Cyber Security

2024

DVWA

Vathna.lay@cadt.edu.kh

Attack

- SQL injection
- Cross Site Scripting (XSS)
- Brute Force with Burp Suite

SQL Injection (Low)

- SQL injection:
  - Test statement: 1' OR '1'='1 (test if the injection work)
  - Find how many column we can return:
  - Find database name:
  - Find database and the system user:
  - Find table name:
  - Find column name:
  - Find value:

SQL Injection (Medium)

- SQL Injection
  - The same but different place
  - use inspect element
  - use Burp Suite

SQL Injection suggestion

- **Solution**
  - **Prepared Statements: Same as Low Level, prepared statements are essential.**
  - **Stronger Input Validation: Implement more robust input validation, considering potential SQL keywords and special characters.**

XSS (DOM), LOW

- Technique:
  - Using javascript
  - testing with alert
  - print all cookie information

- Hint: view source

XSS (DOM), medium & high

- **Technique:**
  - **Using javascript**
  - **Using javascript trick**
  - **testing with alert**
  - **print all cookie information**

- **Hint: view source**

XSS (Reflected), low

- Technique:
  - inspect the source code
  - Using javascript
  - Using javvascript trick
  - testing with alert
  - print all cookie information

- Hint: view source

XSS (Reflected), medium

- Technique:
  - Using javascript
  - Using javascript trick
  - testing with alert
  - print all cookie information

- Hint: view source

XSS (Reflected), high

- Technique:
  - Using html tag
  - use body tag
  - testing with alert
  - print all cookie information

- Hint: view source

XSS (Store), Low

- **Technique:**
  - **try the same like the other XSS**
  - **testing with alert**
  - **print all cookie information**

XSS (Reflected), medium

- **Technique:**
  - **try the same like the other XSS**
  - **testing with alert**
  - **print all cookie information**

XSS (Reflected), High

- Technique:
  - inspect the source code
  - try the same like the other XSS
  - testing with alert
  - print all cookie information

Brute Force with Burp Suite

- Technique:
  - open Burp Suite
  - open browswer using Burp Suite
  - open DVWA url and then Brute Force tab
  - add DVWA website to scope
  - Go to proxy->HTTP History in Burp Suite and then filter to see only item in scope
  - Turn intercept on and try login with the incorrect password
  - Go to proxy->HTTP History and click on the last get request
  - Send the request to intruder
  - Open introder -> positions and clear all variable
  - Choose sniper attack and then add password to variable

Brute Force with Burp Suite

- Technique:
  - Go to payloads
  - use sample file
  - load 1 password list from kali linux
  - start the attack
    - observe the attack
  - try to grab the string
    - incorrect password
    - correct password