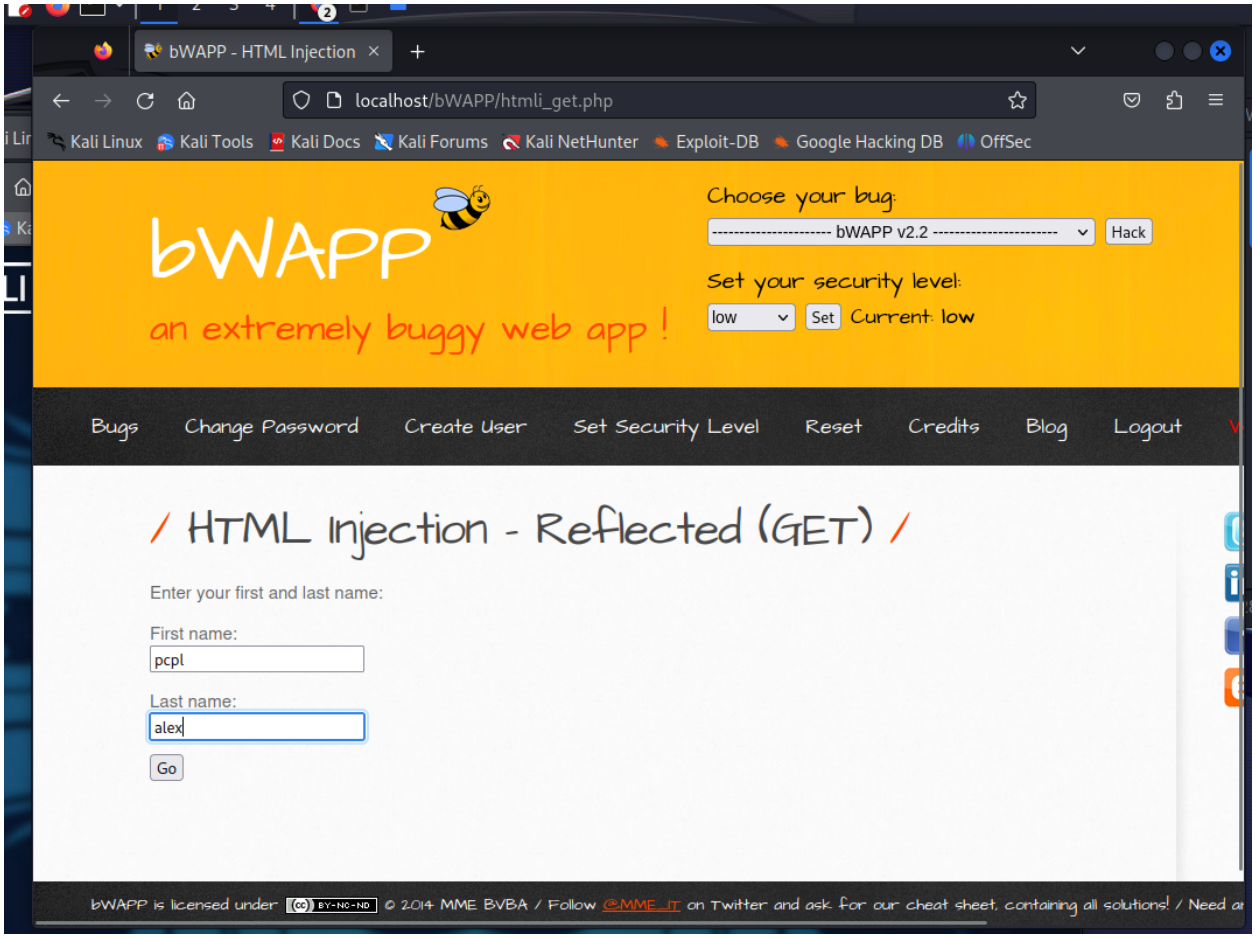
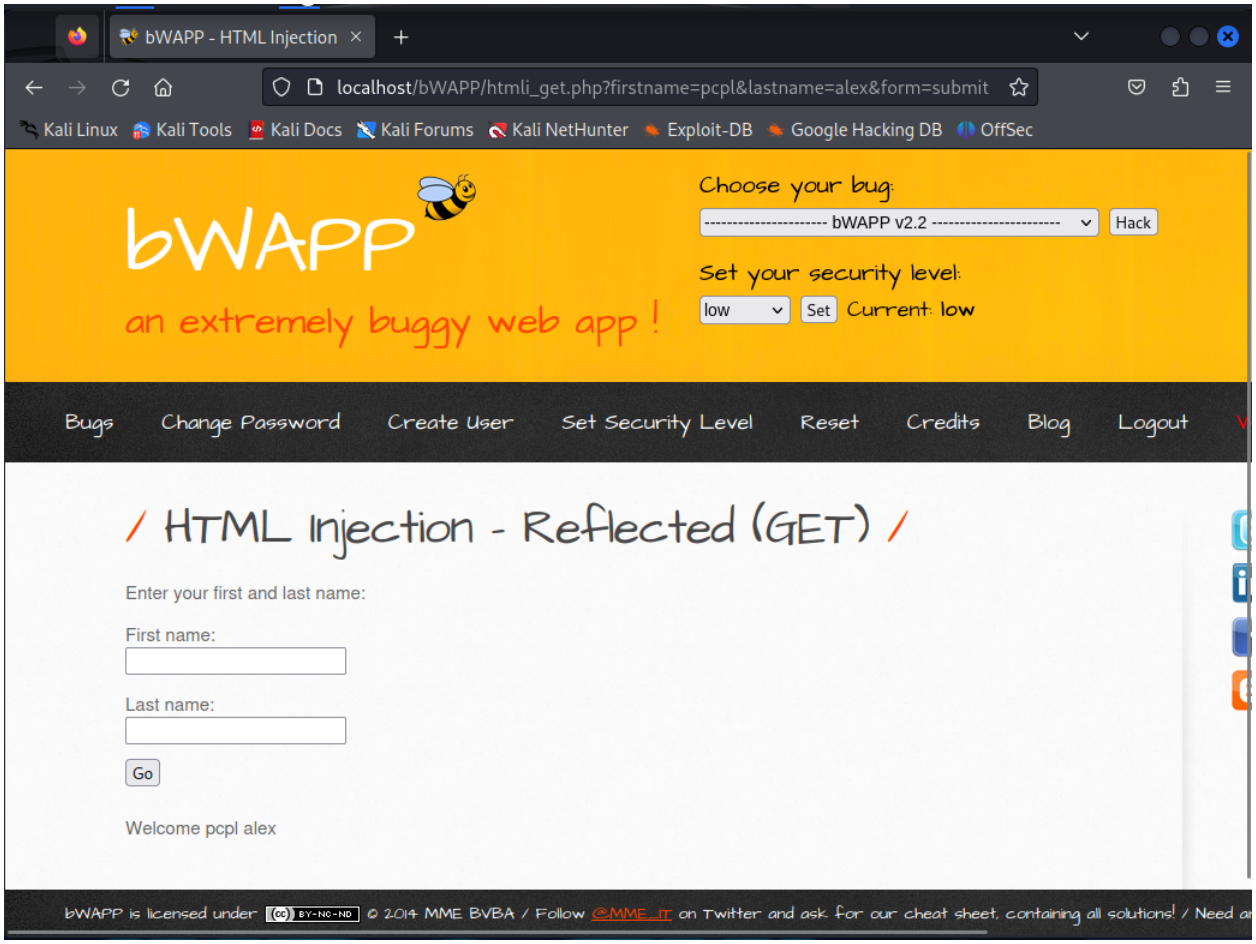
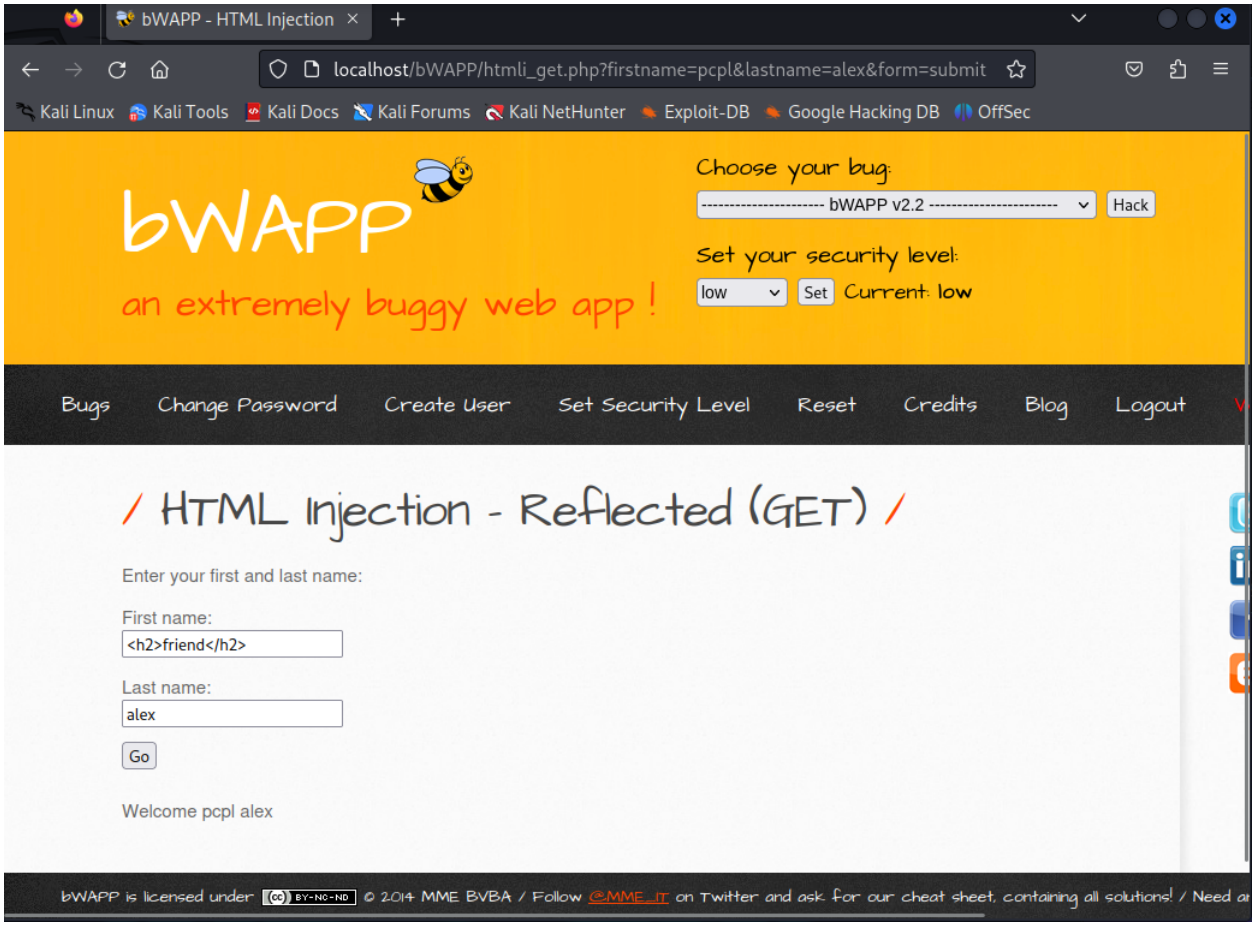
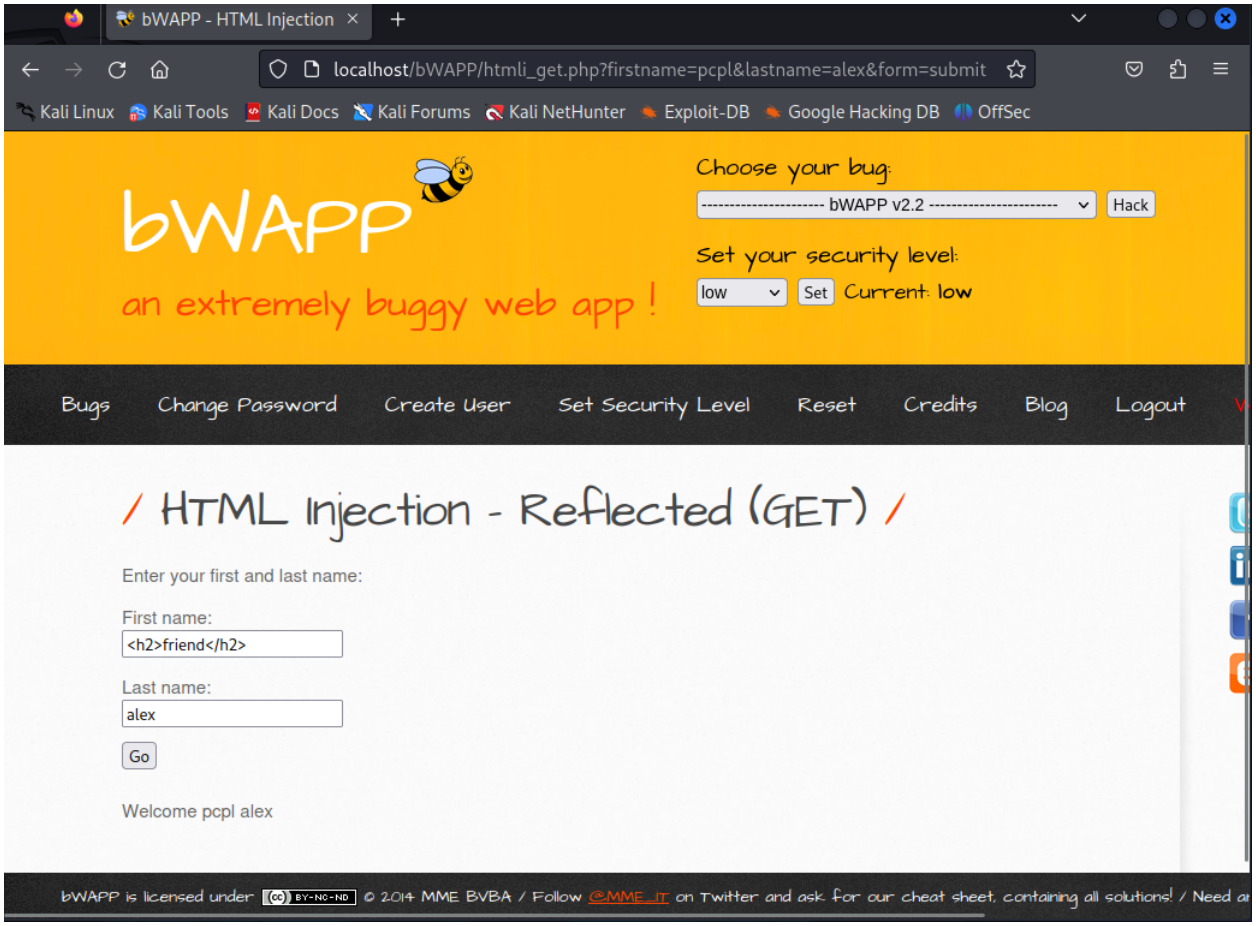
1)**Vulnerability Name**:HTML Injection
CWE:CWE-79
OWASP Category:A7-Cross Site Scripting
Description:The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
Business Impact:It can cause various losses to the organization like financial losses reputation damage,legal issues and operational disruptions. It can also make the system vulnerable to various attacks like Session hijacking and phishing etc.
Vulnerability Path:localhost/bWAPP/htmli_get.php
Vulnerability Parameter:localhost/bWAPP/htmli_get.php
Steps to reproduce:

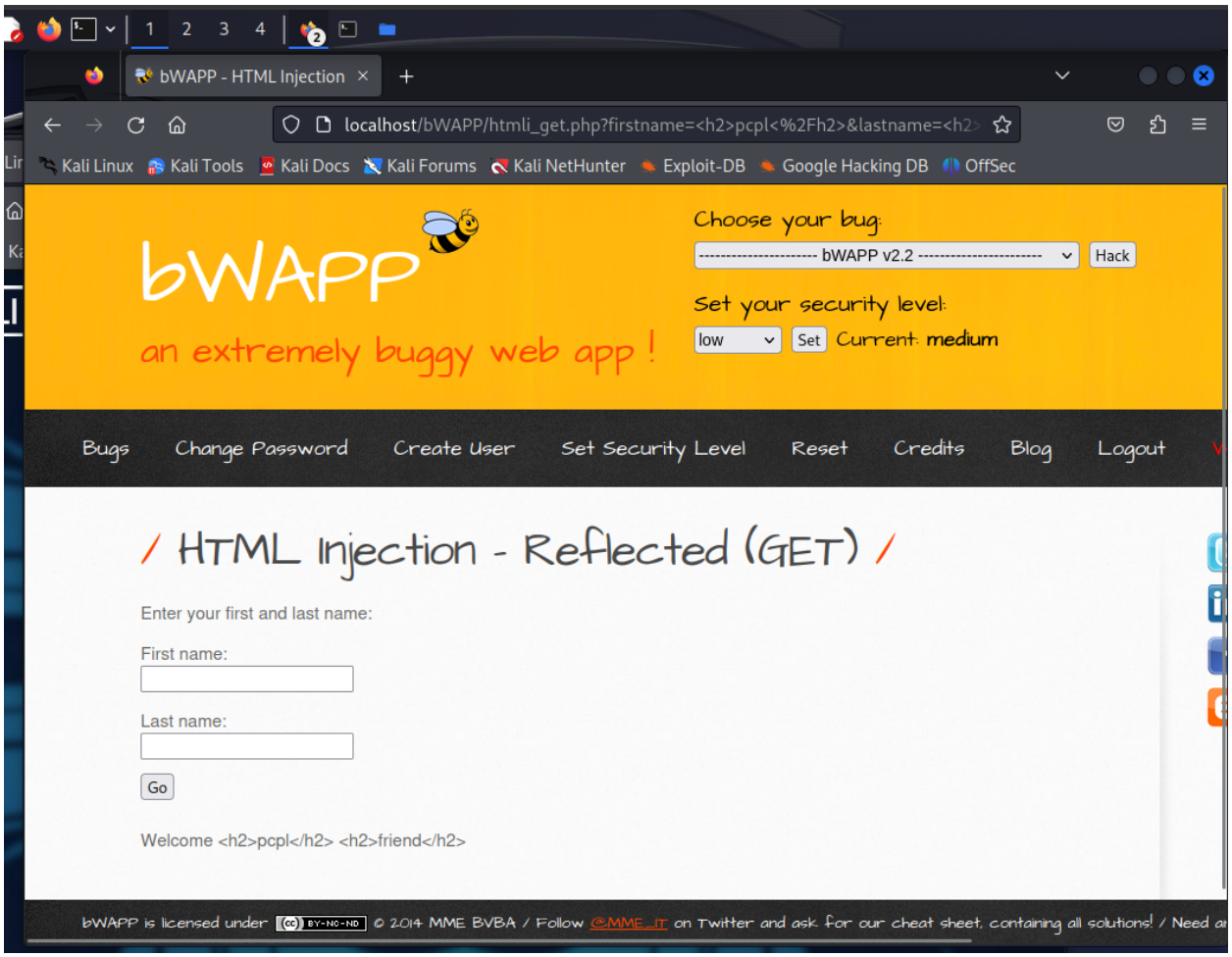

bWAPP - Portal
localhost/bWAPP/portal.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Portal /
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.
Which bug do you want to hack today? :)
---------- bWAPP v2.2 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
bWAPP is licensed under BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

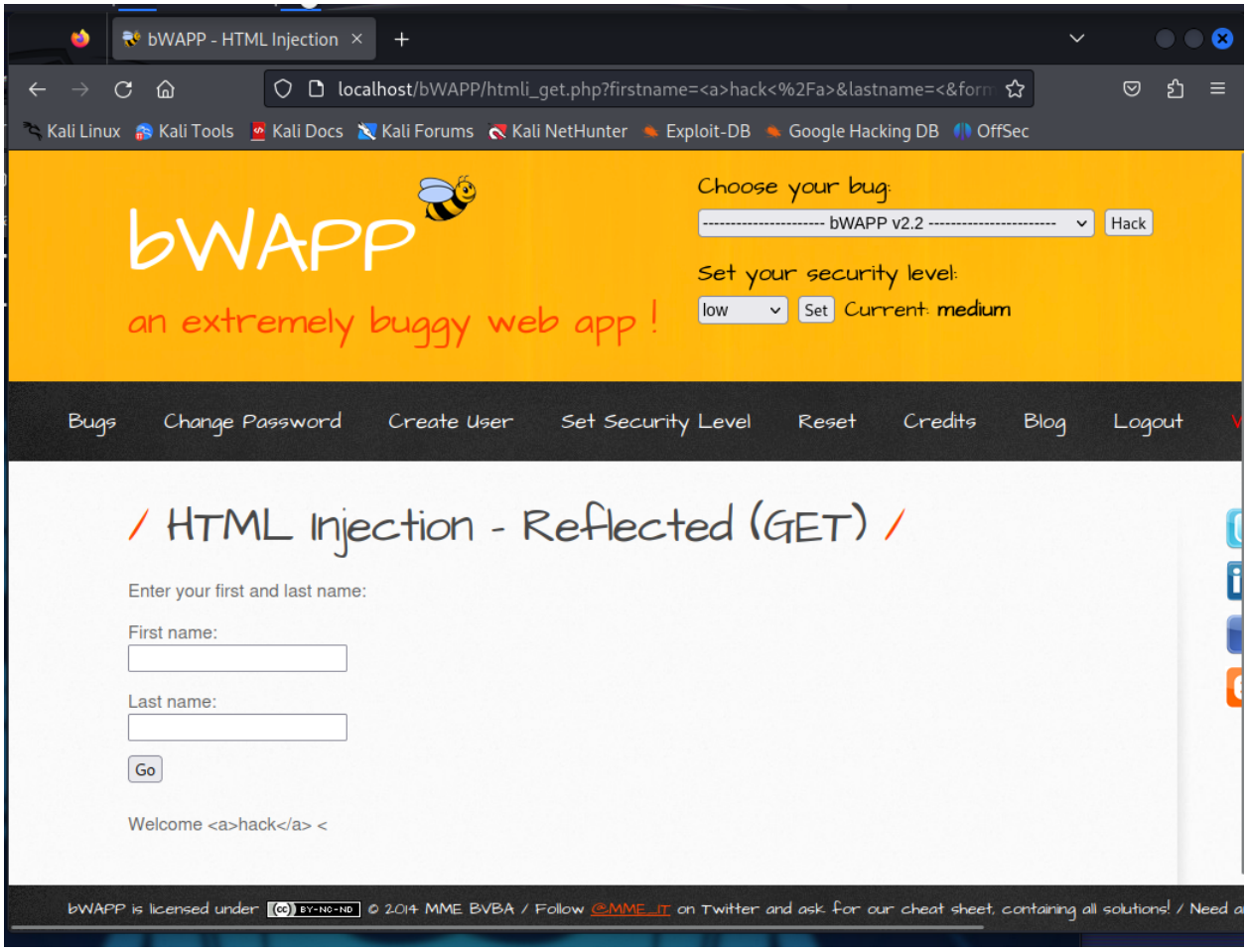

bWAPP - HTML Injection
localhost/bWAPP/htmli_get.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
pcpl
Last name:
alex
Go
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a


bWAPP - HTML Injection
localhost/bWAPP/htmli_get.php?firstname=pcpl&lastname=alex&form=submit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome pcpl alex
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

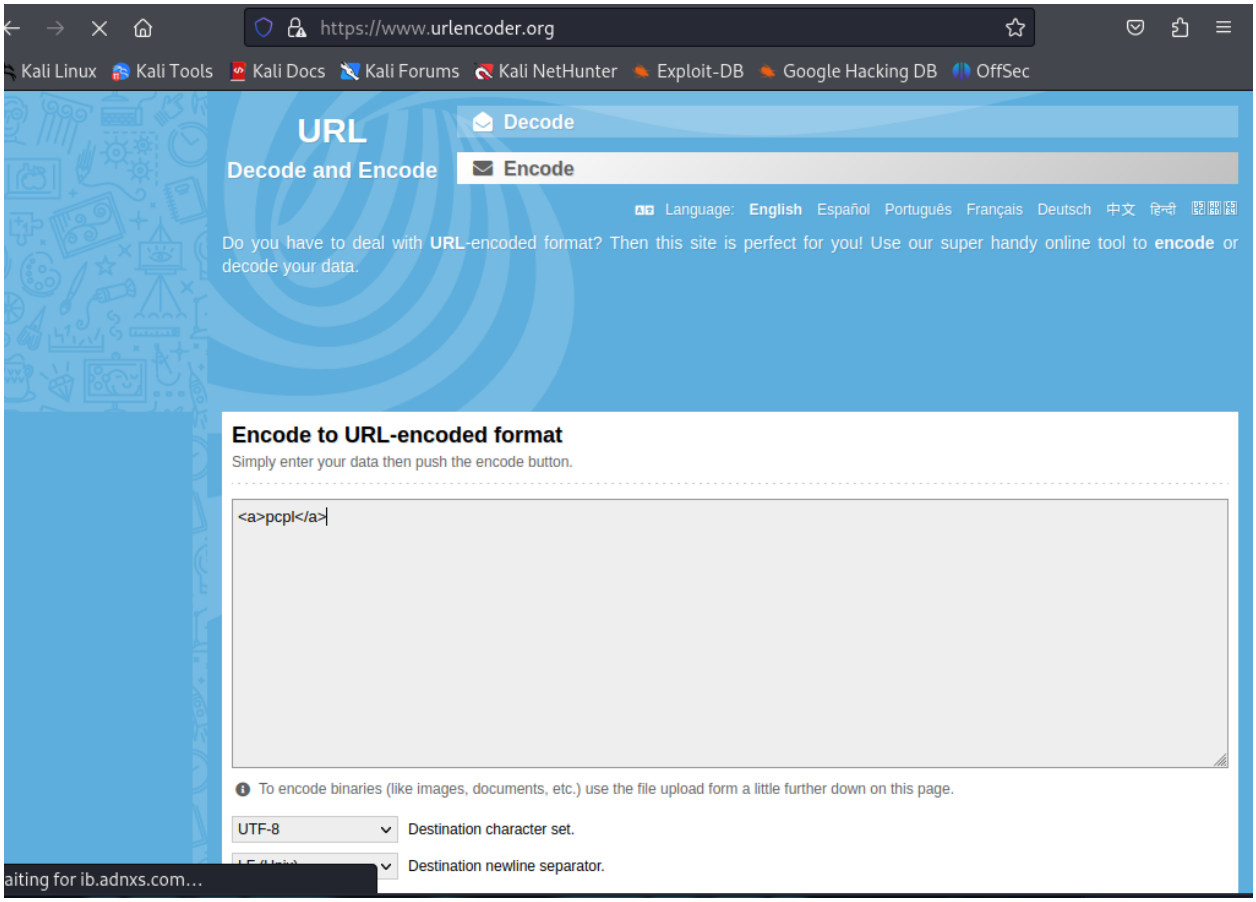

bWAPP - HTML Injection
localhost/bWAPP/htmli_get.php?firstname=pcpl&lastname=alex&form=submit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
<h2>friend</h2>
Last name:
alex
Go
Welcome pcpl alex
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

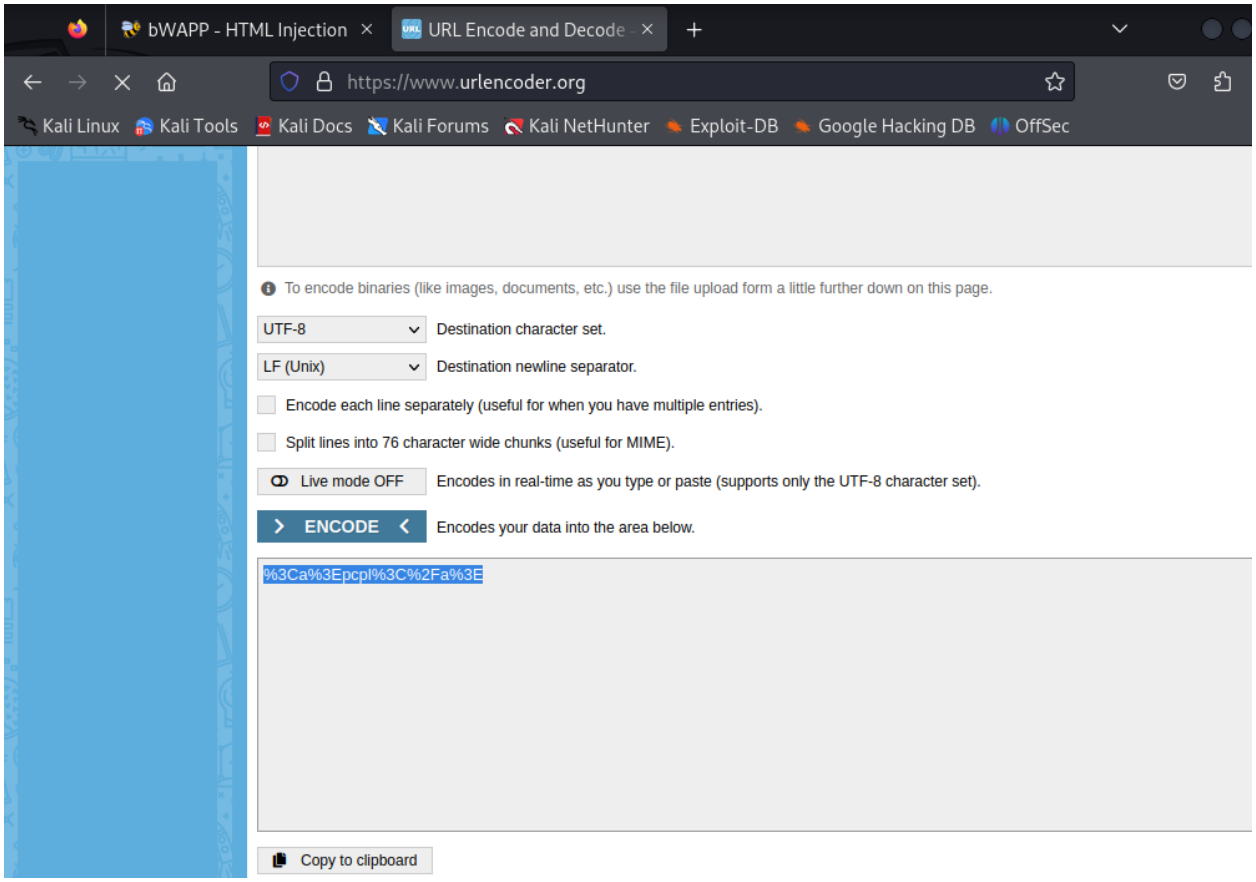

bWAPP - HTML Injection
localhost/bWAPP/htmli_get.php?firstname=pcpl&lastname=alex&form=submit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
<h2>friend</h2>
Last name:
alex
Go
Welcome pcpl alex
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

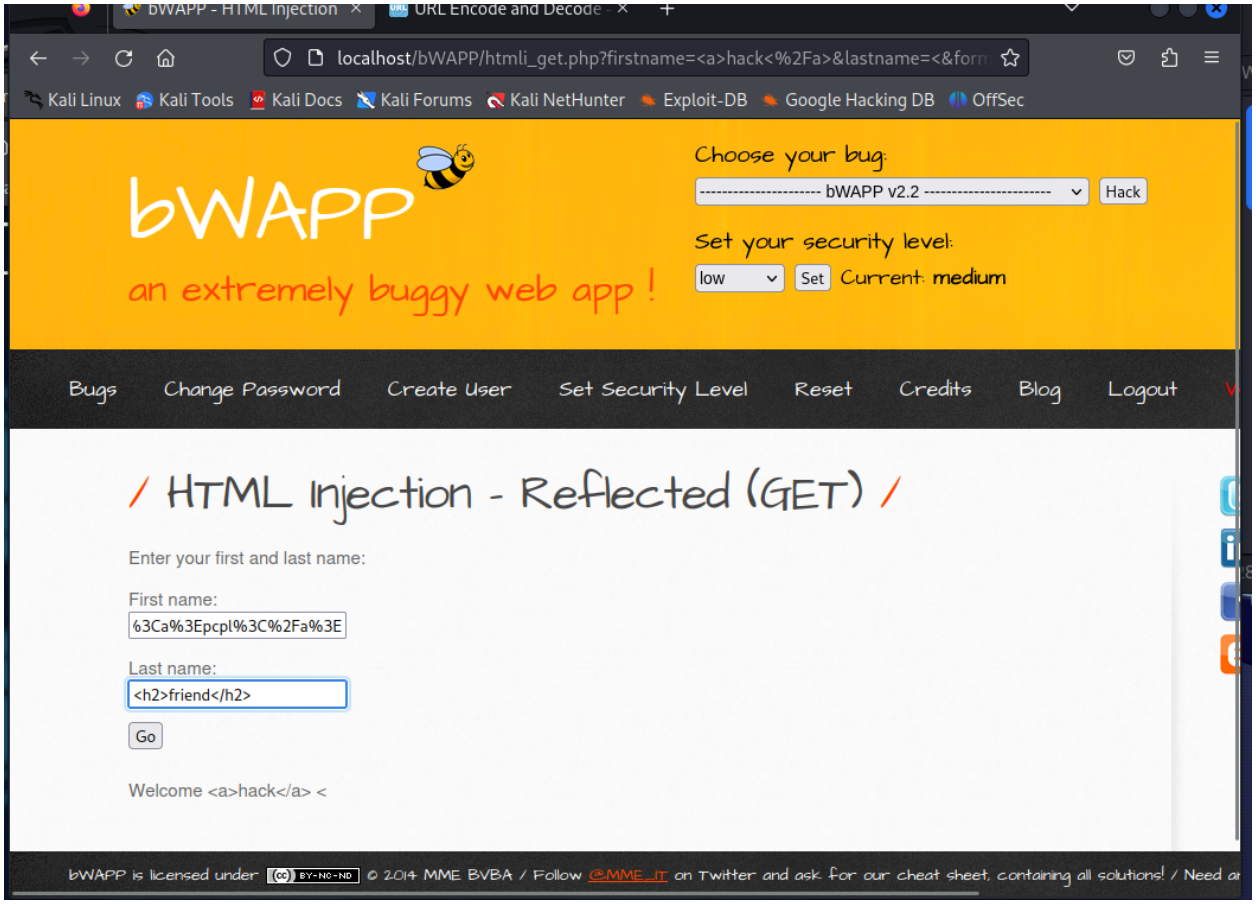

bWAPP - HTML Injection
localhost/bWAPP/htmli_get.php?firstname=<h2>pcpl<%2Fh2>&lastname=<h2>
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome <h2>pcpl</h2> <h2>friend</h2>
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

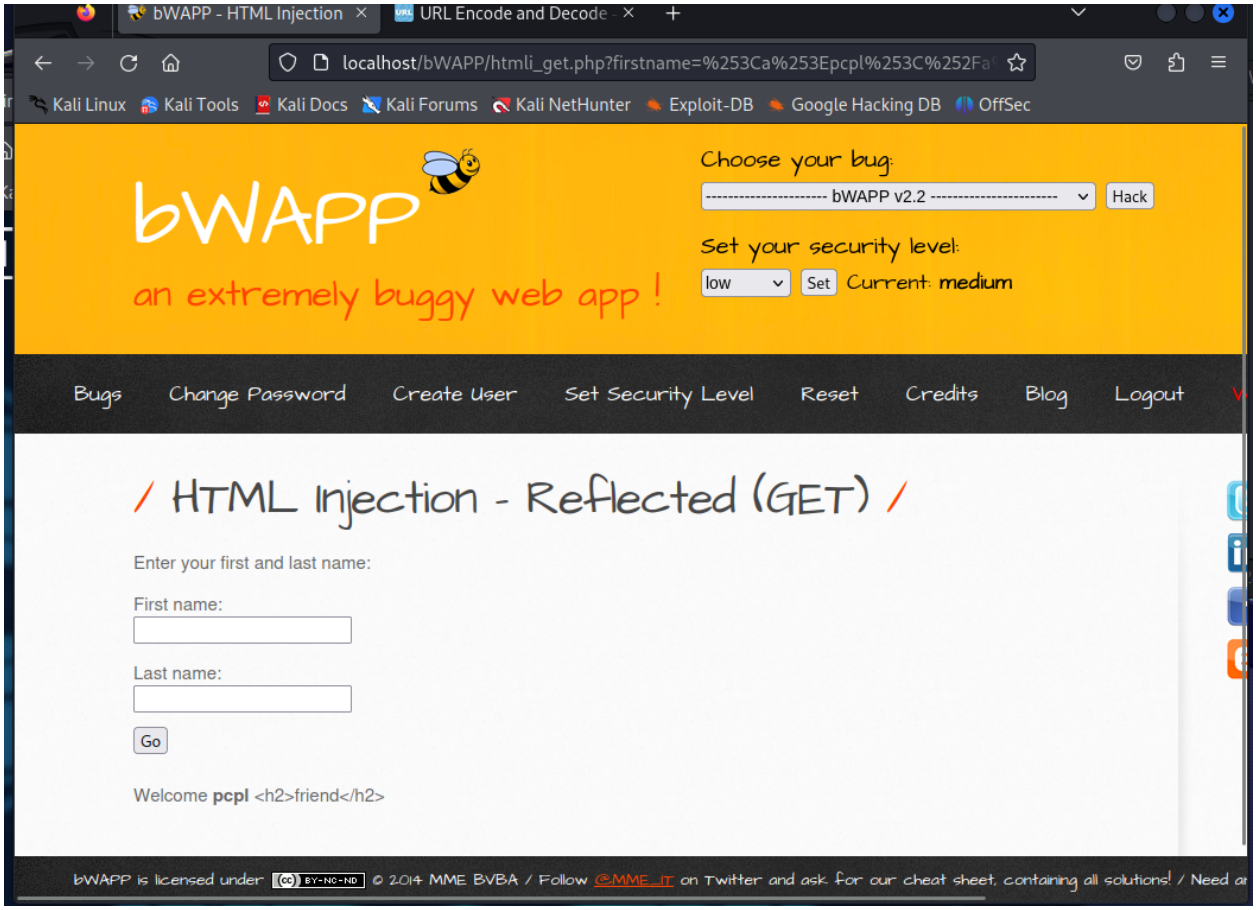


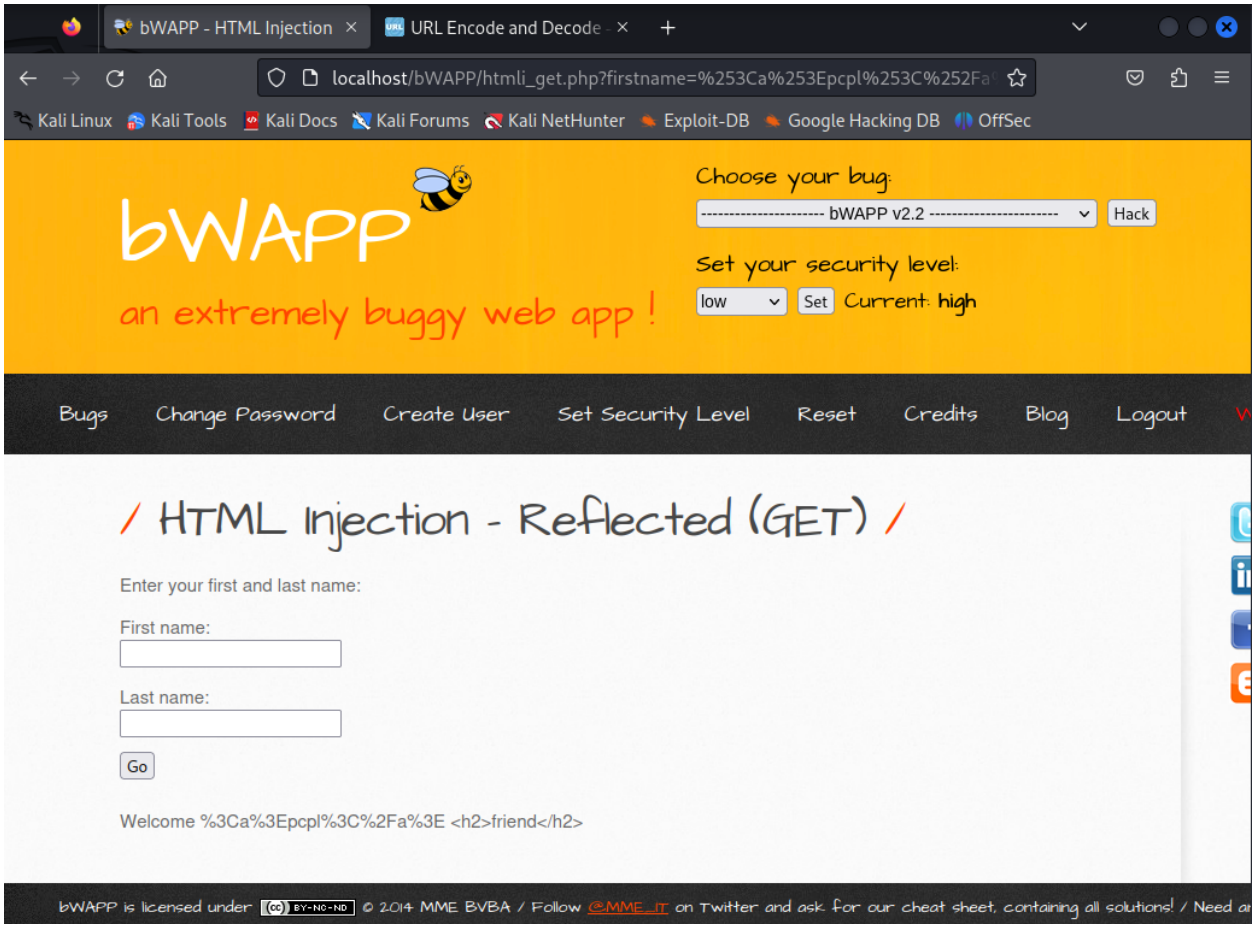
With URL Encoding

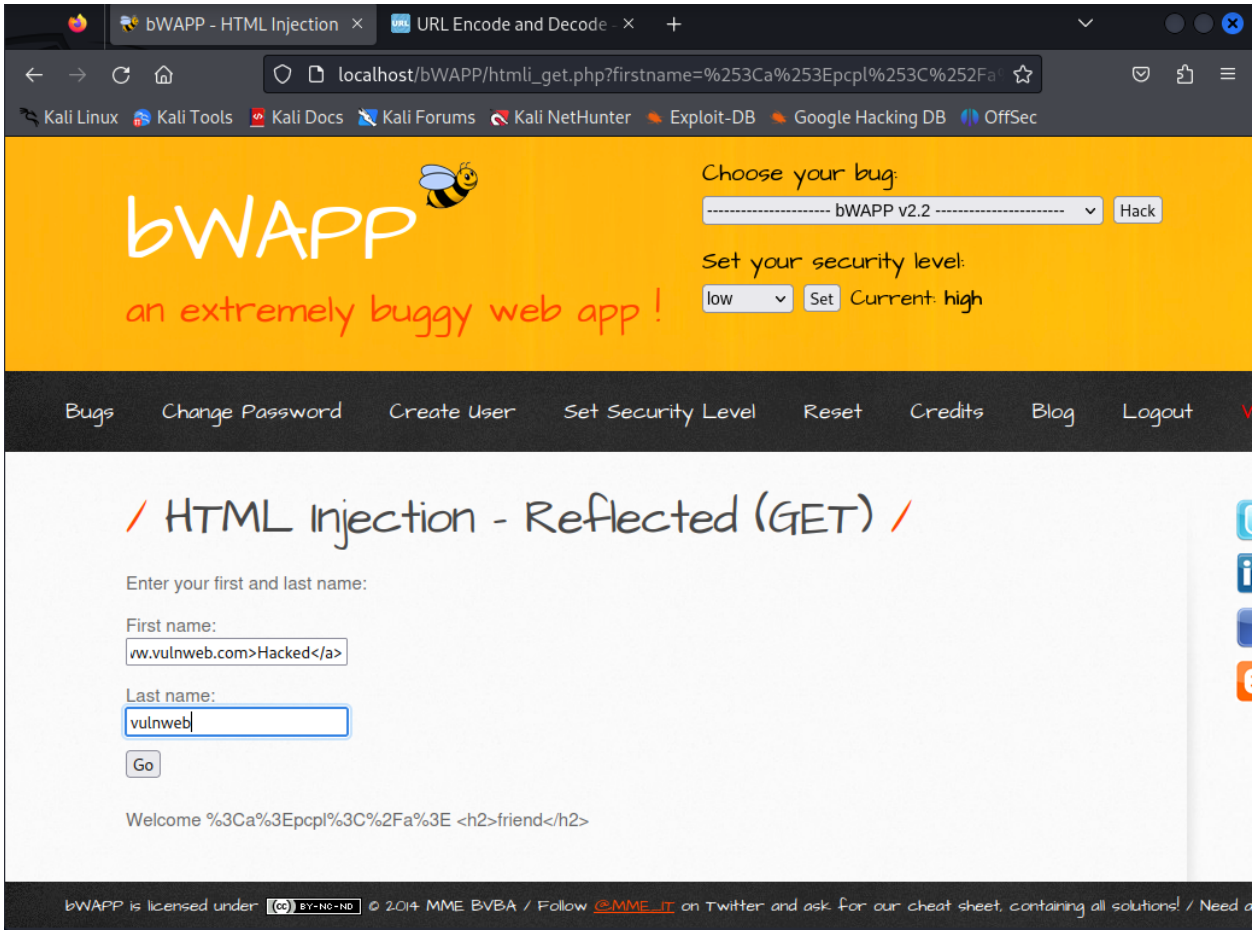

https://www.urlencoder.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
URL
Decode and Encode
Decode
Encode
Language: English Español Português Français Deutsch 中文 हिन्दी
Do you have to deal with URL-encoded format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.
Encode to URL-encoded format
Simply enter your data then push the encode button.
<a>pcpl
To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Destination character set.
Destination newline separator.
aiting for ib.adnxs.com…


bWAPP - HTML Injection
URL Encode and Decode
https://www.urlencoder.org
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Destination character set.
LF (Unix)
Destination newline separator.
Encode each line separately (useful for when you have multiple entries).
Split lines into 76 character wide chunks (useful for MIME).
Live mode OFF
Encodes in real-time as you type or paste (supports only the UTF-8 character set).
ENCODE
Encodes your data into the area below.
%3Ca%3Epcpl%3C%2Fa%3E
Copy to clipboard


bWAPP - HTML Injection
URL Encode and Decode
localhost/bWAPP/htmli_get.php?firstname=<a>hack<%2Fa>&lastname=<&form
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
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
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
%3Ca%3Epcpl%3C%2Fa%3E
Last name:
<h2>friend</h2>
Go
Welcome <a>hack <
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a


bWAPP - HTML Injection
URL Encode and Decode
localhost/bWAPP/htmli_get.php?firstname=%253Ca%253Epcpl%253C%252Fa
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
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
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome pcpl <h2>friend</h2>
bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a


bWAPP - HTML Injection
URL Encode and Decode
localhost/bWAPP/htmli_get.php?firstname=%253Ca%253Epcpl%253C%252Fa
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: high
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ HTML Injection - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome %3Ca%3Epcpl%3C%2Fa%3E <h2>friend</h2>
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a



2)**Vulnerability Name**:iFrame Injection
CWE:CWE-829
OWASP Category:A1-2021-Injection
Description:When including third-party functionality, such as a web widget, library, or other source of functionality, the product must effectively trust that functionality. Without sufficient protection mechanisms, the functionality could be malicious in

nature (either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source). The functionality might also contain its own weaknesses, or grant access to additional functionality and state information that should be kept private to the base system, such as system state information, sensitive application data, or the DOM of a web application.

Business Impact:It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruptions. This makes the websites vulnerable to various attacks like Phishing, Data Leakage, Malware Distribution

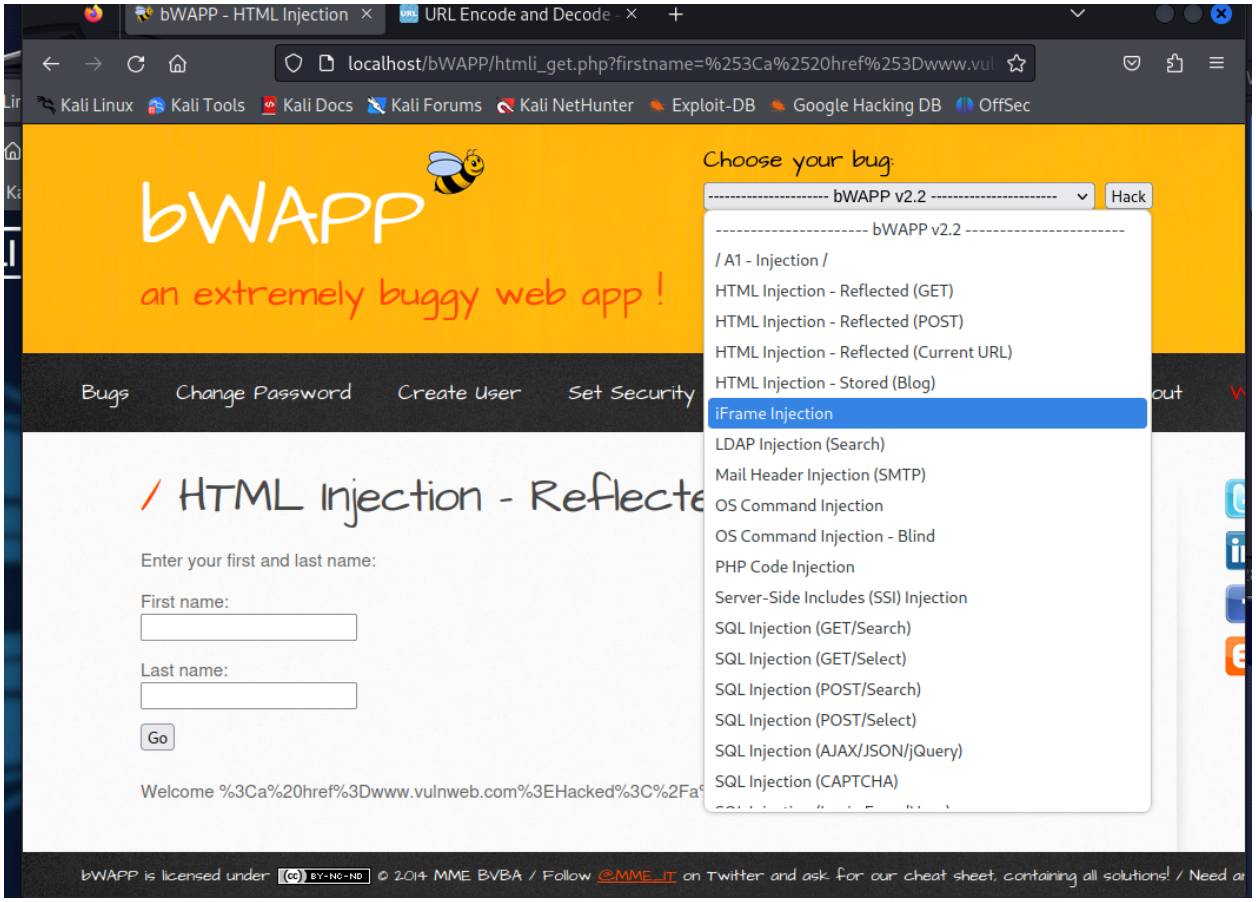
Vulnerability Path:

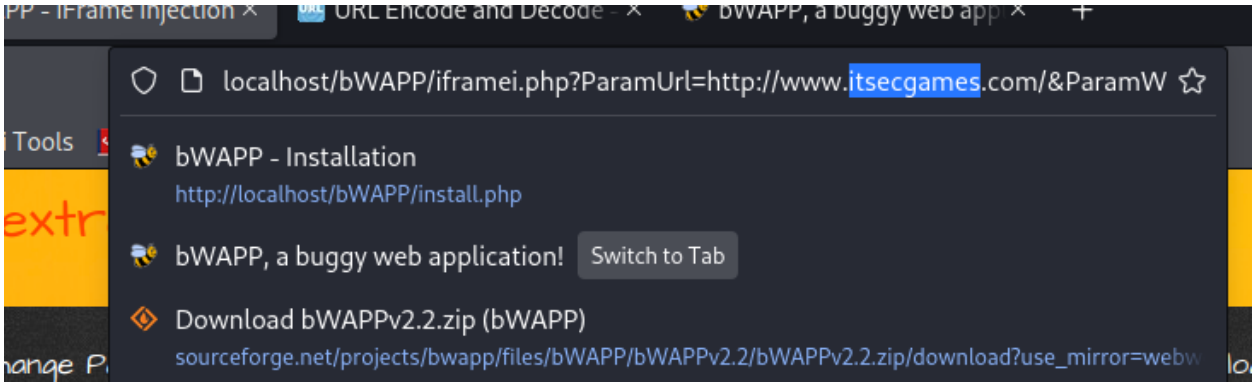
localhost/bWAPP/iframe.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeoghts=250

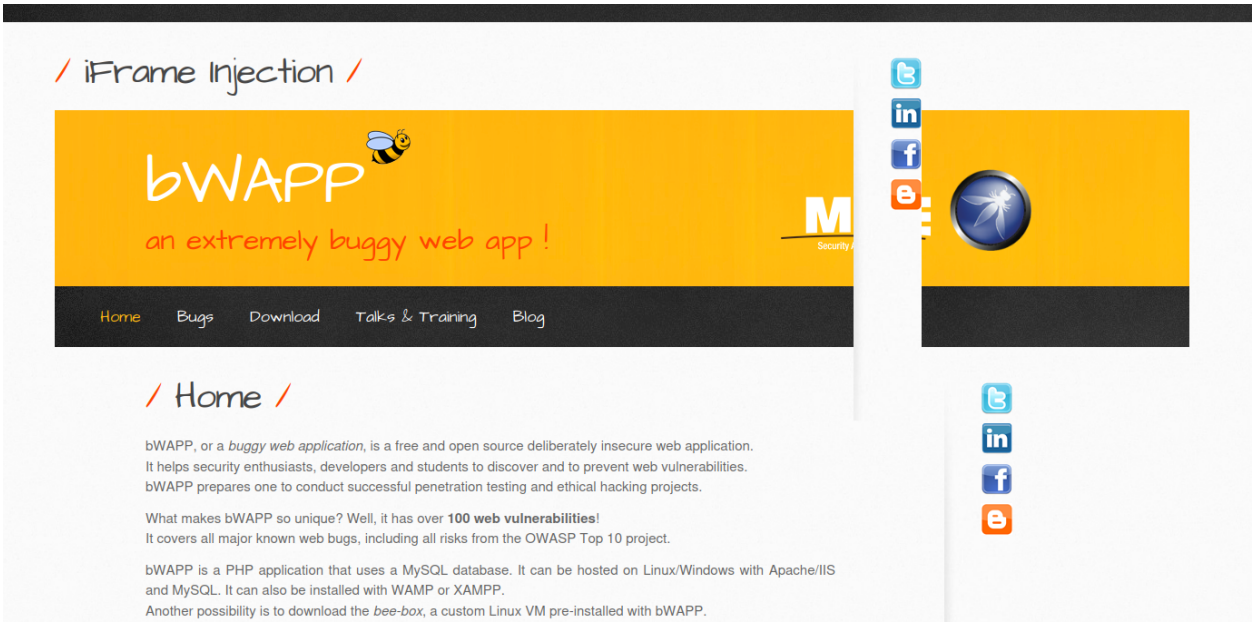
Vulnerability Parameter:

localhost/bWAPP/iframe.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeoghts=250

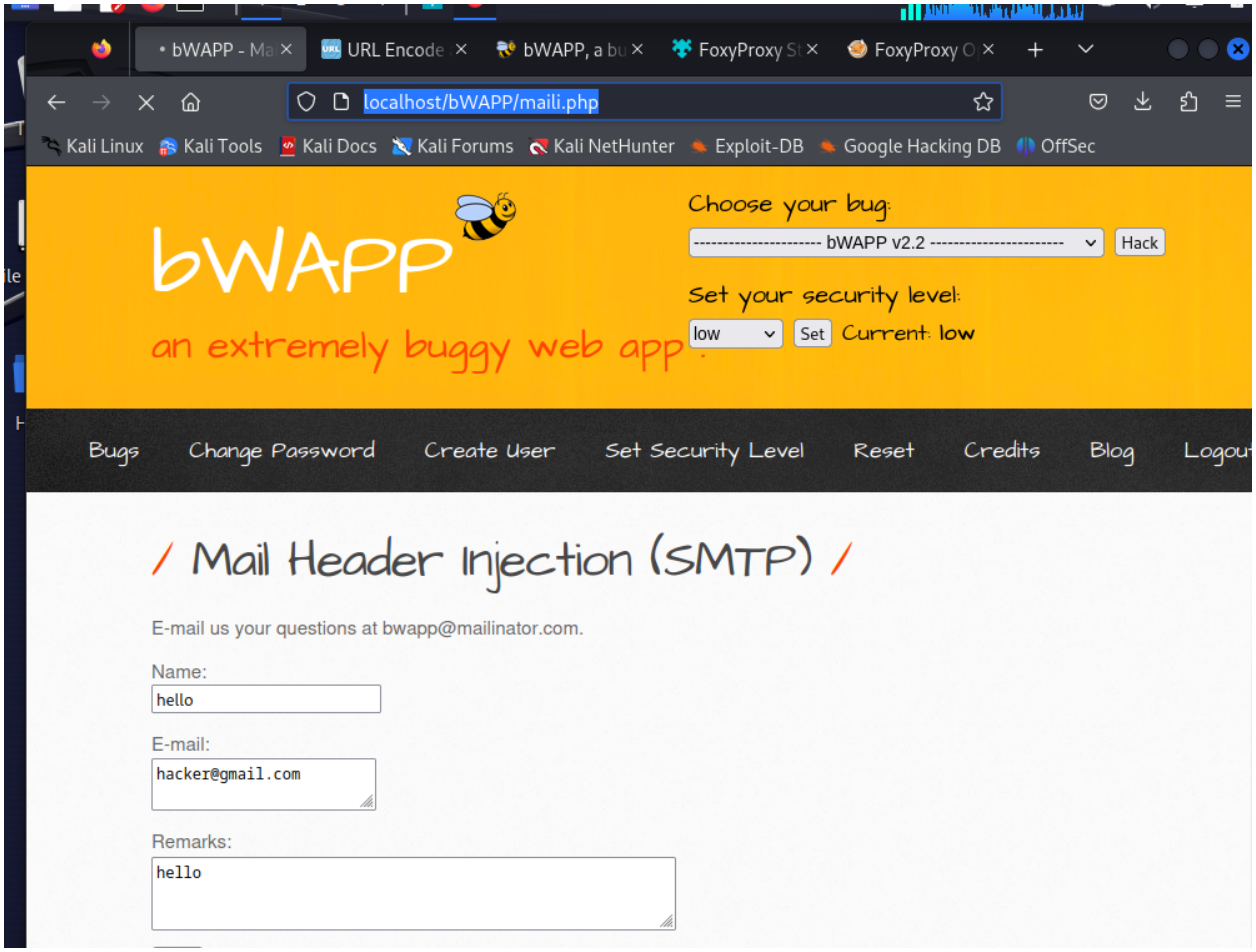
Steps to reproduce:

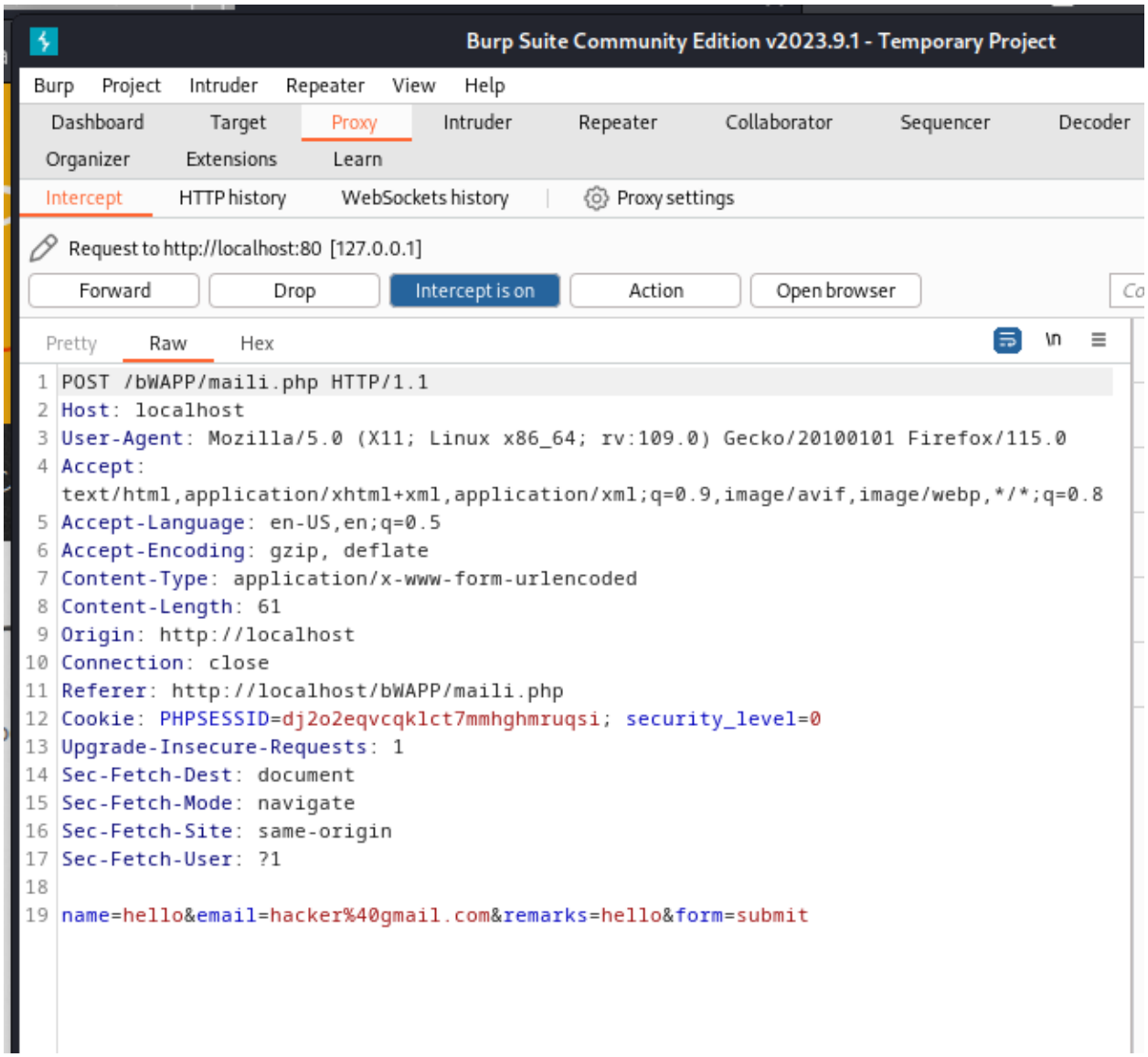

bWAPP - HTML Injection
URL Encode and Decode
localhost/bWAPP/htmli_get.php?firstname=%253Ca%2520href%253Dwww.vul
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
---------- bWAPP v2.2 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
OS Command Injection
OS Command Injection - Blind
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)
SQL Injection (GET/Select)
SQL Injection (POST/Search)
SQL Injection (POST/Select)
SQL Injection (AJAX/JSON/jQuery)
SQL Injection (CAPTCHA)
Bugs
Change Password
Create User
Set Security
/ HTML Injection - Reflecte
Enter your first and last name:
First name:
Last name:
Go
Welcome %3Ca%20href%3Dwww.vulnweb.com%3EHacked%3C%2Fa
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

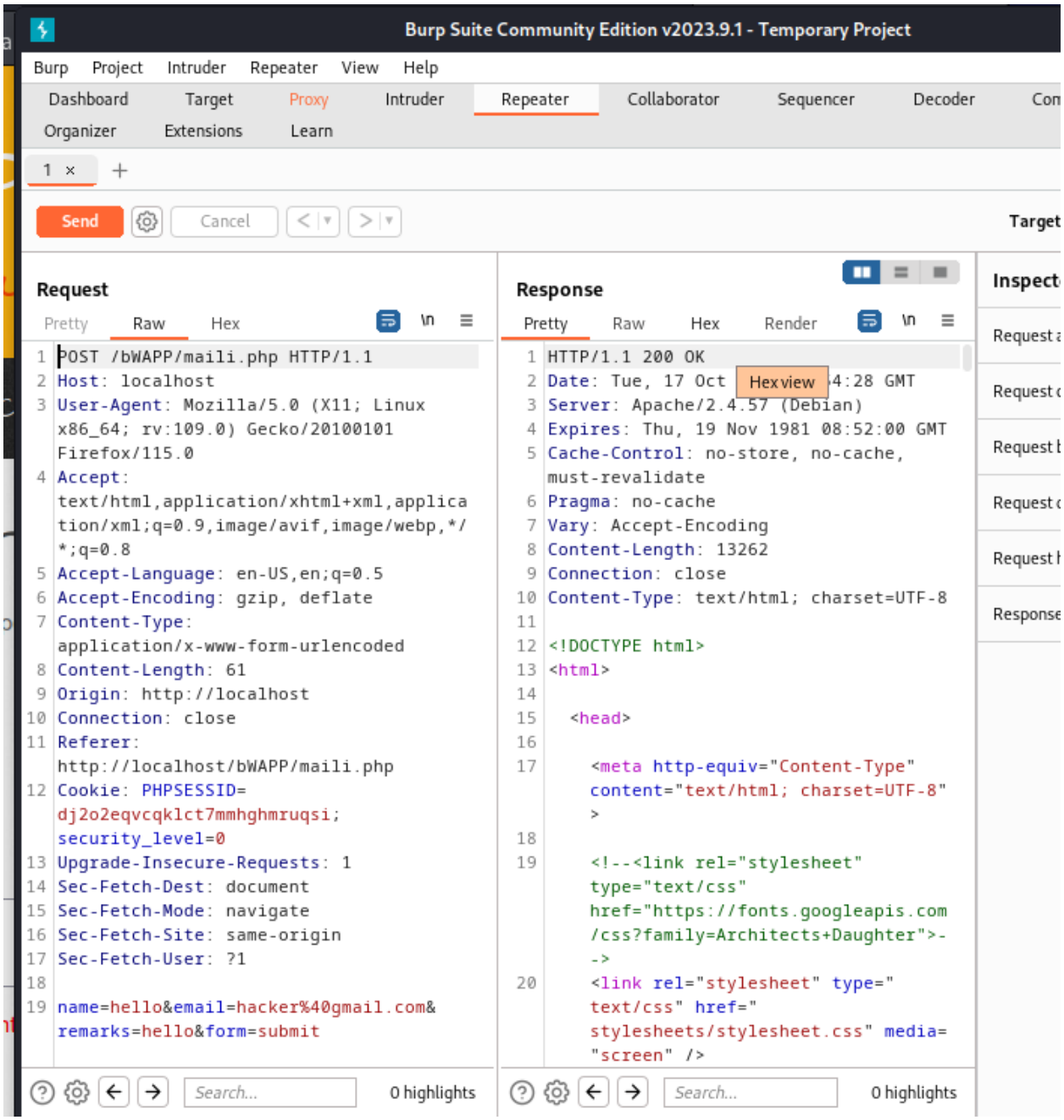

PP - iFrame Injection
URL Encode and Decode
bWAPP, a buggy web app
localhost/bWAPP/iframei.php?ParamUrl=http://www.itsecgames.com/&ParamW
bWAPP - Installation
http://localhost/bWAPP/install.php
bWAPP, a buggy web application!
Switch to Tab
Download bWAPPv2.2.zip (bWAPP)
sourceforge.net/projects/bwapp/files/bWAPP/bWAPPv2.2/bWAPPv2.2.zip/download?use_mirror=webw

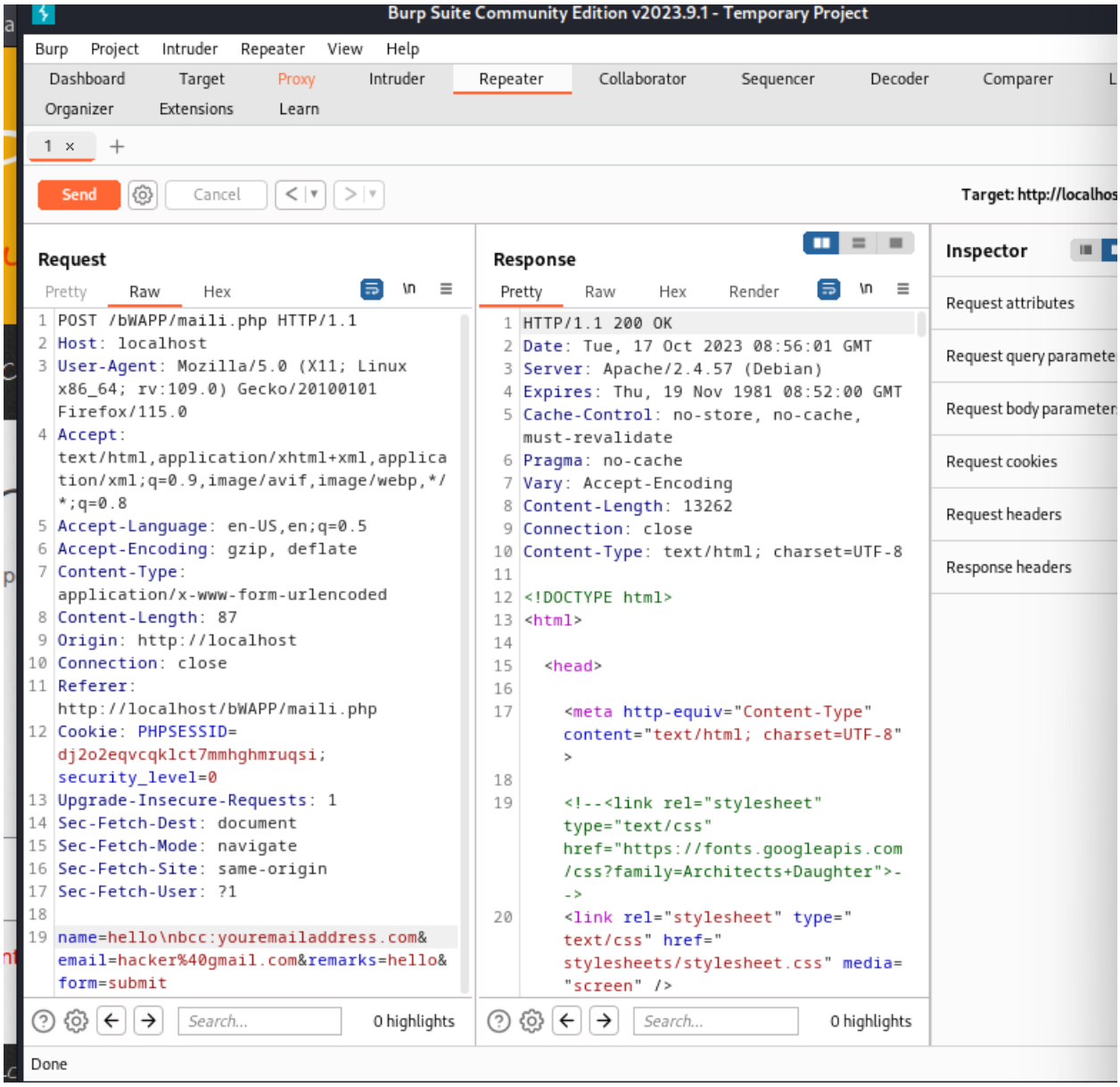


3)**Vulnerability Name**:Mail Header Injection
CWE:CWE-93
OWASP Category:A1-Injection
Description:The product uses CRLF (carriage return line feeds) as a special element, e.g. to separate lines or records, but it does not neutralize or incorrectly neutralizes CRLF sequences from inputs.
Business Impact:It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruptions. It also makes the sites vulnerable to attacks like Email Spoofing, Phishing etc.
Vulnerability Path:localhost/bWAPP/maili.php
Vulnerability Parameter:localhost/bWAPP/maili.php
Steps to reproduce:


• bWAPP - Ma
URL Encode
bWAPP, a bu
FoxyProxy Si
FoxyProxy O
localhost/bWAPP/maili.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Mail Header Injection (SMTP) /
E-mail us your questions at bwapp@mailinator.com.
Name:
hello
E-mail:
hacker@gmail.com
Remarks:
hello


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /bWAPP/maili.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 61
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/maili.php
12 Cookie: PHPSESSID=dj2o2eqvcqklct7mmhghmruqsi; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 name=hello&email=hacker%40gmail.com&remarks=hello&form=submit


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Organizer Extensions Learn
1 ×
Send Cancel
Target
Request
Pretty Raw Hex
1 POST /bWAPP/maili.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 61
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/maili.php
12 Cookie: PHPSESSID=dj2o2eqvcqklct7mmhghmruqsi; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 name=hello&email=hacker%40gmail.com&remarks=hello&form=submit
Search... 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Tue, 17 Oct Hexview 4:28 GMT
3 Server: Apache/2.4.57 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 13262
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html>
14
15 <head>
16
17 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
18
19 <!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
20 <link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
Search... 0 highlights
Inspect
Request a
Request c
Request b
Request c
Request h
Response



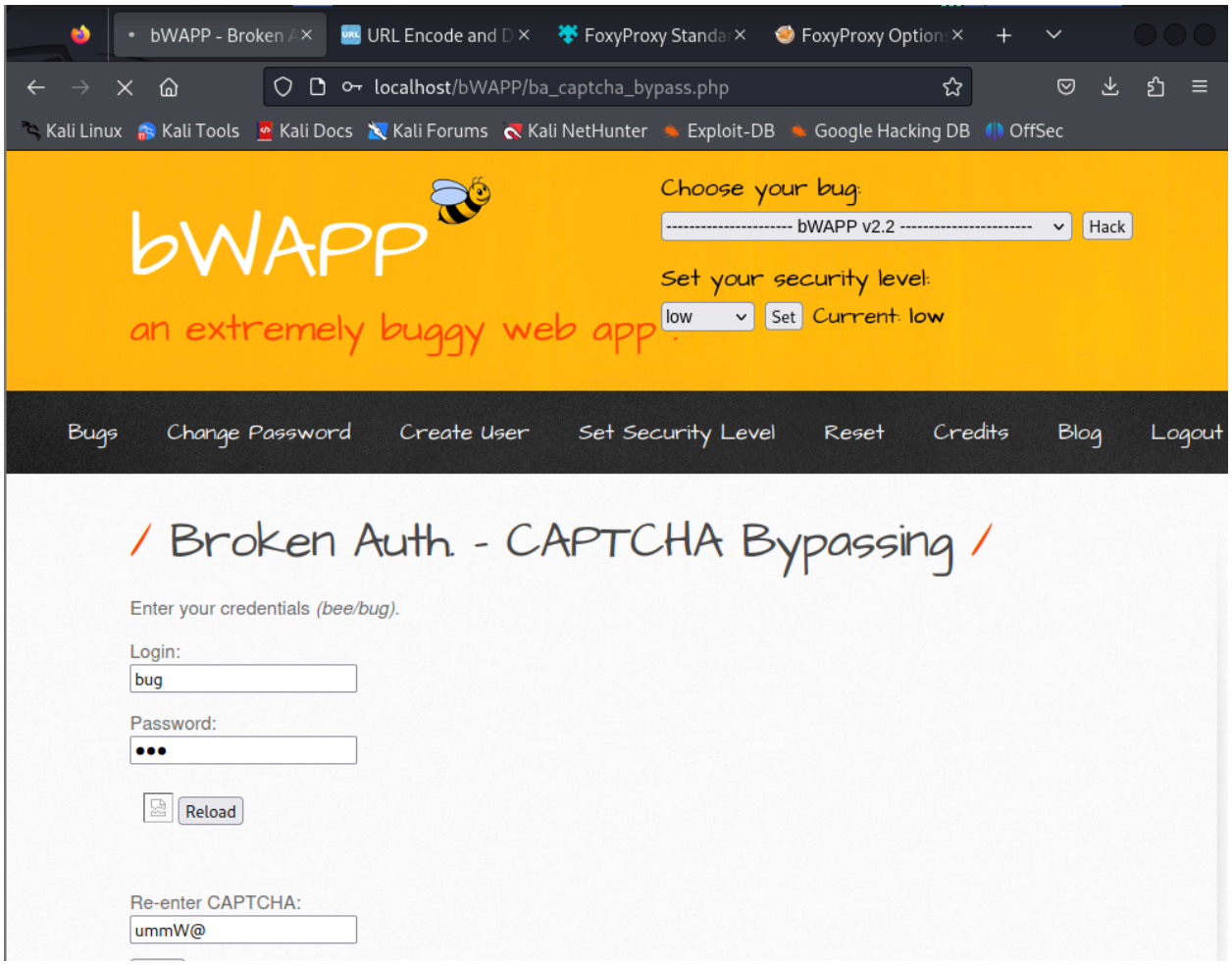
4)**Vulnerability Name**:OS Command Injection
CWE:CWE-78
OWASP Category:A1:2021-Injection
Description: The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.
Business Impact: It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruptions.It makes websites vulnerable to attacks like Unauthorize access, DOS etc.
Vulnerability Path:localhost/bWAPP/commandi.php

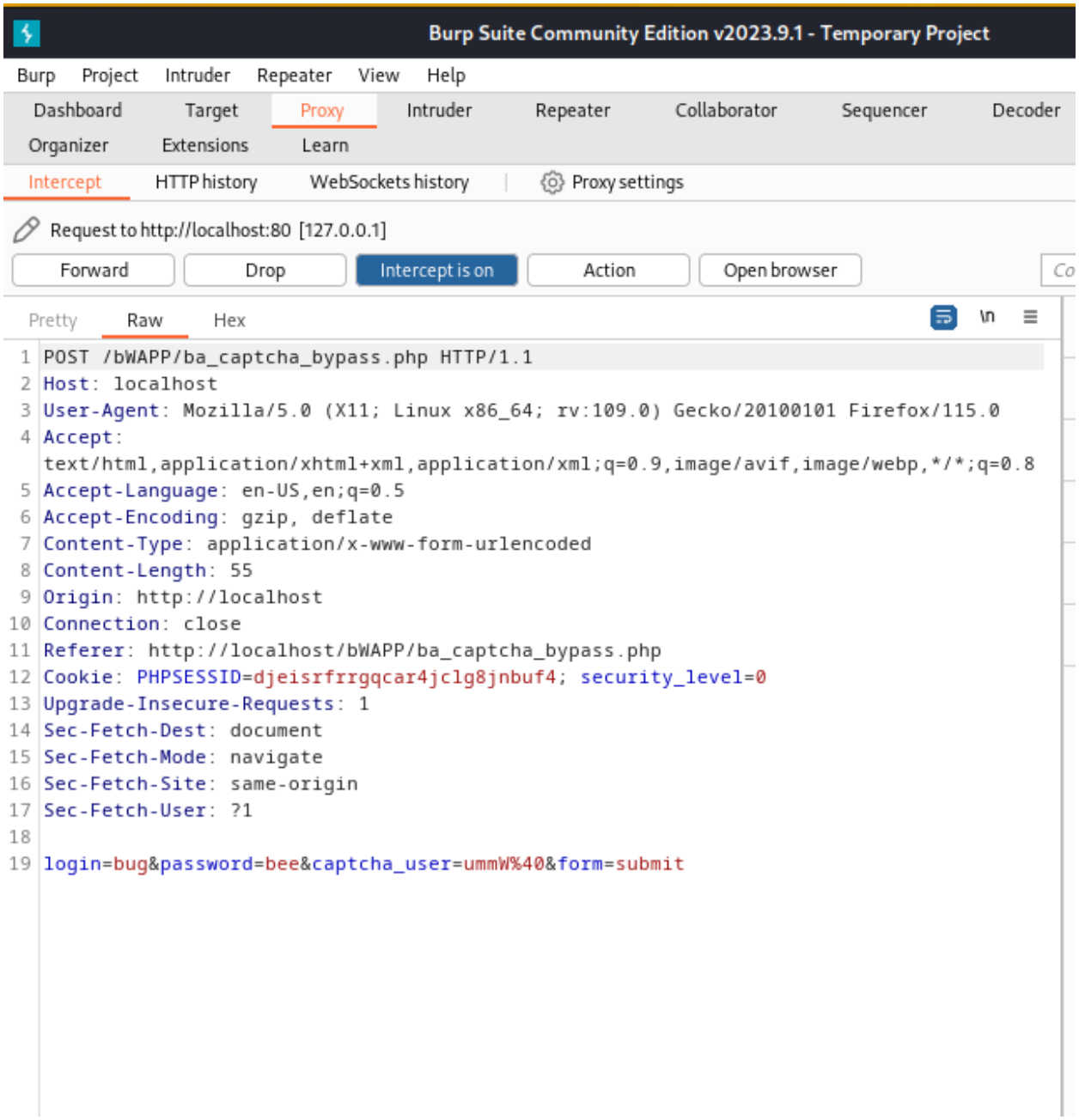
Vulnerability Parameter:localhost/bWAPP/commandi.php
Steps to reproduce:

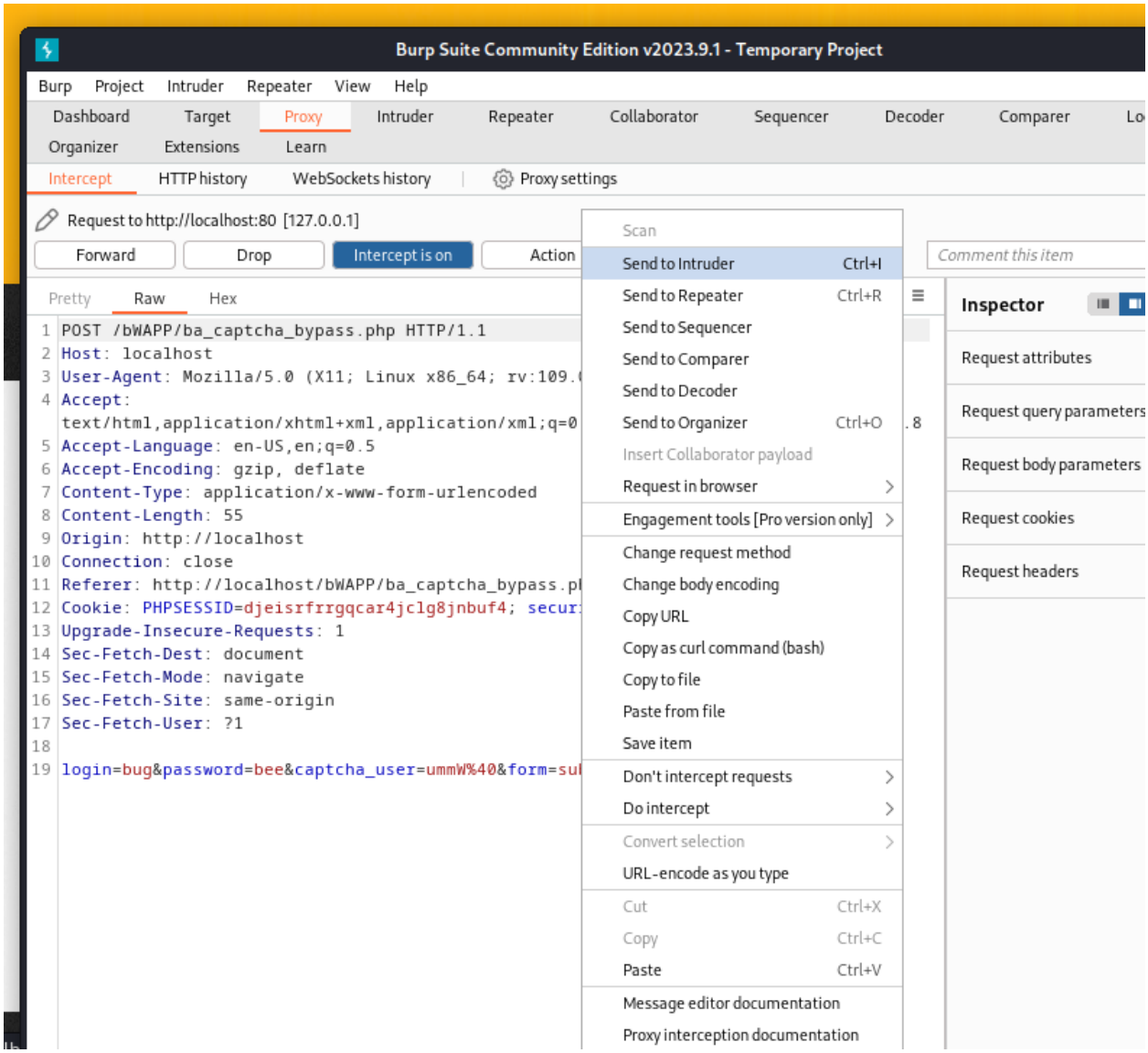

localhost/bWAPP/commandi.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup

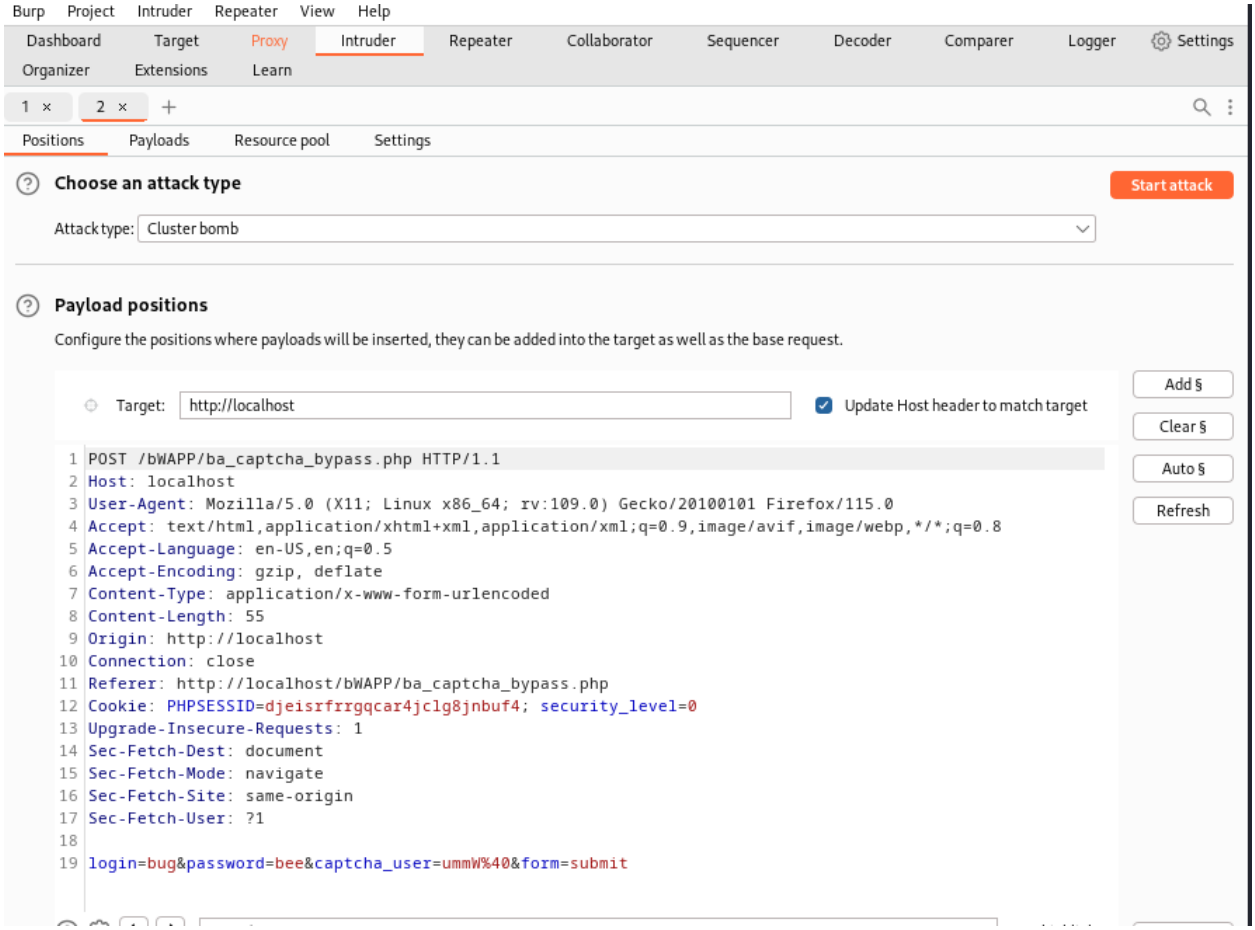
5)**Vulnerability Name**:Broken Authentication And Captcha Bypassing

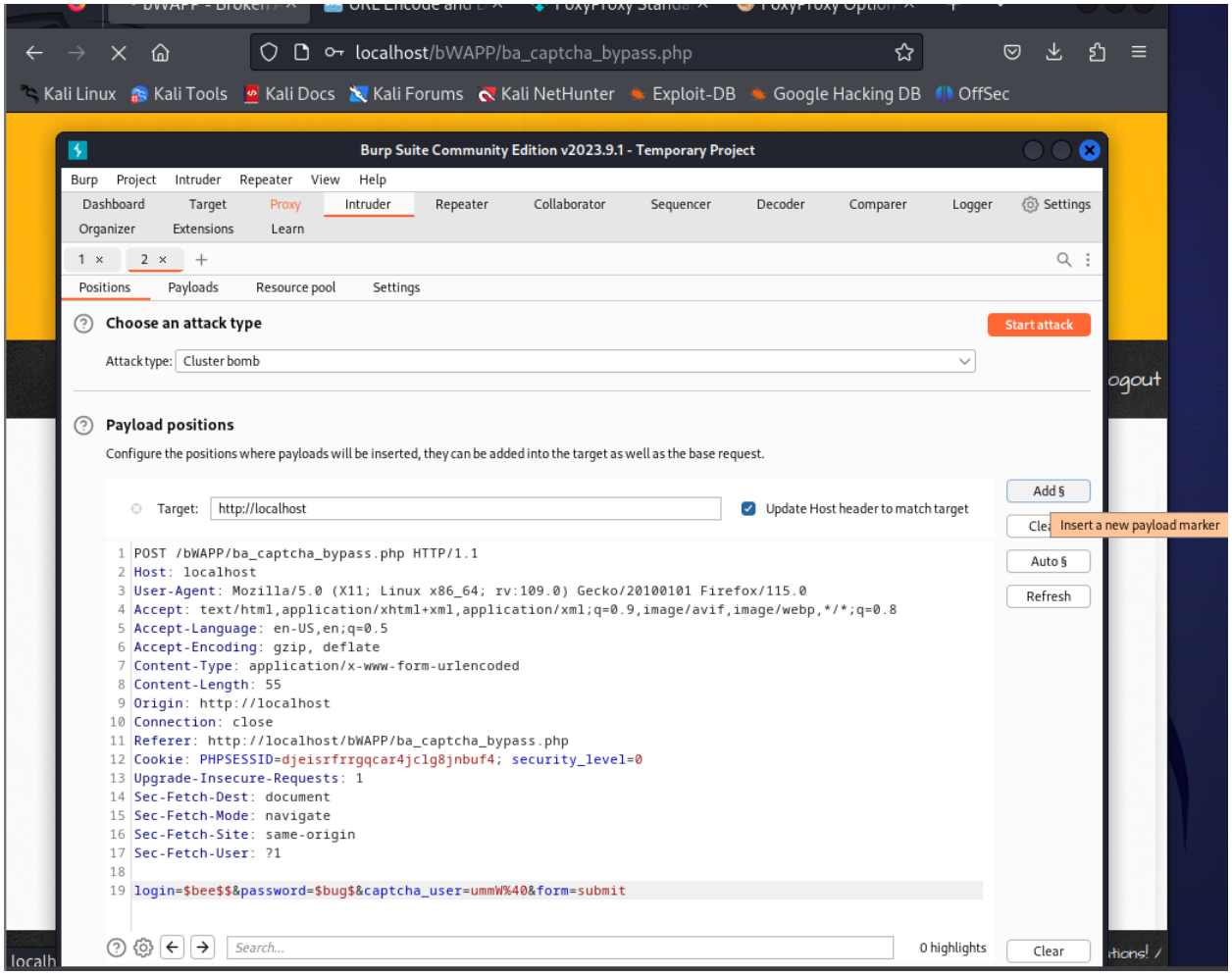
CWE:CWE-287
OWASP Category: A2:2021-Broken Authentication And A7:2021-Security Misconfiguration
Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.
Business Impact: It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruptions. It makes the websites vulnerable to other attacks like Unauthorize access, Data breaches, Data Manipulation etc which can cause other issue about the security of users.
Vulnerability Path:localhost/bWAPP/ba_captch_bypass.php
Vulnerability Parameter:localhost/bWAPP/ba_captch_bypass.php
Steps to reproduce:

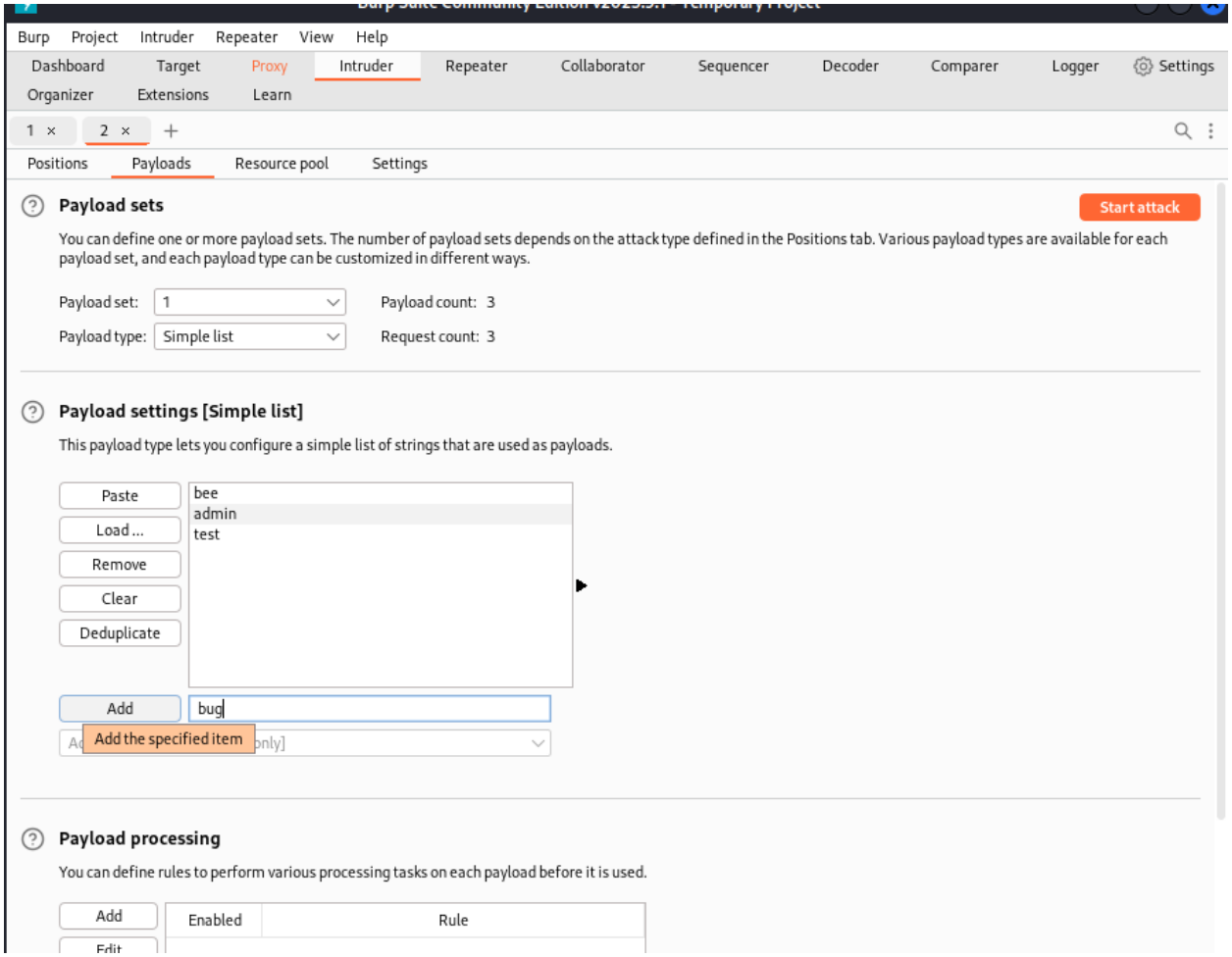

bWAPP - Broken
URL Encode and D
FoxyProxy Standa
FoxyProxy Option
localhost/bWAPP/ba_captcha_bypass.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Broken Auth. - CAPTCHA Bypassing /
Enter your credentials (bee/bug).
Login:
bug
Password:
Reload
Re-enter CAPTCHA:
ummW@

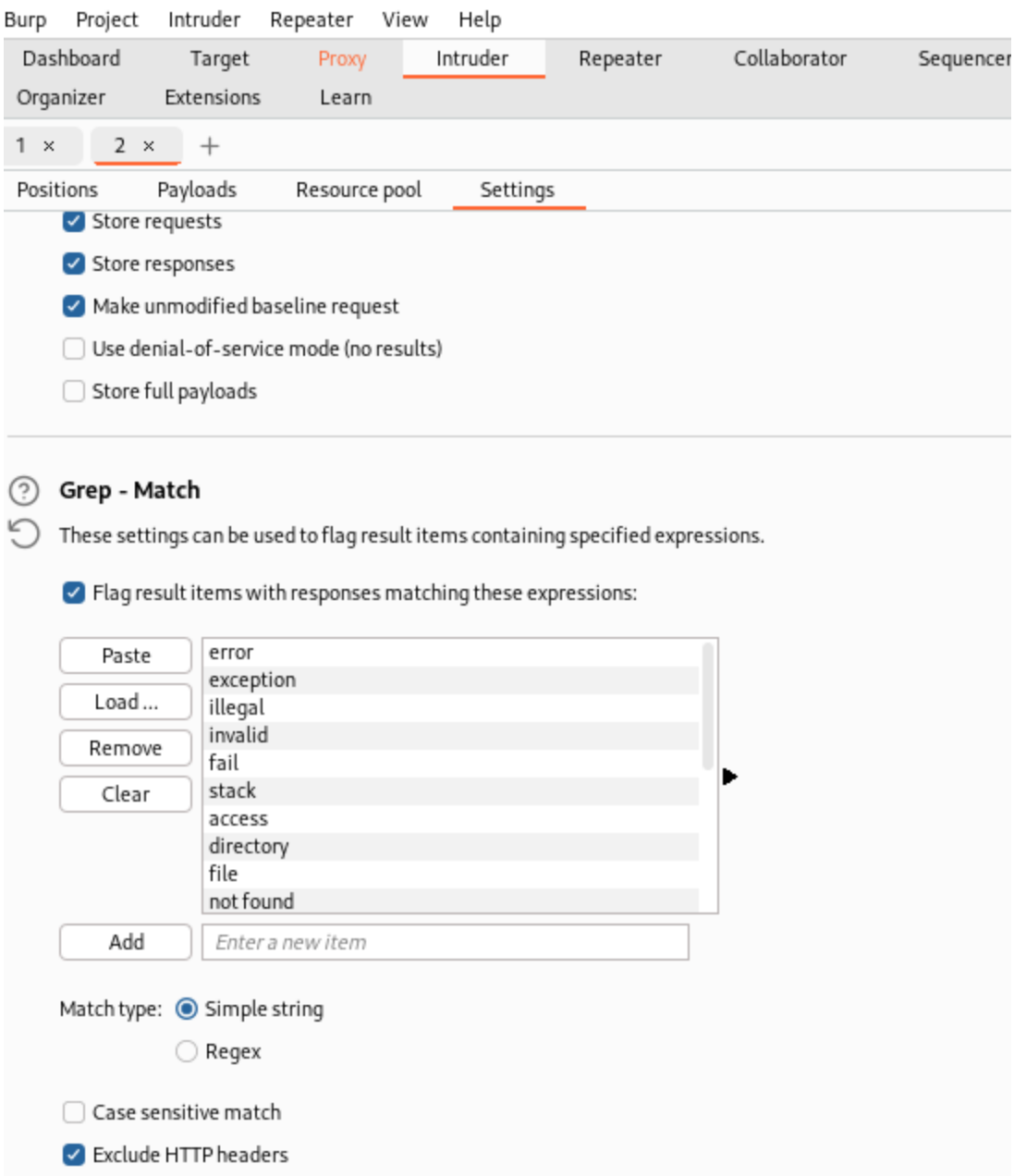

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex \n
1 POST /bWAPP/ba_captcha_bypass.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/ba_captcha_bypass.php
12 Cookie: PHPSESSID=djeisrfrrgqcar4jclg8jnbuf4; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=bug&password=bee&captcha_user=ummW%40&form=submit

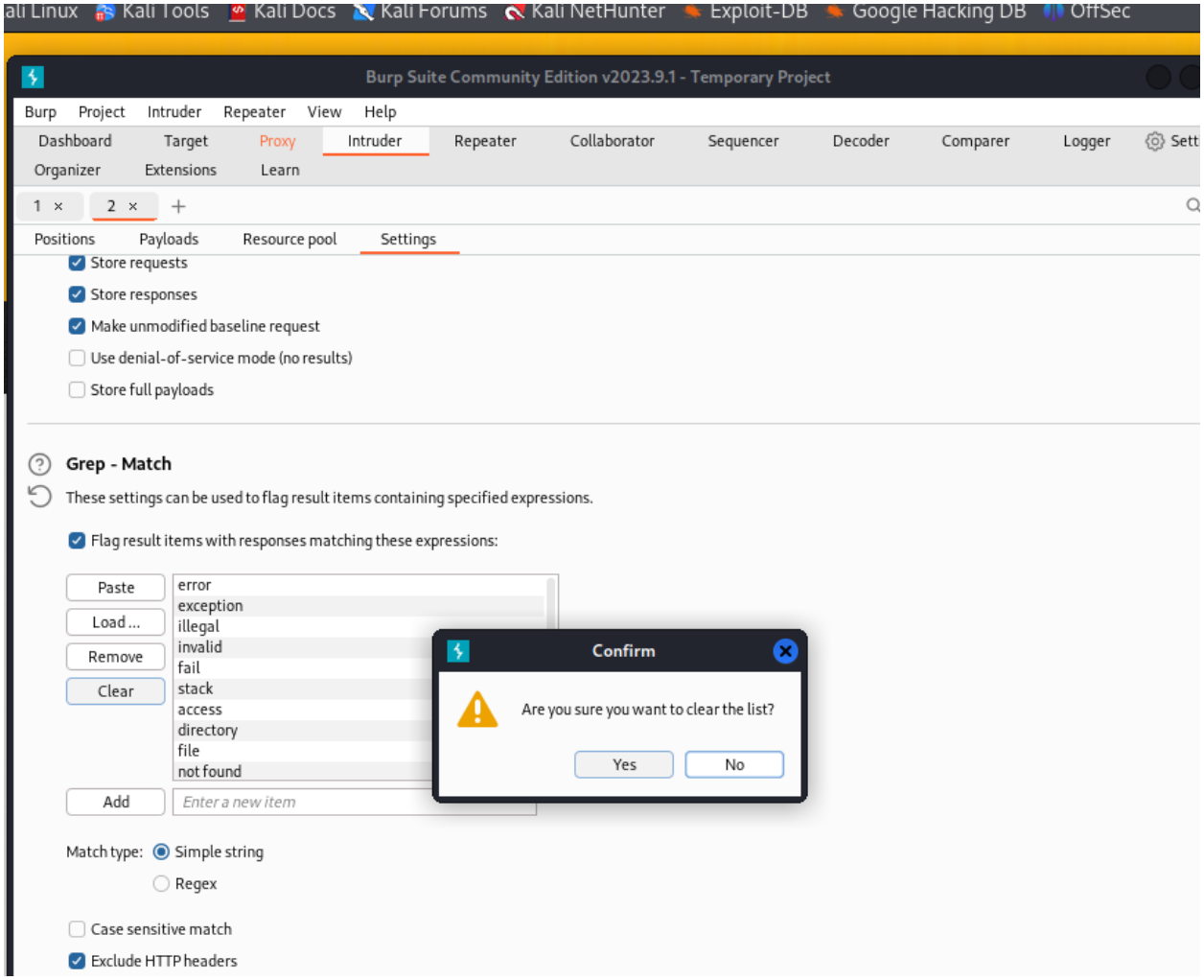

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action
Comment this item
Pretty Raw Hex
1 POST /bWAPP/ba_captcha_bypass.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/ba_captcha_bypass.p
12 Cookie: PHPSESSID=djeisrfrrgqcar4jclg8jnbuf4; secur
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=bug&password=bee&captcha_user=ummW%40&form=su
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

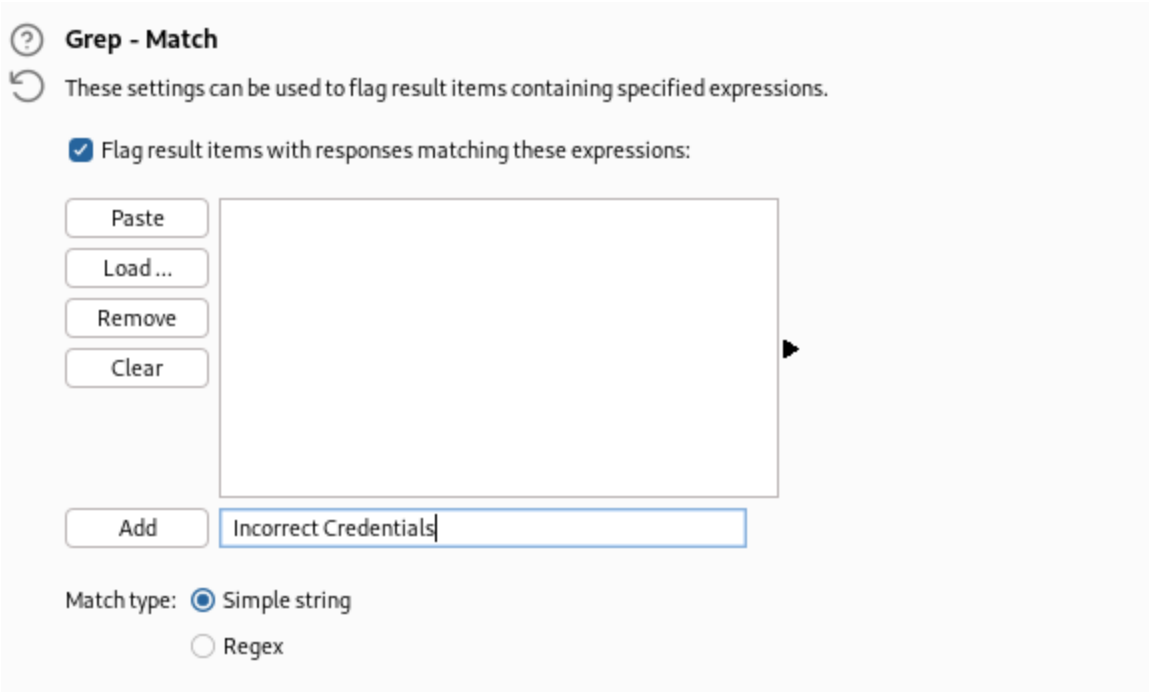

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
1 × 2 ×
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://localhost
Update Host header to match target
Add §
Clear §
Auto §
Refresh
1 POST /bWAPP/ba_captcha_bypass.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/ba_captcha_bypass.php
12 Cookie: PHPSESSID=djeisrfrrgqcar4jclg8jnbuf4; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=bug&password=bee&captcha_user=ummW%40&form=submit


localhost/bWAPP/ba_captcha_bypass.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp
Project
Intruder
Repeater
View
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Settings
Organizer
Extensions
Learn
1 ×
2 ×
Positions
Payloads
Resource pool
Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://localhost
Update Host header to match target
Add §
Clear
Insert a new payload marker
Auto §
Refresh
1 POST /bWAPP/ba_captcha_bypass.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 55
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/ba_captcha_bypass.php
12 Cookie: PHPSESSID=djeisrfrrgqcar4jc1g8jnbuf4; security_level=0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=$bee$$&password=bug&captcha_user=ummW%40&form=submit
Search...
0 highlights
Clear

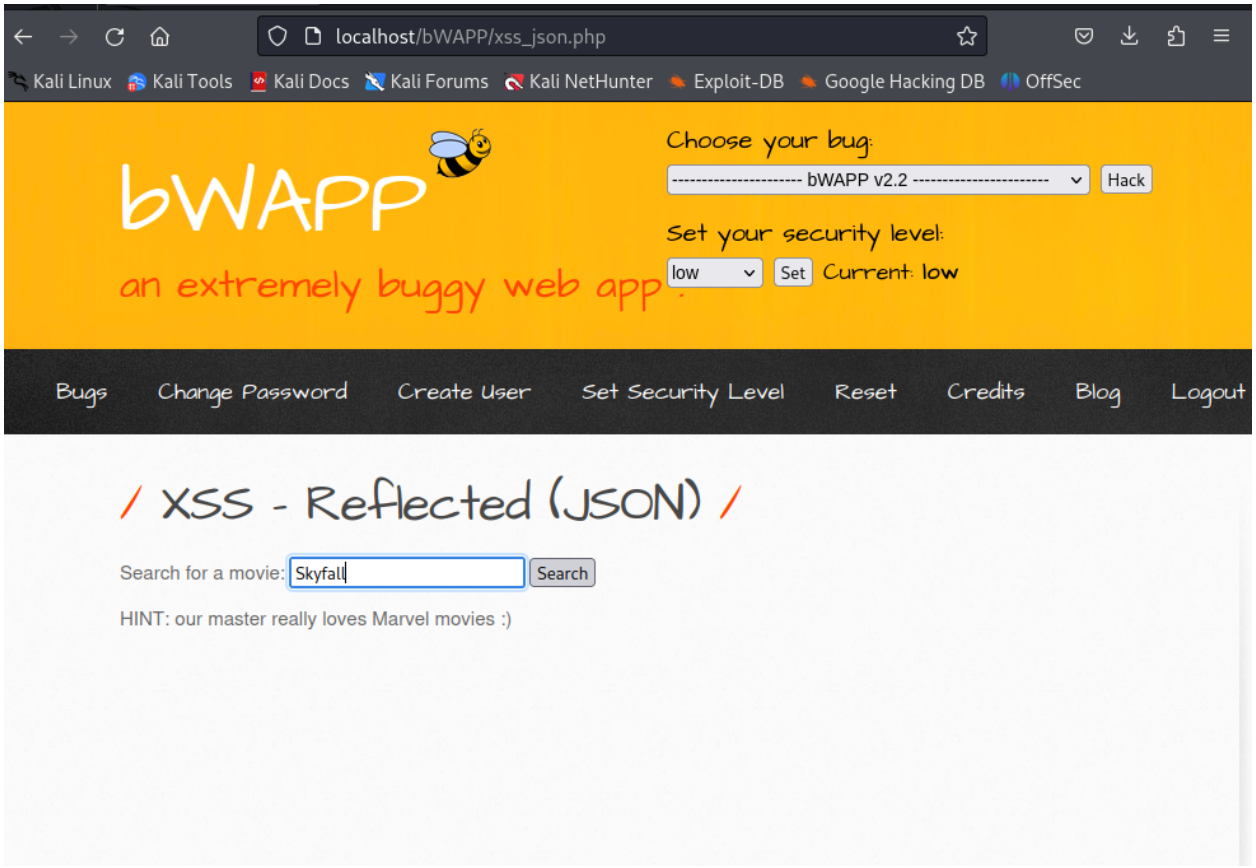

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
1 × 2 ×
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 3
Payload type: Simple list
Request count: 3
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
bee
admin
test
Add
bug
Add the specified item
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule
Edit

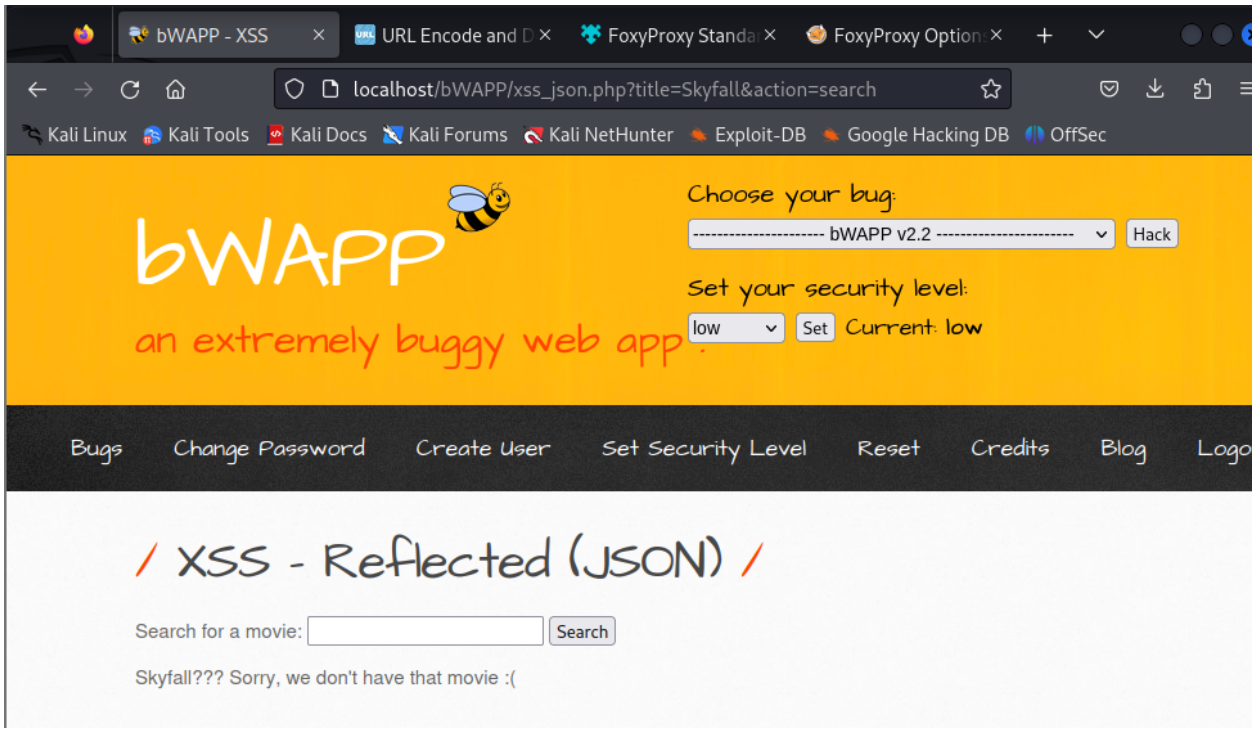

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer
Organizer Extensions Learn
1 × 2 × +
Positions Payloads Resource pool Settings
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
error
exception
illegal
invalid
fail
stack
access
directory
file
not found
Add
Enter a new item
Match type: Simple string
Regex
Case sensitive match
Exclude HTTP headers

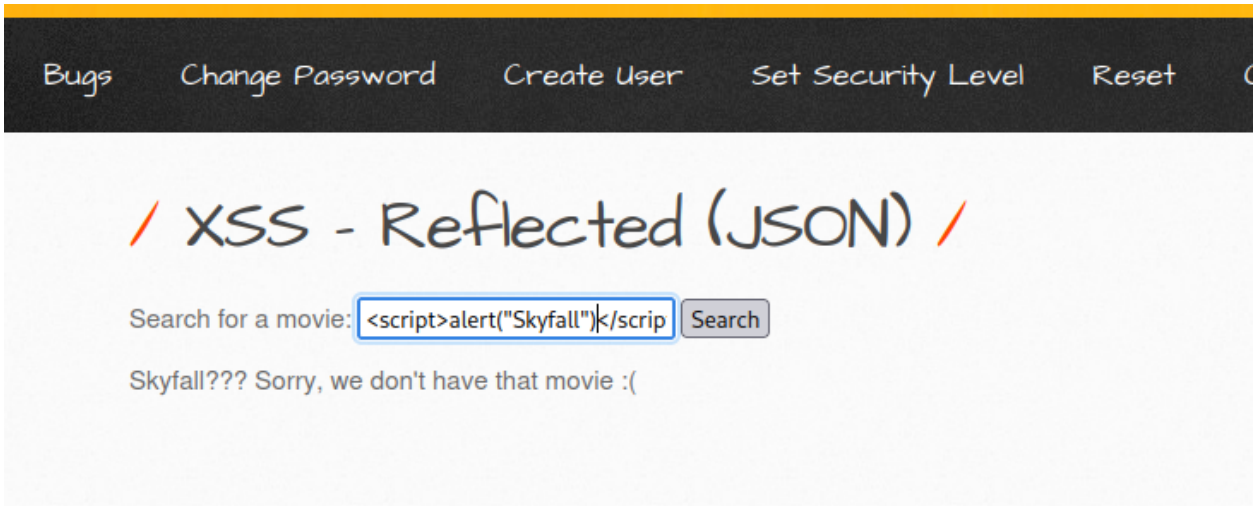

ali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp
Project
Intruder
Repeater
View
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
1 ×
2 ×
Positions
Payloads
Resource pool
Settings
Store requests
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
Add
Enter a new item
error
exception
illegal
invalid
fail
stack
access
directory
file
not found
Confirm
Are you sure you want to clear the list?
Yes
No
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers



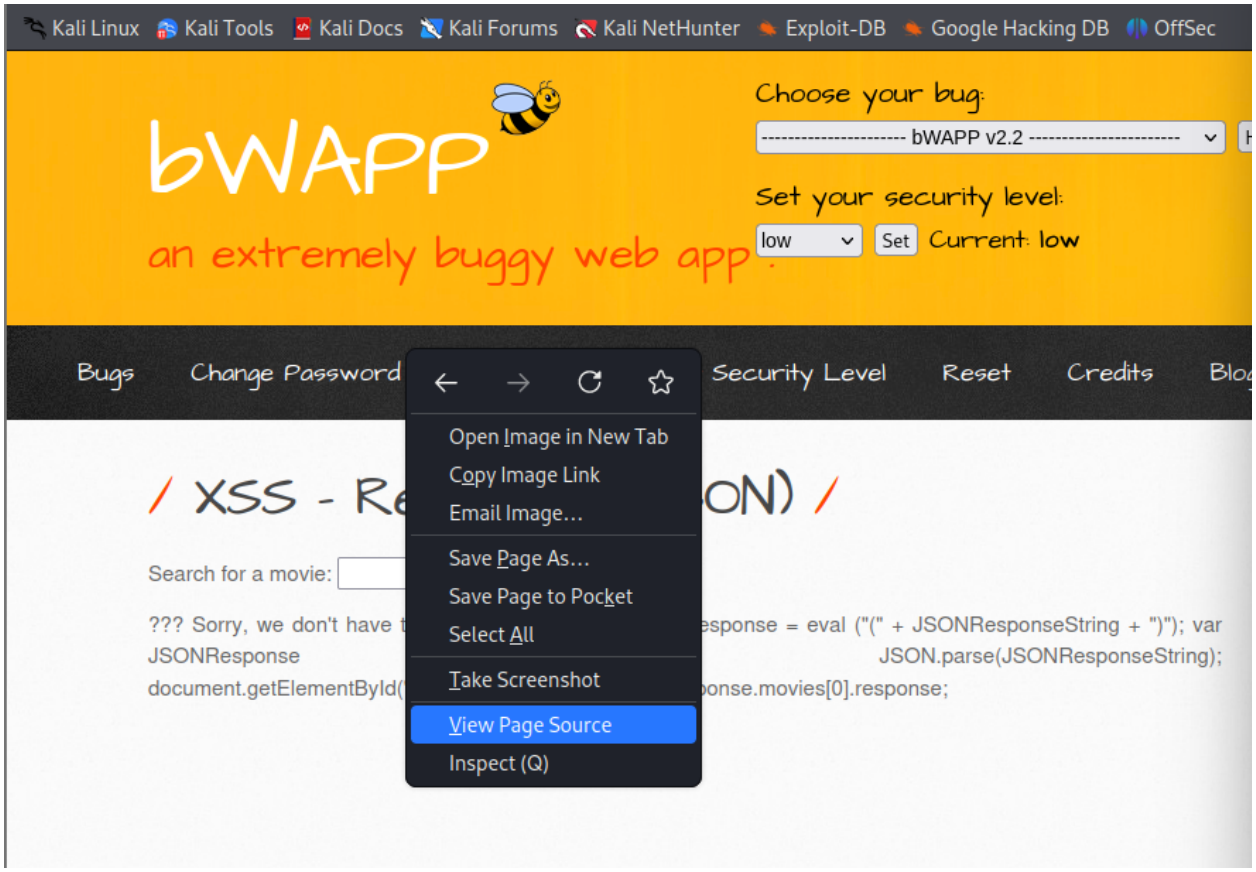
6)**Vulnerability Name**:Cross Site Scripting(JSON)
CWE: CWE-914
OWASP Category:A7:2021-Cross-Site Scripting (XSS).
Description: Many languages offer powerful features that allow the programmer to access arbitrary variables that are specified by an input string. While these features can offer significant flexibility and reduce development time, they can be extremely dangerous if attackers can modify unintended variables that have security implications.
Business Impact: It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruptions.It also makes the website vulnerable to issues like Data Theft, Session Hijacking, Phishing etc. which makes it the website more vulnerable and also causes security issues.
Vulnerability Path: localhost/bWAPP/xss_json.php
Vulnerability Parameter: localhost/bWAPP/xss_json.php
Steps to reproduce:

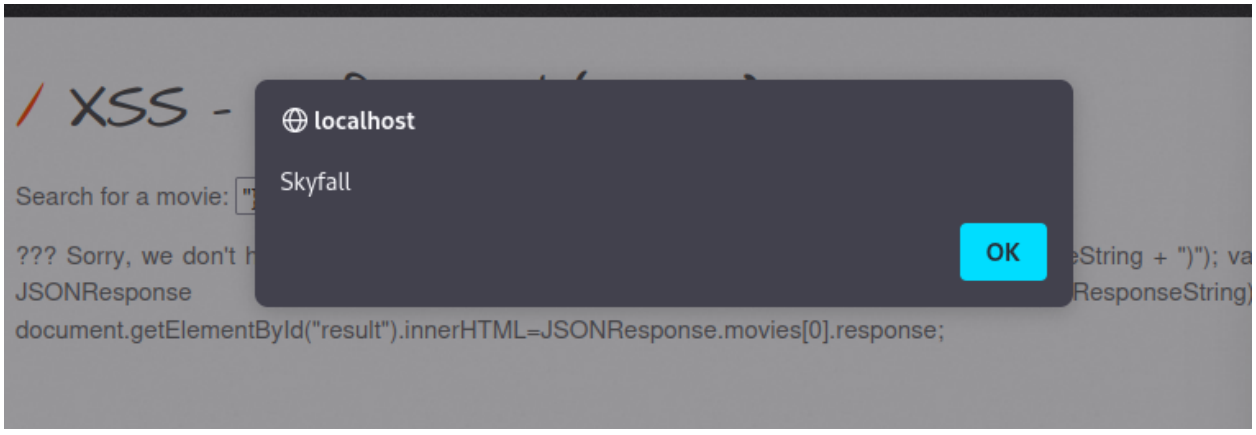

localhost/bWAPP/xss_json.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ XSS - Reflected (JSON) /
Search for a movie: Skyfall
Search
HINT: our master really loves Marvel movies :)


bWAPP - XSS
URL Encode and D
FoxyProxy Standa
FoxyProxy Option
localhost/bWAPP/xss_json.php?title=Skyfall&action=search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logo
/ XSS - Reflected (JSON) /
Search for a movie:
Search
Skyfall??? Sorry, we don't have that movie :(


Bugs
Change Password
Create User
Set Security Level
Reset
/ XSS - Reflected (JSON) /
Search for a movie: <script>alert("Skyfall")</scrip
Search
Skyfall??? Sorry, we don't have that movie :(

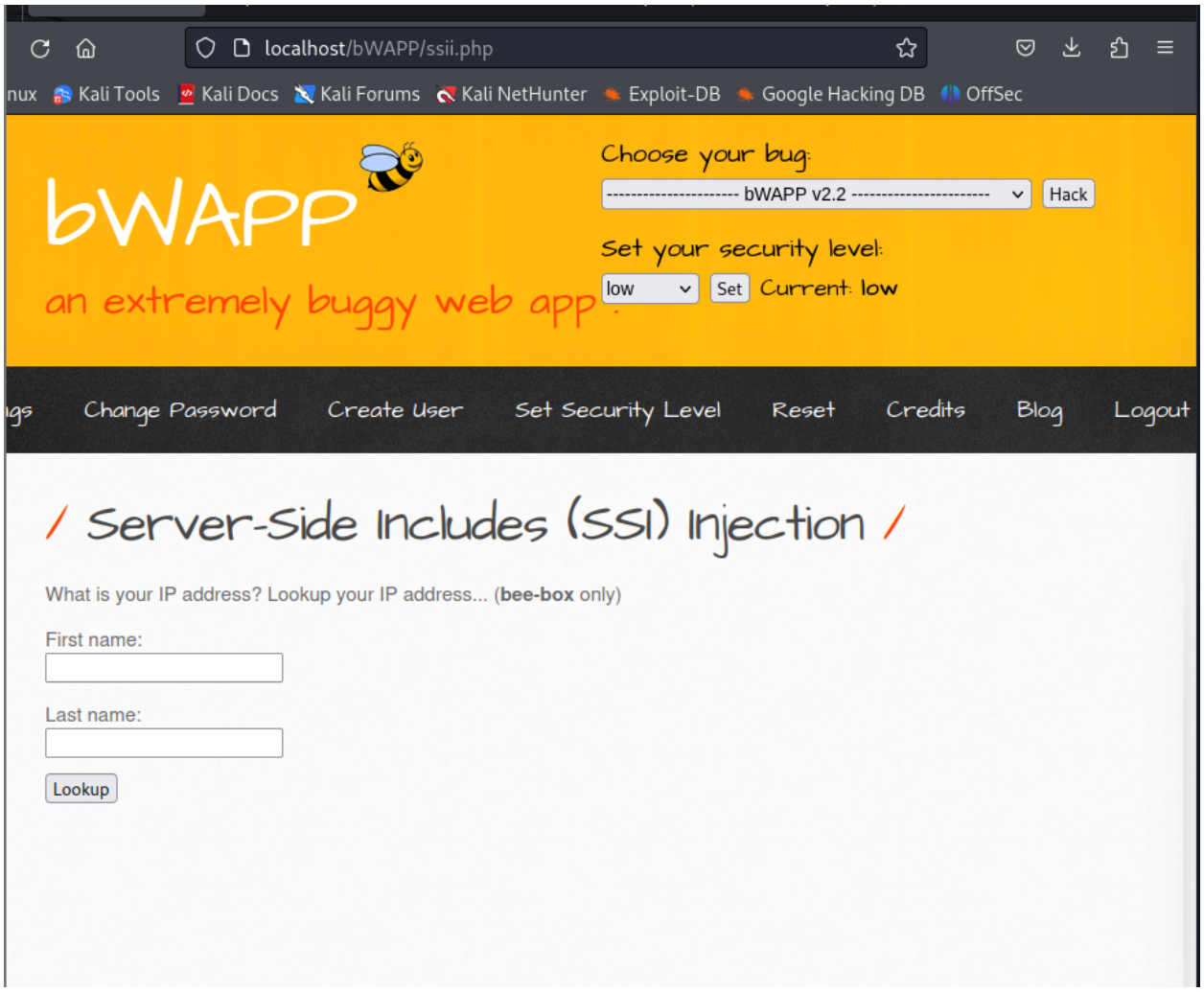

/ XSS - Reflected (JSON) /
Search for a movie:
Search
??? Sorry, we don't have that movie :("}]}'; // var JSONResponse = eval ("(" + JSONResponseString + ")"); var JSONResponse = JSON.parse(JSONResponseString); document.getElementById("result").innerHTML=JSONResponse.movies[0].response;



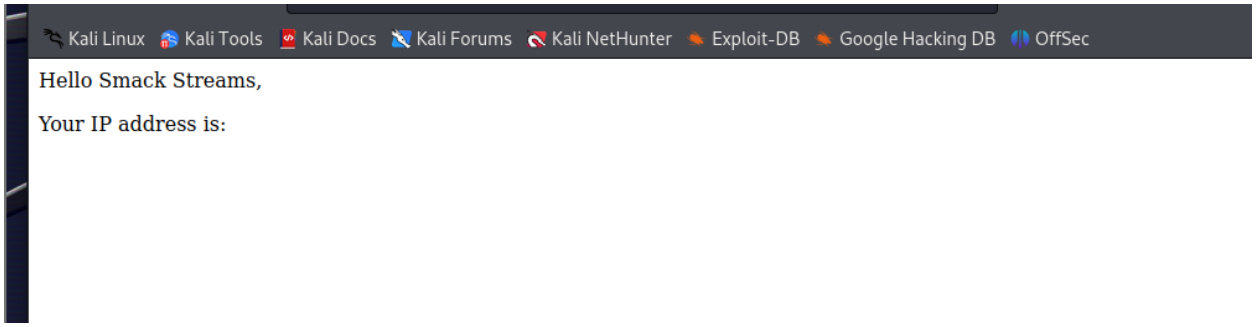


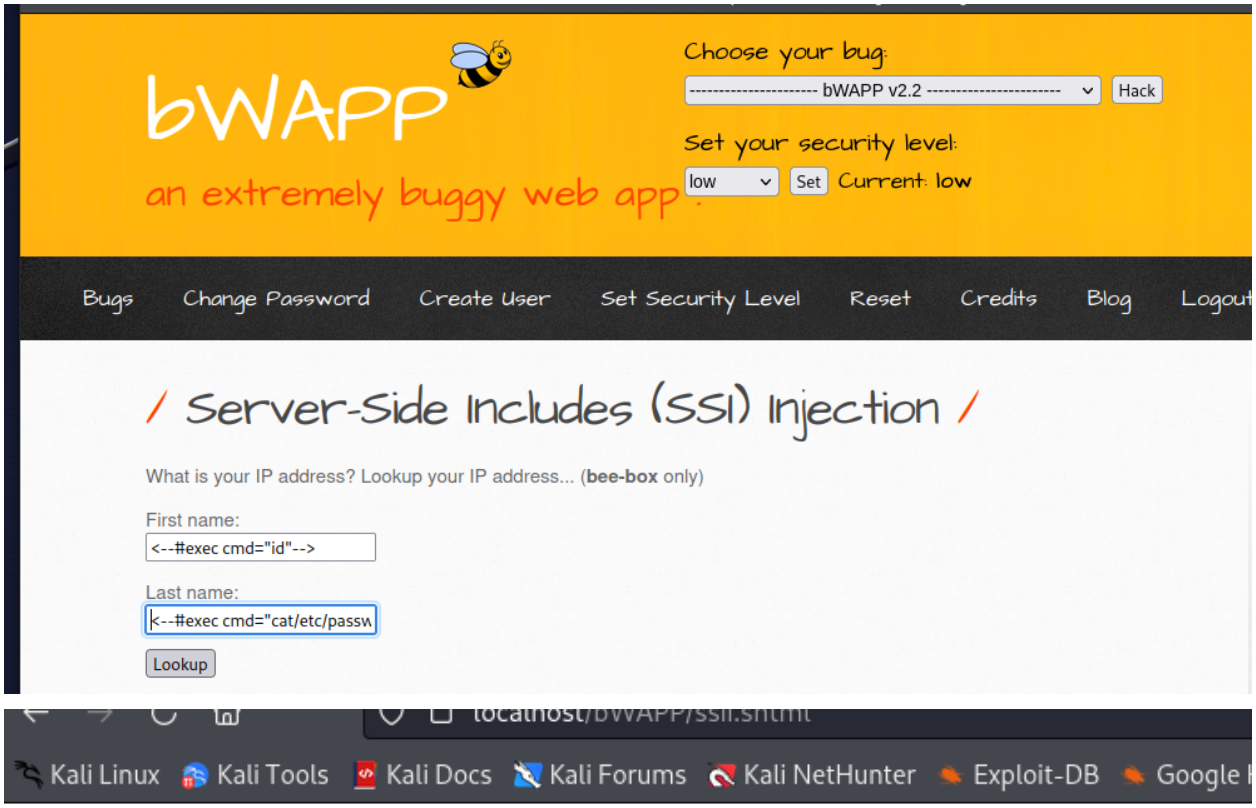
7)**Vulnerability Name**:Server Side Includes Injection

CWE: CWE-97
OWASP Category: A1:2021-Injection
Description: The product generates a web page, but does not neutralize or incorrectly neutralizes user-controllable input that could be interpreted as a server-side include (SSI) directive.
Business Impact: It can cause various losses to the organization like financial losses of reputation damage,legal issues and operational disruption. It makes the website vulnerable to attacks like data leakages, Unauthorized access, Defacement etc.
Vulnerability Path: localhost/bWAPP/ssil.php
Vulnerability Parameter:localhost/bWAPP/ssil.php
Steps to reproduce:

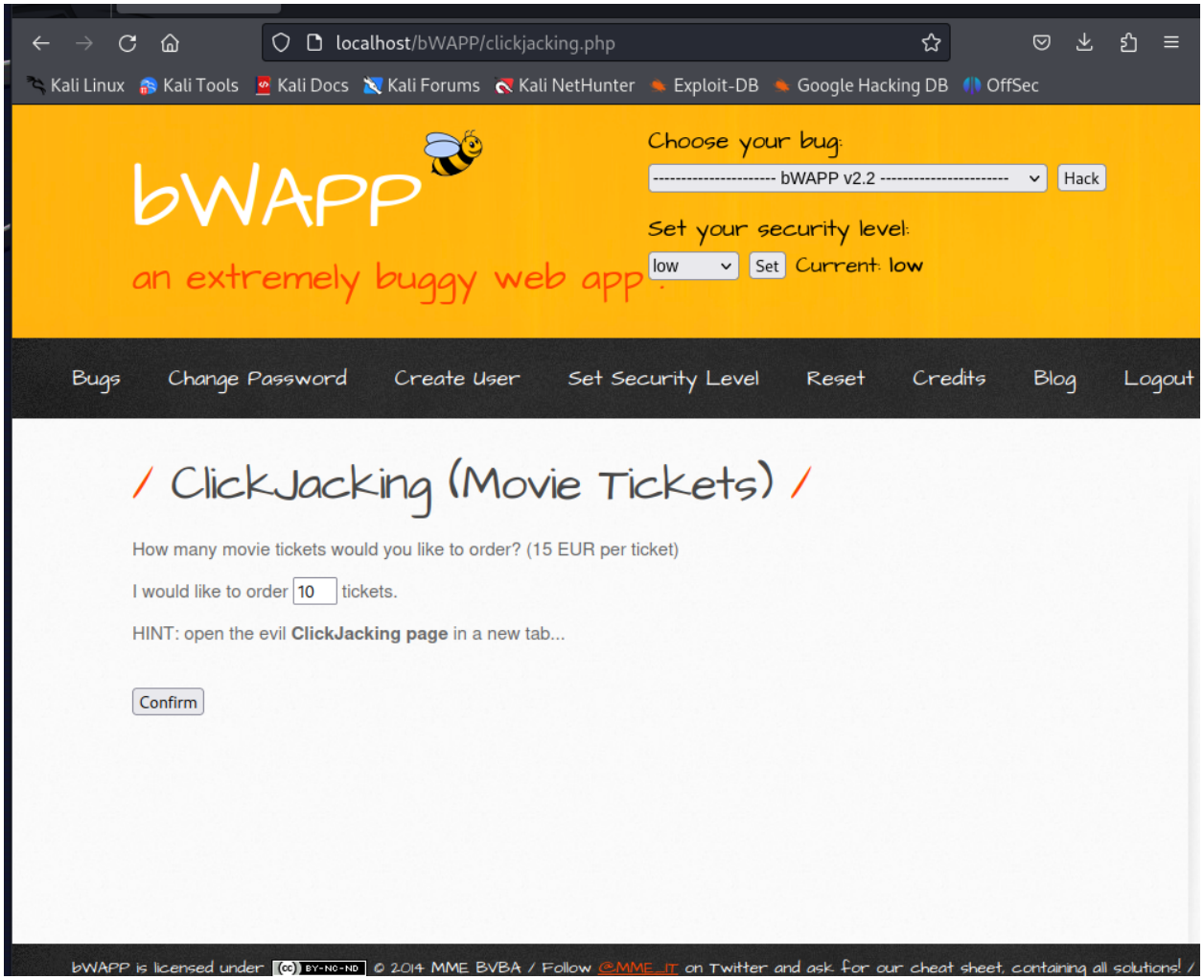


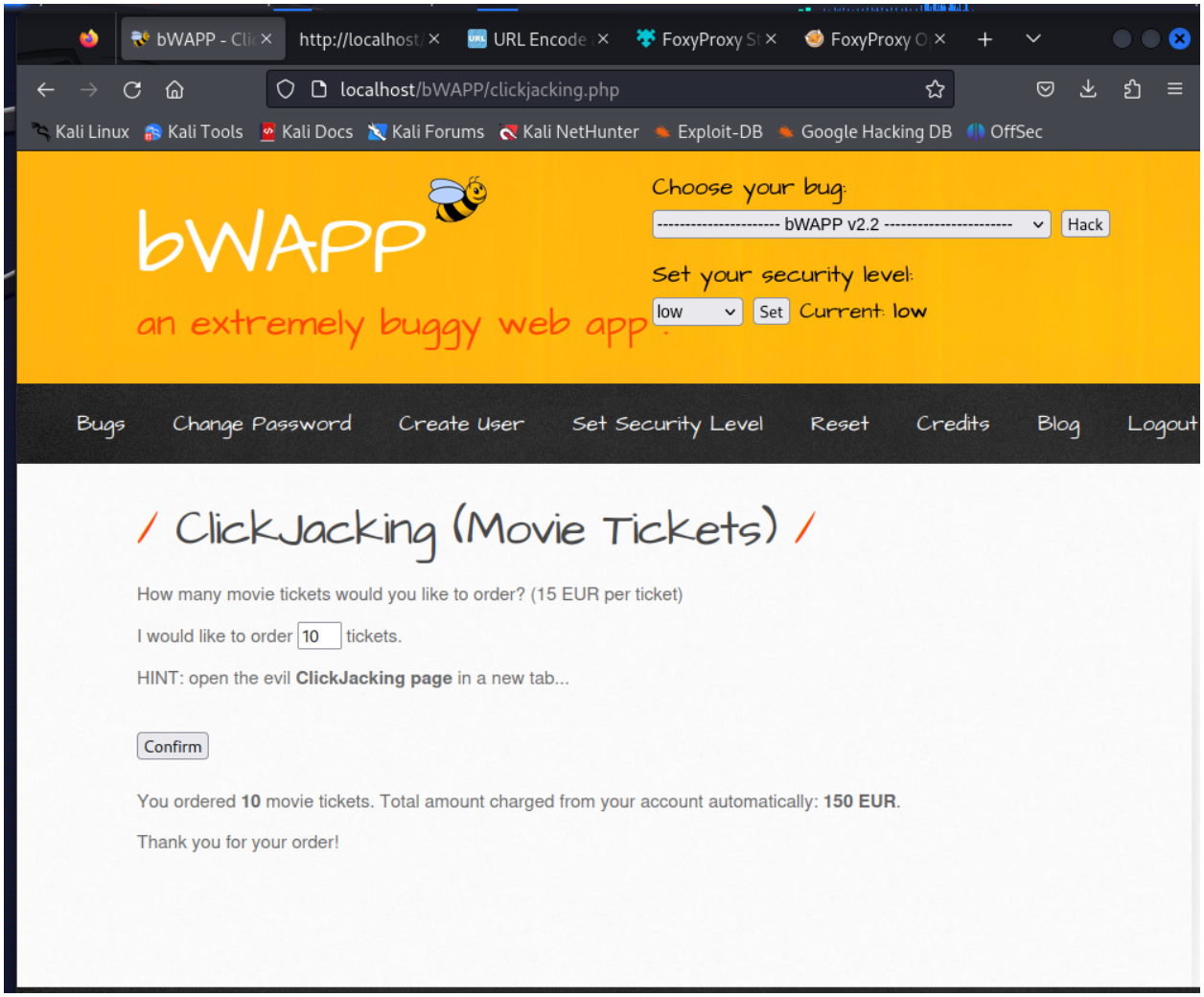

gs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Server-Side Includes (SSI) Injection /
What is your IP address? Lookup your IP address... (bee-box only)
First name:
smack
Last name:
streams
Lookup


Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hello Smack Streams,
Your IP address is:



8)**Vulnerability Name**:Clickjacking
CWE: CWE-1021
OWASP Category: A6:2021-Security Misconfiguration
Description:A web application is expected to place restrictions on whether it is allowed to be rendered within frames, iframes, objects, embed or applet elements. Without the restrictions, users can be tricked into interacting with the application when they were not intending to.
Business Impact: It can affect the website negatively and cause issues like loss in users loosing trust, and can also lead to financial frauds.It can also cause issues like Resource Allocation, Operational Disruption etc.
Vulnerability Path:localhost/bWAPP/clickjacking.php
Vulnerability Parameter:localhost/bWAPP/clickjacking.php
Steps to reproduce:


localhost/bWAPP/clickjacking.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ ClickJacking (Movie Tickets) /
How many movie tickets would you like to order? (15 EUR per ticket)
I would like to order 10 tickets.
HINT: open the evil ClickJacking page in a new tab...
Confirm
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! /



9)**Vulnerability Name**:Directory Traversal

CWE: CWE-22

OWASP Category: A6:2021-Security Misconfiguration

Description: Many file operations are intended to take place within a restricted directory. By using special elements such as ".." and "/" separators, attackers can escape outside of the restricted location to access files or directories that are elsewhere on the system. One of the most common special elements is the "../" sequence, which in most modern operating systems is interpreted as the parent directory of the current location. This is referred to as relative path traversal. Path traversal also covers the use of absolute pathnames such as "/usr/local/bin", which may also be useful in accessing unexpected files. This is referred to as absolute path traversal.

Business Impact: It can cause various issues to the website like losing the users trust it can also cause issues like compromising user data and also financial issues and also can cause issues with resource allocation.

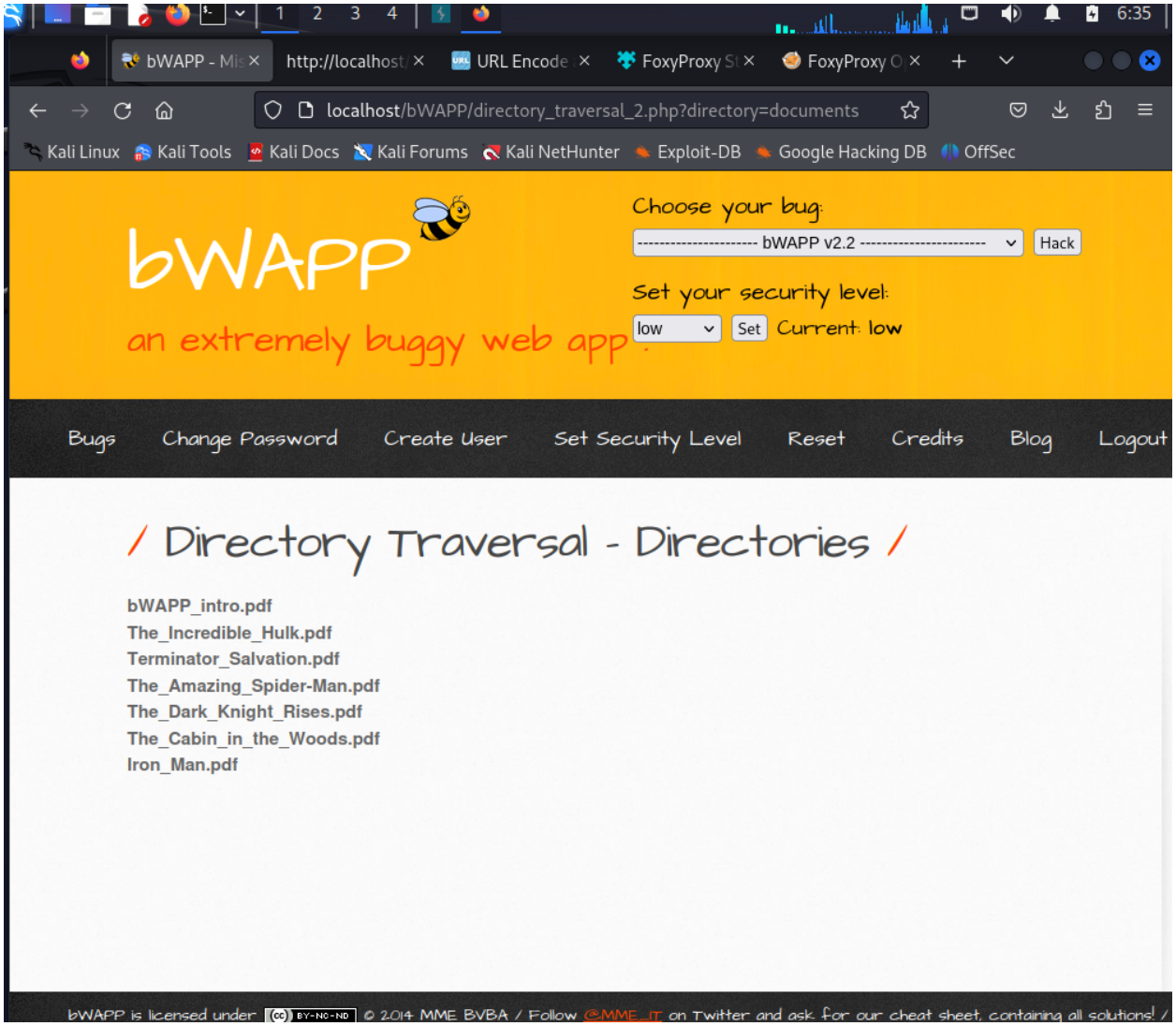
Vulnerability Path:

localhost/bWAPP/driectory_traversal_2.php?driectory=documents

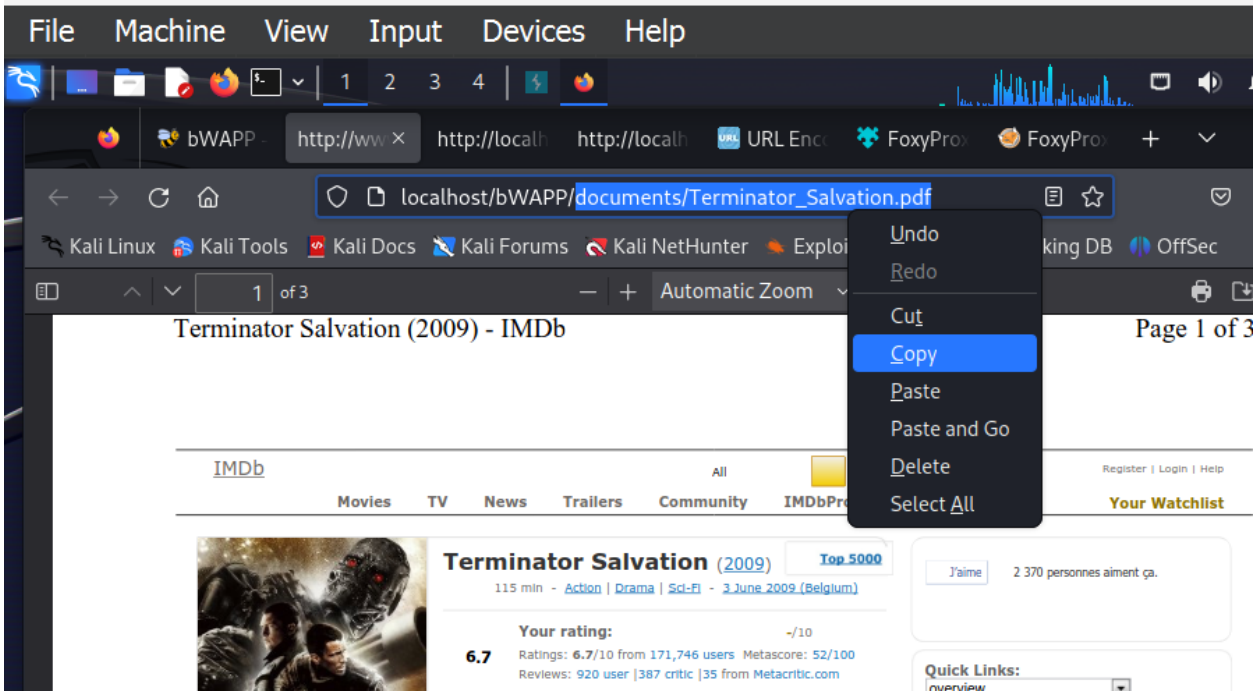
Vulnerability Parameter:

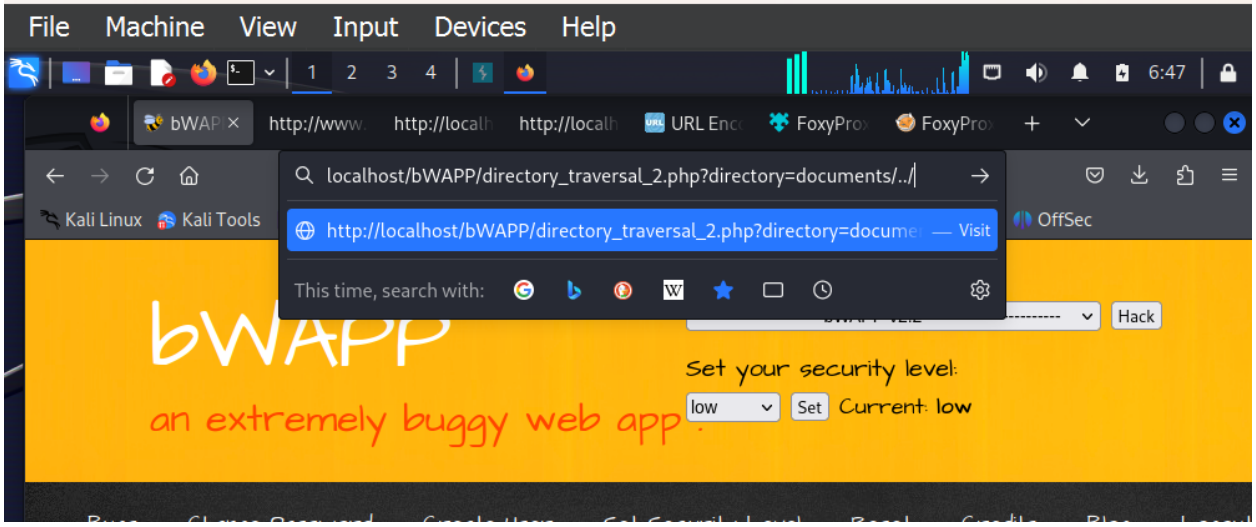
localhost/bWAPP/driectory_traversal_2.php?driectory=documents

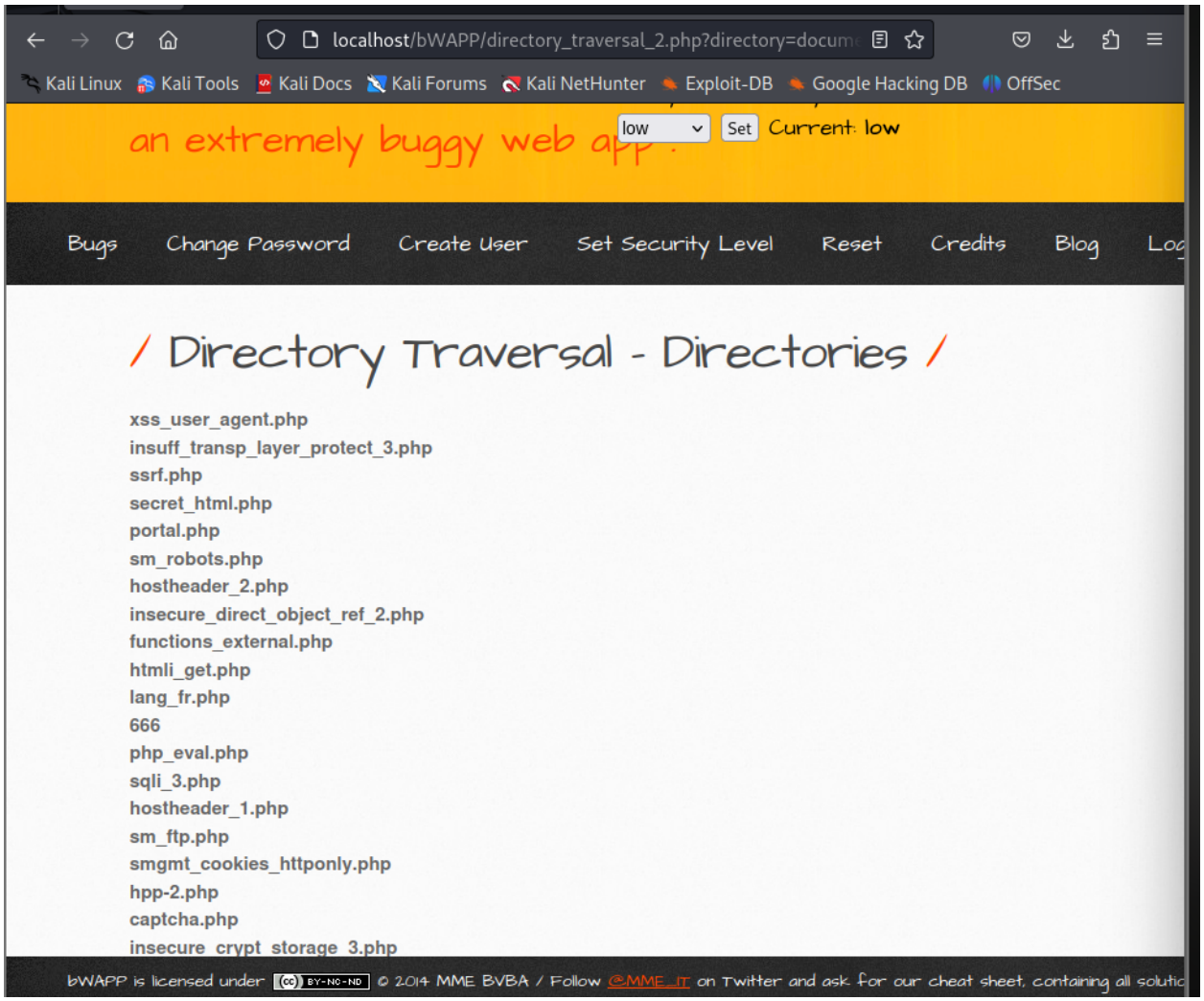
Steps to reproduce:


bWAPP - Mis
http://localhost
URL Encode
FoxyProxy St
FoxyProxy O
localhost/bWAPP/directory_traversal_2.php?directory=documents
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ Directory Traversal - Directories /
bWAPP_intro.pdf
The_Incredible_Hulk.pdf
Terminator_Salvation.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Cabin_in_the_Woods.pdf
Iron_Man.pdf
bWAPP is licensed under
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! /


bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Directory Traversal - Directories /
bWAPP_intro.pdf
The_Incredible_Hulk.pdf
Terminator_Salvation.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Cabin_in_the_Woods.pdf
Iron_Man.pdf
Open Image in New Tab
Copy Image Link
Email Image...
Save Page As...
Save Page to Pocket
Select All
Take Screenshot
View Page Source
Inspect (Q)


File
Machine
View
Input
Devices
Help
bWAPP
localhost/bWAPP/documents/Terminator_Salvation.pdf
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
OffSec
1 of 3
Automatic Zoom
Undo
Redo
Cut
Copy
Paste
Paste and Go
Delete
Select All
Terminator Salvation (2009) - IMDb
Page 1 of 3
IMDb
Movies
TV
News
Trailers
Community
Your Watchlist
Terminator Salvation (2009)
Top 5000
115 min - Action | Drama | Sci-Fi - 3 June 2009 (Belgium)
Your rating:
6.7
Ratings: 6.7/10 from 171,746 users Metascore: 52/100
Reviews: 920 user | 387 critic | 35 from Metacritic.com
J'aime
2 370 personnes aiment ça.
Quick Links:





10)**Vulnerability Name**:Restrict Device Access

CWE: CWE-264

OWASP Category:

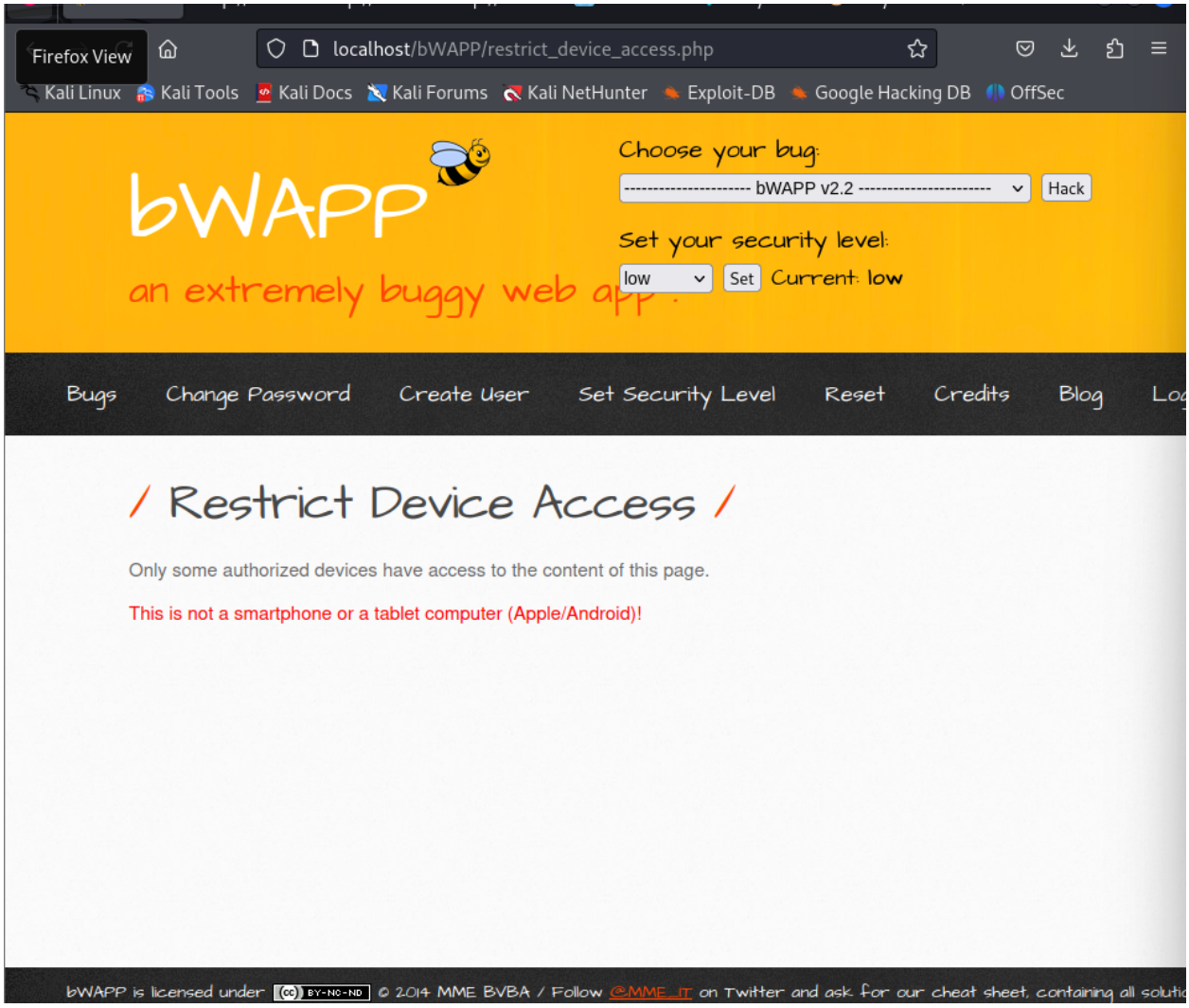
Description: Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control.

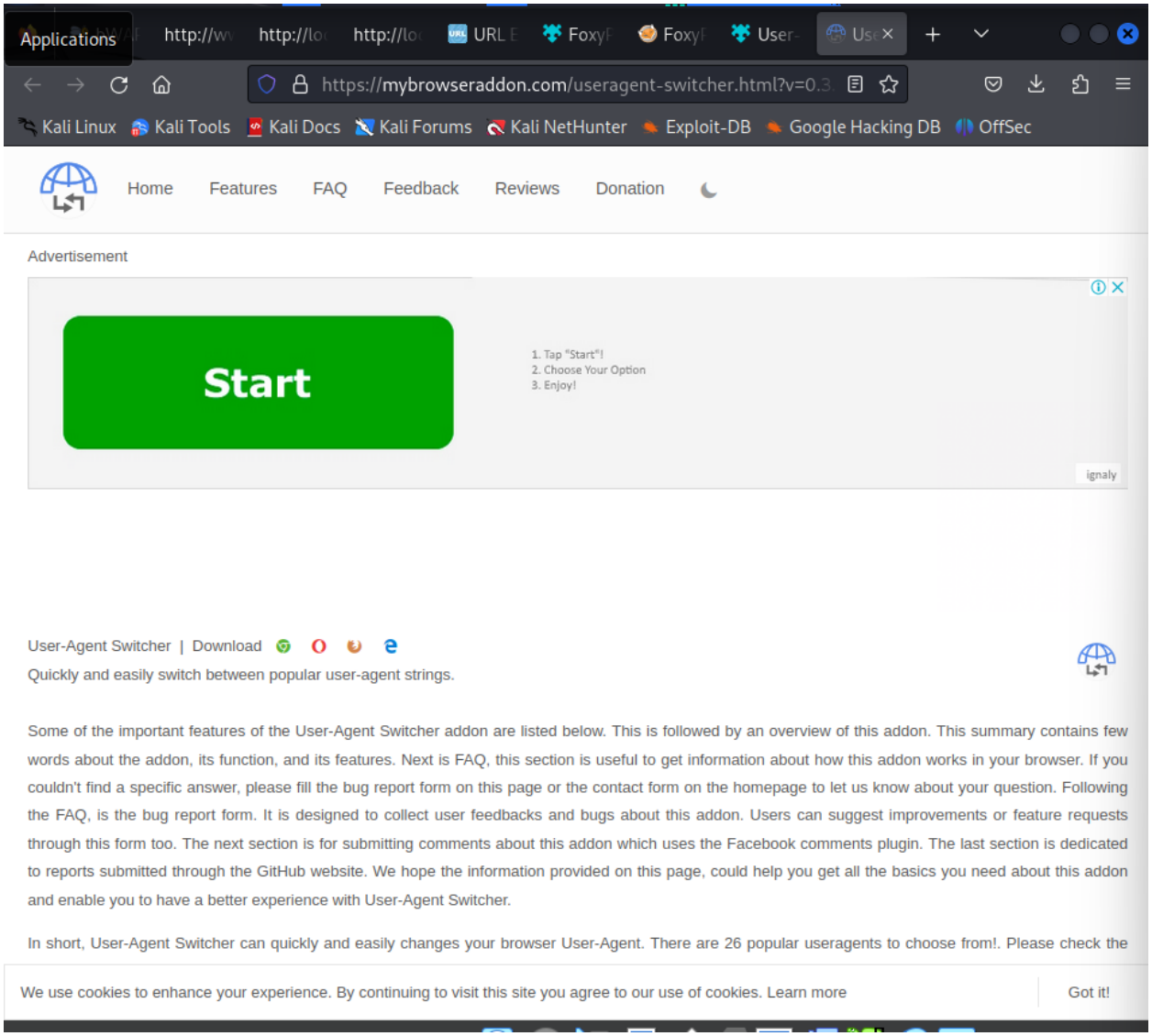
Business Impact:

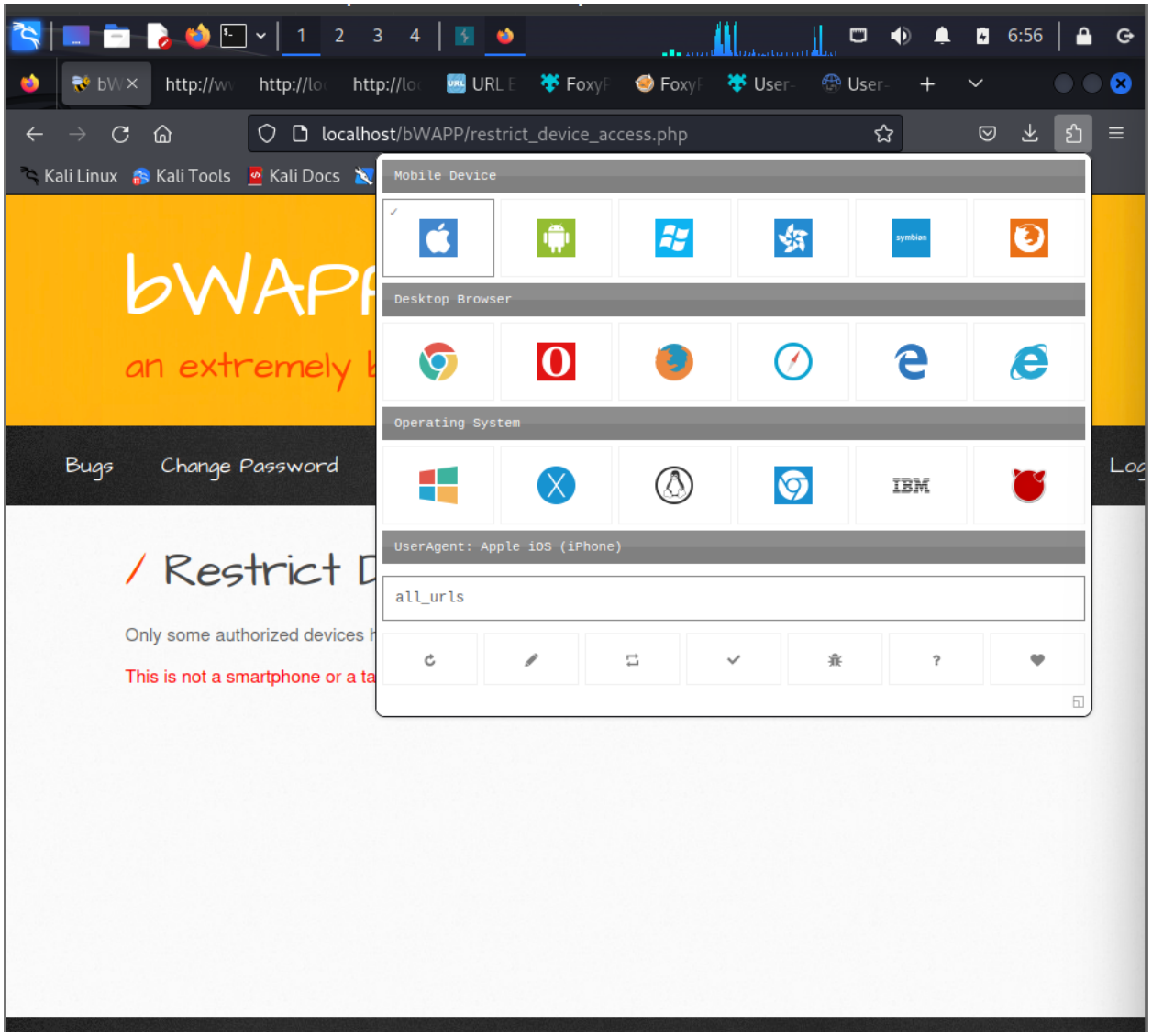
Vulnerability Path: localhost/bWAPP/restrict_device_access.php

Vulnerability Parameter: localhost/bWAPP/restrict_device_access.php

Steps to reproduce:


Firefox View
localhost/bWAPP/restrict_device_access.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Restrict Device Access /
Only some authorized devices have access to the content of this page.
This is not a smartphone or a tablet computer (Apple/Android)!
bWAPP is licensed under
BY-NC-ND
© 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutio


Applications
https://mybrowseraddon.com/useragent-switcher.html?v=0.3
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Home
Features
FAQ
Feedback
Reviews
Donation
Advertisement
Start
1. Tap "Start"!
2. Choose Your Option
3. Enjoy!
ignaly
User-Agent Switcher | Download
Quickly and easily switch between popular user-agent strings.
Some of the important features of the User-Agent Switcher addon are listed below. This is followed by an overview of this addon. This summary contains few words about the addon, its function, and its features. Next is FAQ, this section is useful to get information about how this addon works in your browser. If you couldn't find a specific answer, please fill the bug report form on this page or the contact form on the homepage to let us know about your question. Following the FAQ, is the bug report form. It is designed to collect user feedbacks and bugs about this addon. Users can suggest improvements or feature requests through this form too. The next section is for submitting comments about this addon which uses the Facebook comments plugin. The last section is dedicated to reports submitted through the GitHub website. We hope the information provided on this page, could help you get all the basics you need about this addon and enable you to have a better experience with User-Agent Switcher.
In short, User-Agent Switcher can quickly and easily changes your browser User-Agent. There are 26 popular useragents to choose from!. Please check the
We use cookies to enhance your experience. By continuing to visit this site you agree to our use of cookies. Learn more
Got it!


localhost/bWAPP/restrict_device_access.php
Kali Linux
Kali Tools
Kali Docs
Mobile Device
Desktop Browser
Operating System
UserAgent: Apple iOS (iPhone)
all_urls
Bugs
Change Password
/ Restrict
Only some authorized devices
This is not a smartphone or a


6:56
localhost/bWAPP/restrict_device_access.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
/ Restrict Device Access /
Only some authorized devices have access to the content of this page.
This is a smartphone or a tablet computer!