

BEZPIECZEŃSTWO APLIKACJI INTERNETOWYCH

LABORATORIUM 5

KONTROLA PROCESU LOGOWANIA III

DR INŻ. SABINA SZYMONIAK

KATEDRA INFORMATYKI

WYDZIAŁ INŻYNIERII MECHANICZNEJ I INFORMATYKI

POLITECHNIKA CZĘSTOCHOWSKA

ROK AKADEMICKI 2023/2024



NARZĘDZIE burp suite

NARZĘDZIE BURP SUITE

The screenshot displays the Burp Suite Community Edition v1.7.34 interface. The top menu bar includes Burp, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The main window is divided into three panes. The left pane shows a 'Site map' with a list of URLs, including http://be.linkedin.com, http://creativecommons.org, http://detectportal.firefox.com, https://fonts.googleapis.com, https://github.com, http://html5shiv.googlecode.com, http://itsecgames.blogspot.com, http://localhost (selected), http://meyerweb.com, http://twitter.com, http://www.facebook.com, http://www.missingkids.com, http://www.mmevbva.com, https://www.netparker.com, and https://www.owasp.org. The middle pane displays a table of HTTP requests with columns: Host, Method, URL, Params, Sta..., Length, MIME type, Title, and Comment. The selected request is a GET request to http://localhost/bWAPP/login.php. The right pane shows the details of the selected request, including the raw HTTP request and response. The raw request is: GET /bWAPP/login.php HTTP/1.1, Host: localhost, User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Accept-Language: en-GB,en;q=0.5, Accept-Encoding: gzip, deflate, Connection: close, Upgrade-Insecure-Requests: 1. The raw response is: 200 13665 HTML bWAPP - CSRF. The bottom status bar shows 0 matches.

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment
http://localhost	GET	/bWAPP/csrf_2.php		200	13665	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/csrf_2.php?...	✓	200	13668	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/csrf_2.php?...	✓	200	13665	HTML	bWAPP - CSRF	
http://localhost	GET	/bWAPP/shtml5.js		200	2684	script		
http://localhost	GET	/bWAPP/login.php		200	4321	HTML	bWAPP - Login	
http://localhost	GET	/bWAPP/portal.php		200	23676	HTML	bWAPP - Portal	
http://localhost	GET	/bWAPP/reset.php		200	13598	HTML	bWAPP - Reset	
http://localhost	GET	/bWAPP/sqli_7.php		200	13553	HTML	bWAPP - SQL Injection	
http://localhost	POST	/bWAPP/sqli_7.php	✓	200	13847	HTML	bWAPP - SQL Injection	
http://localhost	POST	/bWAPP/sqli_7.php	✓	200	13814	HTML	bWAPP - SQL Injection	

Request Response

Raw Params Headers Hex

GET /bWAPP/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0; PHPSESSID=i6q80lthjc13l1dnl3743n3q7
Connection: close
Upgrade-Insecure-Requests: 1

Type a search term 0 matches

Źródło: <https://portswigger.net/>

ZADANIA DO WYKONANIA

Testowanie podatności na ataki typu Cross-Site Scripting (XSS). XSS to rodzaj ataku, w którym niezaufane dane są wstrzykiwane do strony internetowej i wykonują kod JavaScript w przeglądarce ofiary.

- Skonfiguruj Burp Suite jako pośrednika (proxy) między przeglądarką a aplikacją internetową. Upewnij się, że ruch przepływający między nimi jest przechwytywany.
- Przejdź do strony logowania na aplikacji internetowej i przeprowadź normalną próbę logowania. Upewnij się, że ruch jest przechwytywany przez Burp Suite.
- W Burp Suite, wybierz żądanie logowania w zakładce "Proxy" i użyj funkcji "Intercept" w celu przechwycenia żądania. Następnie zmodyfikuj jedno z pól, takich jak pole nazwy użytkownika, i wstrzyknij kod XSS. Przykład:

W oryginalnym żądaniu

```
POST /login HTTP/1.1
```

```
Host: example.com
```

```
Content-Length: 27
```

```
Content-Type: application/x-www-form-urlencoded
```

```
username=john&password=secret
```

Zmodyfikowane żądanie z wstrzykniętym XSS

```
POST /login HTTP/1.1
Host: example.com
Content-Length: 63
Content-Type: application/x-www-form-urlencoded

username=<script>alert('XSS')</script>&password=secret
```

- Po wstrzyknięciu żądania, przejdź do zakładki "Proxy" i upewnij się, że odpowiedź jest przechwytywana. Sprawdź, czy kod XSS jest reflektowany w odpowiedzi.
- Jeśli kod XSS jest wykonywany w odpowiedzi, to oznacza, że strona jest podatna na atak XSS. Dokładnie zanalizuj, jak kod XSS jest renderowany przez przeglądarkę ofiary.

Uwaga

Jeśli kod XSS zostanie wykonany, oznacza to, że strona jest podatna na atak XSS i wymaga podjęcia działań naprawczych.

W sprawozdaniu należy zamieścić kilka screenów potwierdzających wykonanie zadań.

Wykorzystano materiały pochodzące z:

- <https://portswigger.net/>

DZIĘKUJĘ ZA UWAGĘ!
PYTANIA?
SPOSTRZEŻENIA I SUGESTIE:

SABINA.SZYMONIAK@ICIS.PCZ.PL