TUGAS SESSION 7
READING LOGS

IMMANUEL BILLY CHRISTIAN S
RICHARD TAN
JEREMY JULIAN
JOHANES

EXAMPLE LOGS

```
192.168.1.300 - - [30/Oct/2023:17:30:15 +0000] "POST
/login.php" 200 322 "-" "Mozilla/5.0"
192.168.1.301 - - [30/Oct/2023:17:35:30 +0000] "POST
/admin/login.php" 401 322 "-" "Mozilla/5.0"
192.168.1.302 - - [30/Oct/2023:17:40:45 +0000] "POST
/wp-login.php" 401 322 "-" "Mozilla/5.0"
192.168.1.303 - - [30/Oct/2023:17:46:00 +0000] "POST
/user/login" 401 322 "-" "Mozilla/5.0"
192.168.1.304 - - [30/Oct/2023:17:51:15 +0000] "POST
/adminpanel/index.html" 401 322 "-" "Mozilla/5.0"
```

BRUTEFORCE ATTACK

Contoh potongan log yang diberikan tadi merupakan contoh seseorang melakukan sub domain enumeration, dari log diketahui bahwa web memiliki login.php

EXAMPLE LOGS 2

```
192.168.1.200 - - [30/Oct/2023:18:15:20 +0000] "GET /vulnerable_page.php?
name=<script>alert('XSS')</script> HTTP/1.1" 200 620 "-" "Mozilla/5.0"
192.168.1.201 - - [30/Oct/2023:18:18:05 +0000] "GET /comments.php?
comment=<img src='x' onerror='alert("XSS")'> HTTP/1.1" 200 512 "-"
"Mozilla/5.0"
192.168.1.202 - - [30/Oct/2023:18:21:30 +0000] "POST /contact_form" 200
324 "http://malicious-site.com" "Mozilla/5.0"
192.168.1.203 - - [30/Oct/2023:18:25:10 +0000] "GET /profile.php?user=
<svg/onload=alert('XSS')> HTTP/1.1" 200 752 "-" "Mozilla/5.0"
192.168.1.204 - - [30/Oct/2023:18:28:35 +0000] "GET /search?q=
<iframe/src=javascript:alert('XSS')>" 200 420 "-" "Mozilla/5.0"
```

CROSS SITE SCRIPTING (XSS)

Dari potongan Log yang diberikan, kita bisa melihat bahwa seseorang berusaha mencoba untuk menampilkan huruf yang semestinya tidak bisa, tetapi dari lognya orang tersebut bisa menampilkannya dengan script yang ditaruh oleh orang tersebut, sehingga ketika victim berinteraksi dengan script tersebut, maka akan muncul pop up alert.

EXAMPLE LOGS

```
192.168.1.100 - - [30/Oct/2023:15:15:20 +0000] "GET /vulnerable_page.php?
id=1%20OR%201=1-- HTTP/1.1" 200 515 "-" "Mozilla/5.0"
192.168.1.101 - - [30/Oct/2023:15:18:05 +0000] "GET /login.php?username=admin' OR
'1'='1'--&password=pass HTTP/1.1" 401 322 "-" "Mozilla/5.0"
192.168.1.102 - - [30/Oct/2023:15:22:30 +0000] "GET /search.php?
q=%27%20UNION%20SELECT%20null%2Cpassword%20FROM%20users-- HTTP/1.1" 500 731 "-"
"Mozilla/5.0"
192.168.1.103 - - [30/Oct/2023:15:26:15 +0000] "GET /products.php?
id=5%20AND%20(SELECT%20COUNT(*)%20FROM%20users)-- HTTP/1.1" 403 421 "-"
"Mozilla/5.0"
192.168.1.104 - - [30/Oct/2023:15:30:10 +0000] "GET /profile.php?user=admin'--
HTTP/1.1" 200 652 "-" "Mozilla/5.0"
```

SQL INJECTION (SQLI)

Dari contoh potongan log yang ada, kita bisa melihat bahwa ada seseorang sedang mencoba melakukan SQL injection dari pagenya untuk mendapatkan user admin, mencoba beberapa query dan pada akhirnya orang tersebut mendapatkan akun admin.

THANK YOU

I HOPE YOU LEARNED SOMETHING NEW!