Task 1: Perform a Brute-force Attack using Burp Suite

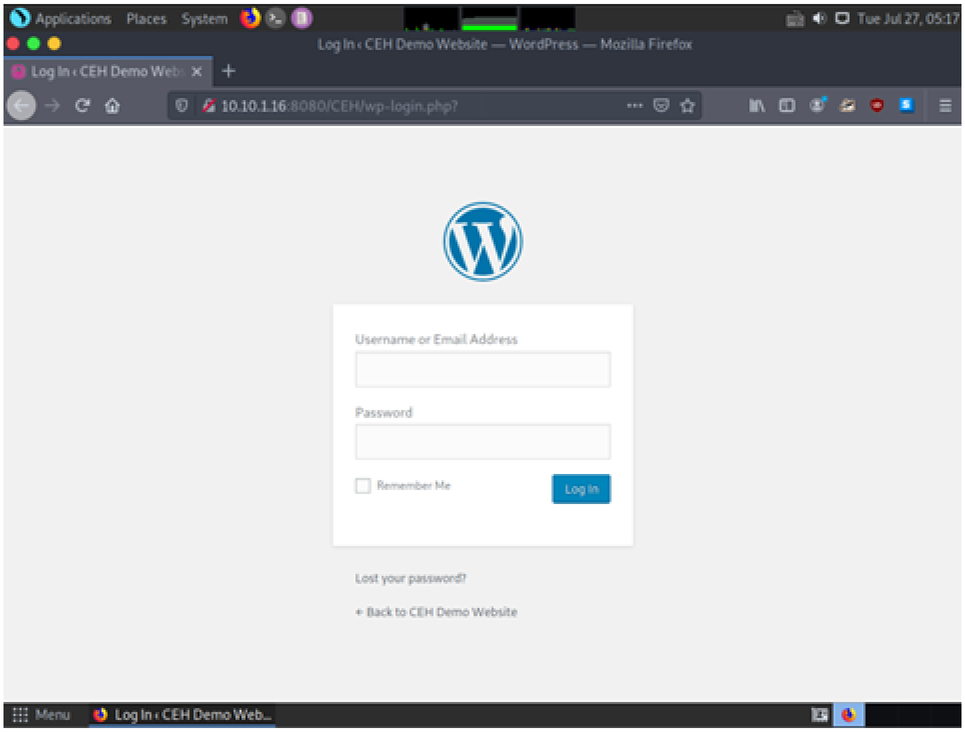
Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

Here, we will perform a brute-force attack on the target website using Burp Suite.

Note: In this task, the target WordPress website (**http://10.10.1.16:8080/CEH**) is hosted by the victim machine, **Windows Server 2016**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** machine.

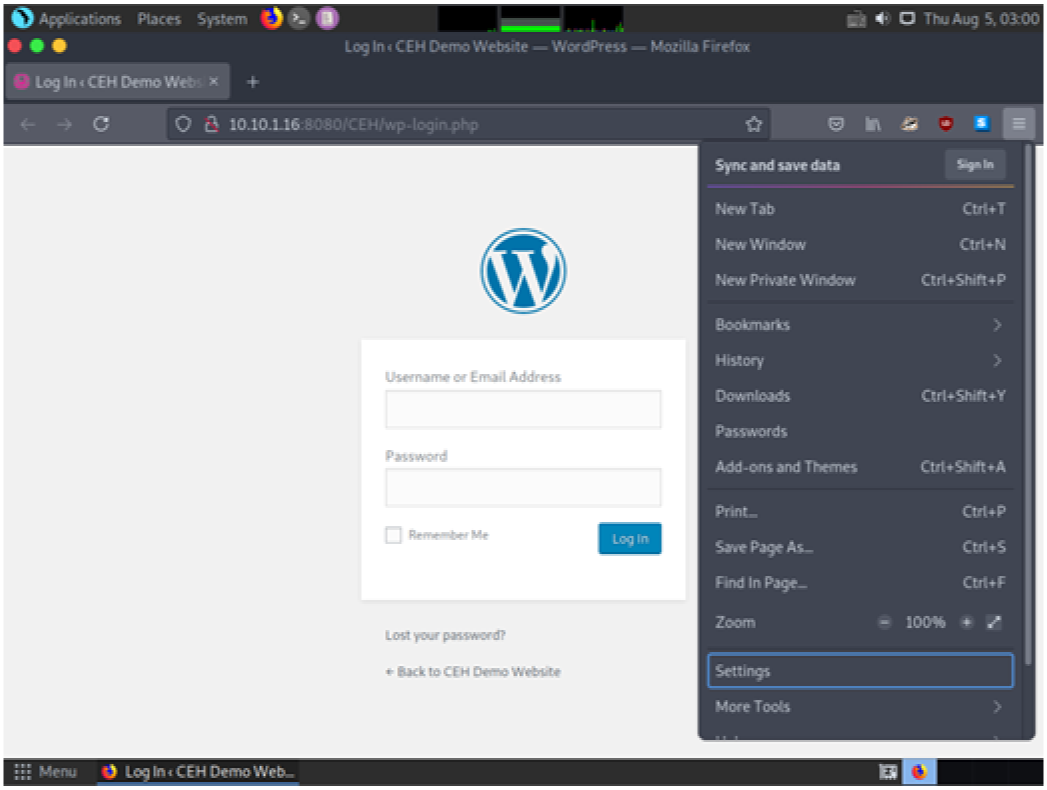
1. Click **CEHv11 Parrot Security** to switch to the Parrot Security machine.
2. Click the **Firefox** icon from the top section of Desktop to launch the Mozilla Firefox browser.
3. The Mozilla Firefox window appears; type http://10.10.1.16:8080/CEH/wp-login.php? Into the address bar and press **Enter**.

    > Note: Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2016** machine.

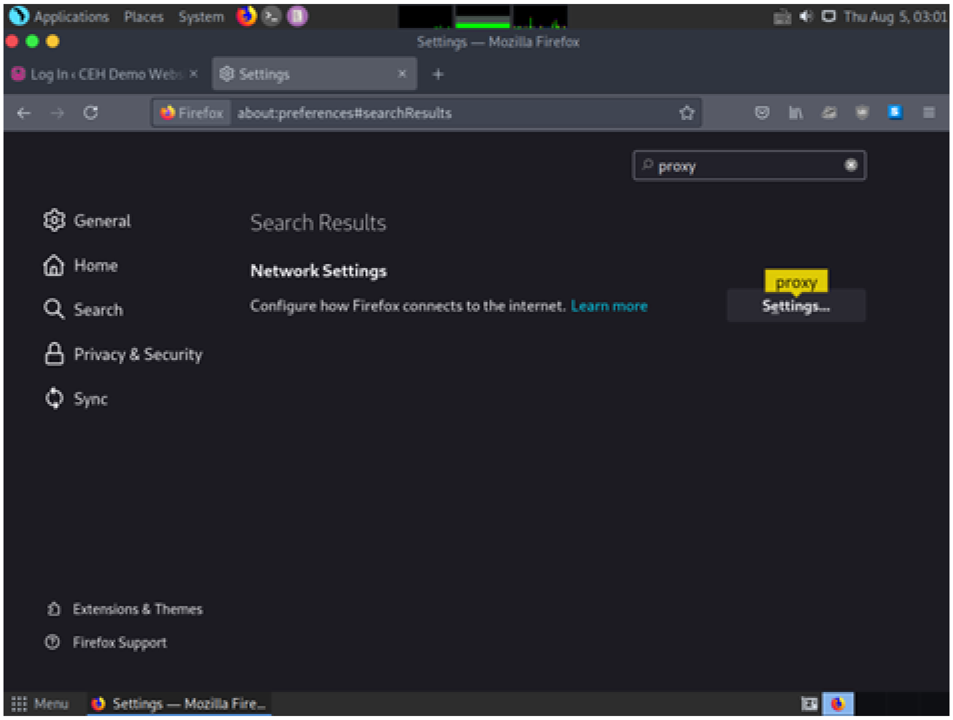

Applications Places System
Tue Jul 27, 05:17
Log In ‹ CEH Demo Website — WordPress — Mozilla Firefox
Log In ‹ CEH Demo Web
10.10.1.16:8080/CEH/wp-login.php?
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Back to CEH Demo Website
Menu
Log In ‹ CEH Demo Web...

4. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
5. In the Mozilla Firefox browser, click the **Hamburger button** in the right corner of the menu bar and click **Settings** from the list.

> Note: While performing the lab tasks if the browser got updated with its latest version then options and screenshots will differ.



6. The **General settings** tab appears. In the **Find in Settings** search bar, type **proxy**, and press **Enter**.
7. The Search Results appear. Click the **Settings** button under the **Network Settings** option.



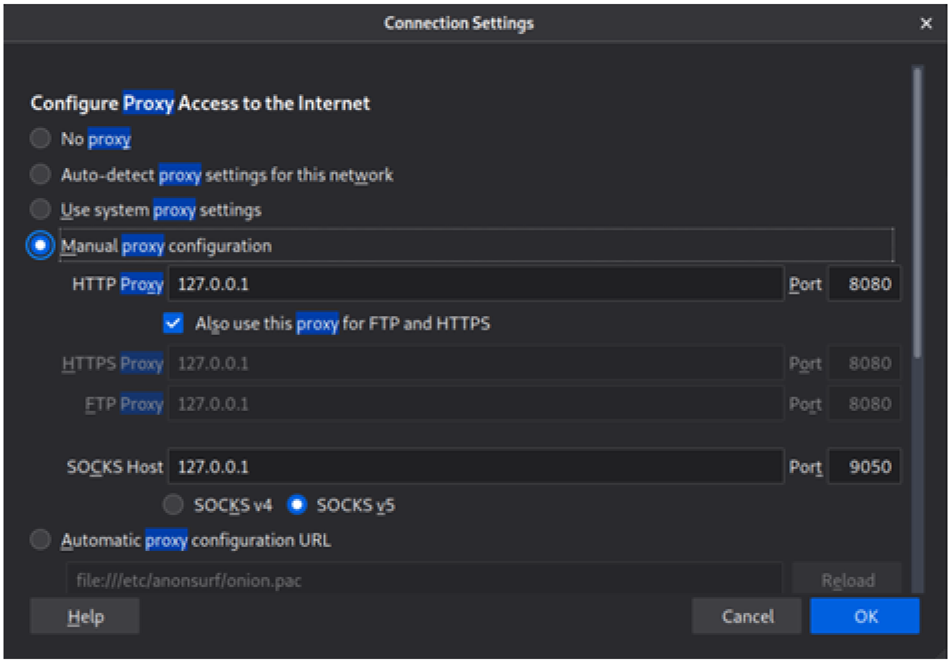
Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more

proxy
Settings...

8. The **Connection Settings** window appears; select the **Manual proxy configuration** radio button and specify the HTTP Proxy as **127.0.0.1** and the Port as **8080**. Tick the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the Preferences tab and minimize the browser window.


Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

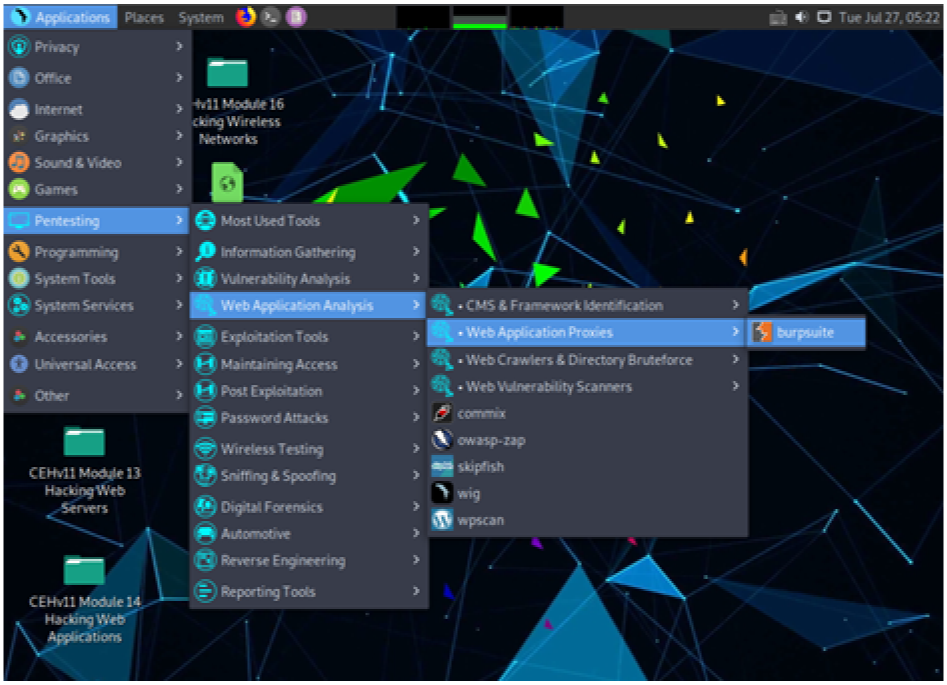
SOCKS Host 127.0.0.1 Port 9050

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

file:///etc/anonsurf/onion.pac Reload

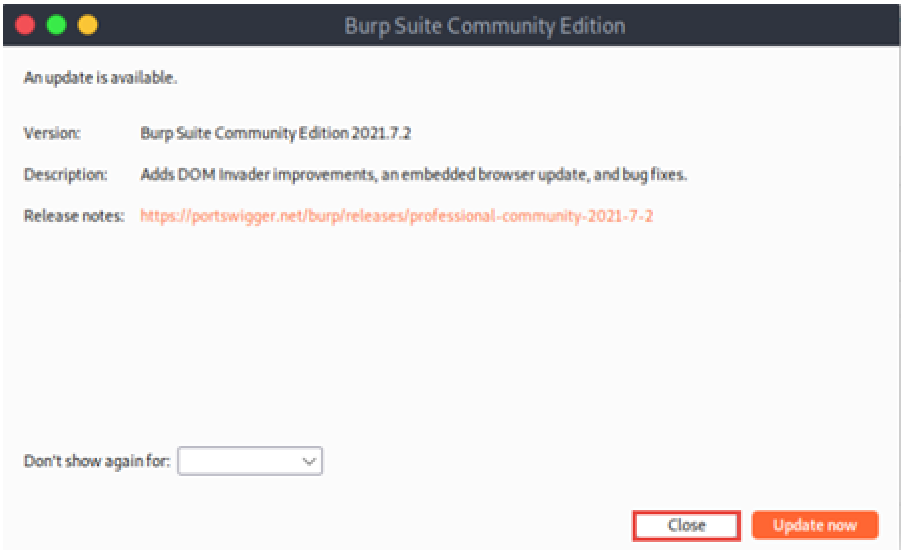
9. Now, minimize the browser window, click the **Applications** menu from the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the Burp Suite application.



10. In the next **Burp Suite Community Edition** notification, click **OK**.
11. In the Terms and Conditions wizard, click the **I Accept** button.

> Note: If Delete old temporary files? notification appears, click **Leave**.

12. A Burp Suite Community Edition wizard appears asking for an update, click **Close**.



Burp Suite Community Edition

An update is available.

Version: Burp Suite Community Edition 2021.7.2

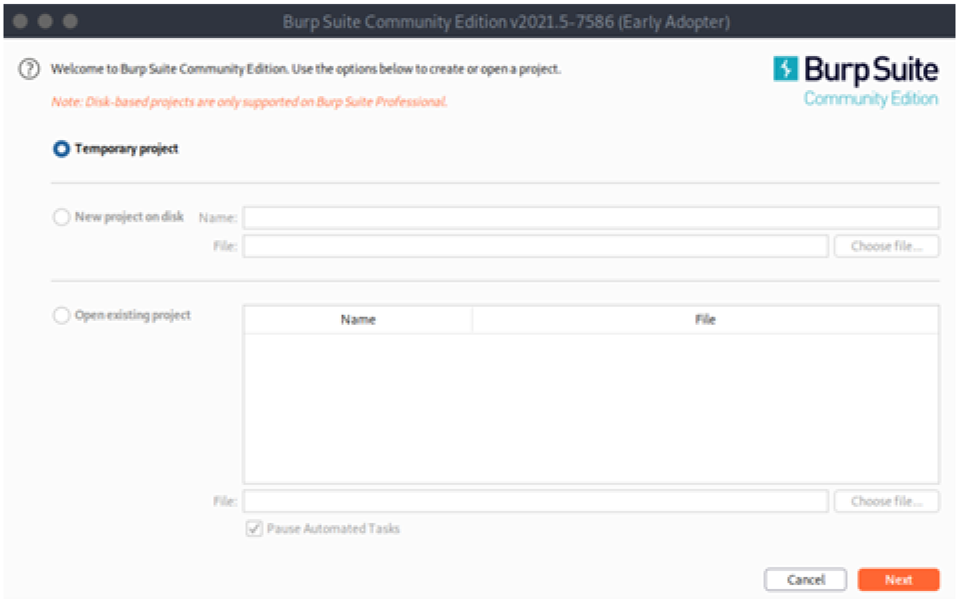
Description: Adds DOM Invader improvements, an embedded browser update, and bug fixes.

Release notes: https://portswigger.net/burp/releases/professional-community-2021-7-2

Don't show again for:

13. The Burp Suite main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

Note: If an update window appears, click **Close**.



Burp Suite Community Edition v2021.5-7586 (Early Adopter)

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

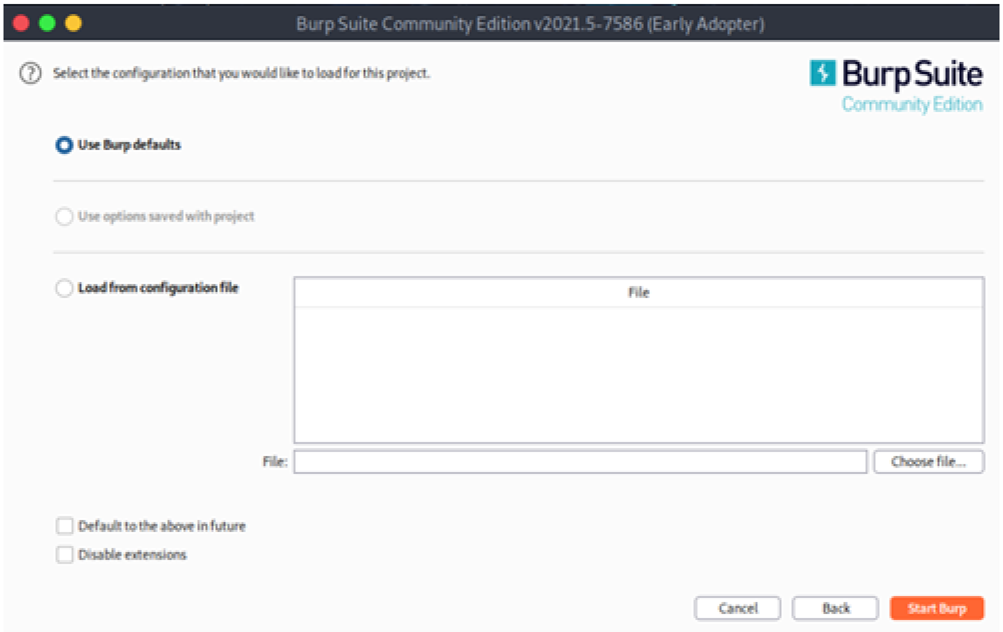
○ New project on disk Name: File:

○ Open existing project

File:

☑ Pause Automated Tasks

14. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.



Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

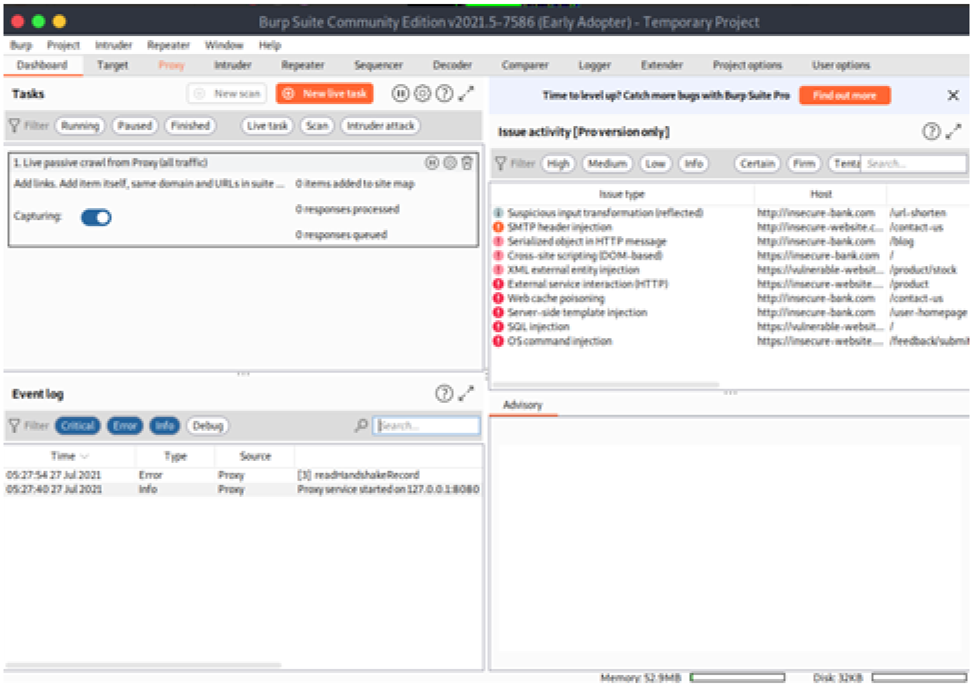
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

15. The Burp Suite main window appears; click the **Proxy** tab from the available options in the top section of the window.



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite ... 0 items added to site map

Capturing: 0 responses processed

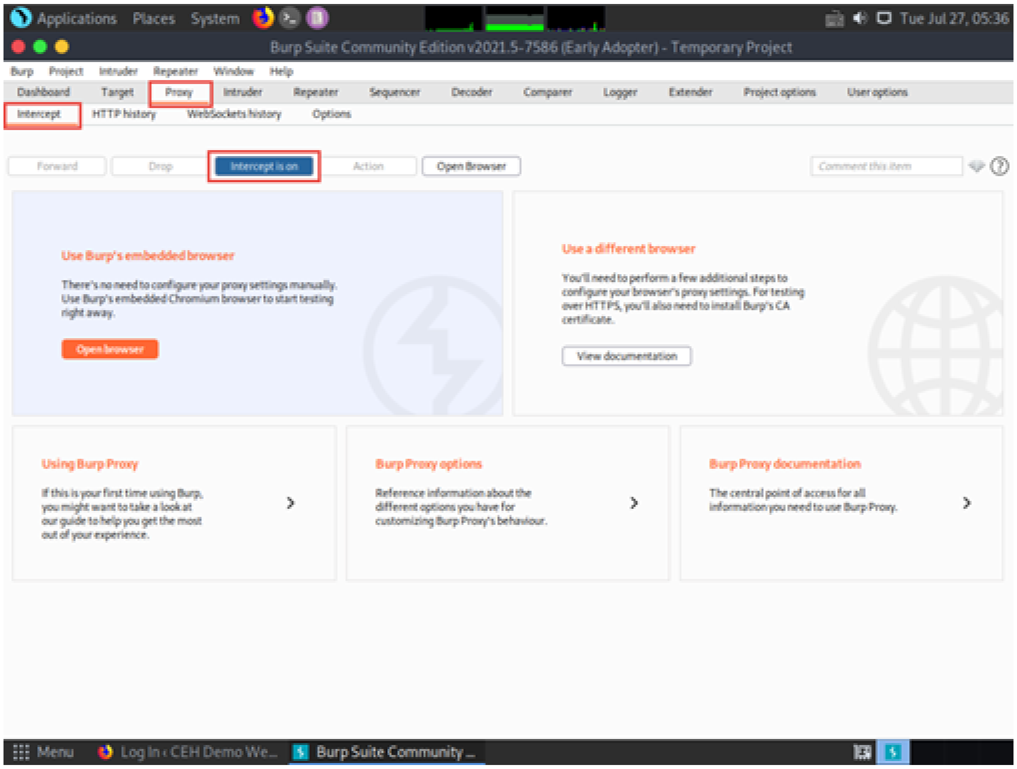
0 responses queued

Issue type	Host	
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submi

Time	Type	Source	
05:27:54 27 Jul 2021	Error	Proxy	[3] readHandshakeRecord
05:27:40 27 Jul 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

16. In the Proxy settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says Intercept is on. Leave it running.

Note: Turn the interception on if it is off.


Applications Places System
Tue Jul 27, 05:36
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Open browser
View documentation
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options

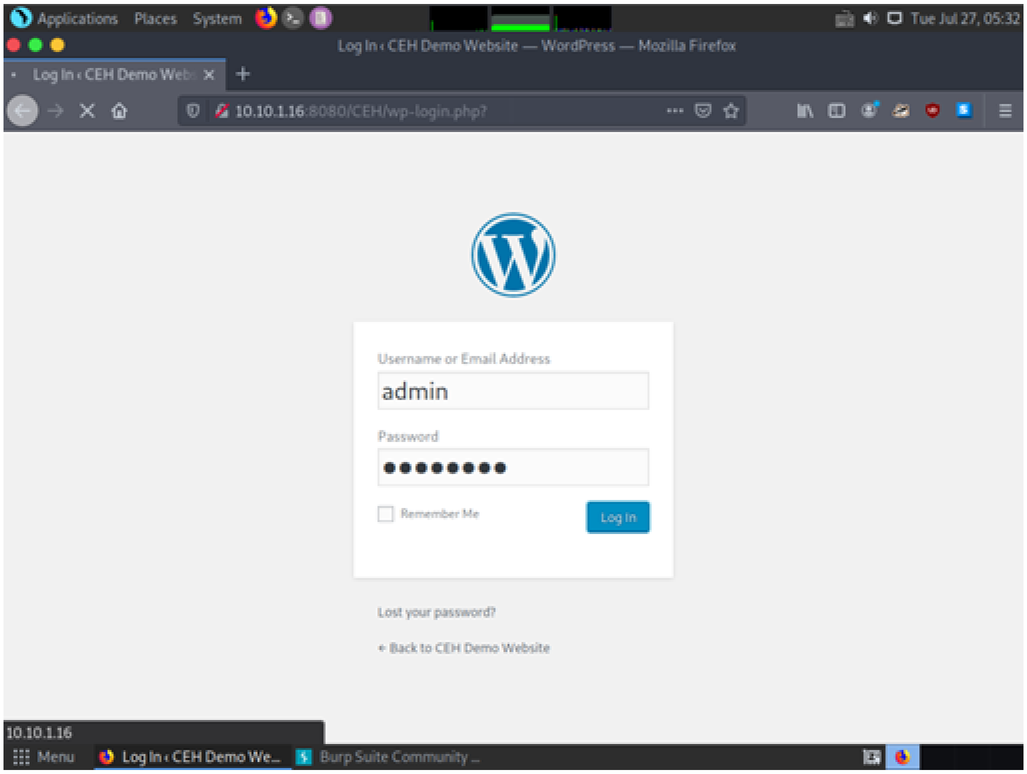
Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

17. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

Note: You can enter the credentials of your choice here.


Applications Places System
Tue Jul 27, 05:32
Log In ‹ CEH Demo Website — WordPress — Mozilla Firefox
Log In ‹ CEH Demo Web
10.10.1.16:8080/CEH/wp-login.php?
Remember Me
Log In
Lost your password?
← Back to CEH Demo Website
10.10.1.16
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

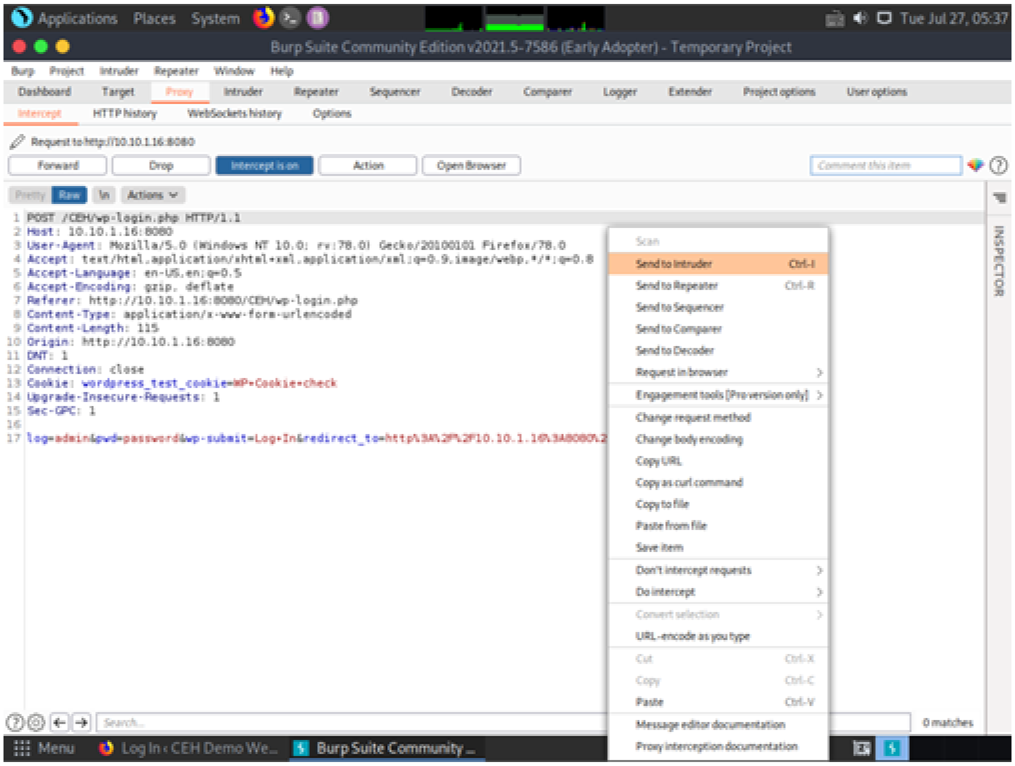
Username or Email Address
admin

Password
●●●●●●●●●

18. Switch back to the Burp Suite window; observe that the **HTTP** request was intercepted by the application.
19. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

Note: Observe that Burp Suite intercepted the entered login credentials.

Note: If you do not get the request as shown in the screenshot, then press the **Forward** button.

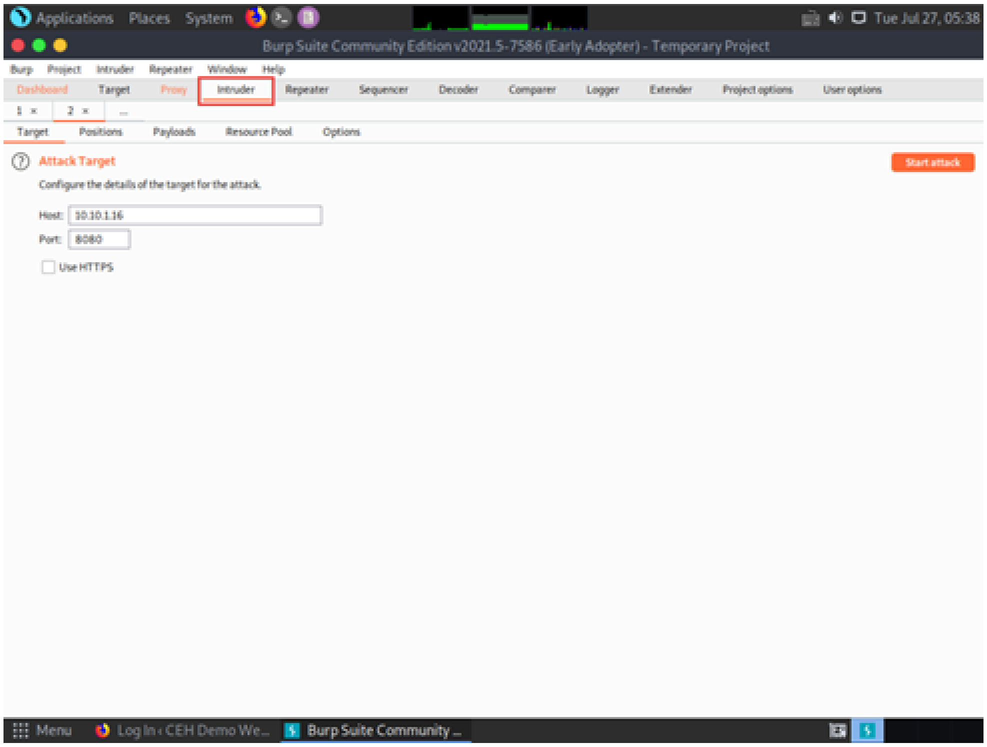


Request to http://10.10.1.16:8080

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.1.16:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.1.16:8080/CEH/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 115
Origin: http://10.10.1.16:8080
DNT: 1
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.1.16%3A8080%2
```

20. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.
21. Observe the target **host** and **port** values in the Host and Port fields.



Applications Places System
Tue Jul 27, 05:38
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

Attack Target

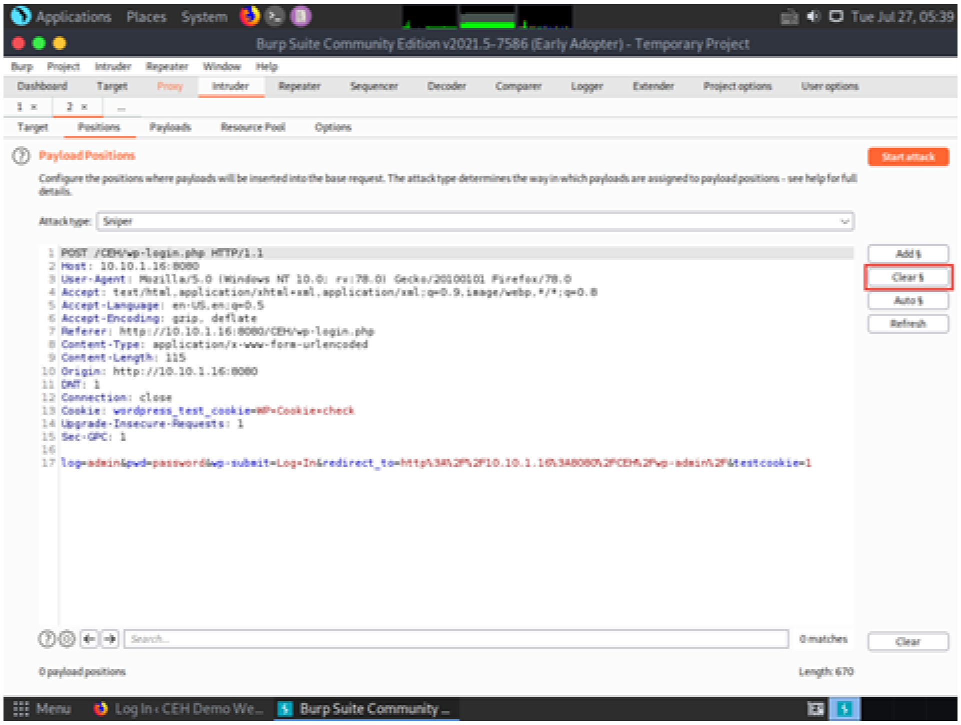
Configure the details of the target for the attack.

Host: 10.10.1.16

Port: 8080

□ Use HTTPS

22. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the **HTTP** request. Click the **Clear §** button from the right-pane to clear the default payload values.



Applications Places System
Tue Jul 27, 05:39
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Payload Positions
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
0 payload positions
Length: 670
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

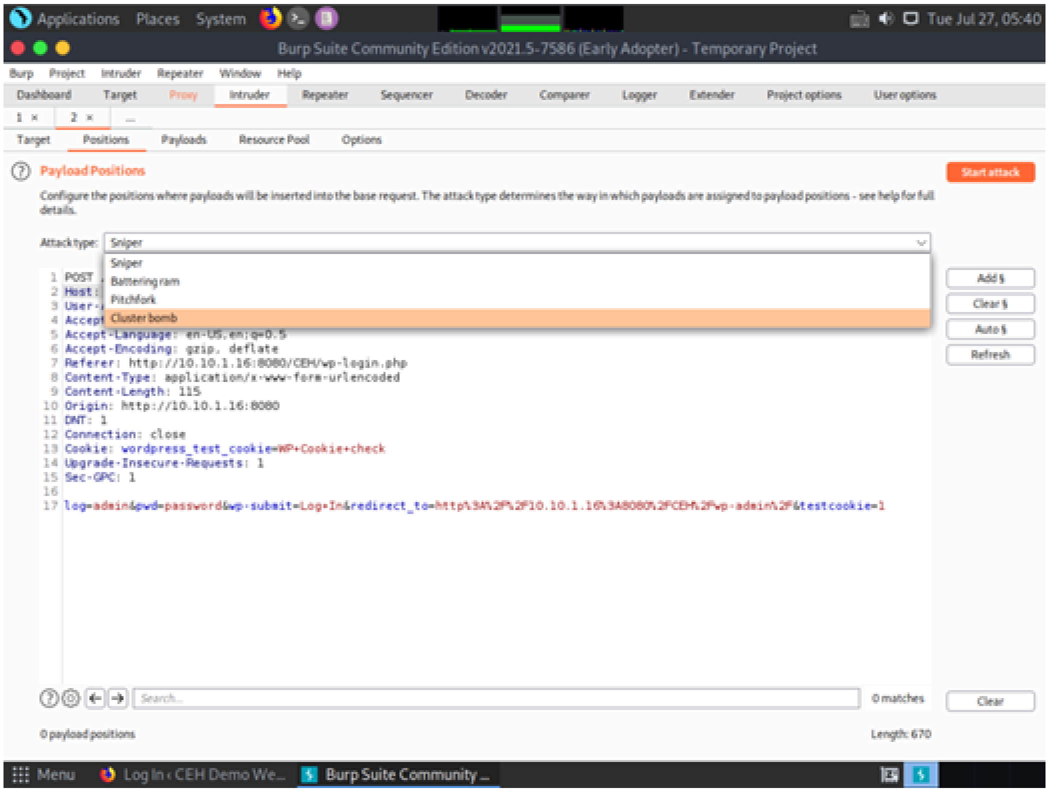
Attack type: Sniper

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.1.16:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.1.16:8080/CEH/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 115
Origin: http://10.10.1.16:8080
DNT: 1
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.1.16%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```

23. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

> Note: Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.



Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

- Sniper
- Battering ram
- Pitchfork
- Cluster bomb

```
POST
Host:
User-
Accept
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.1.16:8080/CEH/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 115
Origin: http://10.10.1.16:8080
DNT: 1
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.1.16%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```

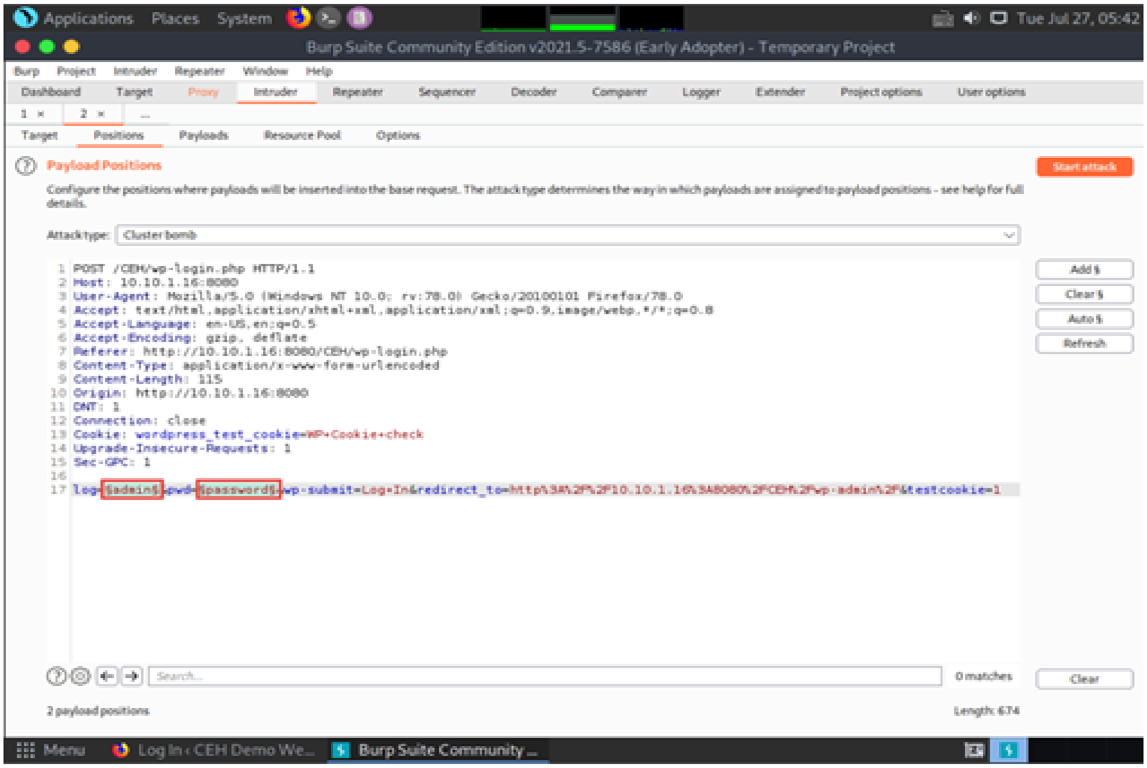
0 payload positions

Length: 670

24. Now, we will set the **username** and **password** as the payload values. To do so, select the username value entered in **Step 17** and click **Add §** from the left-pane.
25. Similarly, select the **password** value entered in **Step 17** and click **Add §** from the left-pane.

> Note: Here, the username and password are admin and password.

26. Once the username and password payloads are added. The symbol **§** will be added at the **start** and **end** of the selected payload values. Here, as the screenshot shows, the values are admin and password.



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

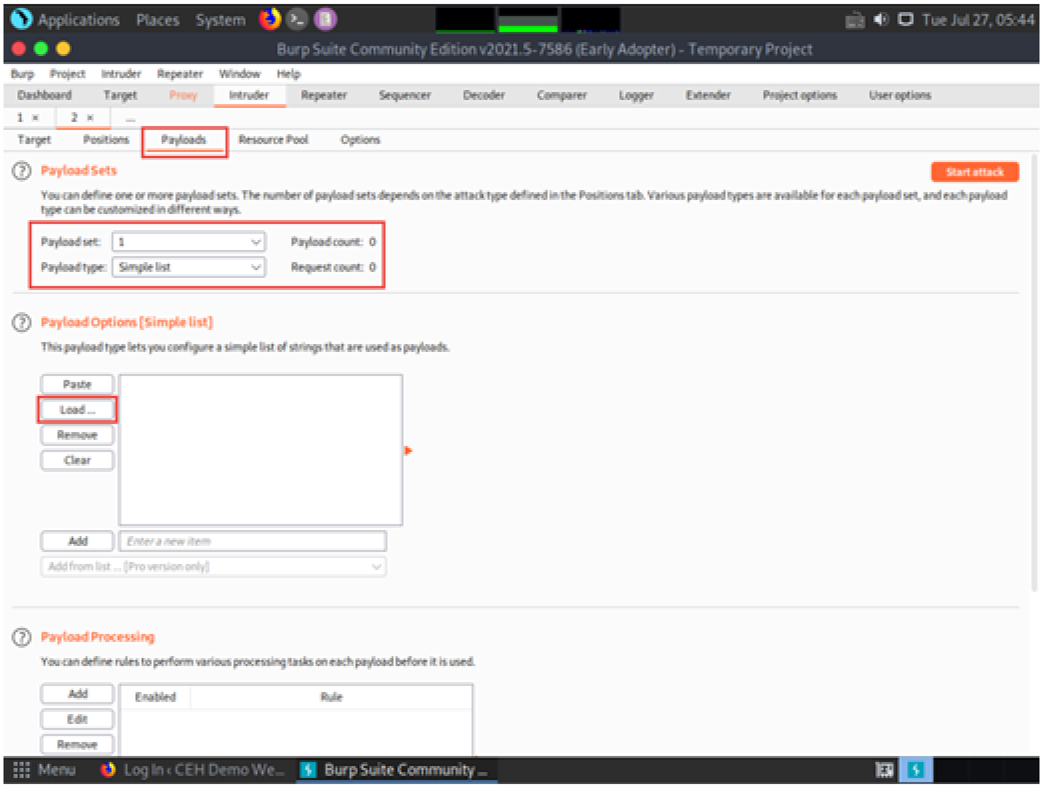
```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.1.16:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.1.16:8080/CEH/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 115
Origin: http://10.10.1.16:8080
DNT: 1
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

log=§admin§&pwd=§password§&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.1.16%3A8080%2FCEH%2Fwp-admin%2F&testcookie=1
```

2 payload positions

Length: 674

27. Navigate to the Payloads tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the Payload set is selected as **1**, and the Payload type is selected as **Simple list**.
28. Under the Payload Options [Simple list] section, click the **Load…** button.


Applications Places System
Tue Jul 27, 05:44
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled
Rule
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

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: 1 Payload count: 0

Payload type: Simple list Request count: 0

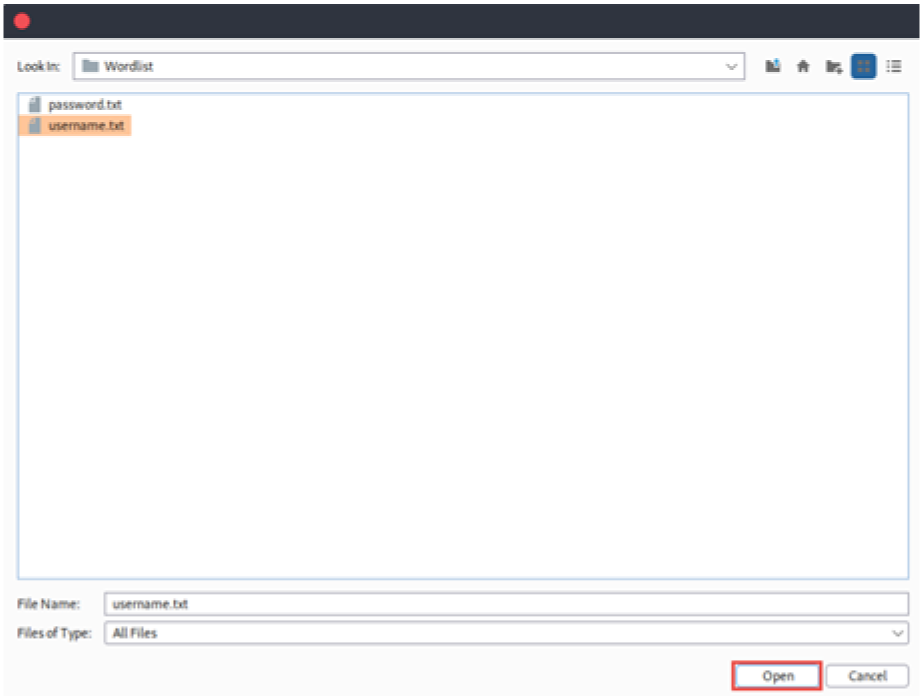
Payload Options [Simple list]

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

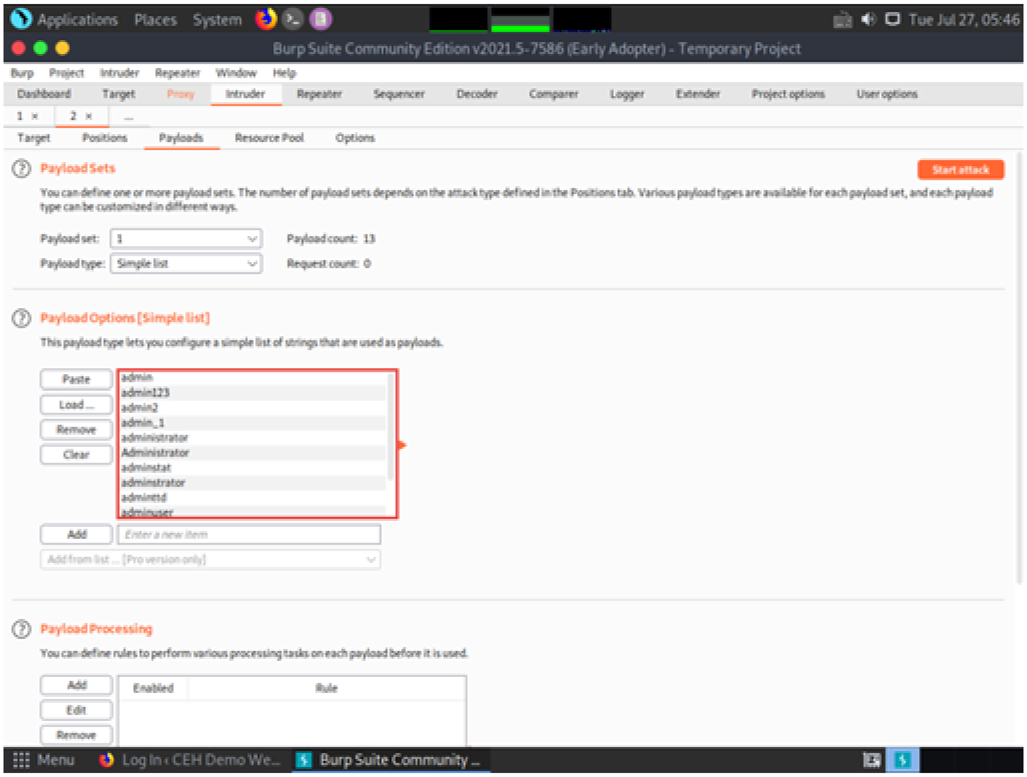
Payload Processing

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

29. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv11 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button.



30. Observe that the selected **username.txt** file content appears under the Payload Options [Simple list] section, as shown in the screenshot.



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: 1
Payload count: 13
Payload type: Simple list
Request count: 0

Payload Options [Simple list]

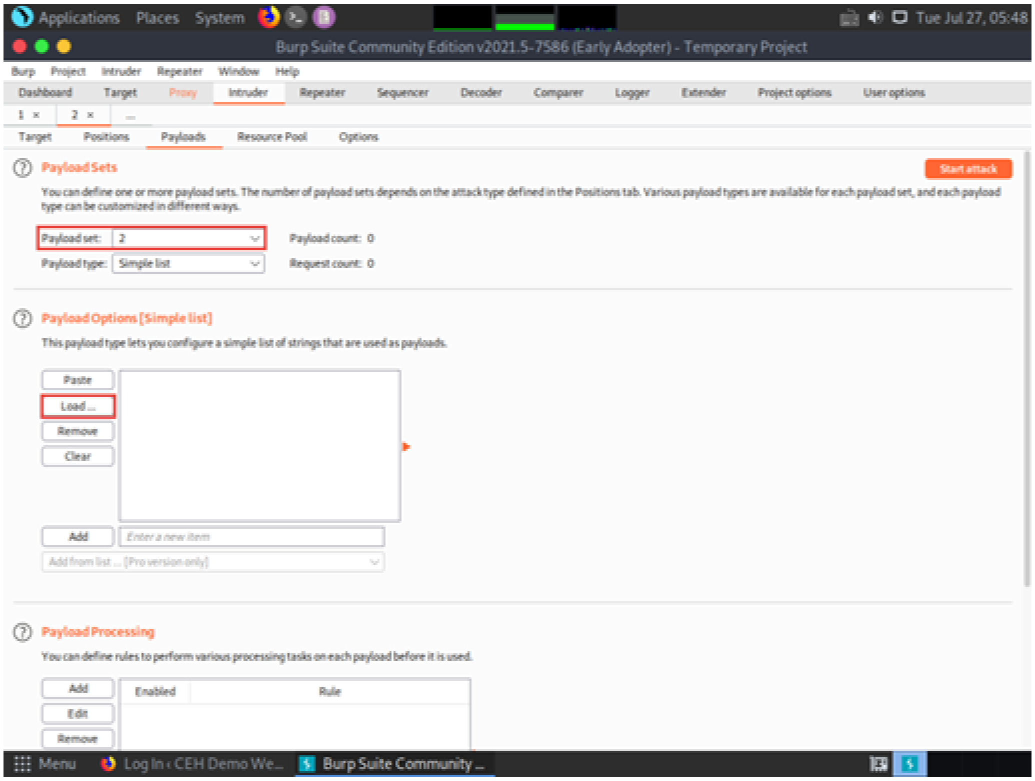
This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
admin123
admin2
admin_1
administrator
Administrator
adminstat
adminstrator
admintd
adminuser
```

Payload Processing

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

31. Similarly, load a password file for the payload **set 2**. To do so, under the Payload Sets section, select the Payload set as 2 from the drop-down options and ensure that the Payload type is selected as **Simple list**.
32. Under the Payload Options [Simple list] section, click the **Load…** button.


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - 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 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: 0
Payload type: Simple list Request count: 0

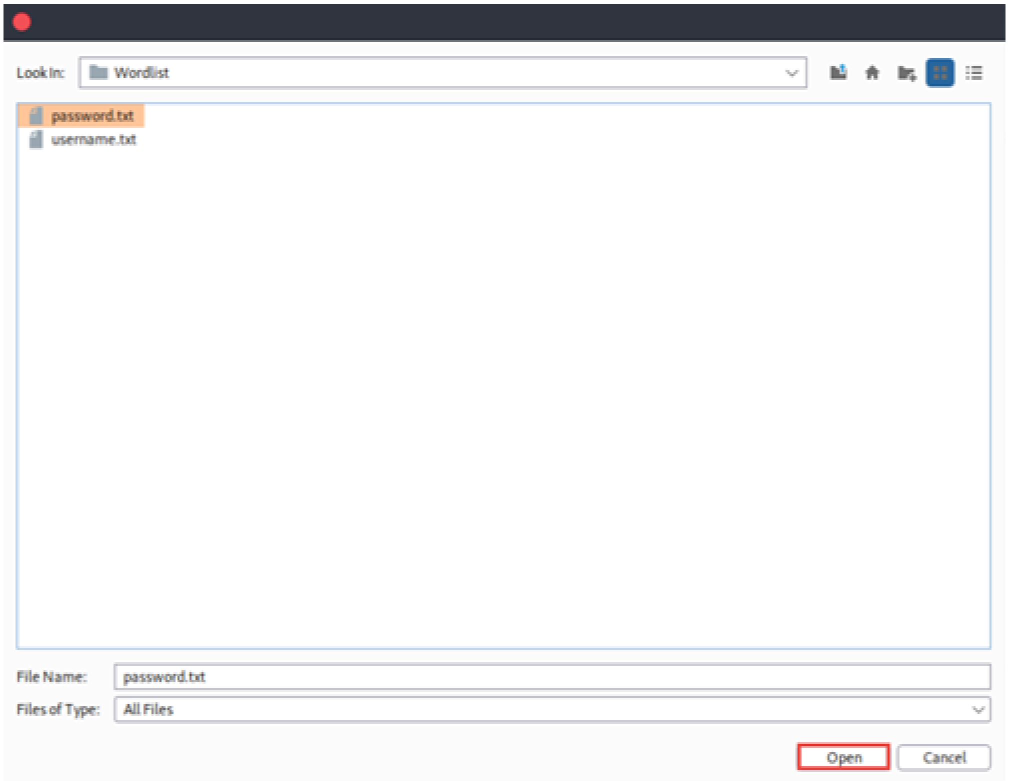
Payload Options [Simple list]

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.

33. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv11 Module 14 Hacking Web Applications/Wordlist**, select the **password.txt** file, and click the **Open** button.



Look In: Wordlist

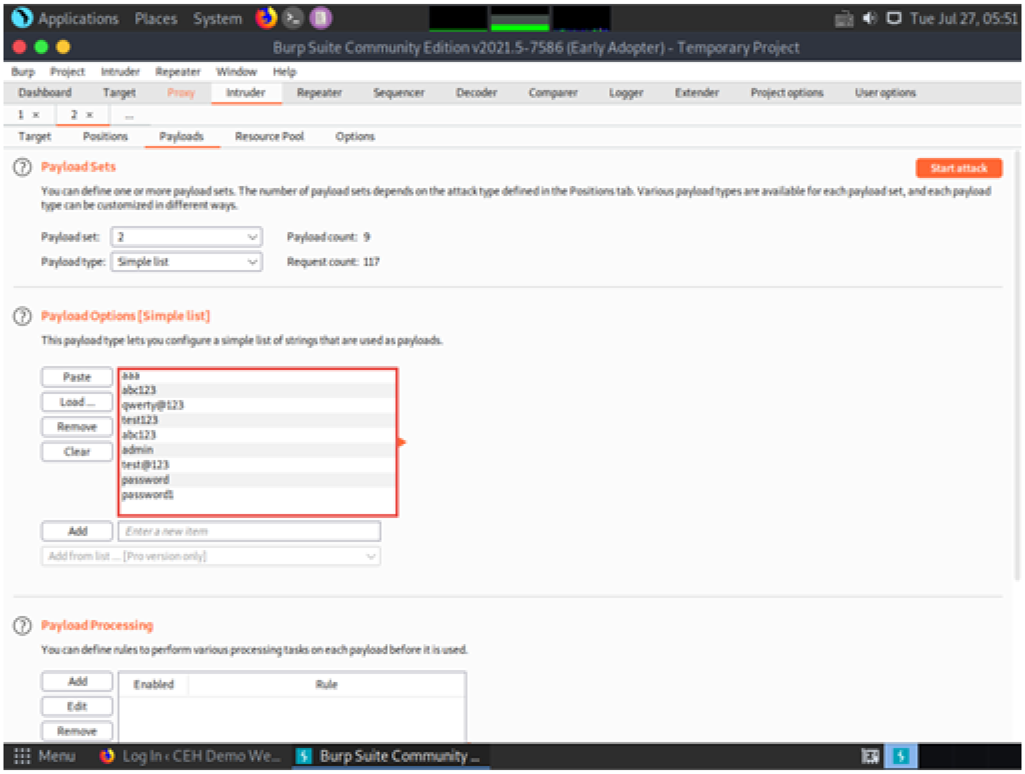
password.txt

username.txt

File Name: password.txt

Files of Type: All Files

34. Observe that selected **password.txt** file content appears under the Payload Options [Simple list] section, as shown in the screenshot.



Applications Places System
Tue Jul 27, 05:51
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled
Rule
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

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: 9

Payload type: Simple list Request count: 117

Payload Options [Simple list]

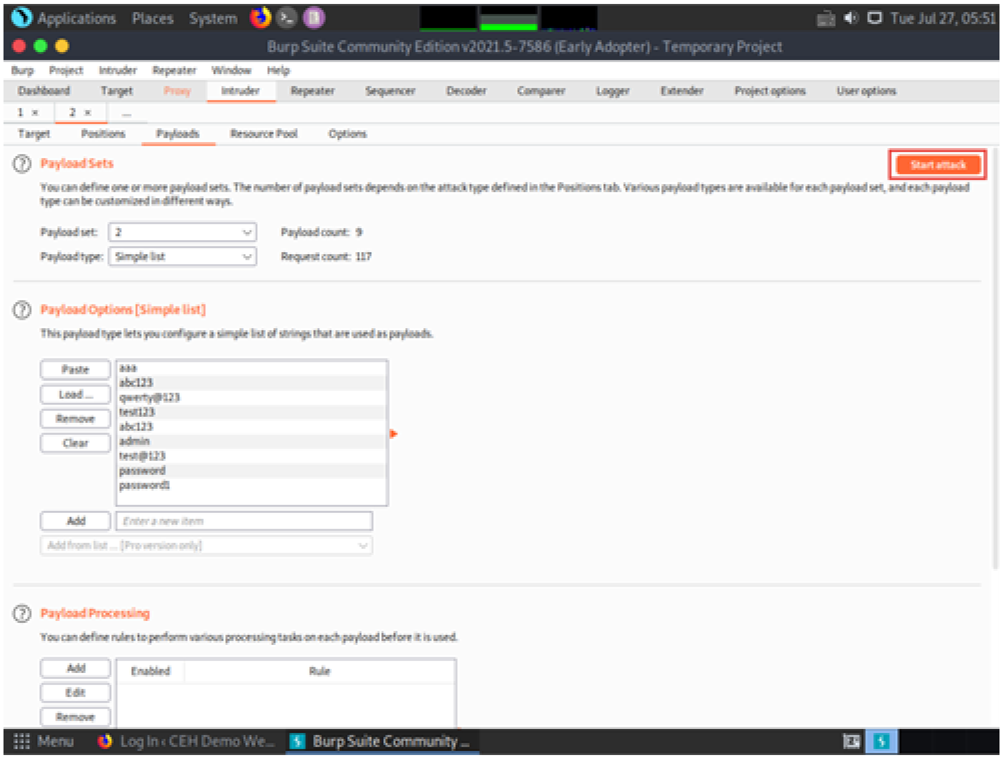
This payload type lets you configure a simple list of strings that are used as payloads.

```
aaa
abc123
qwerty@123
test123
abc123
admin
test@123
password
password1
```

Payload Processing

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

35. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.



Applications Places System
Tue Jul 27, 05:51
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Target Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Enabled
Rule
Menu
Log In ‹ CEH Demo We...
Burp Suite Community ...

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: 9

Payload type: Simple list Request count: 117

Payload Options [Simple list]

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

```
aaa
abc123
qwerty@123
test123
abc123
admin
test@123
password
password1
```

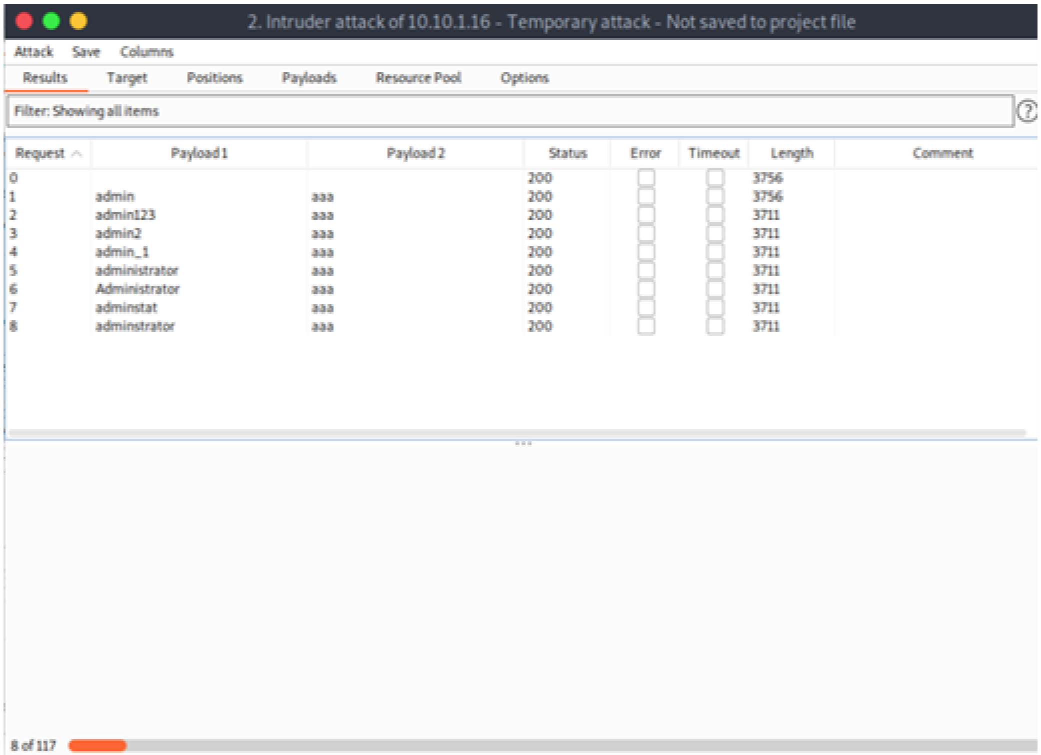
Payload Processing

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

36. A Burp Intruder notification appears. Click **OK** to proceed.

37. The Intruder attack window appears as the **brute-attack** initializes. It displays various username-password combinations along with the Length of the response and the Status.

38. Wait for the progress bar at the bottom of the window to complete.



2. Intruder attack of 10.10.1.16 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Target
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
8 of 117

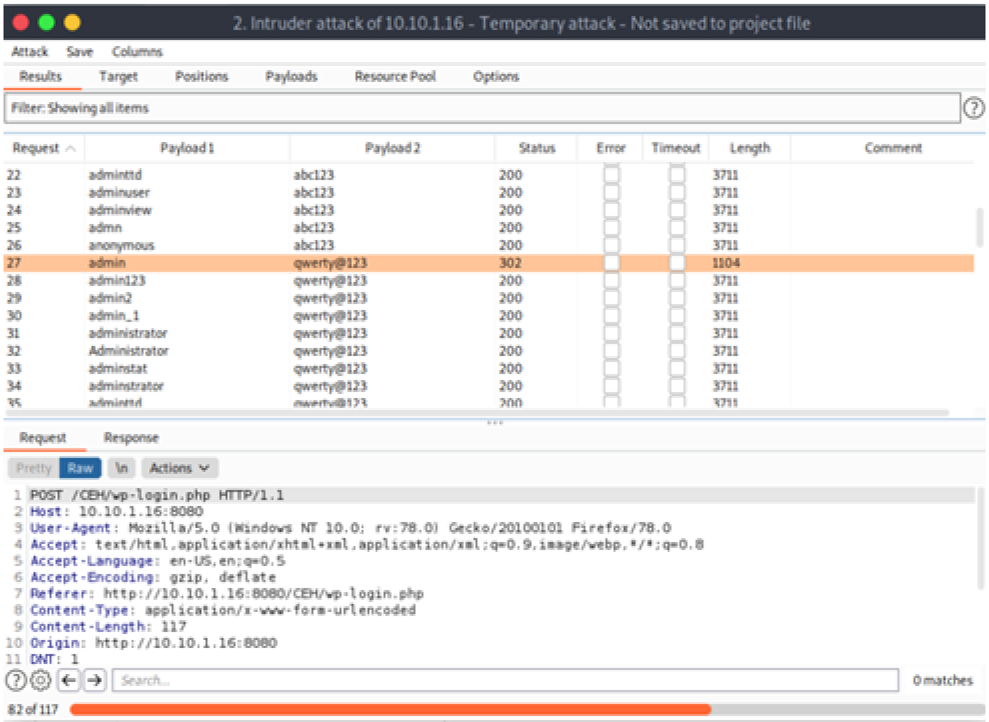
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	3756	
1	admin	aaa	200	□	□	3756	
2	admin123	aaa	200	□	□	3711	
3	admin2	aaa	200	□	□	3711	
4	admin_1	aaa	200	□	□	3711	
5	administrator	aaa	200	□	□	3711	
6	Administrator	aaa	200	□	□	3711	
7	adminstat	aaa	200	□	□	3711	
8	adminstrator	aaa	200	□	□	3711	

39. After the progress bar completes, scroll down and observe the different values of Status and Length. Here, **Status=302** and **Length= 1104**.

Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.

Note: The values might differ in your lab environment.

40. In the **Raw** tab under the **Request** tab, the **HTTP** request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.



2. Intruder attack of 10.10.1.16 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Target
Positions
Payloads
Resource Pool
Options
Filter: Showing all items

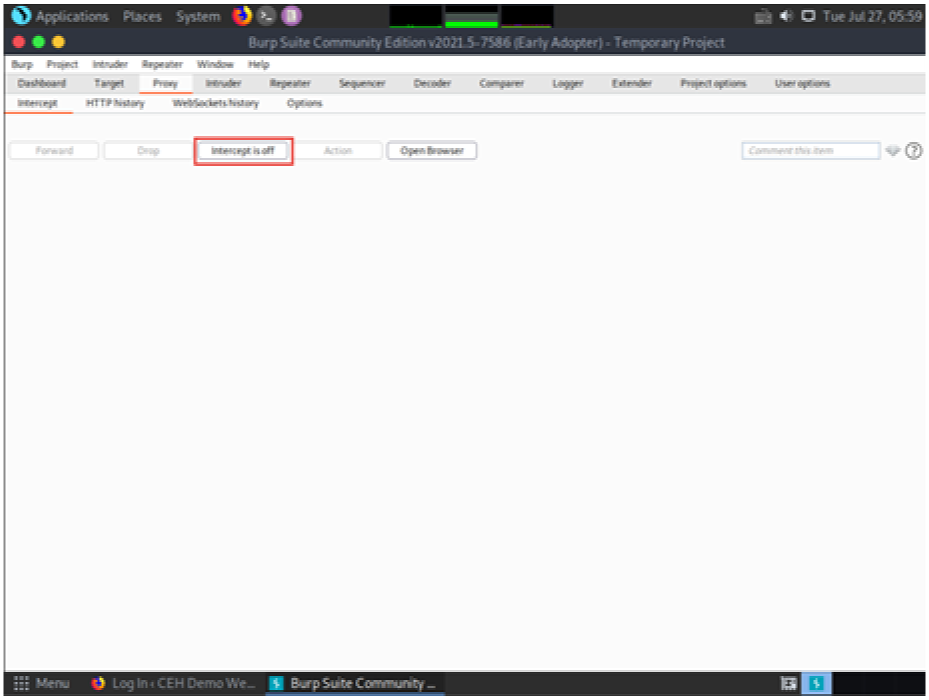
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
22	adminttd	abc123	200	□	□	3711	
23	adminuser	abc123	200	□	□	3711	
24	adminview	abc123	200	□	□	3711	
25	admn	abc123	200	□	□	3711	
26	anonymous	abc123	200	□	□	3711	
27	admin	qwerty@123	302	□	□	1104	
28	admin123	qwerty@123	200	□	□	3711	
29	admin2	qwerty@123	200	□	□	3711	
30	admin_1	qwerty@123	200	□	□	3711	
31	administrator	qwerty@123	200	□	□	3711	
32	Administrator	qwerty@123	200	□	□	3711	
33	adminstat	qwerty@123	200	□	□	3711	
34	adminstrator	qwerty@123	200	□	□	3711	
35	adminttd	qwerty@123	200	□	□	3711	

```
POST /CEH/wp-login.php HTTP/1.1
Host: 10.10.1.16:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.1.16:8080/CEH/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: http://10.10.1.16:8080
DNT: 1
```

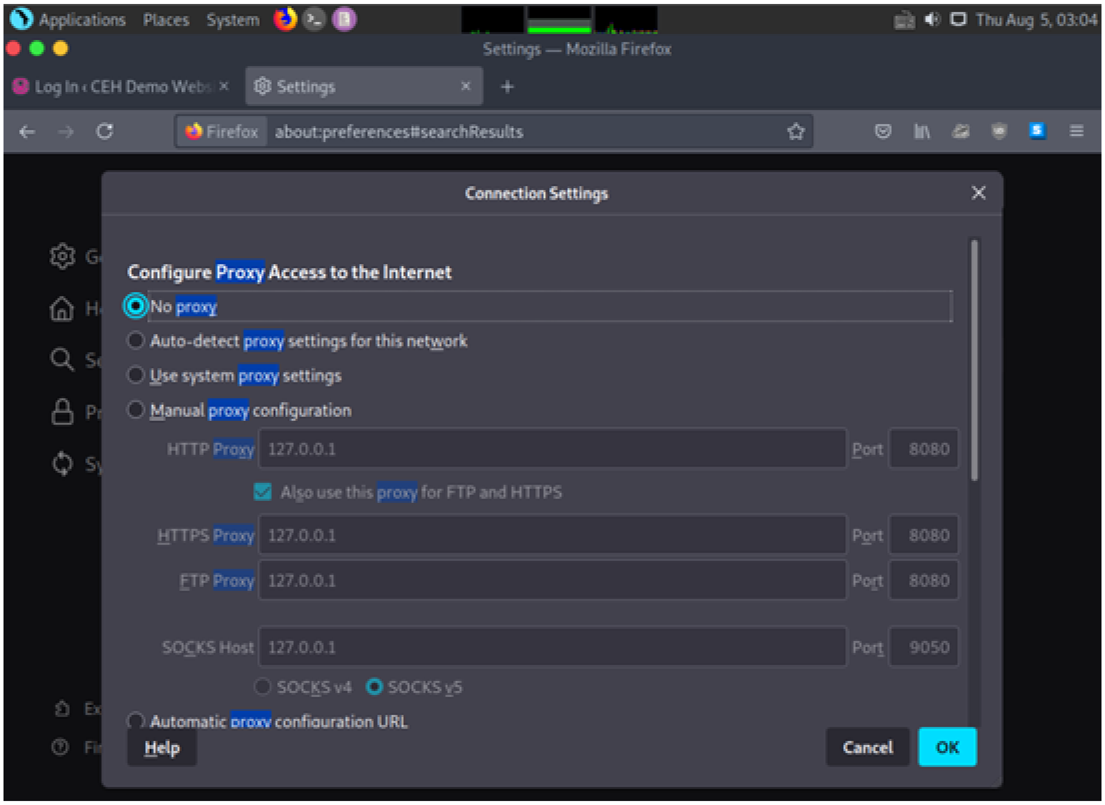
41. Now, that you have obtained the correct user credentials, close the **Intruder** attack window.

    Note: If a Warning pop-up appears, click **Discard**.

42. Navigate back to the **Proxy** tab and click the **Intercept** is on button to turn off the interception. The Intercept is on button **toggles** to Intercept is **off**, indicating that the interception is off.


Applications Places System
Tue Jul 27, 05:59
Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Open Browser
Comment this item
Menu Log In ‹ CEH Demo We... Burp Suite Community ...

43. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the No proxy radio-button in the Connection Settings window and click **OK**. Close the tab.


Applications Places System
Thu Aug 5, 03:04
Settings — Mozilla Firefox
Log In ‹ CEH Demo Webs
Settings
Firefox about:preferences#searchResults
Connection Settings
Help
Cancel
OK

Configure Proxy Access to the Internet

● No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

○ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 9050

○ SOCKS v4 ● SOCKS v5

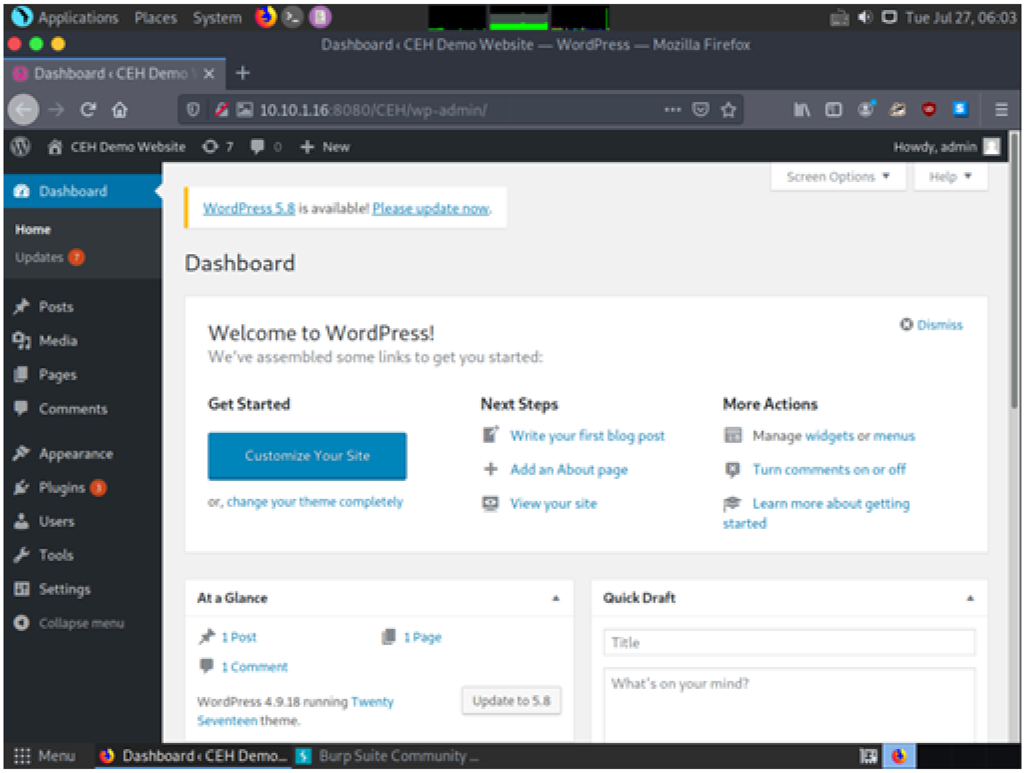
○ Automatic proxy configuration URL

44. Reload the target website http://10.10.1.16:8080/CEH/wp-login.php? enter the **Username** and **Password** obtained in **Step 40** and click **Log In**.

Note: Here, the username and password are admin and qwerty@123.

Note: If a pop-up appears, click **Resend**.

45. You are **successfully** logged in using the brute-forced credentials. The Welcome to WordPress! Page appears, as shown in the screenshot.



46. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.
47. Close all open windows and document all the acquired information.

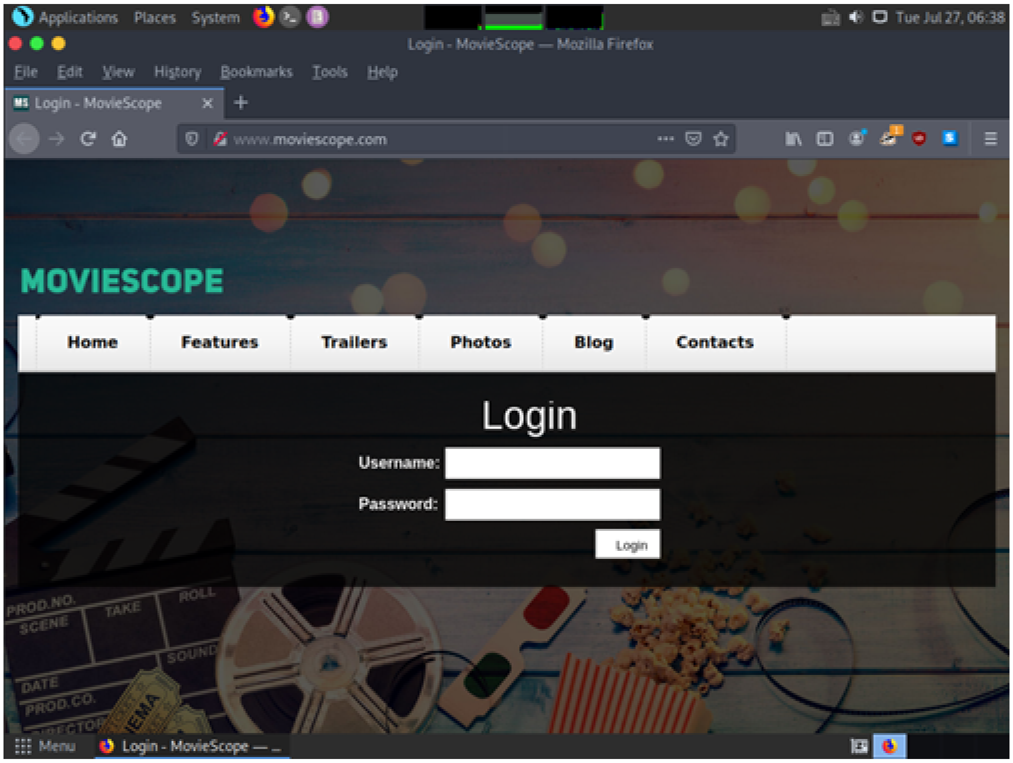
Task 2: Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

Here, we will use the Burp Suite tool to perform parameter tampering.

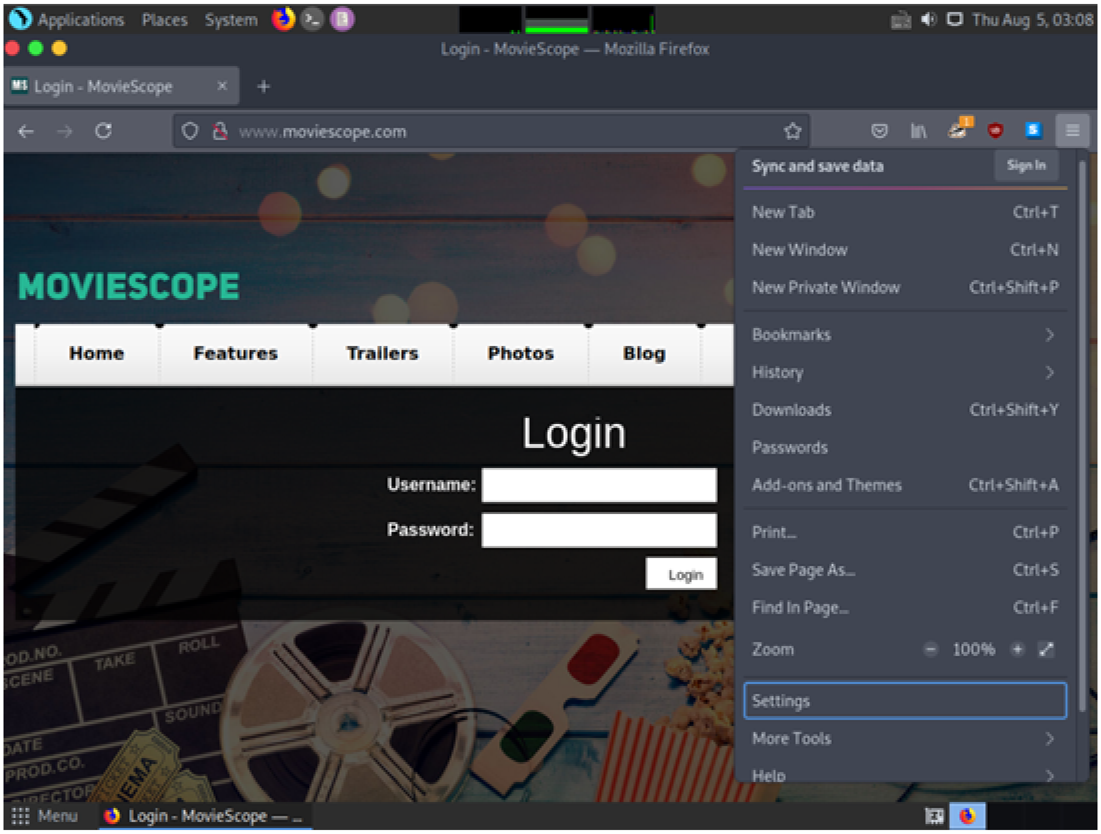
Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Here, the host machine is the **Parrot Security** machine.

1. In Parrot Security machine click the **Firefox** icon from the top section of **Desktop** to launch the Mozilla Firefox browser.
2. The Mozilla Firefox window appears; type http://www.moviescope.com into the address bar and press **Enter**.

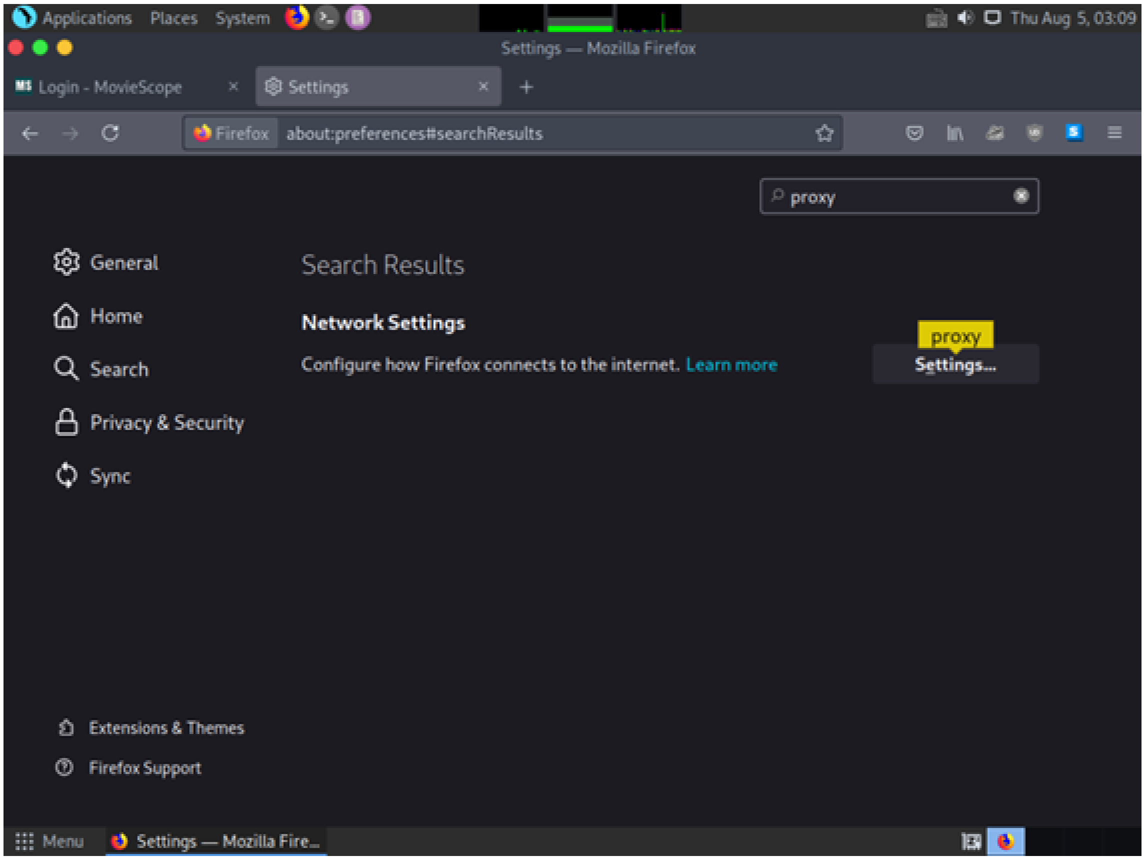


3. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
4. In the Mozilla Firefox browser, click the **Hamburger button** in the right corner of the menu bar and click **Settings** from the list.

   Note: While performing the lab tasks if the browser got updated with its latest version then options and screenshots will differ.



5. The **General** settings tab appears. In the **Find in Settings** search bar, type **proxy**, and press **Enter**.
6. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



about:preferences#searchResults

proxy

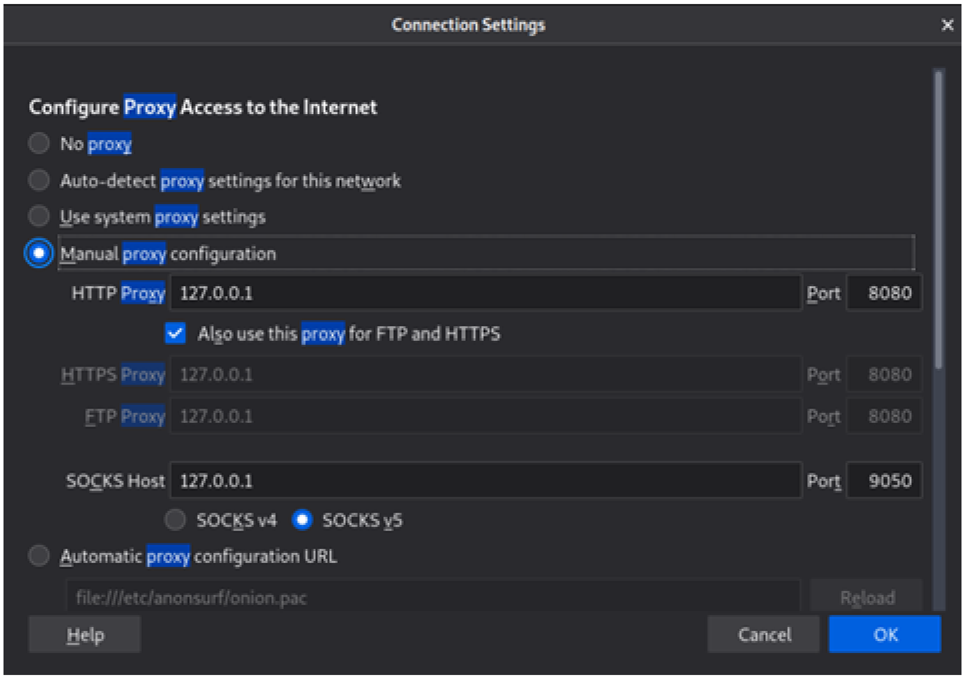
Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more

proxy
Settings...

7. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. **Close** the Preferences tab.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

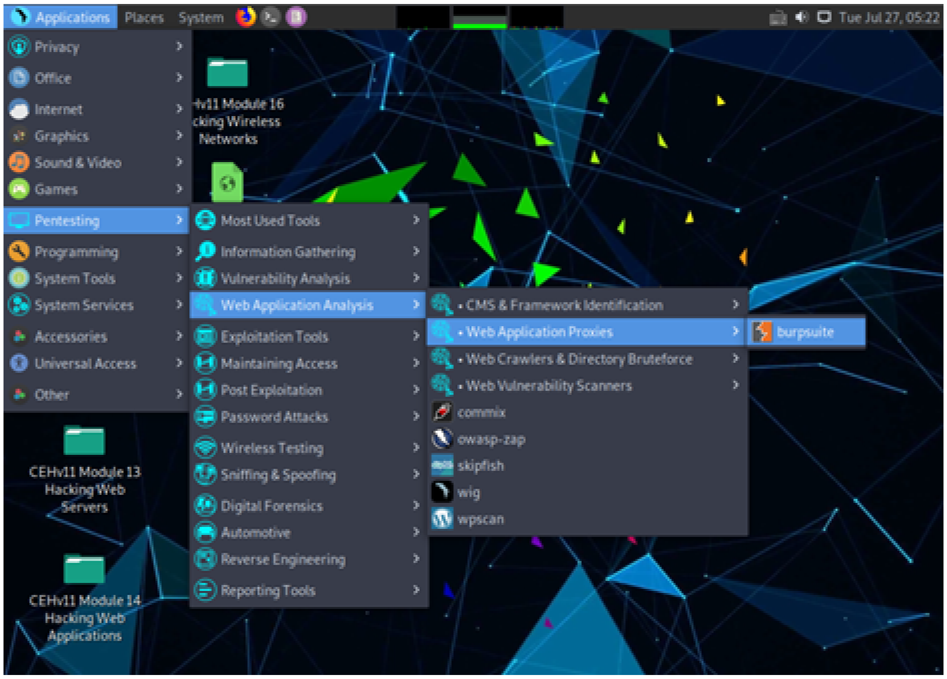
SOCKS Host 127.0.0.1 Port 9050

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

file:///etc/anonsurf/onion.pac

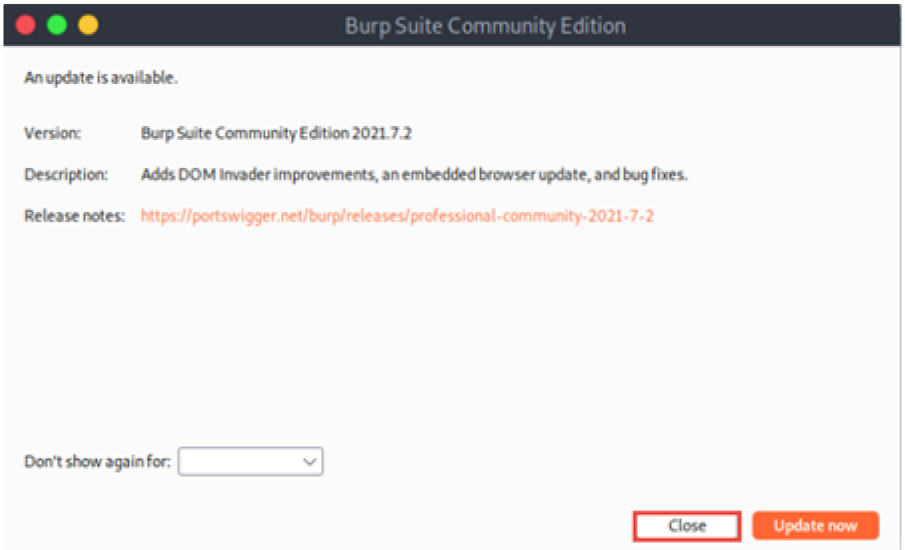
8. Now, minimize the browser window, click the **Applications** menu from the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the Burp Suite application.



9. In the next Burp Suite Community Edition notification, click **OK**.

10. In the **Delete old temporary files?** notification, click **Leave**.

11. A Burp Suite Community Edition wizard appears asking for an update, click **Close**.



Burp Suite Community Edition

An update is available.

Version: Burp Suite Community Edition 2021.7.2

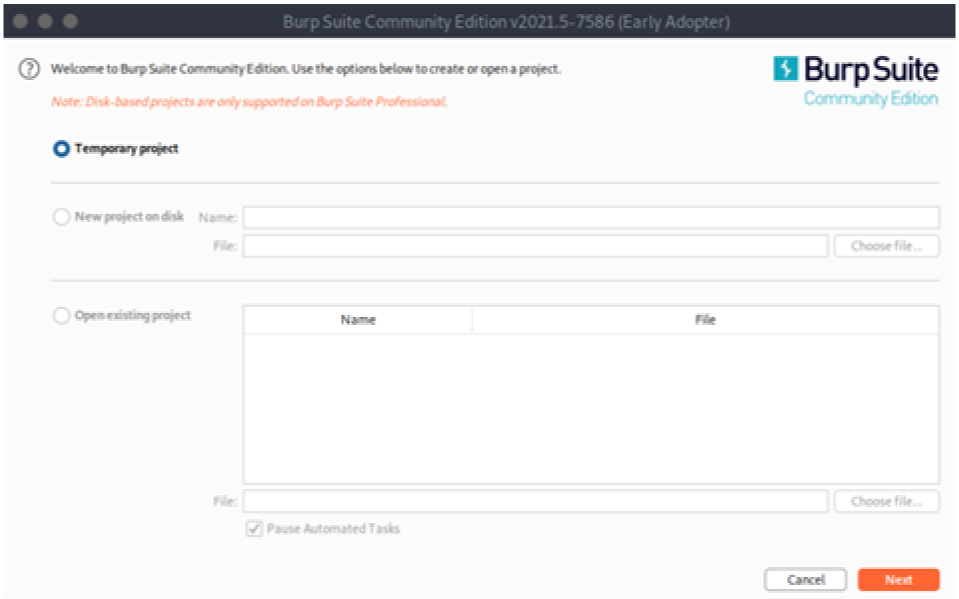
Description: Adds DOM Invader improvements, an embedded browser update, and bug fixes.

Release notes: https://portswigger.net/burp/releases/professional-community-2021-7-2

Don't show again for:

12. The Burp Suite main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

Note: If an update window appears, click **Close**.



Burp Suite Community Edition v2021.5-7586 (Early Adopter)

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk Name: File:

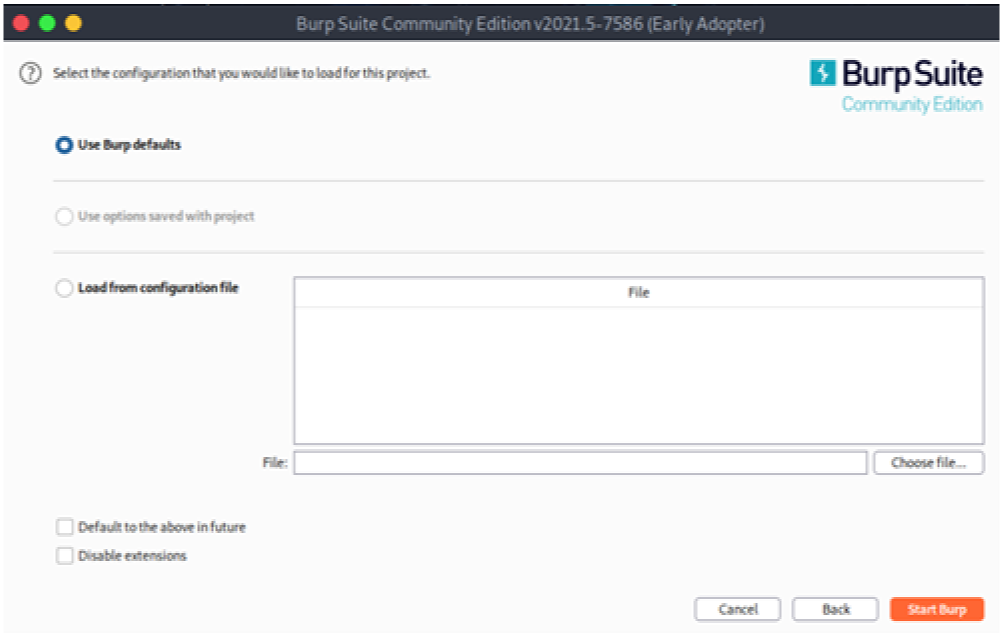
○ Open existing project

Name	File

File:

☑ Pause Automated Tasks

13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.



Burp Suite Community Edition v2021.5-7586 (Early Adopter)

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

○ Load from configuration file

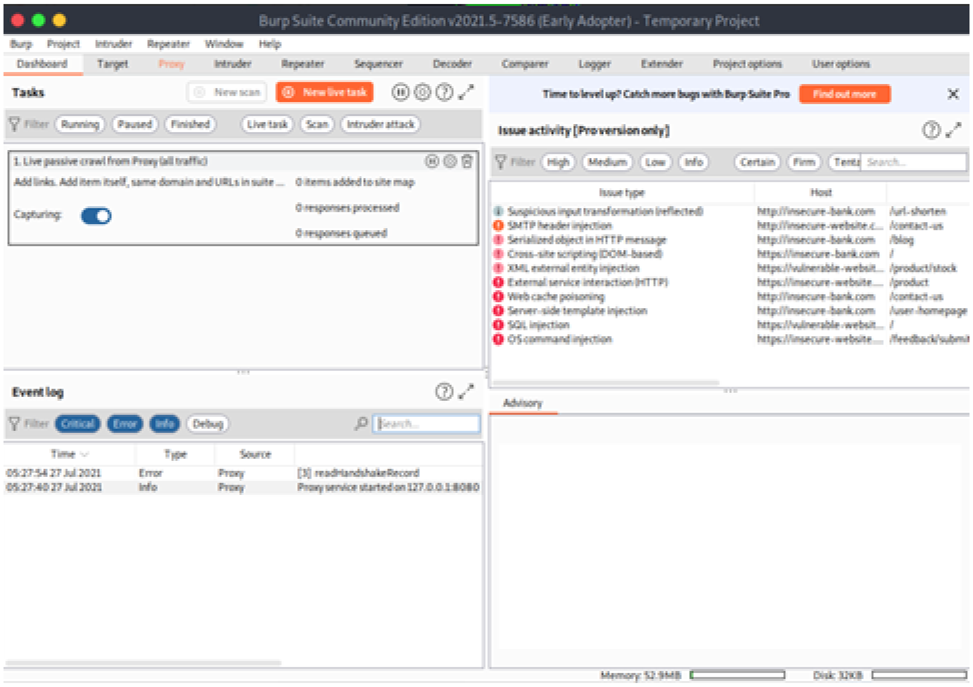
File

File:

□ Default to the above in future

□ Disable extensions

14. The Burp Suite main window appears; click the **Proxy** tab from the available options in the top section of the window.



Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory
Memory: 52.9MB
Disk: 32KB

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite ... 0 items added to site map

Capturing: ● 0 responses processed

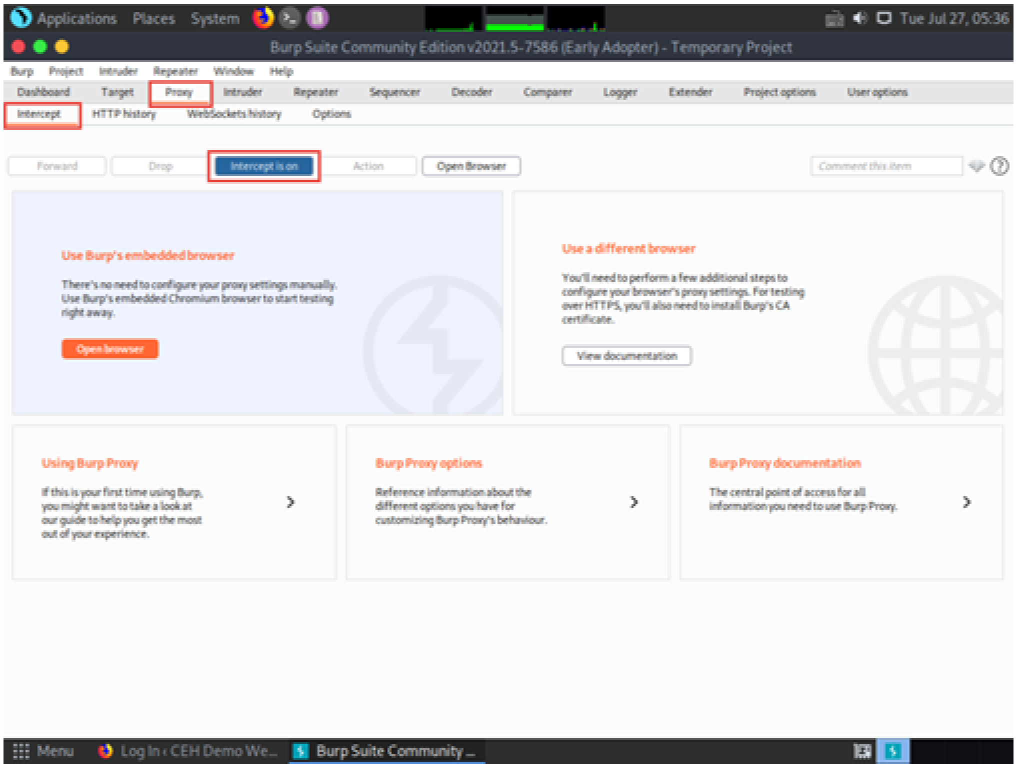
0 responses queued

Issue type	Host	
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Time	Type	Source	
05:27:54 27 Jul 2021	Error	Proxy	[3] readHandshakeRecord
05:27:40 27 Jul 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

15. In the Proxy settings, by default, the Intercept tab opens-up. Observe that by default, the interception is **active** as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.



Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options

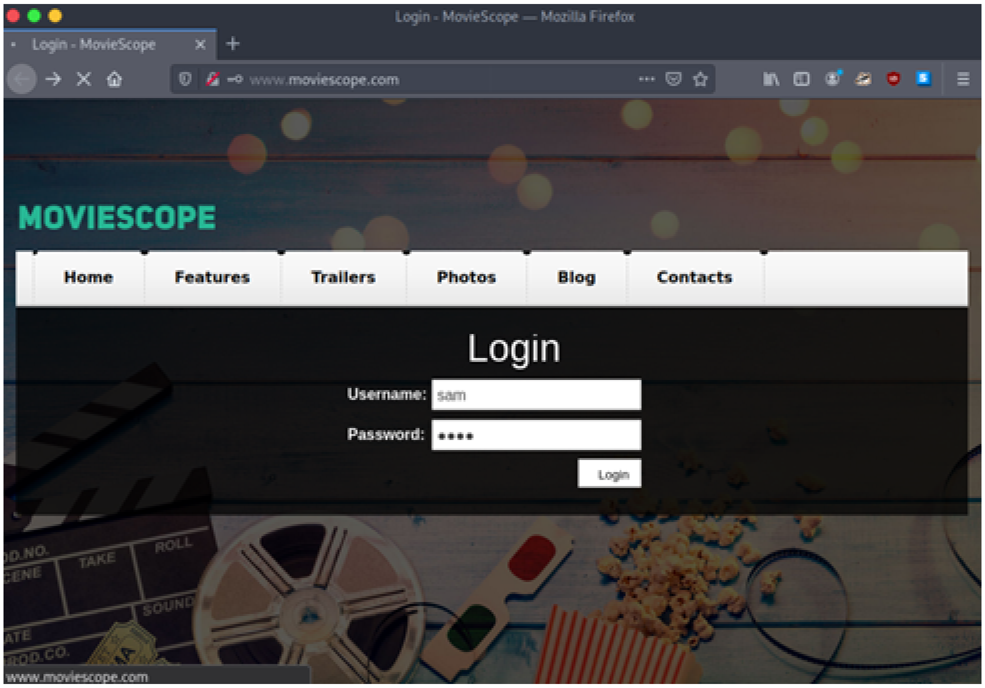
Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

16. Switch back to the browser window, and on the login page of the target website (www.moviescope.com), enter the credentials **sam** and **test**. Click the **Login** button.

Note: Here, we are logging in as a registered user on the website.



Login

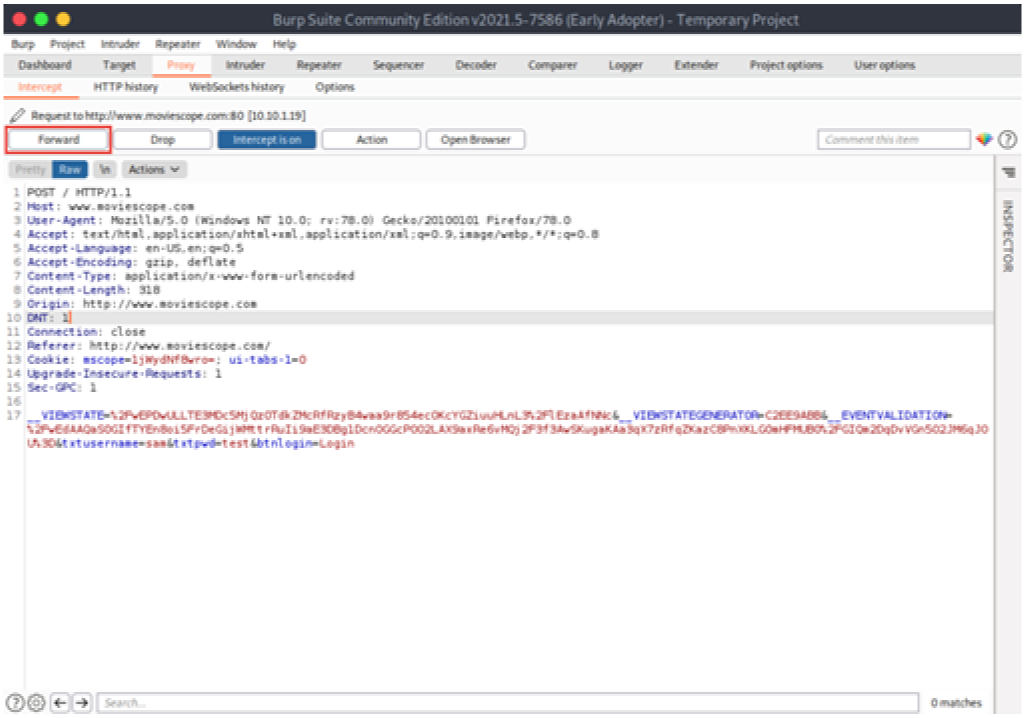
Username: sam

Password: ••••

17. Switch back to the Burp Suite window and observe that the **HTTP** request was intercepted by the application.

    Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

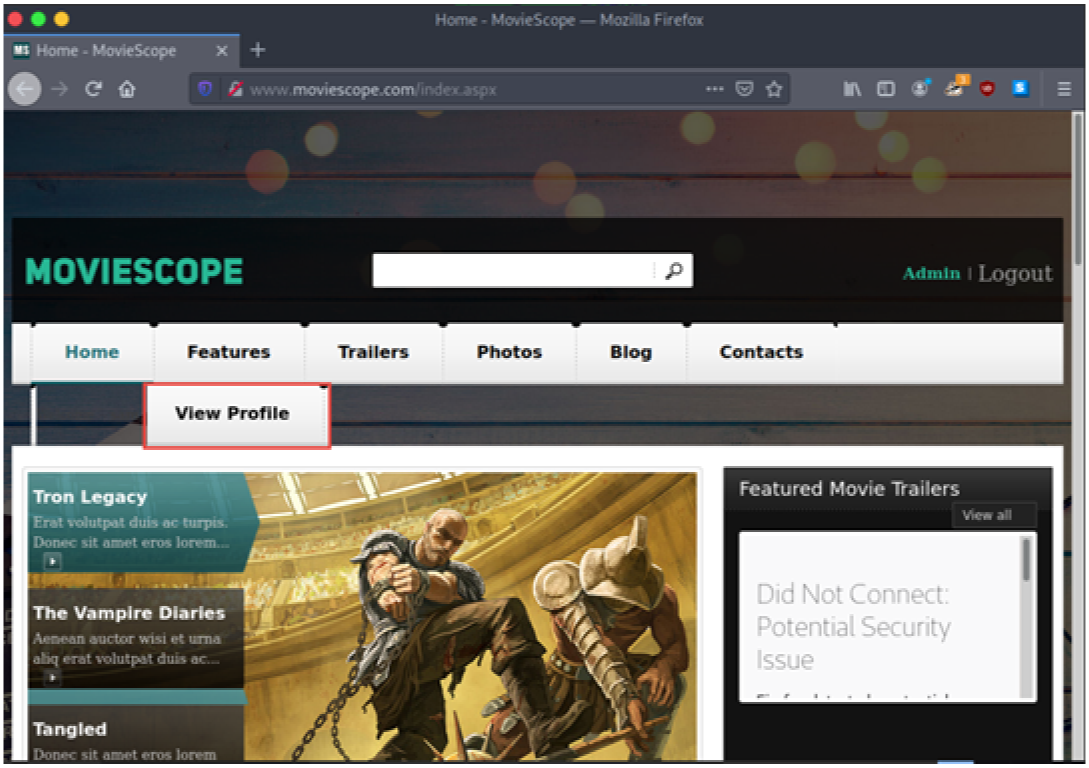
18. Now, keep clicking the **Forward** button until you are logged into the user account.


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.moviescope.com:80 [10.10.1.19]
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
Search...
0 matches

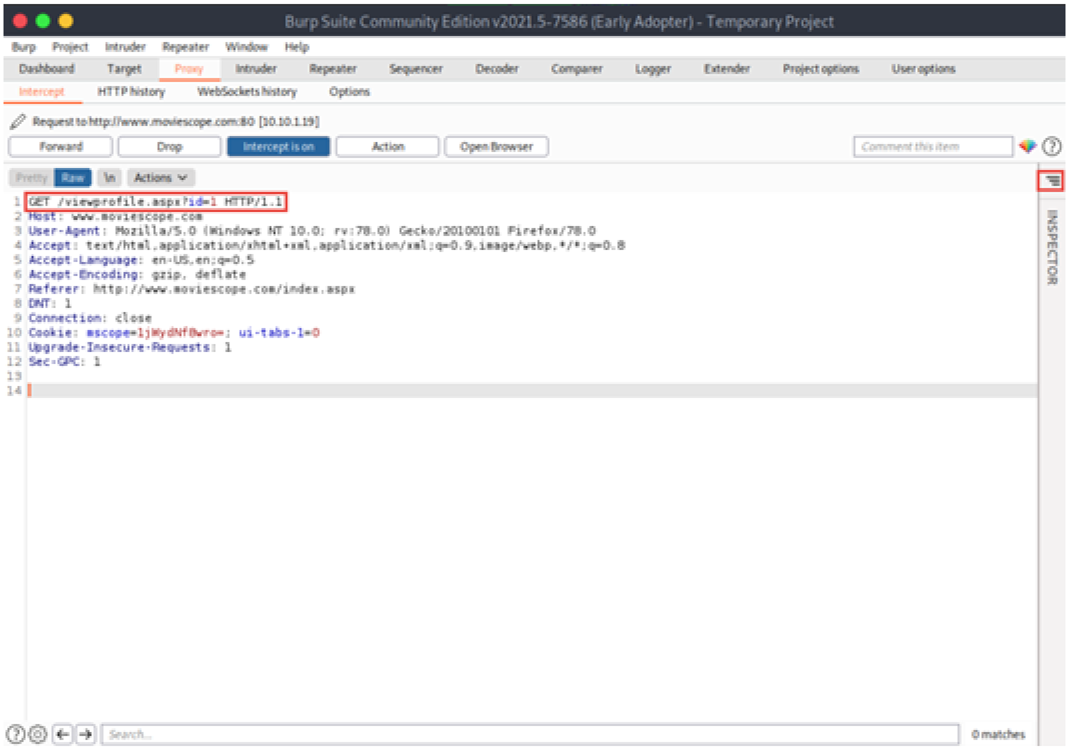
```
POST / HTTP/1.1
Host: www.moviescope.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
Origin: http://www.moviescope.com
DNT: 1
Connection: close
Referer: http://www.moviescope.com/
Cookie: mscope=1jWydNf8wro=; ui-tabs-1=0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

__VIEWSTATE=%2FwEPDwULLTE3MDc5MjQz0TdkZMcRfRzyB4waa9r854ecOKcYGZiuuHLnL3%2FlEzaAfNNc&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=
%2FwEdAAQaSOGIfTYEn8oi5FrDeGijWMttrRuIi9aE3DBg1DcnOGGcPOO2LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfqZKazC8PnXKLGOmHFMUB0%2FGIQm2DqDvVGn5O2JM6qJO
U%3D&txtusername=sam&txtpwd=test&btnlogin=Login
```

19. Switch to the browser and observe that you are now logged into the user account, as shown in the screenshot.
20. Now, click the **View Profile** tab from the menu bar to view the user information.

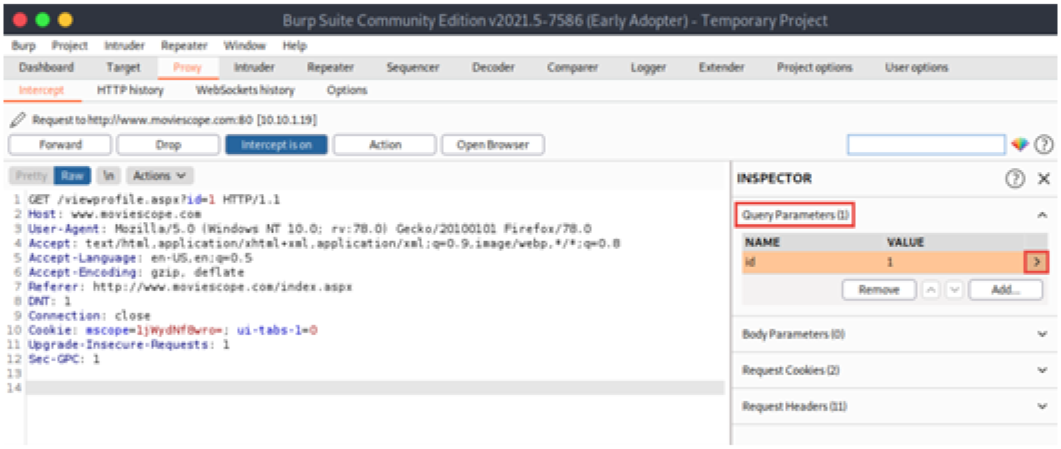

Home - MovieScope — Mozilla Firefox
Home - MovieScope
www.moviescope.com/index.aspx
MOVIESCOPE
Admin | Logout
Home
Features
Trailers
Photos
Blog
Contacts
View Profile
Tron Legacy
Erat volutpat duis ac turpis. Donec sit amet eros lorem...
The Vampire Diaries
Aenean auctor wisi et urna aliq erat volutpat duis ac...
Tangled
Donec sit amet eros lorem
Featured Movie Trailers
View all
Did Not Connect: Potential Security Issue

21. After clicking the View Profile tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the **HTTP** request, as shown in the screenshot.
22. Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section.


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.moviescope.com:80 [10.10.1.19]
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
Search...
0 matches

```
GET /viewprofile.aspx?id=1 HTTP/1.1
Host: www.moviescope.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.moviescope.com/index.aspx
DNT: 1
Connection: close
Cookie: mscope=1jWydNf8wro=; ui-tabs-1=0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

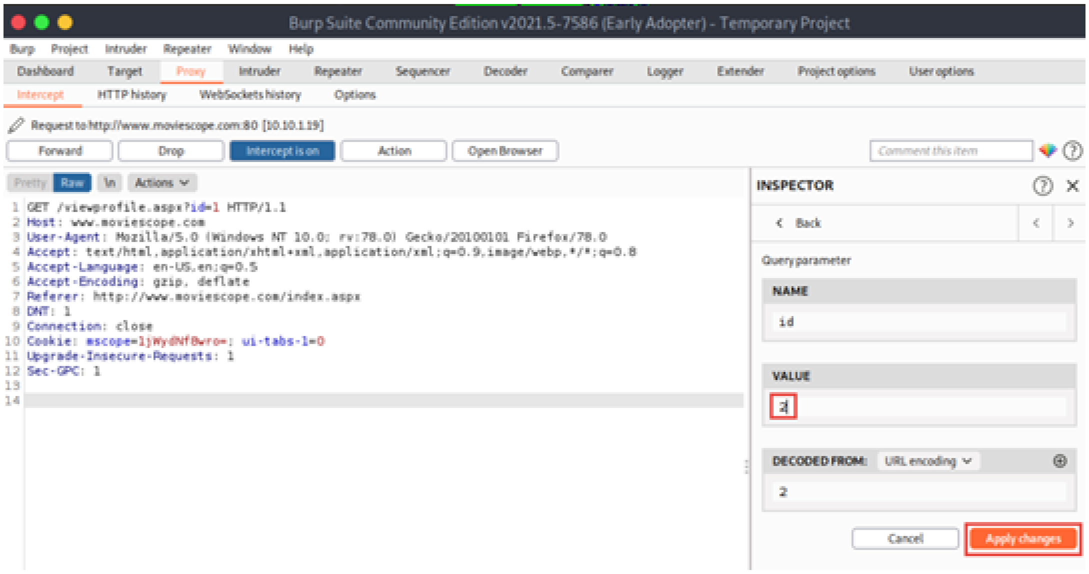
23. Inspector wizard appears, click to expand **Query Parameters**.
24. You can observe **NAME** and **VALUE** columns, double click on the **value**, or **click arrow icon** (>)


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.moviescope.com:80 [10.10.1.19]
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
INSPECTOR
Query Parameters (1)
Remove
Add...
Body Parameters (0)
Request Cookies (2)
Request Headers (11)

```
GET /viewprofile.aspx?id=1 HTTP/1.1
Host: www.moviescope.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.moviescope.com/index.aspx
DNT: 1
Connection: close
Cookie: mscope=1jWydNf8wro=; ui-tabs-1=0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

NAME	VALUE
id	1

25. In the next wizard, change the **VALUE** from **1** to **2** and click **Apply Changes** button.


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
Back
Cancel
Apply changes

Request to http://www.moviescope.com:80 [10.10.1.19]

```
GET /viewprofile.aspx?id=1 HTTP/1.1
Host: www.moviescope.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.moviescope.com/index.aspx
DNT: 1
Connection: close
Cookie: mscope=1jWydNf8wro=; ui-tabs-1=0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1


```

Query parameter

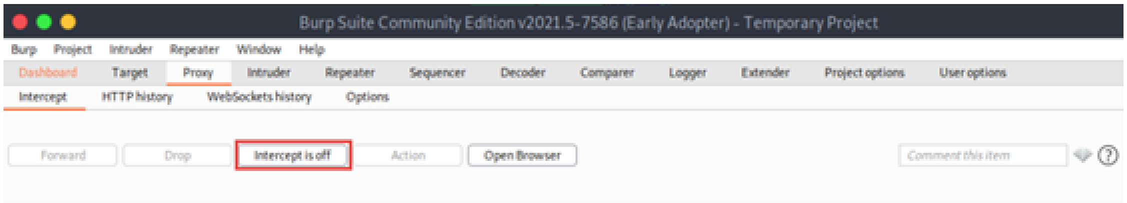
NAME: id

VALUE: 2

DECODED FROM: URL encoding

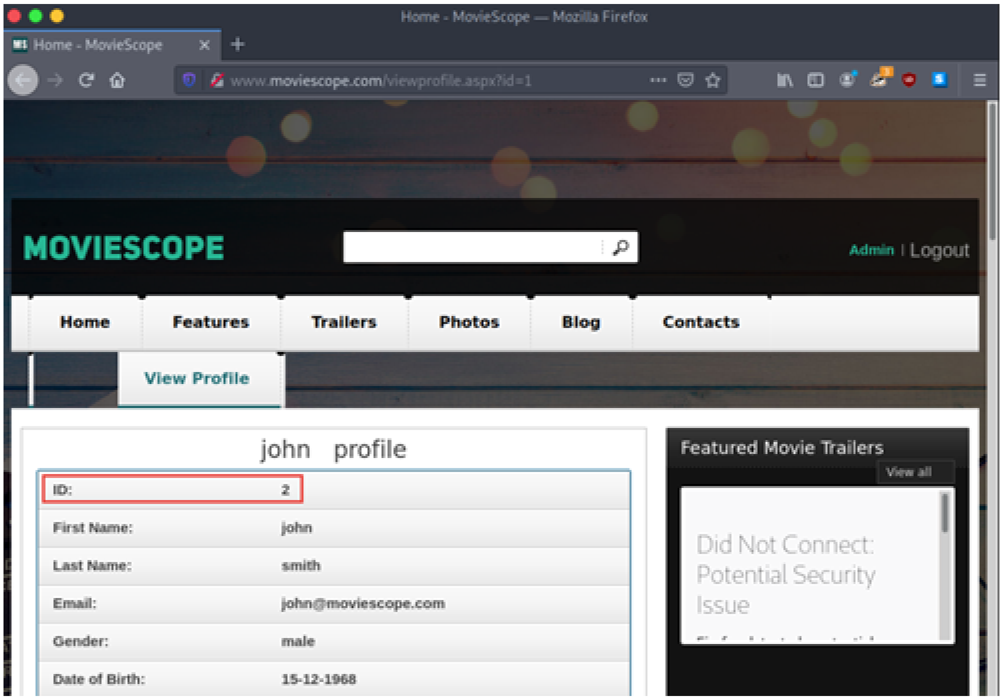
2

26. Now, click the **Intercept** is on button to turn off the interception.


Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is off
Action
Open Browser
Comment this item

27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

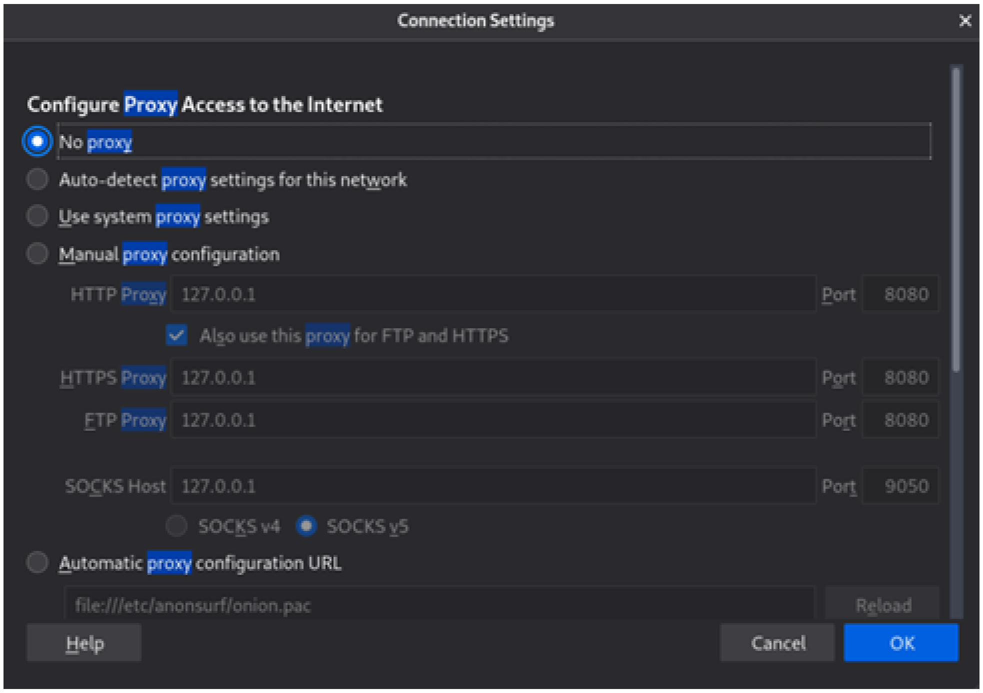
Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.



john profile

ID:	2
First Name:	john
Last Name:	smith
Email:	john@moviescope.com
Gender:	male
Date of Birth:	15-12-1968

28. Similarly, you can edit the id parameter in Burp Suite with any random numeric value to view information about other user accounts.
29. Switch to the browser window and perform **Steps 4-6**. Remove the browser proxy set up in **Step 7**, by selecting the **No proxy** radio-button in the Connection Settings window and click **OK**. **Close** the tab.



Configure Proxy Access to the Internet

● No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
○ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080
☑ Also use this proxy for FTP and HTTPS
HTTPS Proxy 127.0.0.1 Port 8080
FTP Proxy 127.0.0.1 Port 8080
SOCKS Host 127.0.0.1 Port 9050
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL
file:///etc/anonsurf/onion.pac

30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.

31. Close all open windows and document all the acquired information.