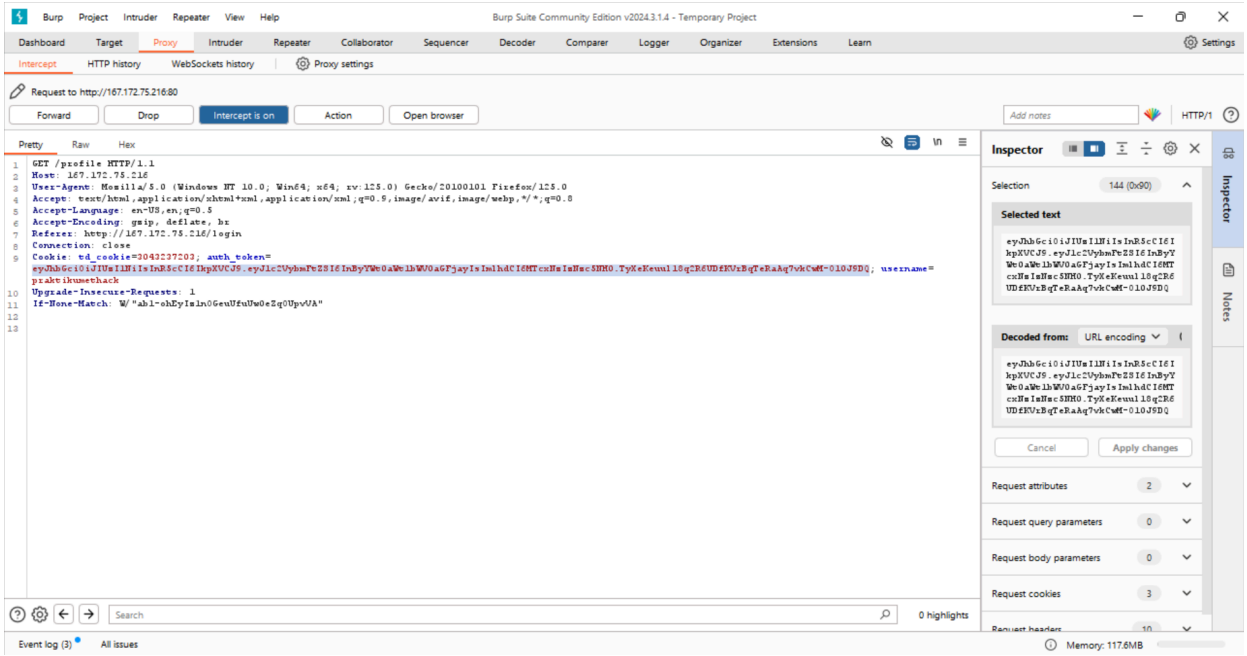
SQLMAP

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://167.172.75.216/login" --cookie="td_cookie=3043237203" --tables --schema --batch --delay=1 --threads=10

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#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 applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:50:42 /2024-06-01/

[06:50:42] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST para
meters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] Y
[06:50:42] [INFO] testing connection to the target URL
[06:50:43] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:50:44] [INFO] testing if the target URL content is stable
[06:50:45] [INFO] target URL content is stable
[06:50:45] [INFO] testing if URI parameter '#1*' is dynamic
[06:50:46] [WARNING] URI parameter '#1*' does not appear to be dynamic
[06:50:47] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[06:50:48] [INFO] testing for SQL injection on URI parameter '#1*'
[06:50:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:50:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[06:51:01] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:51:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[06:51:11] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[06:51:16] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[06:51:21] [INFO] testing 'Generic inline queries'
[06:51:22] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[06:51:27] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[06:51:31] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[06:51:37] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[06:51:42] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[06:51:47] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[06:51:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requ
ests? [Y/n] Y
[06:51:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[06:52:03] [WARNING] URI parameter '#1*' does not seem to be injectable
[06:52:03] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform mor
e tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spa
ce2comment') and/or switch '--random-agent'
[06:52:03] [WARNING] HTTP error codes detected during run:
```

Auth Token

---

1. Menggunakan burpsuite, kita bisa mendapatkan auth_token untuk suatu akun (contoh disini: praktikumethack)



2. Apabila auth_token tersebut kita pakai pada akun lain, maka kita bisa masuk ke akun praktikumethack tersebut tanpa tahu password