Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 07/09/2023

Assignment Details

Assigned Date: 06/09/2023

Due Date: 07/09/2023

Topic: Fuzzing

Introduction

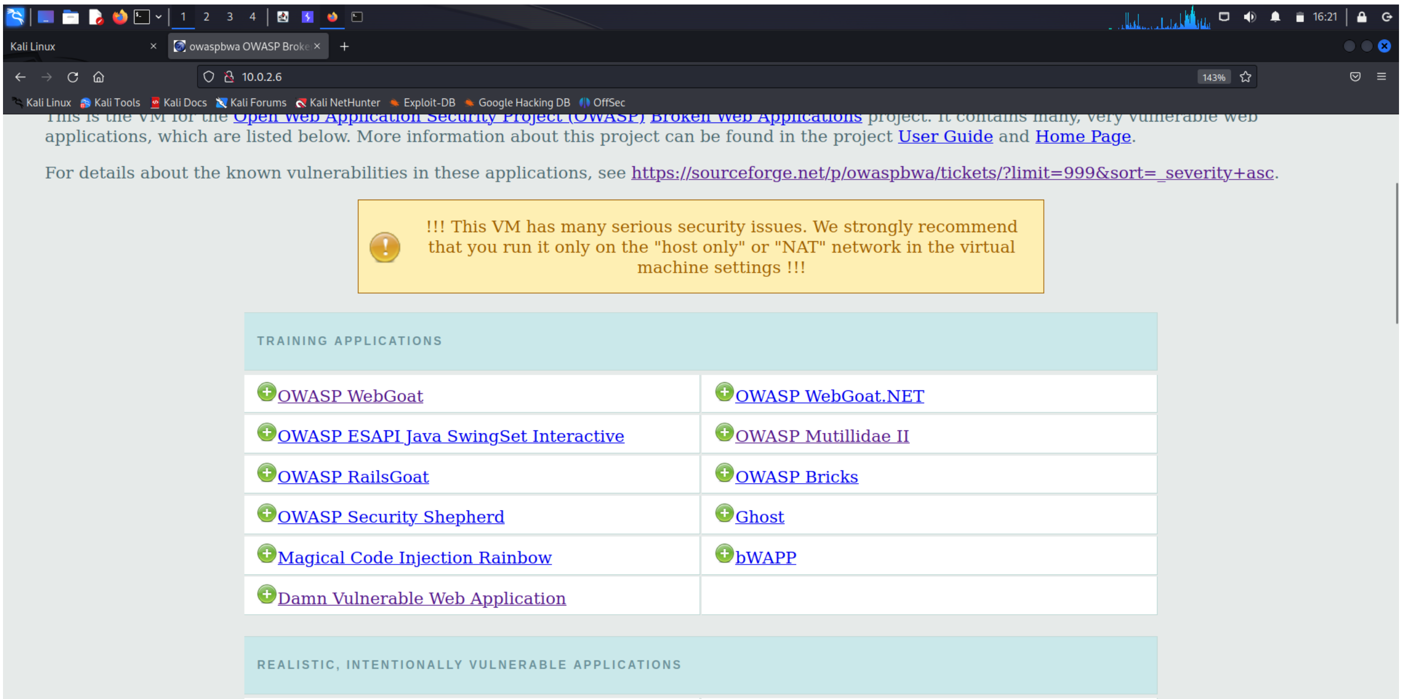
Fuzzing is a software testing technique used to uncover vulnerabilities and weaknesses in computer programs, applications, or systems. It involves the automated generation and submission of a large volume of unexpected, invalid, or random data as input to the target software. The primary goal of fuzzing is to identify security flaws, crashes, and unexpected behaviour that may be indicative of vulnerabilities that can be exploited by attackers.

During the fuzzing process, a fuzzing tool or framework generates various inputs, such as malformed data packets, unexpected command sequences, or random values, and sends them to the target software's input points, such as user interfaces, APIs, network protocols, or file parsers. The fuzzing tool monitors the target for any signs of abnormal behaviour, including crashes, hangs, excessive resource consumption, or error messages.

Fuzzing is particularly effective for uncovering memory-related vulnerabilities like buffer overflows, as well as input validation issues and boundary conditions that can lead to security vulnerabilities. It is an essential part of the security testing process, helping organizations identify and mitigate potential security risks in their software before they can be exploited by malicious actors. Fuzzing can be applied at different stages of the software development lifecycle, from early development to post-deployment security assessments, making it a valuable tool in ensuring the robustness and security of software systems.

Content

Open the OWASP Broken Web Application


Kali Linux
owaspbwa OWASP Broke
10.0.2.6
143%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
16:21

This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

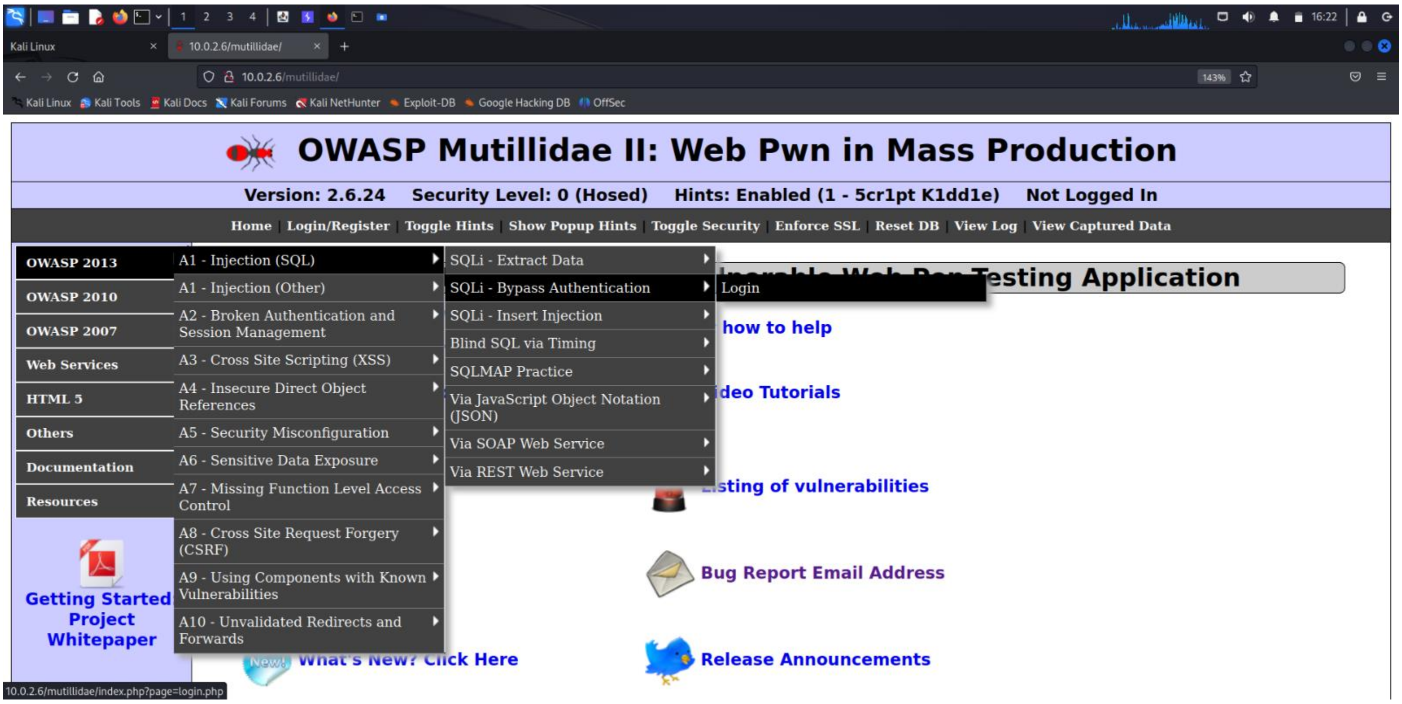
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS

Open the Mutillidae II broken application in the OWASP BWA.

Open the Login page. The path of the Login page is displayed below.

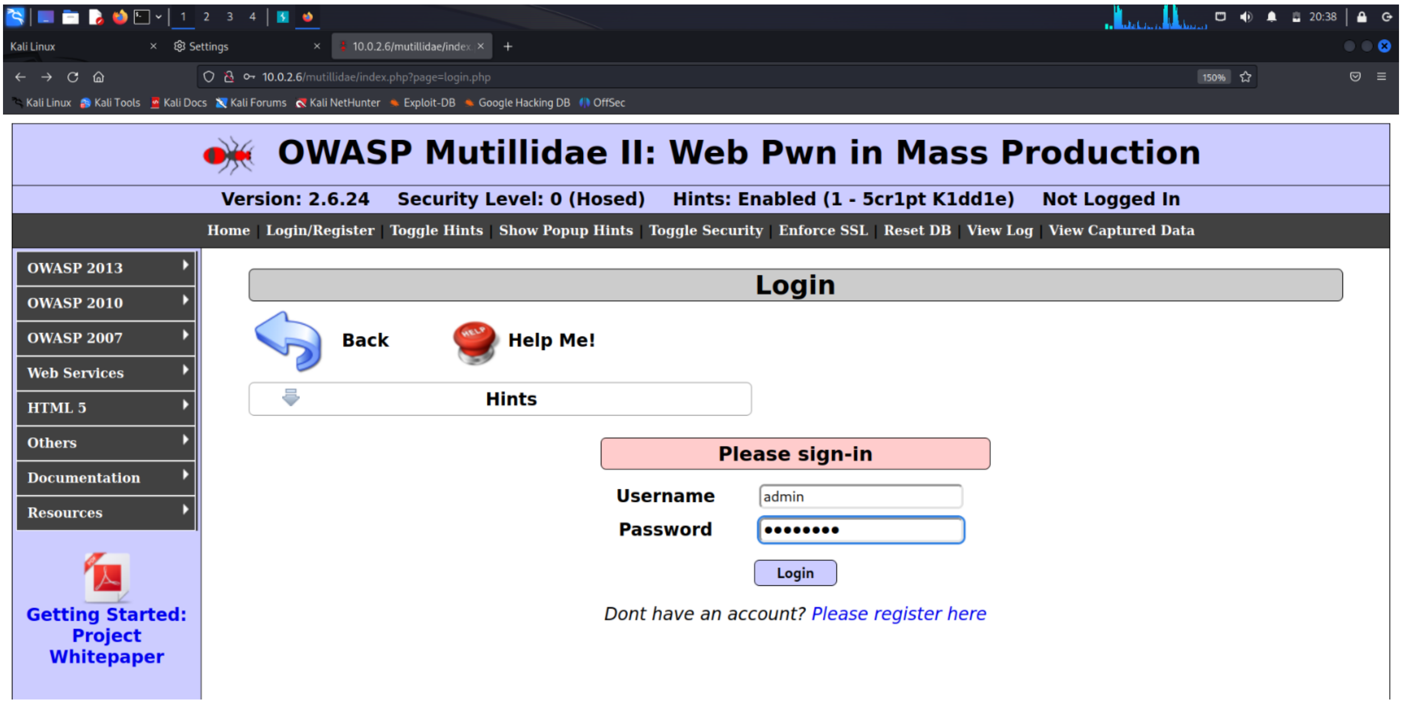

Kali Linux
10.0.2.6/mutillidae/
10.0.2.6/mutillidae/
143%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
16:22
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
SQLi - Extract Data
SQLi - Bypass Authentication
SQLi - Insert Injection
Blind SQL via Timing
SQLMAP Practice
Via JavaScript Object Notation (JSON)
Via SOAP Web Service
Via REST Web Service
Login
...nerable Web Pen Testing Application
...how to help
...ideo Tutorials
...isting of vulnerabilities
Bug Report Email Address
Release Announcements
Getting Started Project Whitepaper
What's New? Click Here
10.0.2.6/mutillidae/index.php?page=login.php

Enter the username ‘admin’ since this parameter is known.

Enter any password.

Username: admin

Password: password


Kali Linux
Settings
10.0.2.6/mutillidae/index
10.0.2.6/mutillidae/index.php?page=login.php
Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Back
Help Me!
Hints
Login

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Login

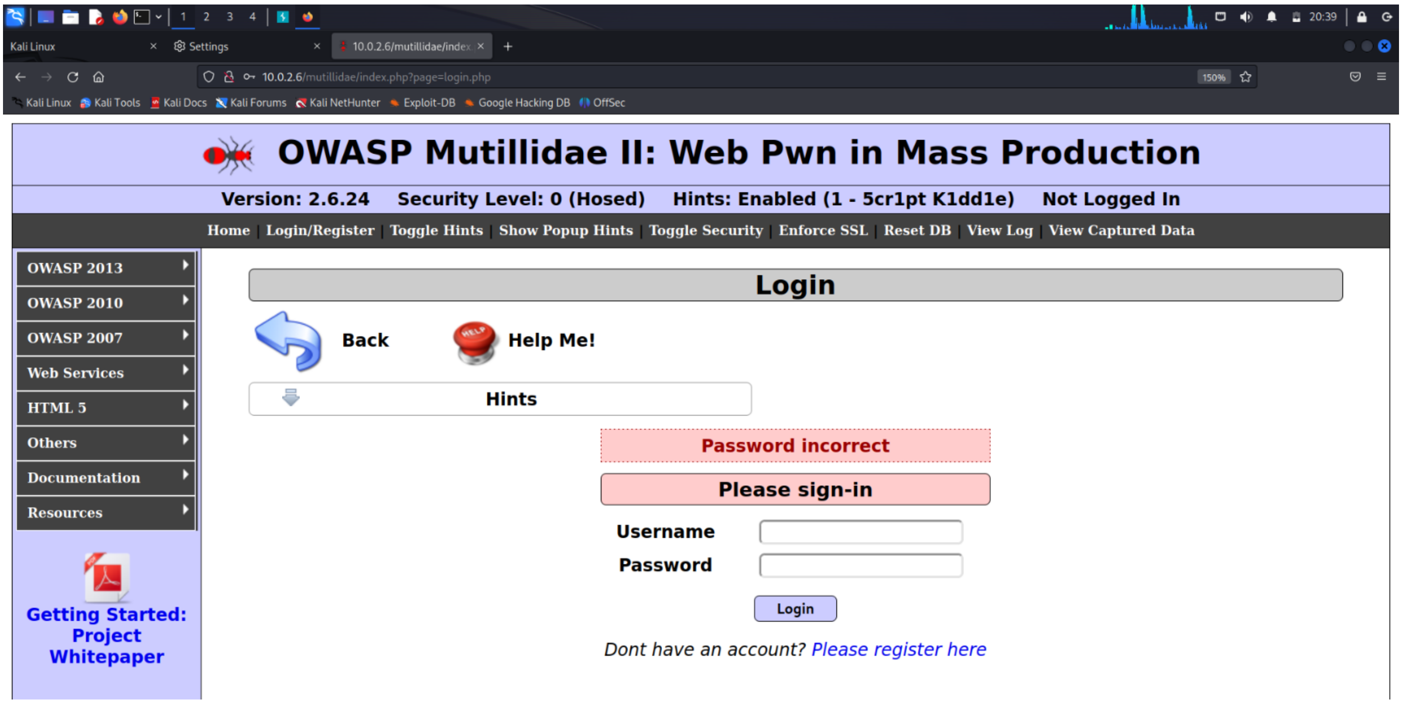
Please sign-in

Username: admin

Password: ••••••••

Dont have an account? Please register here

The entered password is incorrect and obviously denied.


Kali Linux
Settings
10.0.2.6/mutillidae/index
10.0.2.6/mutillidae/index.php?page=login.php
Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Back
Help Me!
Hints
Login

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Login

Password incorrect

Please sign-in

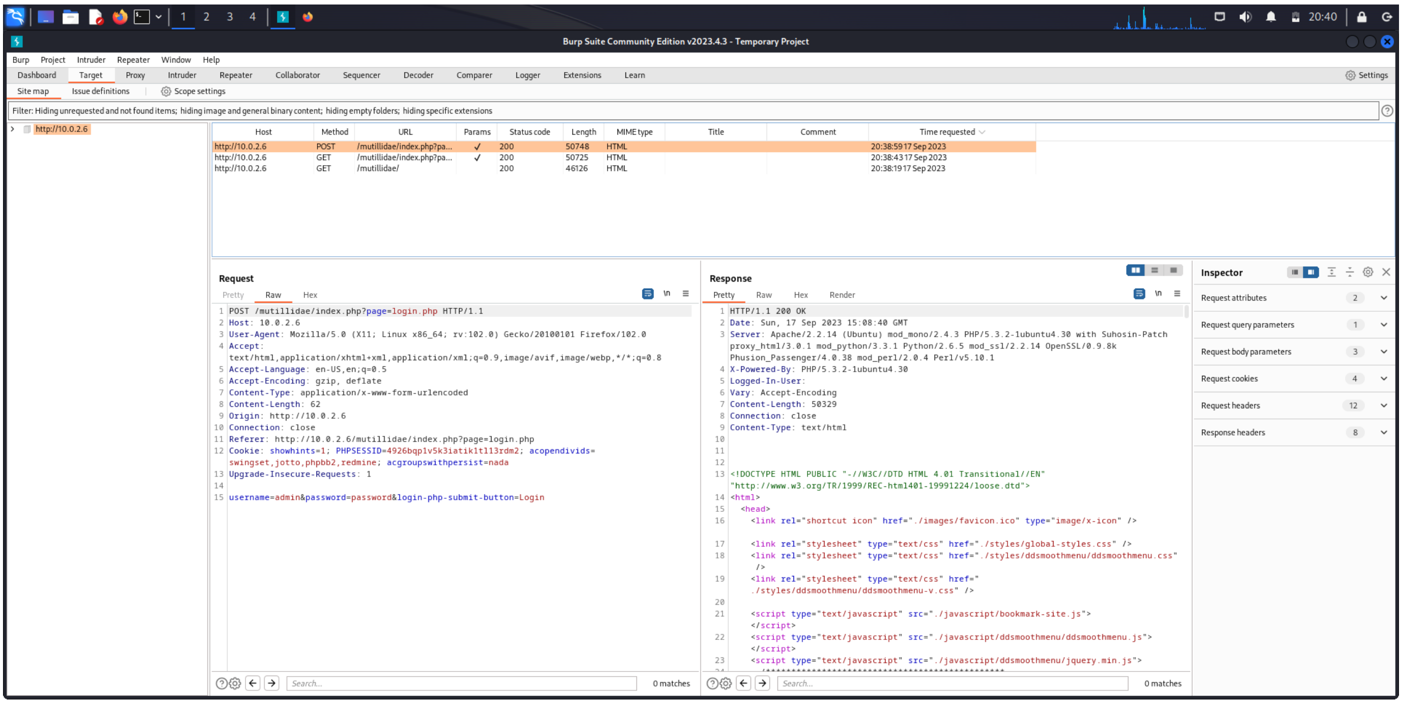
Username:

Password:

Dont have an account? Please register here

Catch the entered username and password int the Target tab of the burpsuite.

The Request makes use of the POST method.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Site map Issue definitions Scope settings
http://10.0.2.6
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 3
Request cookies 4
Request headers 12
Response headers 8
0 matches

Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
http://10.0.2.6	POST	/mutillidae/index.php?pa...	✓	200	50748	HTML			20:38:59 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/index.php?pa...	✓	200	50725	HTML			20:38:43 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/		200	46126	HTML			20:38:19 17 Sep 2023

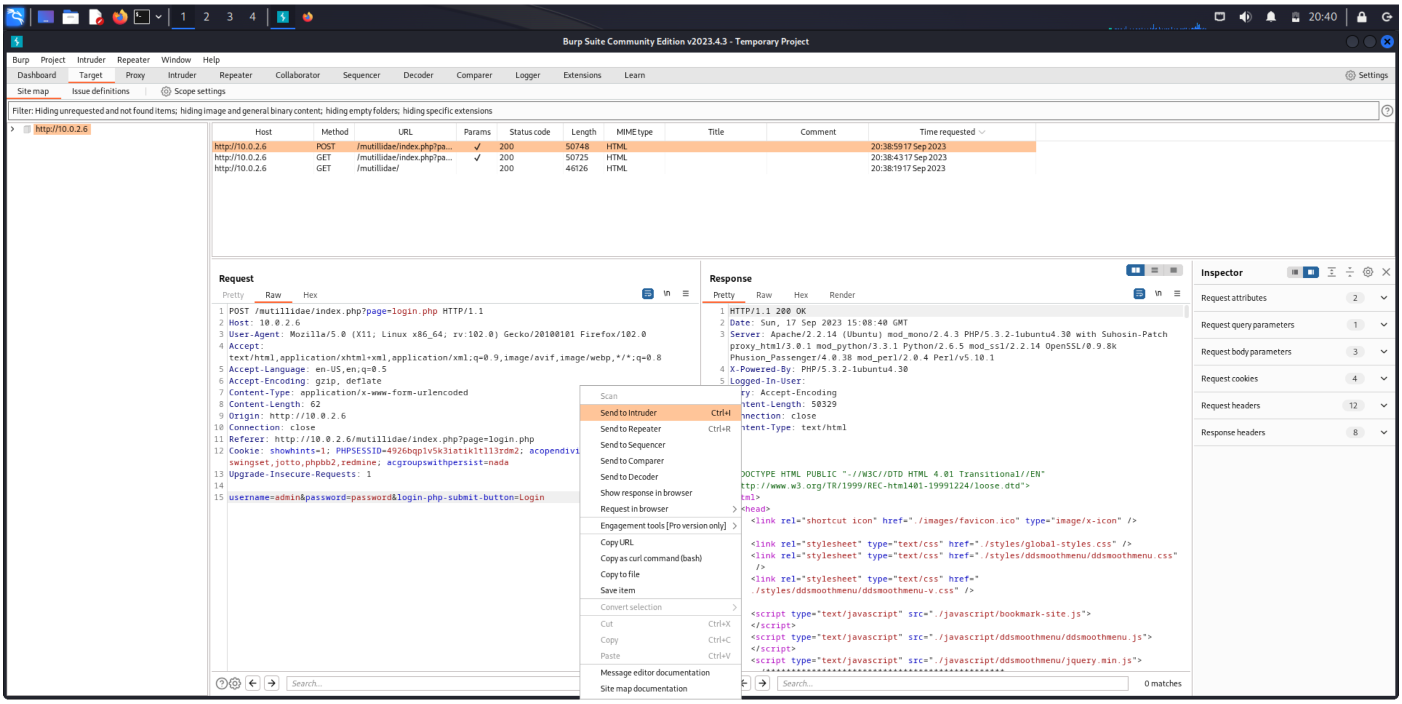
Request

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivids=
swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

username=admin&password=password&login-php-submit-button=Login
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 17 Sep 2023 15:08:40 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50329
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
  <head>
    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />

    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css"
     />
    <link rel="stylesheet" type="text/css" href="
    ./styles/ddsmoothmenu/ddsmoothmenu-v.css" />

    <script type="text/javascript" src="./javascript/bookmark-site.js">
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js">
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
```

Right click the HTTP Request Message in the burpsuite and click on ‘Send to Intruder’.

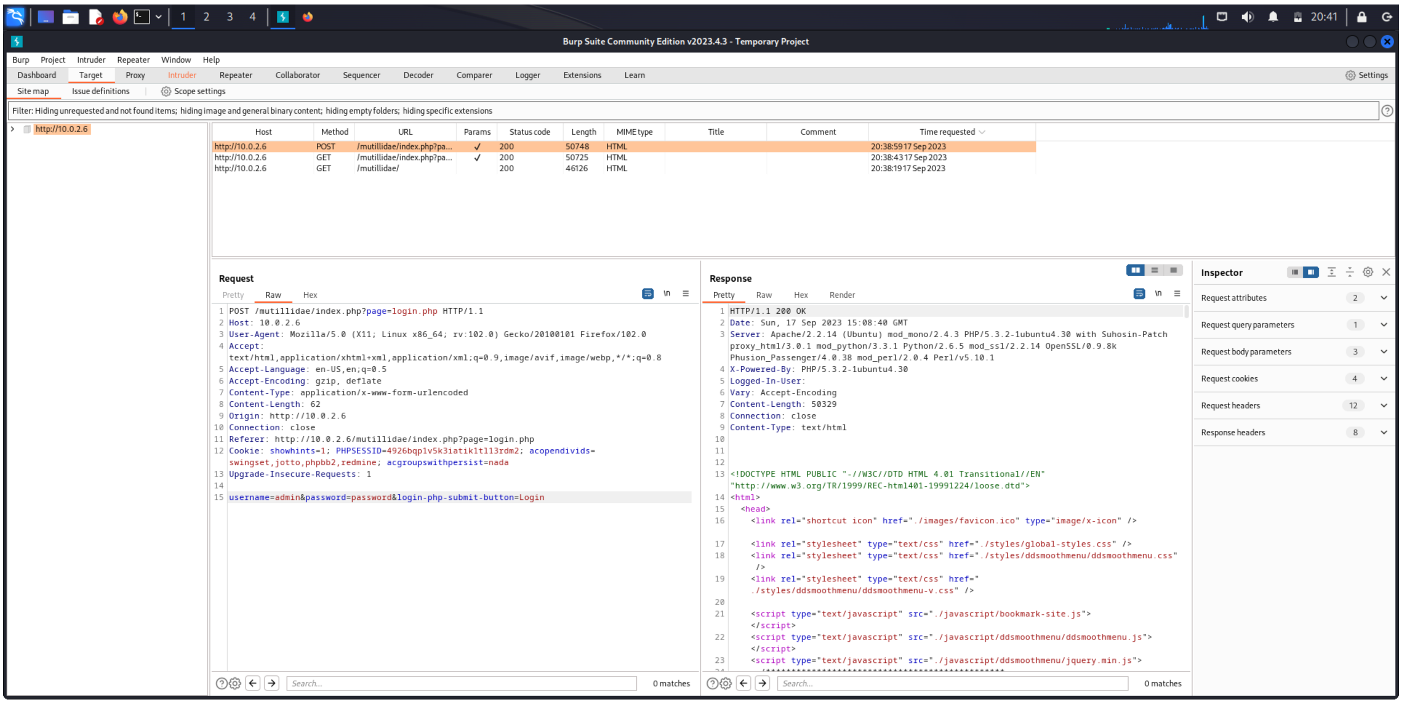


Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
http://10.0.2.6	POST	/mutillidae/index.php?pa...	✓	200	50748	HTML			20:38:59 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/index.php?pa...	✓	200	50725	HTML			20:38:43 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/		200	46126	HTML			20:38:19 17 Sep 2023

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivi
swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

username=admin&password=password&login-php-submit-button=Login
```

When the HTTP Request Message is sent to the Intruder tab, it is highlighted in red color indicating that the message has been successfully sent to the Intruder tab.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Site map Issue definitions Scope settings
http://10.0.2.6
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 3
Request cookies 4
Request headers 12
Response headers 8
Search...
0 matches

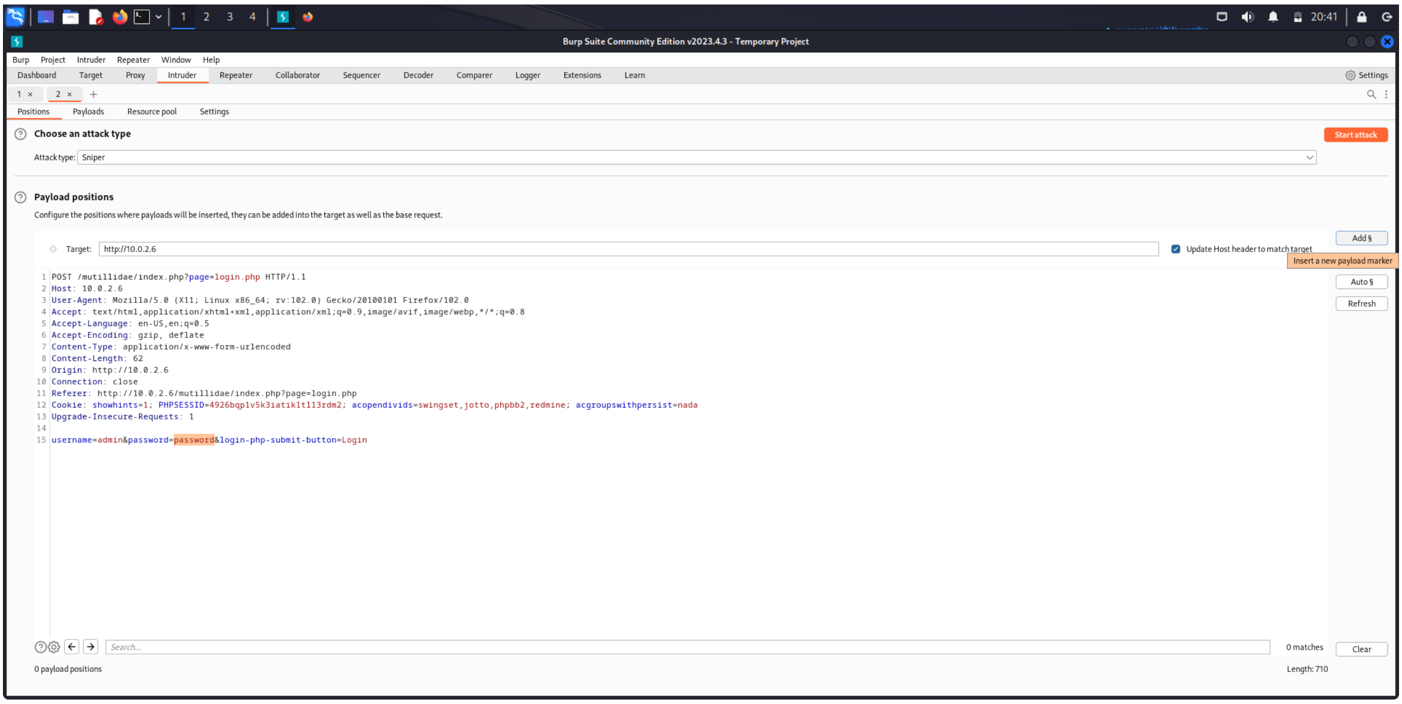
Filter: Hiding unrequested and not found items; hiding image and general binary content; hiding empty folders; hiding specific extensions

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
http://10.0.2.6	POST	/mutillidae/index.php?pa...	✓	200	50748	HTML			20:38:59 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/index.php?pa...	✓	200	50725	HTML			20:38:43 17 Sep 2023
http://10.0.2.6	GET	/mutillidae/		200	46126	HTML			20:38:19 17 Sep 2023

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivids=
swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

username=admin&password=password&login-php-submit-button=Login
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Sep 2023 15:08:40 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 50329
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
  <head>
    <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />

    <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css"
     />
    <link rel="stylesheet" type="text/css" href="
    ./styles/ddsmoothmenu/ddsmoothmenu-v.css" />

    <script type="text/javascript" src="./javascript/bookmark-site.js">
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js">
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
```

Select the fake password which was entered during the login process and click on Add on the right edge of Burpsuite.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Insert a new payload marker
Auto §
Refresh
Search...
0 matches
Clear

Choose an attack type

Attack type: Sniper

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://10.0.2.6

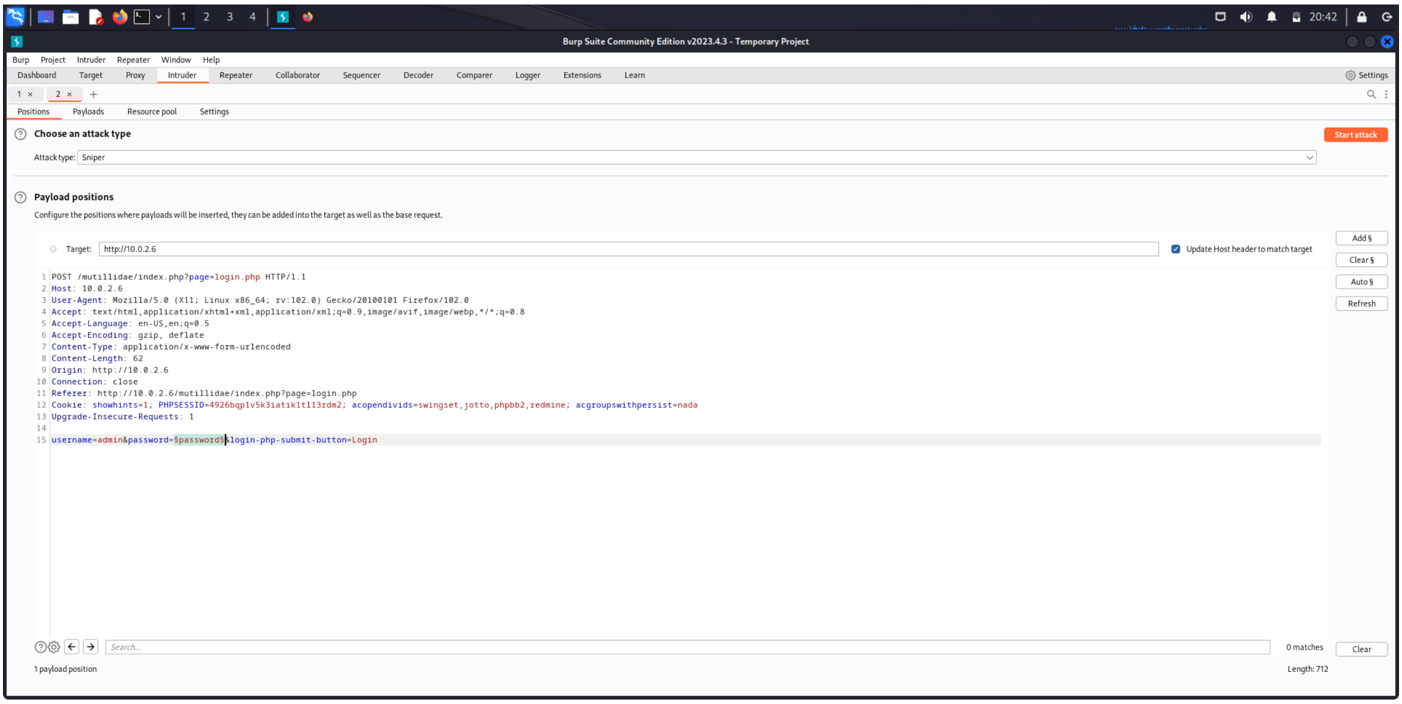
☑ Update Host header to match target

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

username=admin&password=password&login-php-submit-button=Login
```

0 payload positions

Length: 710

After adding the password, it is marked.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear

Choose an attack type

Attack type: Sniper

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://10.0.2.6

☑ Update Host header to match target

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

username=admin&password=§password§&login-php-submit-button=Login
```

Search...

0 matches

1 payload position

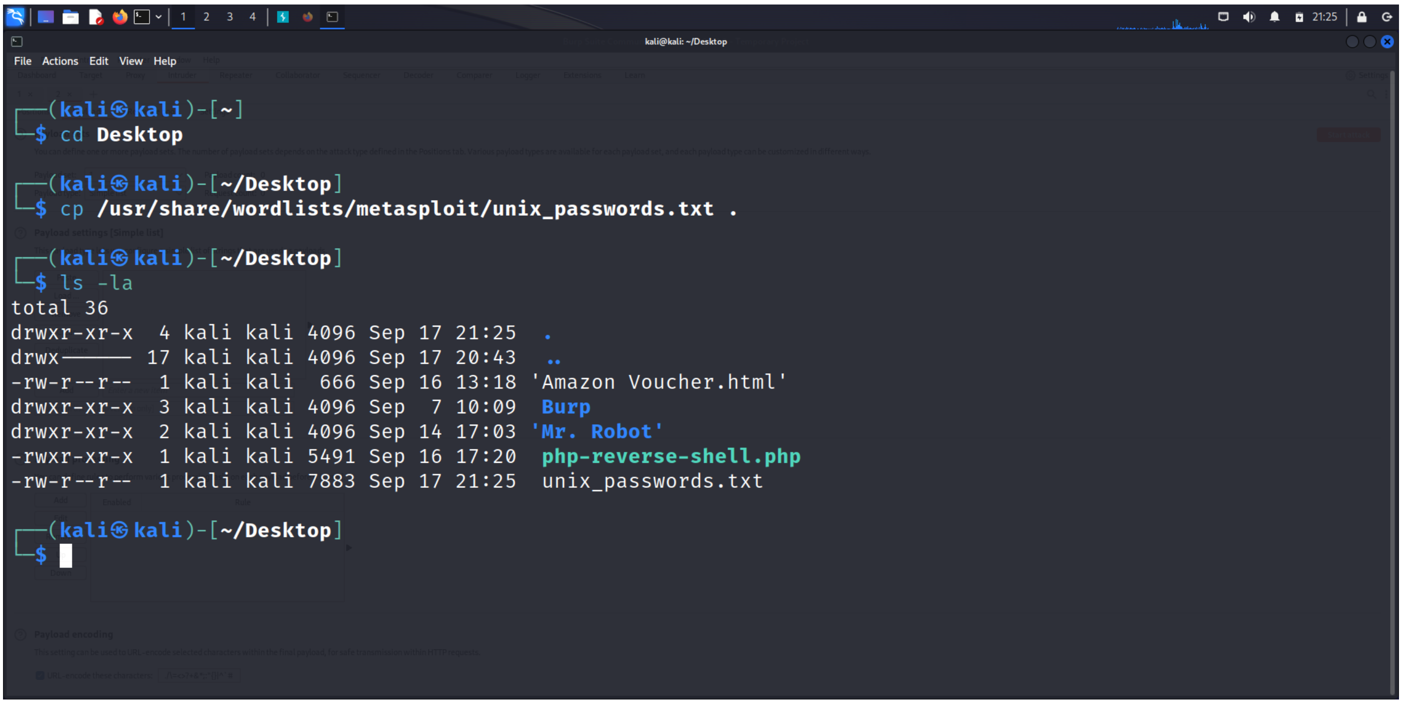
Length: 712

A file unix_passwords.txt contains all the common passwords which are used int web.

Copy the unix_passwords.txt file onto a desired location.

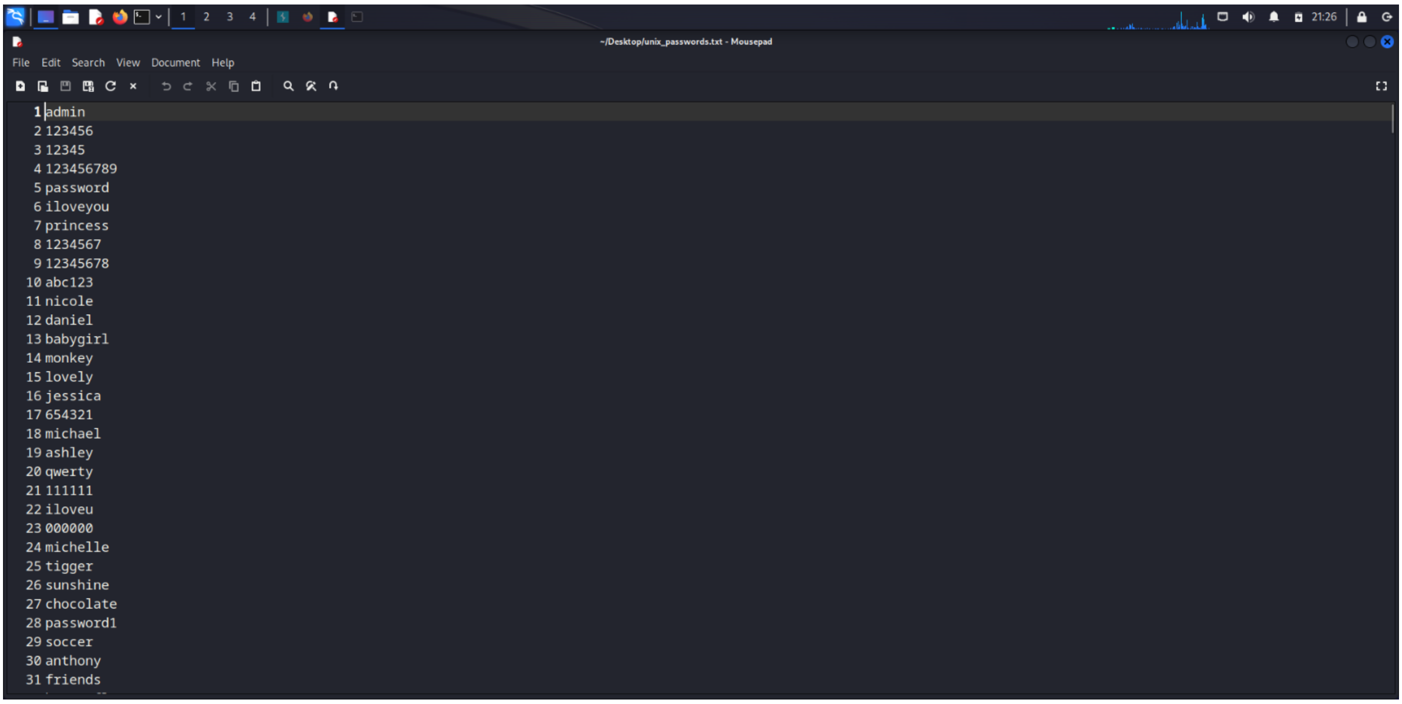
Syntax: cp source destination //Copy command from source to destination

Command: cp /usr/share/wordlists/metasploit/unix_passwords.txt . // . represents the pwd



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cp /usr/share/wordlists/metasploit/unix_passwords.txt .

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -la
total 36
drwxr-xr-x  4 kali kali 4096 Sep 17 21:25  .
drwx------ 17 kali kali 4096 Sep 17 20:43  ..
-rw-r--r--  1 kali kali  666 Sep 16 13:18 'Amazon Voucher.html'
drwxr-xr-x  3 kali kali 4096 Sep  7 10:09  Burp
drwxr-xr-x  2 kali kali 4096 Sep 14 17:03 'Mr. Robot'
-rwxr-xr-x  1 kali kali 5491 Sep 16 17:20  php-reverse-shell.php
-rw-r--r--  1 kali kali 7883 Sep 17 21:25  unix_passwords.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

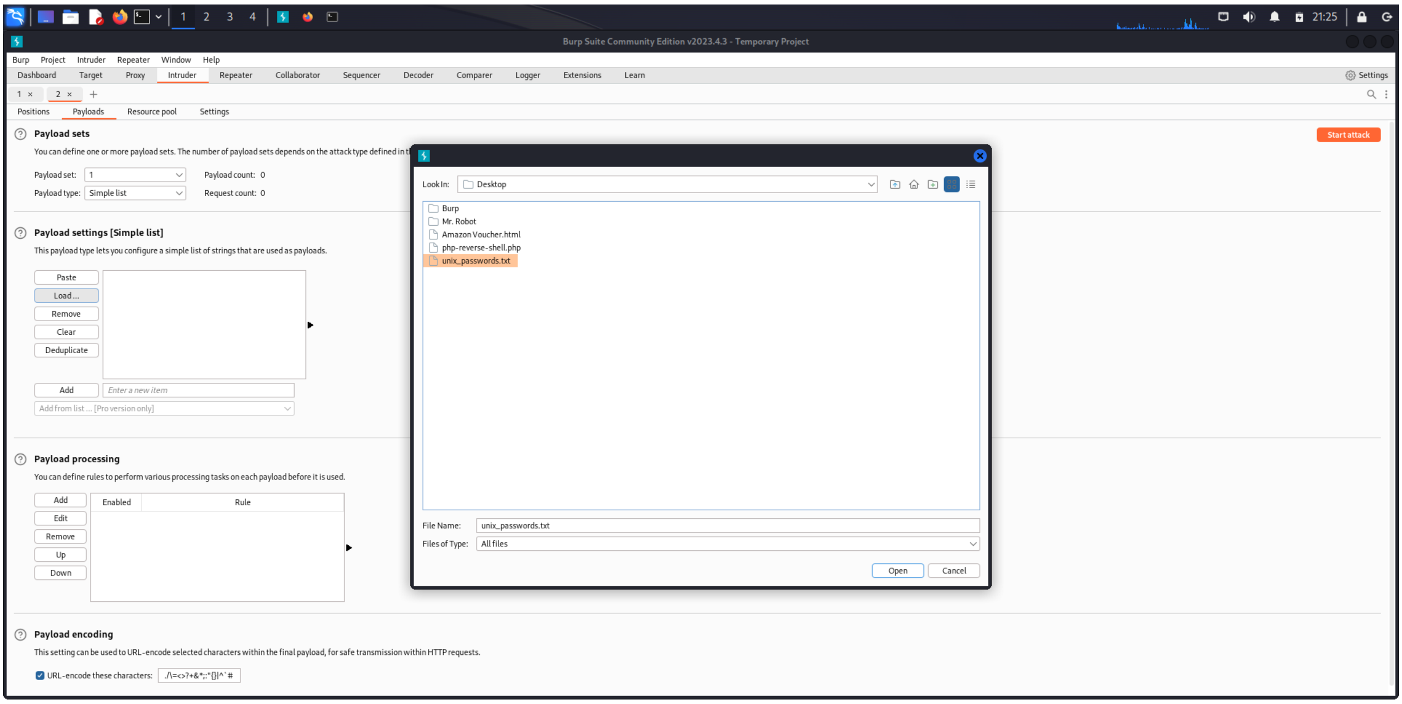
List of all the keywords in the unix_passwords.txt dictionary file.


~/Desktop/unix_passwords.txt - Mousepad
File Edit Search View Document Help

```
admin
123456
12345
123456789
password
iloveyou
princess
1234567
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
```

Open the Payloads section in the Intruder tab.

Load the unix_passwords.txt file in the Payload settings.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in t

Payload set: 1

Payload type: Simple list

Payload count: 0

Request count: 0

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
Add
Enter a new item
Add from list ... [Pro version only]

Payload processing

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

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

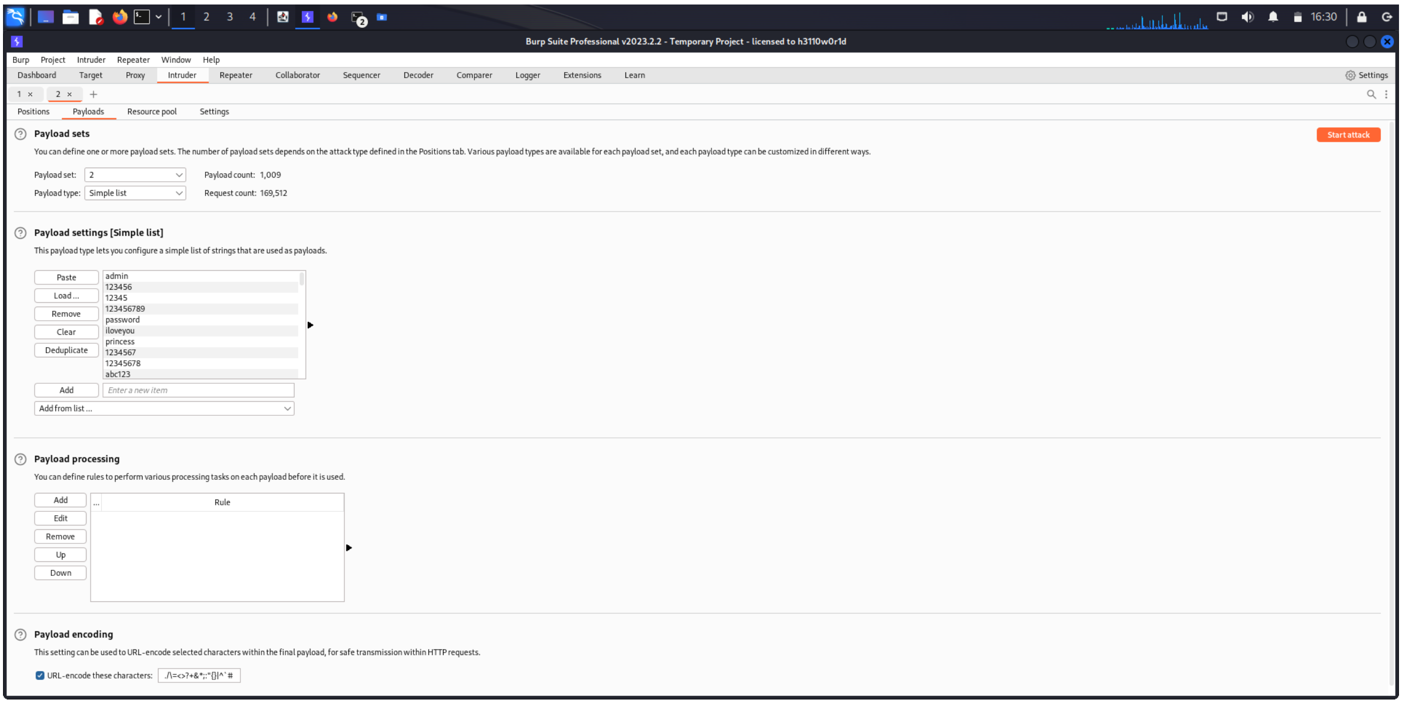
Look In: Desktop

- Burp
- Mr. Robot
- Amazon Voucher.html
- php-reverse-shell.php
- unix_passwords.txt

File Name: unix_passwords.txt

Files of Type: All files

We can see that unix_passwords.txt has been loaded onto the burpsuite.



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack

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: 2 Payload count: 1,009

Payload type: Simple list Request count: 169,512

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
123456
12345
123456789
password
iloveyou
princess
1234567
12345678
abc123
```

Payload processing

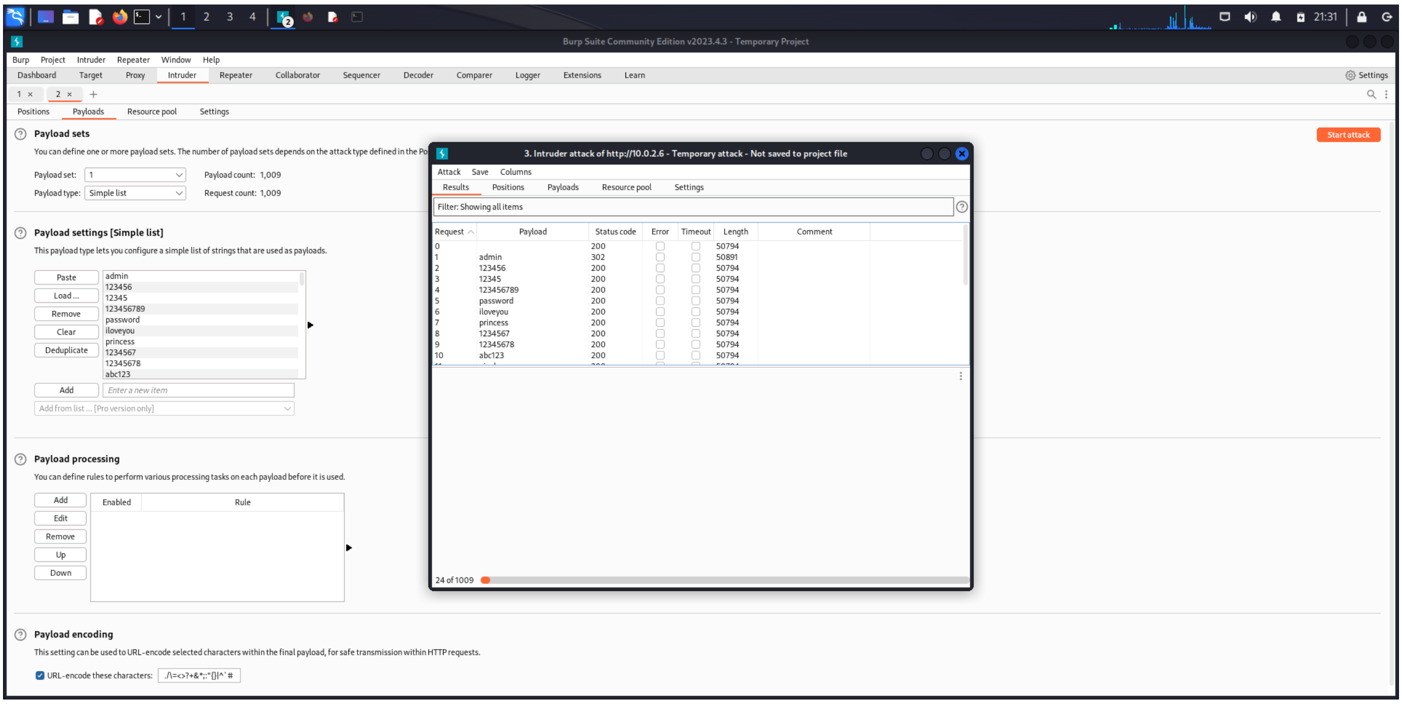
You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

After configuring the payload, start the attack by clicking on the Start Attack button on the top-right corner of burpsuite. The attack has been started.



Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack
Add from list ... [Pro version only]
Enabled Rule

Payload set: 1 Payload count: 1,009

Payload type: Simple list Request count: 1,009

3. Intruder attack of http://10.0.2.6 - Temporary attack - Not saved to project file

Attack Save Columns
Results Positions Payloads Resource pool Settings

Filter: Showing all items

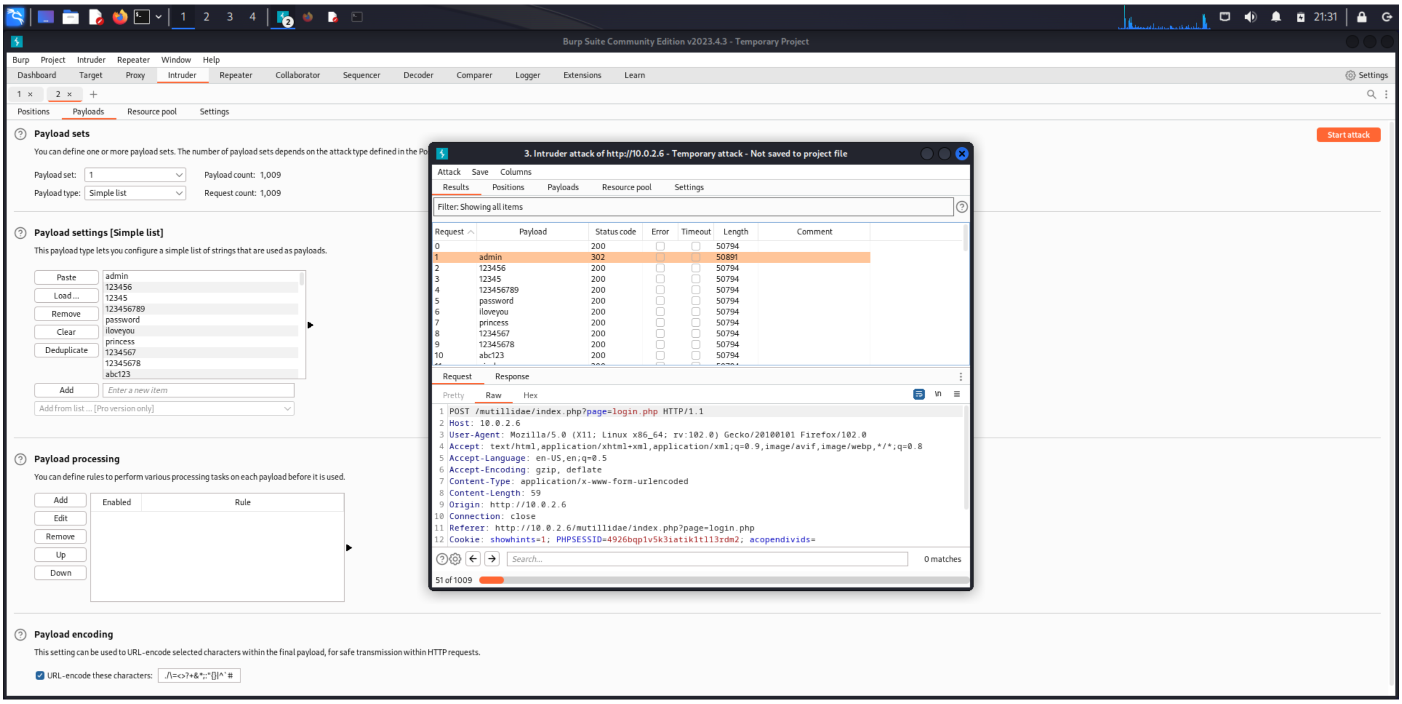
Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	50794	
1	admin	302	□	□	50891	
2	123456	200	□	□	50794	
3	12345	200	□	□	50794	
4	123456789	200	□	□	50794	
5	password	200	□	□	50794	
6	iloveyou	200	□	□	50794	
7	princess	200	□	□	50794	
8	1234567	200	□	□	50794	
9	12345678	200	□	□	50794	
10	abc123	200	□	□	50794	

24 of 1009

Click on the cracked password.

It displays the HTTP Request message sent to that Login page.

In this case, the password turned out to be the ‘admin’.



Burp Suite Community Edition v2023.4.3 - Temporary Project

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Po

Payload set: 1 Payload count: 1,009

Payload type: Simple list Request count: 1,009

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Payload processing

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

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

3. Intruder attack of http://10.0.2.6 - Temporary attack - Not saved to project file

Filter: Showing all items

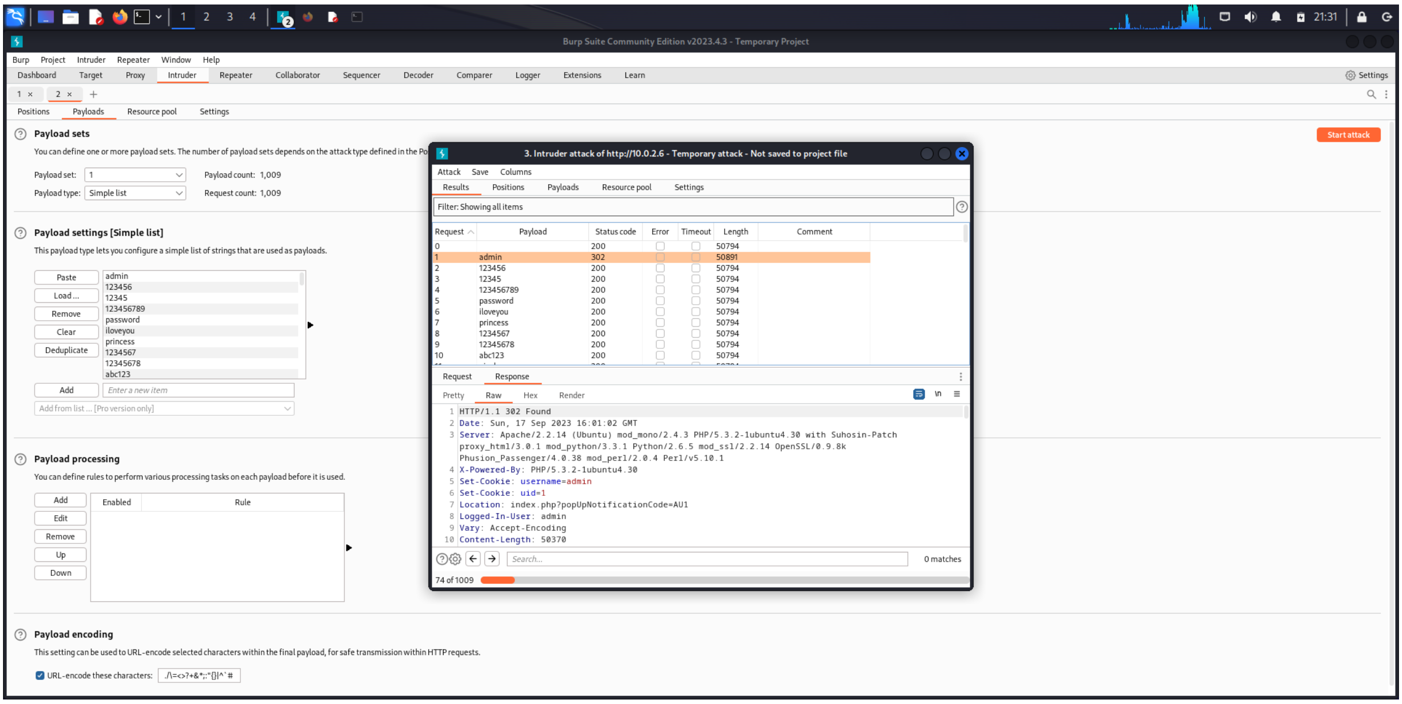
Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	50794	
1	admin	302	□	□	50891	
2	123456	200	□	□	50794	
3	12345	200	□	□	50794	
4	123456789	200	□	□	50794	
5	password	200	□	□	50794	
6	iloveyou	200	□	□	50794	
7	princess	200	□	□	50794	
8	1234567	200	□	□	50794	
9	12345678	200	□	□	50794	
10	abc123	200	□	□	50794	

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin: http://10.0.2.6
Connection: close
Referer: http://10.0.2.6/mutillidae/index.php?page=login.php
Cookie: showhints=1; PHPSESSID=4926bqp1v5k3iatik1tl13rdm2; acopendivids=
```

0 matches

51 of 1009

We can also see the HTTP Response message sent by the webpage to the request which was made.

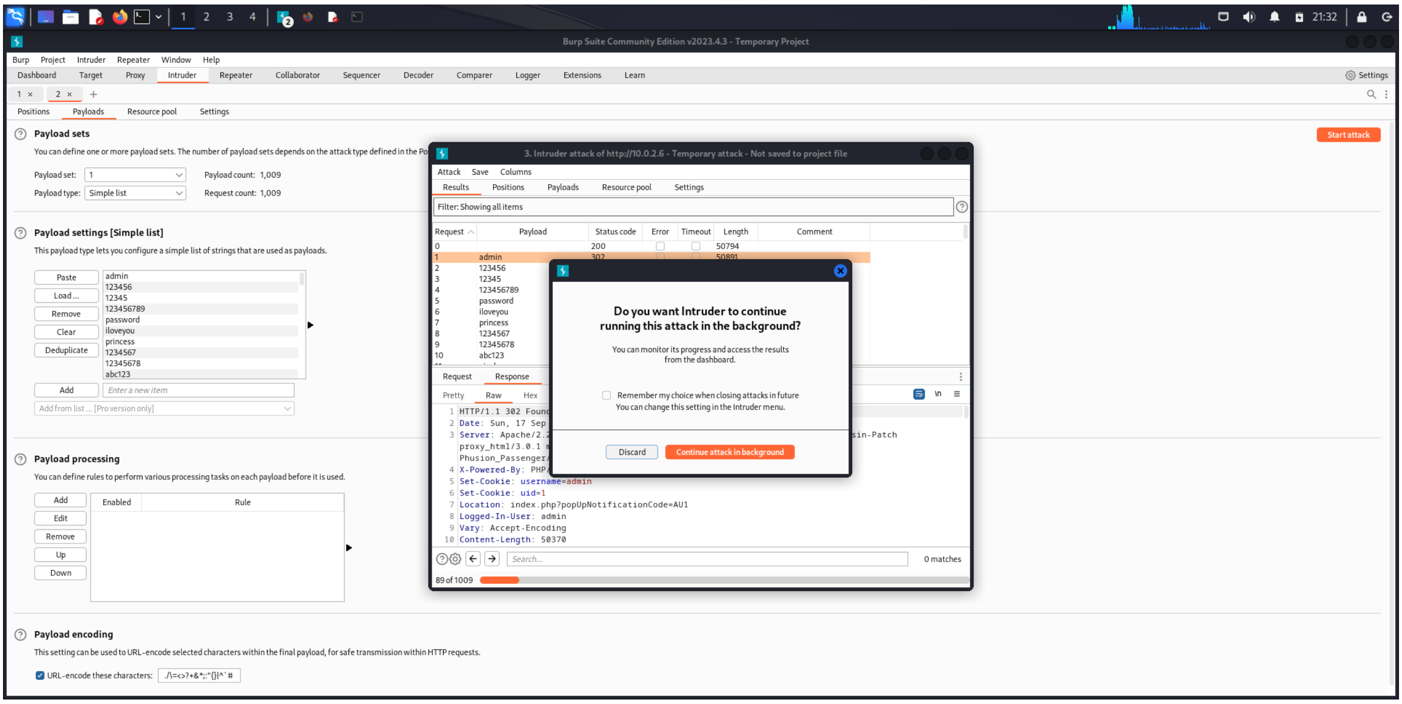


```
HTTP/1.1 302 Found
Date: Sun, 17 Sep 2023 16:01:02 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Set-Cookie: username=admin
Set-Cookie: uid=1
Location: index.php?popUpNotificationCode=AU1
Logged-In-User: admin
Vary: Accept-Encoding
Content-Length: 50370
```

0 matches

74 of 1009

We can end the attack as we have attained the username and password of the login page in just the fifth request.



Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Po

Payload set: 1   Payload count: 1,009

Payload type: Simple list   Request count: 1,009

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
Add
Enter a new item
Add from list ... [Pro version only]

admin
123456
12345
123456789
password
iloveyou
princess
1234567
12345678
abc123

Payload processing

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

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

3. Intruder attack of http://10.0.2.6 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	50794	
1	admin	302	□	□	50891	
2	123456					
3	12345					
4	123456789					
5	password					
6	iloveyou					
7	princess					
8	1234567					
9	12345678					
10	abc123					

```
HTTP/1.1 302 Found
Date: Sun, 17 Sep
Server: Apache/2.2                                   sin-Patch
proxy_html/3.0.1 m
Phusion_Passenger/
X-Powered-By: PHP/
Set-Cookie: username=admin
Set-Cookie: uid=1
Location: index.php?popUpNotificationCode=AU1
Logged-In-User: admin
Vary: Accept-Encoding
Content-Length: 50370
```

Do you want Intruder to continue running this attack in the background?

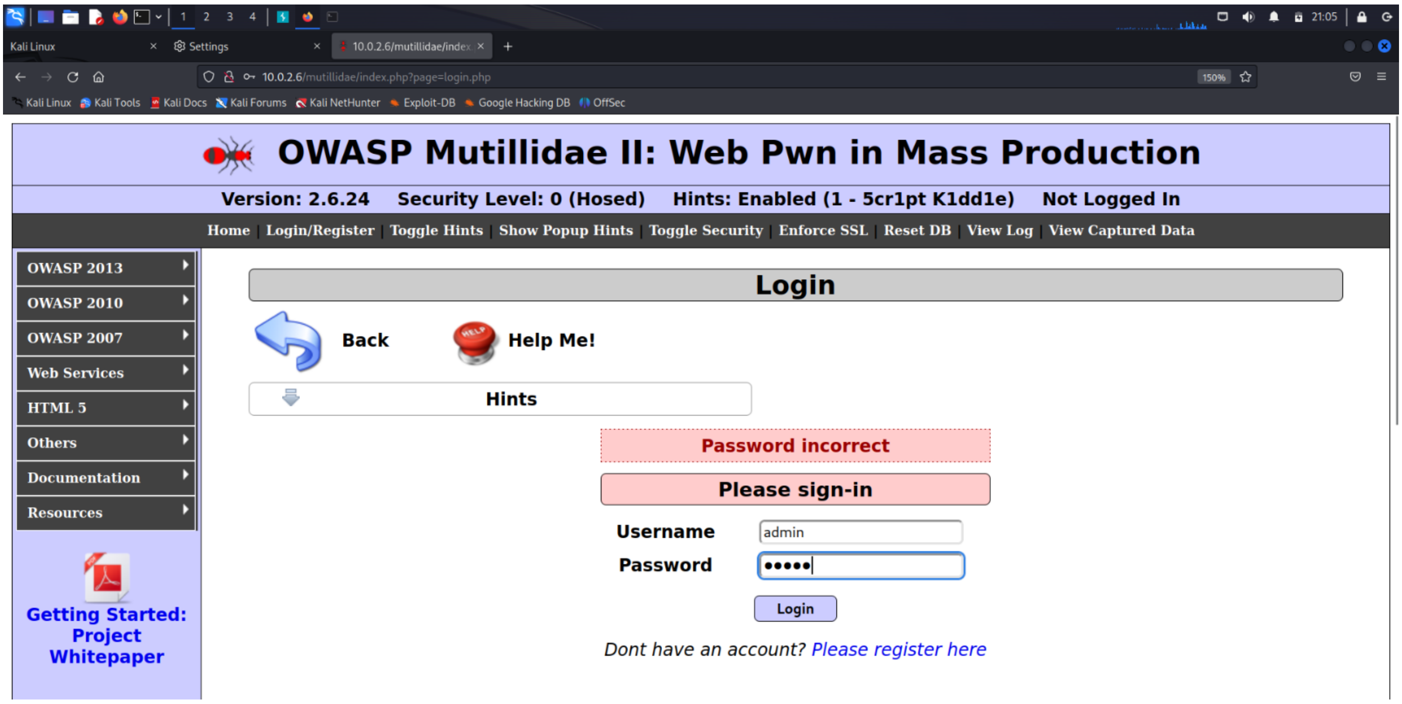
You can monitor its progress and access the results from the dashboard.

□ Remember my choice when closing attacks in future
You can change this setting in the Intruder menu.

We enter the cracked password in the login page.

Username: admin

Password: admin



Kali Linux
Settings
10.0.2.6/mutillidae/index
10.0.2.6/mutillidae/index.php?page=login.php
150%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24   Security Level: 0 (Hosed)   Hints: Enabled (1 - 5cr1pt K1dd1e)   Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Back
Help Me!
Hints

Login

Password incorrect

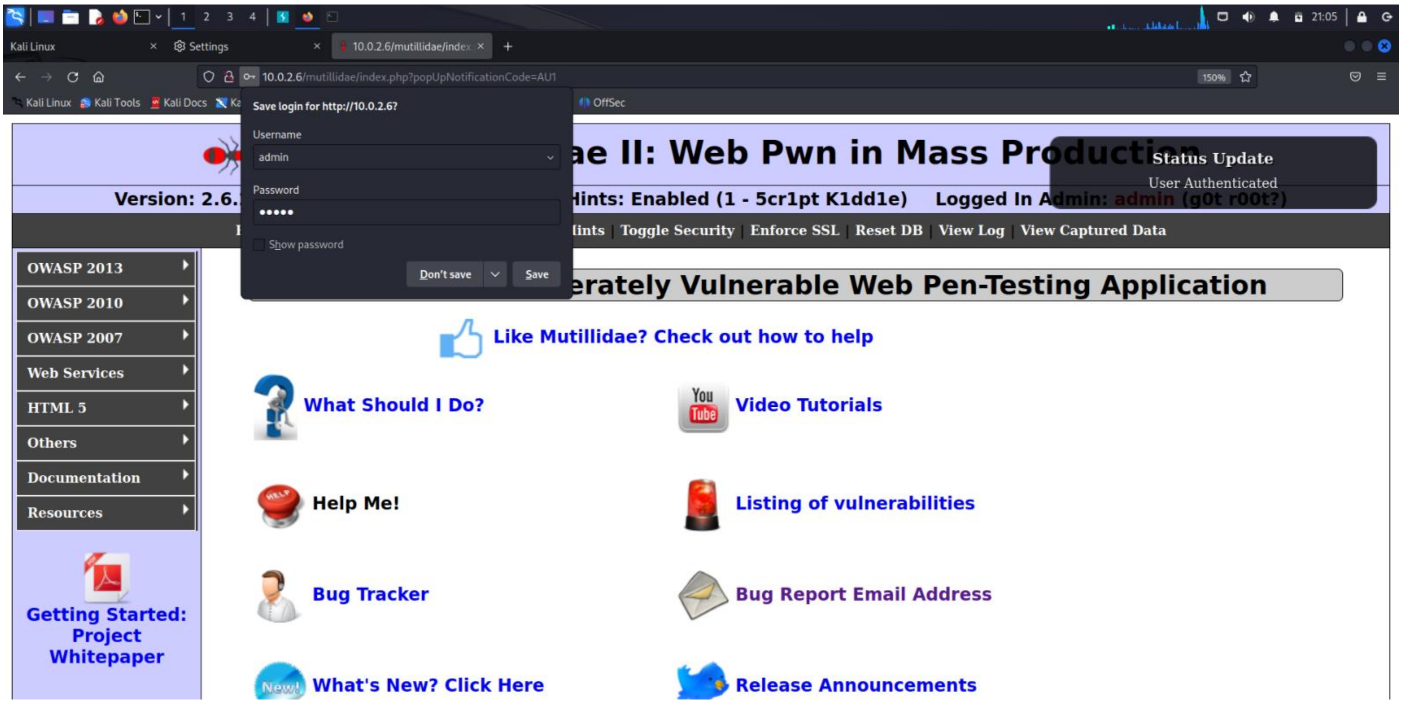
Please sign-in

Username: admin

Password: •••••

Dont have an account? Please register here

We have successfully logged in with the given username and password.



10.0.2.6/mutillidae/index.php?popUpNotificationCode=AU1

Save login for http://10.0.2.6?

Username: admin

Password: •••••

□ Show password

Version: 2.6.

Hints: Enabled (1 - 5cr1pt K1dd1e)

Logged In Admin: admin (g0t r00t?)

Status Update

User Authenticated

Kali Linux
Settings
10.0.2.6/mutillidae/index
150%
Kali Linux
Kali Tools
Kali Docs
OffSec
Don't save
Save
ae II: Web Pwn in Mass Production
lints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
erately Vulnerable Web Pen-Testing Application
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Like Mutillidae? Check out how to help
What Should I Do?
Video Tutorials
Help Me!
Listing of vulnerabilities
Bug Tracker
Bug Report Email Address
What's New? Click Here
Release Announcements

Analysis

In this report, we provide a comprehensive analysis of the fuzzing technique as a pivotal component of modern software security testing. Fuzzing, a systematic method of sending unexpected and malformed data inputs to software applications, plays a critical role in identifying vulnerabilities and defects that may otherwise go unnoticed. Our analysis highlights the effectiveness of fuzzing in uncovering security weaknesses, including buffer overflows, injection attacks, and denial-of-service vulnerabilities. We also discuss the importance of integrating fuzzing into software development and quality assurance processes to proactively enhance software security and reduce the risk of exploitation.

Conclusion

In conclusion, this report underscores the significant value of fuzzing as a vital tool in the realm of software security testing. Fuzzing has proven to be a highly effective technique for systematically identifying vulnerabilities and defects within software applications and systems. Its ability to provoke unexpected behaviour, crashes, and security issues enables early detection and mitigation of potential threats. As software security continues to be a paramount concern in our interconnected world, the integration of fuzzing into development and testing processes remains a critical step toward enhancing software resilience and reducing the risk of security breaches.