Fakultät für Informatik
Prof. Dr. Reiner Hüttl

IT-Security

Exercise 10

Task 1: OWASP Mutillidae 2 Web Pen Test

In this exercise, we will continue to work with the OWASP Mutillidae 2 Web Pen Test Training Environment.

Each participant of the exercise chooses a securitygap from Mutillidae as homework before the exercise and demonstrates it to the others in the exercise.

In doing so, we are looking for the vulnerabilities from the OWASP Top 10 of **2017**:
(the Top 10 of 2021 are not yet implemented)

- A1 Injection
- A2 Broken Authentication
- A3 Sensitive data exposure
- A4 XML External Entities
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 XSS Cross Site Scripting
- A8 Insecure Desirialization
- A10 Insufficient Logging and monitoring:

Task 2: Burp Suite Community Edition

Burp Suite is a security testing tool for web applications https://portswigger.net/burp
We can only use the free Community Edition https://portswigger.net/burp/communitydownload

After installing we will test some features of the tool.
You can use the tool for modifying requests and responses to our vulnerable application Mutillidae.

Test Burp Proxy: Burp Proxy operates as a web proxy server between the browser and target applications. It enables you to intercept, inspect, and modify traffic that passes in both directions. (https://portswigger.net/burp/documentation/desktop/tools/proxy)

- Switch Intercept to on in Proxy settings
- Open Burp's Browser
- Start request in Burp Browser, e.g. 127.0.0.1
- Watch request in Burp Proxy
- Forward request
- View response
- Alternate a request and watch the response

Test Burp Intruder: Burp Intruder is a tool for automating customized attacks against web applications.
https://portswigger.net/burp/documentation/desktop/tools/intruder

- See Video https://portswigger.net/burp/documentation/desktop/tools/intruder/getting-started
- Intercept request
- Send request to Intruder
- Define positions to intrude in request
- Set payload to intrude
  e.g. Candidate User Names: https://portswigger.net/web-security/authentication/auth-lab-usernames
- Start attack
- View results (reqausts and responses)
  fillter results is not available in Community Edition -> you must manually inspect results

Test Burp Repeater and Comparer:
Burp Repeater is a tool that enables you to modify and send an interesting HTTP or WebSocket message over and over.
Burp Comparer enables you to compare any two items of data. You can use Comparer to quickly and easily identify subtle differences between requests or responses.

Test Burp Sequencer: Burp Sequencer enables you to analyze the quality of randomness in a sample of tokens (e.g. Session Tokens, Anti-CSRF tokens).

- Goto "Add to your blog" page in Mutillidae
- Set Security level to 1
- Intercept request and send to Sequencer
- Search for CSRF token in response of Sequencer
- Mark CSRF Token in response
- Start live Capture and analyze live capture

See https://www.youtube.com/watch?v=YGRoFU0USRA&list=PLZOToVAK85MorLmAqD3117C0s9h7ccxaV&index=18