Student  Number:220966950

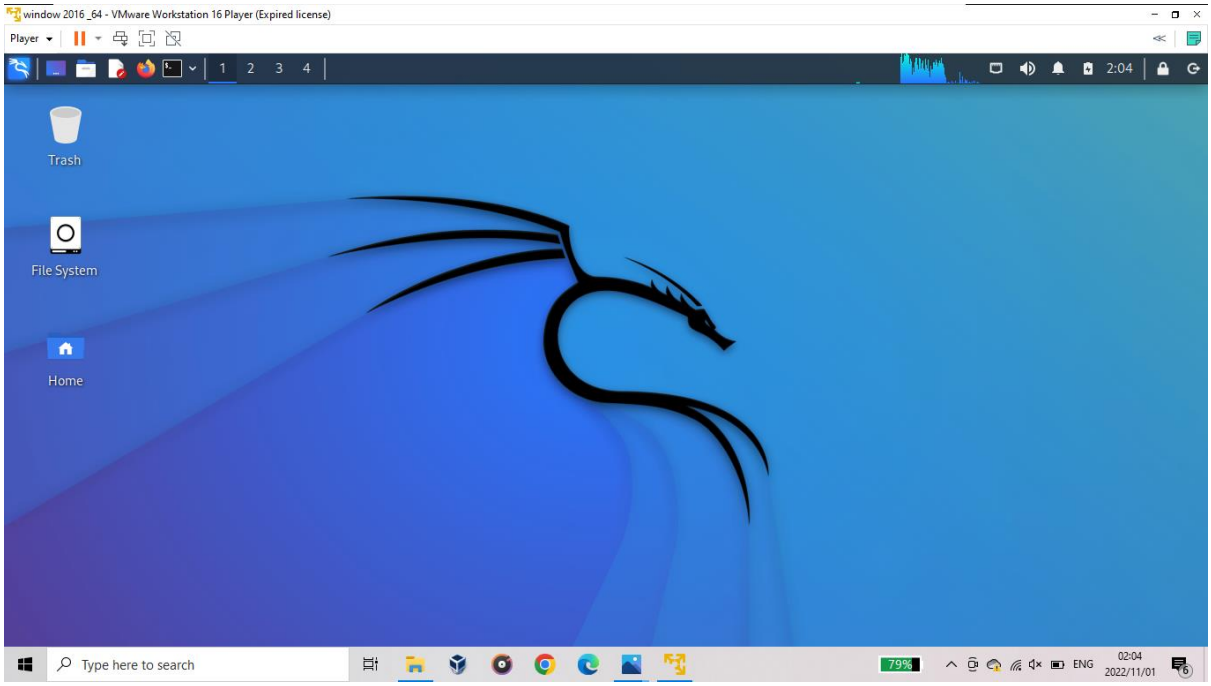
Name: Juliet

Surname:Ngoni

Exercise 1

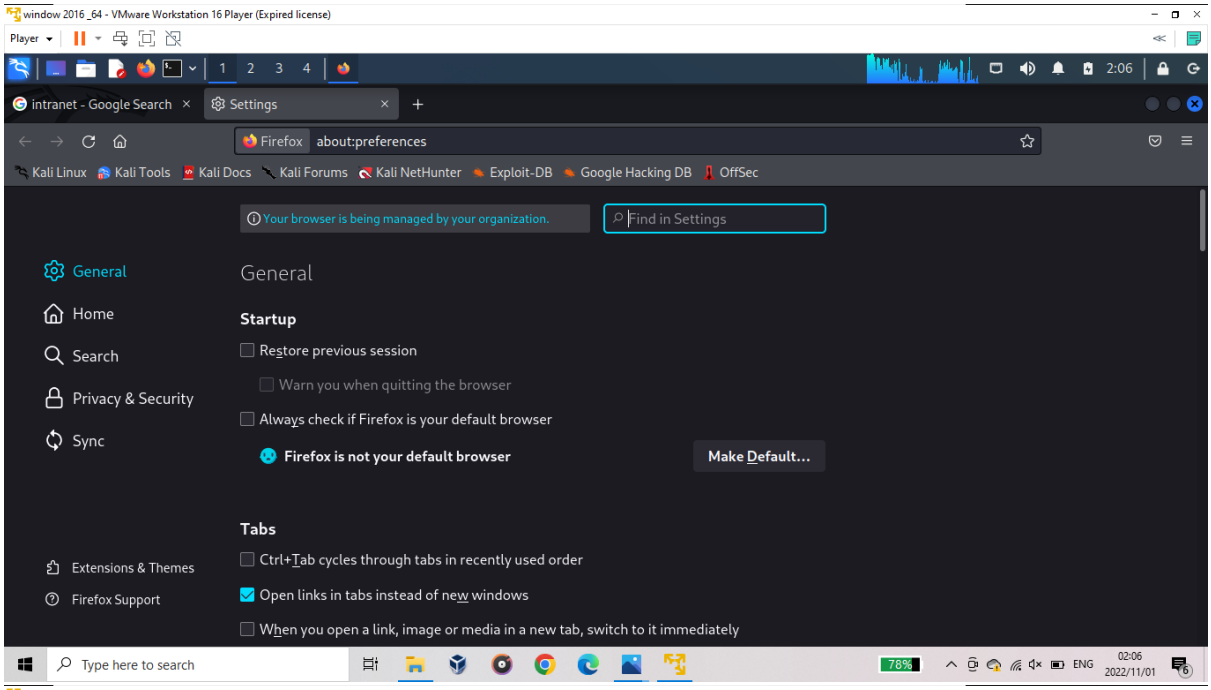
Web Application Password Cracking

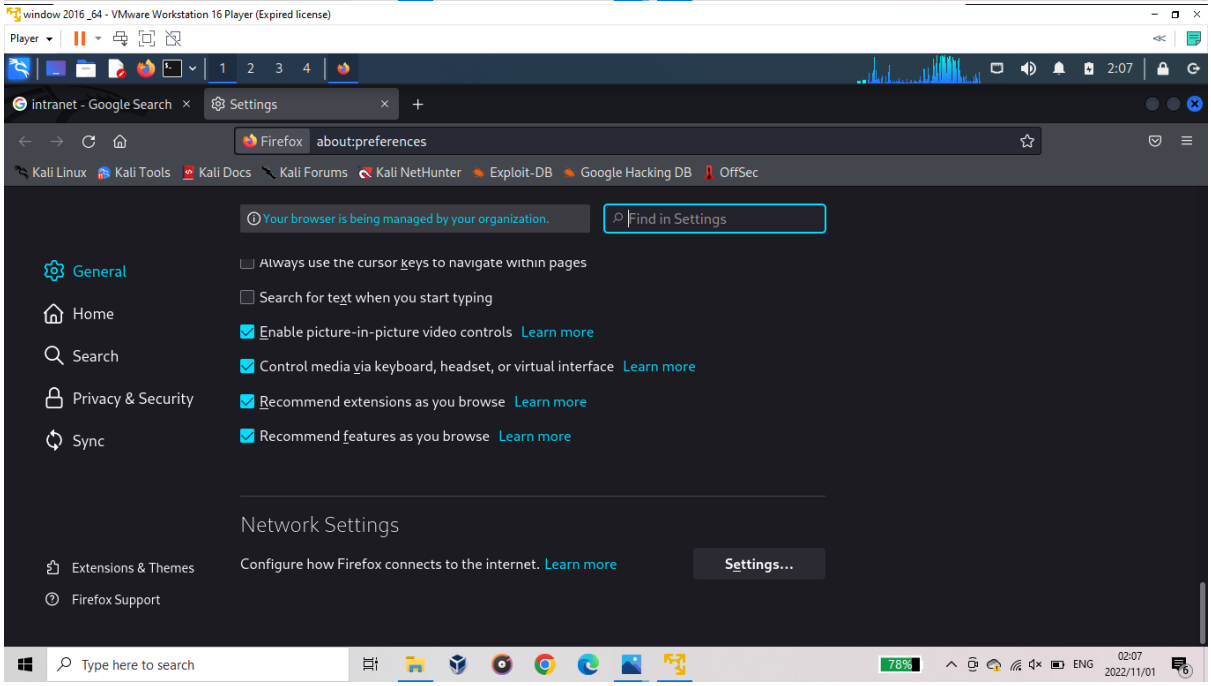
1.Desktop showing firefox and other applications.

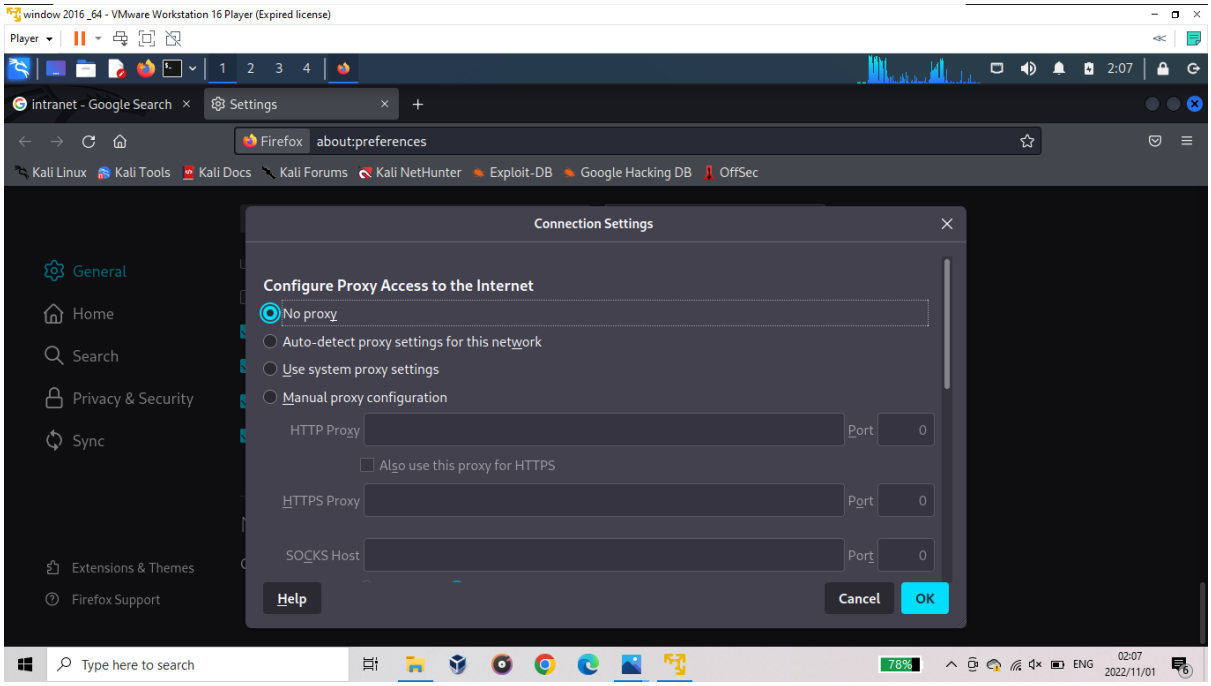



2.Click menu icon at the top right and then click Preferences, Network proxy and click settings

Select no proxy.


window 2016 _64 - VMware Workstation 16 Player (Expired license)
Player
2:06
intranet - Google Search
Settings
Firefox
about:preferences
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
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
Type here to search
78%
ENG
02:06
2022/11/01


window 2016 _64 - VMware Workstation 16 Player (Expired license)
Player
2:07
intranet - Google Search
Settings
Firefox
about:preferences
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Always use the cursor keys to navigate within pages
Search for text when you start typing
Enable picture-in-picture video controls Learn more
Control media via keyboard, headset, or virtual interface Learn more
Recommend extensions as you browse Learn more
Recommend features as you browse Learn more
Network Settings
Configure how Firefox connects to the internet. Learn more
Settings...
Type here to search
78%
ENG
02:07
2022/11/01



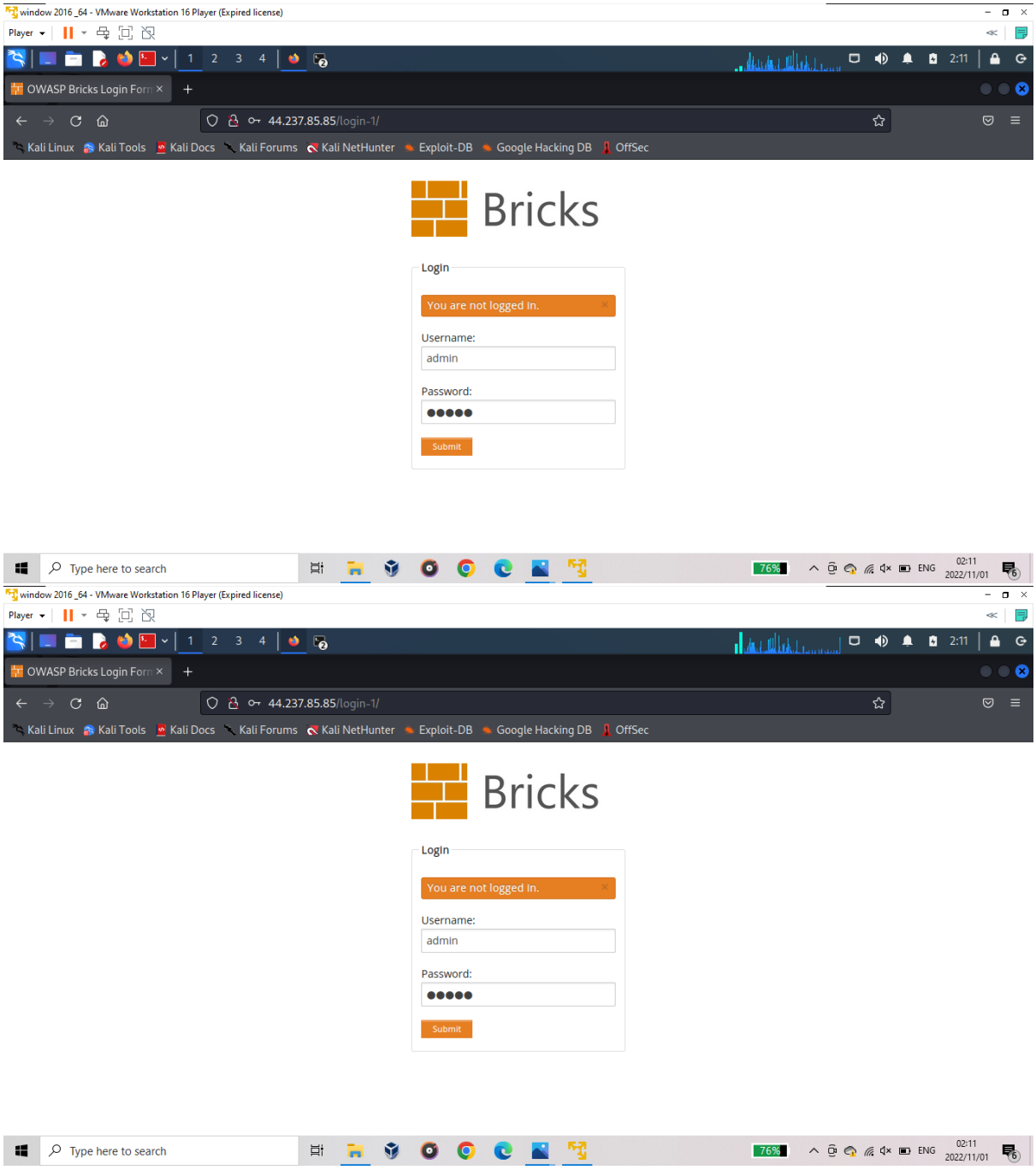

On the kali terminal enter command ettercap -T grep password to ;grab the password

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.

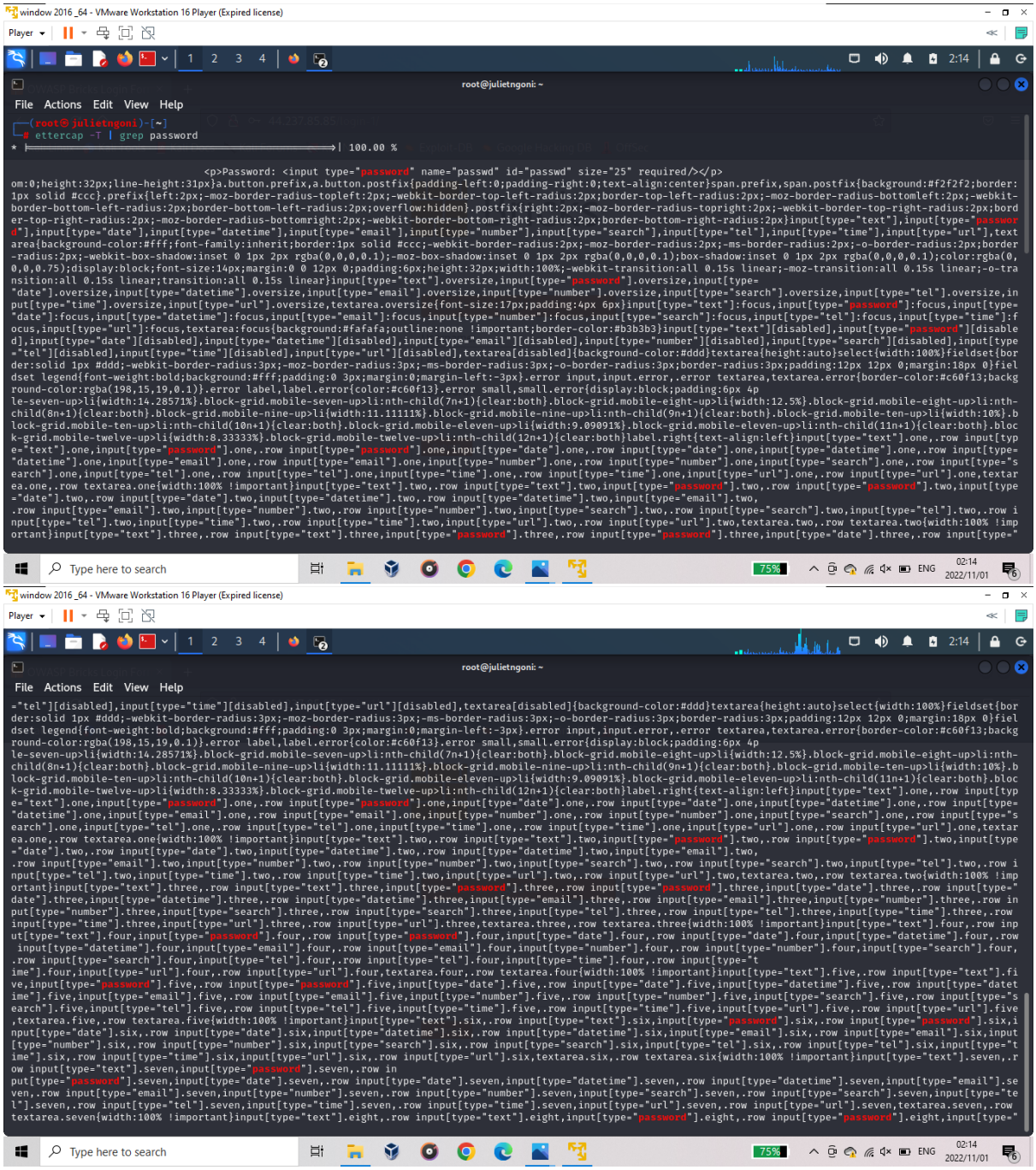
OWASP Bricks is the same as the BWAPP(Buggy Web Application) ,they work the same as Bwapp helps with security ,developers and student to discover and prevent web vulnerabilities and to prepare one to conduct successful penetration testing and ethical hacking projects .bwapp also have over 100 web bugs 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.




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

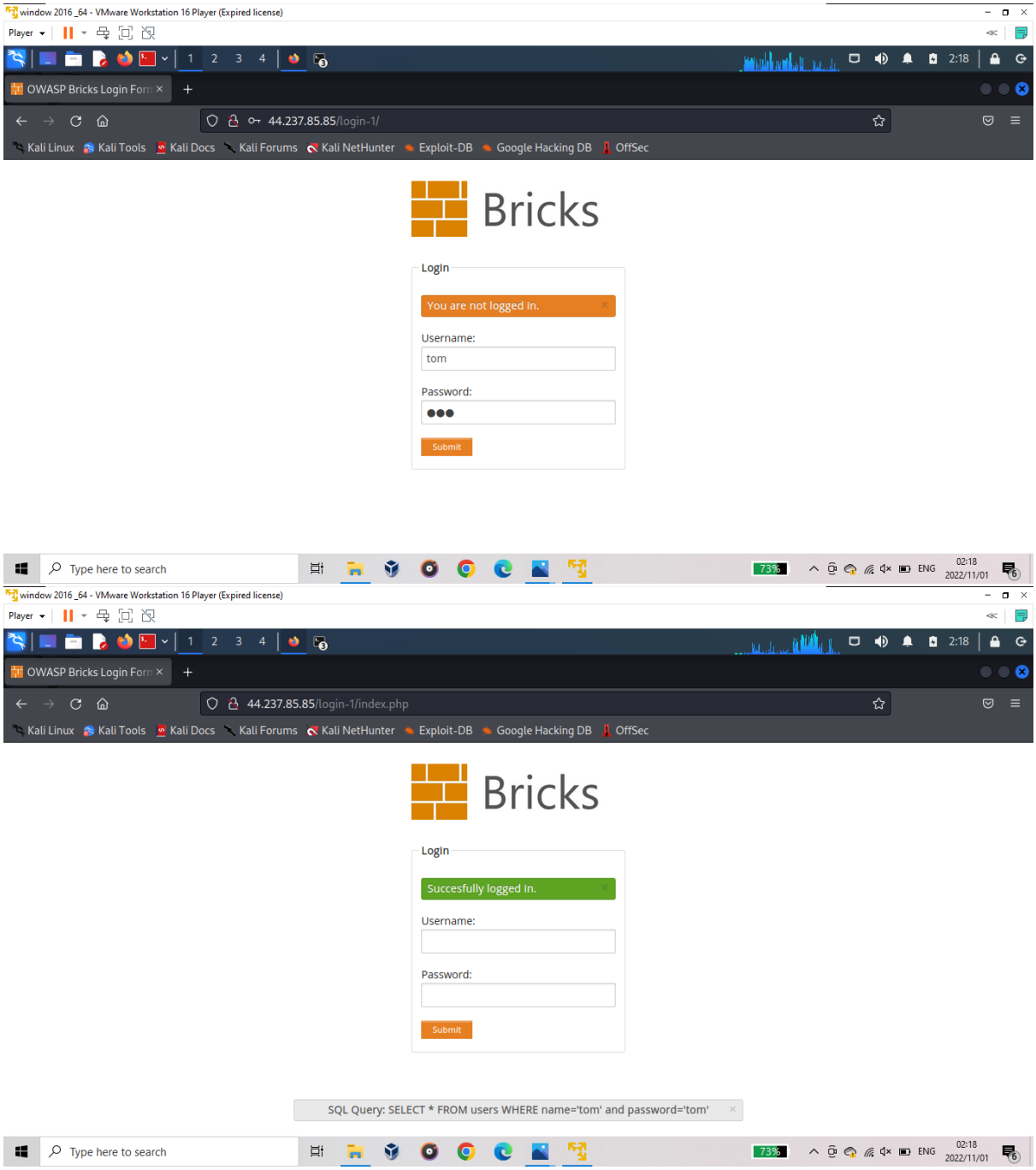
I first used the credentials admin adminand the result were the following



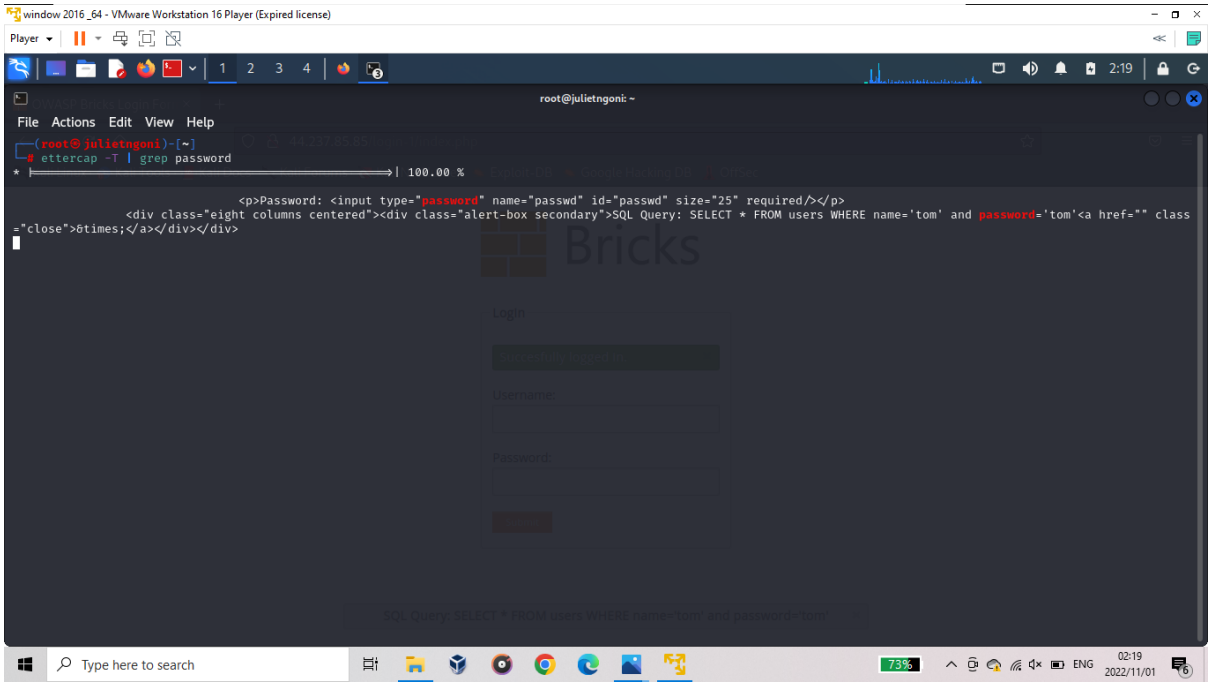




Then I used the credentials tom tom then the results are the following bshowing that the name as username is tom and the password is also tom.

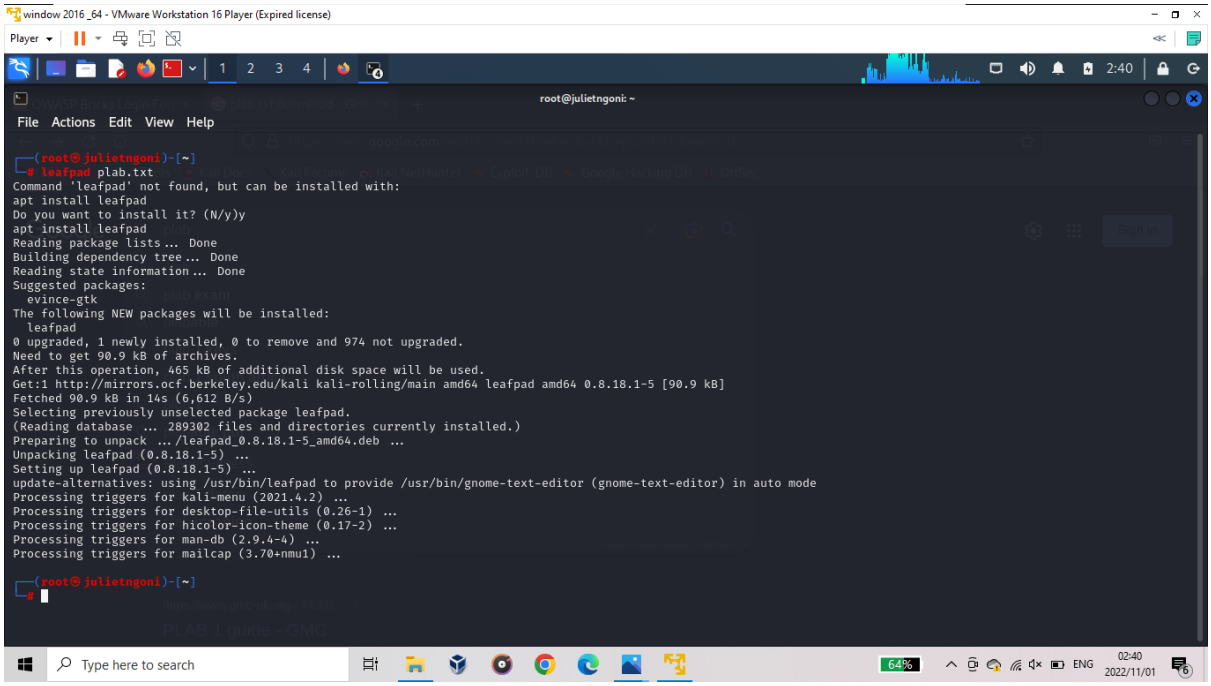

window 2016 _64 - VMware Workstation 16 Player (Expired license)
Player
OWASP Bricks Login Form
44.237.85.85/login-1/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Bricks
Login
You are not logged in.
Username:
tom
Password:
Submit


Type here to search
window 2016 _64 - VMware Workstation 16 Player (Expired license)
Player
OWASP Bricks Login Form
44.237.85.85/login-1/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Bricks
Login
Succesfully logged in.
Username:
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='tom' and password='tom'
Type here to search



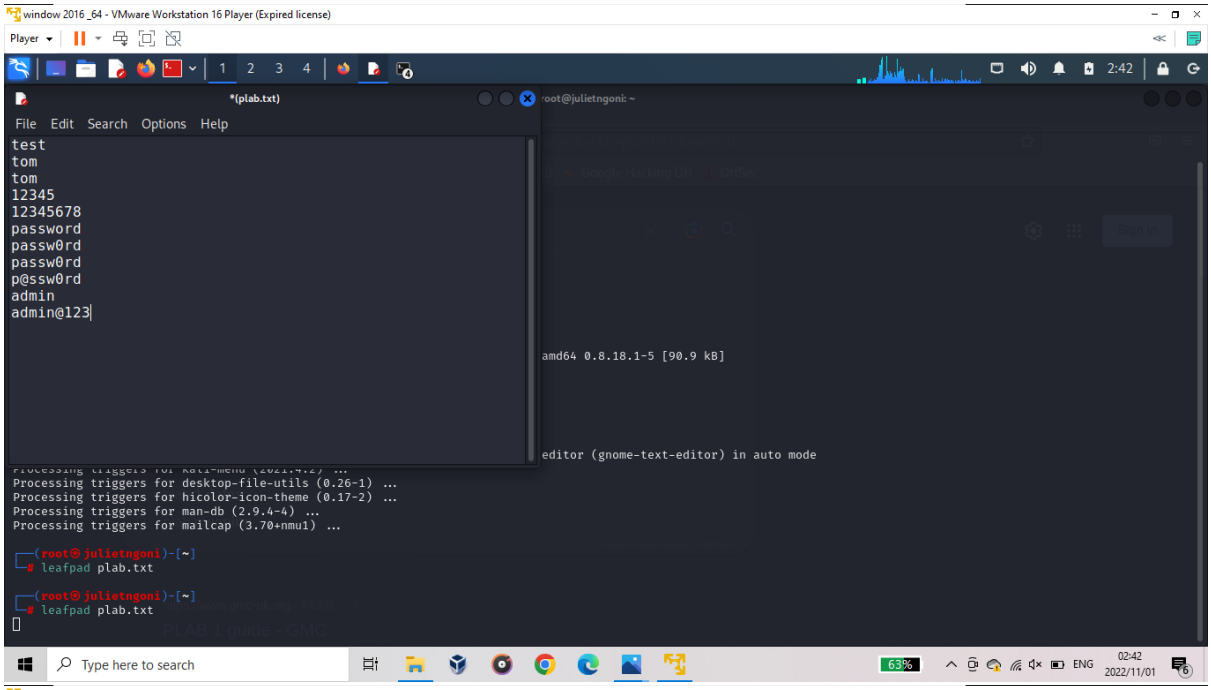

Task 2 : using medusa to crack the password.

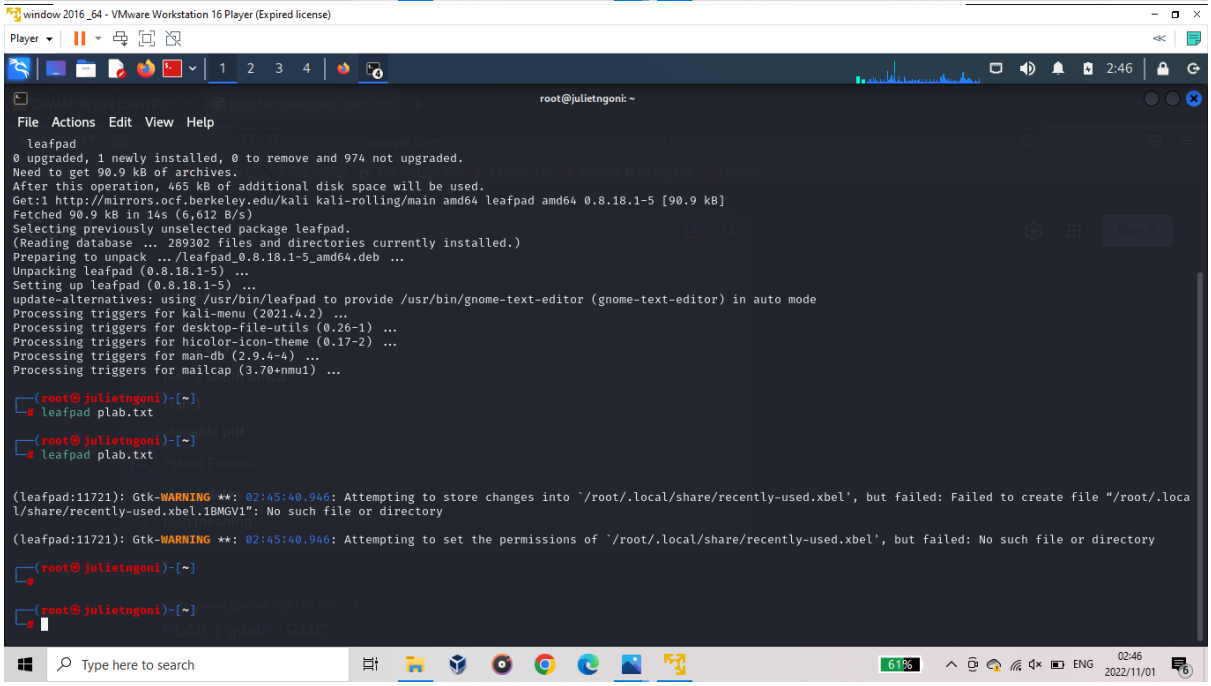
Install leafpad since my version of kali  does not have the leafpad

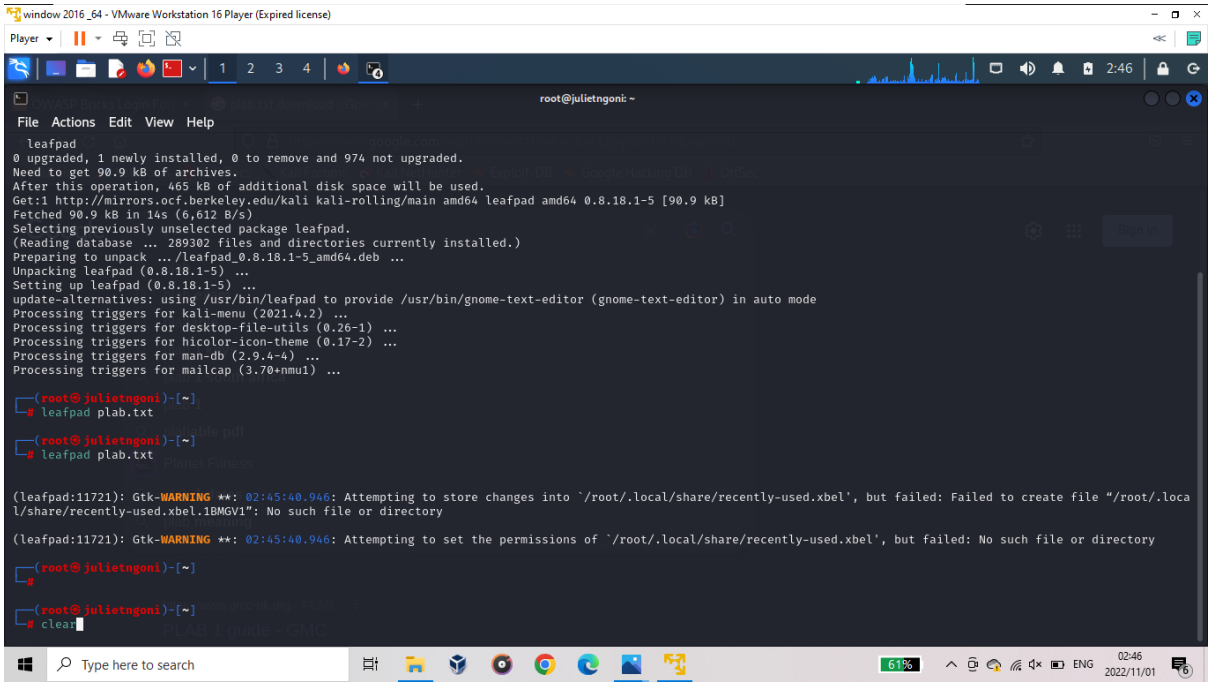



After downloading enter the command leafpad plab.txt.

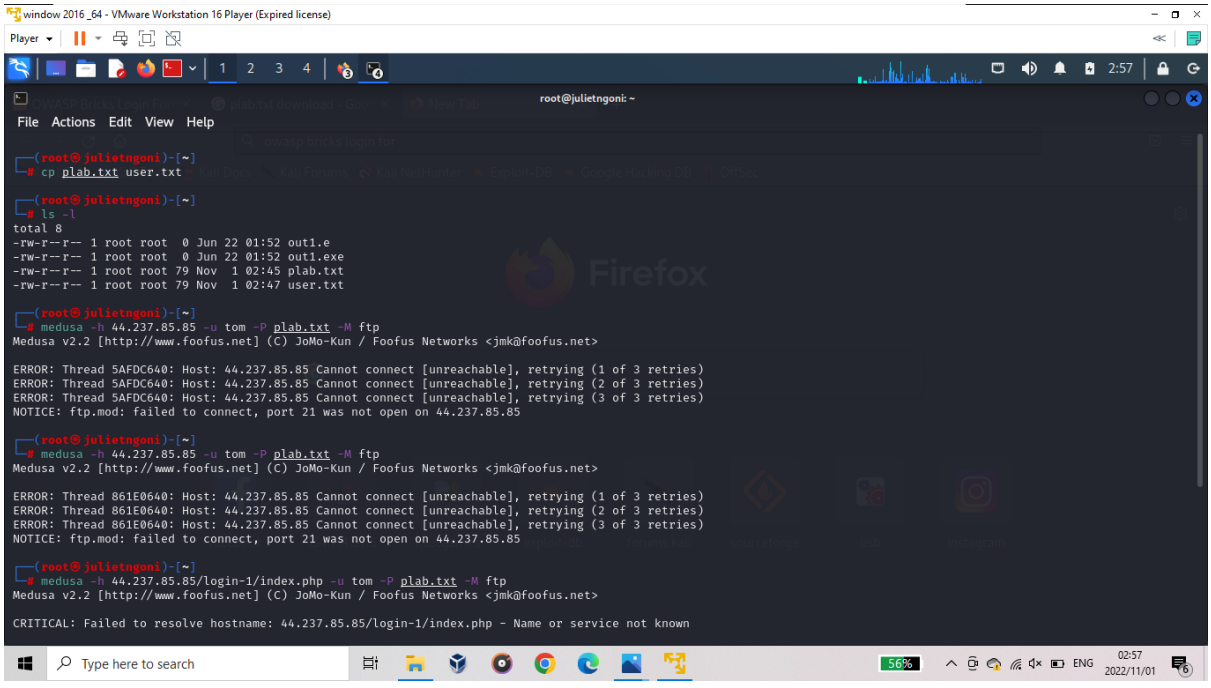
And it will show the blank space for the leafpad file text and ente rvarious different password(edit). Then after save as plab.txt.



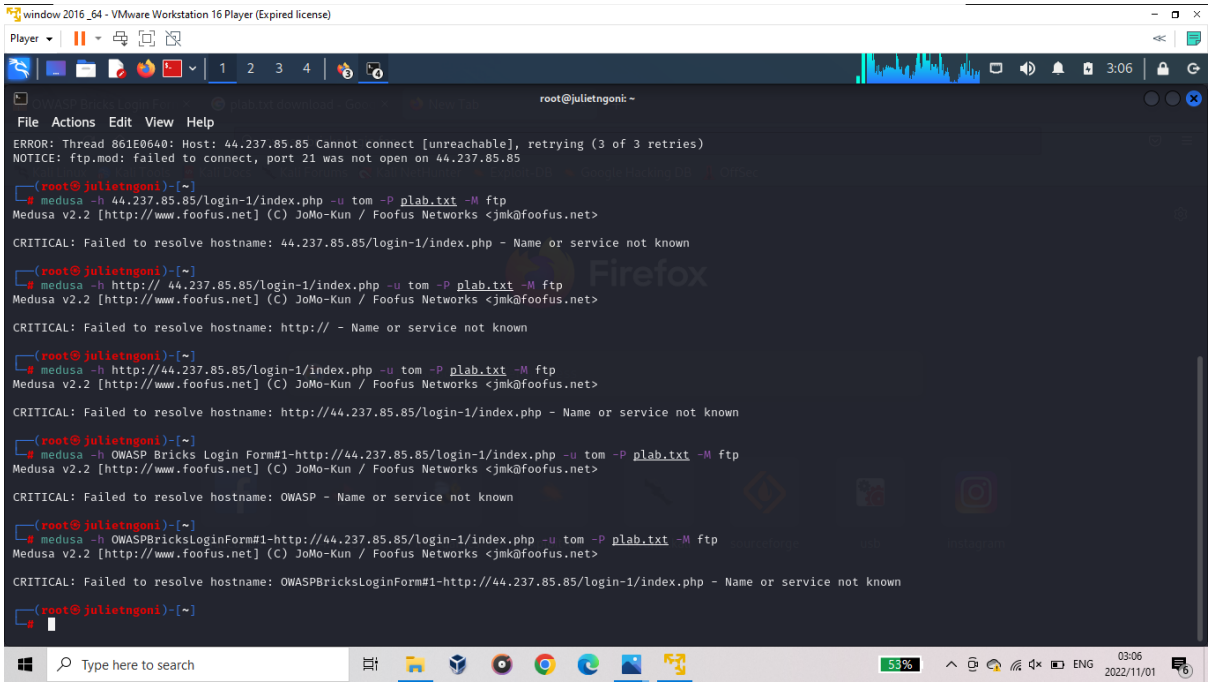


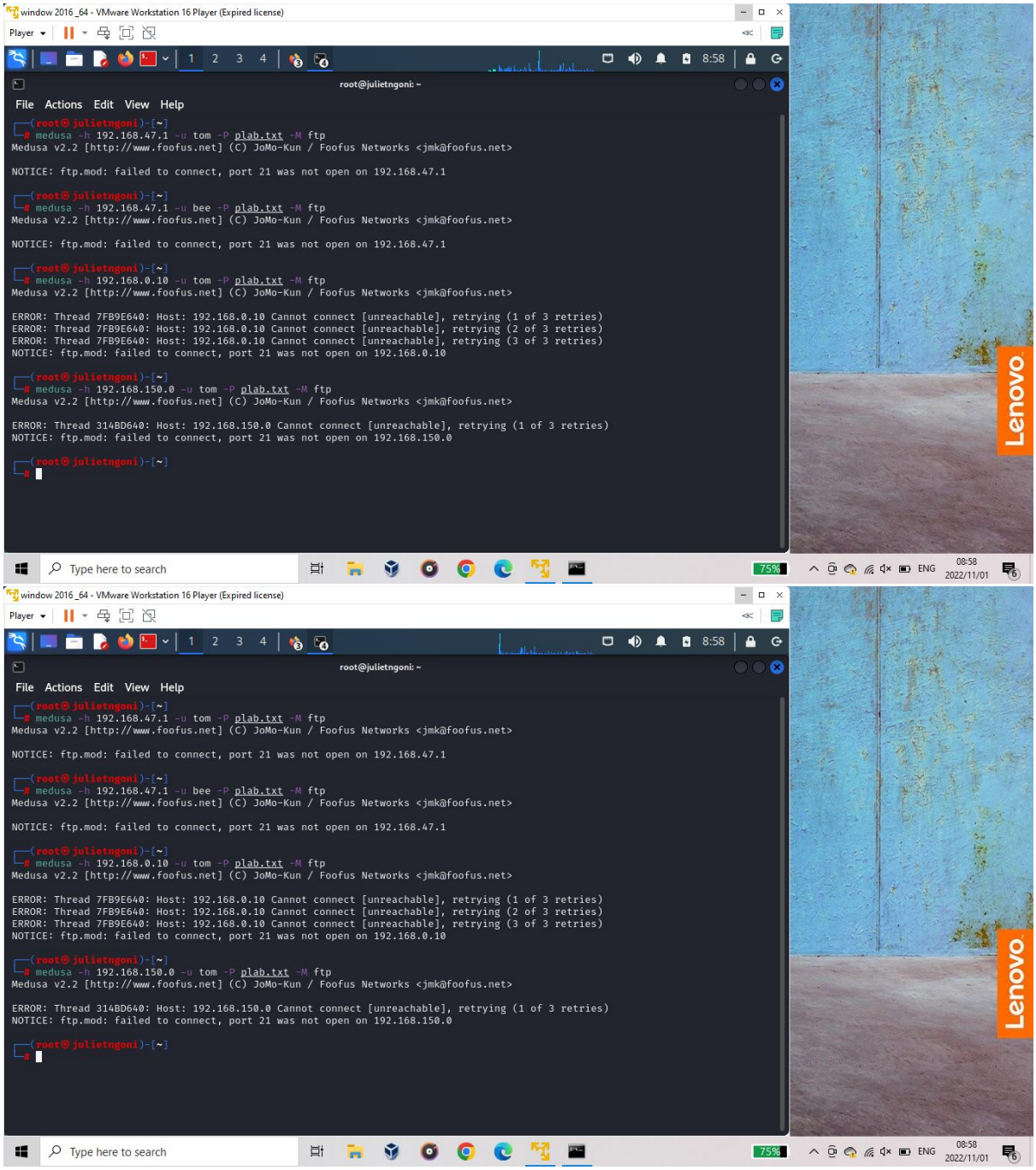

Enter the command ls -l to see where plab.txt and the user.txt(command: cp plab.txt user.txt) of which is the copy of plab.txt is allocated(Location).And ensure that it is indeed saved and contain both the files.




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 coonectionfailed 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





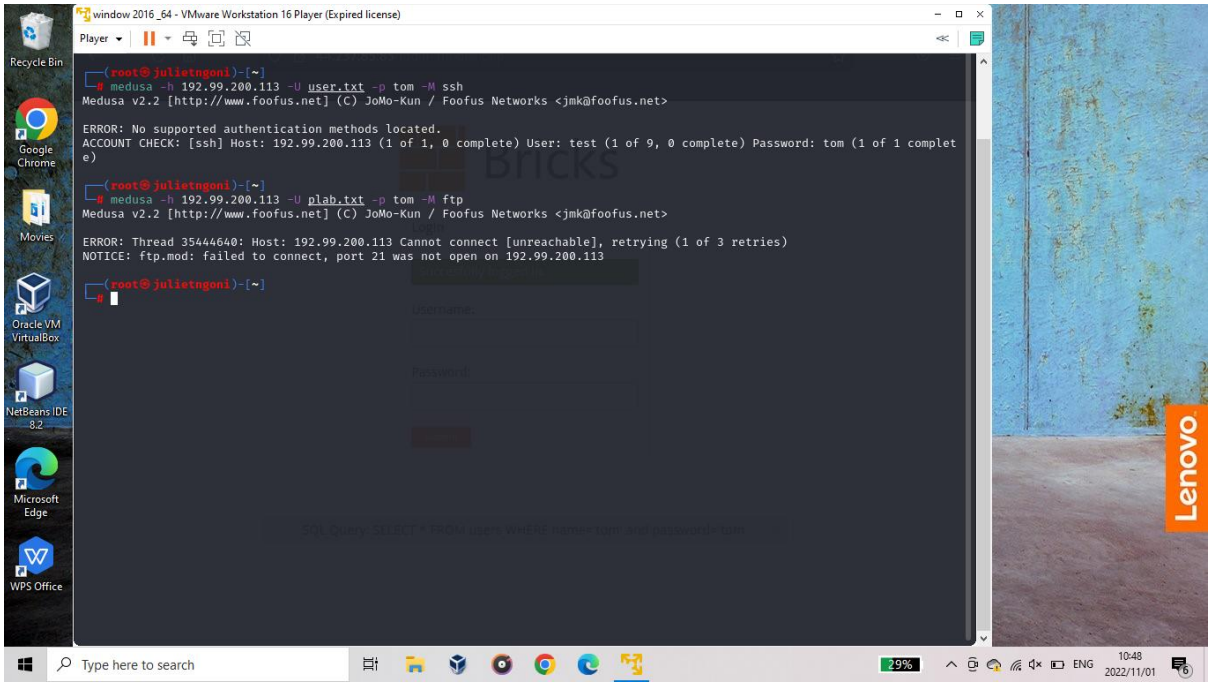




Enter command: medusa -h 192.99.200.113 -u tom -P plab.txt -M ssh and also command: medusa -h 192.99.200.113 -u tom -P user.txt -M ssh

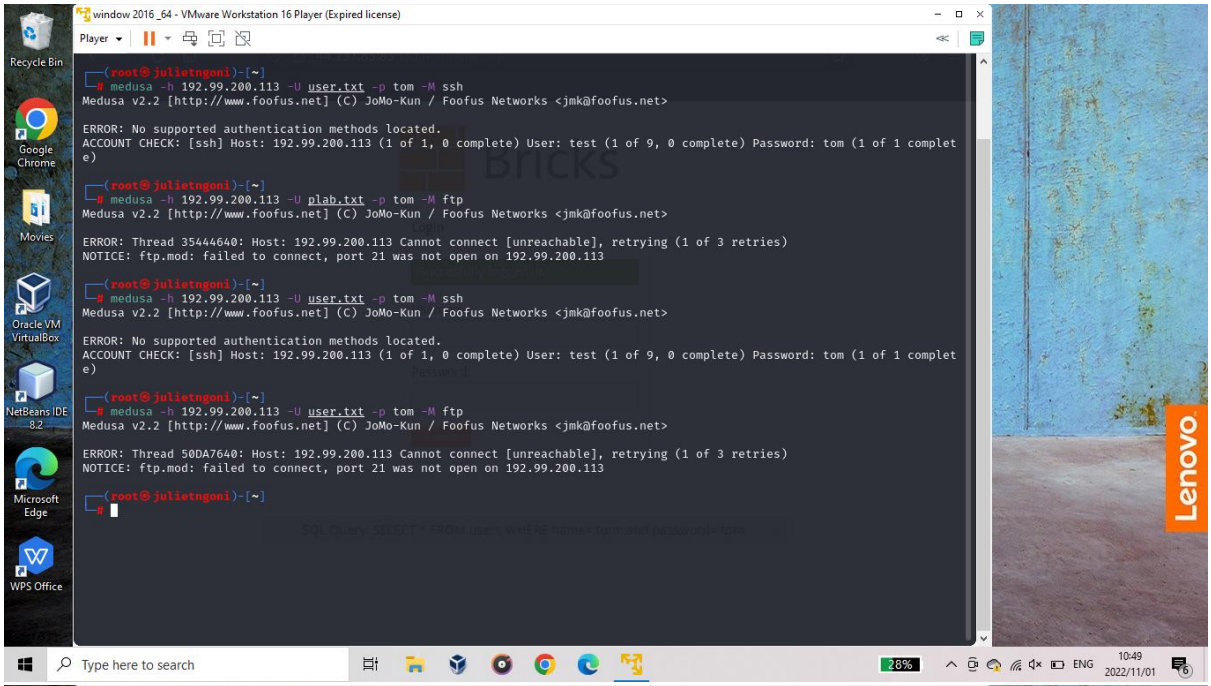
And it shows the following results that checks the account and discovers that 1 out of 9 are

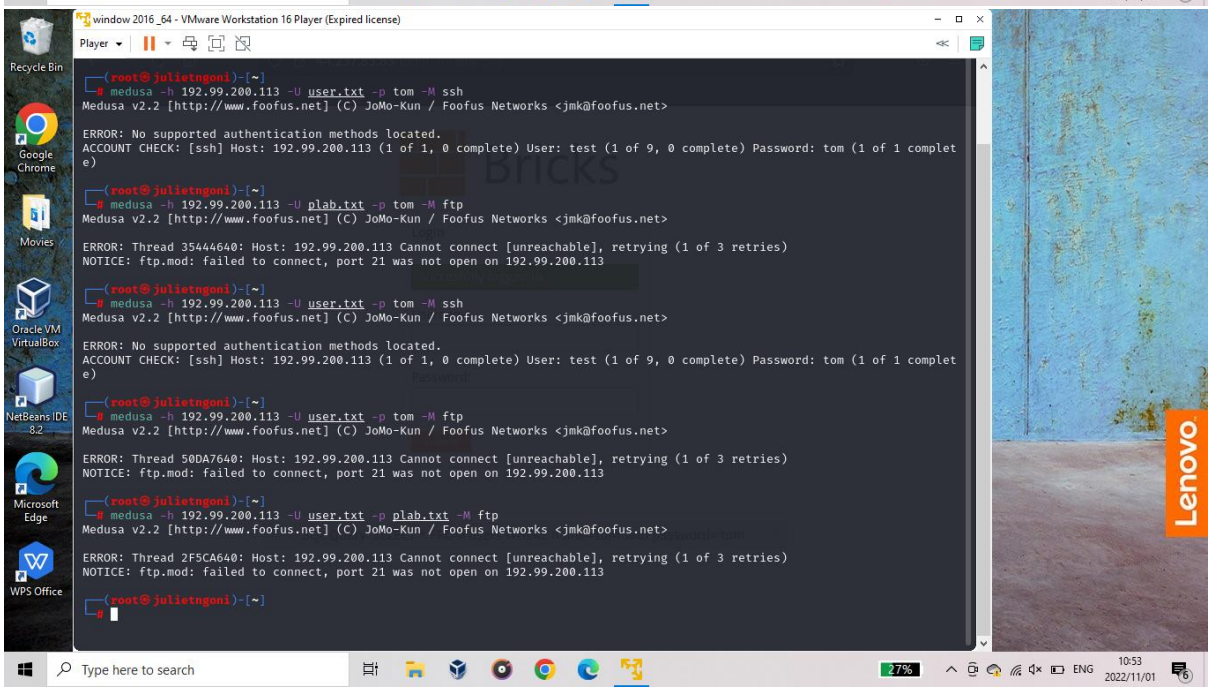
complete and that the password is tom




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

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

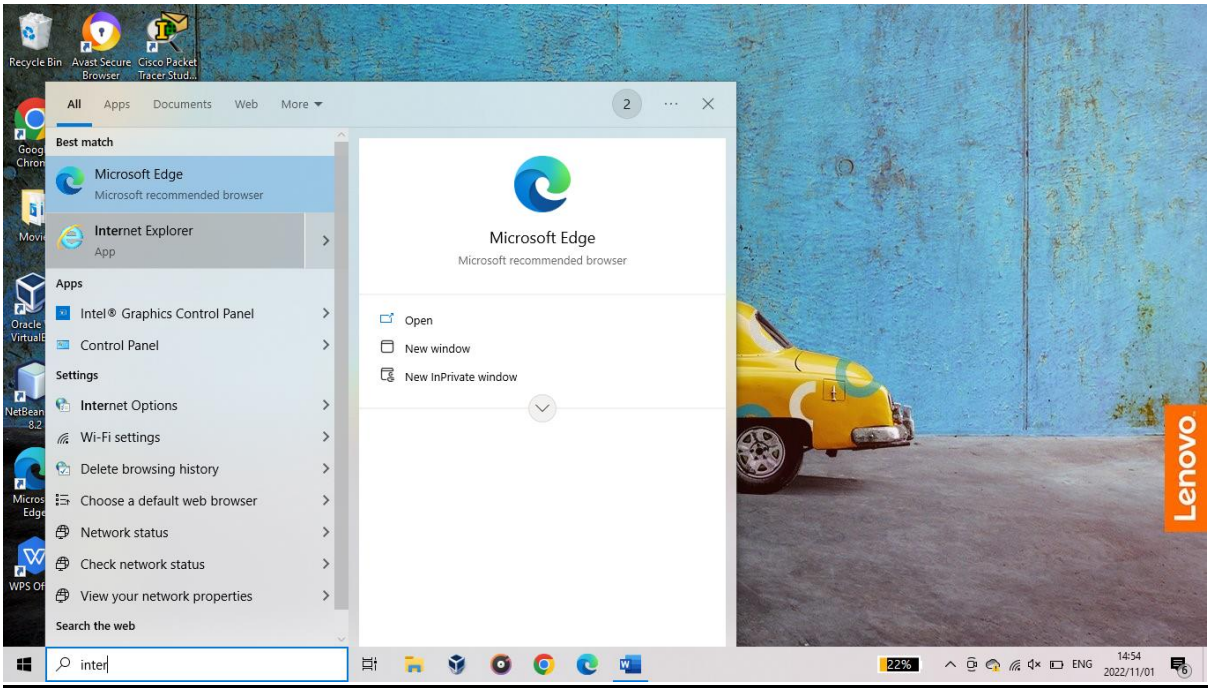


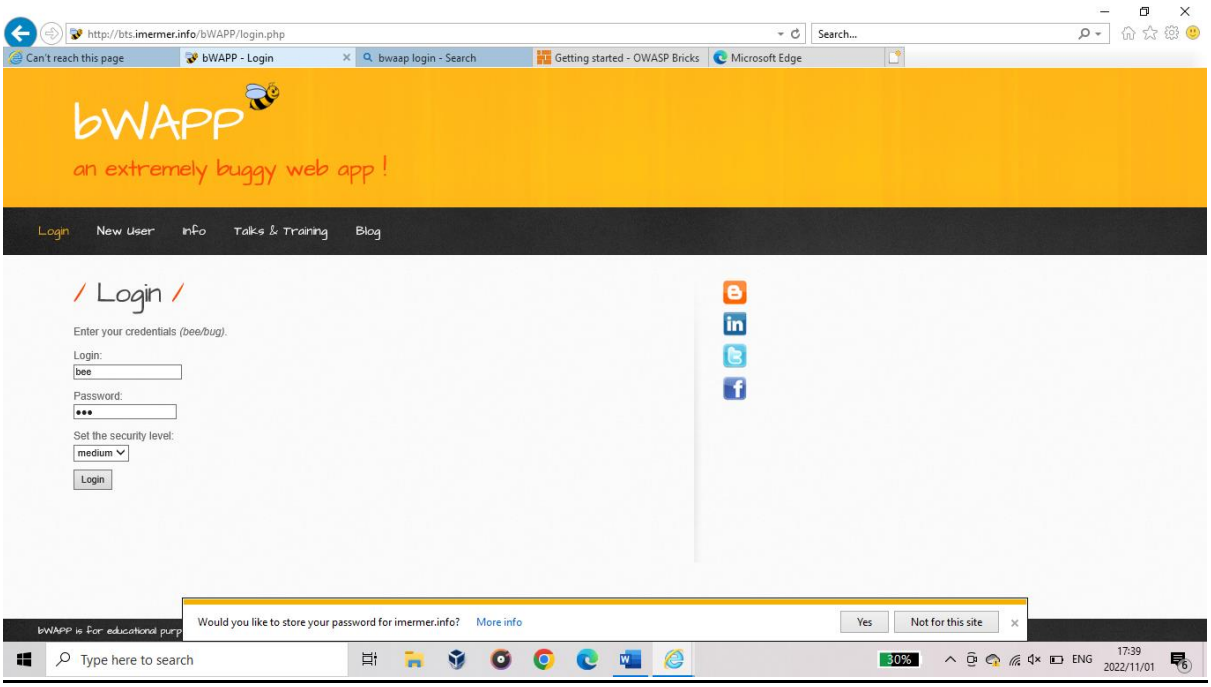



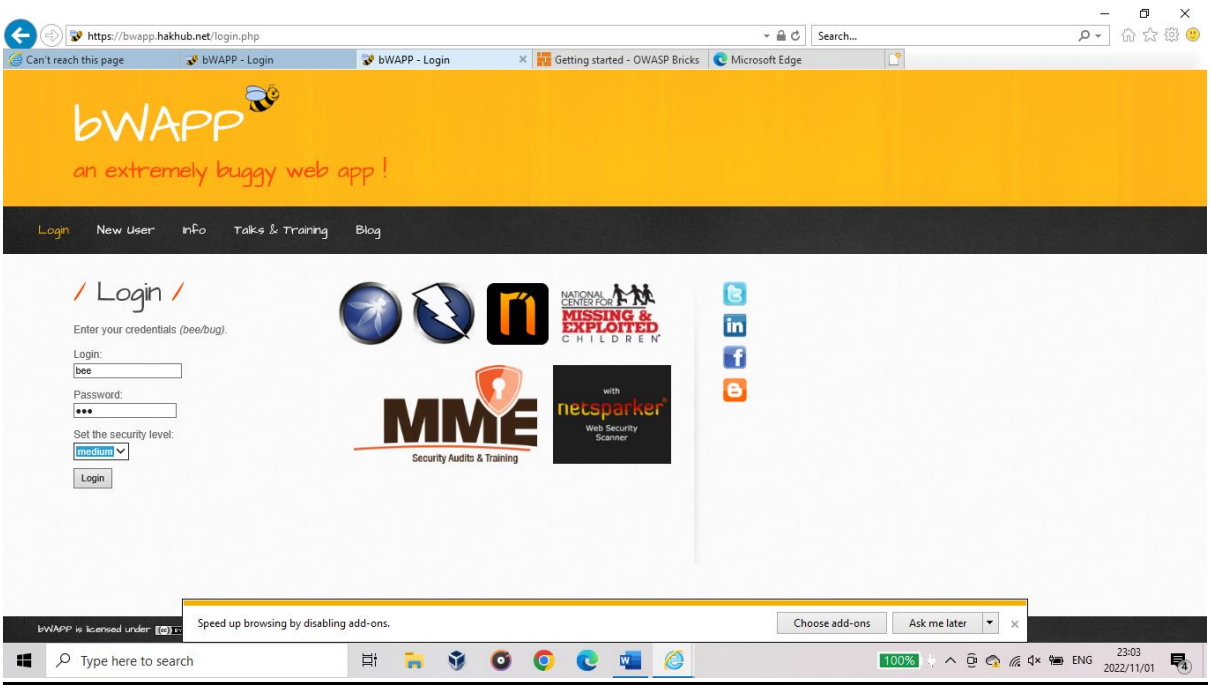

# Exercise 2

# Testing web application vulnerabilities

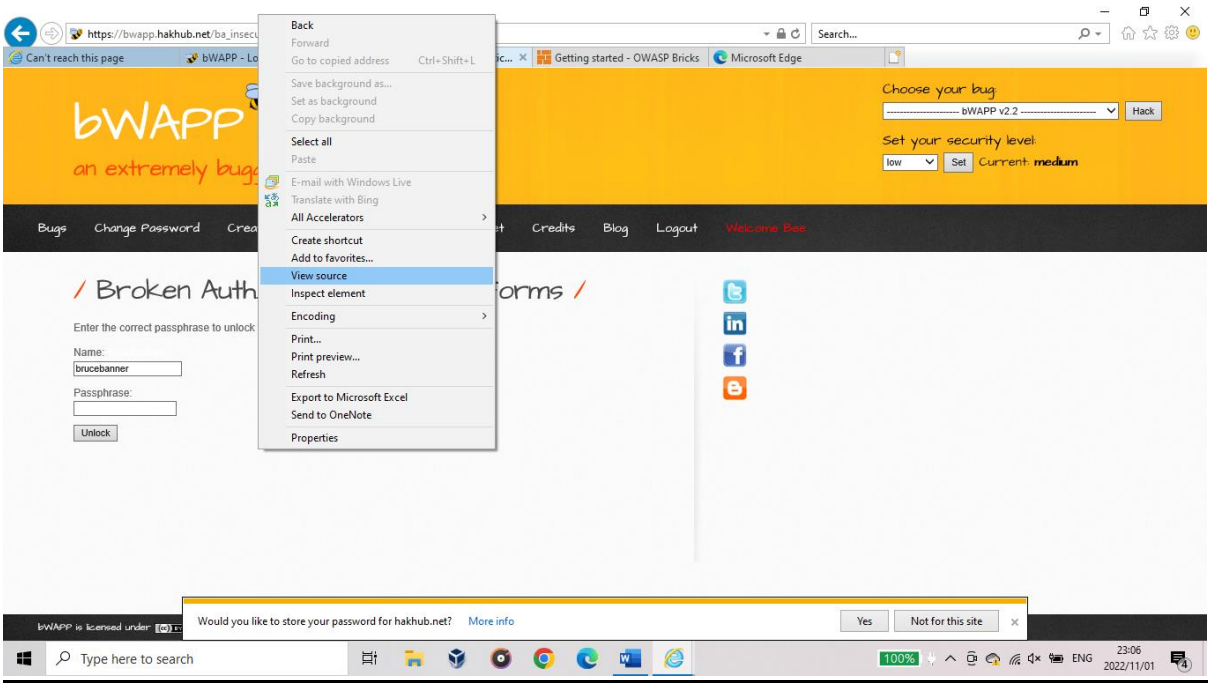
# 1.Desktop dislay

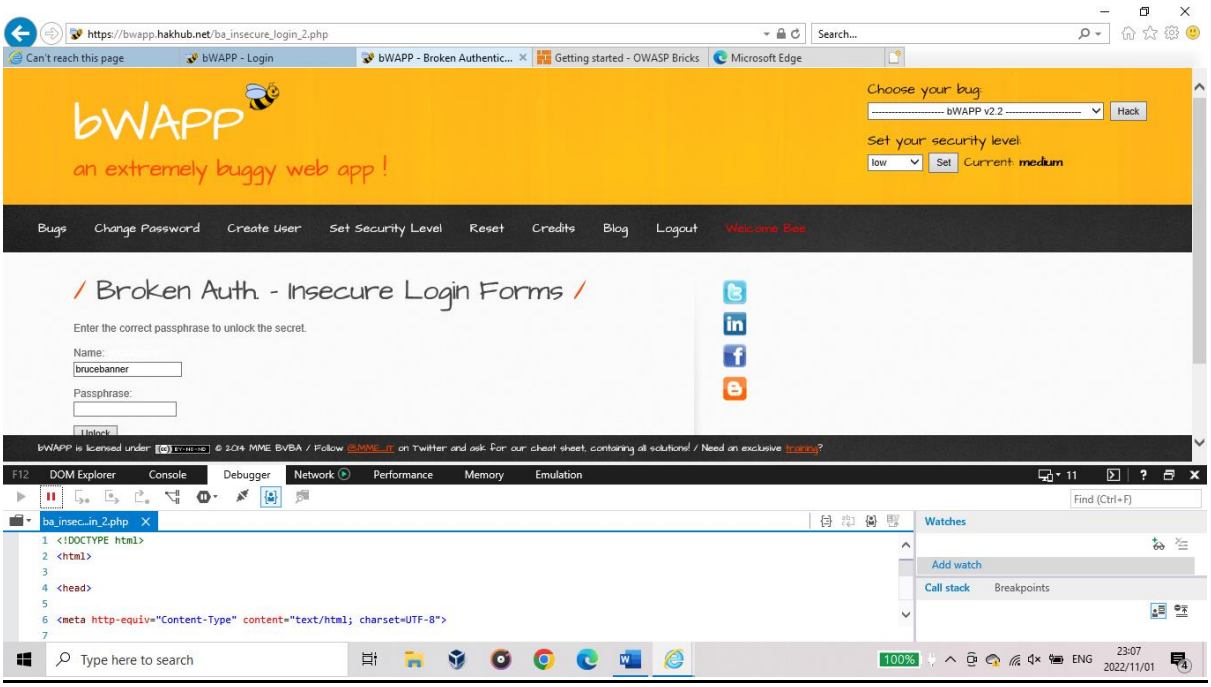



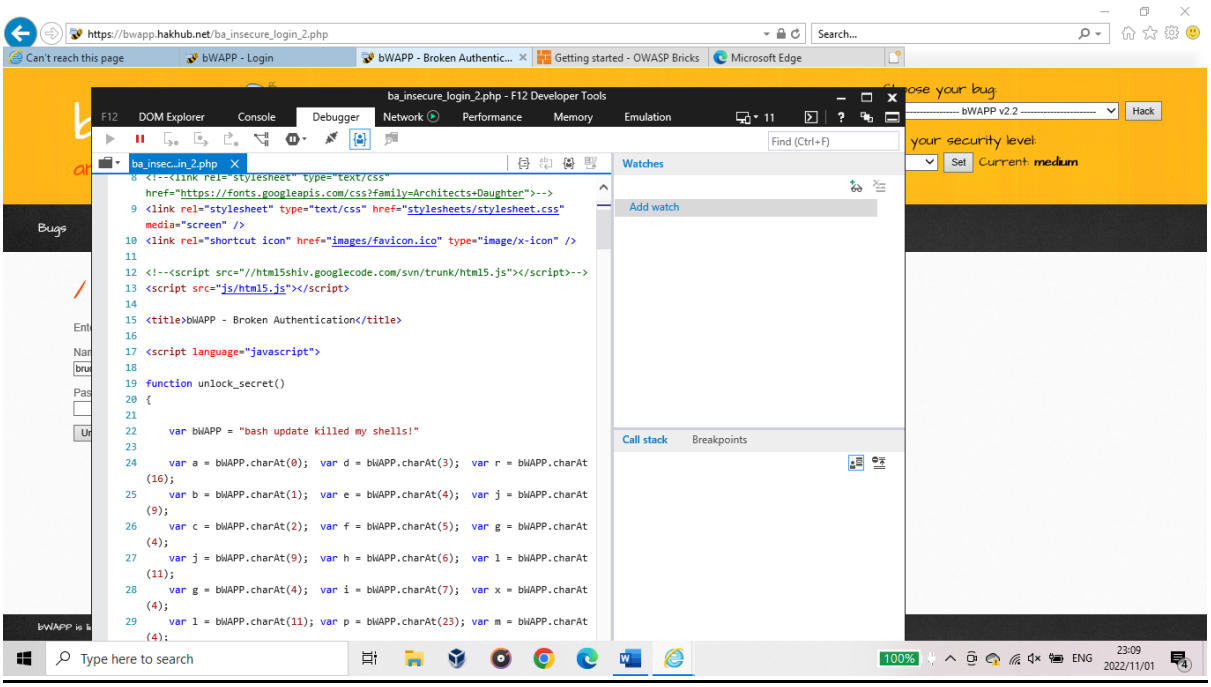

http://bts.imermer.info/bWAPP/login.php
Search...
Can't reach this page
bWAPP - Login
bwaap login - Search
Getting started - OWASP Bricks
Microsoft Edge
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Login /
Enter your credentials (bee/bug).
Login:
bee
Password:
Set the security level:
medium
Login
Would you like to store your password for imermer.info?
More info
Yes
Not for this site
bWAPP is for educational purp
Type here to search
30%
ENG
17:39
2022/11/01

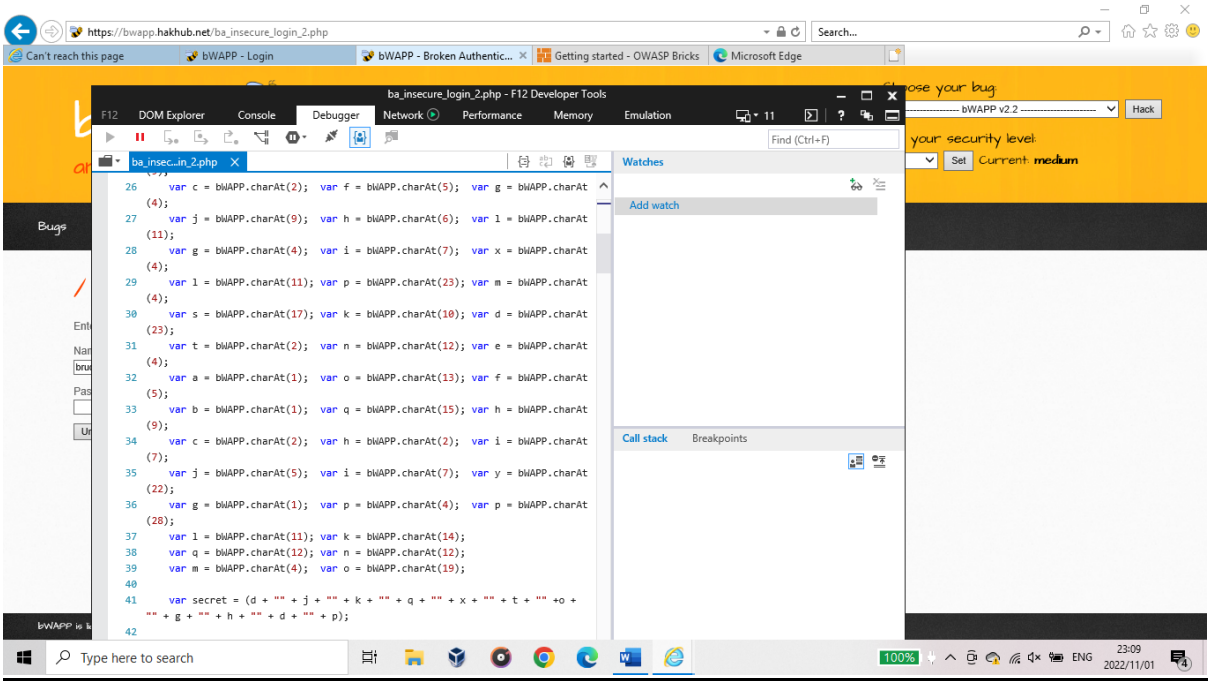

https://bwapp.hakhub.net/login.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Login
Getting started - OWASP Bricks
Microsoft Edge
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Login /
Enter your credentials (bee/bug).
Login:
bee
Password:
Set the security level:
medium
Login
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
with netsparker
Web Security Scanner
Speed up browsing by disabling add-ons.
Choose add-ons
Ask me later
bWAPP is licensed under
Type here to search
100%
ENG
23:03
2022/11/01

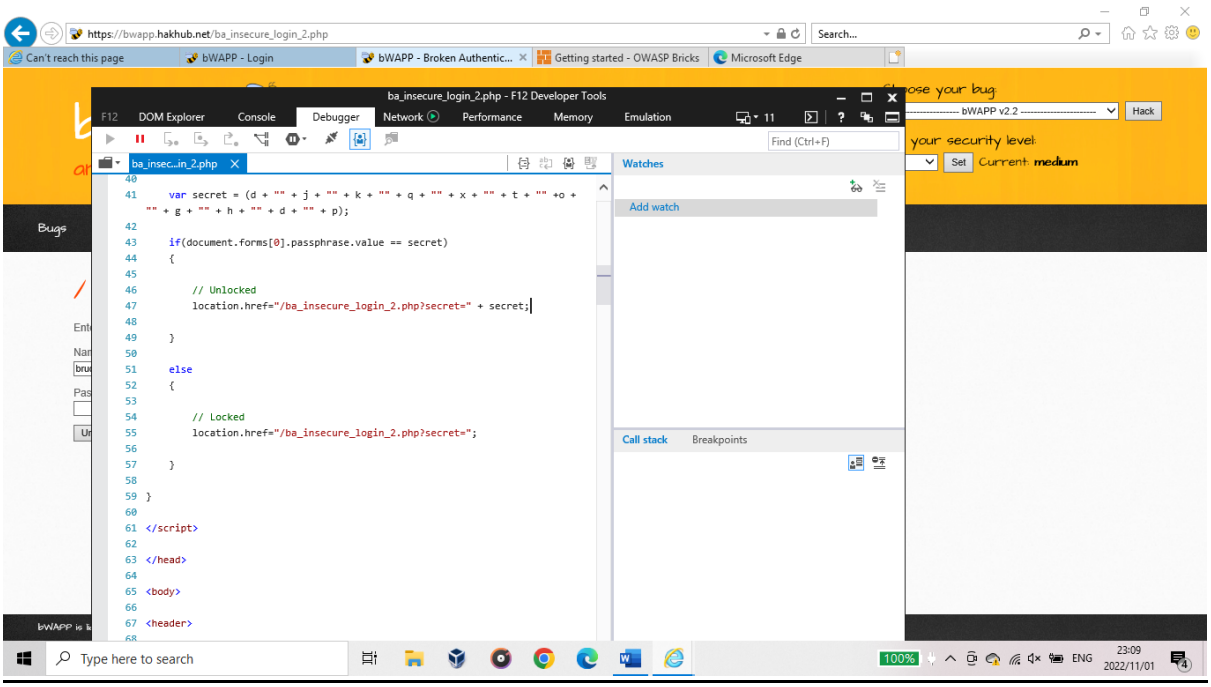

https://bwapp.hakhub.net/portal.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Portal
Getting started - OWASP Bricks
Microsoft Edge
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ 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 - Blind (SQLite)
SQL Injection - Blind (Web Services/SOAP)
XML/XPath Injection (Login Form)
XML/XPath Injection (Search)
/
/ A2 - Broken Auth. & Session Mgmt. /
Broken Authentication - CAPTCHA Bypassing
Broken Authentication - Forgotten Function
Broken Authentication - Insecure Login Forms
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
https://bwapp.hakhub.net/portal.php
Would you like to store your password for hakhub.net?
More info
Yes
Not for this site
Type here to search
100%
ENG
23:04
2022/11/01

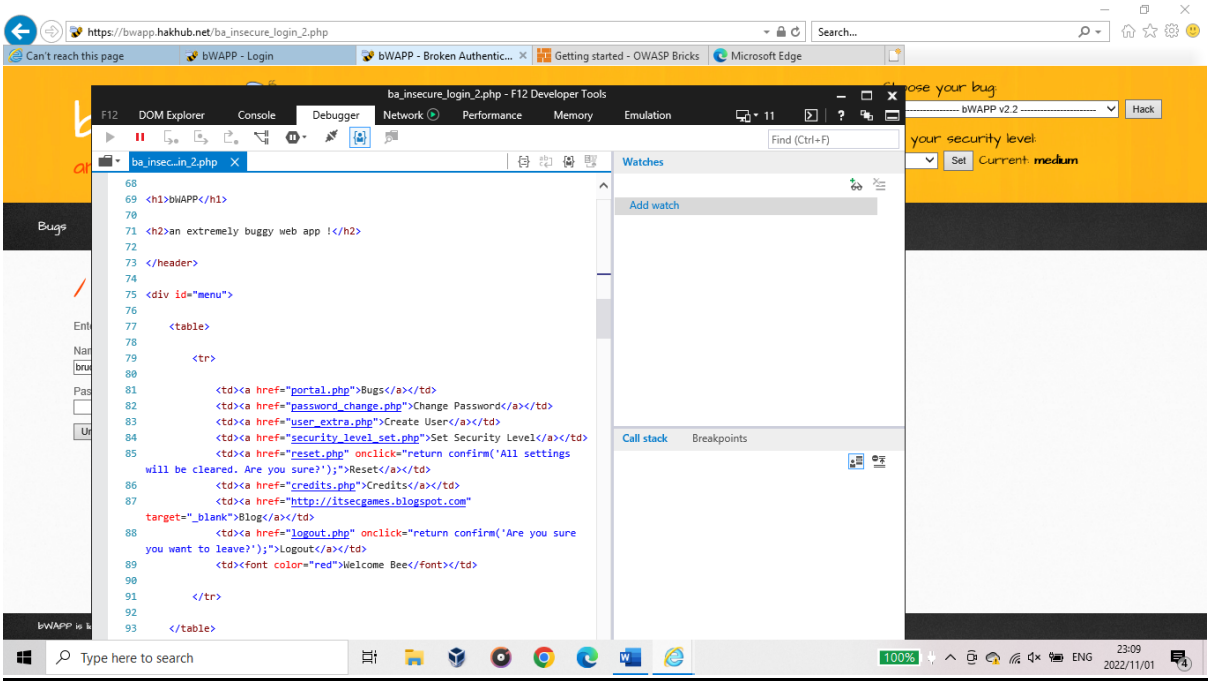

Back
Forward
Go to copied address
Ctrl+Shift+L
Save background as...
Set as background
Copy background
Select all
Paste
E-mail with Windows Live
Translate with Bing
All Accelerators
Create shortcut
Add to favorites...
View source
Inspect element
Encoding
Print...
Print preview...
Refresh
Export to Microsoft Excel
Send to OneNote
Properties
/ Broken Auth
orms /
Enter the correct passphrase to unlock
Name:
brucebanner
Passphrase:
Unlock
bWAPP is licensed under
Would you like to store your password for hakhub.net?
More info
Yes
Not for this site
Type here to search
100%
ENG
23:06
2022/11/01

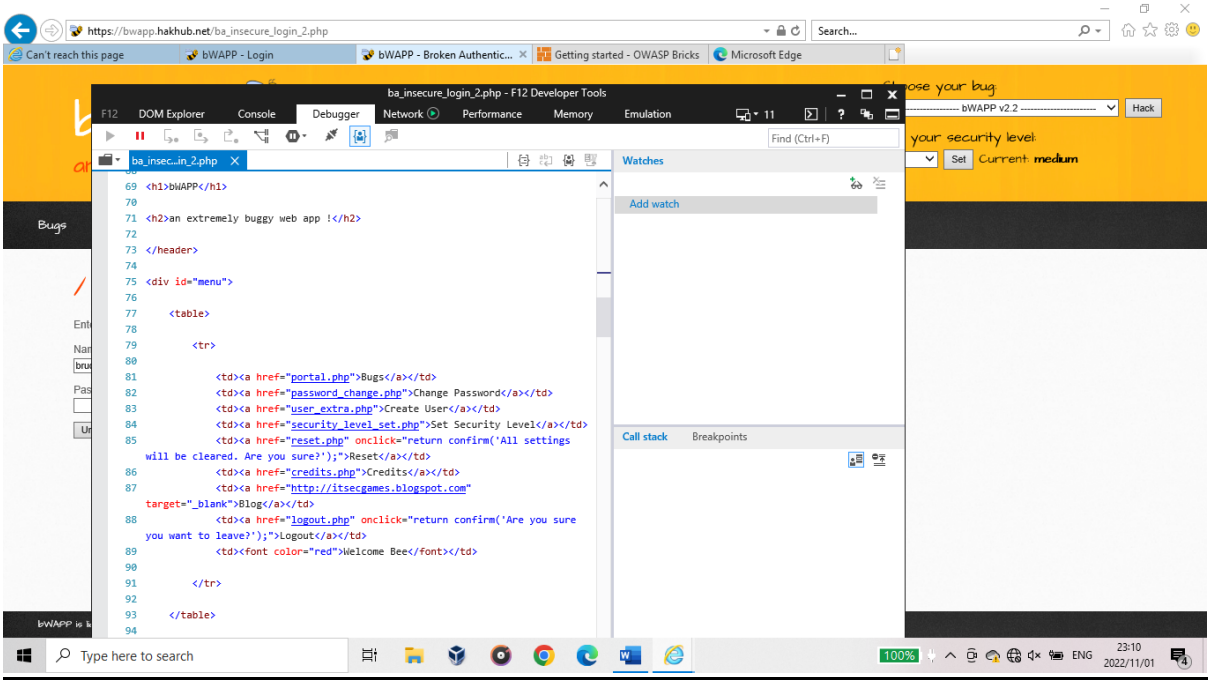

https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Broken Auth. - Insecure Login Forms /
Enter the correct passphrase to unlock the secret.
Name:
brucebanner
Passphrase:
Unlock
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
ba_insec...in_2.php
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5
6 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
7
Watches
Add watch
Call stack
Breakpoints
Type here to search
100%
ENG
23:07
2022/11/01


https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
ba_insecure_login_2.php - F12 Developer Tools
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
Find (Ctrl+F)
ba_insec...in_2.php
8 <!--<link rel="stylesheet" type="text/css"
href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
9 <link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css"
media="screen" />
10 <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />
11
12 <!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
13 <script src="js/html5.js"></script>
14
15 <title>bWAPP - Broken Authentication</title>
16
17 <script language="javascript">
18
19 function unlock_secret()
20 {
21
22 var bWAPP = "bash update killed my shells!"
23
24 var a = bWAPP.charAt(0); var d = bWAPP.charAt(3); var r = bWAPP.charAt
(16);
25 var b = bWAPP.charAt(1); var e = bWAPP.charAt(4); var j = bWAPP.charAt
(9);
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
(4);
Watches
Add watch
Call stack
Breakpoints
Choose your bug:
bWAPP v2.2
Hack
your security level:
Set
Current: medium
Bugs
Type here to search
100%
ENG
23:09
2022/11/01

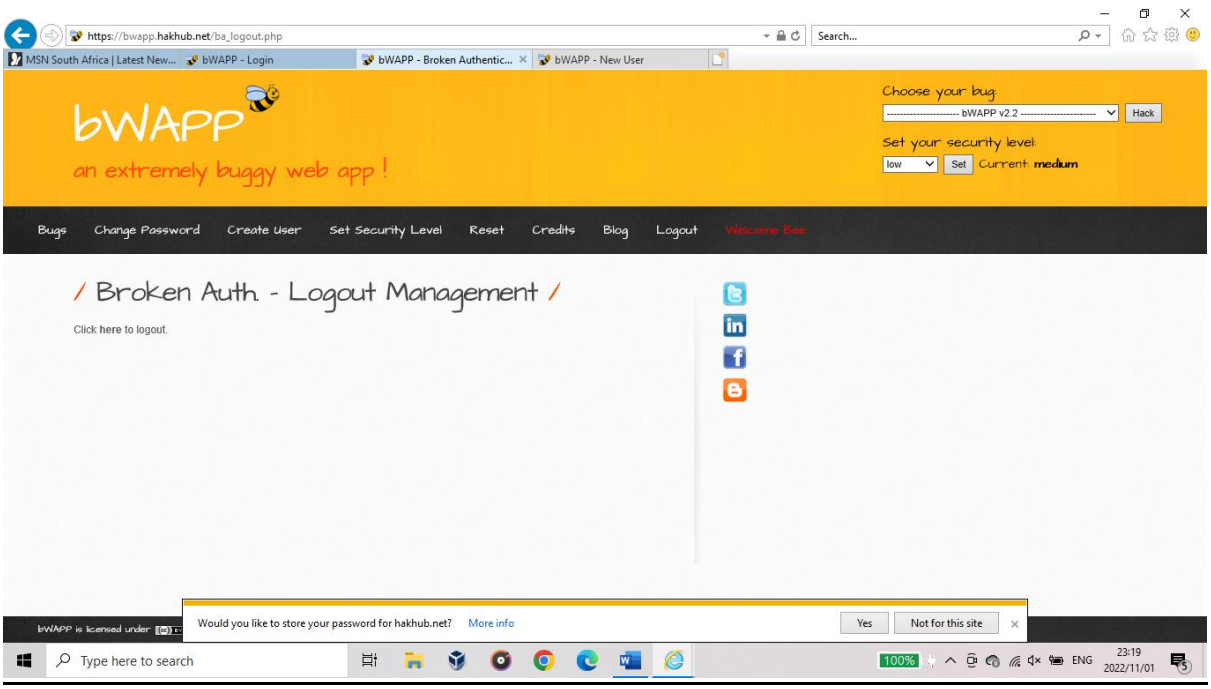

https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
ba_insecure_login_2.php - F12 Developer Tools
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
Find (Ctrl+F)
ba_insec...in_2.php
Watches
Add watch
Call stack
Breakpoints
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(4);
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 + "" + g + "" + h + "" + d + "" + p);
42
Choose your bug:
bWAPP v2.2
Hack
your security level:
Set
Current: medium
Bugs
Type here to search
100%
ENG
23:09
2022/11/01


https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
ba_insecure_login_2.php - F12 Developer Tools
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
Find (Ctrl+F)
ba_insec...in_2.php
Watches
Add watch
Call stack
Breakpoints
40
41 var secret = (d + "" + j + "" + k + "" + q + "" + x + "" + t + "" +o + "" + g + "" + h + "" + d + "" + p);
42
43 if(document.forms[0].passphrase.value == secret)
44 {
45
46 // Unlocked
47 location.href="/ba_insecure_login_2.php?secret=" + secret;
48
49 }
50
51 else
52 {
53
54 // Locked
55 location.href="/ba_insecure_login_2.php?secret=";
56
57 }
58
59 }
60
61 </script>
62
63 </head>
64
65 <body>
66
67 <header>
68
Choose your bug:
bWAPP v2.2
Hack
your security level:
Set
Current: medium
Bugs
Type here to search
100%
ENG
23:09
2022/11/01


https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
ba_insecure_login_2.php - F12 Developer Tools
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
Find (Ctrl+F)
ba_insec...in_2.php
Watches
Add watch
Call stack
Breakpoints
Bugs
Hack
Set
Current: medium
Type here to search
ENG
23:09
2022/11/01

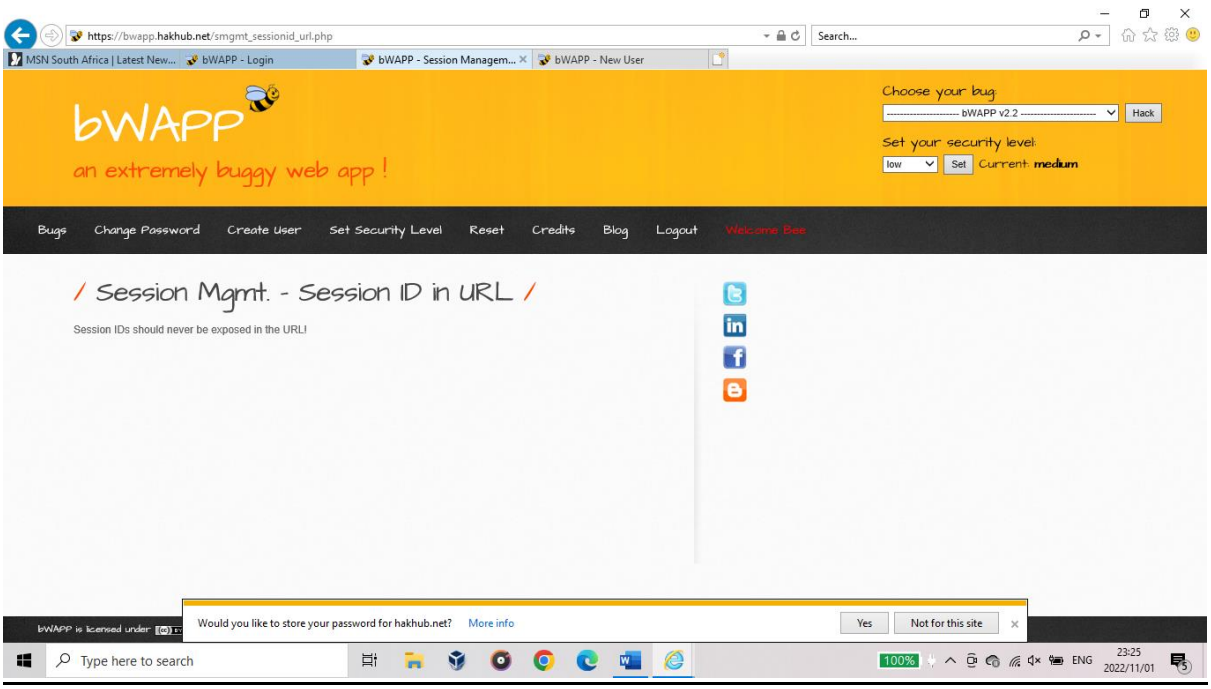

https://bwapp.hakhub.net/ba_insecure_login_2.php
Search...
Can't reach this page
bWAPP - Login
bWAPP - Broken Authentic...
Getting started - OWASP Bricks
Microsoft Edge
ba_insecure_login_2.php - F12 Developer Tools
F12
DOM Explorer
Console
Debugger
Network
Performance
Memory
Emulation
Find (Ctrl+F)
ba_insec...in_2.php
Watches
Add watch
Call stack
Breakpoints
Bugs
Hack
Set
Current: medium
Type here to search
ENG
23:10
2022/11/01


https://bwapp.hakhub.net/portal.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - Portal
bWAPP - New User
bWAPP
an extremely buggy web app !
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
/ 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 Authentication - Weak Passwords
Session Management - Administrative Portals
Session Management - Cookies (HTTPOnly)
Session Management - Cookies (Secure)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
bWAPP is licensed under
Would you like to store your password for hakhub.net?
More info
Yes
Not for this site
Type here to search
100%
ENG
23:18
2022/11/01


https://bwapp.hakhub.net/ba_logout.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - Broken Authentic...
bWAPP - New User
bWAPP
an extremely buggy web app !
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. - Logout Management /
Click here to logout.
bWAPP is licensed under
Would you like to store your password for hakhub.net?
More info
Yes
Not for this site
Type here to search
100%
ENG
23:19
2022/11/01

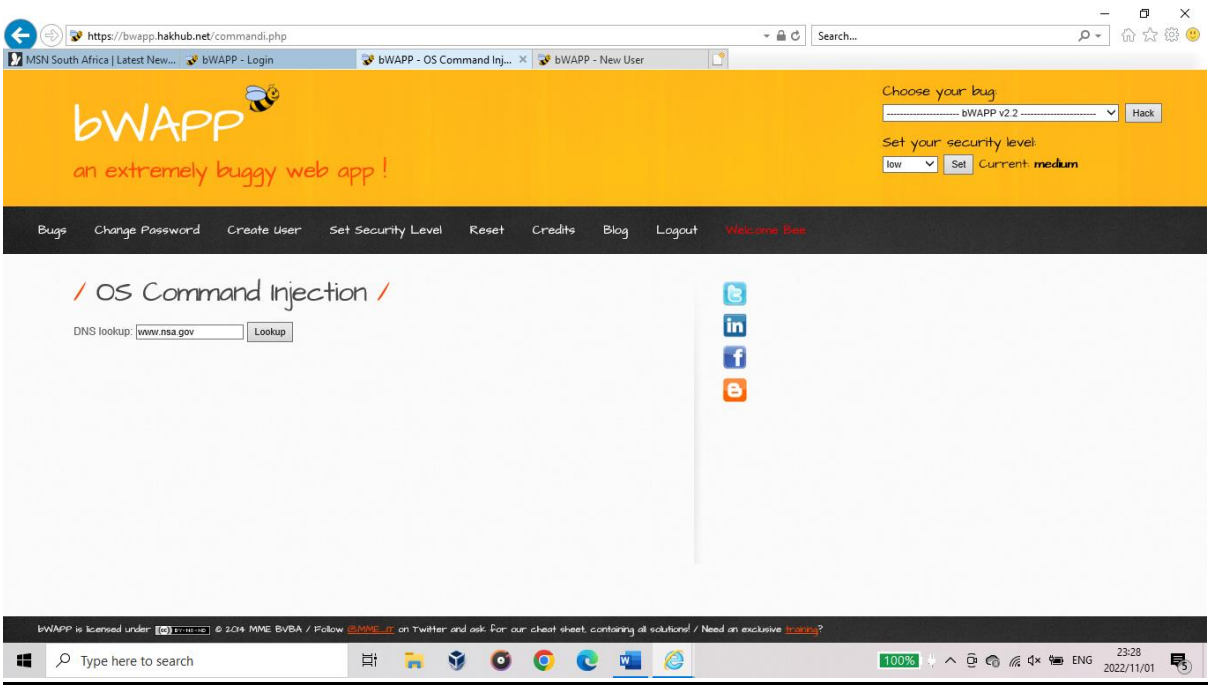


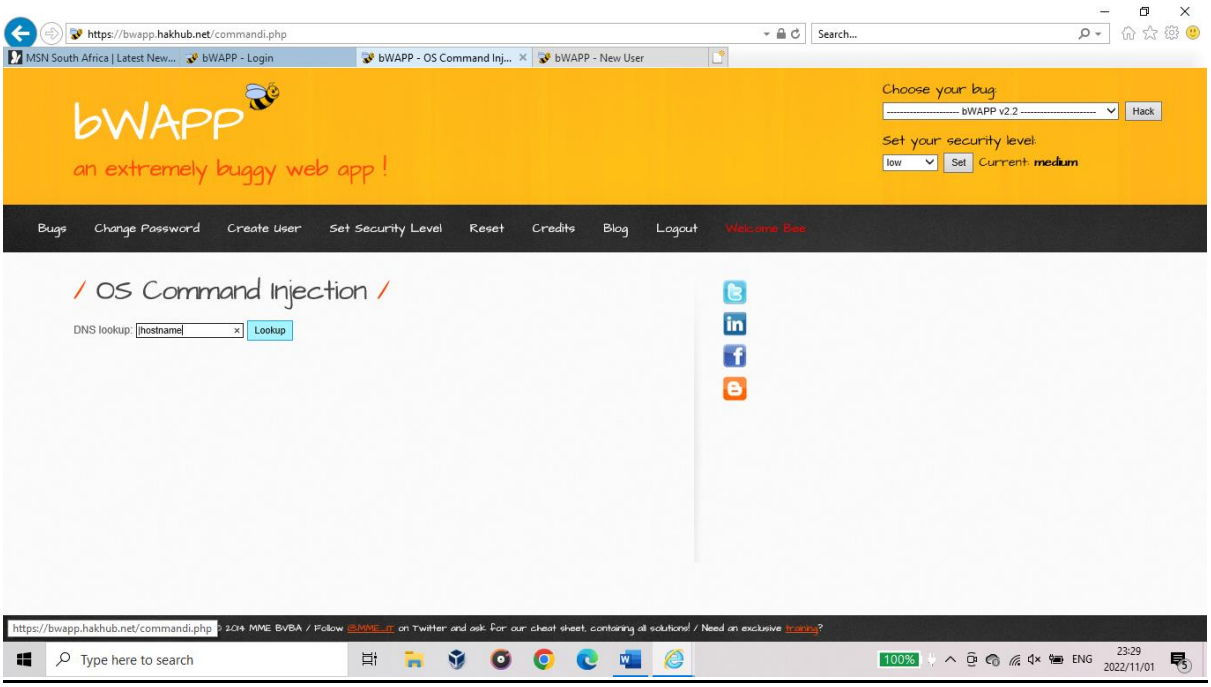
# Task 2 view session id in url

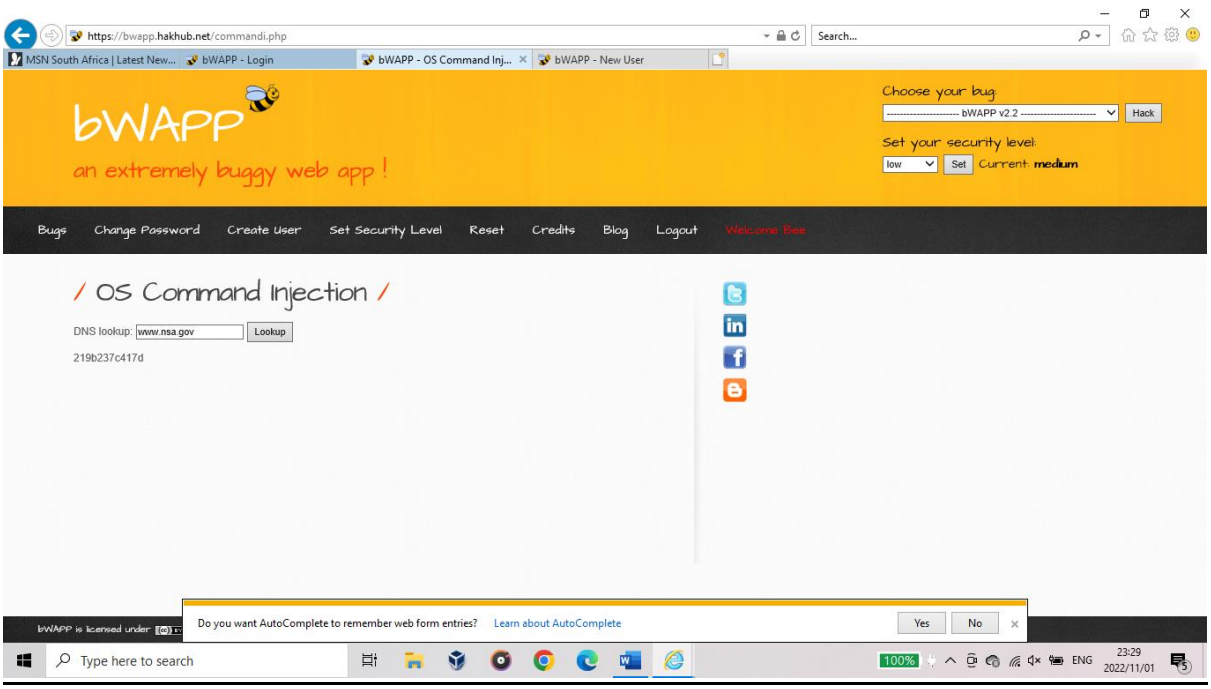



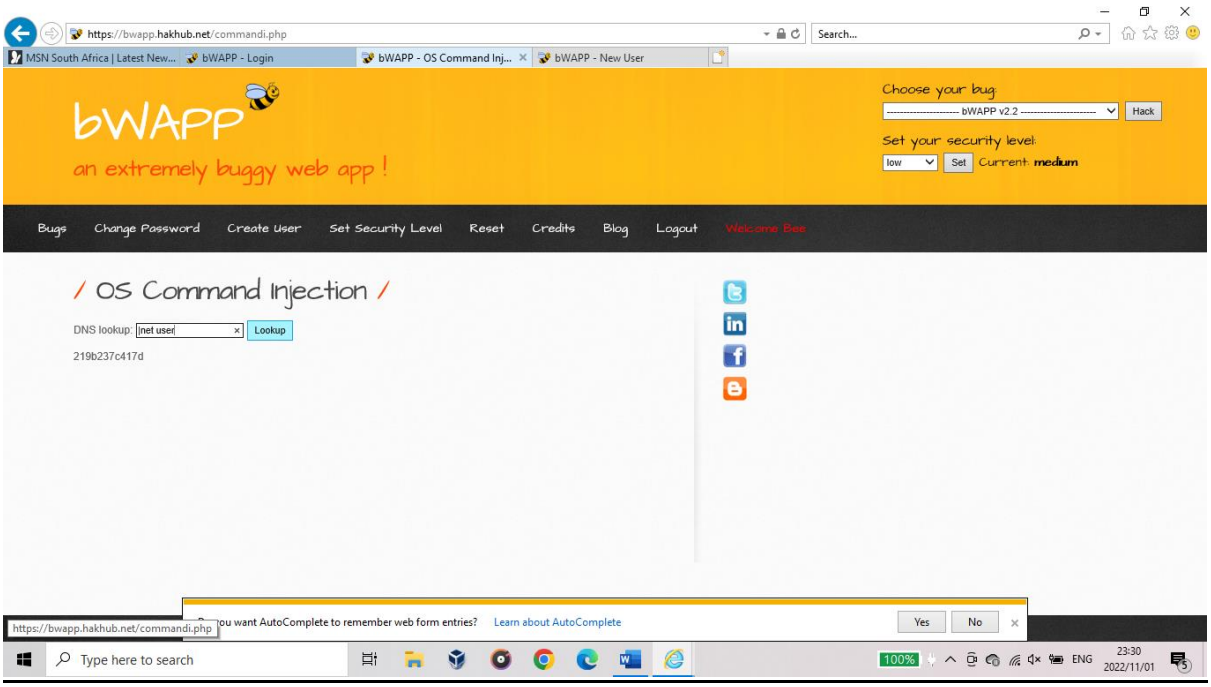

# Task 3 conduct os command injection attack


https://bwapp.hakhub.net/portal.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - Portal
bWAPP - New User
bWAPP
an extremely buggy web app !
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
/ 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 - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
OS Command Injection
OS Command Injection - Blind
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
https://bwapp.hakhub.net/portal.php
Would you like to store your password for hakhub.net?
More info
Yes
Not for this site
Type here to search
100%
ENG
23:28
2022/11/01

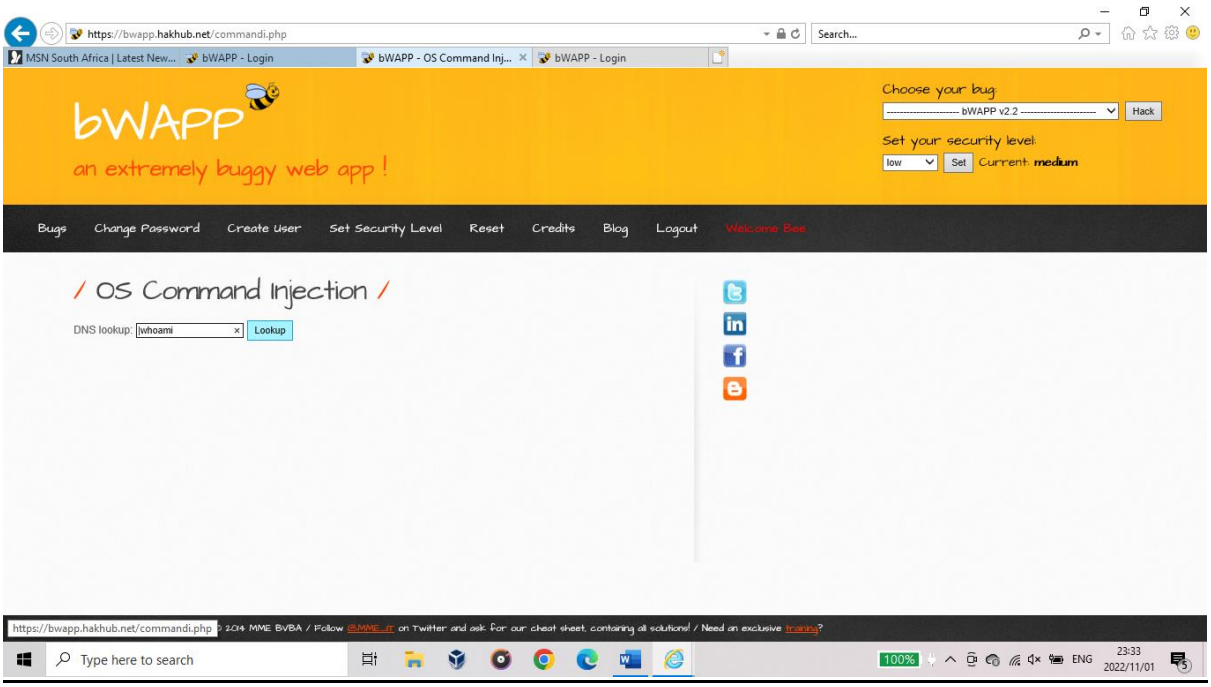

https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - New User
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
23:28
2022/11/01

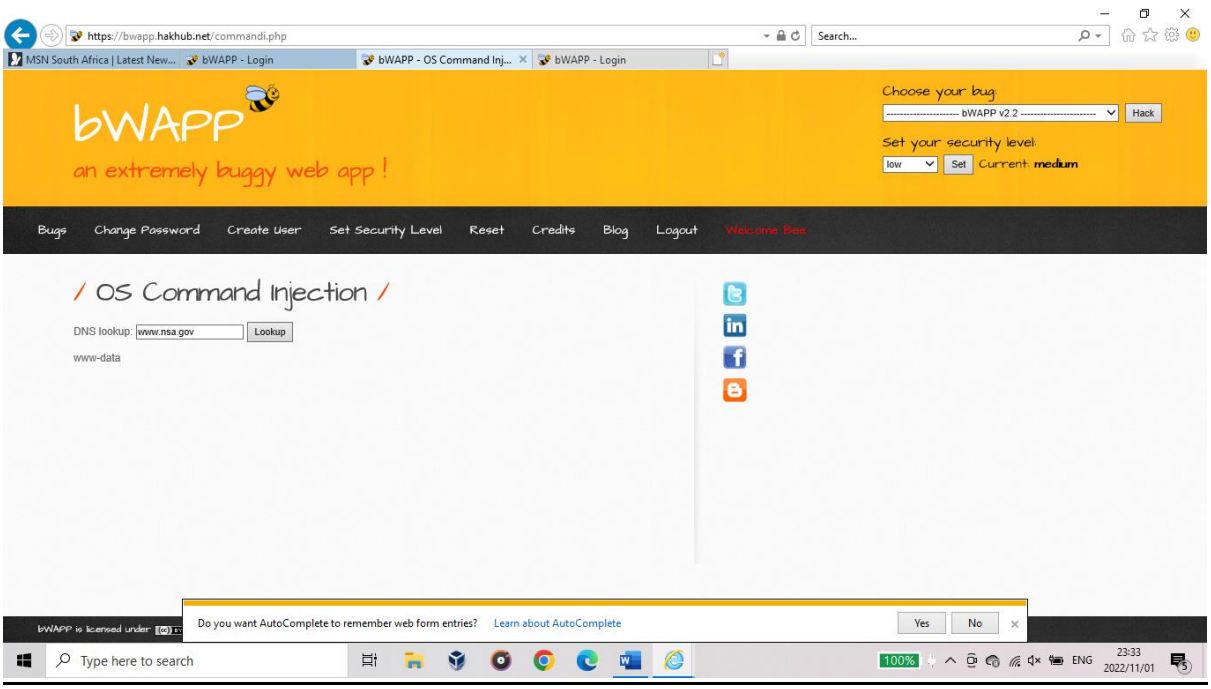

https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - New User
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
lhostname
Lookup
https://bwapp.hakhub.net/commandi.php
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
23:29
2022/11/01

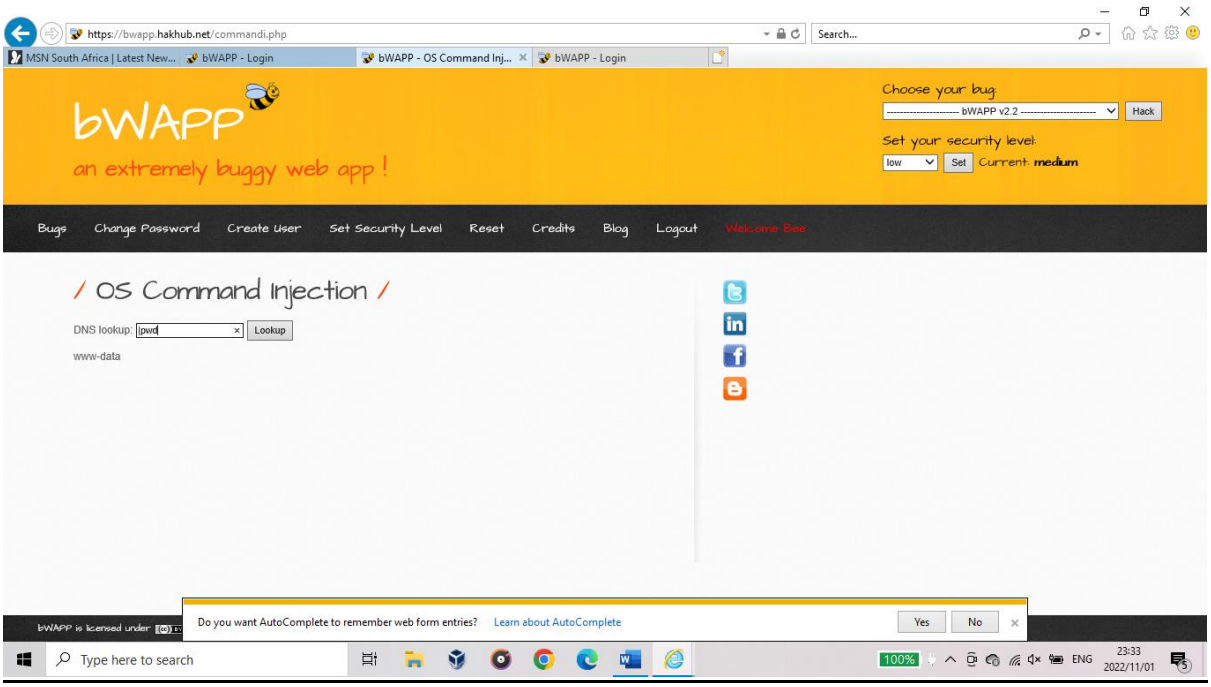

https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - New User
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
219b237c417d
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:29
2022/11/01

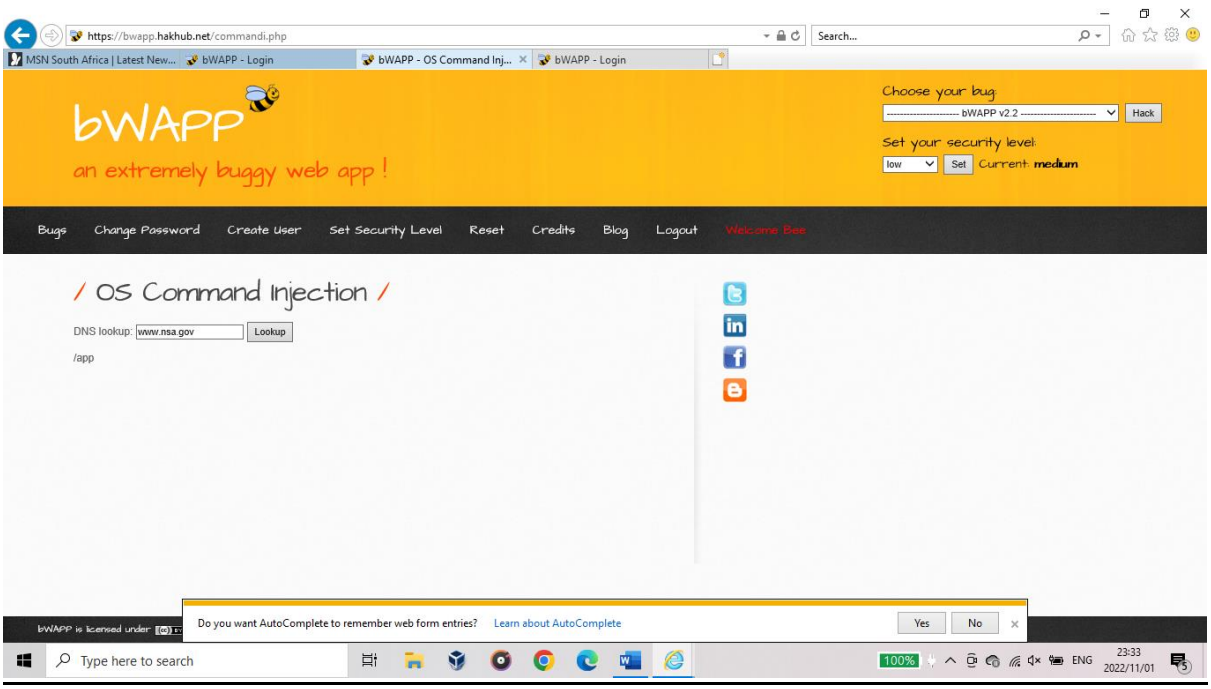

https://bwapp.hakhub.net/commandi.php
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - New User
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
inet user
Lookup
219b237c417d
Learn about AutoComplete
Yes
No
Type here to search
ENG
23:30
2022/11/01

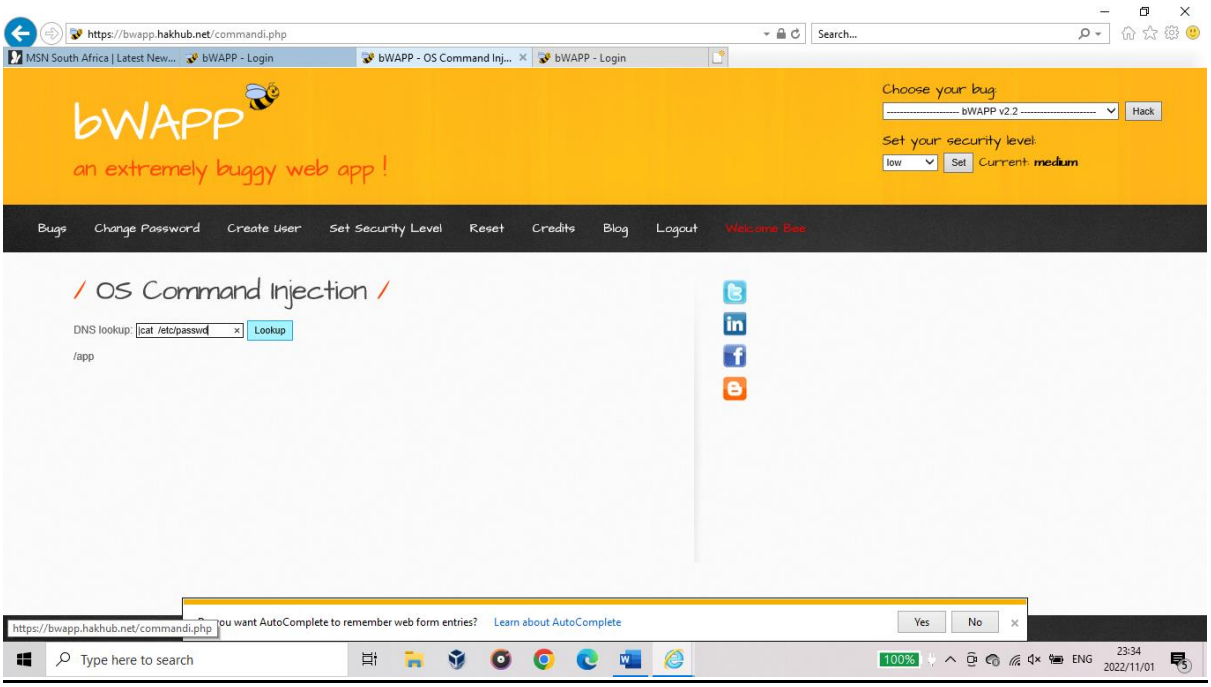

https://bwapp.hakhub.net/portal.php
bWAPP - Login
bWAPP - Portal
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Portal /
bWAPP, or a buggy 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? :)
/ 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)
OS Command Injection
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
ENG
23:32
2022/11/01

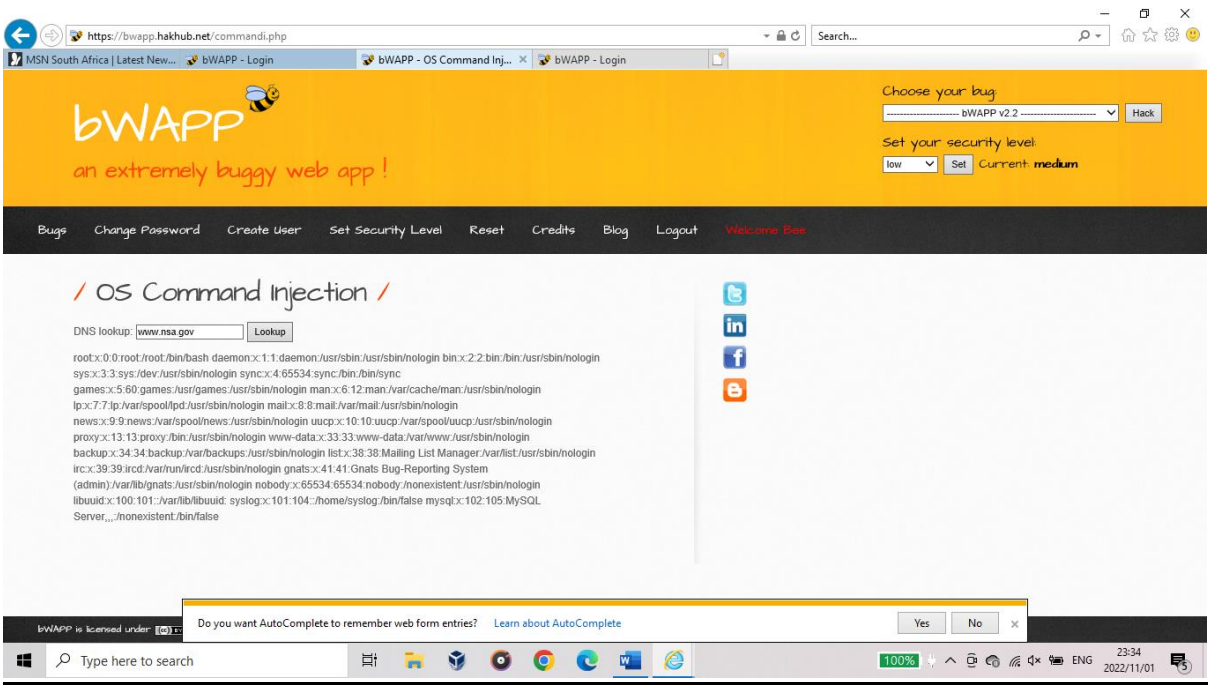

https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - Login
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
lwhoami
Lookup
https://bwapp.hakhub.net/commandi.php
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
23:33
2022/11/01


https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - Login
bWAPP
an extremely buggy web app !
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
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
www-data
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:33
2022/11/01


https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - Login
bWAPP
an extremely buggy web app !
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
/ OS Command Injection /
DNS lookup:
pwd
Lookup
www-data
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:33
2022/11/01

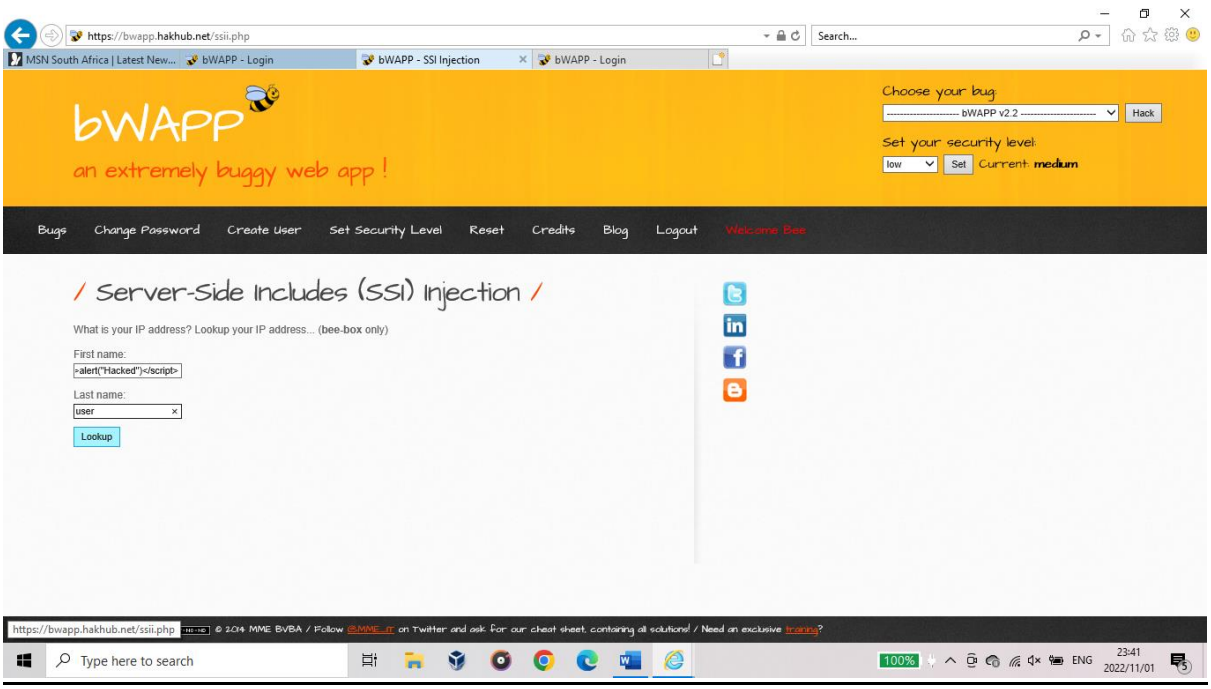

https://bwapp.hakhub.net/commandi.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - OS Command Inj...
bWAPP - Login
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
/app
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:33
2022/11/01

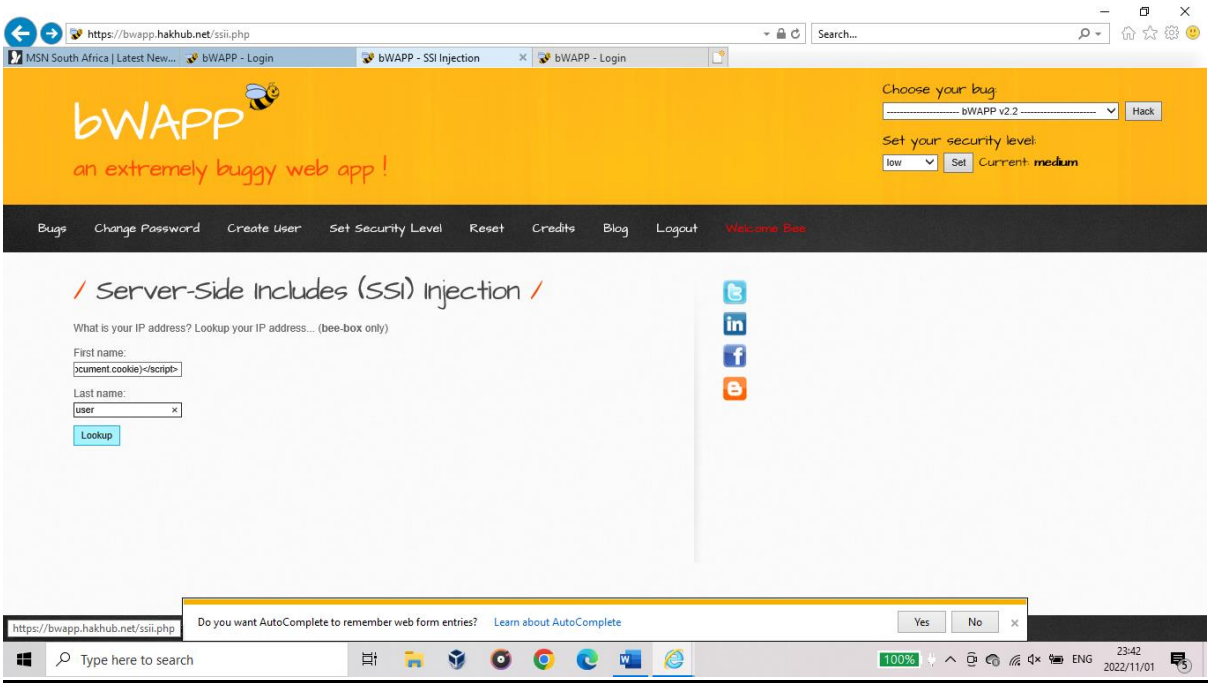


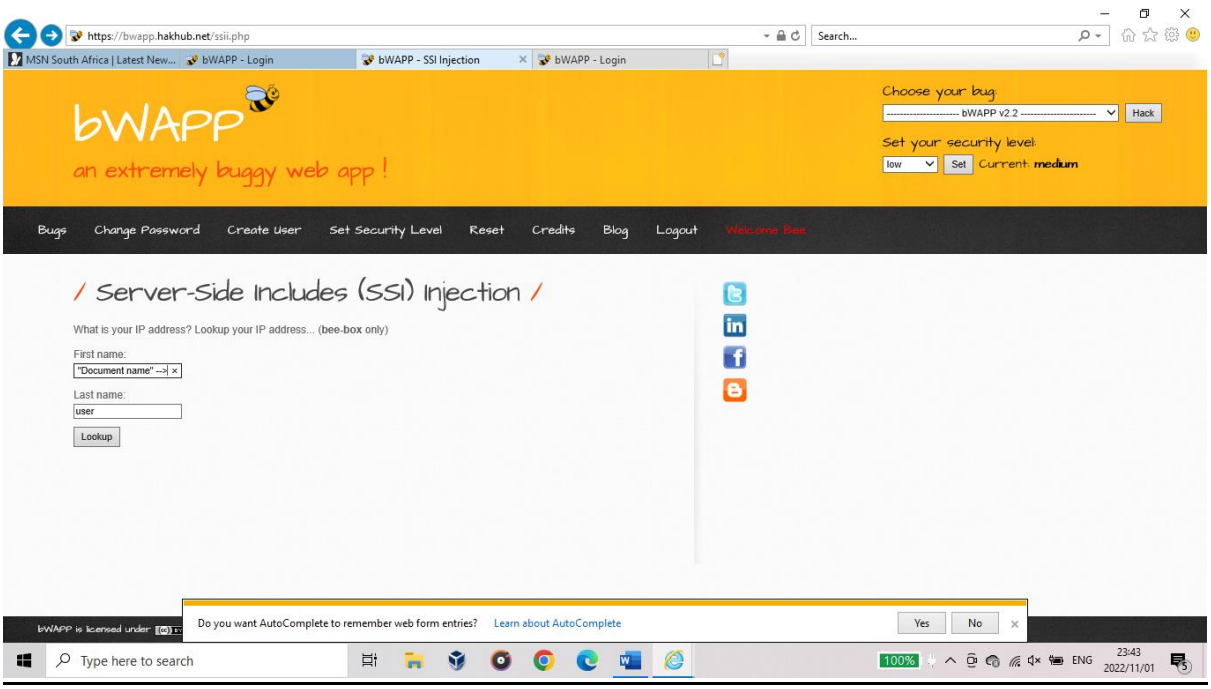



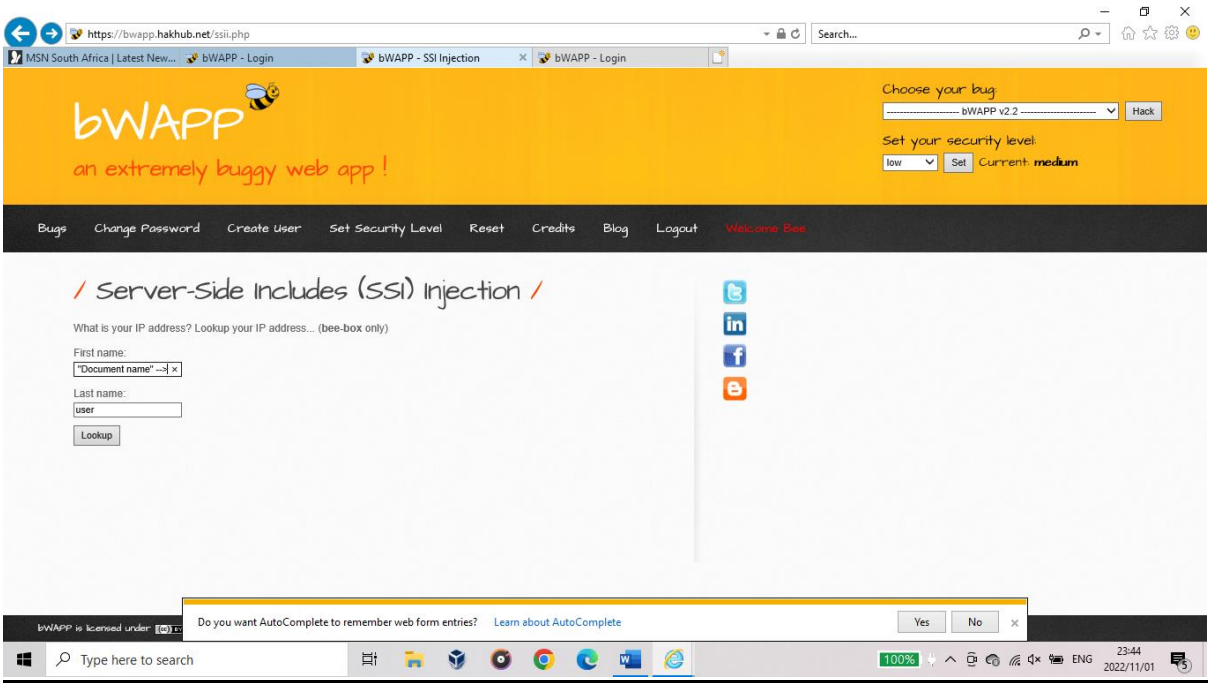

## Task 4 perform server-side includes injection attack(SSI)


https://bwapp.hakhub.net/portal.php
bWAPP - Portal
bWAPP - Login
bWAPP
an extremely buggy web app !
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
/ 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
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
ENG
23:40
2022/11/01

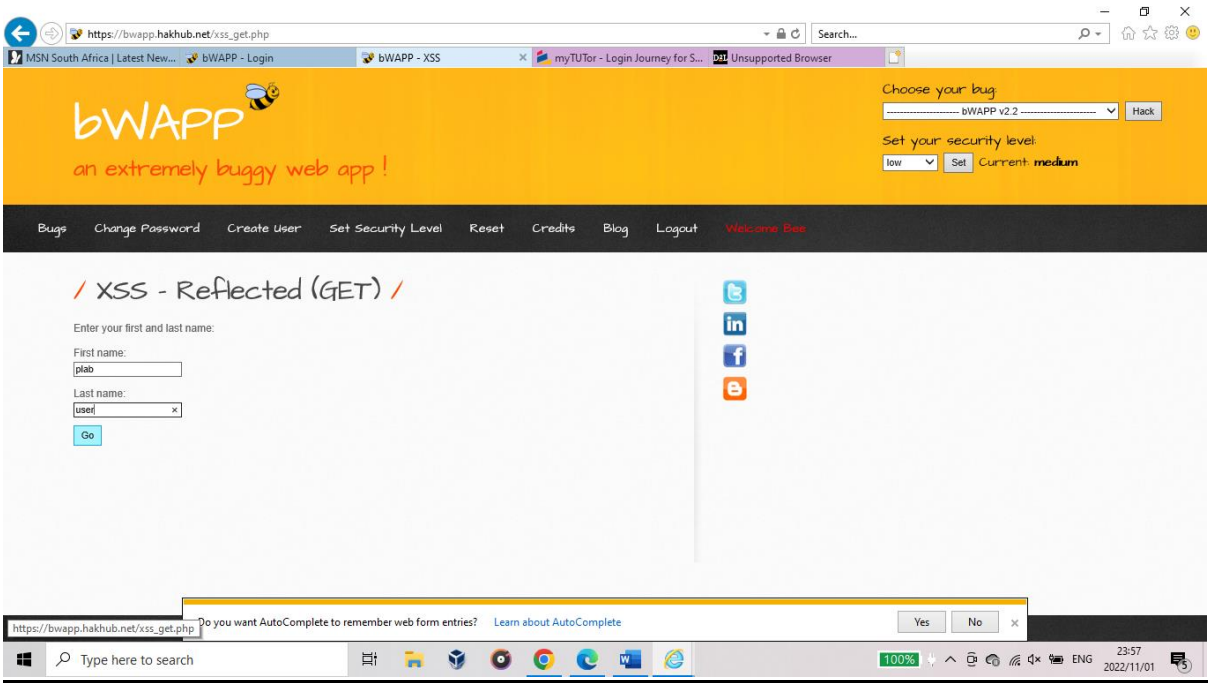

https://bwapp.hakhub.net/ssii.php
bWAPP - SSI Injection
bWAPP - Login
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Server-Side Includes (SSI) Injection /
What is your IP address? Lookup your IP address... (bee-box only)
First name:
>alert("Hacked")</script>
Last name:
user
Lookup
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
ENG
23:41
2022/11/01

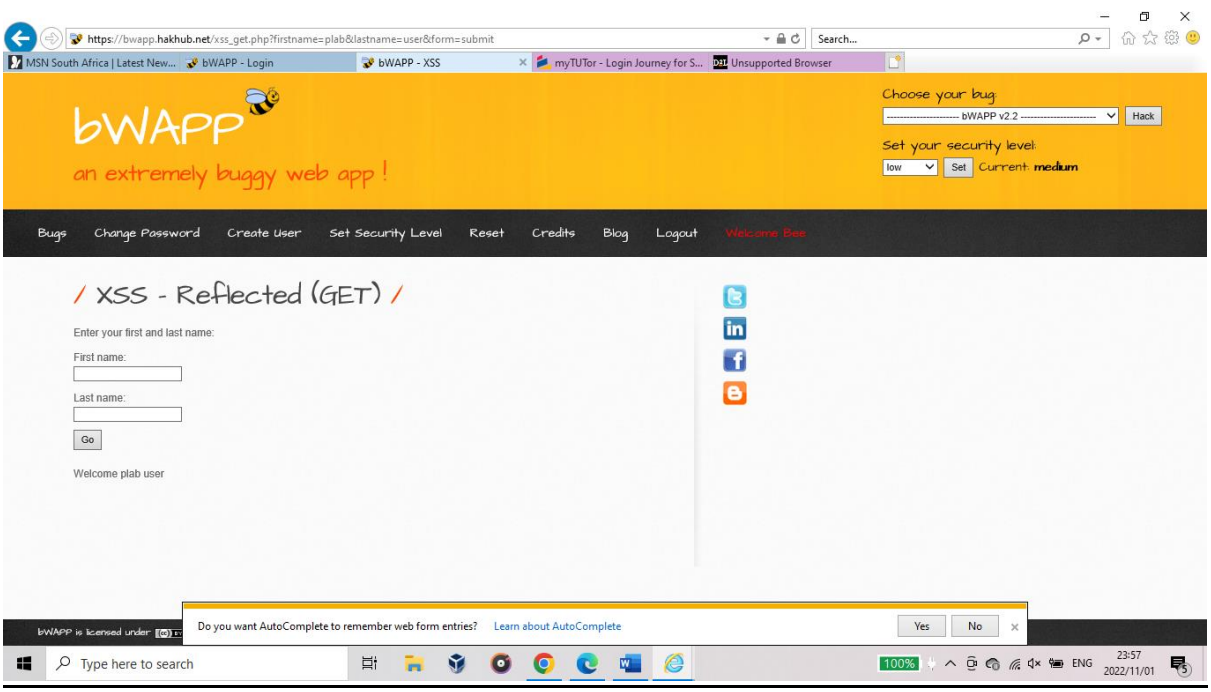

https://bwapp.hakhub.net/ssii.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - SSI Injection
bWAPP - Login
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Server-Side Includes (SSI) Injection /
What is your IP address? Lookup your IP address... (bee-box only)
First name:
>cument.cookie)</script>
Last name:
user
Lookup
https://bwapp.hakhub.net/ssii.php
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

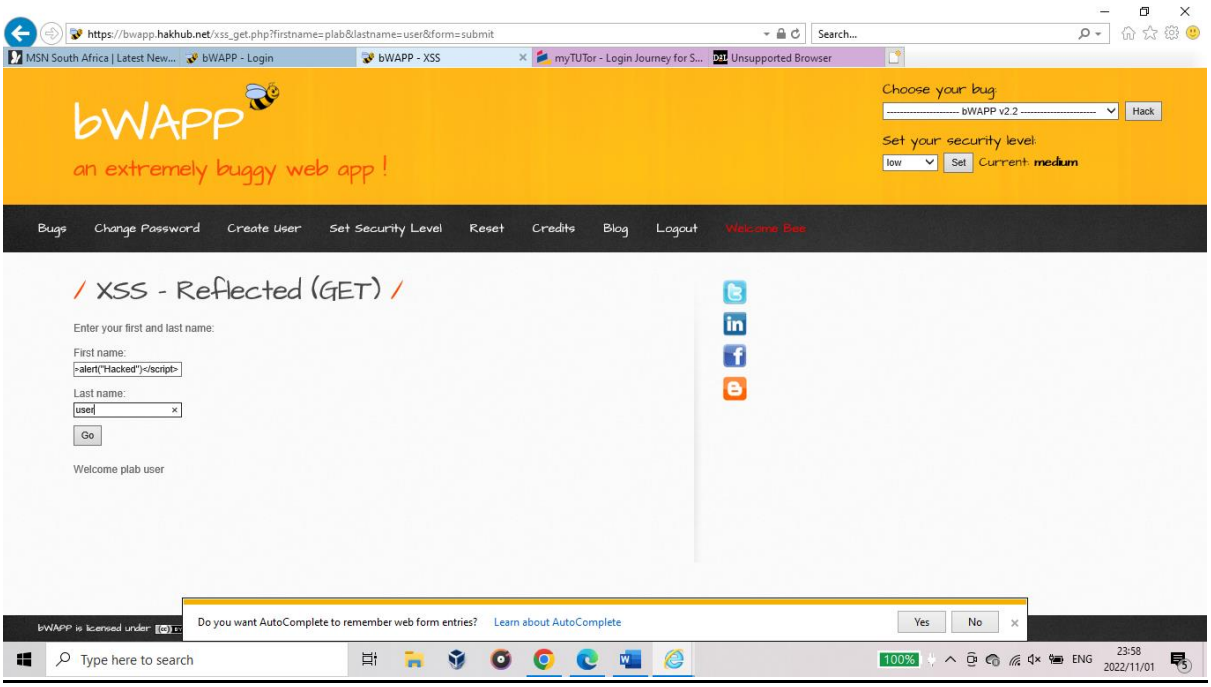

https://bwapp.hakhub.net/ssii.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - SSI Injection
bWAPP - Login
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Server-Side Includes (SSI) Injection /
What is your IP address? Lookup your IP address... (bee-box only)
First name:
"Document name" --></script>
Last name:
user
Lookup
bWAPP is licensed under
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

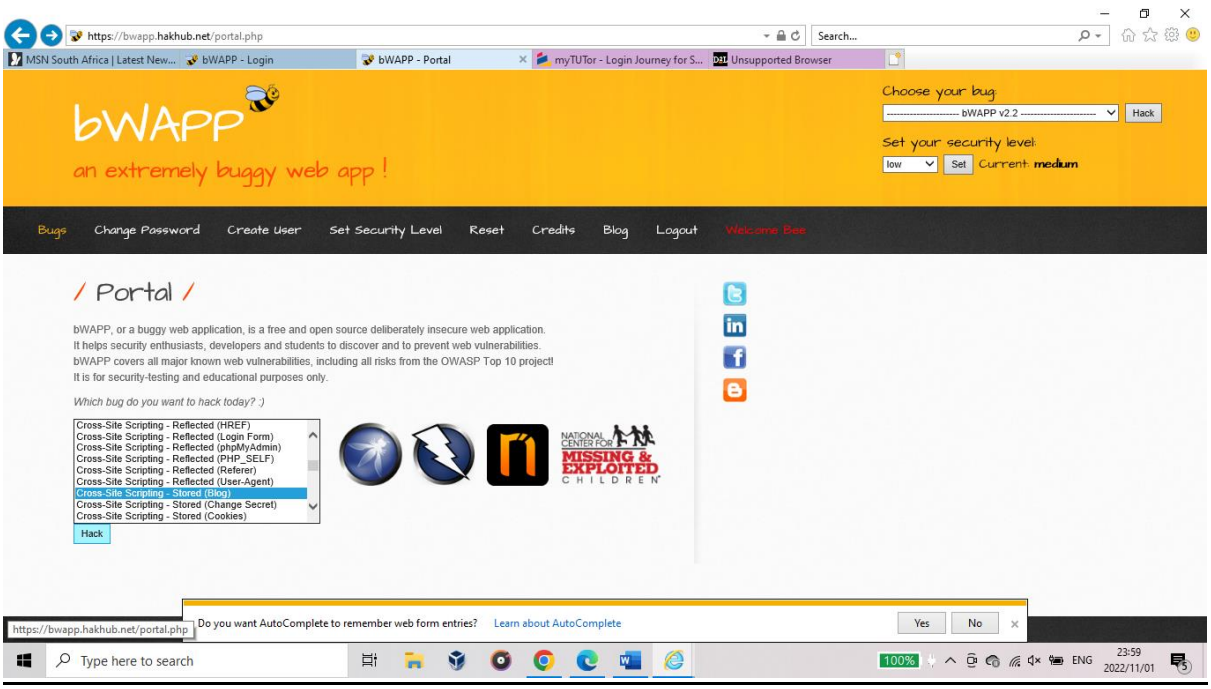


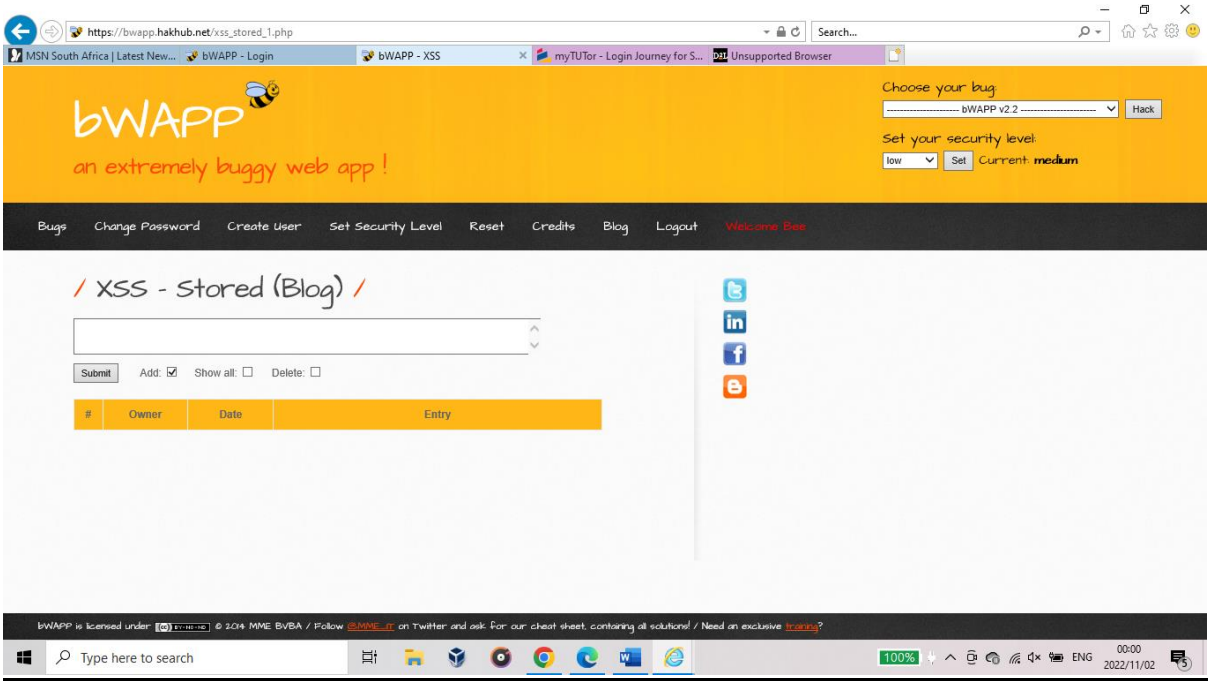

# Task 5 Perform cross-site Scripting Attack


https://bwapp.hakhub.net/xss_get.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - XSS
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
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
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
plab
Last name:
user
Go
https://bwapp.hakhub.net/xss_get.php
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:57
2022/11/01


https://bwapp.hakhub.net/xss_get.php?firstname=plab&lastname=user&form=submit
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - XSS
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
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
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome plab user
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:57
2022/11/01

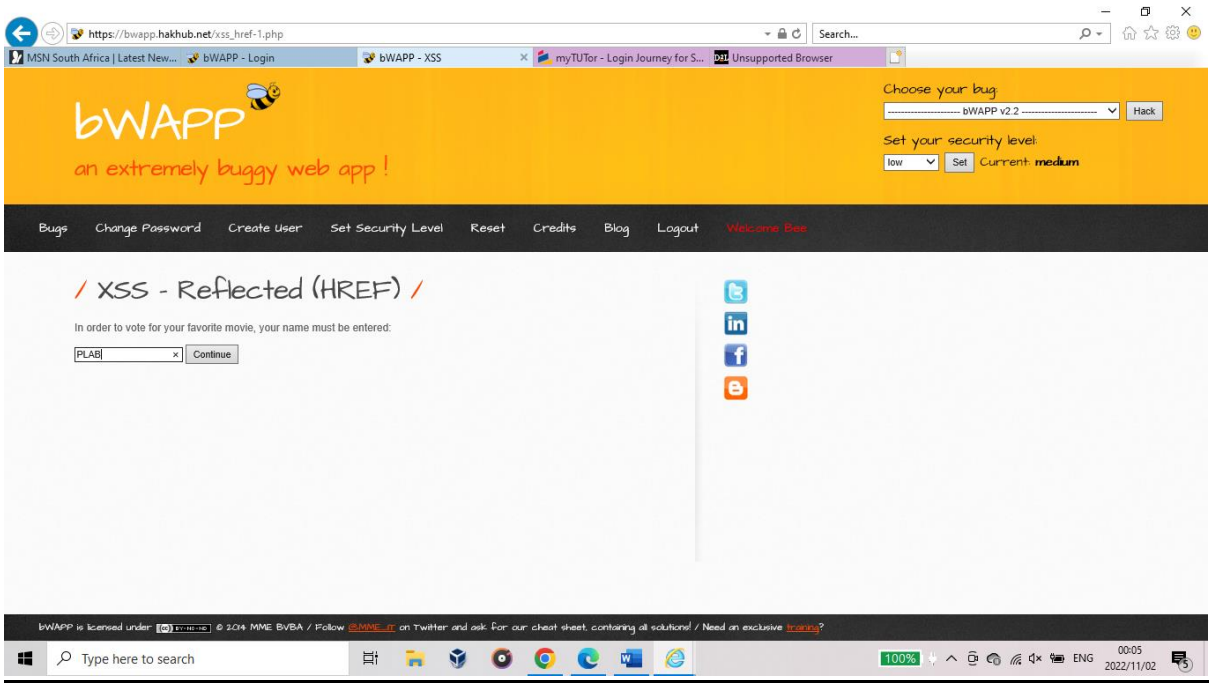

https://bwapp.hakhub.net/xss_get.php?firstname=plab&lastname=user&form=submit
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - XSS
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
>alert("Hacked")</script>
Last name:
user
Go
Welcome plab user
bWAPP is licensed under
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:58
2022/11/01

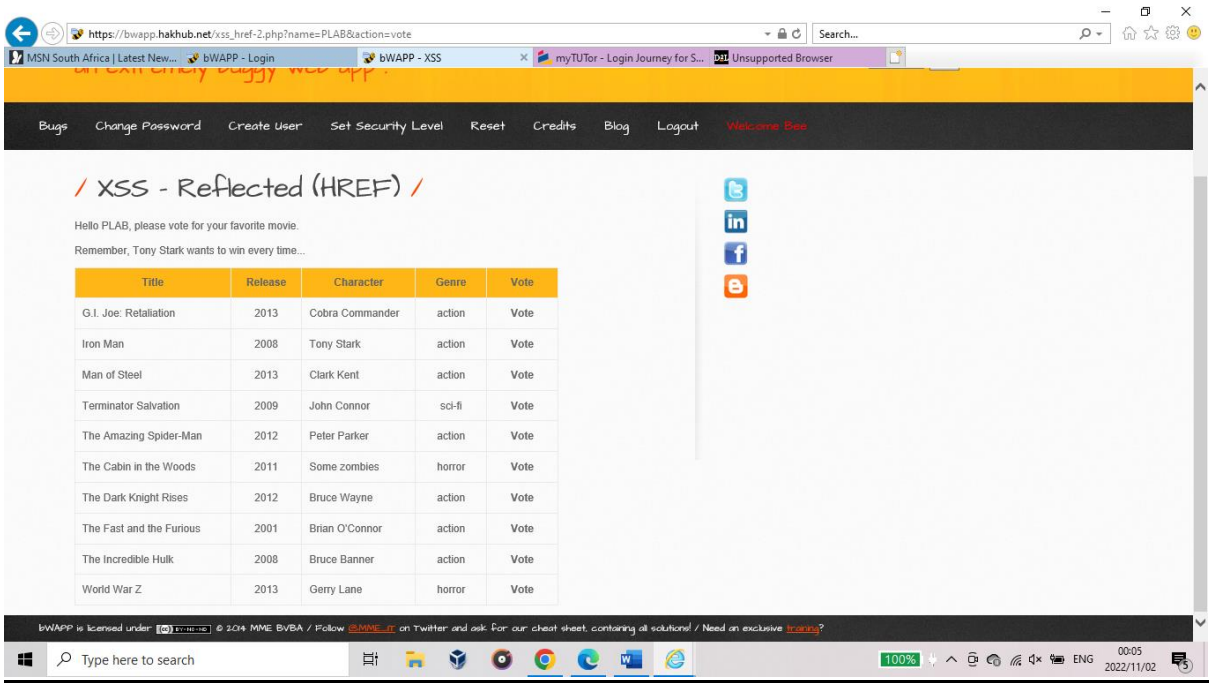

https://bwapp.hakhub.net/portal.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - Portal
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ 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 (HREF)
Cross-Site Scripting - Reflected (Login Form)
Cross-Site Scripting - Reflected (phpMyAdmin)
Cross-Site Scripting - Reflected (PHP_SELF)
Cross-Site Scripting - Reflected (Referer)
Cross-Site Scripting - Reflected (User-Agent)
Cross-Site Scripting - Stored (Blog)
Cross-Site Scripting - Stored (Change Secret)
Cross-Site Scripting - Stored (Cookies)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
https://bwapp.hakhub.net/portal.php
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
23:59
2022/11/01

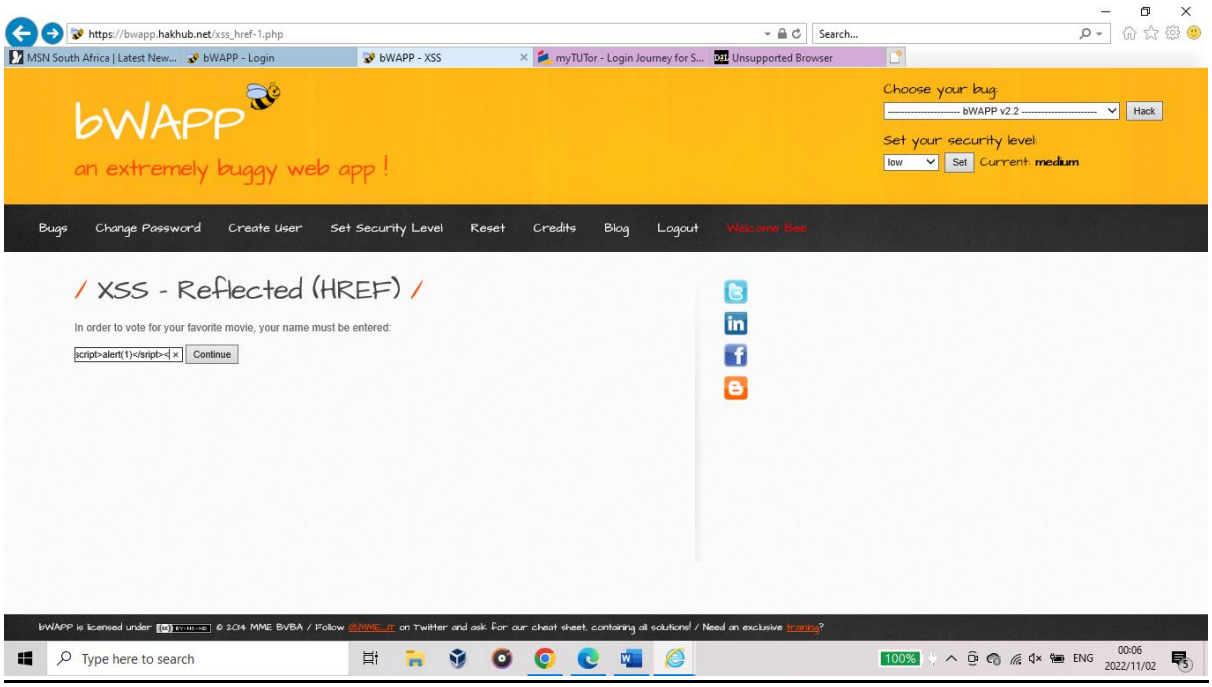


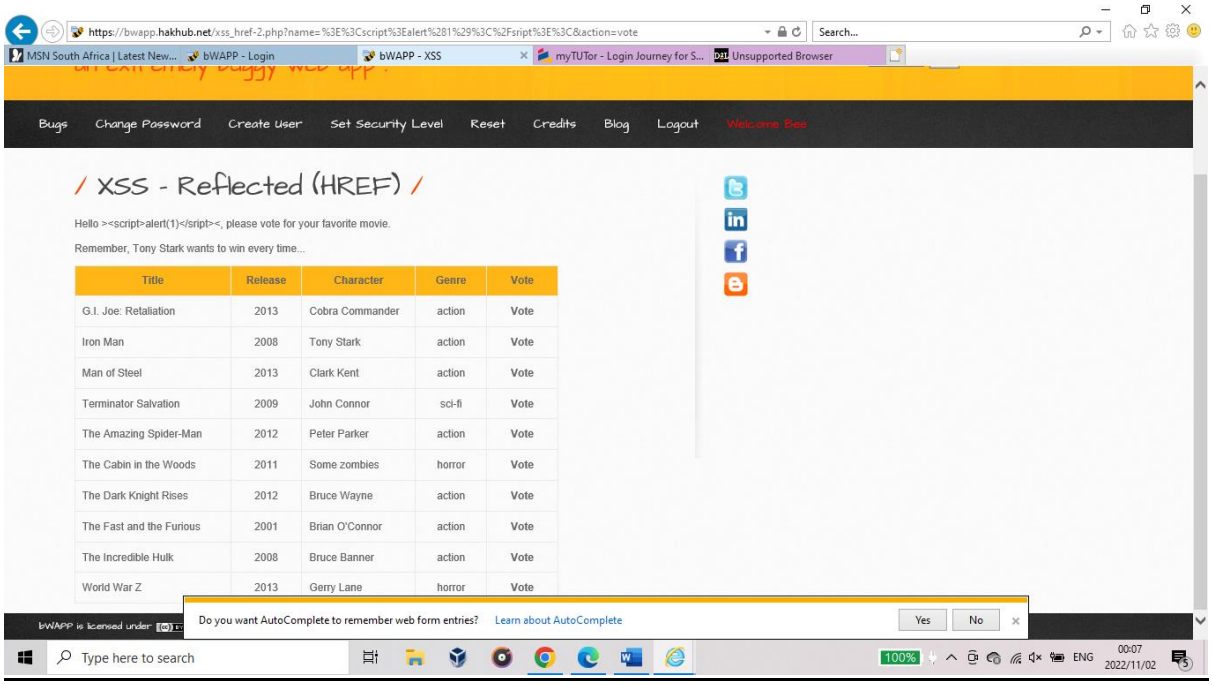

## Task 6 Perform cross-site scripting(Xss)-Reflected(HREF)Attack


https://bwapp.hakhub.net/portal.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - Portal
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
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
/ 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 (Login Form)
Cross-Site Scripting - Reflected (phpMyAdmin)
Cross-Site Scripting - Reflected (PHP_SELF)
Cross-Site Scripting - Reflected (Referer)
Cross-Site Scripting - Reflected (User-Agent)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
https://bwapp.hakhub.net/portal.php
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
00:04
2022/11/02


https://bwapp.hakhub.net/xss_href-1.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - XSS
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
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
/ XSS - Reflected (HREF) /
In order to vote for your favorite movie, your name must be entered:
PLAB
Continue
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
00:05
2022/11/02


https://bwapp.hakhub.net/xss_href-2.php?name=PLAB&action=vote
Search...
MSN South Africa | Latest New...
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_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
00:05
2022/11/02


https://bwapp.hakhub.net/xss_href-1.php
Search...
MSN South Africa | Latest New...
bWAPP - Login
bWAPP - XSS
myTUTor - Login Journey for S...
Unsupported Browser
bWAPP
an extremely buggy web app !
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
/ XSS - Reflected (HREF) /
In order to vote for your favorite movie, your name must be entered:
<script>alert(1)</script><
Continue
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Type here to search
100%
ENG
00:06
2022/11/02


https://bwapp.hakhub.net/xss_href-2.php?name=%3E%3Cscript%3Ealert%281%29%3C%2Fsript%3E%3C&action=vote
Search...
MSN South Africa | Latest New...
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 ><script>alert(1)</sript><, 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
Do you want AutoComplete to remember web form entries?
Learn about AutoComplete
Yes
No
Type here to search
100%
ENG
00:07
2022/11/02