# CHANDIGARH UNIVERSITY

## UNIVERSITY INSTITUTE OF NGINEERING

## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

**Submitted By:**
Vivek Kumar(21BCS8129)

**Submitted To:**
Er. Himanshi (13362)

| | |
|---|---|
| **Subject Name** | Web and Mobile Security Lab |
| **Subject Code** | 20CSP-338 |
| **Branch** | Computer Science and Engineering |
| **Semester** | 5th |

## Experiment - 7

**Student Name: Vivek Kumar** **UID: 21BCS8129**
**Branch: BE-CSE(LEET)** **Section/Group: WM-20BCS-616/A**
**Semester: 5th** **Date of Performance: 02/11/2022**
**Subject Name: Web and Mobile Security Lab** **Subject Code: 20CSP-338**

### 1. Aim/Overview of the practical:

Implementation of Session hijacking attack on http-enabled website.

### 2. Task to be done/ Which logistics used:

To Implementation of Session hijacking attack on http-enabled website.

**3. Apparatus / Simulator Used:**

- Windows 7 & above version.
- Google Chrome
- OWASP ZAP
- JHijack - a numeric session hijacking tool

### Session Hijacking:

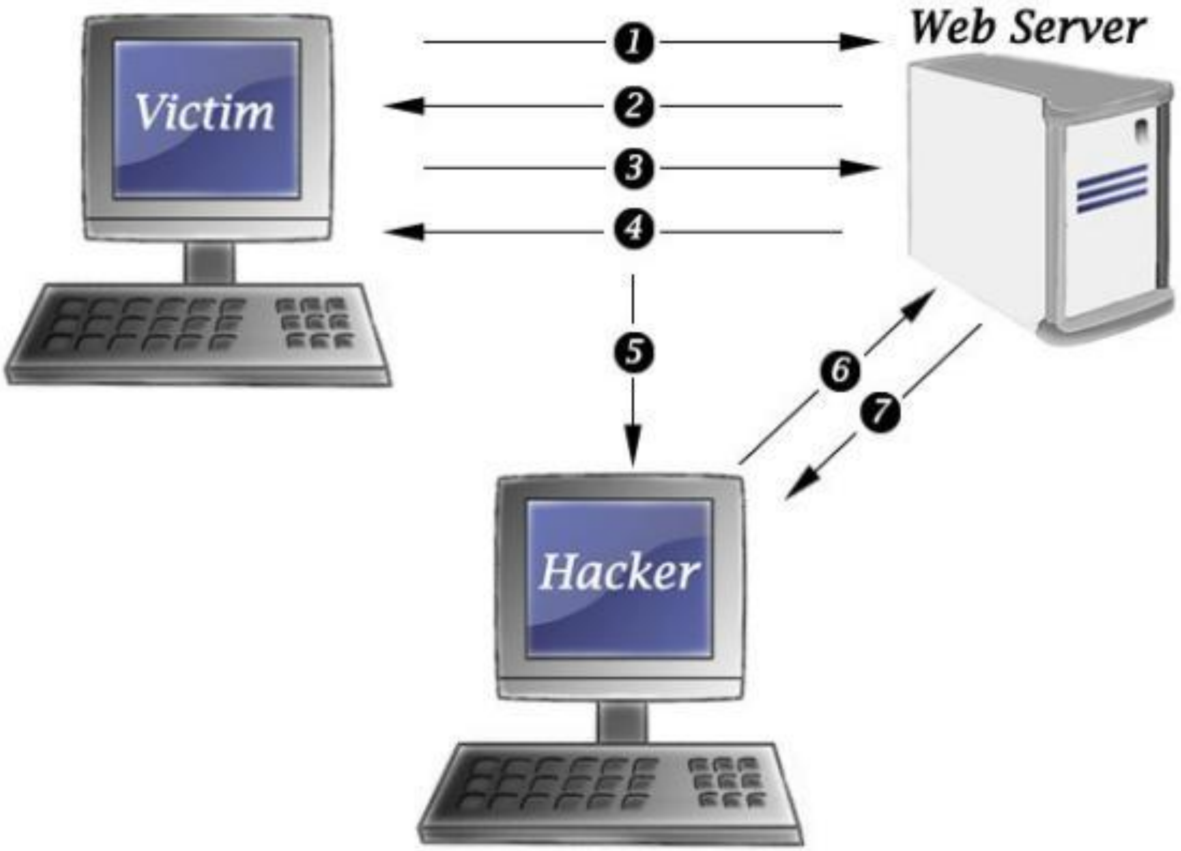
The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connection. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

The session token could be compromised in different ways; the most common are:

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
- Man-in-the-middle attack
- Man-in-the-browser attack
- Sniffer and Session Hijacking

**How Session Hijacking Works**



Session hijacking takes place when the trust of two host, services or accounts is compromised by an attacker who is known as the Man-In-The-Middle (MiTM)

Session hijacking can happen in multiple ways. There are web-based hijacks, wireless AP hijacks, also known as an evil twin attack, and TCP session-based hijacks. The principle is the same in all attacks and that is to attack the lower layers on the OSI model than the actual session is occurring. As an example, in a TCP attack, the idea is to let Layers 5 to 7 establish trust and then take the Layer 4 socket.

There are five key methods of Session hijacking: **Session Fixation**. **Session Side Jacking**. **Cross-Site Scripting**.

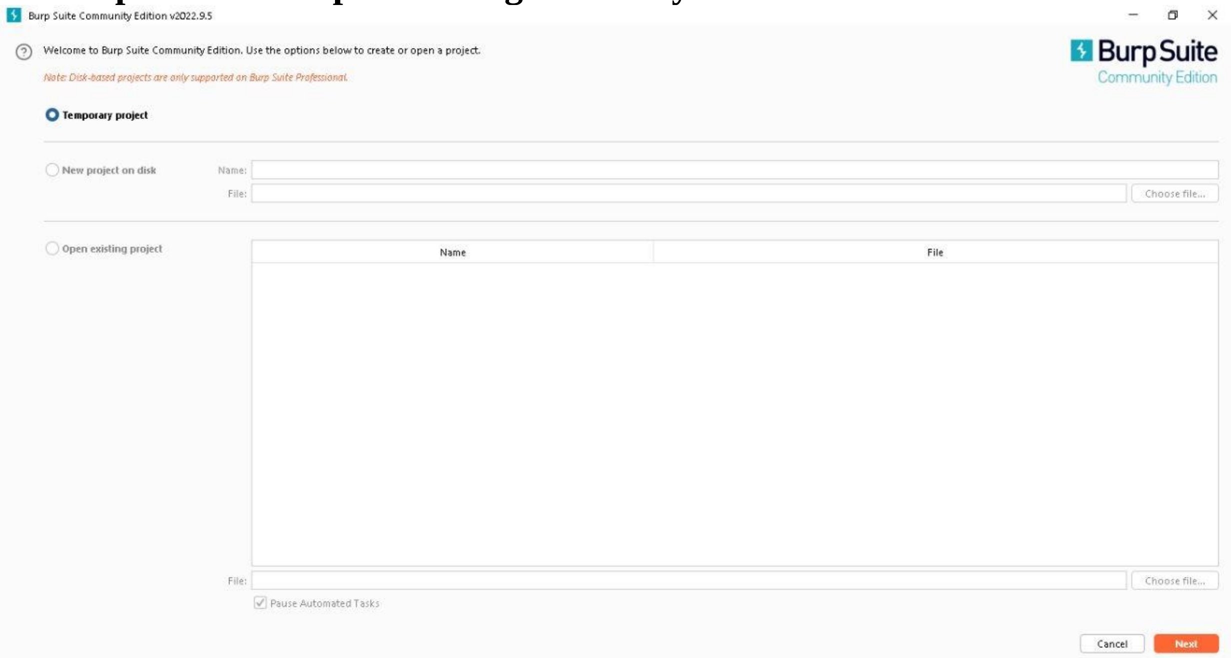
**4. Program/ Steps/ Method:**

1. Login to the website as the victim and reach any page offering a secure function requiring authentication.
2. Delete from the cookie jar all the cookies which satisfy any of the following conditions.
   - in case there is no HSTS adoption: the Secure attribute is set.
   - in case there is partial HSTS adoption: the Secure attribute is set or the Domain attribute is not set.
3. Save a snapshot of the cookie jar.
4. Trigger the secure function identified at step 1.
5. Observe whether the operation at step 4 has been performed successfully. If so, the attack was successful.
6. Clear the cookie jar, login as the attacker and reach the page at step 1.
7. Write in the cookie jar, one by one, the cookies saved at step 3.
8. Trigger again the secure function identified at step 1.
9. Clear the cookie jar and login again as the victim.
10. Observe whether the operation at step 8 has been performed successfully in the victim’s account. If so, the attack was successful; otherwise, the site is secure against session hijacking.

Session Sniffing:

1. Capture a valid token session called “Session ID” using sniffer.
2. Use the valid token session to gain unauthorized access to the Web Server.

## 5. DBMS Script/Result/Output/Writing Summary:



Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

*Note: Disk-based projects are only supported on Burp Suite Professional.*

● Temporary project

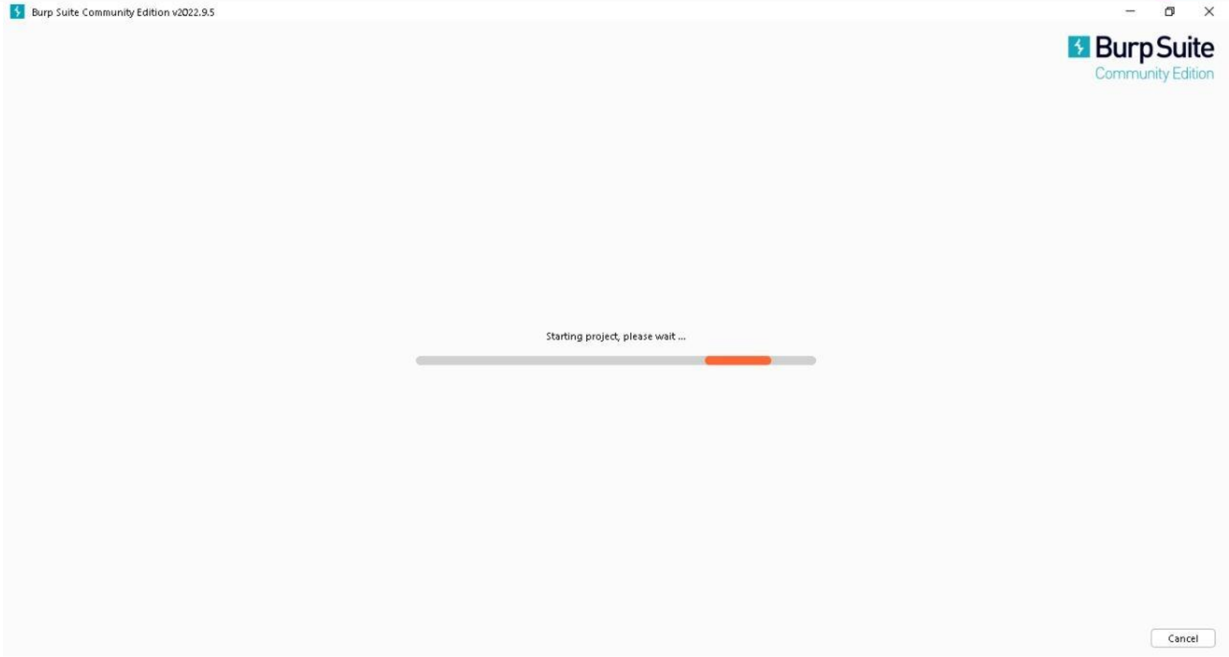
○ New project on disk Name: File: Choose file...

○ Open existing project

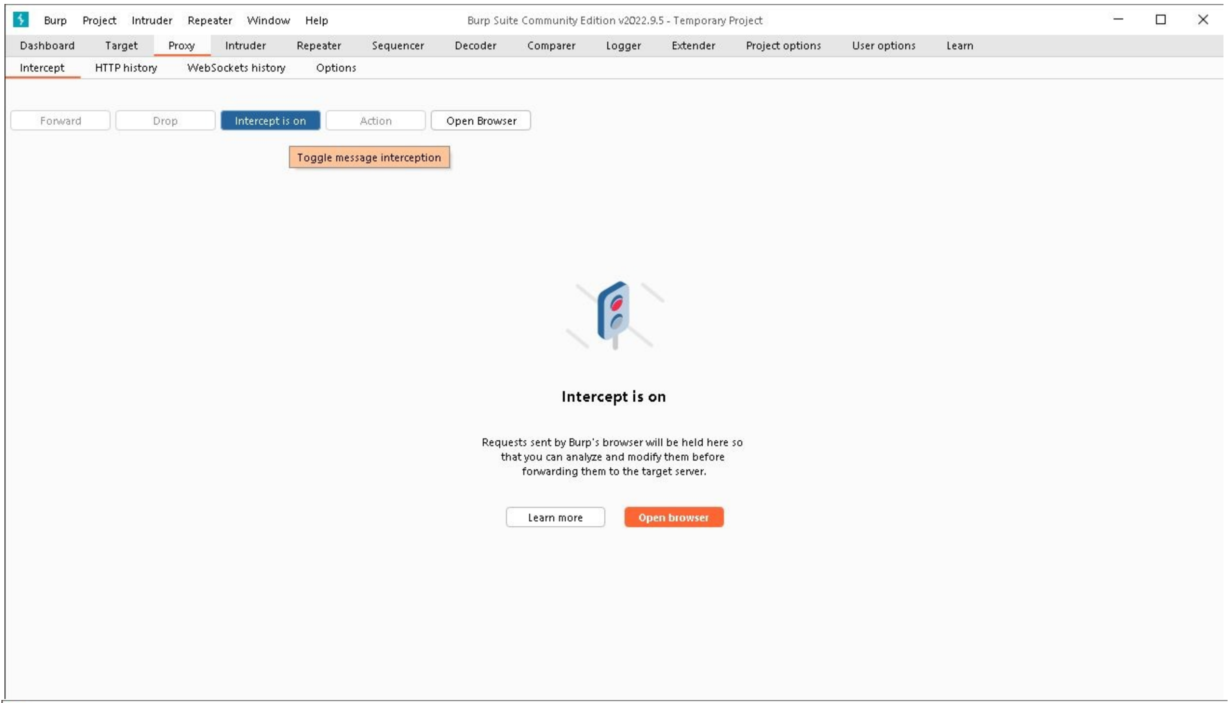
| Name | File |
|---|---|

File: Choose file...

☑ Pause Automated Tasks

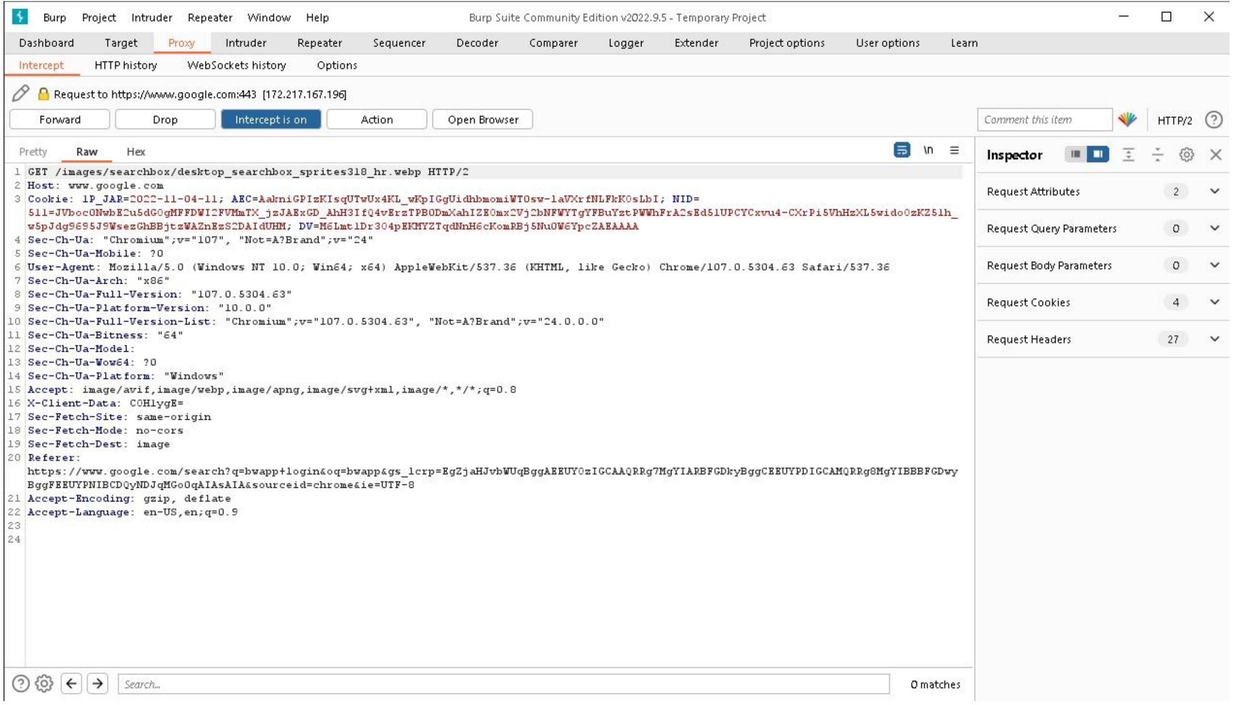


Starting project, please wait ...



**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.

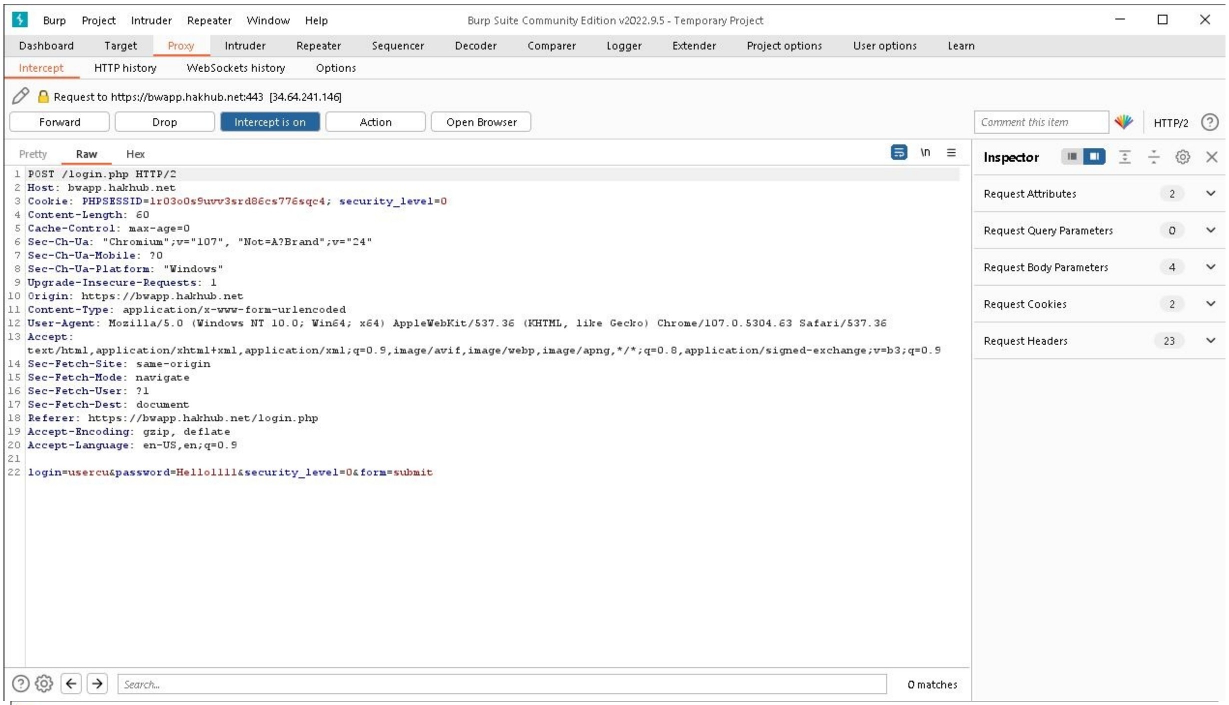


Request to https://www.google.com:443 [172.217.167.196]

```
GET /images/searchbox/desktop_searchbox_sprites318_hr.webp HTTP/2
Host: www.google.com
Cookie: 1P_JAR=2022-11-04-11; AEC=AakniGPIzKIsqUTwUx4KL_wKpIGgUidhbmomiWT0sw-1aVXrfNLFkK0sLbI; NID=
511=JVboc0NwbE2u5dG0gMFFDWI2FVMmTX_jzJAExGD_AhH3IfQ4vErzTPB0DmXahIZE0mx2Vj2bNFWYTgYFBuYztPWWhFrA2sEd51UPCYCxvu4-CXrPi5VhHzXL5wido0zKZ51h_
w5pJdg9695J9WsezGhBBjtzWAZnEzS2DAIdUHM; DV=M6Lmt1Dr304pEKMYZTqdNnH6cKomRBj5NuOW6YpcZAEAAAA
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
Sec-Ch-Ua-Arch: "x86"
Sec-Ch-Ua-Full-Version: "107.0.5304.63"
Sec-Ch-Ua-Platform-Version: "10.0.0"
Sec-Ch-Ua-Full-Version-List: "Chromium";v="107.0.5304.63", "Not=A?Brand";v="24.0.0.0"
Sec-Ch-Ua-Bitness: "64"
Sec-Ch-Ua-Model:
Sec-Ch-Ua-Wow64: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
X-Client-Data: COHlygE=
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://www.google.com/search?q=bwapp+login&oq=bwapp&gs_lcrp=EgZjaHJvbWUqBggAEEUYOzIGCAAQRRg7MgYIARBFGDkyBggCEEUYPDIGCAMQRRg8MgYIBBBFGDwy
BggFEEUYPNIBCDQyNDJqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

| | |
|---|---|
| Request Attributes | 2 |
| Request Query Parameters | 0 |
| Request Body Parameters | 0 |
| Request Cookies | 4 |
| Request Headers | 27 |

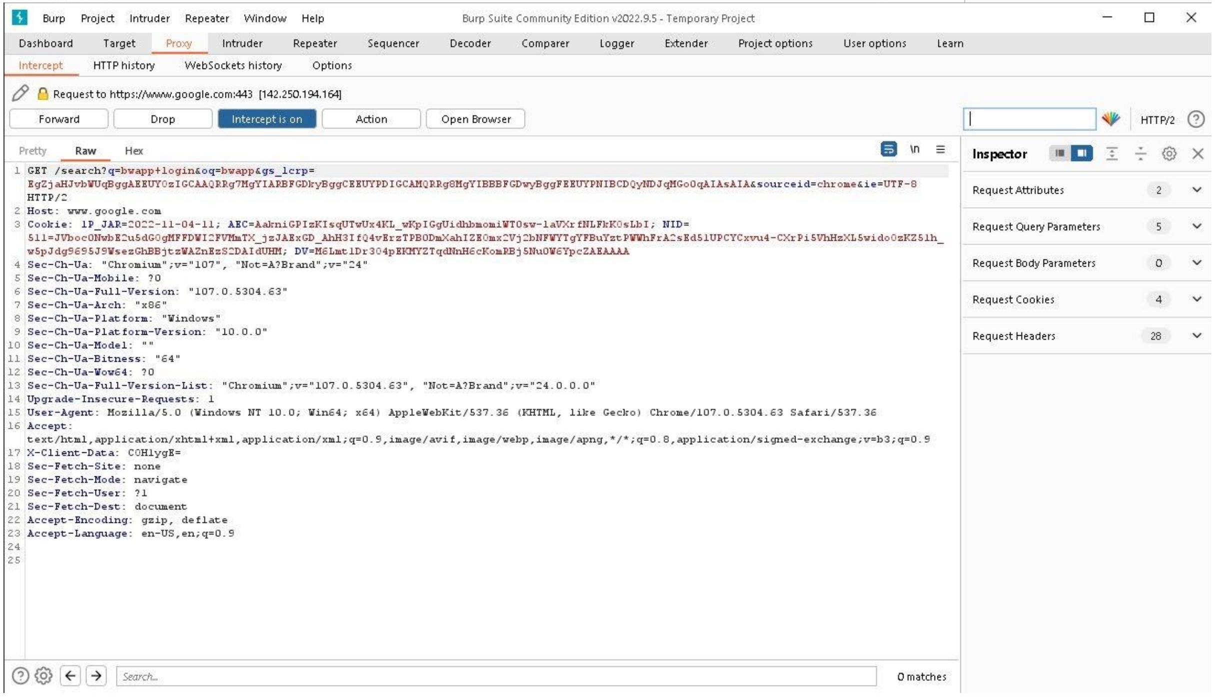

Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/2
Pretty Raw Hex
\n
Inspector
Search...
0 matches

Request to https://bwapp.hakhub.net:443 [34.64.241.146]

```
POST /login.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=1r03o0s9uvv3srd86cs776sqc4; security_level=0
Content-Length: 60
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

login=usercu&password=Hello1111&security_level=0&form=submit
```

Request Attributes 2
Request Query Parameters 0
Request Body Parameters 4
Request Cookies 2
Request Headers 23

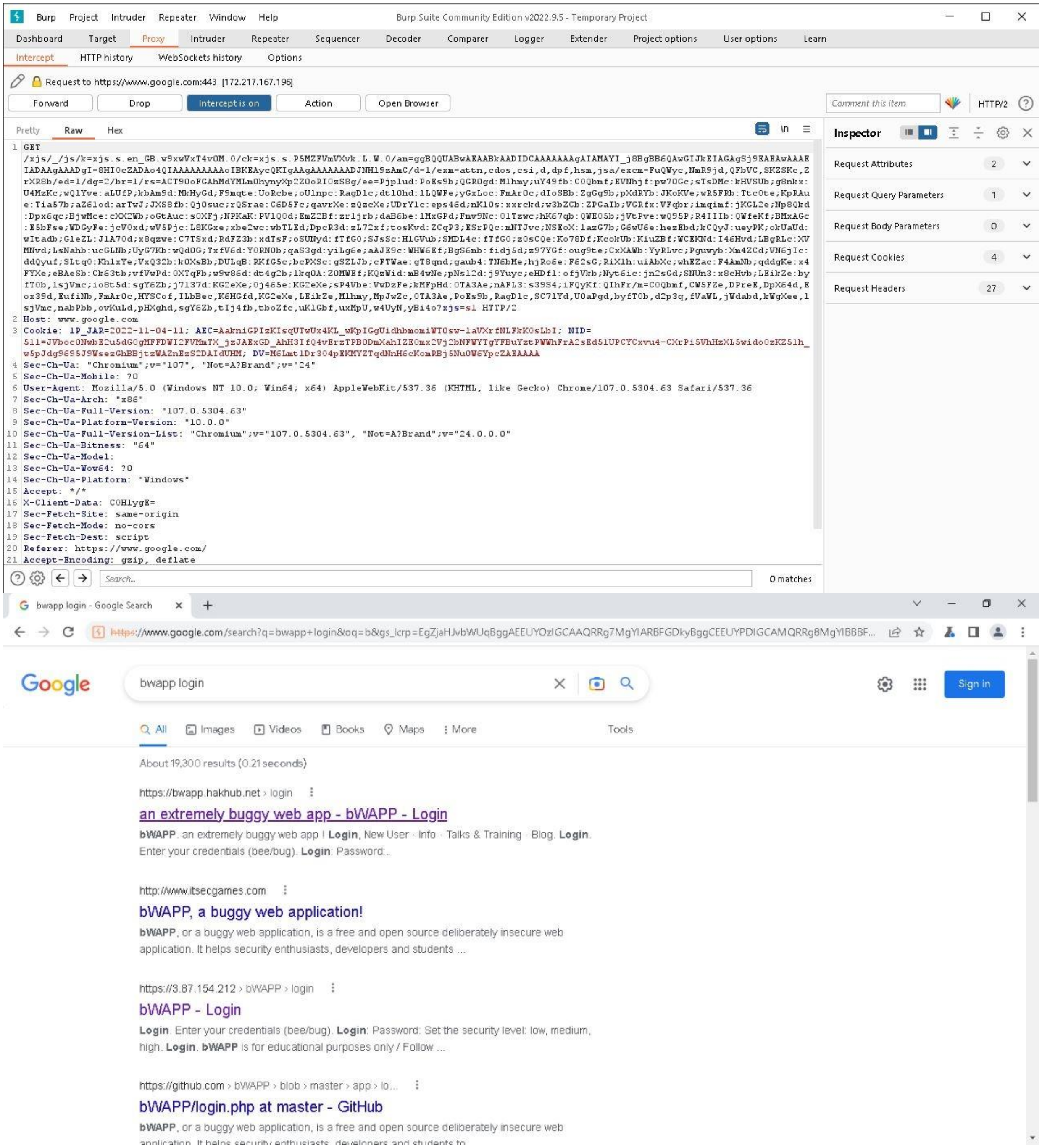

Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
HTTP/2
Pretty Raw Hex
\n
Inspector
Search...
0 matches

Request to https://www.google.com:443 [142.250.194.164]

```
GET /search?q=bwapp+login&oq=bwapp&gs_lcrp=
EgZjaHJvbWUqBggAEEUYOzIGCAAQRRg7MgYIARBFGDkyBggCEEUYPDIGCAMQRRg8MgYIBBBFGDwyBggFEEUYPNIBCDQyNDJqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8
HTTP/2
Host: www.google.com
Cookie: 1P_JAR=2022-11-04-11; AEC=AakniGPIzKIsqUTwUx4KL_wKpIGgUidhbmomiWT0sw-1aVXrfNLFkK0sLbI; NID=
511=JVboc0NwbE2u5dG0gMFFDWI2FVMmTX_jzJAExGD_AhH3If Q4vErzTPB0DmXahIZE0mx2Vj2bNFWYTgYFBuYztPWWhFrA2sEd51UPCYCxvu4-CXrPi5VhHzXL5wido0zKZ51h_
w5pJdg9695J9WsezGhBBjtzWAZnEzS2DAIdUHM; DV=M6Lmt1Dr304pEKMYZTqdNnH6cKomRBj5Nu0W6YpcZAEAAAA
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Full-Version: "107.0.5304.63"
Sec-Ch-Ua-Arch: "x86"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Platform-Version: "10.0.0"
Sec-Ch-Ua-Model: ""
Sec-Ch-Ua-Bitness: "64"
Sec-Ch-Ua-Wow64: ?0
Sec-Ch-Ua-Full-Version-List: "Chromium";v="107.0.5304.63", "Not=A?Brand";v="24.0.0.0"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
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=0.9
X-Client-Data: COHlygE=
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

Request Attributes 2
Request Query Parameters 5
Request Body Parameters 0
Request Cookies 4
Request Headers 28


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/2
Pretty Raw Hex
\n
Inspector
Search...
0 matches
bwapp login - Google Search
All Images Videos Books Maps More Tools
Sign in

Request to https://www.google.com:443 [172.217.167.196]

```
GET
/xjs/_/js/k=xjs.s.en_GB.w9xwVxT4vOM.0/ck=xjs.s.P5MZFVmVXvk.L.W.0/am=ggBQQUABwAEAABkAADIDCAAAAAAAgAIAMAYI_j8BgBB6QAwGIJkEIAGAgSj9EAEAwAAAE
IADAAgAAADgI-8HI0cZADAo4QIAAAAAAAAAoIBKEAycQKIgAAgAAAAAAADJNH19zAmC/d=1/exm=attn,cdos,csi,d,dpf,hsm,jsa/excm=FuQWyc,NmR9jd,QFbVC,SKZSKc,Z
rXR8b/ed=1/dg=2/br=1/rs=ACT90oFGAhMdYMLm0hynyXp2Z0oRI0zS8g/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:C0Qbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:
U4MzKc;wQ1Yve:aLUfP;kbAm9d:MrHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;dtl0hd:lLQWFe;yGxLoc:FmAr0c;dIoSBb:ZgGg9b;pXdRYb:JKoKVe;wR5FRb:Ttc0te;KpRAu
e:Tia57b;aZ61od:arTwJ;JXS8fb:Qj0suc;rQSrae:C6D5Fc;qavrXe:zQzcXe;UDrY1c:eps46d;nKl0s:xxrckd;w3bZCb:ZPGaIb;VGRfx:VFqbr;imqimf:jKGL2e;Np8Qkd
:Dpx6qc;BjwMce:cXX2Wb;oGtAuc:s0XFj;NPKaK:PV1Q0d;EmZ2Bf:zrljrb;daB6be:lMxGPd;Fmv9Nc:01Tzwc;hK67qb:QWE05b;jVtPve:wQ95P;R4IIIb:QWfeKf;BMxAGc
:E5bFse;WDGyFe:jcV0xd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;kCQyJ:ueyPK;okUaUd:
wItadb;GleZL:J1A70d;x8qzwe:C7TSxd;RdFZ3b:xdTsF;oSUNyd:fTfG0;SJsSc:H1GVub;SMDL4c:fTfG0;z0sCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XV
MNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;TxfV6d:Y0RN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;z97YGf:oug9te;CxXAWb:YyRLvc;Pguwyb:Xm4ZCd;VN6jIc:
ddQyuf;SLtq0:Kh1xYe;VxQ32b:k0XsBb;DULqB:RKfG5c;bcPXSc:gSZLJb;cFTWae:gT8qmd;gaub4:TN6bMe;hjRo6e:F62sG;RiX1h:uiAbXc;whEZac:F4AmNb;qddgKe:x4
FYXe;eBAeSb:Ck63tb;vfVwPd:0XTqFb;w9w86d:dt4g2b;lkq0A:Z0MWEf;KQzWid:mB4wNe;pNsl2d:j9Yuyc;eHDfl:ofjVkb;Nyt6ic:jn2sGd;SNUn3:x8cHvb;LEikZe:by
fT0b,lsjVmc;io8t5d:sgY6Zb;j7137d:KG2eXe;0j465e:KG2eXe;sP4Vbe:VwDzFe;kMFpHd:0TA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=C0Qbmf,CW5FZe,DPreE,DpX64d,E
ox39d,EufiNb,FmAr0c,HYSCof,ILbBec,K6HGfd,KG2eXe,LEikZe,Mlhmy,MpJwZc,0TA3Ae,PoEs9b,RagDlc,SC71Yd,U0aPgd,byfT0b,d2p3q,fVaWL,jWdabd,kWgXee,l
sjVmc,nabPbb,ovKuLd,pHXghd,sgY6Zb,tIj4fb,tboZfc,uK1Gbf,uxMpU,w4UyN,yBi4o?xjs=sl HTTP/2
Host: www.google.com
Cookie: 1P_JAR=2022-11-04-11; AEC=AakniGPIzKIsqUTwUx4KL_wKpIGgUidhbmomiWT0sw-1aVXrfNLFkK0sLbI; NID=
511=JVboc0NwbE2u5dG0gMFFDWI2FVMmTX_jzJAExGD_AhH3IfQ4vErzTPB0DmXahIZE0mx2Vj2bNFWYTgYFBuYztPWWhFrA2sEd51UPCYCxvu4-CXrPi5VhHzXL5wido0zKZ51h_
w5pJdg9695J9WsezGhBBjtzWAZnEzS2DAIdUHM; DV=M6Lmt1Dr304pEKMYZTqdNnH6cKomRBj5NuOW6YpcZAEAAAA
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
Sec-Ch-Ua-Arch: "x86"
Sec-Ch-Ua-Full-Version: "107.0.5304.63"
Sec-Ch-Ua-Platform-Version: "10.0.0"
Sec-Ch-Ua-Full-Version-List: "Chromium";v="107.0.5304.63", "Not=A?Brand";v="24.0.0.0"
Sec-Ch-Ua-Bitness: "64"
Sec-Ch-Ua-Model:
Sec-Ch-Ua-Wow64: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
X-Client-Data: COHlygE=
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
```

| | |
|---|---|
| Request Attributes | 2 |
| Request Query Parameters | 1 |
| Request Body Parameters | 0 |
| Request Cookies | 4 |
| Request Headers | 27 |

https://www.google.com/search?q=bwapp+login&oq=b&gs_lcrp=EgZjaHJvbWUqBggAEEUYOzIGCAAQRRg7MgYIARBFGDkyBggCEEUYPDIGCAMQRRg8MgYIBBBF...

bwapp login

About 19,300 results (0.21 seconds)

https://bwapp.hakhub.net › login

an extremely buggy web app - bWAPP - Login

**bWAPP**. an extremely buggy web app ! **Login**, New User · Info · Talks & Training · Blog. **Login**. Enter your credentials (bee/bug). **Login**: Password:.

http://www.itsecgames.com

bWAPP, a buggy web application!

**bWAPP**, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students ...

https://3.87.154.212 › bWAPP › login

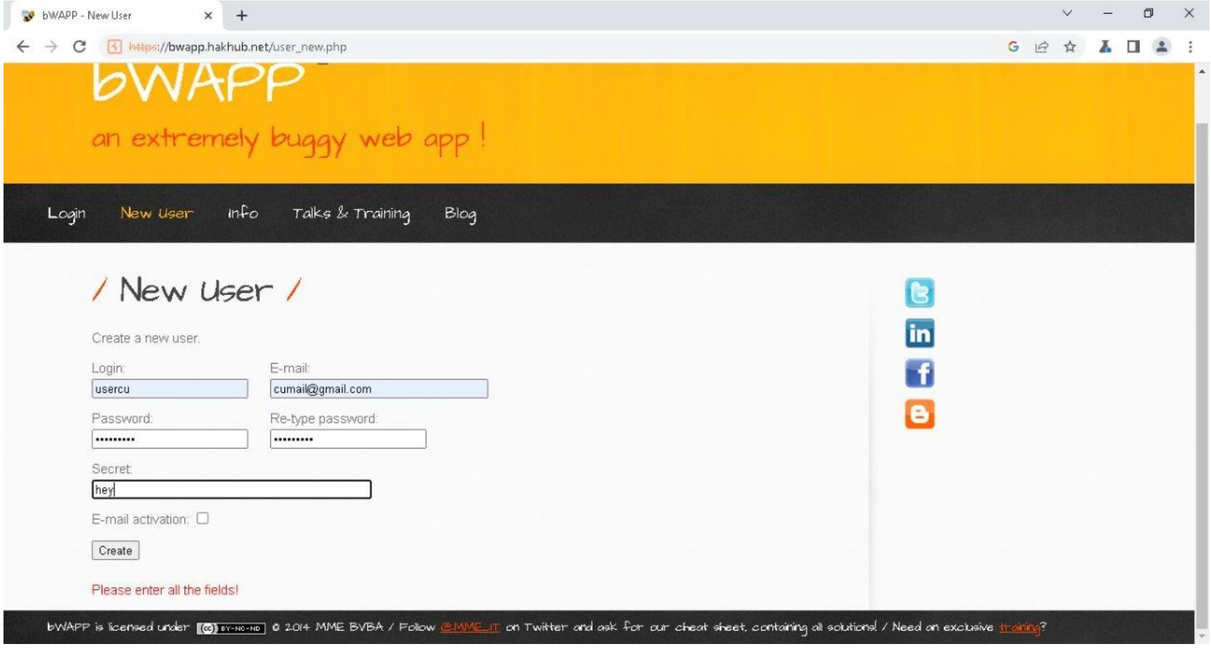
bWAPP - Login

**Login**. Enter your credentials (bee/bug). **Login**: Password: Set the security level: low, medium, high. **Login**. **bWAPP** is for educational purposes only / Follow ...

https://github.com › bWAPP › blob › master › app › lo...

bWAPP/login.php at master - GitHub

**bWAPP**, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to


bWAPP - New User
https://bwapp.hakhub.net/user_new.php
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog

/ New User /

Create a new user.

Login: usercu

E-mail: cumail@gmail.com

Password: •••••••••

Re-type password: •••••••••

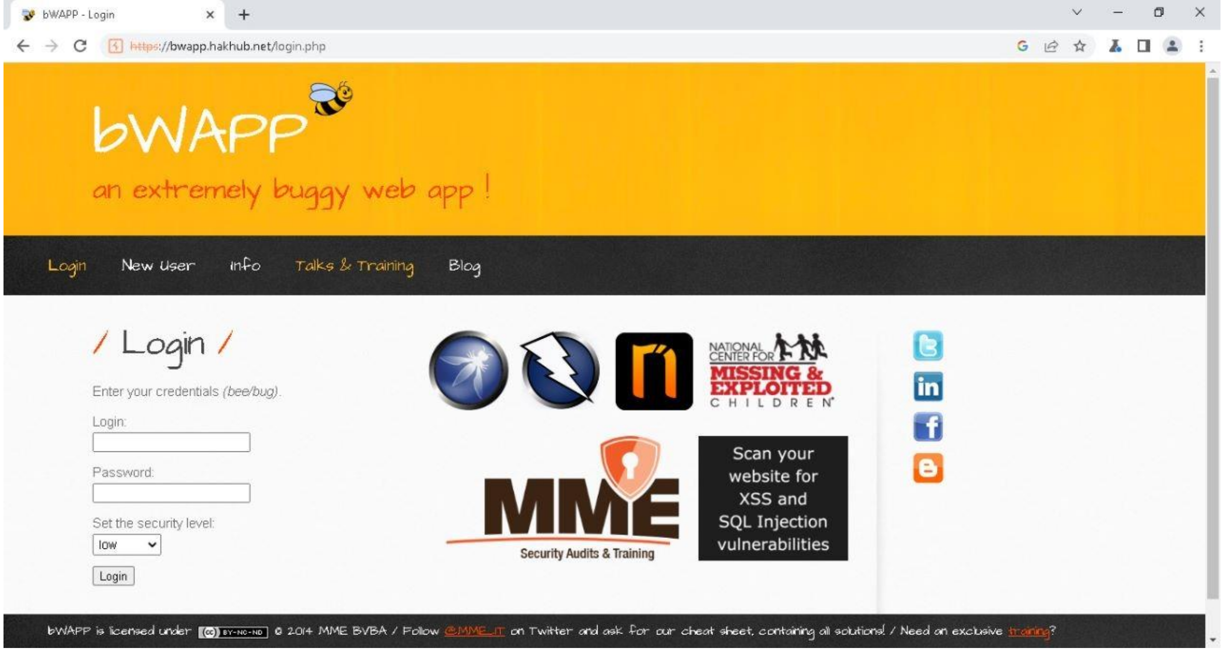
Secret: hey

E-mail activation: □

Create

Please enter all the fields!

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?


bWAPP - Login
https://bwapp.hakhub.net/login.php
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
Scan your website for XSS and SQL Injection vulnerabilities

/ Login /

Enter your credentials *(bee/bug)*.

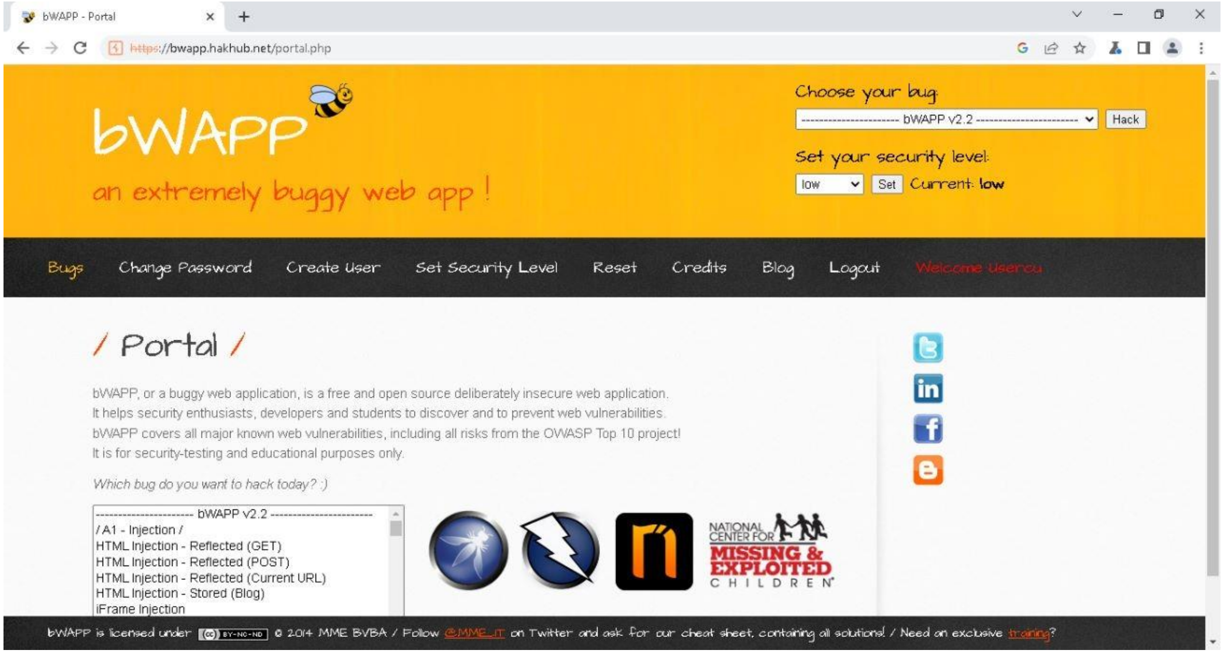
Login:

Password:

Set the security level: low

Login

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?



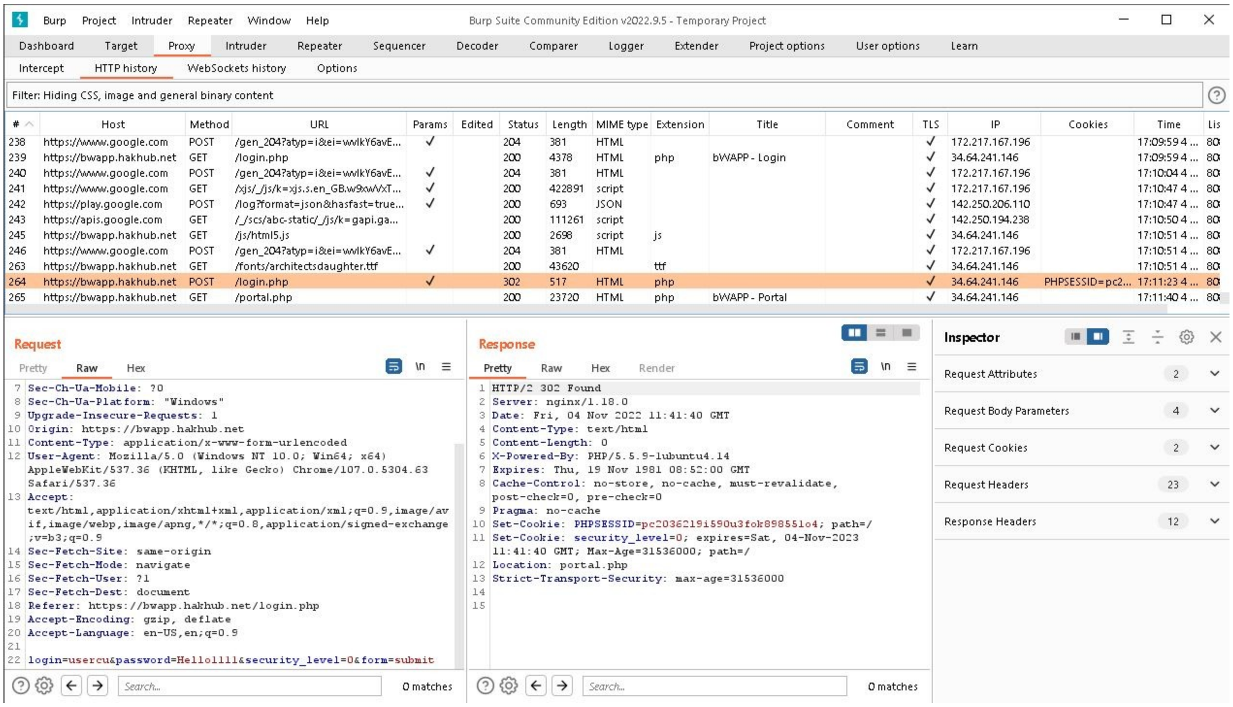
/ Portal /

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 v2.2 ----------------------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection

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?


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title | Comment | TLS | IP | Cookies | Time | Lis |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 238 | https://www.google.com | POST | /gen_204?atyp=i&ei=wvlkY6avE... | ✓ | | 204 | 381 | HTML | | | | ✓ | 172.217.167.196 | | 17:09:59 4 ... | 80 |
| 239 | https://bwapp.hakhub.net | GET | /login.php | | | 200 | 4378 | HTML | php | bWAPP - Login | | ✓ | 34.64.241.146 | | 17:09:59 4 ... | 80 |
| 240 | https://www.google.com | POST | /gen_204?atyp=i&ei=wvlkY6avE... | ✓ | | 204 | 381 | HTML | | | | ✓ | 172.217.167.196 | | 17:10:04 4 ... | 80 |
| 241 | https://www.google.com | GET | /xjs/_/js/k=xjs.s.en_GB.w9xwVxT... | ✓ | | 200 | 422891 | script | | | | ✓ | 172.217.167.196 | | 17:10:47 4 ... | 80 |
| 242 | https://play.google.com | POST | /log?format=json&hasfast=true... | ✓ | | 200 | 693 | JSON | | | | ✓ | 142.250.206.110 | | 17:10:47 4 ... | 80 |
| 243 | https://apis.google.com | GET | /_/scs/abc-static/_/js/k=gapi.ga... | | | 200 | 111261 | script | | | | ✓ | 142.250.194.238 | | 17:10:50 4 ... | 80 |
| 245 | https://bwapp.hakhub.net | GET | /js/html5.js | | | 200 | 2698 | script | js | | | ✓ | 34.64.241.146 | | 17:10:51 4 ... | 80 |
| 246 | https://www.google.com | POST | /gen_204?atyp=i&ei=wvlkY6avE... | ✓ | | 204 | 381 | HTML | | | | ✓ | 172.217.167.196 | | 17:10:51 4 ... | 80 |
| 263 | https://bwapp.hakhub.net | GET | /fonts/architectsdaughter.ttf | | | 200 | 43620 | | ttf | | | ✓ | 34.64.241.146 | | 17:10:51 4 ... | 80 |
| 264 | https://bwapp.hakhub.net | POST | /login.php | ✓ | | 302 | 517 | HTML | php | | | ✓ | 34.64.241.146 | PHPSESSID=pc2... | 17:11:23 4 ... | 80 |
| 265 | https://bwapp.hakhub.net | GET | /portal.php | | | 200 | 23720 | HTML | php | bWAPP - Portal | | ✓ | 34.64.241.146 | | 17:11:40 4 ... | 80 |

Request

```
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

login=usercu&password=Hello1111&security_level=0&form=submit
```

Response

```
HTTP/2 302 Found
Server: nginx/1.18.0
Date: Fri, 04 Nov 2022 11:41:40 GMT
Content-Type: text/html
Content-Length: 0
X-Powered-By: PHP/5.5.9-1ubuntu4.14
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
Set-Cookie: PHPSESSID=pc2036219i590u3fok898551o4; path=/
Set-Cookie: security_level=0; expires=Sat, 04-Nov-2023
11:41:40 GMT; Max-Age=31536000; path=/
Location: portal.php
Strict-Transport-Security: max-age=31536000
```

Inspector

| | |
|---|---|
| Request Attributes | 2 |
| Request Body Parameters | 4 |
| Request Cookies | 2 |
| Request Headers | 23 |
| Response Headers | 12 |

**Learning outcomes (What I have learnt):**

In the above experiment we have learnt that using session hijacking attack how the token session can be manipulated.

**Evaluation Grid (To be created per the faculty's SOP and Assessment guidelines):**

| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
|---|---|---|---|
| 1. | Worksheet completion including writing learning objectives/Outcomes.<br>(To be submitted at the end of the day). | | |
| 2. | Post-Lab Quiz Result. | | |
| 3. | Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions. | | |
| | Signature of Faculty (with Date): | Total Marks Obtained: | |