ADVANCED WEB APPLICATION PENETRATION TESTING WITH BURP SUITE & OWASP DVWA

Identifying and Exploiting Web Vulnerabilities to Demonstrate Real-World Attack Surfaces

BY JACINTA IZUNDU

INTRODUCTION

- This hands-on lab teaches practical web hacking skills.
- You used tools like Nikto and Burp Suite.
- You tested a vulnerable website (OWASP BWA / DVWA).
- You practiced scanning, intercepting traffic, mapping a site, and brute forcing a login.

LAB OBJECTIVES

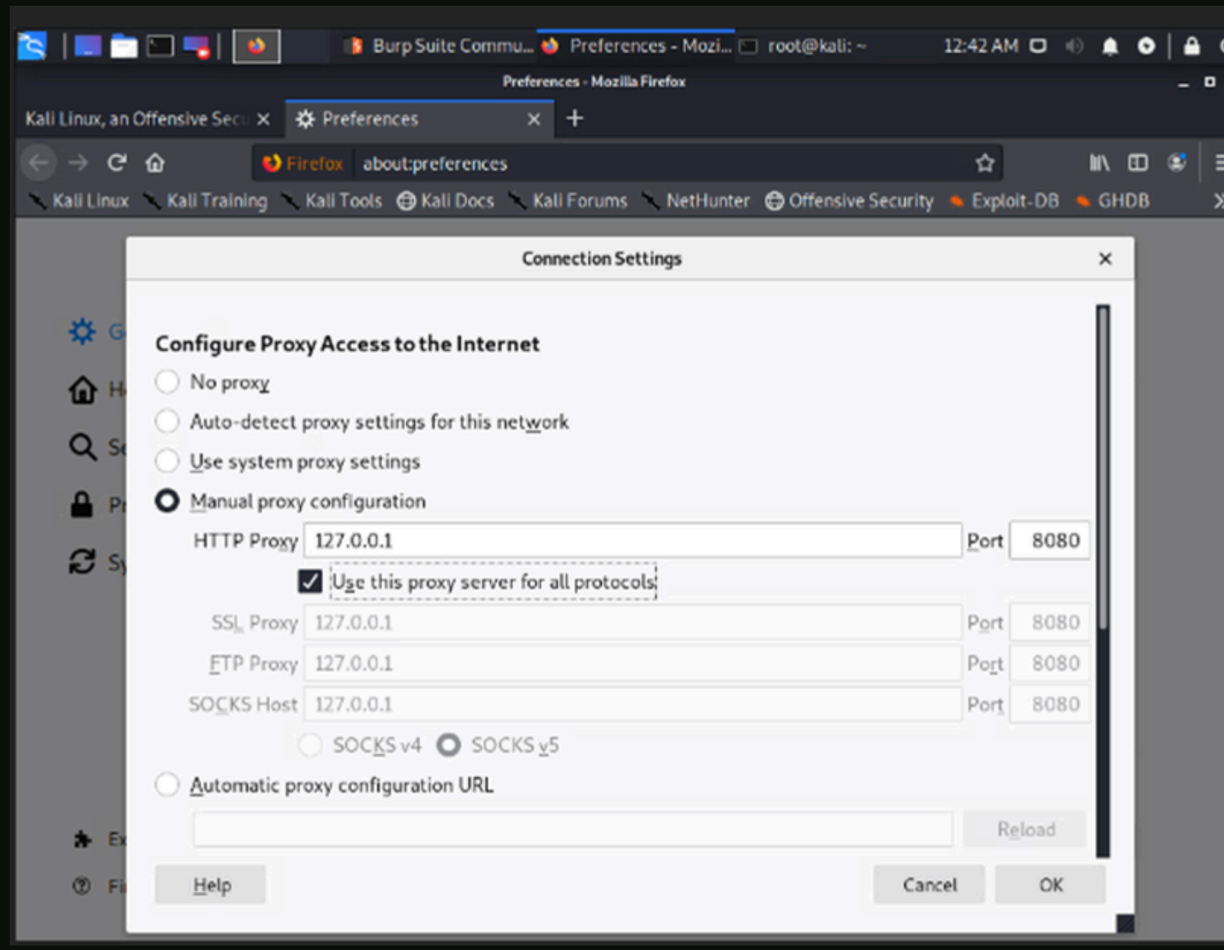
1. Scanning with Nikto
2. Setting up Burp Suite
3. Building a Site Map in Burp Suite
4. Performing Brute Force Attack on DVWA

TOOLS USED

- **Nikto:** Web server vulnerability scanner
- **Burp Suite**: Web penetration testing framework
- **Firefox:** Browser used for intercepting HTTP requests
- **OWASP BWA / DVWA:** Deliberately vulnerable target website

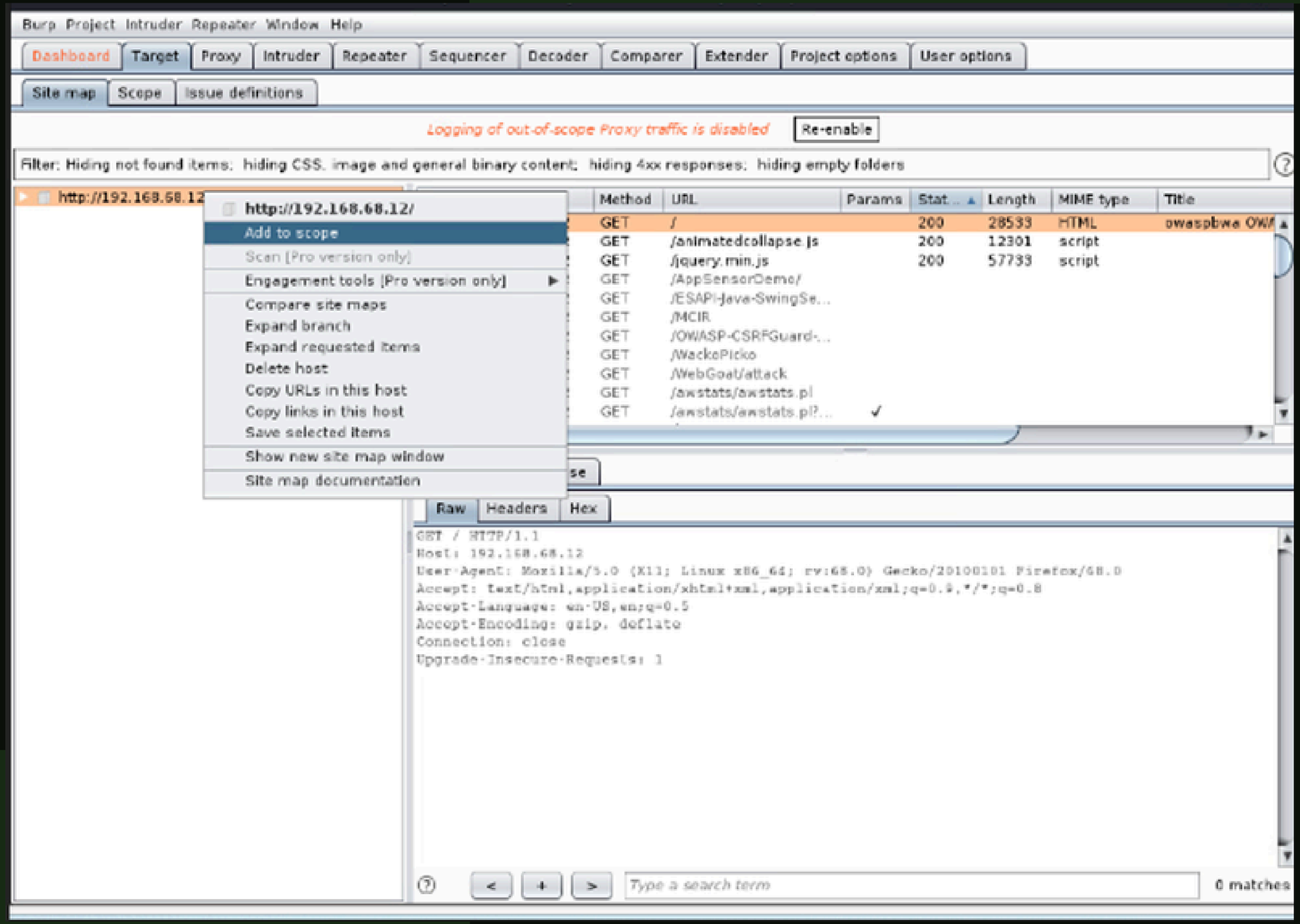
NIKTO SCAN (OVERVIEW)

- I logged into Kali (root/toor)
- I ran Nikto to scan a web server
- Nikto checks for vulnerabilities, outdated softwarw, HTTP options, plugins.

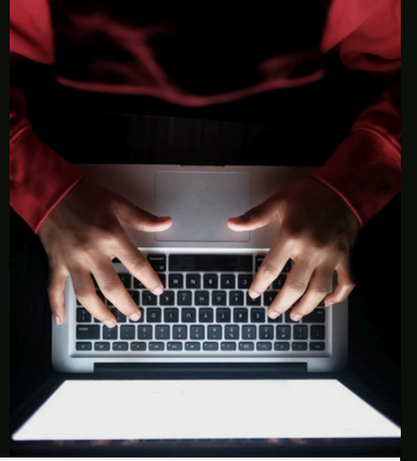


NIKTO: PLUGIN SCAN RESULTS

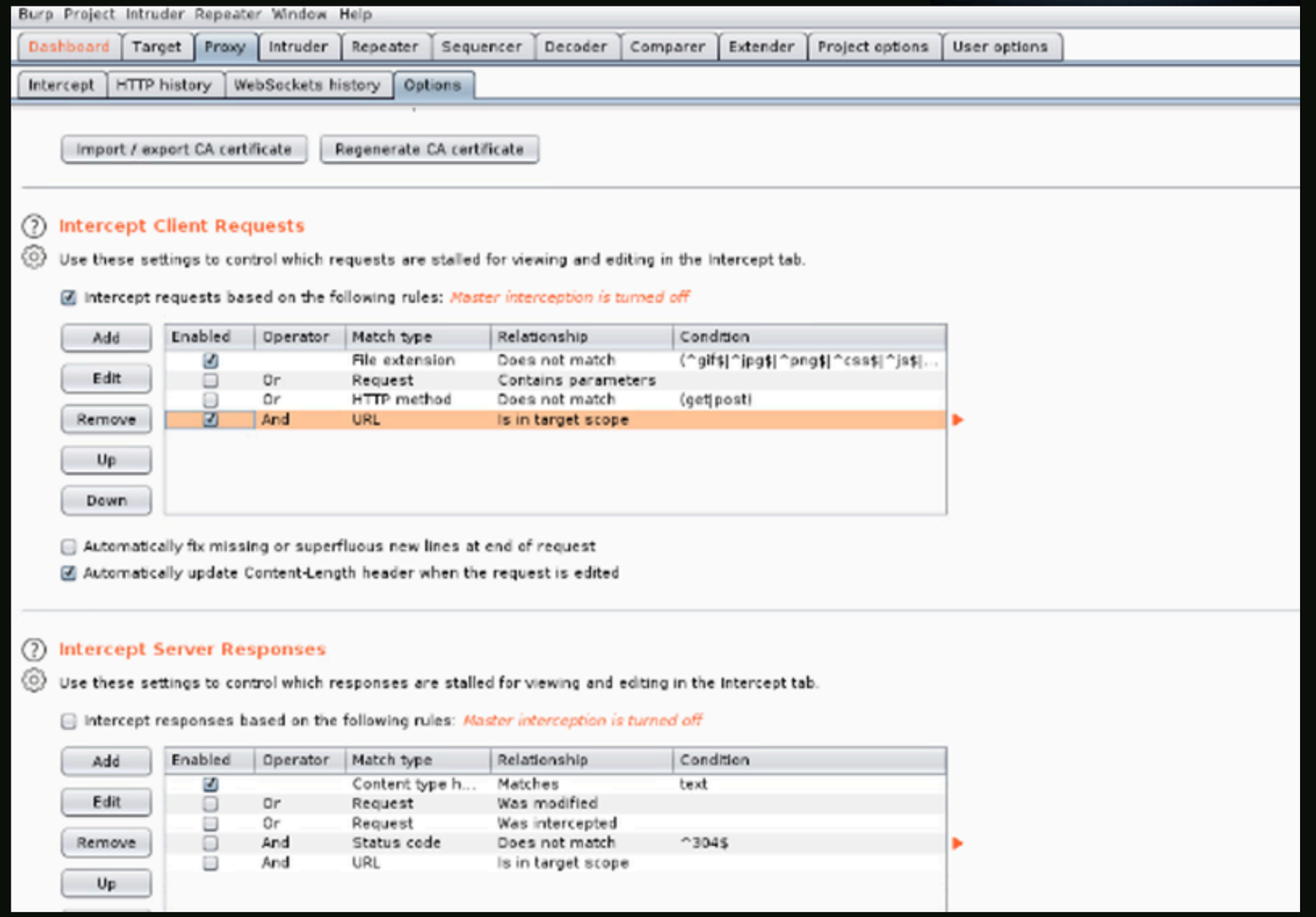
- **I USED NIKTO PLUGINS TO SCAN FOR:**
  - Outdated software
  - HTTP options
  - Sever messages
  - Vulnerable configurations



NIKTO: STANDARD TESTS & OSVDB FINDINGS

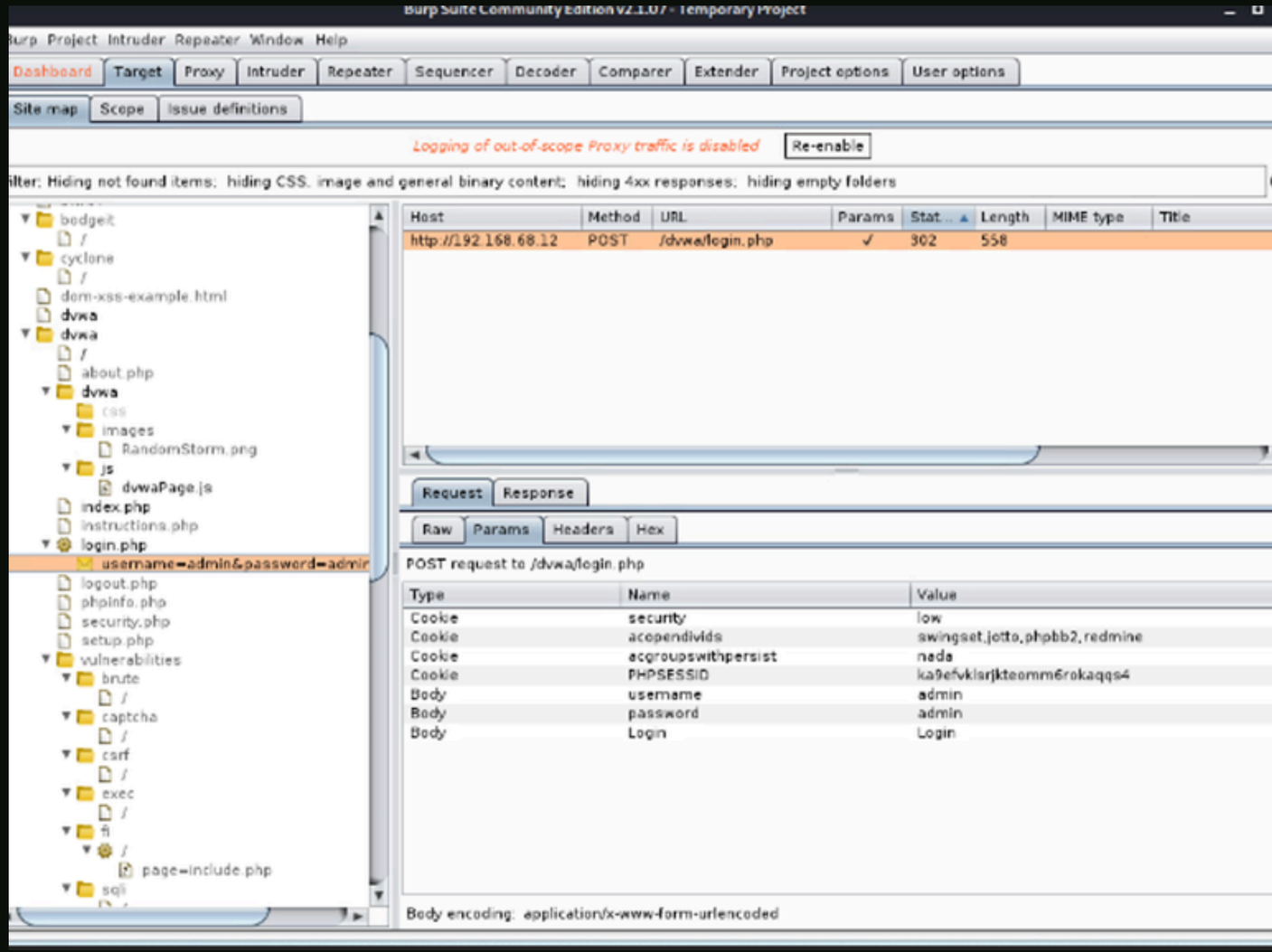


- Nikto: Web server vulnerability scanner
- Burp Suite: Web penetration testing framework
- Firefox: Browser used for intercepting HTTP requests
- OWASP BWA / DVWA: Deliberately vulnerable target website



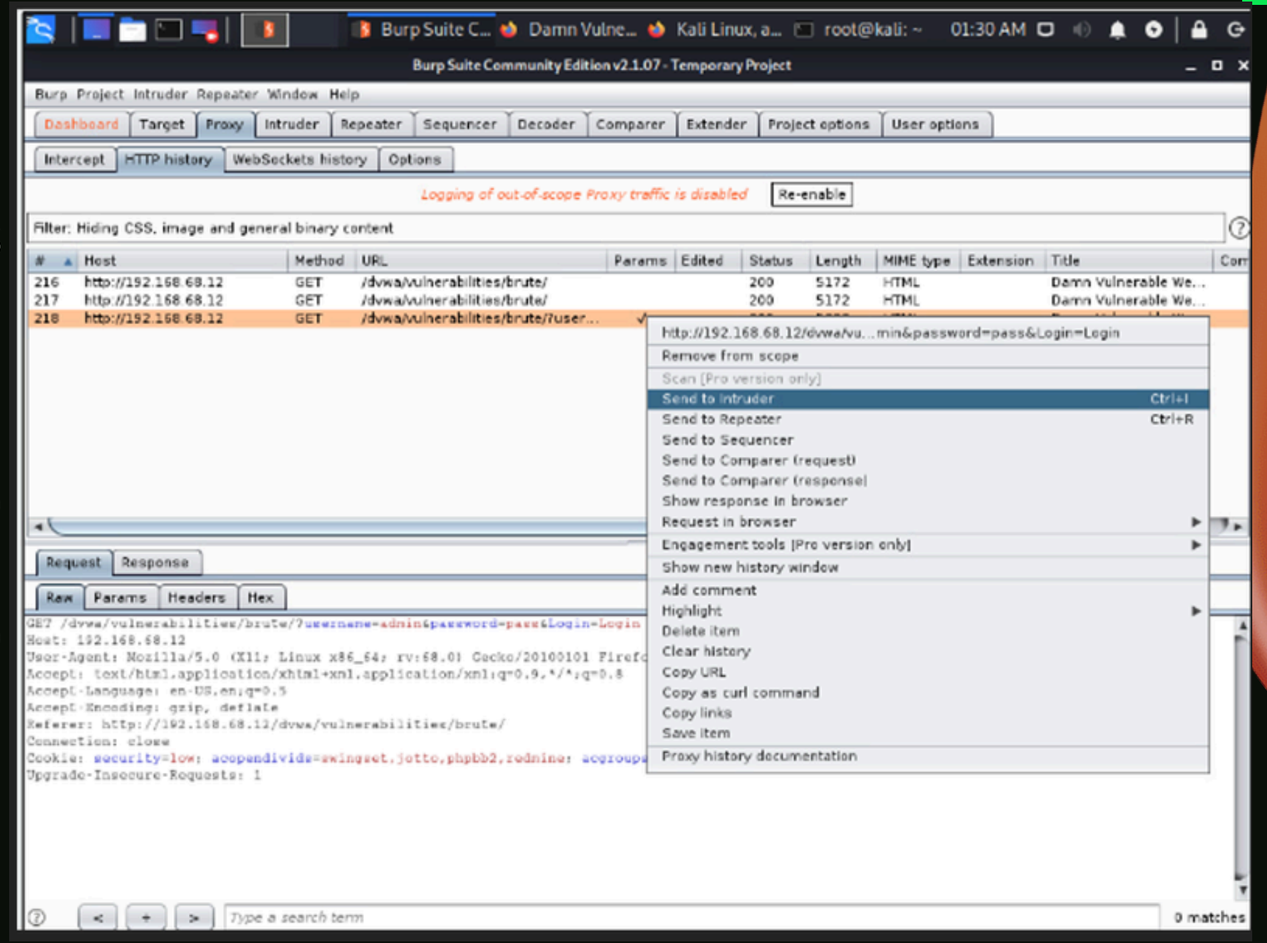
NIKTO: HTML REPORT

- I generated a complete HTML vulnerability report
- Opened it in Firefox
- Reviewed findings



SETTING UP BURP SUITE

- I launched Burp Suite
- Set up a temporary project
- Enabled it as Firefox's proxy
- Configured Firefox to route traffic through Burp (127.0.0.1:8080)

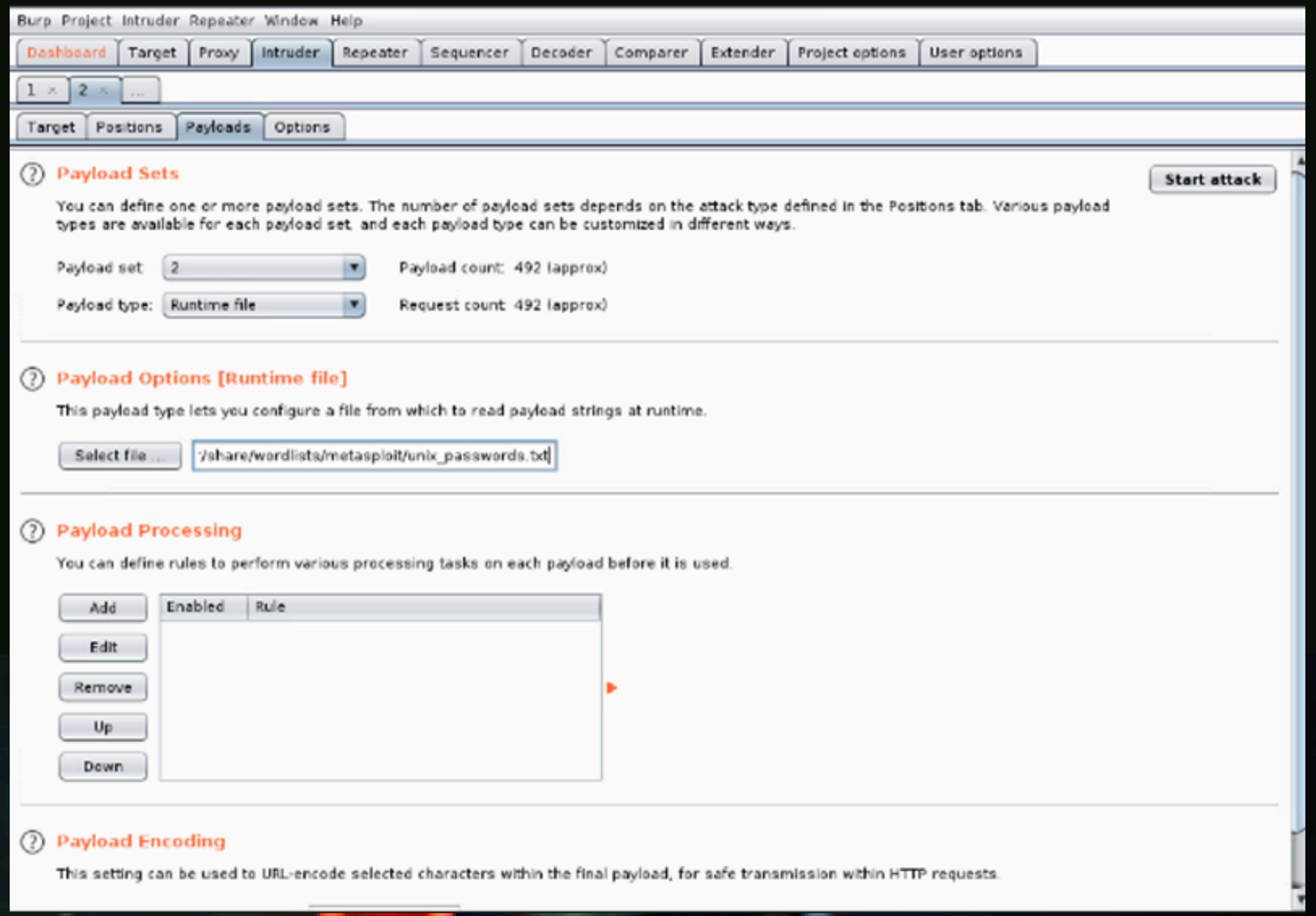


BURP SUITE INTERCEPT MODE

- I turned intercept OFF to allow traffic to flow
- I navigated to the vulnerable web app (192.168.68.12

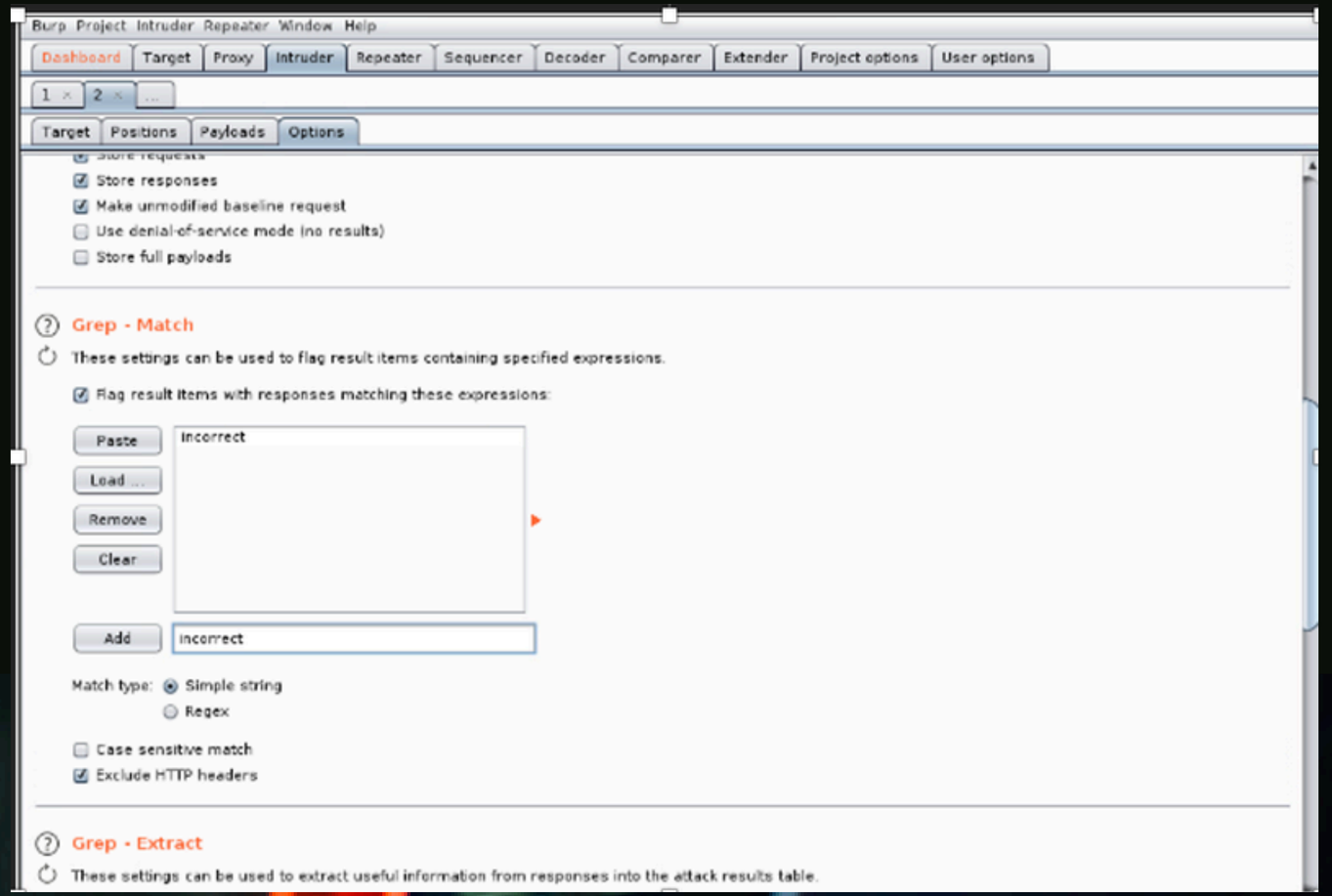
BUILDING A SITE MAP

- Burp Suite begins mapping the site
- As I clicked DVWA, directories turned from grey → black
- Burp logs usernames, passwords, and HTTP parameters



CAPTURED CREDENTIALS

- Burp Suite captured DVWA login parameters
- You viewed them under the “Params” tab
- Shows username=admin & password=admin

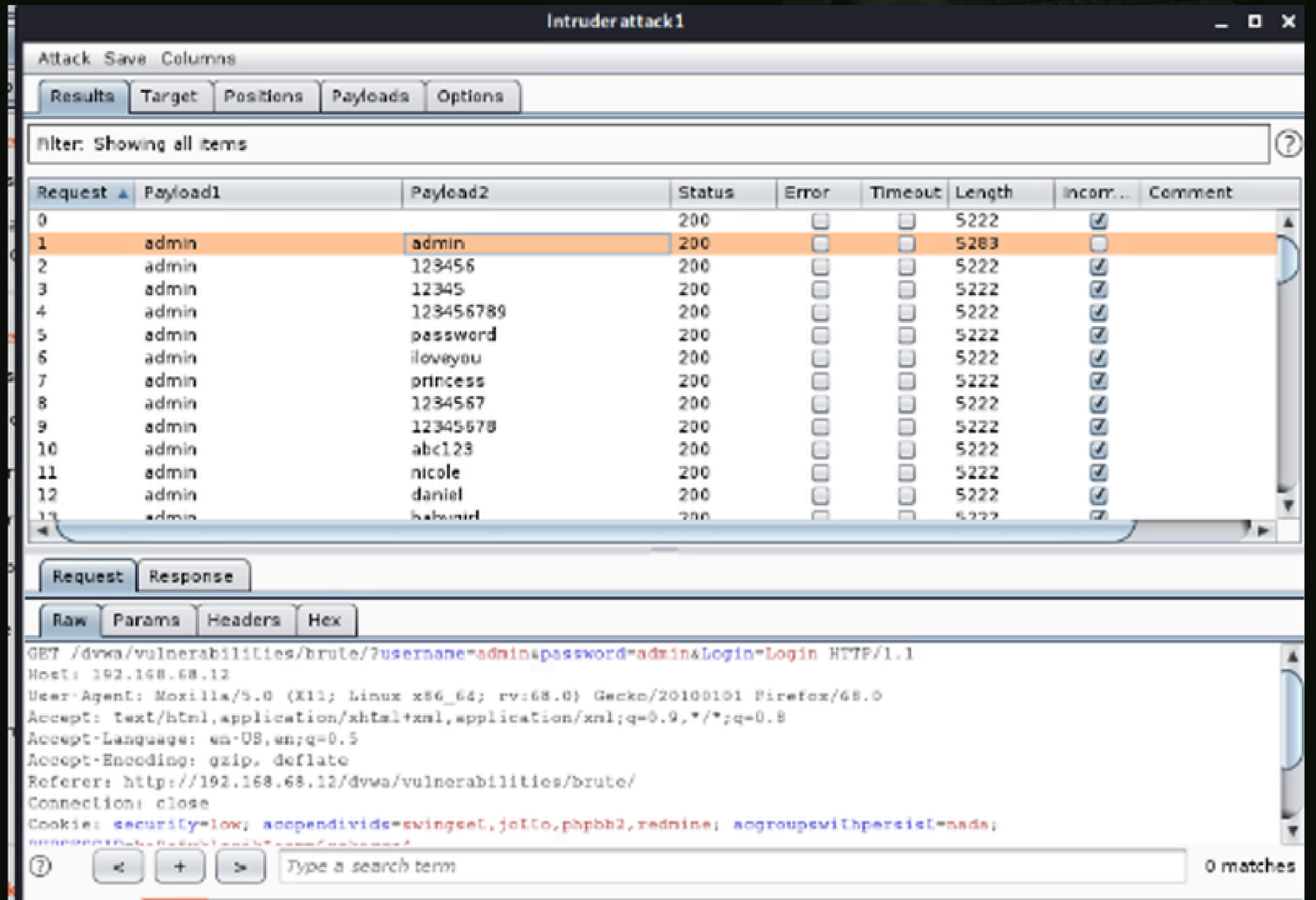


BRUTE FORCE ATTACK (OVERVIEW)

- Used Burp Intruder to brute-force the DVWA login pagSteps:
- Clear history
- Submit login attempt
- Send request to Intruder
- Set payloads (username + password list)
- Run attack
-

SENDING REQUEST TO INTRUDER

- I grabbed the login request
- Sent it to the intruder module
- Intruder turned orange

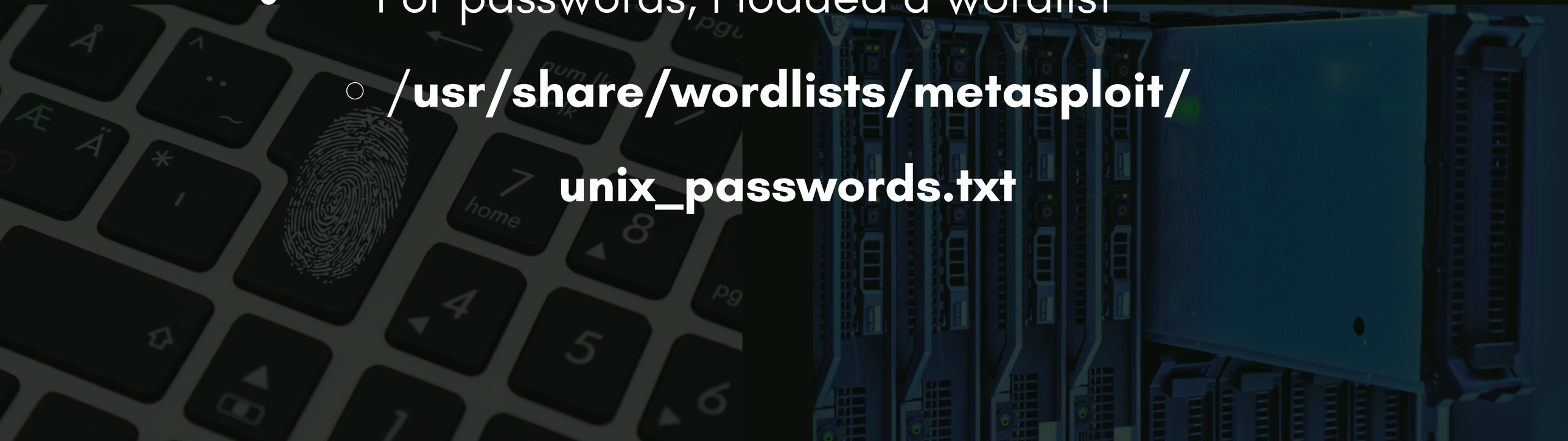


CONFIGURING PAYLOAD POSITIONS

- I cleared all variables
- Selected admin and pass parameters
- Added $ markers for both

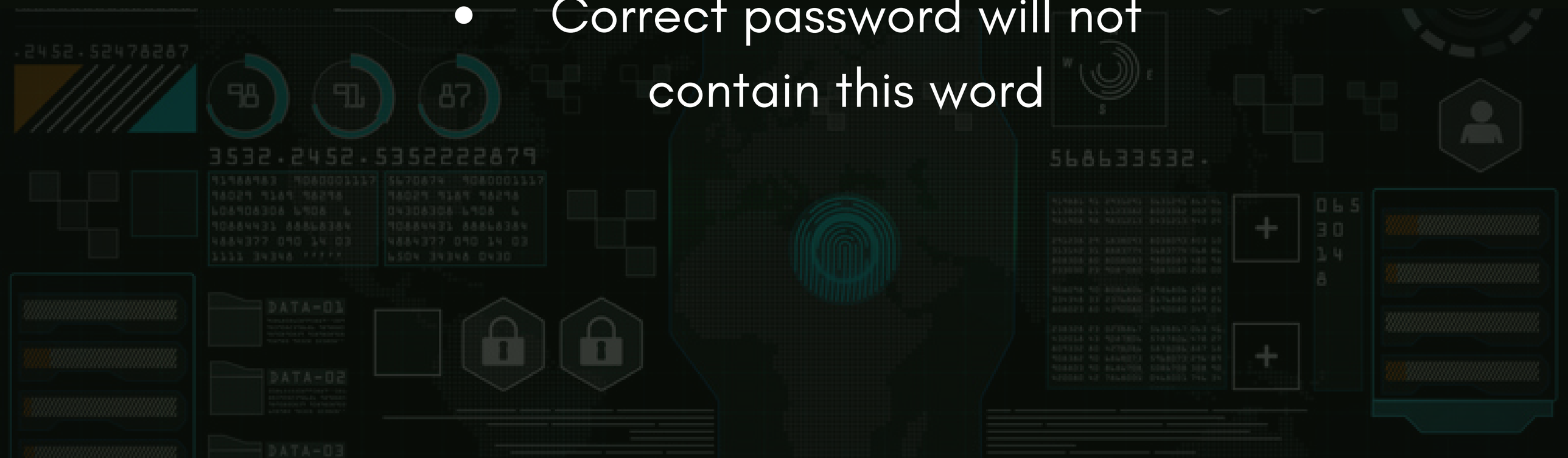
LOADING PASSWORD WORDLIST

- For usernames, I used **admin**
- For passwords, I loaded a wordlist
  - **/usr/share/wordlists/metasploit/unix_passwords.txt**



SETTING GREP-MATCH RULE

- To identify failed attempts, I added rule: **Incorrect**
- Correct password will not contain this word



RUNNING THE ATTACK

- I started the brute force attack
- Burp Suite Community Edition slows results
- I looked for the password without an “incorrect” flag

SUCCESSFUL PASSWORD FOUND

- I identified the correct DVWA password
- It appears under Payload2 without the “incorrect” mark

KEY FINDINGS

- Nikto revealed outdated software & weak HTTP options
- Burp Suite intercepted all web traffic
- Site map exposed sensitive parameters
- Intruder successfully brute-forced DVWA login
- Demonstrates why strong passwords & secure configs matter

CONCLUSION

- The exercise taught real-world ethical hacking skills
- Showed how vulnerable misconfigured systems can be
- Reinforced importance of monitoring, patching and hardening web apps

THANK YOU!

Thank you for being part of the secure digital journey.
Together, we create a safer internet for everyone.

+1 217 670 4436

clemsjacy@gmail.com

LinkedIn http://linkedin.com/in/jacinta-izundu-b36a20233