Bezpieczeństwo aplikacji internetowych
Laboratorium 5

Kontrola procesu logowania III

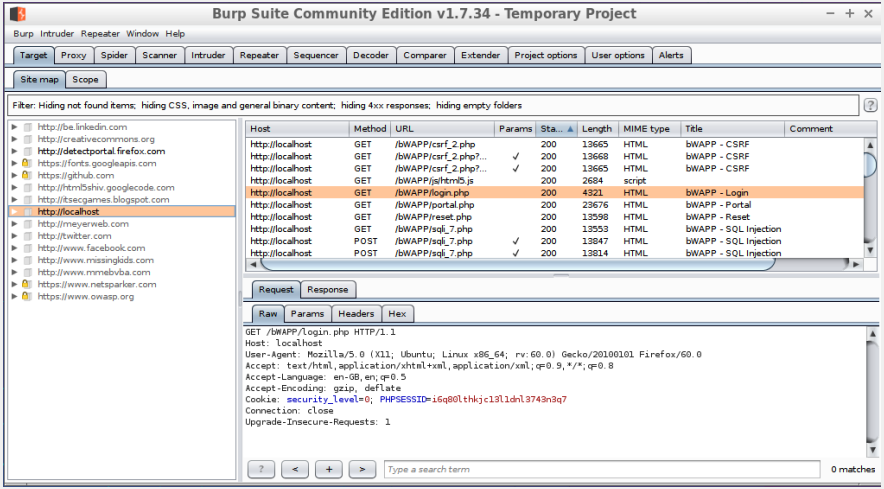
dr inż. Sabina Szymoniak

Katedra Informatyki
Wydział Inżynierii Mechanicznej i Informatyki
Politechnika Częstochowska

Rok akademicki 2023/2024

Narzędzie burp suite

Narzędzie BURP SUITE



Źródło: https://portswigger.net/

Zadania do wykonania

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.

Literatura

Wykorzystano materiały pochodzące z:

- https://portswigger.net/

Dziękuję za uwagę!
Pytania?
Spostrzeżenia i sugestie:

SABINA.SZYMONIAK@ICIS.PCZ.PL