

POLITECHNIKA CZĘSTOCHOWSKA Katedra Informatyki		Laboratorium z przedmiotu Bezpieczeństwo aplikacji internetowych	
Nazwisko i mię Maciej Kurek		LABORATORIUM nr 5	Rok akademicki 2023/2024
			Data zajęć 07.11.2023r.
Temat ćwiczenia Kontrola procesu logowania III		GRUPA: 2	

1. Wprowadzenie teoretyczne i cel laboratorium

Celem zajęć jest dalsze poznawanie funkcjonalności narzędzia Burp Suite polegające na testowaniu podatności stron internetowych na ataki XSS.

2. Przebieg zajęć

Na początku zajęć skonfigurowałem Burp Suite jako pośrednika (proxy) między przeglądarką a aplikacją internetową. Upewniłem się, że ruch przepływający między nimi jest przechwytywany. Następnie przechwyciłem żądanie i wstrzyknąłem kod XSS.

3. Podsumowanie

XSS to rodzaj ataku, w którym niechciane dane są wstrzykiwane do strony internetowej i wykonują kod JavaScript w przeglądarce ofiary. Jeśli kod XSS zostanie wykonany, oznacza to, że strona jest podatna na atak XSS i wymaga podjęcia działań naprawczych. Wykonanie zadania dokumentują poniższe zrzuty ekranu.

The screenshot displays the Burp Suite interface with a request and response captured. The request is a GET request to the URL `https://swiatkryptowalut.com/chat/`. The response is a 200 OK status with HTML content. The response body includes a 'LIVE CHAT 2.0 (Anonymous)' section with various meta tags and a 'LIVE CHAT 2.0 (Anonymous)' section.

```

Request
1 GET /chat/ HTTP/2
2 Host: swiatkryptowalut.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-CH-UA:
11 Sec-CH-UA-Mobile: ?0
12 Sec-CH-UA-Platform: ""
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
16

Response
1 HTTP/2 200 OK
2 Server: hcdn
3 Date: Tue, 24 Oct 2023 07:31:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Vary: Accept-Encoding
6 X-Powered-By: PHP/7.4.33
7 Set-Cookie: PHPSESSID=c3930bc53aa5a1d9c32bccc4d3de7f; path=/; secure
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 Platform: hostinger
12 Content-Security-Policy: upgrade-insecure-requests
13 X-Turbo-Charged-By: LiteSpeed
14 X-Hcdn-Request-Id: c49388ca9c42a4bd8788211f8184fa-srv-edge2
15 X-Hcdn-Cache-Status: MISS
16 X-Hcdn-Upstream-Error: 0
17
18
19 <!DOCTYPE HTML>
20 <html lang="pl">
21 <head>
22 <meta charset="utf-8" />
23 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
24 <title>
25 LIVE CHAT 2.0 (Anonymous)
26 </title>
27 <meta name="viewport" content="width=device-width,initial-scale=0.85,maximum-scale=0.85,minimum-scale=0.85">
28 <link rel="shortcut icon" href="img/adm.png">
29 <link href="https://fonts.googleapis.com/css?family=Lilita+One&display=swap" rel="stylesheet">
30 <link rel="stylesheet" href="css/full.css"/>

```

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
https://ajax.googleapis.com	GET	/chat/		200	84830	HTML	LIVE CHAT 2.0 (Anonymous)		03:31:35.24 O...
https://swiatkrypowalut.com	POST	/chat/messages.php		200	846	HTML			03:34:11.24 O...
https://www.wykop.pl	POST	/chat/send.php		200	457	HTML			03:34:42.24 O...
https://swiatkrypowalut.com	POST	/chat/send.php		200	679	text			03:34:11.24 O...
https://swiatkrypowalut.com	POST	/chat/users.php		200	194312	HTML			03:31:53.24 O...
https://swiatkrypowalut.com	GET	/chat		301	1103	HTML	301 Moved Permanently		03:31:33.24 O...
https://swiatkrypowalut.com	GET	/addon							
https://swiatkrypowalut.com	GET	/chat/css/							
https://swiatkrypowalut.com	GET	/chat/messages.php							
https://swiatkrypowalut.com	GET	/chat/send.php							
https://swiatkrypowalut.com	GET	/chat/users.php							

Request

```

1 POST /chat/send.php HTTP/1.2
2 Host: swiatkrypowalut.com
3 Cookie: PHPSESSID=e3938bc53aa5a1d9c32bcec4d73de7f
4 Content-Length: 37
5 Sec-CH-UA:
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Sec-CH-UA-Mobile: 0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5798.171 Safari/537.36
11 Sec-CH-UA-Platform: ""
12 Origin: https://swiatkrypowalut.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://swiatkrypowalut.com/chat/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
20 user=message&kanil=zdum&type=message

```

Response

```

1 HTTP/2.2 200 OK
2 Server: hcdn
3 Date: Tue, 24 Oct 2023 07:34:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 197
6 Vary: Accept-Encoding
7 X-Powered-By: PHP/7.4.33
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 Platform: hostingier
12 Content-Security-Policy: upgrade-insecure-requests
13 X-Turbo-Charged-By: LiteSpeed
14 X-Hcdn-Request-Id: 3a638245499c3ba23c6ae1c327b681-1rv-edge1
15 X-Hcdn-Upstream-Rt: 0.110
16
17 <div />
18 <div />
19
20 <div />

```

Inspector

- Request attributes: 2
- Request body parameters: 3
- Request cookies: 1
- Request headers: 20
- Response headers: 14

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
https://ajax.googleapis.com	GET	/chat/		200	84830	HTML	LIVE CHAT 2.0 (Anonymous)		03:31:35.24 O...
https://swiatkrypowalut.com	POST	/chat/messages.php		200	457	HTML			03:35:50.24 O...
https://www.wykop.pl	POST	/chat/users.php		200	194312	HTML			03:31:53.24 O...
https://swiatkrypowalut.com	GET	/chat		301	1103	HTML	301 Moved Permanently		03:31:33.24 O...
https://swiatkrypowalut.com	GET	/addon							
https://swiatkrypowalut.com	GET	/chat/css/							
https://swiatkrypowalut.com	GET	/chat/messages.php							
https://swiatkrypowalut.com	GET	/chat/users.php							
https://swiatkrypowalut.com	GET	/clear							
https://swiatkrypowalut.com	GET	/commands							
https://swiatkrypowalut.com	GET	/file.php							

Request

```

1 GET /chat/ HTTP/1.2
2 Host: swiatkrypowalut.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5798.171 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-CH-UA:
11 Sec-CH-UA-Mobile: 0
12 Sec-CH-UA-Platform: ""
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
16

```

Response

```

1 HTTP/2.2 200 OK
2 Server: hcdn
3 Date: Tue, 24 Oct 2023 07:31:34 GMT
4 Content-Type: text/html; charset=UTF-8
5 Vary: Accept-Encoding
6 X-Powered-By: PHP/7.4.33
7 Set-Cookie: PHPSESSID=e3938bc53aa5a1d9c32bcec4d73de7f; path=/; secure
8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
9 Cache-Control: no-store, no-cache, must-revalidate
10 Pragma: no-cache
11 Platform: hostingier
12 Content-Security-Policy: upgrade-insecure-requests
13 X-Turbo-Charged-By: LiteSpeed
14 X-Hcdn-Request-Id: c49388ca9c42a4bd8788211f8184fa-1rv-edge2
15 X-Hcdn-Cache-Status: MISS
16 X-Hcdn-Upstream-Rt: 0.110
17
18 <doctype html>
19
20 <html lang="pl">
21 <head>
22 <meta charset="utf-8" />
23 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
24 <title>
25 LIVE CHAT 2.0 (Anonymous)
26 </title>
27 <meta name="viewport" content="width=device-width,initial-scale=0.85,maximum-scale=0.85,minimum-scale=0.85">
28 <link rel="shortcut icon" href="img/adm.png">
29 <link href="https://fonts.googleapis.com/css?family=LilitaOne&display=swap" rel="stylesheet">
30 <link href="https://www.wykop.pl/css/full.css" rel="stylesheet">
31 </head>

```

Inspector

- Request attributes: 2
- Request headers: 16
- Response headers: 15