

Student Number:220966950

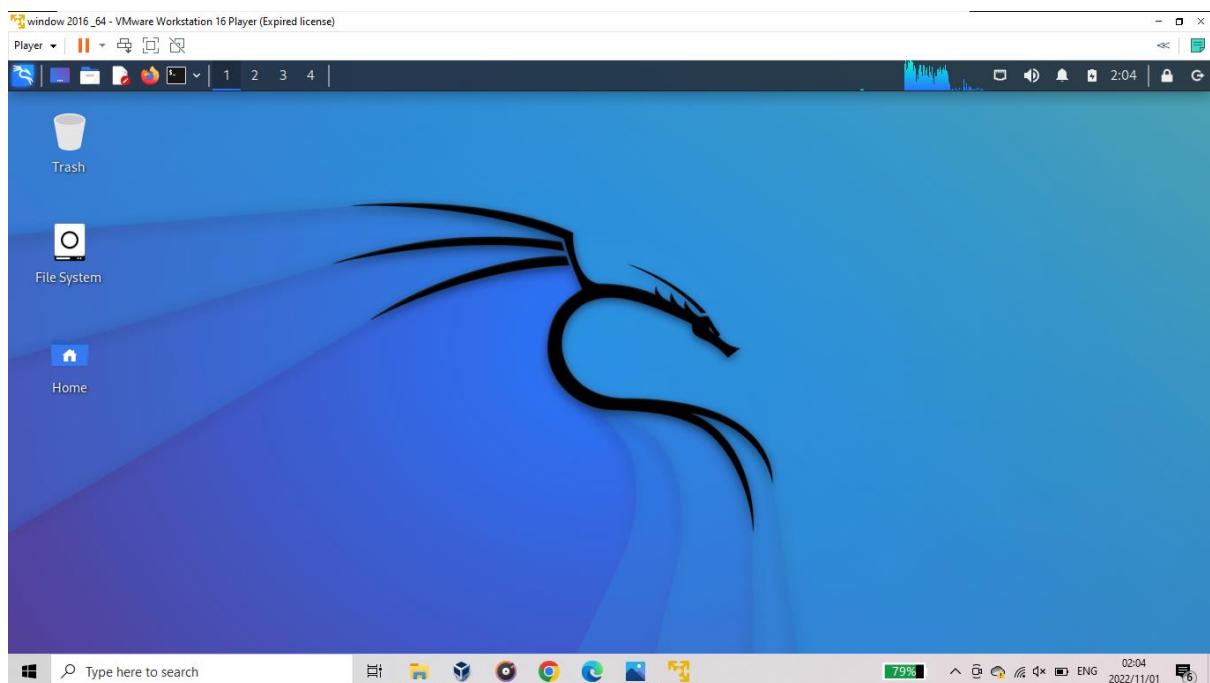
Name: Juliet

Surname:Ngoni

Exercise 1

Web Application Password Cracking

1. Desktop showing firefox and other applications.



2. Click menu icon at the top right and then click Preferences, Network proxy and click settings
Select no proxy.

The screenshot shows the Firefox settings page within a VMware Workstation window. The title bar indicates "window 2016_64 - VMware Workstation 16 Player (Expired license)". The main content area displays the "about:preferences" page.

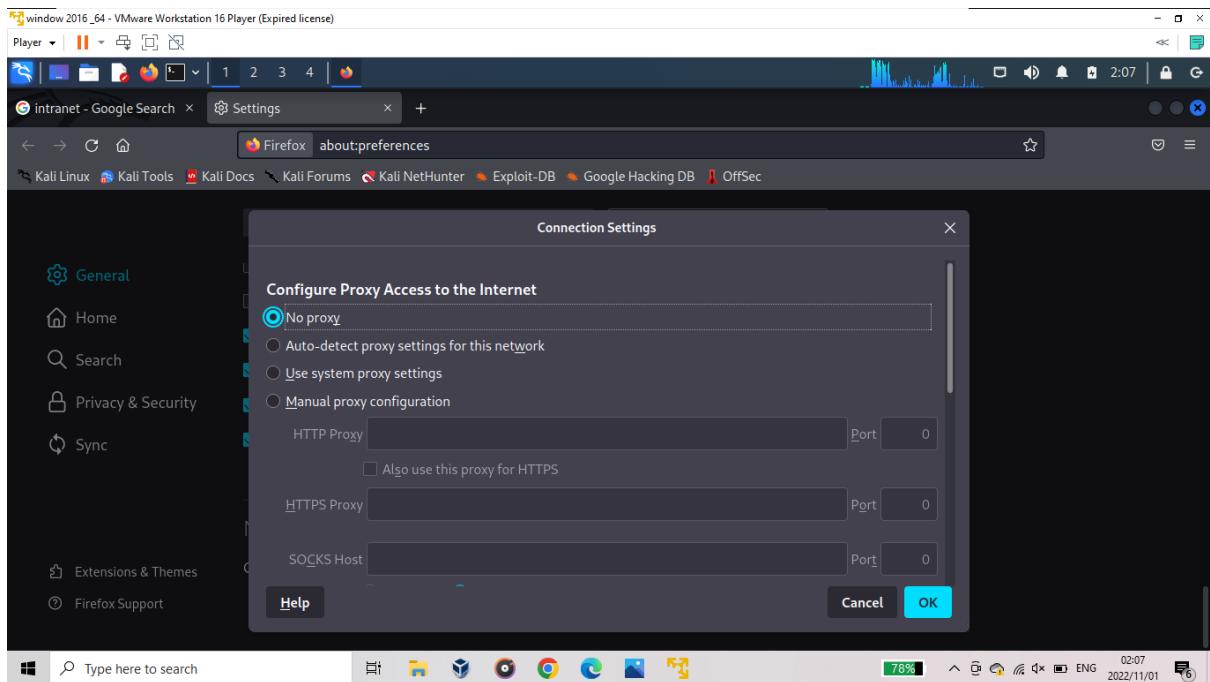
General

- Startup**
 - Restore previous session
 - Warn you when quitting the browser
 - Always check if Firefox is your default browser
 - Firefox is not your default browser** [Make Default...](#)
- Tabs**
 - Ctrl+Tab cycles through tabs in recently used order
 - Open links in tabs instead of new windows
 - When you open a link, image or media in a new tab, switch to it immediately

Network Settings

Configure how Firefox connects to the internet. [Learn more](#) [Settings...](#)

At the bottom of the window, the taskbar shows the Windows Start button, a search bar, and several pinned icons for various applications like File Explorer, Task View, and Edge.



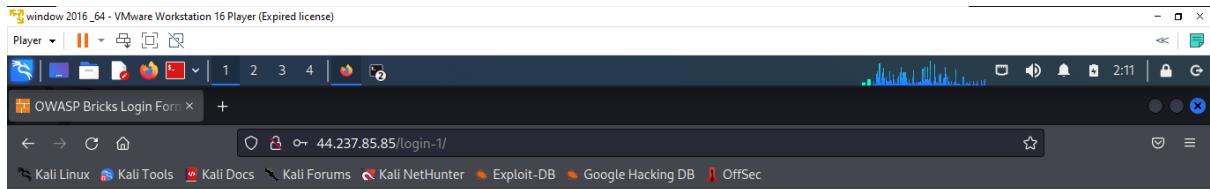
On the kali terminal enter command [ettercap -T grep password](#) to ;grab the password

Then on the firefox enter the url for OWASP Bricks

I decided to use owasp bricks because Bwapp url was down and did not go through.

OWASP Bricks is the same as the [BWAPP\(Buggy Web Application\)](#), they work the same as Bwapp helps with security ,developers and student to discover and prevent web vulnerabilities and to prepare one to conduct successful penetration testing and ethical hacking projects .bwapp also have over 100 web bugs and cover all major known web vulnerabilities.it is open source and is built on php and mySQL.

Then OWASP Bricks is a web application security learning platform built on php and mySQL.The mission of OWASP Bricks is to “Break the Bricks” and thus learn the various aspects of web application security.It has over 100 bugs and is also an open source.

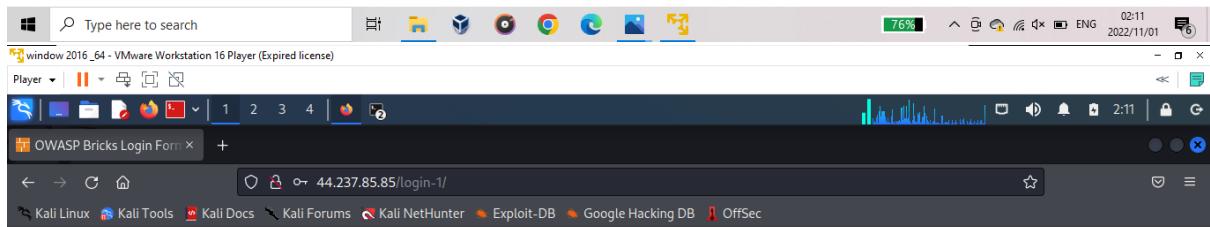


Login

You are not logged in.

Username:

Password:



Login

You are not logged in.

Username:

Password:

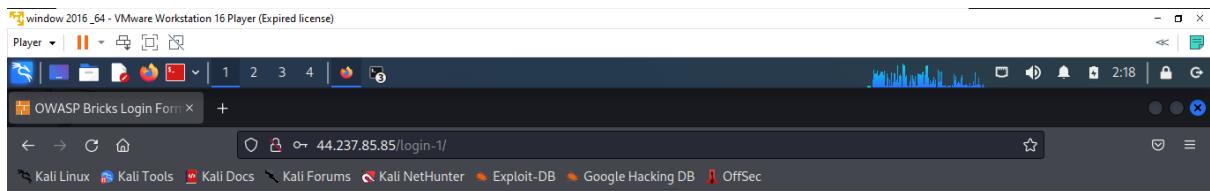


The OWASP have the credentials (username, password), admin admin, tom tom, ron ron.

I first used the credentials admin admin and the result were the following

The screenshot displays a terminal window titled "root@julietngonzi ~" running on a Linux system. The terminal is showing the results of a search operation using the "grep" command on a file named "password". The output indicates that the search is still in progress, with approximately 100.00% completion. The terminal window is part of a larger VMware Workstation interface, with other windows and icons visible in the background.

Then I used the credentials tom tom then the results are the following bshowing that the name as username is tom and the password is also tom.

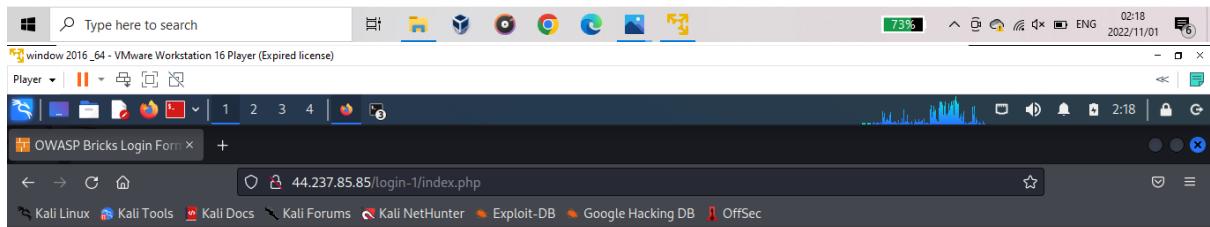


Login

You are not logged in.

Username:

Password:



Login

Successfully logged in.

Username:

Password:

SQL Query: SELECT * FROM users WHERE name='tom' and password='tom'



```
root@julietngoni:~# ettercap -T | grep password
<p>Password: <input type="password" name="passwd" id="passwd" size="25" required></p>
<div class="eight columns centered"><div class="alert-box secondary">SQL Query: SELECT * FROM users WHERE name='tom' and password='tom'<a href="" class="close">&times;</a></div></div>
```

Bricks

Login

successfully logged in

Username:

Password:

Submit

SQL Query: SELECT * FROM users WHERE name='tom' and password='tom'

Task 2 : using medusa to crack the password.

Install leafpad since my version of kali does not have the leafpad

```
root@julietngoni:~# apt install leafpad
Command 'leafpad' not found, but can be installed with:
apt install leafpad
Do you want to install it? (N/y)
apt install leafpad
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  evince-gtk
The following NEW packages will be installed:
  leafpad
0 upgraded, 1 newly installed, 0 to remove and 974 not upgraded.
Need to get 90.9 kB in 14s (6,612 B/s).
After this operation, 465 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 14s (6,612 B/s)
Selecting previously unselected package leafpad.
(Reading database ... 289302 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.9.4-6) ...
Processing triggers for mailcap (3.70+nmu1) ...
```

```
[root@julietngoni:~]# ./leafpad plab.txt
```

After downloading enter the command leafpad plab.txt.

And it will show the blank space for the leafpad file text and enter various different password(edit). Then after save as plab.txt.

The screenshot shows two terminal windows in a Kali Linux environment. The top window displays the contents of a file named 'plab.txt' containing various password entries. The bottom window shows the terminal history of installing the 'leafpad' package and saving the file.

```
root@julietngoni:~# leafpad
leafpad 0.8.18.1-5 is already the newest version.
0 upgraded, 1 newly installed, 0 to remove and 974 not upgraded.
Need to get 90.9 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/Kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 14s (6,612 B/s)
Selecting previously unselected package leafpad.
(Reading database ... 289302 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for mailcap (3.70+nmu1) ...

(root@julietngoni:~) # leafpad plab.txt
(root@julietngoni:~) # leafpad plab.txt
(root@julietngoni:~) #
```

window 2016_64 - VMware Workstation 16 Player (Expired license)

Player | ||| ↻

File Actions Edit View Help

leafpad
0 upgraded, 1 newly installed, 0 to remove and 974 not upgraded.
Need to get 90.9 kB of archives.
After this operation, 465 kB of additional disk space will be used.
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 14s (6,612 B/s)
Selecting previously unselected package leafpad.
(Reading database ... 289302 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for mailcap (3.70+nmu1) ...

(root@julietngoni:~) # leafpad plab.txt

(root@julietngoni:~) # leafpad plab.txt

(root@julietngoni:~) # leafpad plab.txt

(leafpad:11721): Gtk-WARNING **: 02:45:40.946: Attempting to store changes into `/root/.local/share/recently-used.xbel', but failed: Failed to create file "/root/.local/share/recently-used.xbel.IBMGV1": No such file or directory

(leafpad:11721): Gtk-WARNING **: 02:45:40.946: Attempting to set the permissions of `/root/.local/share/recently-used.xbel', but failed: No such file or directory

(root@julietngoni:~) #

(root@julietngoni:~) # clear

Enter the `command ls -l` to see where plab.txt and the user.txt(command: `cp plab.txt user.txt`) of which is the copy of plab.txt is allocated(Location).And ensure that it is indeed saved and contain both the files.

window 2016 _64 - VMware Workstation 16 Player (Expired license)

Player | 1 2 3 4 | 5 6

owasp bricks Login For XLSX download Google Sheets New Tab

File Actions Edit View Help

(root@julietngoni:~) # cp plab.txt user.txt

(root@julietngoni:~) # ls -l

total 8

-rw-r--r-- 1 root root 0 Jun 22 01:52 out1.e

-rw-r--r-- 1 root root 0 Jun 22 01:52 out1.exe

-rw-r--r-- 1 root root 79 Nov 1 02:45 plab.txt

-rw-r--r-- 1 root root 79 Nov 1 02:47 user.txt

(root@julietngoni:~) # medusa -n 44.237.85.85 -u tom -P plab.txt -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ERROR: Thread 5AFDC640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (1 of 3 retries)

ERROR: Thread 5AFDC640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (2 of 3 retries)

ERROR: Thread 5AFDC640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (3 of 3 retries)

NOTICE: ftp.mod: failed to connect, port 21 was not open on 44.237.85.85

(root@julietngoni:~) # medusa -n 44.237.85.85 -u tom -P plab.txt -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ERROR: Thread 861E0640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (1 of 3 retries)

ERROR: Thread 861E0640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (2 of 3 retries)

ERROR: Thread 861E0640: Host: 44.237.85.85 Cannot connect [unreachable], retrying (3 of 3 retries)

NOTICE: ftp.mod: failed to connect, port 21 was not open on 44.237.85.85

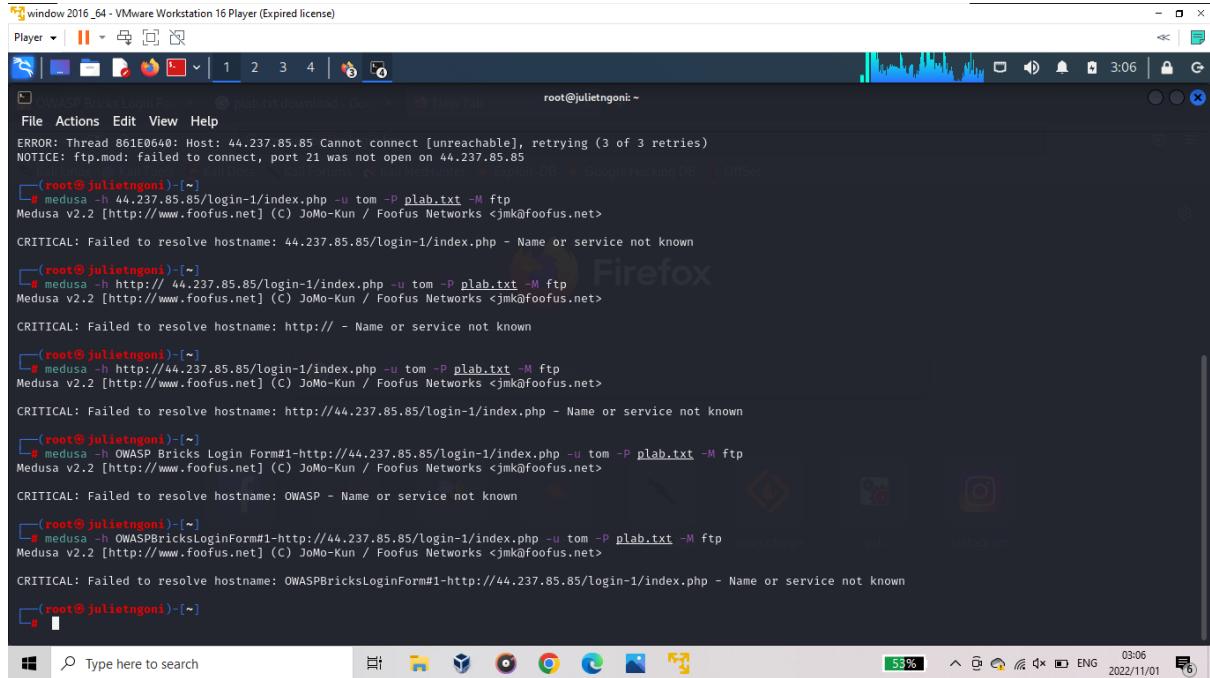
(root@julietngoni:~) # medusa -n 44.237.85.85/Login-1/index.php -u tom -P plab.txt -M ftp

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

CRITICAL: Failed to resolve hostname: 44.237.85.85/Login-1/index.php - Name or service not known

Enter Command `medusa -h 192.99.200.113 -u tom -P plab.txt -M ftp` and the result are as follow whereby it shows tha the coonection failed due to threads and the port 21 being closed or disabled.

This varies even on the command: medusa -h
192.99.200.113 -u tom -P user.txt -M ftp



The screenshot shows a terminal window titled "window 2016_64 - VMware Workstation 16 Player (Expired license)". The terminal is running on a root shell, indicated by the prompt "root@julietngoni:~". The user is executing the medusa command with various host and port specifications. The output includes error messages about connection failures and critical errors related to hostname resolution.

```
root@julietngoni:~#
root@julietngoni:~# medusa -h 44.237.85.85 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
CRITICAL: Failed to resolve hostname: 44.237.85.85/login-1/index.php - Name or service not known

root@julietngoni:~# medusa -h http:// 44.237.85.85/login-1/index.php -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
CRITICAL: Failed to resolve hostname: http:// - Name or service not known

root@julietngoni:~# medusa -h http://44.237.85.85/Login-1/index.php -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
CRITICAL: Failed to resolve hostname: http://44.237.85.85/login-1/index.php - Name or service not known

root@julietngoni:~# medusa -h OWASPBricsLoginForm#1=http://44.237.85.85/login-1/index.php -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
CRITICAL: Failed to resolve hostname: OWASPBricsLoginForm#1=http://44.237.85.85/login-1/index.php - Name or service not known

root@julietngoni:~#
```

```

window 2016_64 - VMware Workstation 16 Player (Expired license)
Player | || | 1 2 3 4 | 8:58 | 
root@julietngoni: ~
File Actions Edit View Help
[root@julietngoni] ~]
g medusa -h 192.168.47.1 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.47.1

[root@julietngoni] ~]
g medusa -h 192.168.47.1 -u bee -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.47.1

[root@julietngoni] ~]
g medusa -h 192.168.0.10 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (1 of 3 retries)
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (2 of 3 retries)
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (3 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.0.10

[root@julietngoni] ~]
g medusa -h 192.168.150.0 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 314BD640: Host: 192.168.150.0 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.150.0

[root@julietngoni] ~]
g

```



```

Type here to search 75% 08:58 2022/11/01
window 2016_64 - VMware Workstation 16 Player (Expired license)
Player | || | 1 2 3 4 | 8:58 | 
root@julietngoni: ~
File Actions Edit View Help
[root@julietngoni] ~]
g medusa -h 192.168.47.1 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.47.1

[root@julietngoni] ~]
g medusa -h 192.168.47.1 -u bee -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.47.1

[root@julietngoni] ~]
g medusa -h 192.168.0.10 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (1 of 3 retries)
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (2 of 3 retries)
ERROR: Thread 7FB9E640: Host: 192.168.0.10 Cannot connect [unreachable], retrying (3 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.0.10

[root@julietngoni] ~]
g medusa -h 192.168.150.0 -u tom -P plab.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 314BD640: Host: 192.168.150.0 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.150.0

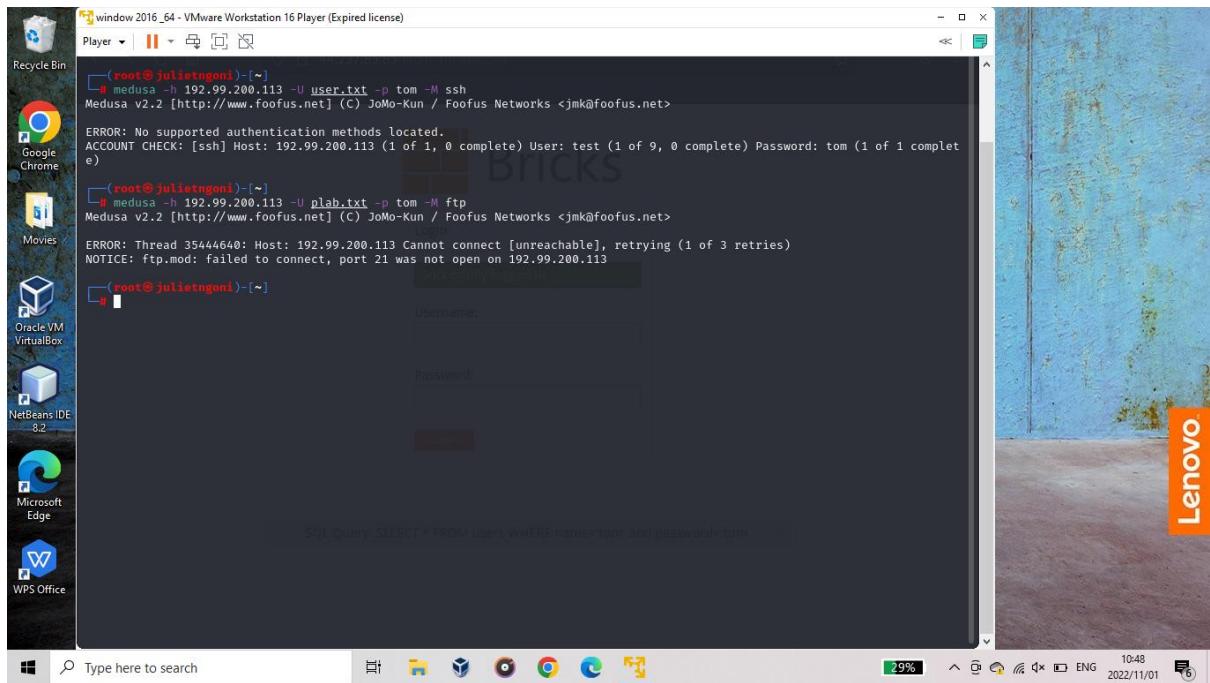
[root@julietngoni] ~]
g

```

Enter command: `medusa -h 192.99.200.113 -u tom -P plab.txt -M ssh` and also command: `medusa -h 192.99.200.113 -u tom -P user.txt -M ssh`

And it shows the following results that checks the account and discovers that 1 out of 9 are

complete and that the password is tom



Enter the command : medusa -h 192.99.200.113 -u user.txt -P plab.txt -M ftp

And then it shows the following results, this command is for both ftp and ssh.

```

window 2016_64 - VMware Workstation 16 Player (Expired license)
Player | [~] | Recycle Bin
[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: No supported authentication methods located.
ACCOUNT CHECK: [ssh] Host: 192.99.200.113 (1 of 1, 0 complete) User: test (1 of 9, 0 complete) Password: tom (1 of 1 complete)

[~] # medusa -h 192.99.200.113 -U plab.txt -p tom -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 35444640: Host: 192.99.200.113 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.99.200.113

[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: No supported authentication methods located.
ACCOUNT CHECK: [ssh] Host: 192.99.200.113 (1 of 1, 0 complete) User: test (1 of 9, 0 complete) Password: tom (1 of 1 complete)

[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 50DA7640: Host: 192.99.200.113 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.99.200.113

[~] # 

```

SQL Query: SELECT * FROM users WHERE name='tom' AND password='tom'


```

window 2016_64 - VMware Workstation 16 Player (Expired license)
Player | [~] | Recycle Bin
[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: No supported authentication methods located.
ACCOUNT CHECK: [ssh] Host: 192.99.200.113 (1 of 1, 0 complete) User: test (1 of 9, 0 complete) Password: tom (1 of 1 complete)

[~] # medusa -h 192.99.200.113 -U plab.txt -p tom -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 35444640: Host: 192.99.200.113 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.99.200.113

[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: No supported authentication methods located.
ACCOUNT CHECK: [ssh] Host: 192.99.200.113 (1 of 1, 0 complete) User: test (1 of 9, 0 complete) Password: tom (1 of 1 complete)

[~] # medusa -h 192.99.200.113 -U user.txt -p tom -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 50DA7640: Host: 192.99.200.113 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.99.200.113

[~] # medusa -h 192.99.200.113 -U plab.txt -p tom -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: Thread 2F5CA640: Host: 192.99.200.113 Cannot connect [unreachable], retrying (1 of 3 retries)
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.99.200.113

[~] # 

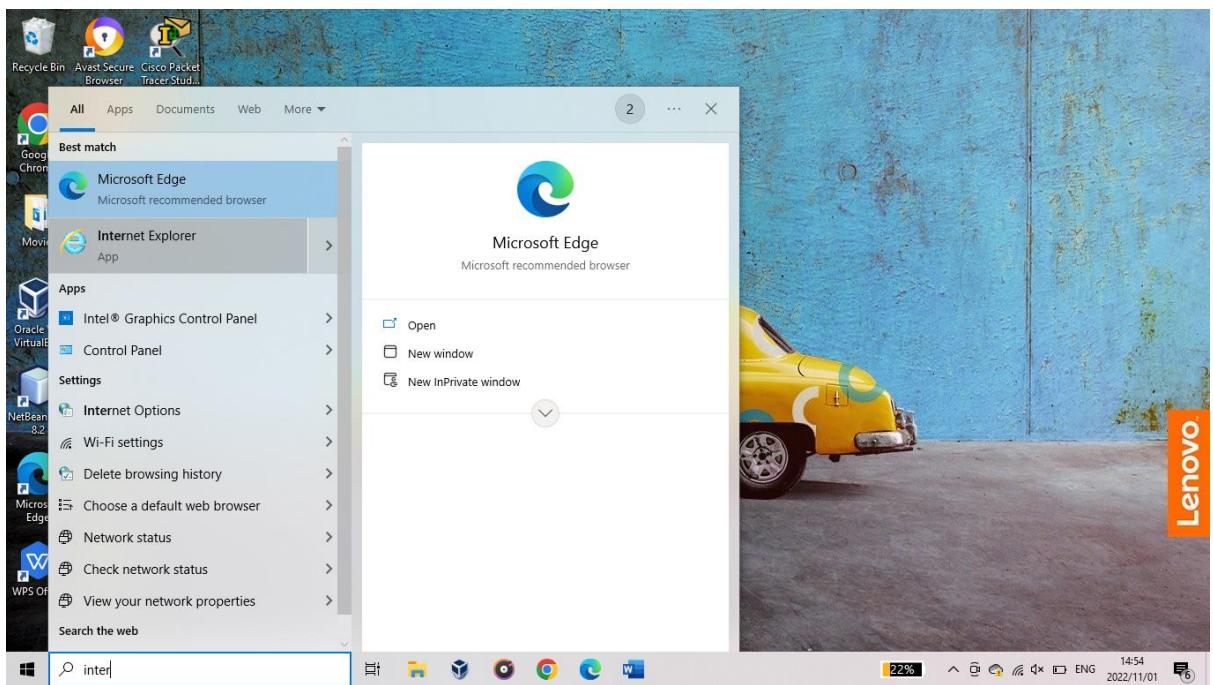
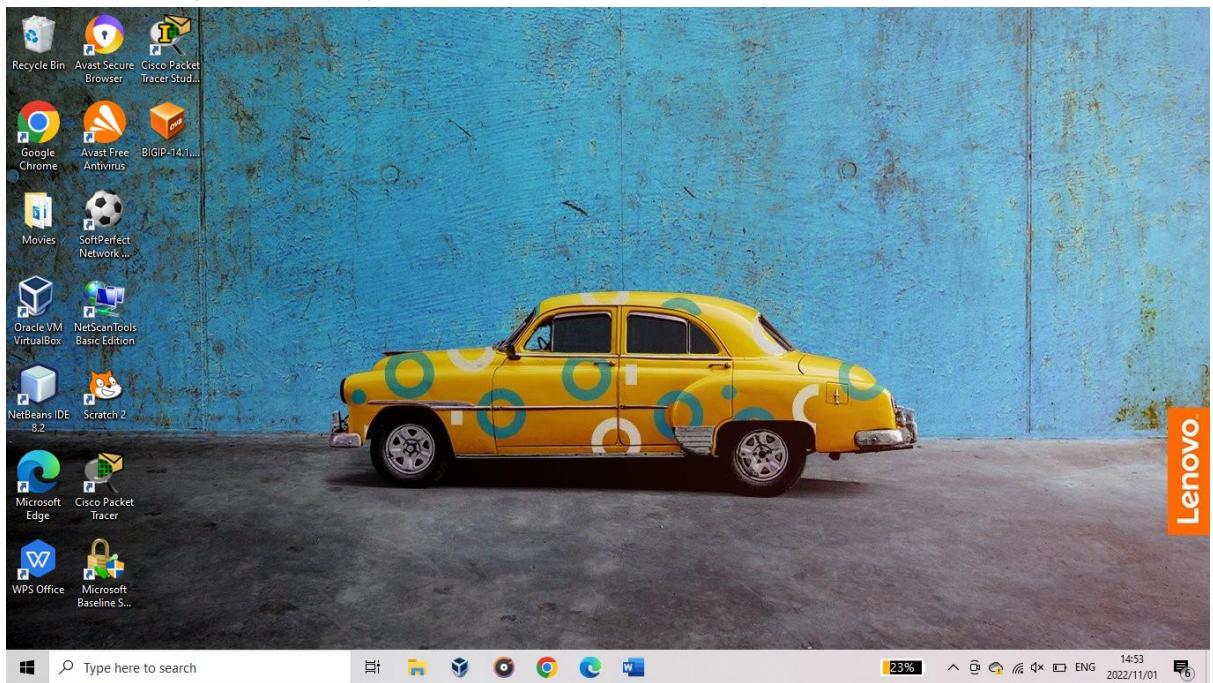
```

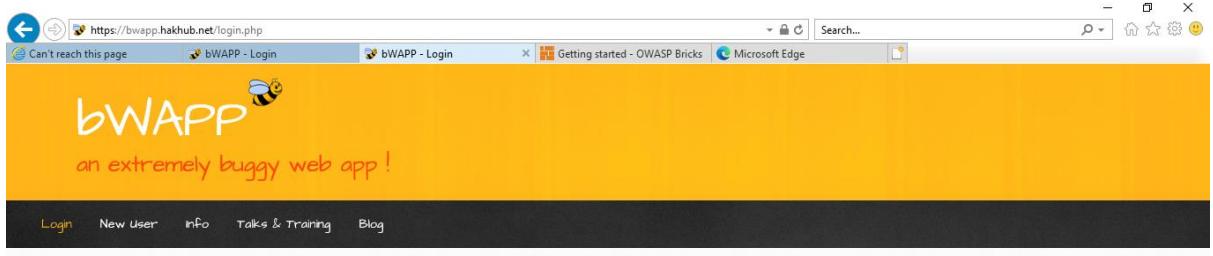
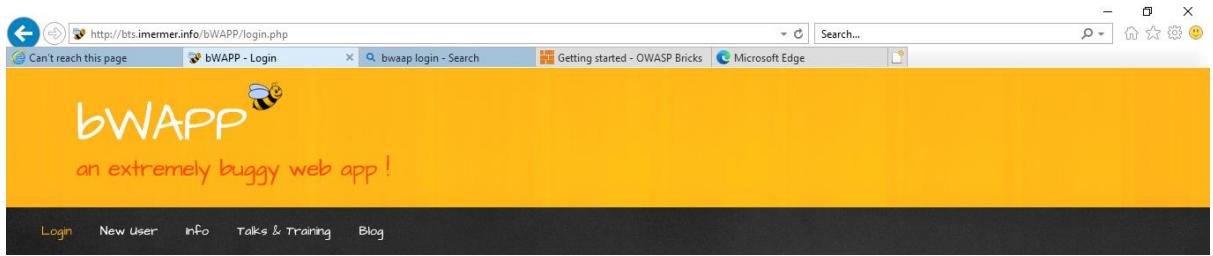
SQL Query: SELECT * FROM users WHERE name='tom' AND password='tom'

Exercise 2

Testing web application vulnerabilities

1. Desktop display





bWAPP
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ 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? :

- SQL Injection - Bind (SQLite)
- SQL Injection - Bind (Web Services/SOAP)
- XML/Path Injection (Login Form)
- XML/Path Injection (Search)
- /
- AS - Broken Auth & Session Manag.
- Broken Authentication - CAPTCHA Bypassing
- Broken Authentication - Forgotten Function
- Broken Authentication - Insecure Login Forms

Hack



Choose your bug

bWAPP v2.2 Hack

Set your security level

low Set Current: medium

Would you like to store your password for hakhub.net? More info

Yes Not for this site

Type here to search

100% 23:04 2022/11/01

Back Forward Go to copied address Ctrl+Shift+L Save background as... Set as background Copy background Select all Paste E-mail with Windows Live Translate with Bing All Accelerators > Create shortcut Add to favorites... View source Inspect element Encoding > Print... Print preview... Refresh Export to Microsoft Excel Send to OneNote Properties

Choose your bug

bWAPP v2.2 Hack

Set your security level

low Set Current: medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Broken Auth /

Enter the correct passphrase to unlock

Name:

Passphrase:

Unlock

Would you like to store your password for hakhub.net? More info

Yes Not for this site

Type here to search

100% 23:06 2022/11/01

The screenshot shows the Microsoft Edge browser window with the URL https://bwapp.hakhub.net/ba_insecure_login_2.php. The page title is "bWAPP - Login". The main content area displays the bWAPP logo and the tagline "an extremely buggy web app!". A navigation bar at the top includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Ben. On the right side, there are social sharing icons for Twitter, LinkedIn, Facebook, and Email. A dropdown menu titled "Choose your bug" is set to "bWAPP v2.2" and "Hack". Below it, a "Set your security level" dropdown is set to "Current: medium". The bottom of the page features a footer with developer tools information and a timestamp: "bwapp is licensed under MIT © 2014 MME BVBA / Follow [@MME_IT](#) on twitter and ask for our cheat sheet containing all solutions! / Need an exclusive [training?](#)". The F12 Developer Tools panel is open, showing the DOM Explorer tab with the file "ba_insec.in_2.php" selected. The code pane contains the following PHP code:

```
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5
6 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
7
```

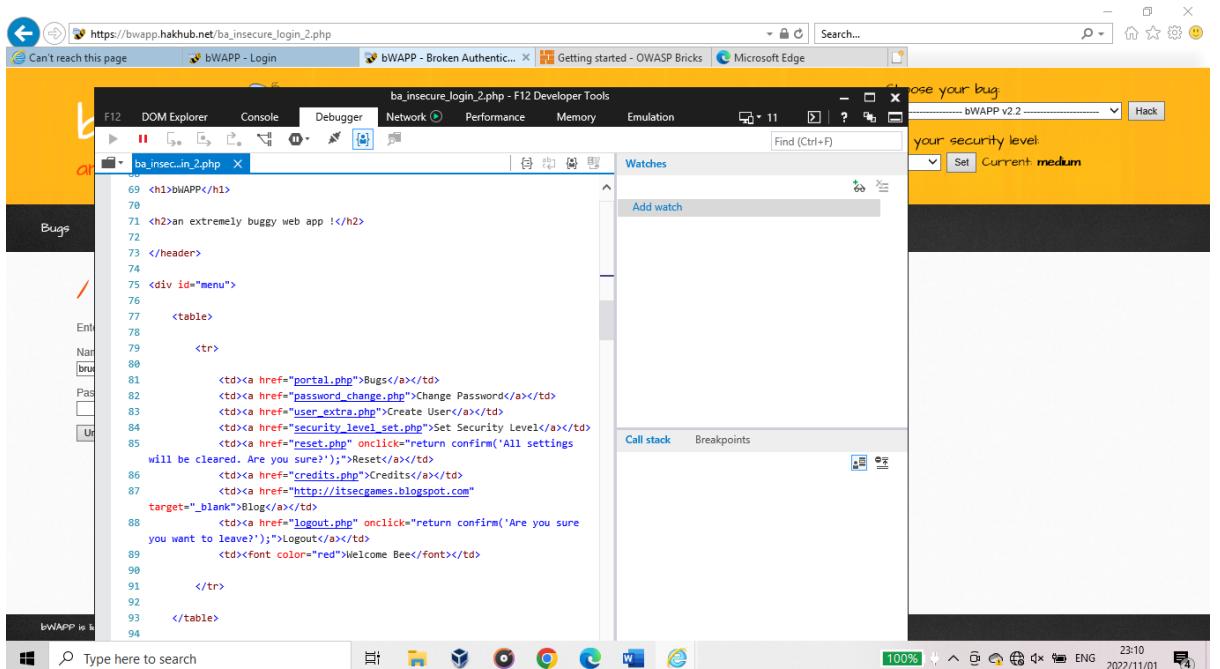
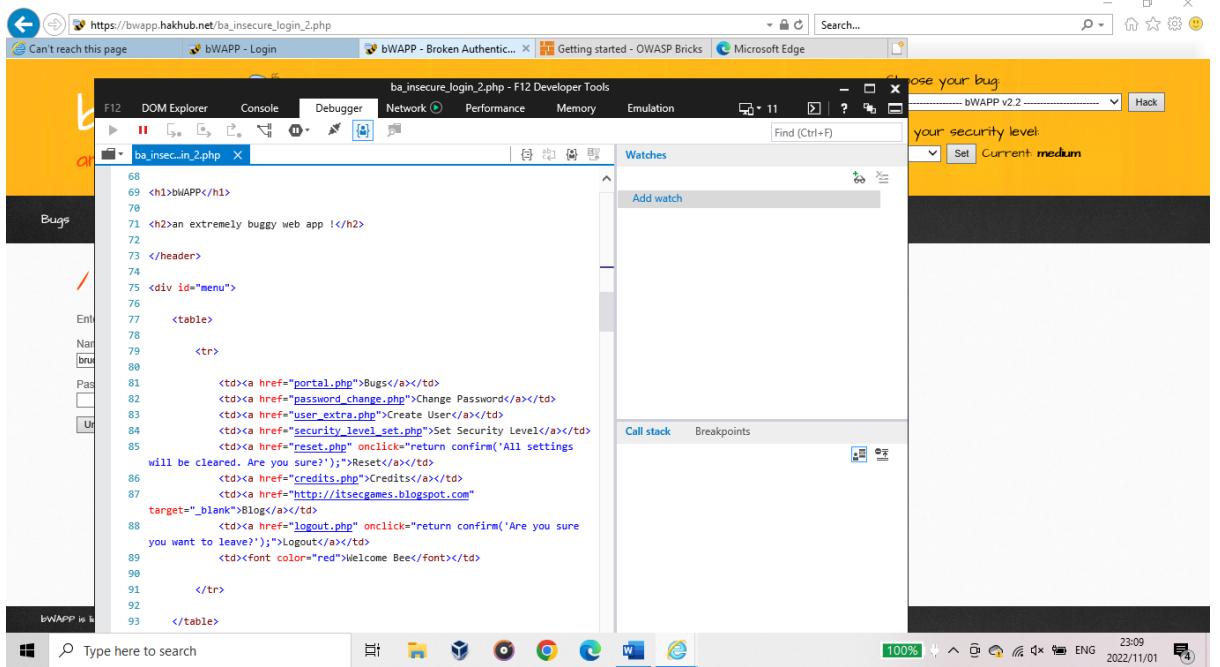
This screenshot is identical to the one above, but the F12 Developer Tools panel is now showing the "Console" tab. The console output pane is empty, indicating no errors or logs have been displayed yet.

ba_insecure_login_2.php - F12 Developer Tools

```
26 var c = bWAPP.charAt(2); var f = bWAPP.charAt(5); var g = bWAPP.charAt(4);
27 var j = bWAPP.charAt(9); var h = bWAPP.charAt(6); var l = bWAPP.charAt(11);
28 var g = bWAPP.charAt(4); var i = bWAPP.charAt(7); var x = bWAPP.charAt(4);
29 var l = bWAPP.charAt(11); var p = bWAPP.charAt(23); var m = bWAPP.charAt(23);
30 var s = bWAPP.charAt(17); var k = bWAPP.charAt(10); var d = bWAPP.charAt(23);
31 var t = bWAPP.charAt(2); var n = bWAPP.charAt(12); var e = bWAPP.charAt(4);
32 var a = bWAPP.charAt(1); var o = bWAPP.charAt(13); var f = bWAPP.charAt(5);
33 var b = bWAPP.charAt(1); var q = bWAPP.charAt(15); var h = bWAPP.charAt(9);
34 var c = bWAPP.charAt(2); var h = bWAPP.charAt(2); var i = bWAPP.charAt(7);
35 var j = bWAPP.charAt(5); var i = bWAPP.charAt(7); var y = bWAPP.charAt(22);
36 var g = bWAPP.charAt(1); var p = bWAPP.charAt(4); var p = bWAPP.charAt(28);
37 var l = bWAPP.charAt(11); var k = bWAPP.charAt(14);
38 var q = bWAPP.charAt(12); var n = bWAPP.charAt(12);
39 var m = bWAPP.charAt(4); var o = bWAPP.charAt(19);
40
41 var secret = (d + "" + j + "" + k + "" + q + "" + x + "" + t + "" + o +
42   "" + g + "" + h + "" + d + "" + p);
43
44 if(document.forms[0].passphrase.value == secret)
45 {
46   // Unlocked
47   location.href="/ba_insecure_login_2.php?secret=" + secret;
48 }
49
50 else
51 {
52   // Locked
53   location.href="/ba_insecure_login_2.php?secret=";
54 }
55
56
57
58
59
60
61 </script>
62
63 </head>
64
65 <body>
66
67 <header>
68
```

ba_insecure_login_2.php - F12 Developer Tools

```
41 var secret = (d + "" + j + "" + k + "" + q + "" + x + "" + t + "" + o +
42   "" + g + "" + h + "" + d + "" + p);
43
44 if(document.forms[0].passphrase.value == secret)
45 {
46   // Unlocked
47   location.href="/ba_insecure_login_2.php?secret=" + secret;
48 }
49
50 else
51 {
52   // Locked
53   location.href="/ba_insecure_login_2.php?secret=";
54 }
55
56
57
58
59
60
61 </script>
62
63 </head>
64
65 <body>
66
67 <header>
68
```



bWAPP
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ 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? :

- Broken Authentication - CAPTCHA Bypassing
- Broken Authentication - Forgotten Function
- Broken Authentication - Insecure Login Forms
- Broken Authentication - Logout Management**
- Broken Authentication - Password Attacks
- Broken Session Management
- Session Management - Administrative Portals
- Session Management - Cookies (HTTPOnly)
- Session Management - Cookies (Secure)



Choose your bug

bWAPP v2.2 Hack

Set your security level

low Set Current: medium



Would you like to store your password for hakhub.net? More info

Yes Not for this site

100% 23:18 ENG 2022/11/01

bWAPP
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Broken Auth - Logout Management /

Click here to logout.



Would you like to store your password for hakhub.net? More info

Yes Not for this site

100% 23:19 ENG 2022/11/01

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

NATIONAL CENTER FOR
MISSING &
EXPLOITED
CHILDREN

MME
Security Audits & Training

Scan your website for XSS and SQL Injection vulnerabilities

Twitter LinkedIn Facebook Email

bWAPP is licensed under MIT Would you like to store your password for hakhub.net? More info Yes Not for this site



bWAPP
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ 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

- /AI - 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)

NATIONAL CENTER FOR
MISSING &
EXPLOITED
CHILDREN

Twitter LinkedIn Facebook Email

bWAPP is licensed under MIT Would you like to store your password for hakhub.net? More info Yes Not for this site

Task 2 view session id in url

The screenshot shows the bWAPP Portal page. At the top right, there are links for "Choose your bug" (set to bWAPP v2.2), "Set your security level" (set to medium), and social sharing icons for Twitter, LinkedIn, Facebook, and Email. Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. A sub-navigation bar below it says "/ Portal /". On the left, there's a sidebar with a dropdown menu listing various bugs: Broken Authentication - Logout Management, Broken Authentication - Password Attacks, Broken Authentication - Weak Passwords, Session Management - Administrative Portals, Session Management - Cookies (HTTPOnly), Session Management - Session ID in URL (selected), and Session Management - Strong Sessions. At the bottom of this sidebar is a "Hack" button. To the right of the sidebar are three circular icons: a blue one with a lightning bolt, a black one with a lightning bolt, and an orange one with a stylized logo. Below these icons is a logo for "NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN".

A screenshot of a browser window showing a prompt: "Would you like to store your password for hakhub.net? More info". There are "Yes" and "Not for this site" buttons. The browser interface includes a search bar, a ribbon with various icons, and status information at the bottom right.

The screenshot shows the bWAPP Session Management - Session ID in URL page. The layout is identical to the Portal page, with the same header, sidebar, and footer. The main content area displays the title "/ Session Mgmt. - Session ID in URL /" and the sub-instruction "Session IDs should never be exposed in the URL".

A screenshot of a browser window showing a prompt: "Would you like to store your password for hakhub.net? More info". There are "Yes" and "Not for this site" buttons. The browser interface includes a search bar, a ribbon with various icons, and status information at the bottom right.

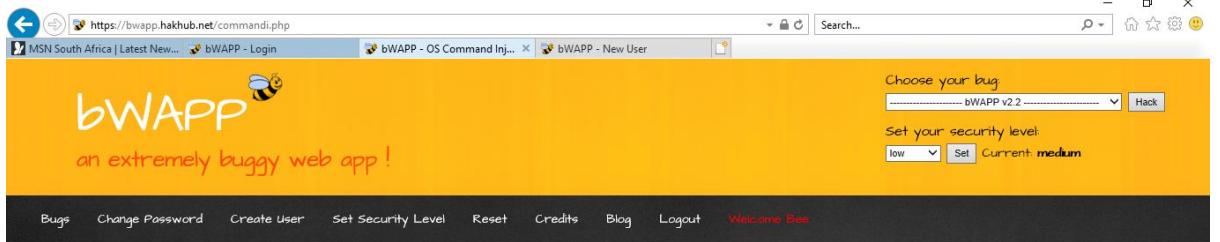
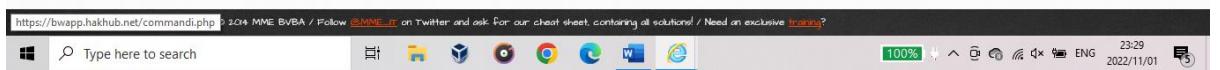
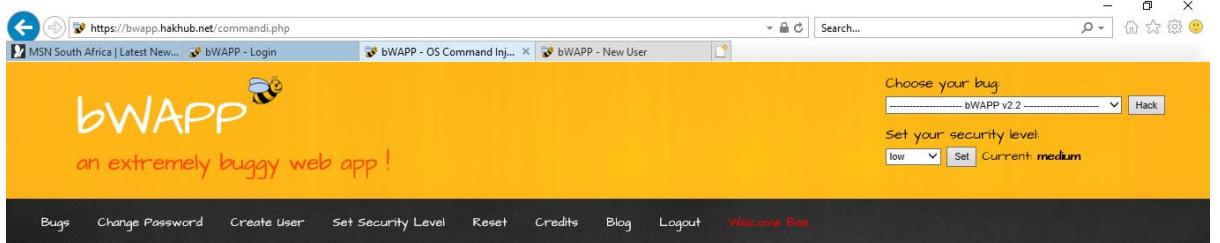
Task 3 conduct os command injection attack

The screenshot shows the bWAPP Portal page. At the top right, there are links for "Choose your bug" (set to bWAPP v2.2), "Set your security level" (set to medium), and social sharing icons for Twitter, LinkedIn, Facebook, and Email. Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. A sub-navigation bar below it has links: /Portal/ (highlighted in orange), /OS Command Injection/, /File Upload/, /SQL Injection/, /XSS (Cross Site Scripting)/, /CSRF (Cross Site Request Forgery)/, /LDAP Injection (Search)/, /Mail Header Injection (SMTP)/, OS Command Injection (highlighted in blue), and OS Command Injection - Blind. A "Hack" button is at the bottom of this list. The main content area features the bWAPP logo and the tagline "an extremely buggy web app!".

A password storage dialog box from Microsoft Edge is shown. It asks, "Would you like to store your password for hakhub.net?". There are "Yes" and "Not for this site" buttons. The URL https://bwapp.hakhub.net/portal.php is visible in the address bar. The system tray shows battery level, signal strength, and the date/time 23:28 2022/11/01.

The screenshot shows the bWAPP OS Command Injection page. The layout is identical to the Portal page, with the same header, navigation, and footer. The main content area now displays the title "/ OS Command Injection /". Below it is a "DNS lookup" input field containing "www.nsa.gov" and a "Lookup" button.

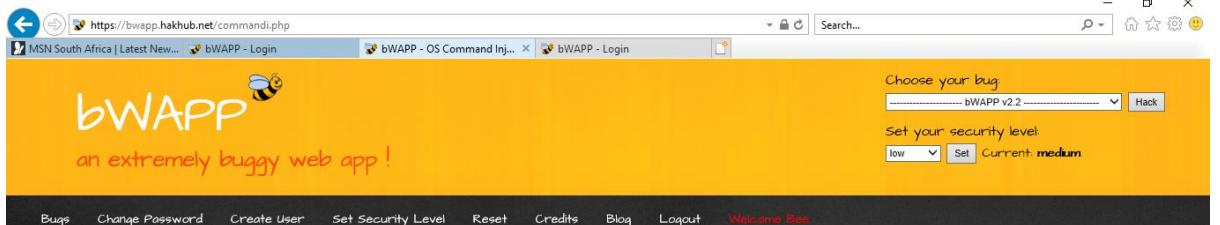
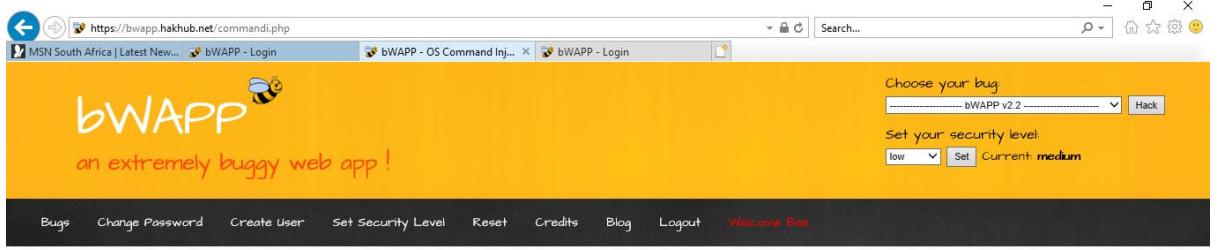
The screenshot shows the bottom of the bWAPP page and the Windows taskbar. The footer contains a license notice: "bWAPP is licensed under AGPLv3+ © 2014 MME BVBA / Follow @MME_BVBA on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive training?". The taskbar shows the Start button, pinned icons for File Explorer, Task View, File History, Task Scheduler, Task Manager, and Edge, and the system tray with battery level, signal strength, and the date/time 23:28 2022/11/01.

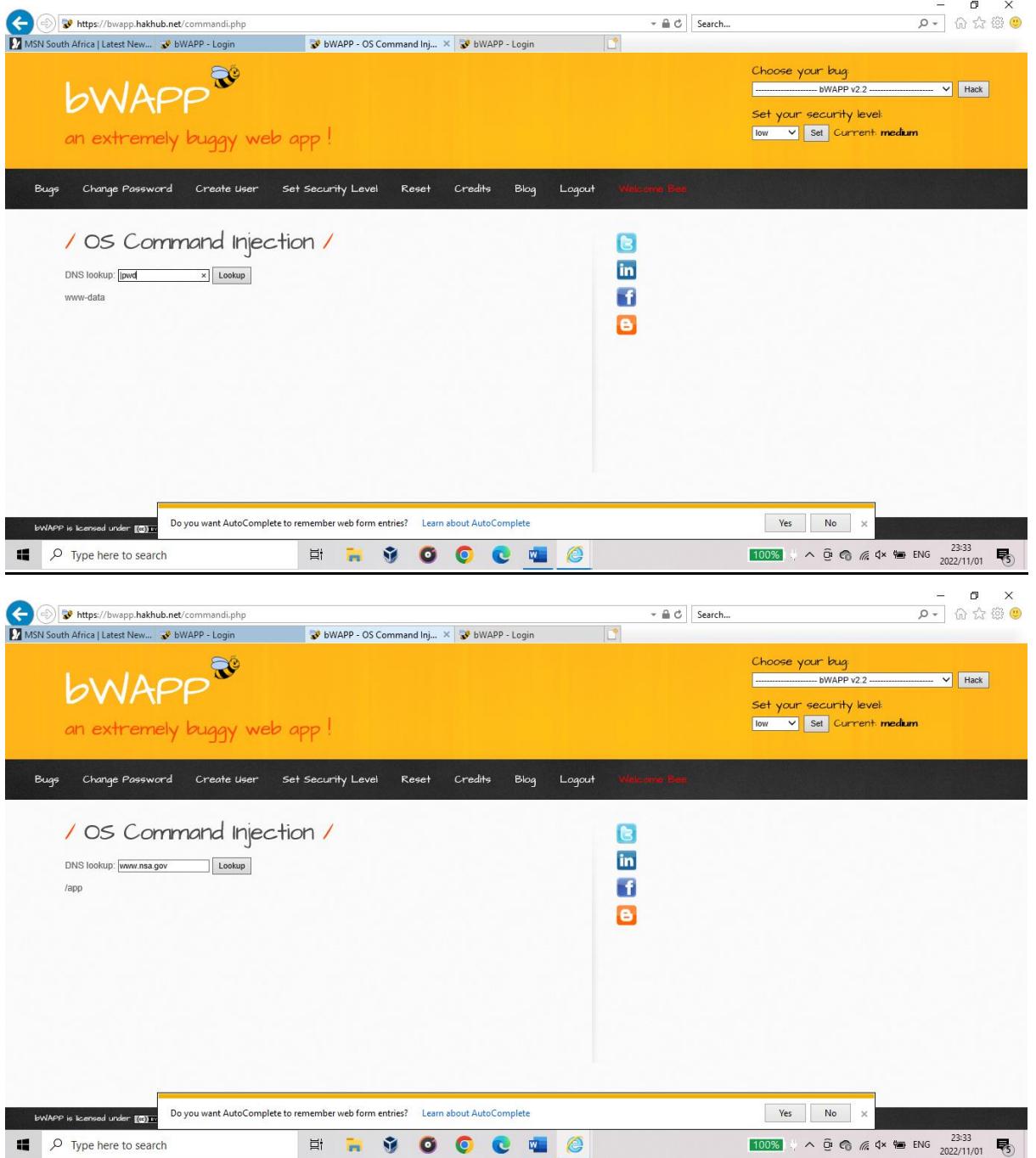


The screenshot shows the bWAPP OS Command Injection page. At the top, there's a navigation bar with links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. A dropdown menu titled "Choose your bug" is set to "bWAPP v2.2" with the "Hack" option selected. Below this, a "Set your security level" dropdown is set to "low". The main content area has a yellow header with the bWAPP logo and the text "an extremely buggy web app!". Below the header, a section titled "/ OS Command Injection /" contains a "DNS lookup" input field with "inet user" and a "Lookup" button. The URL in the address bar is https://bwapp.hakhub.net/commands.php.

The screenshot shows the bWAPP Portal page. It features a similar layout to the OS Command Injection page, with a yellow header and a "Choose your bug" dropdown set to "bWAPP v2.2" with "Hack" selected. The main content area has a yellow header with the bWAPP logo and the text "an extremely buggy web app!". Below the header, a section titled "/ Portal /" contains a dropdown menu listing various bugs: 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), and OS Command Injection. The "OS Command Injection" option is highlighted. To the right of the dropdown is a logo for the National Center for Missing & Exploited Children. The URL in the address bar is https://bwapp.hakhub.net/portal.php.

At the bottom of the page, there's a footer note: "bWAPP is licensed under [MIT](#). © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive training?". The system tray at the bottom right shows the date as 2022/11/01 and the time as 23:30.





The screenshot shows a Microsoft Edge browser window displaying the bWAPP OS Command Injection page. The URL in the address bar is <https://bwapp.hakhub.net/commandi.php>. The page title is "bWAPP - OS Command Inj...". The main content area displays the result of a command injection exploit:

```
cat /etc/passwd
```

The exploit was successful, as evidenced by the output of the command being displayed on the page.

At the bottom of the browser window, there is a message: "Do you want AutoComplete to remember web form entries? Learn about AutoComplete". Below the browser window, the Windows taskbar is visible, showing the Start button, search bar, and pinned icons for File Explorer, File History, Task View, Mail, Photos, OneDrive, Edge, and File Explorer.

Task 4 perform server-side includes injection attack(SSI)

The screenshot shows the bWAPP homepage with a yellow header. The header includes a logo of a bee, the text "an extremely buggy web app!", and a sidebar with options to "Choose your bug" (set to bWAPP v2.2), "Set your security level" (set to medium), and social sharing links for Twitter, LinkedIn, Facebook, and Email.

/ 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? :

- HTML Injection - Stored (Blog)
- iFrame Injection
- LDAP Injection (Search)
- Mail Header Injection (SMTP)
- OS Command Injection
- OS Command Injection - Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection (GET/Search)

[Hack](#)



NATIONAL CENTER FOR
MISSING &
EXPLOITED
CHILDREN



The screenshot shows the browser status bar with the URL https://bwapp.hakhub.net/portal.php. It also displays system information such as battery level, signal strength, and the date and time (23:40, 2022/11/01).

The screenshot shows the bWAPP homepage with a yellow header. The header includes a logo of a bee, the text "an extremely buggy web app!", and a sidebar with options to "Choose your bug" (set to bWAPP v2.2), "Set your security level" (set to medium), and social sharing links for Twitter, LinkedIn, Facebook, and Email.

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (bee-box only)

First name:

`<alert("Hacked")></script>`

Last name:

[Lookup](#)



The screenshot shows the browser status bar with the URL https://bwapp.hakhub.net/ssii.php. It also displays system information such as battery level, signal strength, and the date and time (23:41, 2022/11/01).

Choose your bug
bWAPP v2.2 Hack

Set your security level
low Set Current: medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (bee-box only)

First name:

Last name:

Lookup

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#)

Yes No

Type here to search

100% ENG 23:42 2022/11/01

Choose your bug
bWAPP v2.2 Hack

Set your security level
low Set Current: medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (bee-box only)

First name:

Last name:

Lookup

Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#)

Yes No

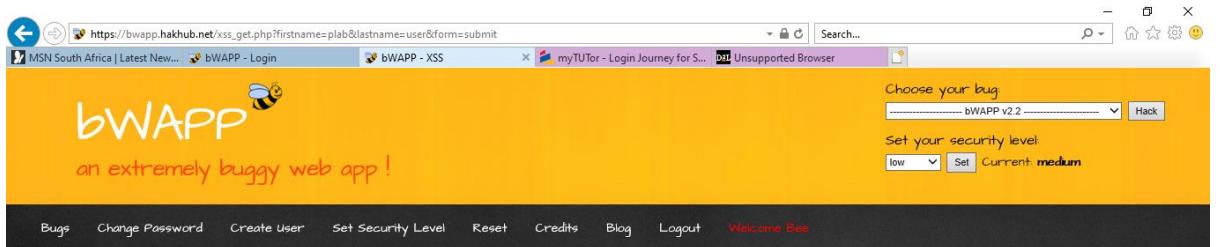
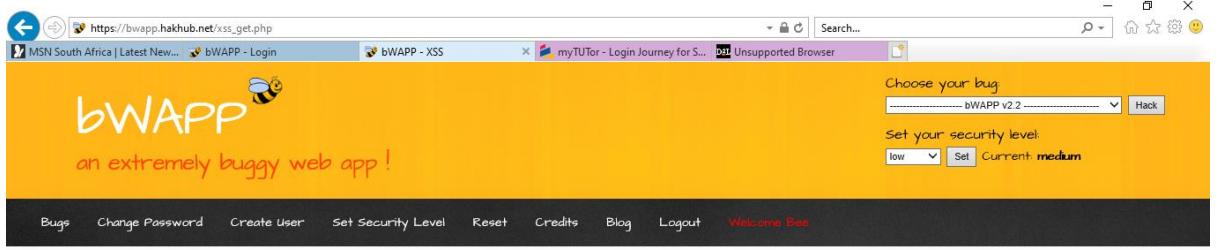
Type here to search

100% ENG 23:43 2022/11/01

The screenshot shows the bWAPP web application interface. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. On the right side of the header, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. Below the header, a yellow banner reads 'Choose your bug' with a dropdown set to 'bWAPP v2.2' and a 'Hack' button. It also has a 'Set your security level' dropdown set to 'low' and a 'Set' button. The main content area has a title 'Server-Side Includes (SSI) Injection /'. Below it, a form asks 'What is your IP address? Lookup your IP address... (bee-box only)'. The form fields include 'First name:' with 'Document name' selected, 'Last name:' with 'user' entered, and a 'Lookup' button. A status message at the bottom of the page says 'bWAPP is licensed under [GPL]'. A Windows taskbar at the bottom shows various pinned icons and the date/time as 23:44 2022/11/01.

Task 5 Perform cross-site Scripting Attack

The screenshot shows the bWAPP web application interface. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. On the right side of the header, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. Below the header, a yellow banner reads 'Choose your bug' with a dropdown set to 'bWAPP v2.2' and a 'Hack' button. It also has a 'Set your security level' dropdown set to 'low' and a 'Set' button. The main content area has a title 'Portal /'. Below it, a paragraph about bWAPP and a dropdown menu for selecting a bug to hack. The dropdown menu is open, showing items like 'Session Management - Cookies (HTTPOnly)', 'Session Management - Cookies (Secure)', 'Session Management - Session ID in URL', 'Session Management - Strong Sessions', and 'A3 - Cross-Site Scripting (XSS) /'. The 'Cross-Site Scripting - Reflected (GET)' item is highlighted with a blue background. To the right of the dropdown, there are three icons: a blue globe, a lightning bolt, and a red square with a white 'M'. A watermark for 'NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN' is visible. A status message at the bottom of the page says 'bWAPP is licensed under [GPL]'. A Windows taskbar at the bottom shows various pinned icons and the date/time as 23:55 2022/11/01.



The screenshot shows the bWAPP XSS page. At the top, there's a navigation bar with links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. On the right, there are social sharing icons for Twitter, LinkedIn, Facebook, and Email. A dropdown menu says "Choose your bug" set to "bWAPP v2.2" and "Hack". Below that, it says "Set your security level" with "low" selected and "Set" and "Current: medium" buttons. The main content area has a yellow header with the bWAPP logo and the text "an extremely buggy web app!". Below this, a form asks for first and last names. The "First name" field contains the JavaScript payload `alert('Hacked'))</script>`. The "Last name" field contains "user". A "Go" button is present. The response shows the user "Welcome plab user".



The screenshot shows the bWAPP Portal page. It has the same navigation bar as the XSS page. The main content area has a yellow header with the bWAPP logo and the text "an extremely buggy web app!". Below this, a dropdown menu says "Choose your bug" set to "bWAPP v2.2" and "Hack". It also says "Set your security level" with "low" selected and "Set" and "Current: medium" buttons. The "Portal" section is visible. On the right, there are social sharing icons for Twitter, LinkedIn, Facebook, and Email. The bottom of the page features a sidebar with various exploit categories and a "Hack" button.



The screenshot shows a web browser window with the URL https://bwapp.haklu.net/xss_stored_1.php. The page title is "bWAPP - XSS". The main content area displays a blog entry form with the heading "/ XSS - Stored (Blog) /". Below the heading is a text input field with a dropdown menu. To the right of the input field are buttons for "Submit", "Add: ", "Show all: ", and "Delete: ". Below these buttons is a table header row with columns labeled "#", "Owner", "Date", and "Entry". On the right side of the page, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. At the top right, there are dropdown menus for "Choose your bug" (set to "bWAPP v2.2") and "Set security level" (set to "medium"). The bottom of the page includes a footer with copyright information and a system tray showing battery level, signal strength, and date/time.

Task 6 Perform cross-site scripting(Xss)-Reflected(HREF)Attack

The screenshot shows the main landing page of bWAPP. At the top right, there are browser control buttons and a search bar. Below the header, there's a yellow banner with the text "Choose your bug" and "Set your security level". A sidebar on the right contains social media icons for Twitter, LinkedIn, Facebook, and Email. The main content area features the bWAPP logo and the tagline "an extremely buggy web app!". A navigation menu at the bottom includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee".

/ 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? :

- Cross-Site Scripting - Reflected (Back Button)
- Cross-Site Scripting - Reflected (Custom Header)
- Cross-Site Scripting - Reflected (Eval)
- Cross-Site Scripting - Reflected (HREF)**
- Cross-Site Scripting - Reflected (Local Form)
- Cross-Site Scripting - Reflected (Path/Admin)
- Cross-Site Scripting - Reflected (PHP_SELF)
- Cross-Site Scripting - Reflected (Referer)
- Cross-Site Scripting - Reflected (User-Agent)

Hack



This screenshot shows the Windows taskbar with the URL "https://bwapp.hakhub.net/portal.php" visible. The taskbar also displays icons for various applications and system status information like battery level and network connection.

The screenshot shows the bWAPP homepage again, but this time the "XSS - Reflected (HREF)" option is highlighted in the dropdown menu. The rest of the interface is identical to the first screenshot.

/ XSS - Reflected (HREF) /

In order to vote for your favorite movie, your name must be entered:

This screenshot shows the Windows taskbar with the URL "https://bwapp.hakhub.net/xss_href-1.php" visible. The taskbar also displays icons for various applications and system status information like battery level and network connection.

https://bwapp.hakhub.net/xss_href-2.php?name=PLAB&action=vote

MSN South Africa | Latest News... bWAPP - Login bWAPP - XSS myTUTOR - Login Journey for S... Unsupported Browser

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ XSS - Reflected (HREF) /

Hello PLAB, please vote for your favorite movie.

Remember, Tony Stark wants to win every time...

Title	Release	Character	Genre	Vote
G.I. Joe: Retaliation	2013	Cobra Commander	action	Vote
Iron Man	2008	Tony Stark	action	Vote
Man of Steel	2013	Clark Kent	action	Vote
Terminator Salvation	2009	John Connor	sci-fi	Vote
The Amazing Spider-Man	2012	Peter Parker	action	Vote
The Cabin in the Woods	2011	Some zombies	horror	Vote
The Dark Knight Rises	2012	Bruce Wayne	action	Vote
The Fast and the Furious	2001	Brian O'Connor	action	Vote
The Incredible Hulk	2008	Bruce Banner	action	Vote
World War Z	2013	Gerry Lane	horror	Vote

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME_BVBA](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [trojan](#)?

100% 00:05 ENG 2022/11/02

https://bwapp.hakhub.net/xss_href-1.php

MSN South Africa | Latest News... bWAPP - Login bWAPP - XSS myTUTOR - Login Journey for S... Unsupported Browser

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

Choose your bug:

bWAPP v2.2 Hack

an extremely buggy web app!

In order to vote for your favorite movie, your name must be entered:

Continue

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME_BVBA](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [trojan](#)?

100% 00:06 ENG 2022/11/02

https://bwapp.hakhub.net/xss_href-2.php?name=%3E%3Cscript%3Ealert(%281%29%3C%2Fscript%3E%3C&action=vote

MSN South Africa | Latest News... bWAPP - Login bWAPP - XSS myiTutor - Login Journey for S... Unsupported Browser

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ XSS - Reflected (HREF) /

Hello ><script>alert(1)</script>, please vote for your favorite movie.

Remember, Tony Stark wants to win every time...

Title	Release	Character	Genre	Vote
G.I. Joe: Retaliation	2013	Cobra Commander	action	Vote
Iron Man	2008	Tony Stark	action	Vote
Man of Steel	2013	Clark Kent	action	Vote
Terminator Salvation	2009	John Connor	sci-fi	Vote
The Amazing Spider-Man	2012	Peter Parker	action	Vote
The Cabin in the Woods	2011	Some zombies	horror	Vote
The Dark Knight Rises	2012	Bruce Wayne	action	Vote
The Fast and the Furious	2001	Brian O'Connor	action	Vote
The Incredible Hulk	2008	Bruce Banner	action	Vote
World War Z	2013	Gerry Lane	horror	Vote

bWAPP is licensed under [MIT](#). Do you want AutoComplete to remember web form entries? [Learn about AutoComplete](#)

Yes No X

Type here to search

100% 00:07 2022/11/02 ENG