

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:

The screenshot shows a Firefox browser window with the title "bWAPP - Portal". The address bar displays "localhost/bWAPP/portal.php". The page itself is titled "bWAPP" with a subtitle "an extremely buggy web app!". It features a yellow header with a bee logo and a dropdown menu labeled "Choose your bug: bWAPP v2.2" with a "Hack" button. Below the header, there's a "Set your security level:" dropdown set to "low". The main content area has a sub-header "/ Portal /" and a paragraph about bWAPP being a free, open-source, deliberately insecure web application for security testing and education. On the right side, there are social media icons for LinkedIn, Facebook, and Twitter, along with a logo for the National Center for Missing & Exploited Children. At the bottom, a footer notes the license as CC BY-NC-ND, the year 2014, and the copyright holder MME BVBA, with a link to their Twitter account @MME_IT. It also mentions a cheat sheet containing solutions.

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)

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

Firefox - bWAPP - HTML Injection x +

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:

Last name:

Go

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

Firefox - 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:

Welcome pcpl alex

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

Firefox bWAPP - HTML Injection

localhost/bWAPP/html_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 CC BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

Firefox bWAPP - HTML Injection

localhost/bWAPP/html_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 CC BY-NC-ND | © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need a

The screenshot shows a Firefox browser window with the URL `localhost/bWAPP/htmli_get.php?firstname=<h2>pcpl<%2Fh2>&lastname=<h2>`. The page title is "bWAPP - HTML Injection". The main content area displays the text "an extremely buggy web app!" in red. Above it, there's a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Set your security level: low Current: medium". Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout. The main content area has a title "**/ HTML Injection - Reflected (GET) /**". It asks for "Enter your first and last name:" and provides two input fields for "First name:" and "Last name:", both containing the value "pcpl". A "Go" button is next to the last name field. Below the inputs, the text "Welcome <h2>pcpl</h2> <h2>friend</h2>" is displayed. At the bottom, a footer notes "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

The screenshot shows a Firefox browser window with the title "bWAPP - HTML Injection". The URL in the address bar is "localhost/bWAPP/html_get.php?firstname=<a>hack<%2Fa>&lastname=<&form". The page has a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Set your security level: low Set Current medium". The main content area has a title "/ HTML Injection - Reflected (GET) /". It asks "Enter your first and last name:" with fields for "First name:" and "Last name:", both containing "<a>hack". A "Go" button is present. Below the form, the text "Welcome <a>hack <" is displayed. The footer contains the text "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" and social media icons for LinkedIn, GitHub, and YouTube.

With URL Encoding

The screenshot shows a web browser window with the URL <https://www.urlencoder.org> in the address bar. The page has a blue header with various Kali Linux links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the header, there's a decorative background with a gear and tools. The main content area has tabs for "Decode" and "Encode", with "Encode" being active. A message at the top says, "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." A text input field contains the URL-encoded string "<a>pcpl". Below the input field are two dropdown menus: "UTF-8" for destination character set and "LF Unix" for destination newline separator. A note at the bottom left says, "To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page."

URL

Decode

Decode and Encode

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

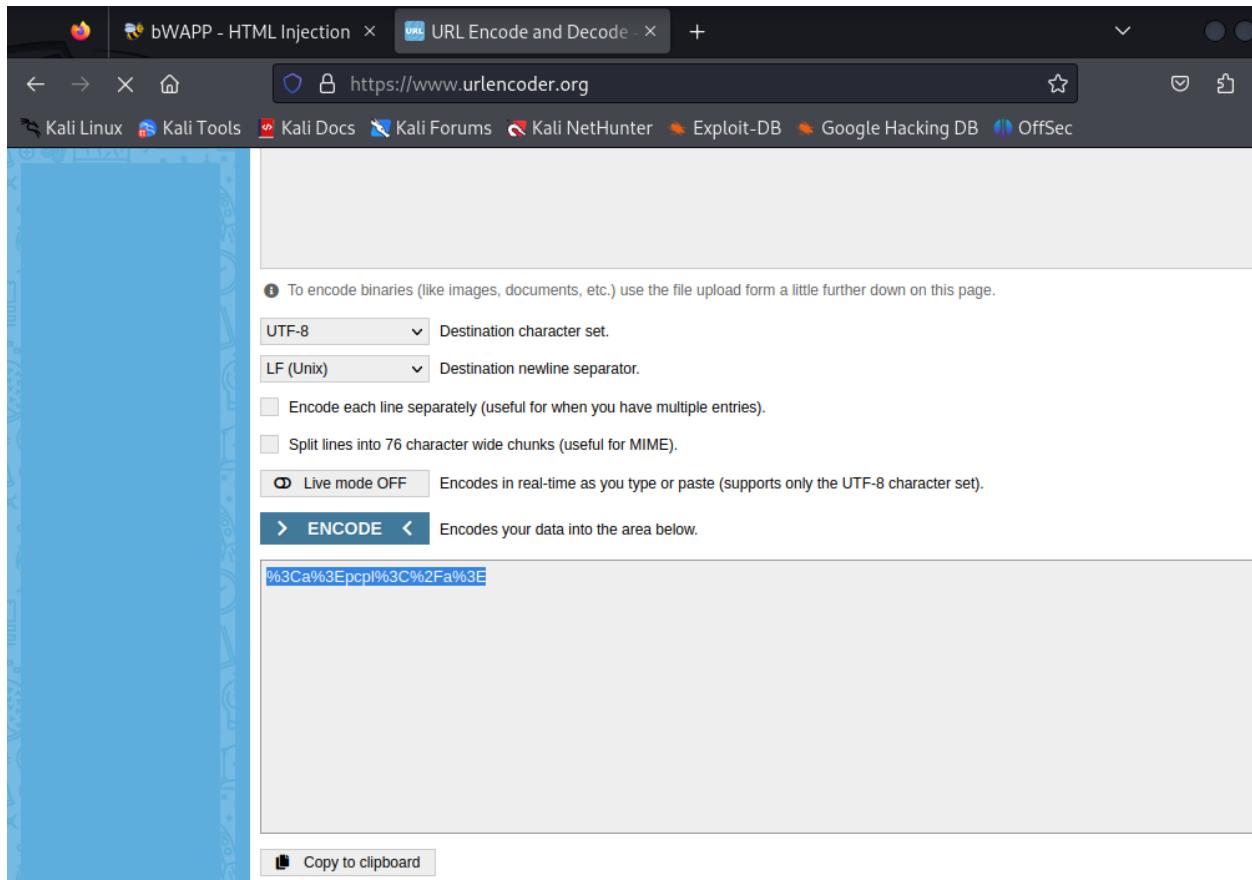
Simply enter your data then push the encode button.

```
<a>pcpl</a>
```

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.



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: 63Ca%3Epcpl%3C%2Fa%3E

Last name: <h2>friend</h2>

Go

Welcome <a>hack <

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%253D

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>

F bWAPP - HTML Injection X URL Encode and Decode +

localhost/bWAPP/htmli_get.php?firstname=%253Ca%253Epcpl%253C%252Fa%253E

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:

Welcome %3Ca%3Epcpl%3C%2Fa%3E <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

The screenshot shows a Firefox browser window with the URL `localhost/bWAPP/html_get.php?firstname=%253Ca%253Epcpl%253C%252Fa%`. The page title is "bWAPP - HTML Injection". The main content area has a yellow header with the text "Choose your bug: bWAPP v2.2" and "Hack". Below it, there's a "Set your security level:" dropdown set to "Current high". The main heading is "an extremely buggy web app!". A navigation bar at the bottom includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout".

The main content area displays the title "/ HTML Injection - Reflected (GET) /". It asks for "Enter your first and last name:". There are two input fields: "First name" containing "`www.vulnweb.com>Hacked`" and "Last name" containing "vulnweb". A "Go" button is present. The response below the form shows the output: "Welcome %3Ca%3Epcpl%3C%2Fa%3E <h2>friend</h2>".

A footer note states: "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".

The bottom part of the screenshot shows a modal dialog box with the same form fields and output, indicating the exploit worked.

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

localhost/bWAPP/htmli_get.php?firstname=%253Ca%2520href%253Dwww.vulnweb.com%253C%2Fa

Choose your bug:

- bWAPP v2.2
- 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)

bWAPP - iFrame Injection

localhost/bWAPP/iframei.php?ParamUrl=http://www.itsecgames.com/&ParamW=100

Tools

- bWAPP - Installation
http://localhost/bWAPP/install.php
- bWAPP, a buggy web application! Switch to Tab
- Download bWAPPv2.2.zip (bWAPP)
sourceforge.net/projects/bwappliance/files/bWAPP/bWAPPv2.2/bWAPPv2.2.zip/download?use_mirror=webw...

/ iFrame Injection /

bWAPP
an extremely buggy web app!

Home Bugs Download Talks & Training Blog

M Security

/ Home /

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 prepares one to conduct successful penetration testing and ethical hacking projects.

What makes bWAPP so unique? Well, it has over **100 web vulnerabilities**! It covers all major known web bugs, including all risks from the OWASP Top 10 project.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with WAMP or XAMPP. Another possibility is to download the *bee-box*, a custom Linux VM pre-installed with bWAPP.

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:

The screenshot shows a Firefox browser window with several tabs open, including "bWAPP - Ma", "URL Encode", "bWAPP, a bu", "FoxyProxy St", and "FoxyProxy O". The main content area displays the bWAPP homepage with a yellow header. The header features the bWAPP logo (a bee icon next to the text "bWAPP") and the tagline "an extremely buggy web app.". To the right of the logo, there are dropdown menus for "Choose your bug" (set to "bWAPP v2.2") and "Set your security level" (set to "low"). Below the header is a navigation bar with links: "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area has a title " / Mail Header Injection (SMTP) / ". Below the title, it says "E-mail us your questions at bwapp@mailinator.com." There are three input fields: "Name" (containing "hello"), "E-mail" (containing "hacker@gmail.com"), and "Remarks" (containing "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 Co

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

Repeater

Request

Response

Inspect

Target

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=dj2o2eqvcqklt7mmhghmruqsi; 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

1 HTTP/1.1 200 OK

2 Date: Tue, 17 Oct 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" />

Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer L

Organizer Extensions Learn

1 x +

Send **Cancel** < >

Target: http://localhost

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: 87
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/bWAPP/maili.php
12 Cookie: PHPSESSID=dj2o2eqvcqk1ct7mmhghmrqsi; 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\nbcc:youremailaddress.com&email=hacker%40gmail.com&remarks=hello&form=submit

```

Done

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Tue, 17 Oct 2023 08:56:01 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" />

```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

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 Unauthorized access, DOS etc.

Vulnerability Path: localhost/bWAPP/commandi.php

Vulnerability Parameter:localhost/bWAPP/commandi.php

Steps to reproduce:

Screenshot of a web browser showing the bWAPP v2.2 OS Command Injection page.

The URL in the address bar is `localhost/bWAPP/commandi.php`.

The page title is "OS Commandi".

The main content area displays the text: "Choose your bug: bWAPP v2.2", "Set your security level: low", and "an extremely buggy web app".

The navigation menu at the top includes links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Bugs, Change Password, Create User, Set Security Level, Reset, Credits, and Blog.

The main content area features a large title: "/ OS Command injection /". Below it is a form for a DNS lookup with the input field containing "www.nsa.gov" and a "Lookup" button.

The screenshot shows a Firefox browser window with three panels of the bWAPP web application. The top panel displays the main bWAPP interface with a yellow header, a logo, and a 'Choose your bug:' dropdown set to 'bWAPP v2.2'. The middle panel shows an OS Command Injection exploit where the user has entered 'www.nsa.gov' into a 'DNS lookup' field and clicked 'Lookup'. The bottom panel shows the result of the exploit, where the user has modified the URL to include '&&cat/etc/passwd' and clicked 'Lookup', resulting in a command injection payload.

bWAPP - OS Command Injection

localhost/bWAPP/commandi.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

bWAPP v2.2 Hack

Choose your bug:

Set your security level:

low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Log

/ OS Command Injection /

DNS lookup:

Server: 192.168.29.1 Address: 192.168.29.1#53 Non-authoritative answer: www.nsa.gov canonical name = nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 23.213.95.101 Name: e16248.dscb.akamaiedge.net Address: 2600:140f:5:a83::3f78 Name: e16248.dscb.akamaiedge.net Address: 2600:140f:5:aa9::3f78

/ OS Command Injection /

DNS lookup:

/ OS Command Injection /

DNS lookup:

Server: 192.168.29.1 Address: 192.168.29.1#53 Non-authoritative answer: www.nsa.gov canonical name = nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 23.213.95.101 Name: e16248.dscb.akamaiedge.net Address: 2600:140f:5:a83::3f78 Name: e16248.dscb.akamaiedge.net Address: 2600:140f:5:aa9::3f78

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 Unauthorized 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:

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:

Password:

Reload

Re-enter CAPTCHA:

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/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 Lo

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

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:109.0) Gecko/20100101 Firefox/109.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
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=djeisrfrrgqcar4jclg8jnbu4; security_level=1
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

Comment this item

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 x 2 x +

Positions Payloads Resource pool Settings

② Choose an attack type **Start attack**

Attacktype: Cluster bomb

③ 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=djeisrfrgqcar4jclg8jnbuf4; 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
```

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

Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings

1 x 2 x +

Positions Payloads Resource pool Settings

Start attack

Choose an attack type

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=djeisrfrrgcar4jclg8jnbuf4; 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: ?
18
19 login=$bee$$&password=$bug$&captcha_user=ummw%40&form=submit
```

Search... 0 highlights Clear Options! /

Burp Suite Community Edition v2020.5.1 Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Settings

1 x 2 x +

Positions **Payloads** Resource pool Settings

Payload sets

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: Payload count: 3
Payload type: 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 [only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

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

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

Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings

1 x 2 x +

Positions Payloads Resource pool Settings

Store requests
 Store responses
 Make unmodified baseline request
 Use denial-of-service mode (no results)
 Store full payloads

② **Grep - Match**

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Paste error exception illegal invalid fail stack access directory file not found

Load ... Remove Clear

Add Enter a new item

Match type: Simple string Regex

Case sensitive match Exclude HTTP headers

Confirm

Are you sure you want to clear the list?

Yes No

Grep - Match

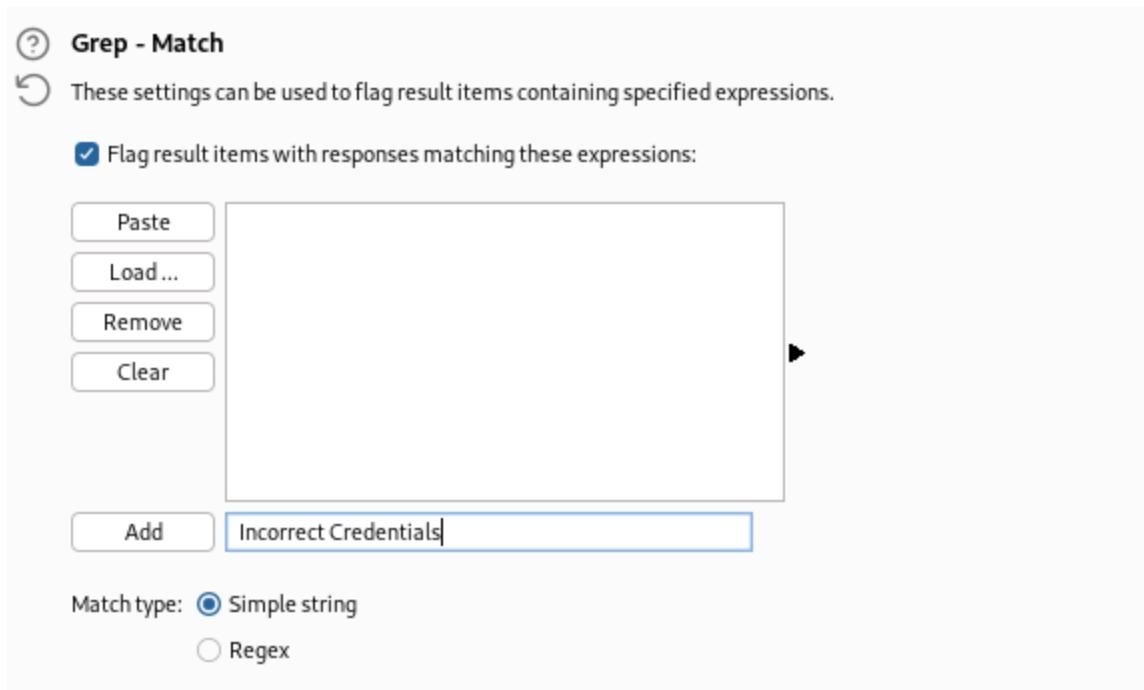
These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Paste
Load ...
Remove
Clear

Add

Match type: Simple string
 Regex



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:

A screenshot of a web browser displaying the bWAPP XSS - Reflected (JSON) page. The URL in the address bar is `localhost/bWAPP/xss_json.php`. The page has a yellow header with the bWAPP logo and a bee icon. It features a search bar with the placeholder "Search for a movie:" containing the text "Skyfall". Below the search bar is a hint message: "HINT: our master really loves Marvel movies :)".

A screenshot of a web browser displaying the bWAPP XSS - Reflected (JSON) page. The URL in the address bar is `localhost/bWAPP/xss_json.php?title=Skyfall&action=search`. The page shows an error message: "Skyfall??? Sorry, we don't have that movie :(

Bugs

Change Password

Create User

Set Security Level

Reset

/ XSS - Reflected (JSON) /

Search for a movie:

Skyfall??? Sorry, we don't have that movie :(

/ XSS - Reflected (JSON) /

Search for a movie:

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

The screenshot shows the bWAPP web application interface. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is the bWAPP logo with a bee icon and the text "an extremely buggy web app". On the right side, there are dropdown menus for "Choose your bug:" (set to "bWAPP v2.2") and "Set your security level:" (set to "low").

The main content area has tabs for "Bugs", "Change Password", "Security Level" (set to "low"), "Reset", "Credits", and "Blog". The "Security Level" tab is currently active. A context menu is open over a search input field containing the value "`"]}]';alert('Skyfall")</script>`". The menu options include "View Page Source" (which is highlighted in blue) and "Inspect (Q)".

The page title is "/ XSS - Reflected (JSON) /". The search input field contains the same malicious payload. The page content shows the following JavaScript code:

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

A modal dialog box is displayed, showing the URL "localhost" and the search term "Skyfall". An "OK" button is visible at the bottom right of the modal.

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/ssi.php

Vulnerability Parameter: localhost/bWAPP/ssi.php

Steps to reproduce:

The screenshot shows a web browser window with the URL `localhost/bWAPP/ssi.php` in the address bar. The page title is "Choose your bug: bWAPP v2.2". The main content area features a large "bWAPP" logo with a bee icon and the text "an extremely buggy web app.". On the right, there are settings for "Set your security level:" with a dropdown set to "low" and a "Set" button. Below the security level are navigation links: "Logs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area has a header "Server-Side Includes (SSI) Injection" and a sub-instruction "What is your IP address? Lookup your IP address... (bee-box only)". It contains two input fields for "First name" and "Last name", and a "Lookup" button.

/ Server-Side Includes (SSI) Injection /

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

First name:

Last name:

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Hello Smack Streams,

Your IP address is:

The screenshot shows the bWAPP web application interface. At the top, there's a yellow header with the bWAPP logo (a bee) and the text "an extremely buggy web app.". On the right side of the header, there are dropdown menus for "Choose your bug:" (set to "bWAPP v2.2") and "Set your security level:" (set to "low"). Below the header, a navigation bar includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area has a title "Server-Side Includes (SSI) Injection". Below the title, there's a note: "What is your IP address? Lookup your IP address... (bee-box only)". There are two input fields: "First name:" containing "<--#exec cmd='id'-->" and "Last name:" containing "<--#exec cmd='cat/etc/passwd'" with a "Lookup" button below it. The browser's address bar shows "localhost/bWAPP/ssi.shtml". The Kali Linux desktop environment is visible at the bottom.

Hello <--#exec Cmd="id"--> <--#exec Cmd="cat/etc/passwd"-->,

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:

The screenshot shows a web browser window with the URL `localhost/bWAPP/clickjacking.php` in the address bar. The page has a yellow header with the text "Choose your bug: bWAPP v2.2" and a "Hack" button. It also features a "Set your security level" dropdown set to "low" with a "Set Current: low" button. The main content area is titled "/ ClickJacking (Movie Tickets) /". It asks "How many movie tickets would you like to order? (15 EUR per ticket)" and has a text input field containing "10". A "Confirm" button is at the bottom. The footer contains a license notice: "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! /".

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 tickets.

HINT: open the evil [ClickJacking page](#) in a new tab...

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! /

The screenshot shows a Firefox browser window with several tabs open, including 'bWAPP - Click', 'http://localhost', 'URL Encode', 'FoxyProxy SI', and 'FoxyProxy O'. The main content is the bWAPP web application. At the top, there's a yellow header with the bWAPP logo and a bee icon. It says 'Choose your bug: bWAPP v2.2' and 'Hack'. Below that, it says 'Set your security level: low' with a dropdown menu set to 'low'. A red note says 'an extremely buggy web app.' In the main area, there's a heading '/ ClickJacking (Movie Tickets) /'. Below it, a question asks 'How many movie tickets would you like to order? (15 EUR per ticket)'. A text input field contains '10'. A hint below says 'HINT: open the evil ClickJacking page in a new tab...'. A 'Confirm' button is at the bottom left. A success message at the bottom right says 'You ordered 10 movie tickets. Total amount charged from your account automatically: 150 EUR.' and 'Thank you for your order!'. The navigation bar at the bottom includes links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'.

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:

The screenshot shows a Firefox browser window with several tabs open. The active tab is http://localhost/bWAPP/directory_traversal_2.php?directory=documents. The page content is as follows:

bWAPP 
an extremely buggy web app.

Choose your bug:

Set your security level: 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 [\(CC\) BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! /

bWAPP

an extremely buggy web app

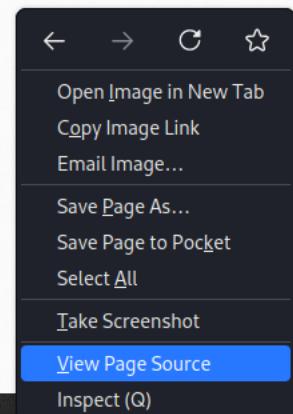
Choose your bug:
----- bWAPP v2.2 -----

Set your security level:
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Log Out

/ 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



File Machine View Input Devices Help

localhost/bWAPP/documents/Terminator_Salvation.pdf

Terminator Salvation (2009) - IMDb

IMDb

Terminator Salvation (2009)

Your rating: 6.7

Ratings: 6.7/10 from 171,746 users Metascore: 52/100

Reviews: 920 user | 387 critic | 35 from Metacritic.com

Undo Redo Cut Copy Paste Paste and Go Delete Select All

Page 1 of 3

J'aime 2 370 personnes aiment ça.

Quick Links: overview

The image shows a Kali Linux desktop environment with two Firefox browser windows open.

Top Browser Window:

- Address bar: `localhost/bWAPP/directory_traversal_2.php?directory=documents/..%2f`
- Title: `http://localhost/bWAPP/directory_traversal_2.php?directory=documents/..%2f`
- Content: The bWAPP homepage with the text "an extremely buggy web app".
- Right sidebar: "Set your security level:" dropdown set to "low".

Bottom Browser Window:

- Address bar: `localhost/bWAPP/directory_traversal_2.php?directory=documents/..%2f`
- Title: `http://localhost/bWAPP/directory_traversal_2.php?directory=documents/..%2f`
- Content: The exploit results page titled "/ Directory Traversal - Directories /". It lists numerous PHP files, likely demonstrating the exploit's success.
- Bottom footer: "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"

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 

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

Set your security level:
 Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Log

/ Restrict Device Access /

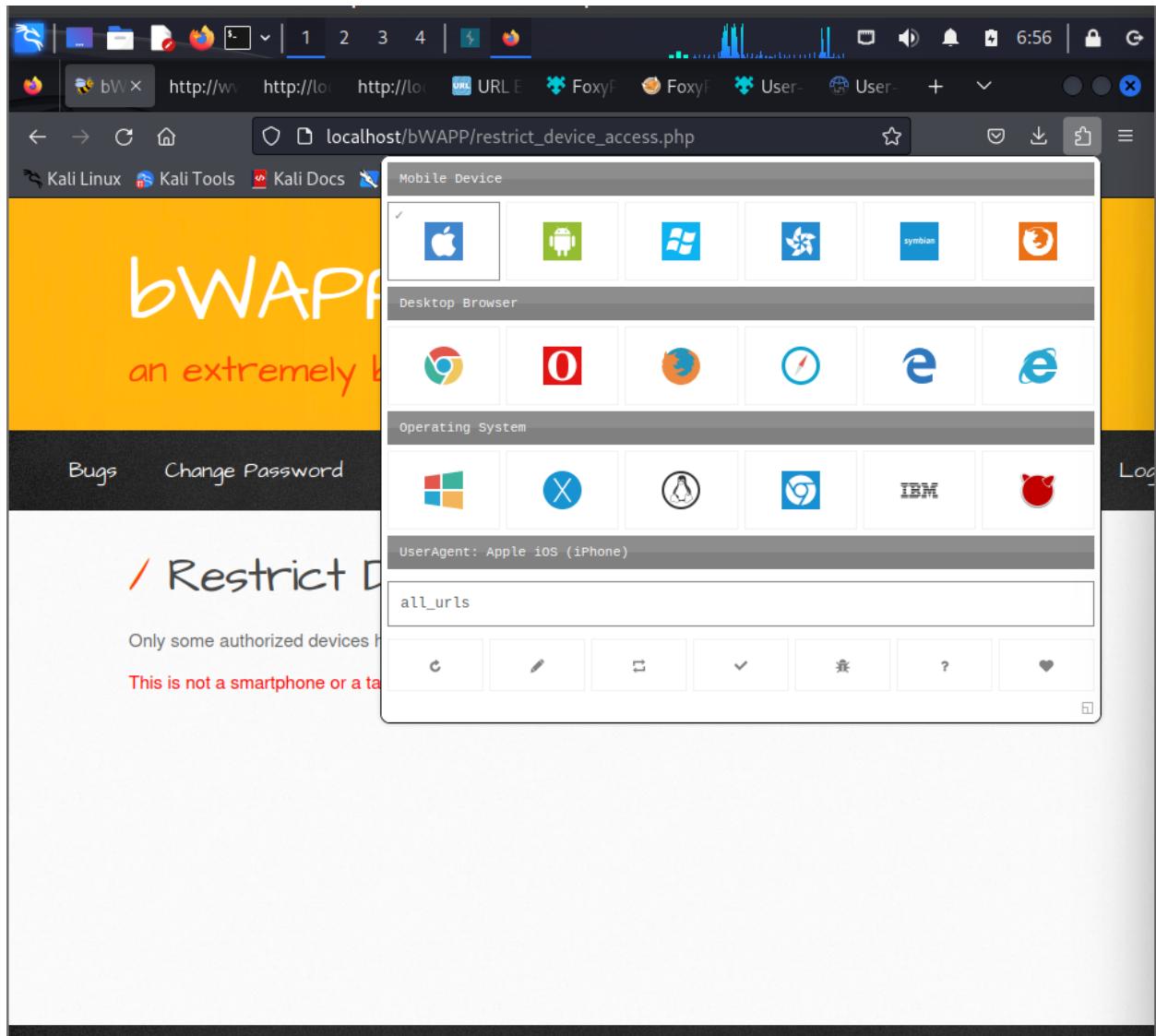
Only some authorized devices have access to the content of this page.

This is not a smartphone or a tablet computer (Apple/Android)!

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

The screenshot shows a web browser window with the following details:

- Address Bar:** https://mybrowseraddon.com/useragent-switcher.html?v=0.3.
- Toolbar:** Applications, http://w..., http://l..., http://l..., URL E, FoxyF, FoxyF, User-, Us...
- Menu Bar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Page Header:** Home, Features, FAQ, Feedback, Reviews, Donation, ☾
- Content Area:**
 - An "Advertisement" section with a large green button labeled "Start". To its right, instructions: 1. Tap "Start"!, 2. Choose Your Option, 3. Enjoy! There is also a "Close" button (ⓘ X) and a "Dismiss" button (ignaly).
 - A link to "User-Agent Switcher | Download" with icons for GitHub, SourceForge, and others.
 - A brief description: "Quickly and easily switch between popular user-agent strings."
 - A paragraph about the addon's features, mentioning its purpose, functions, and how to report bugs or suggest improvements.
 - A summary statement: "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
 - A cookie consent banner at the bottom: "We use cookies to enhance your experience. By continuing to visit this site you agree to our use of cookies. Learn more" with a "Got it!" button.



A screenshot of a Firefox browser window displaying the `localhost/bWAPP/restrict_device_access.php` page. The page has a yellow header with the text "Choose your bug: bWAPP v2.2 Hack" and "Set your security level: low Set Current: low". Below the header, there's a navigation bar with links like "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a title "*/ Restrict Device Access /*" and a message: "Only some authorized devices have access to the content of this page. This is a smartphone or a tablet computer!"