Web Server and Application Security

Burp Suite Intruder/Repeater

March 2021

Ground Rules

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.

Recap – M6 T9

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

- Burp
- Nikto
- CMSEEK
- Wpscan

Agenda

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

- 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

Using Burp Repeater with HTTP Messages

- 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

Sending HTTP Requests

- 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

HTTP Request History

- 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

Created by fae frey
from Noun Project

Using Burp Repeater with WebSocket Messages

- 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

Sending WebSocket Messages

- 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

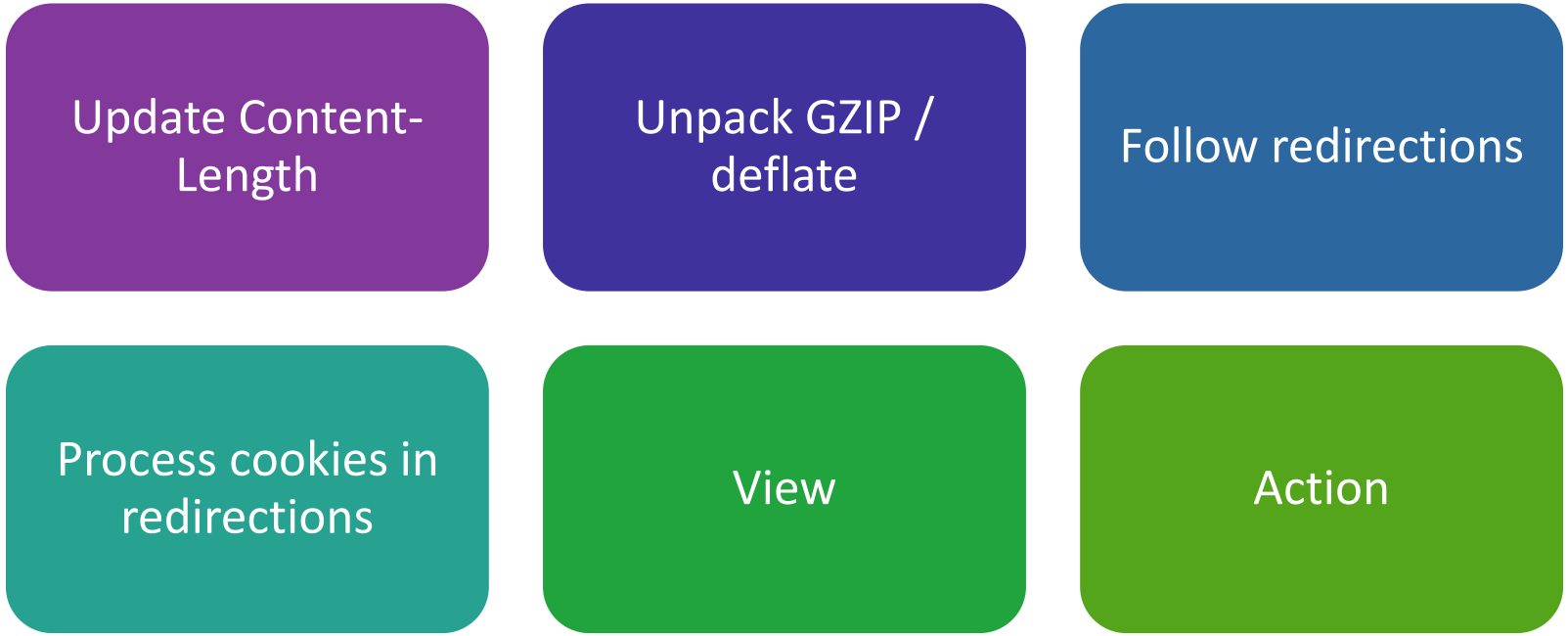
WebSocket Message History

- 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

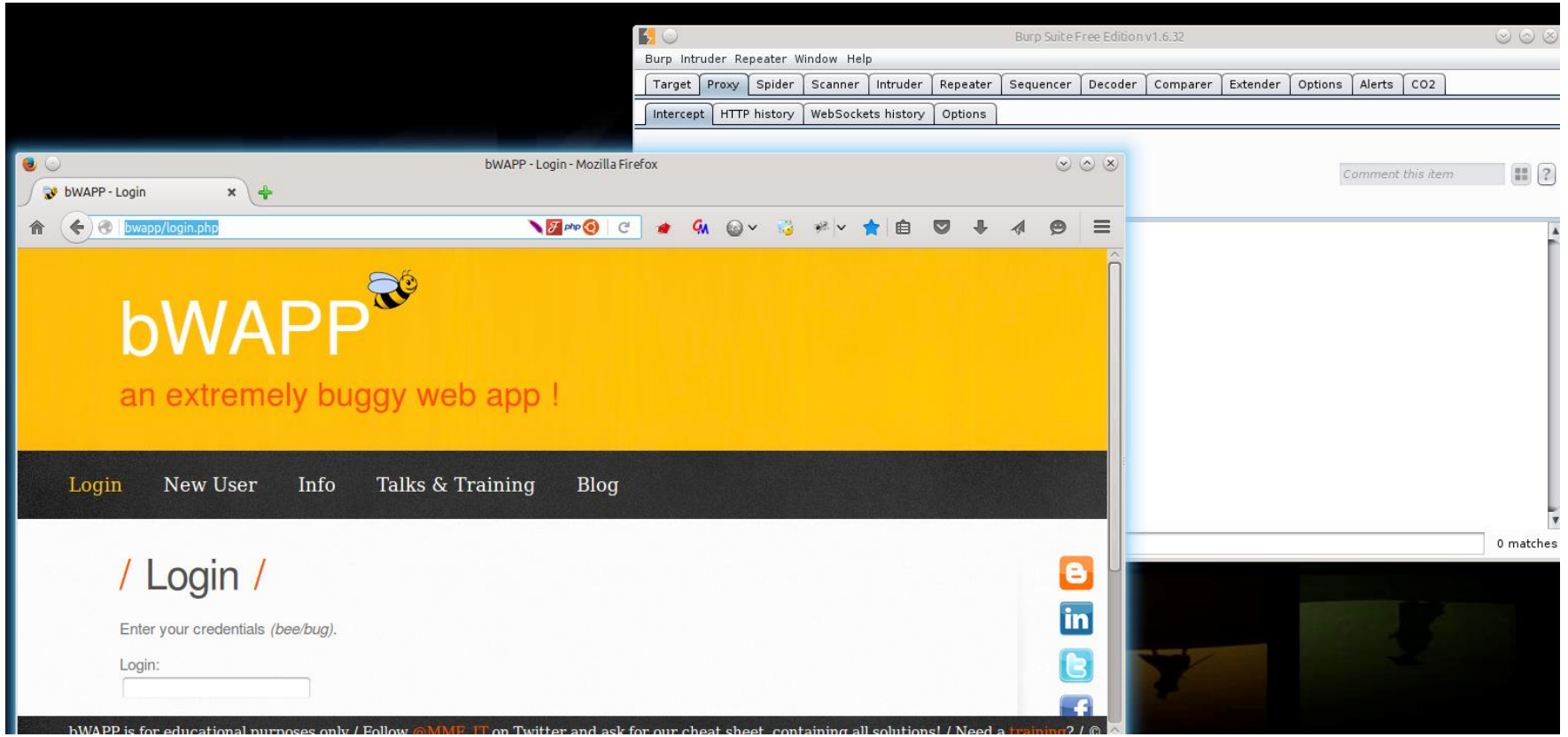
Created by fae frey from Noun Project

Repeater Options

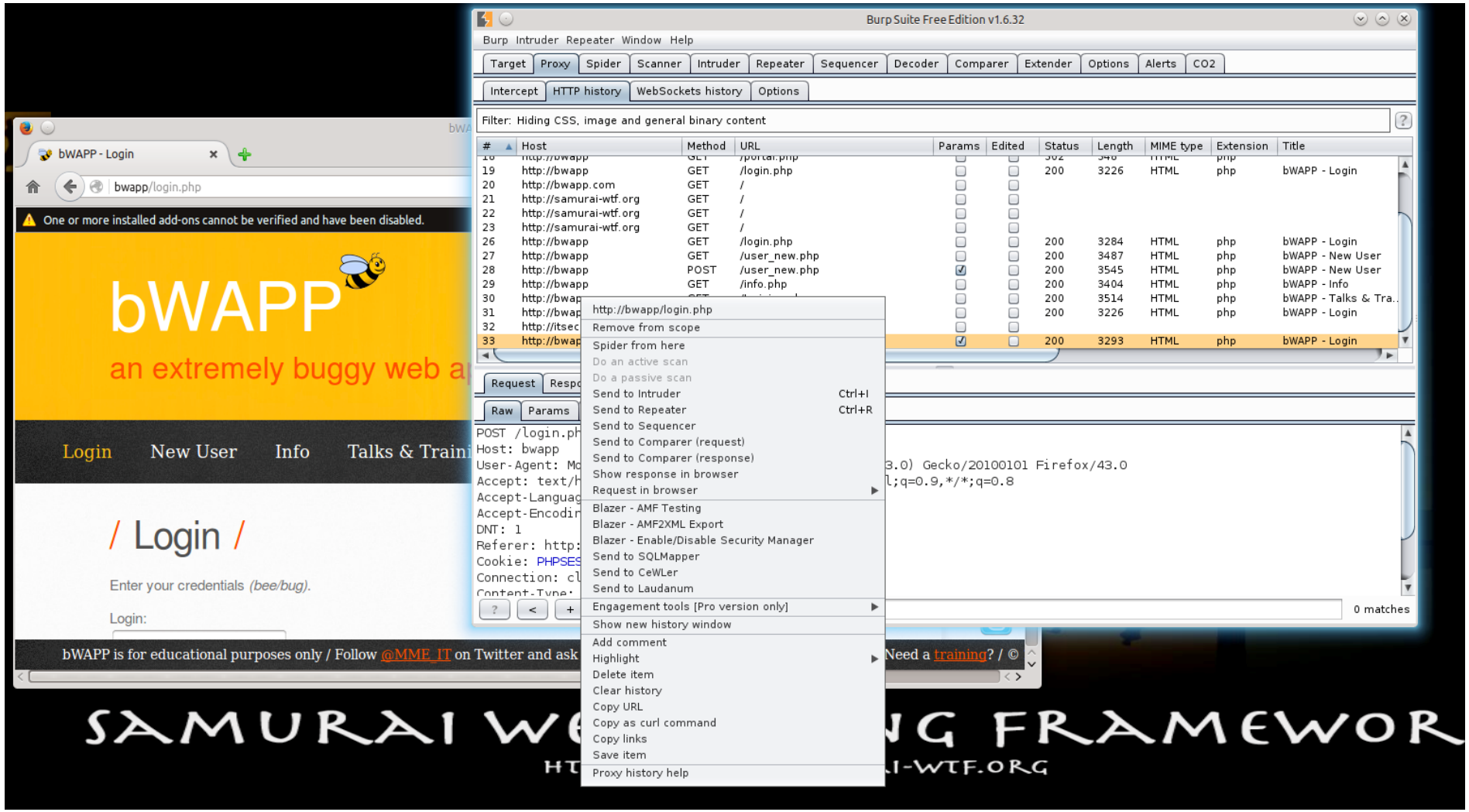
- Burp Repeater has various options that control its behavior, including-



Burp Repeater

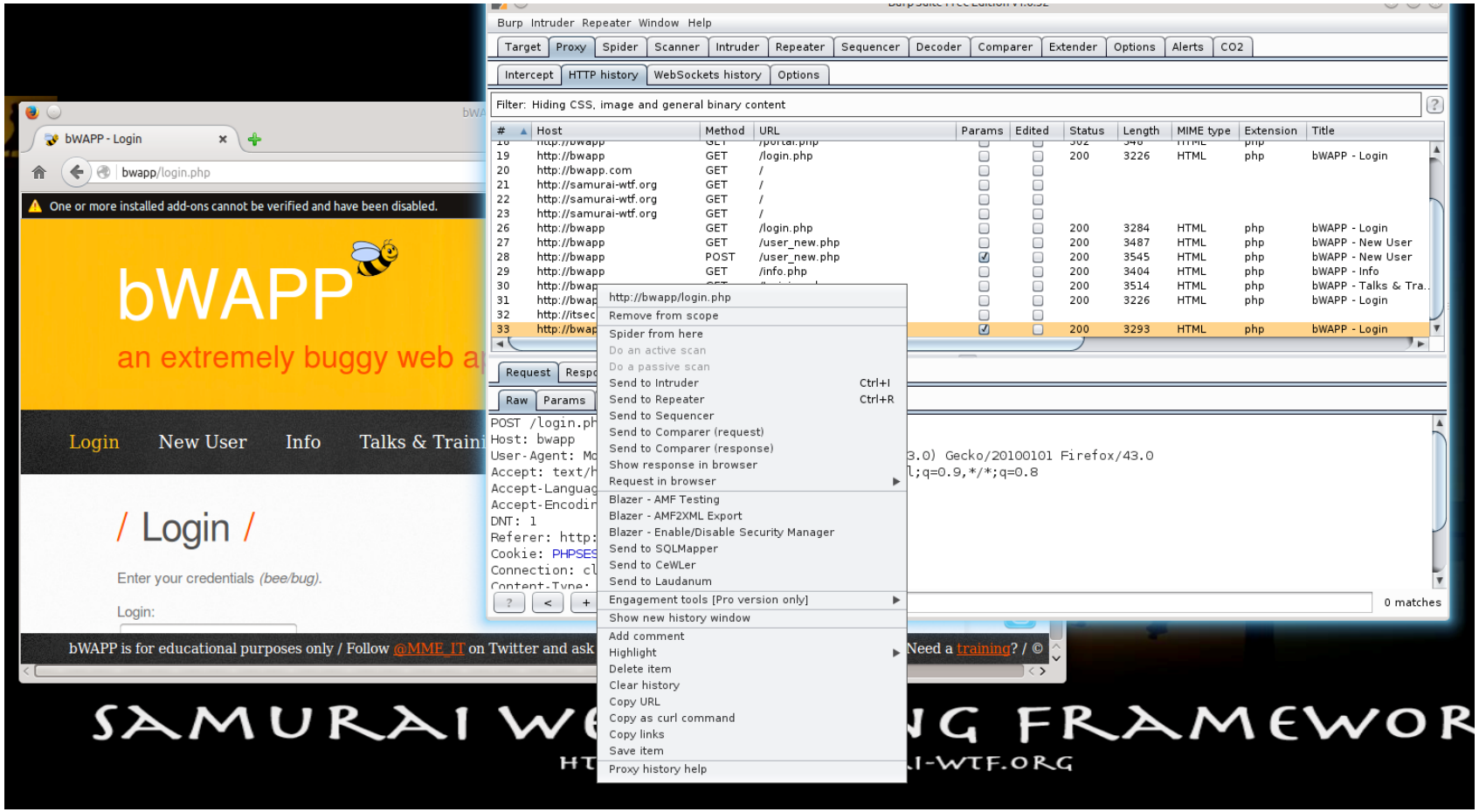


Burp Repeater

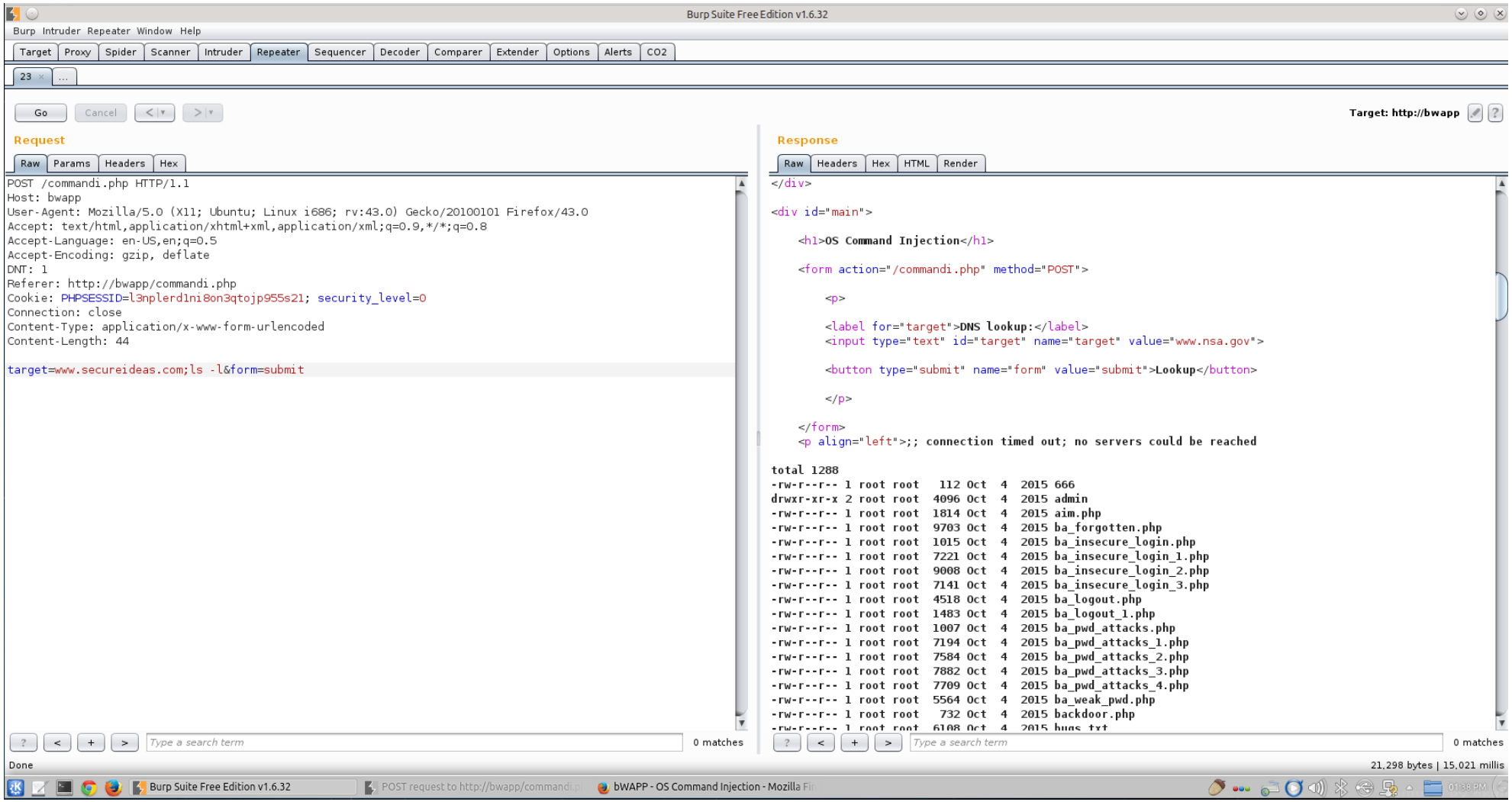


Burp Repeater

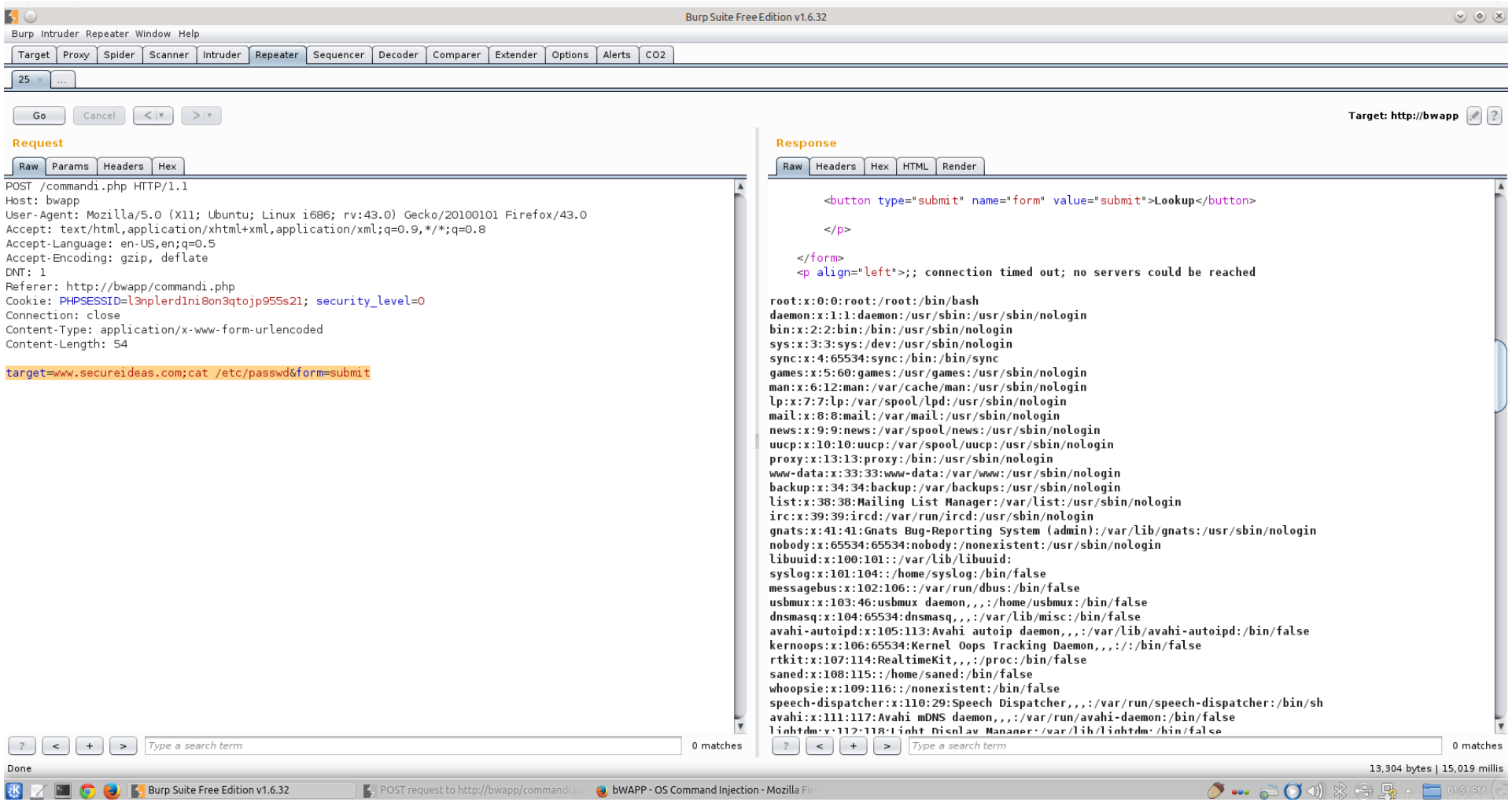
Burp Repeater



Burp Repeater



Burp Repeater



Name of the Activity

Behind the Door Number

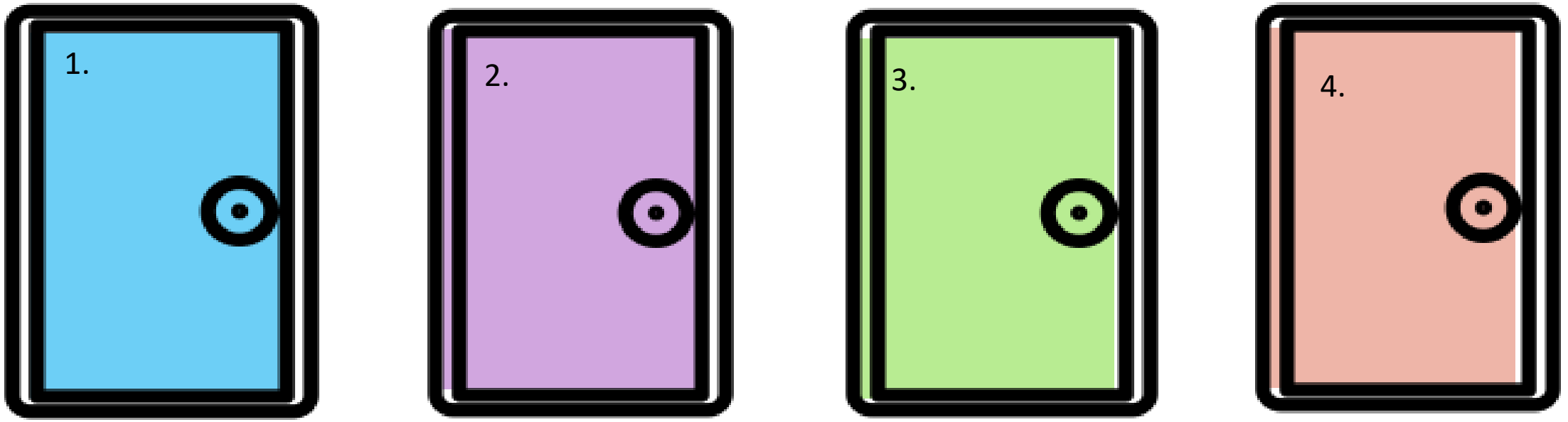
Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Knowledge Check – Behind the Door Number



Source: Noun project

Managing Request Tabs

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

- Rename tabs by double-clicking the tab header.
- Reorder tabs by dragging them.
- Open a new tab by clicking on the right-most "..." tab.
- Close tabs by clicking the X button in the tab header

Created by fae frey from Noun Project

What is Burp Intruder?

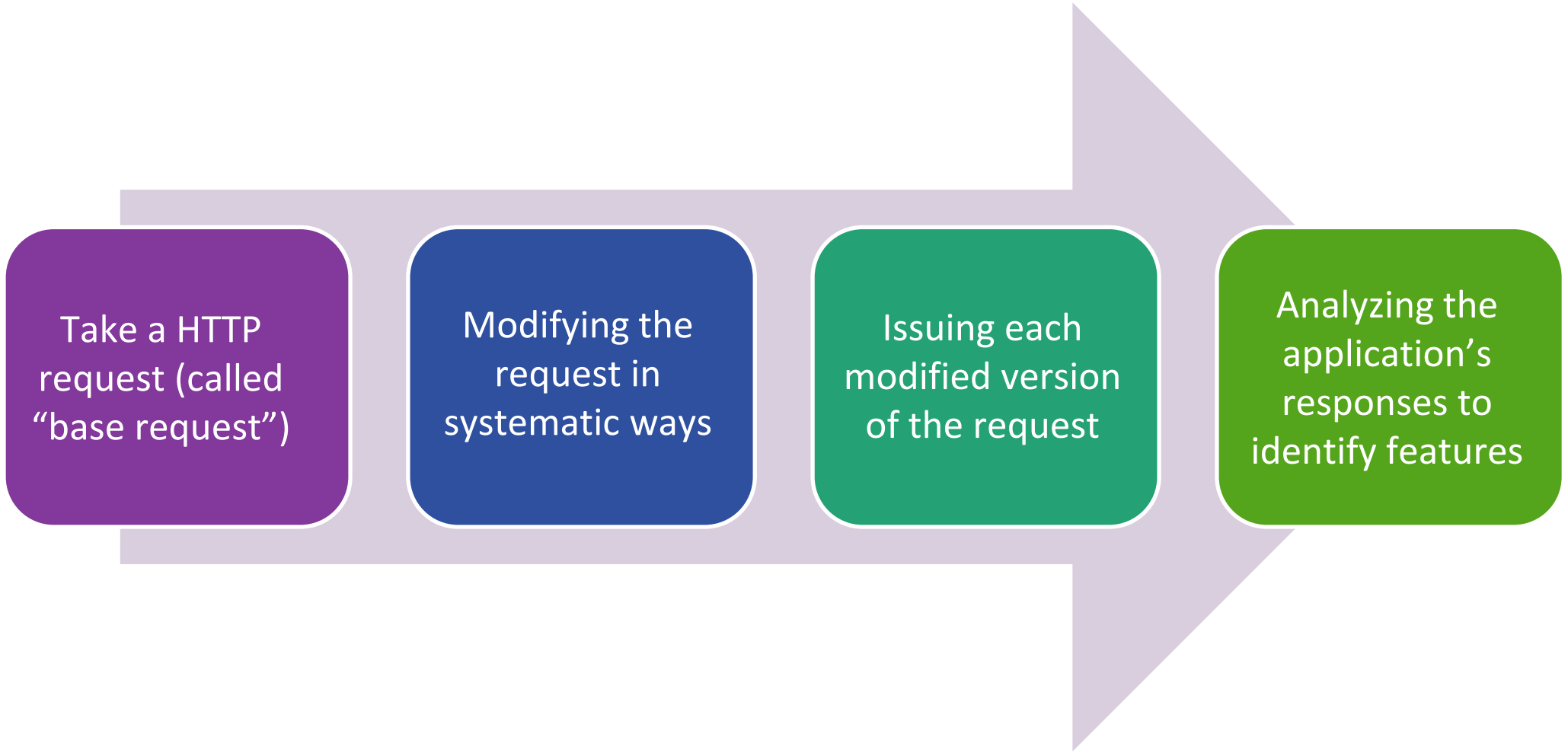
Created by fae frey
from Noun Project

Burp Intruder

- 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

How Burp Intruder Works



Name of the Activity

Complete the Image

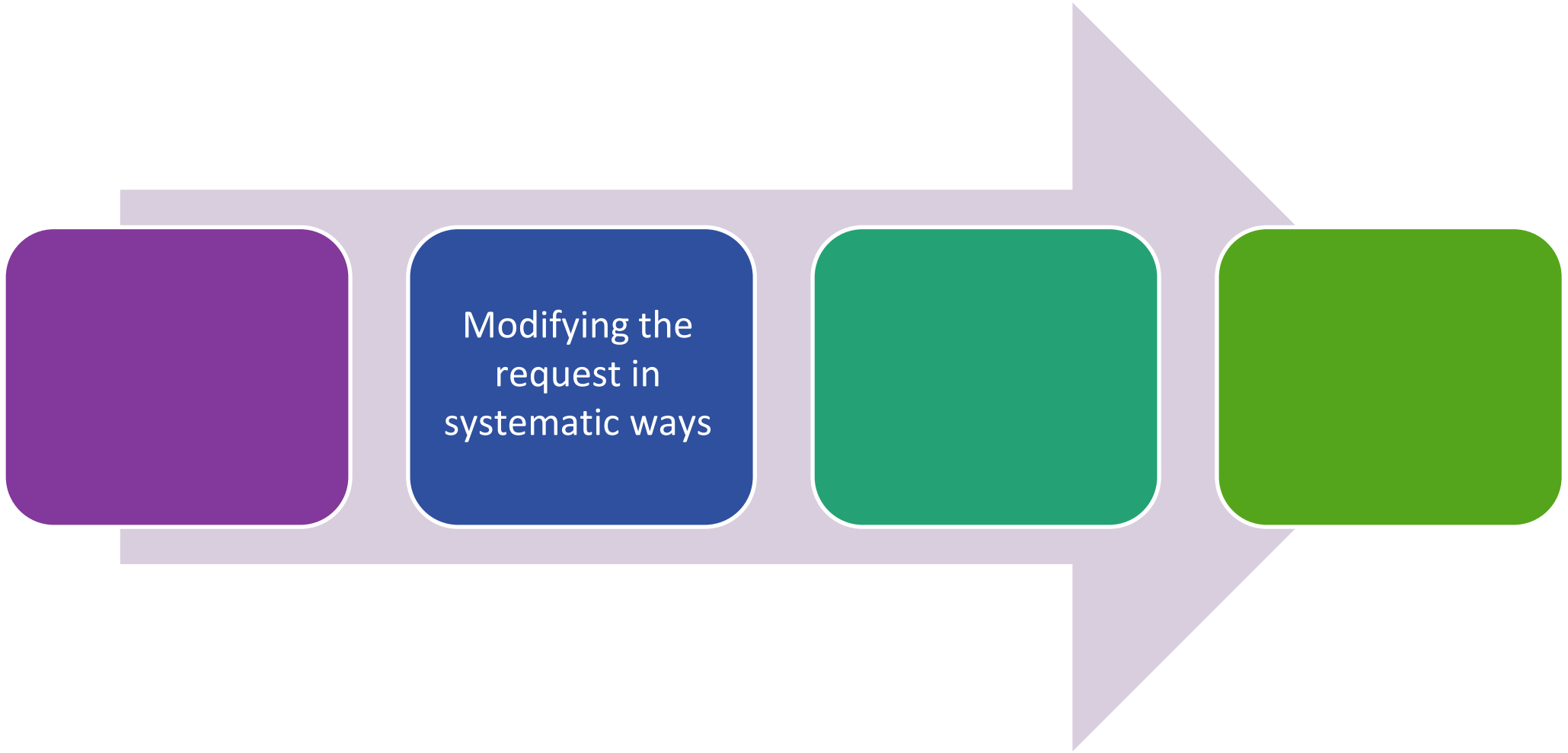
Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity



Typical Uses

- 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:

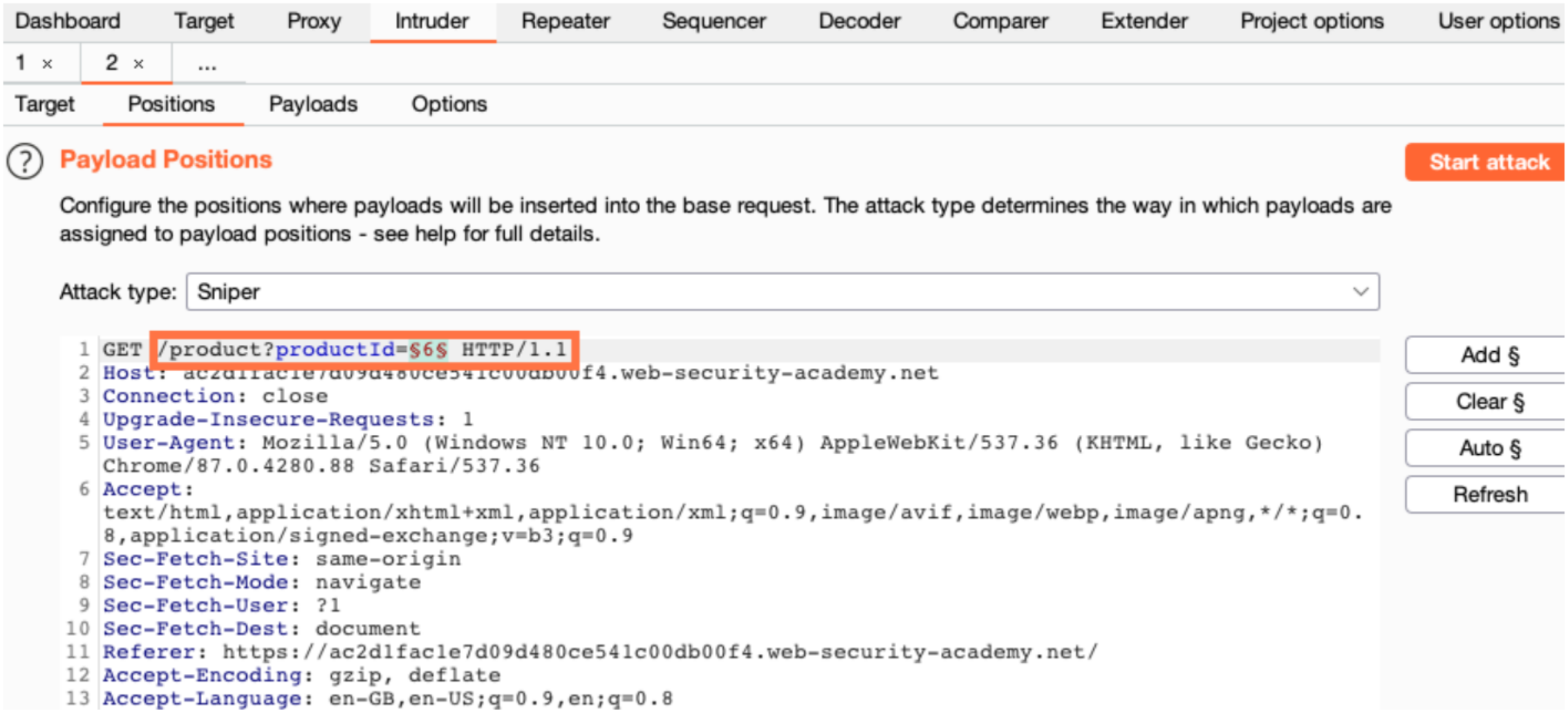
Enumerating Identifiers

Harvesting Useful Data

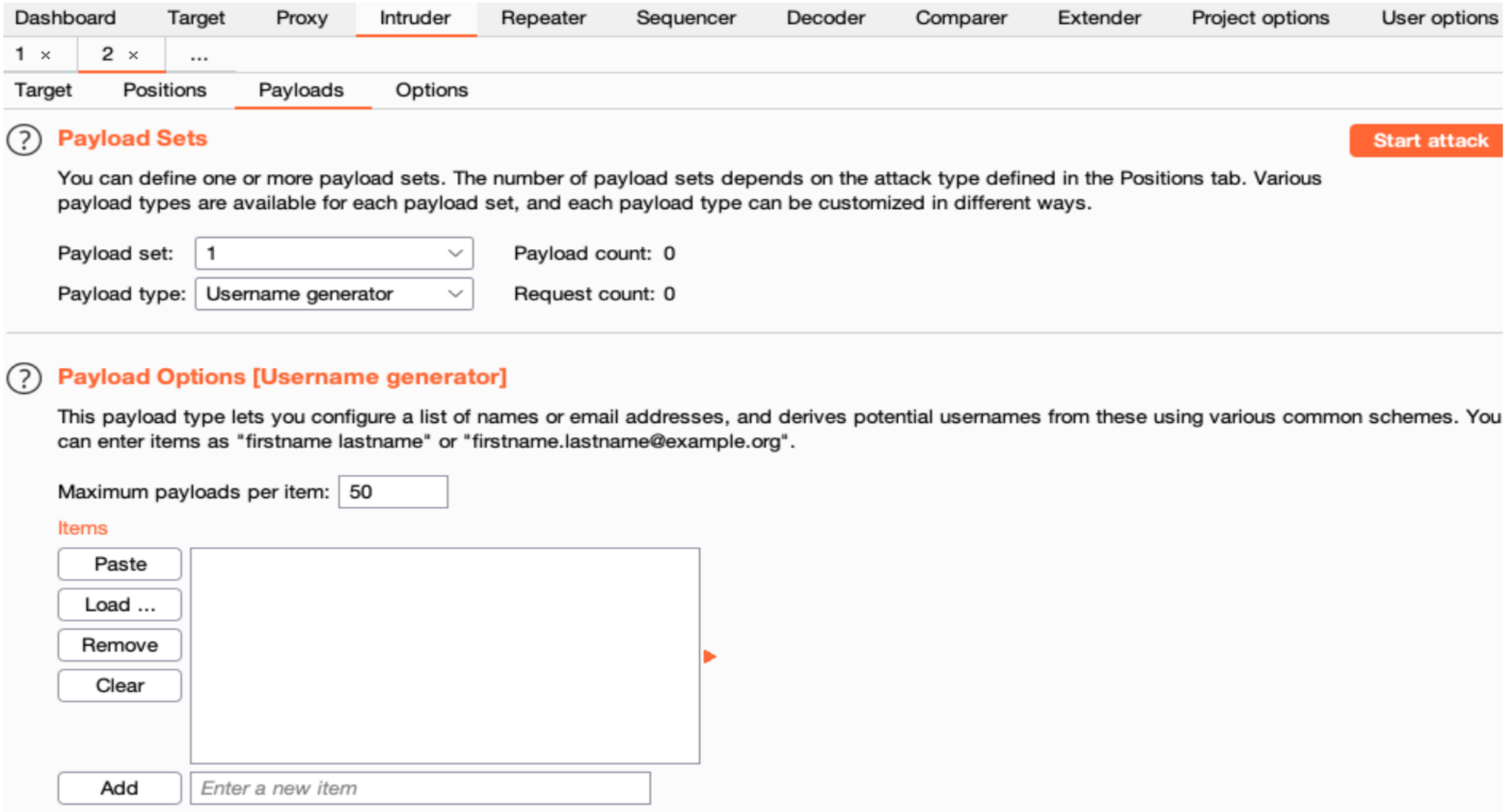
Fuzzing for Vulnerabilities

Created by fae frey
from Noun Project

Enumerating Identifiers



Enumerating Identifiers



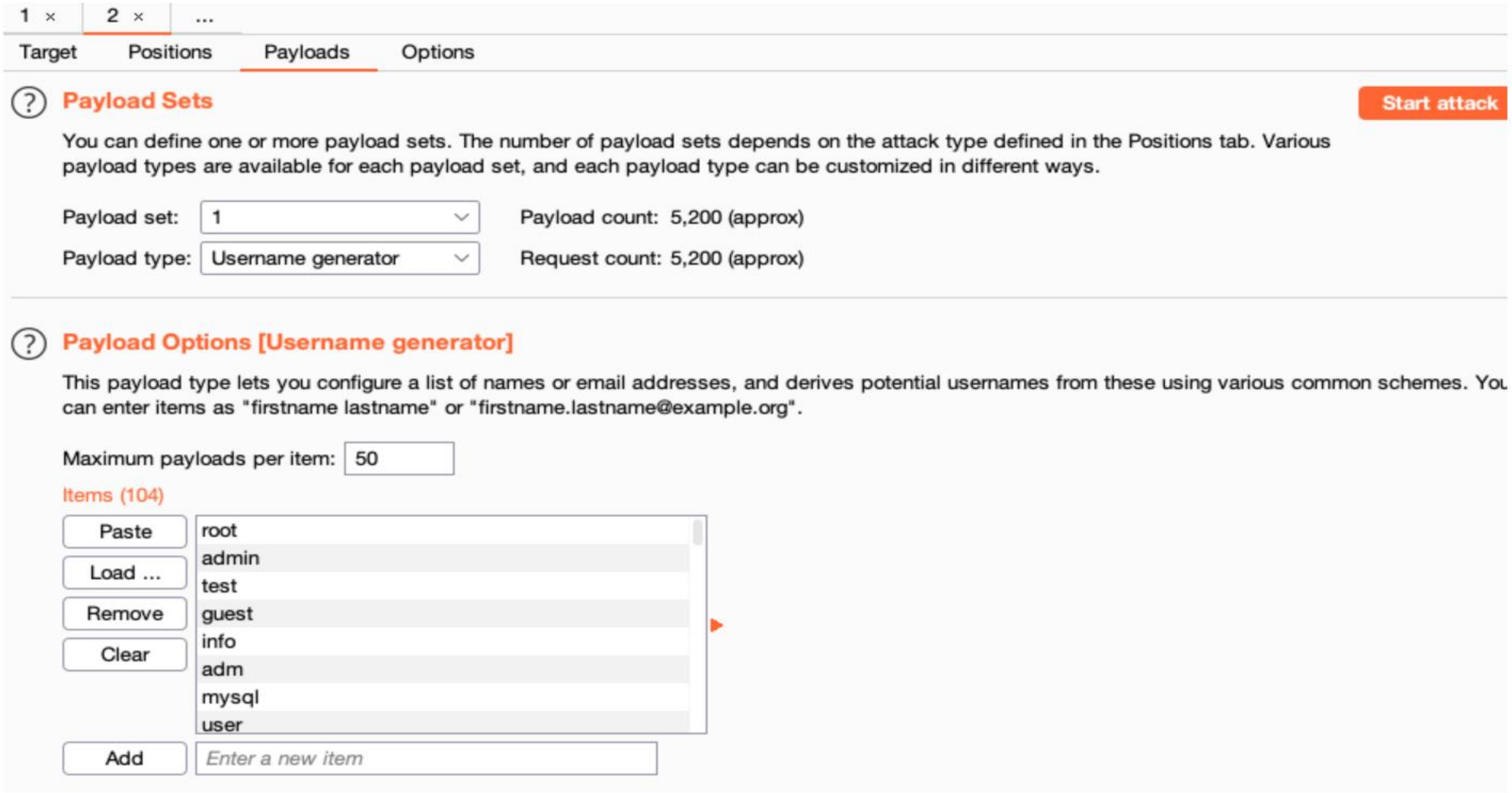
Enumerating Identifiers

Results | Target | Positions | Payloads | Options

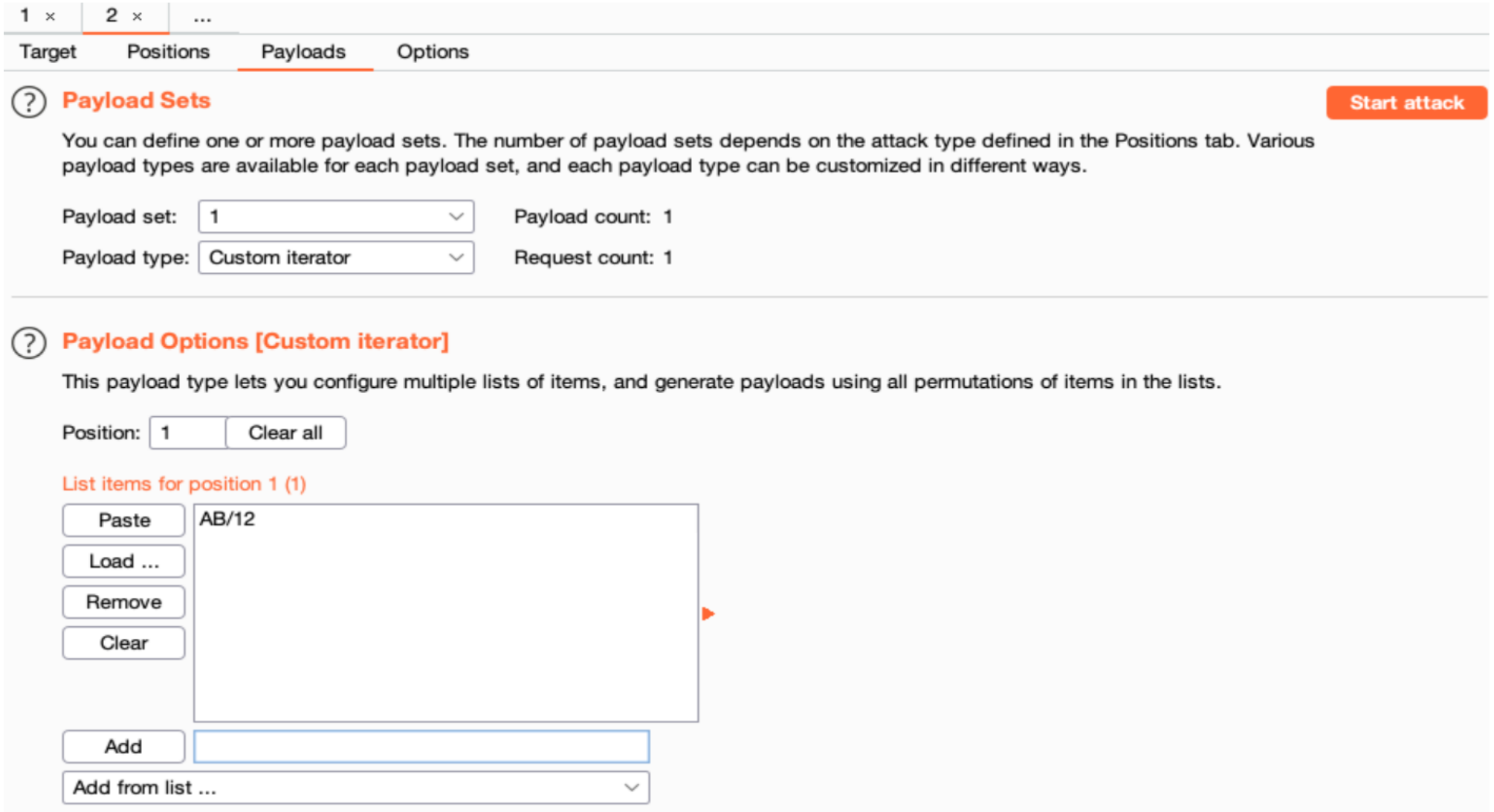
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
26	adam	200			3186	
0		200			3184	
1	root	200			3184	
2	admin	200			3184	
3	test	200			3184	
4	guest	200			3184	
5	info	200			3184	
6	adm	200			3184	
7	mysql	200			3184	
8	user	200			3184	
9	administrator	200			3184	
10	oracle	200			3184	
11	ftp	200			3184	

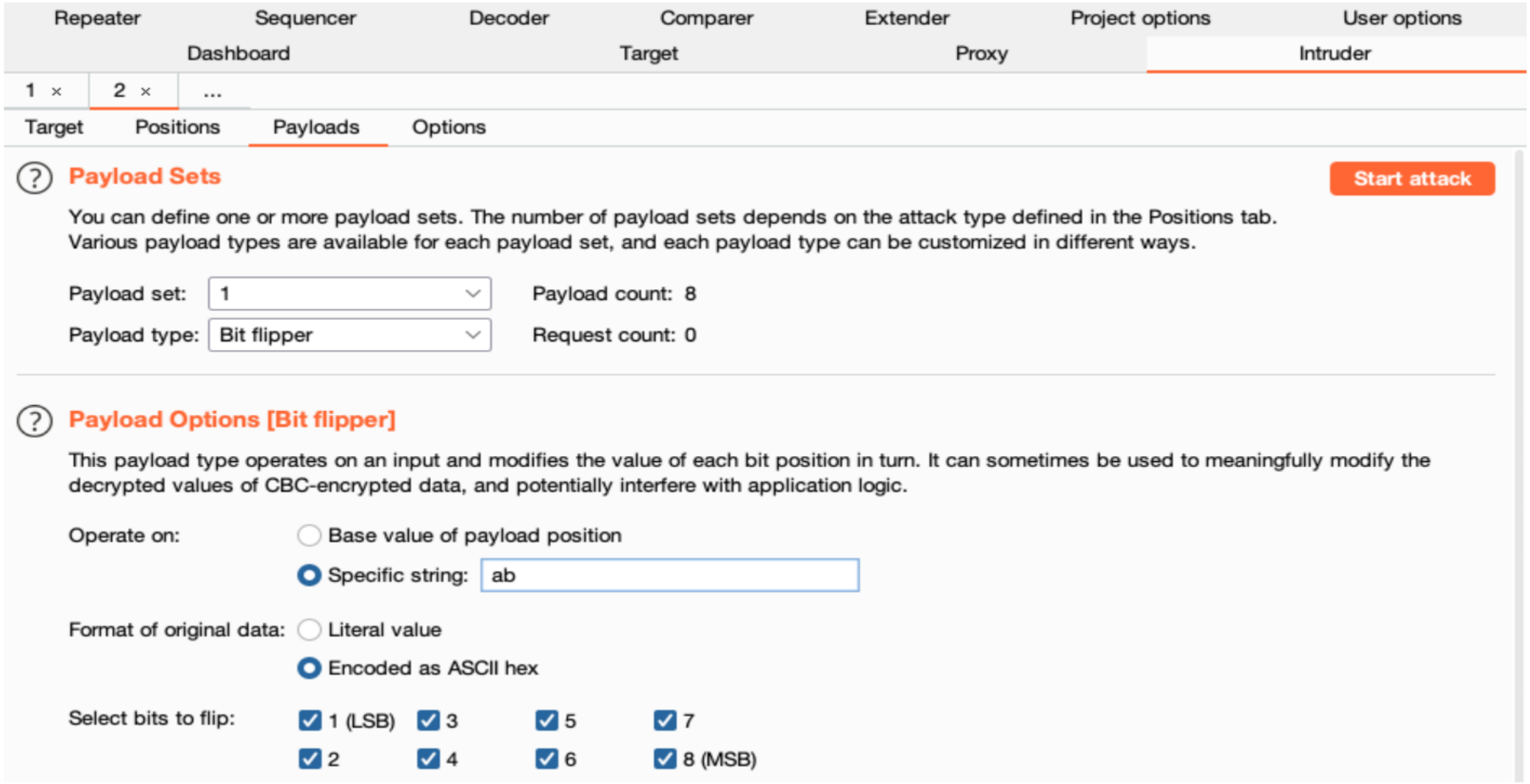
Enumerating Identifiers



Enumerating Identifiers



Enumerating Identifiers



Name of the Activity

Fastest Finger First

Instructions

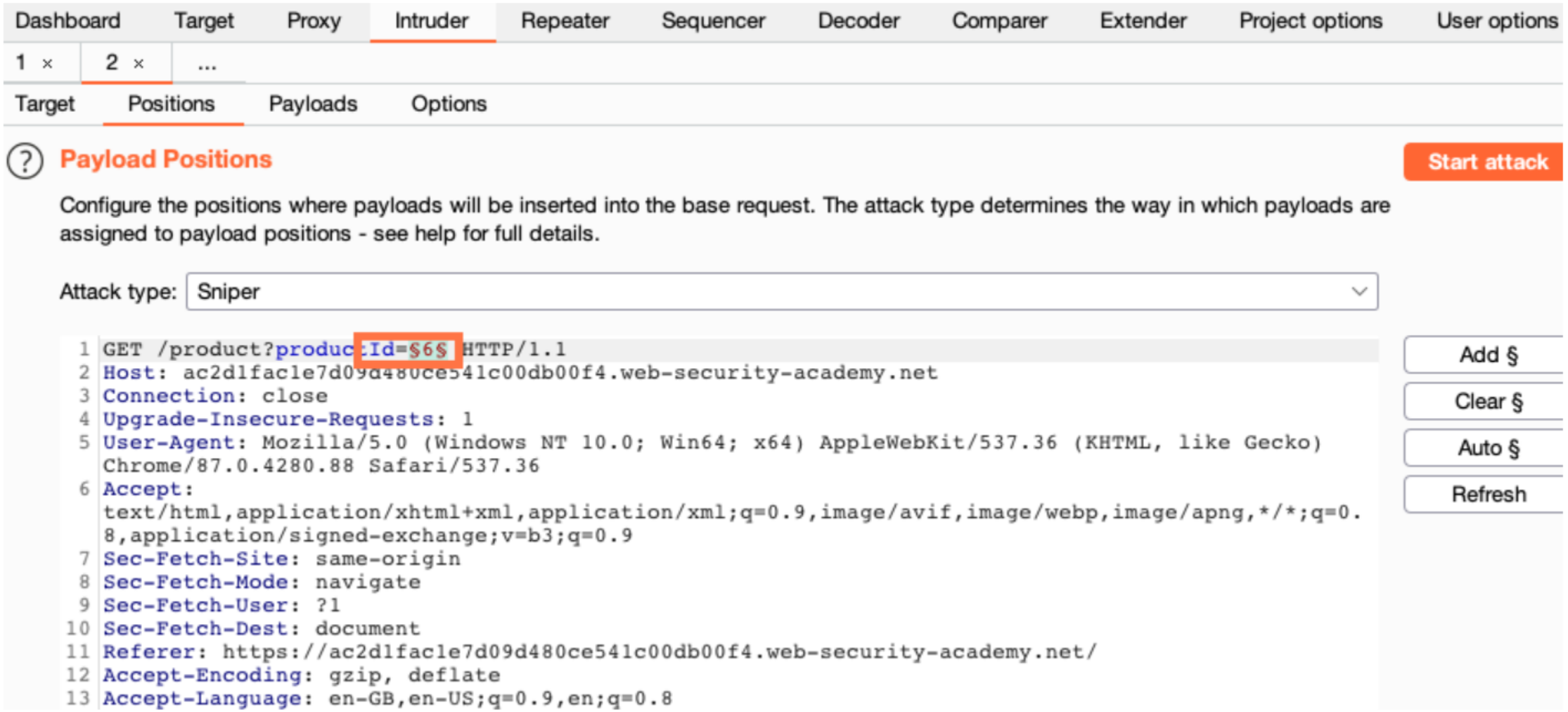
Mode: **In-session**

Duration: **5 minutes**

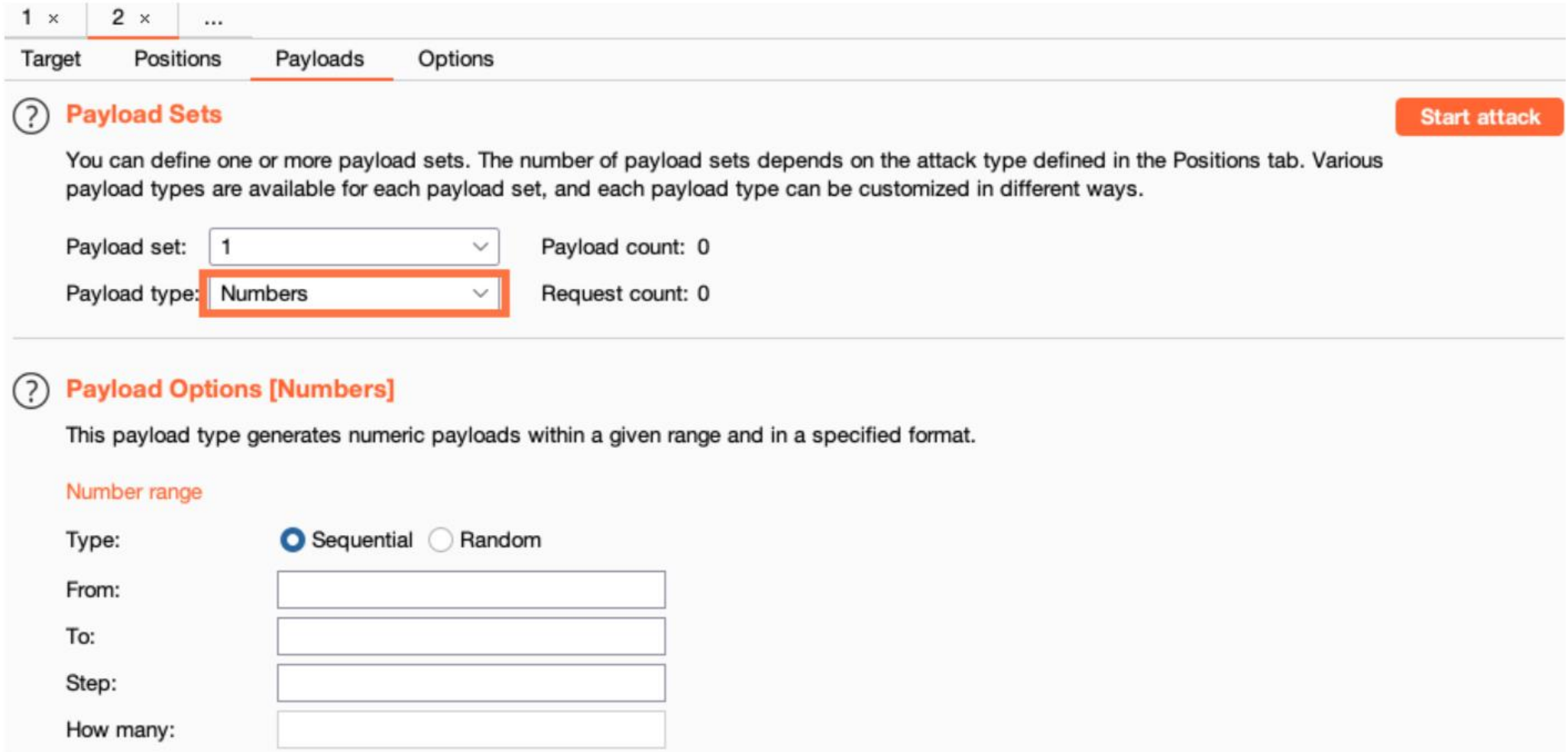
Materials Required: **None**

Explain Enumerating Identifiers

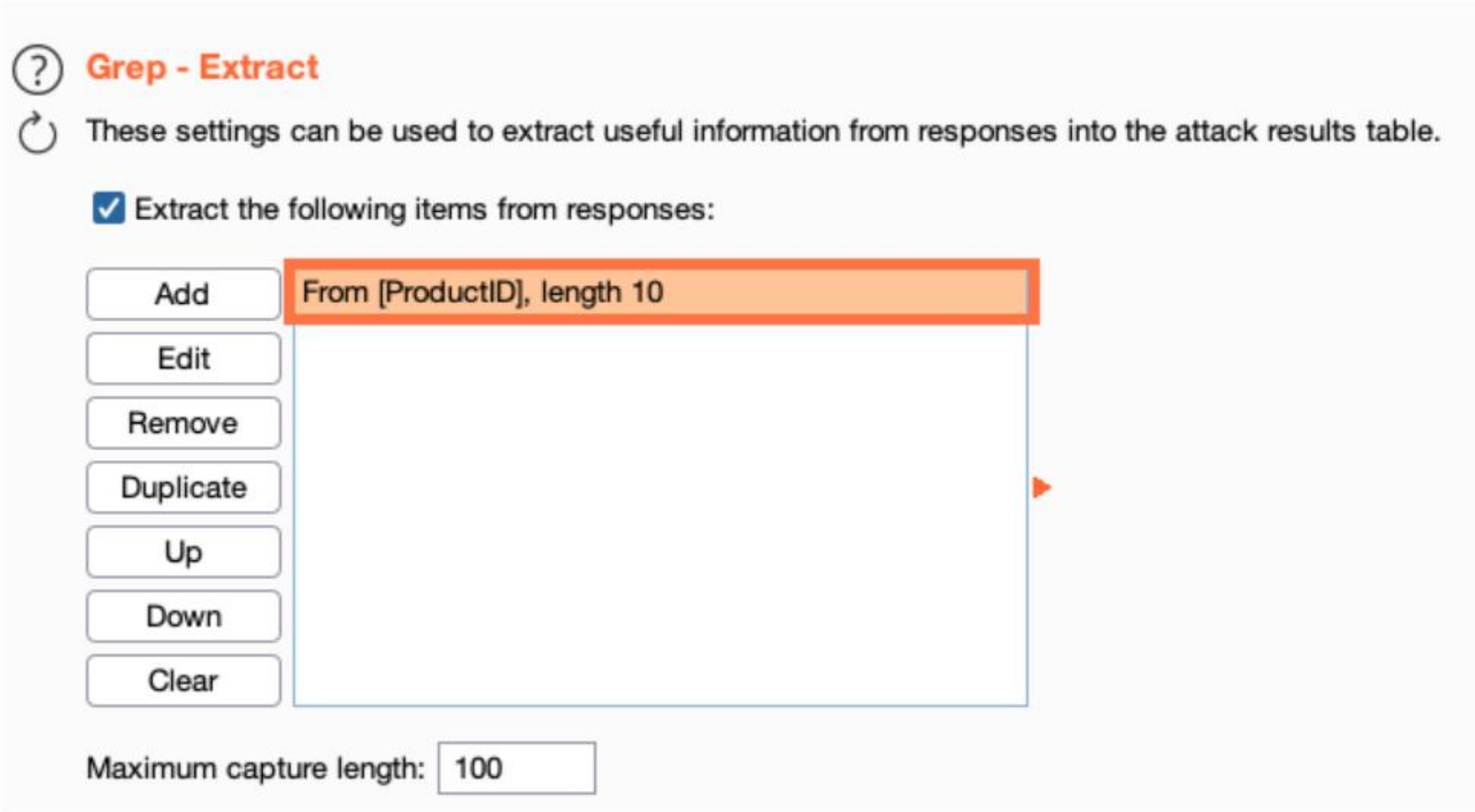
Harvesting Useful Data



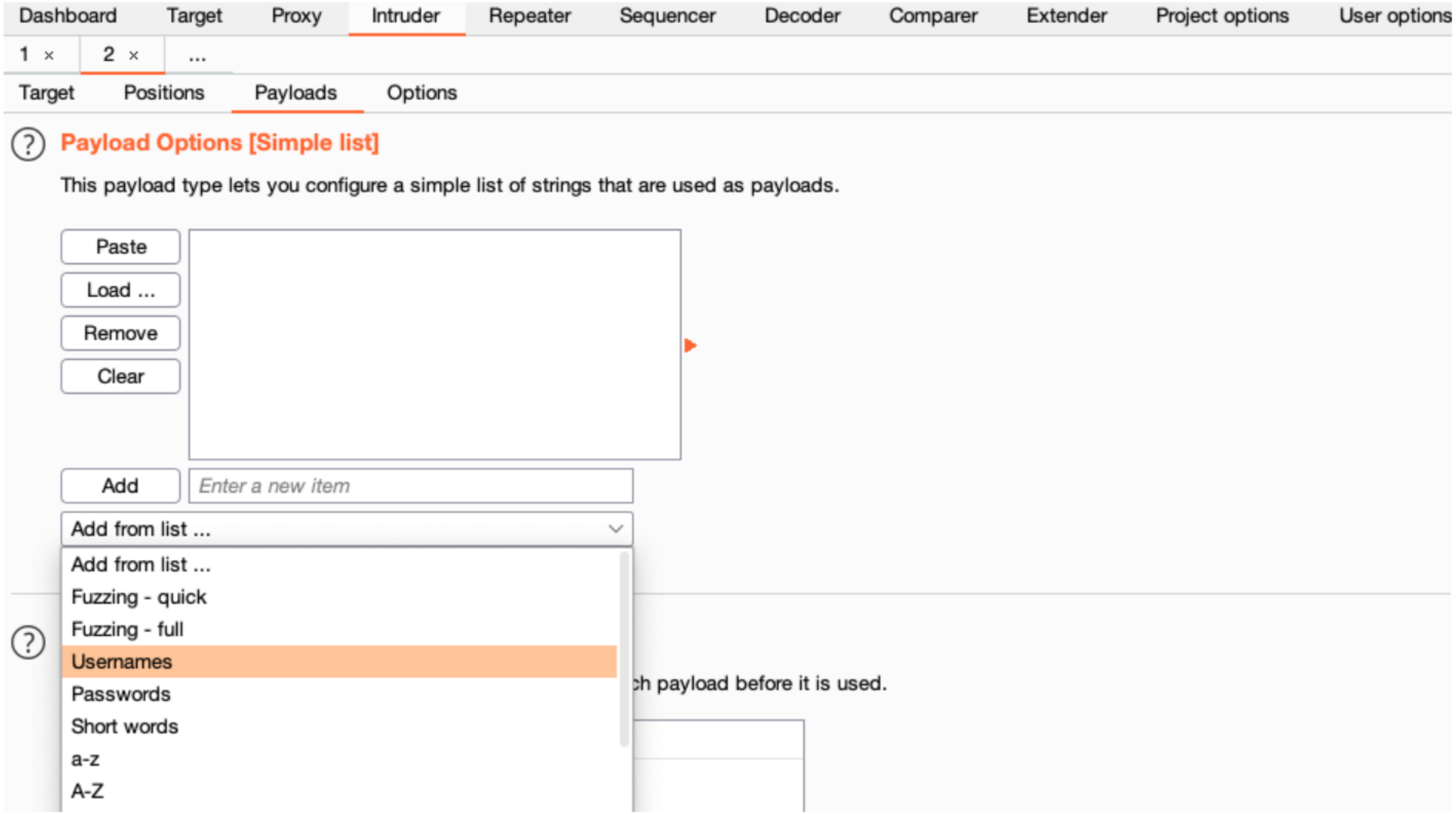
Harvesting Useful Data



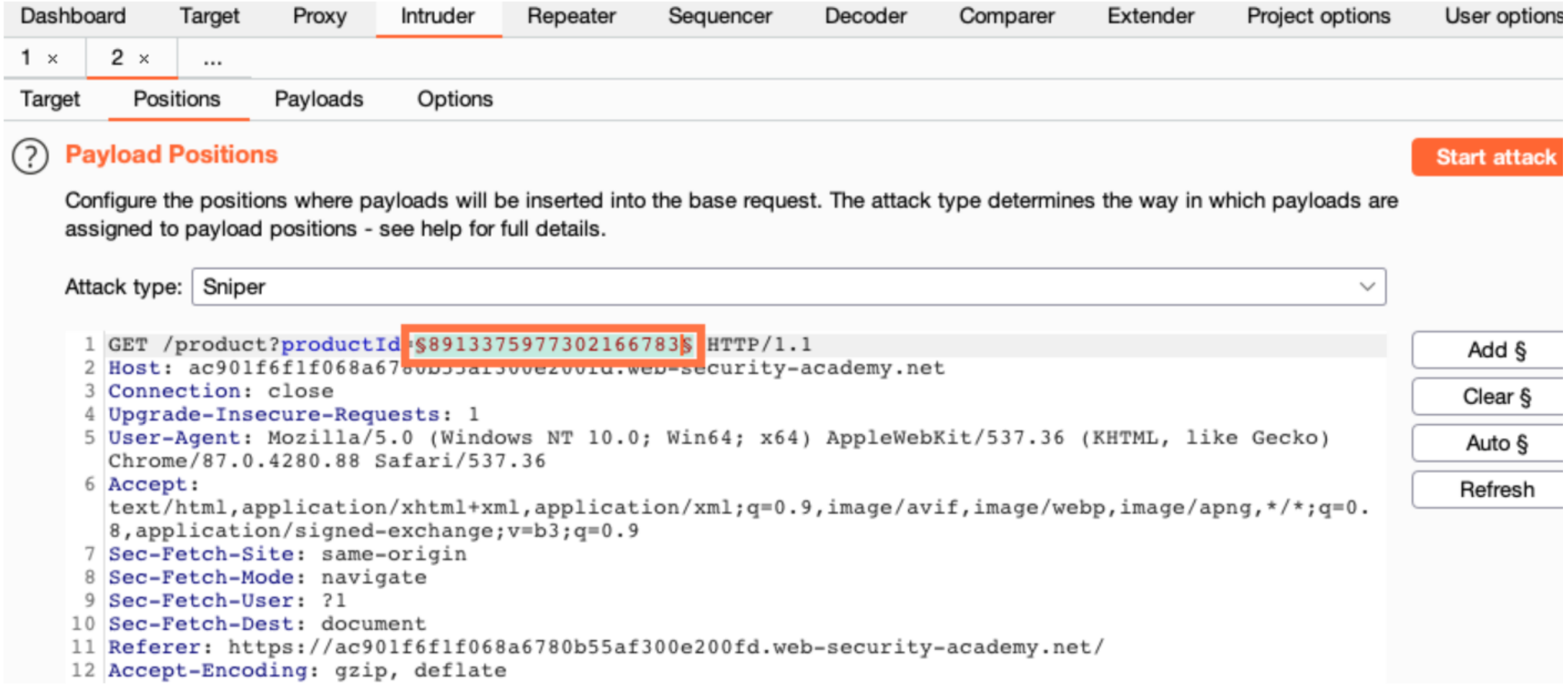
Harvesting Useful Data



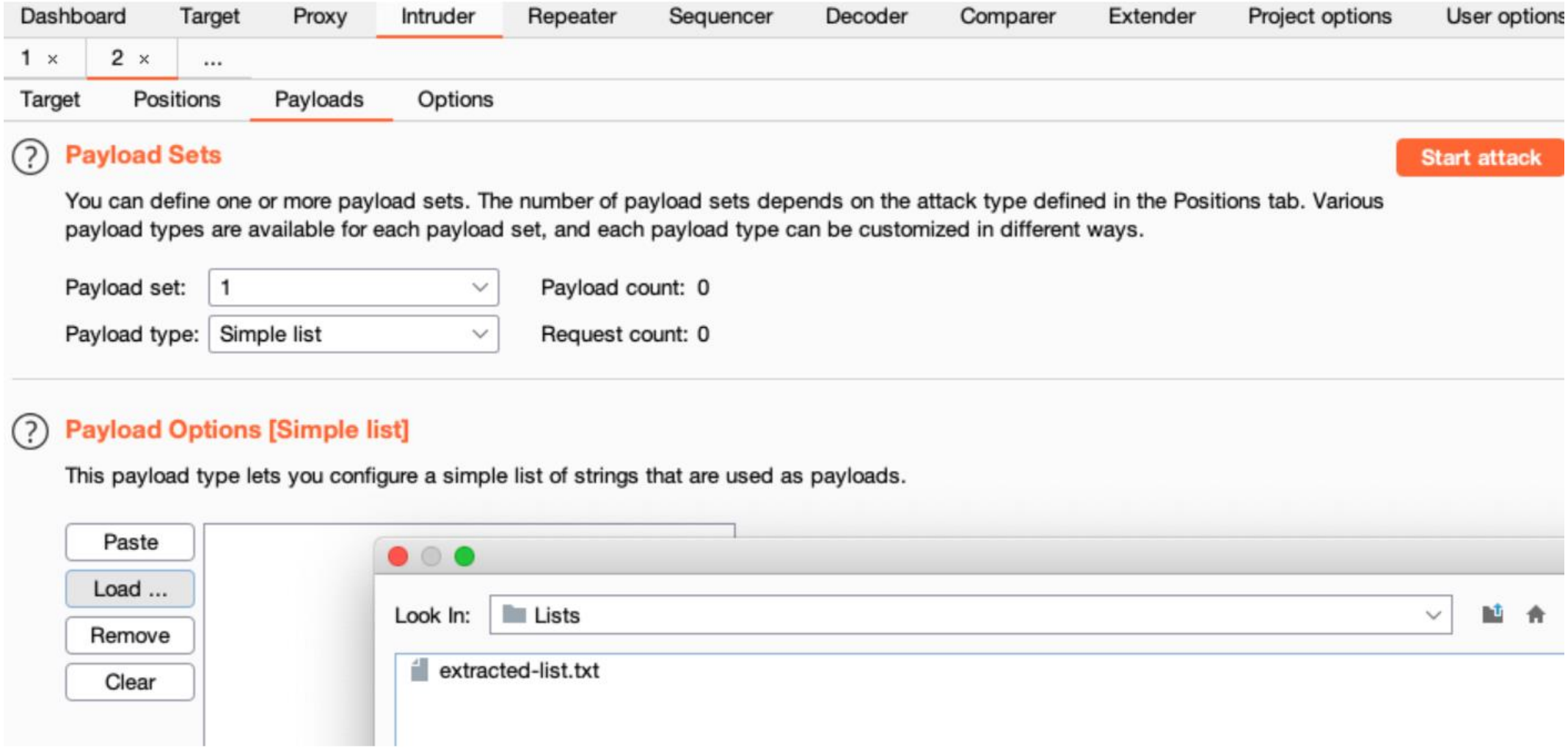
Harvesting Useful Data



Harvesting Useful Data



Harvesting Useful Data



Name of the Activity

Fastest Finger First

Instructions

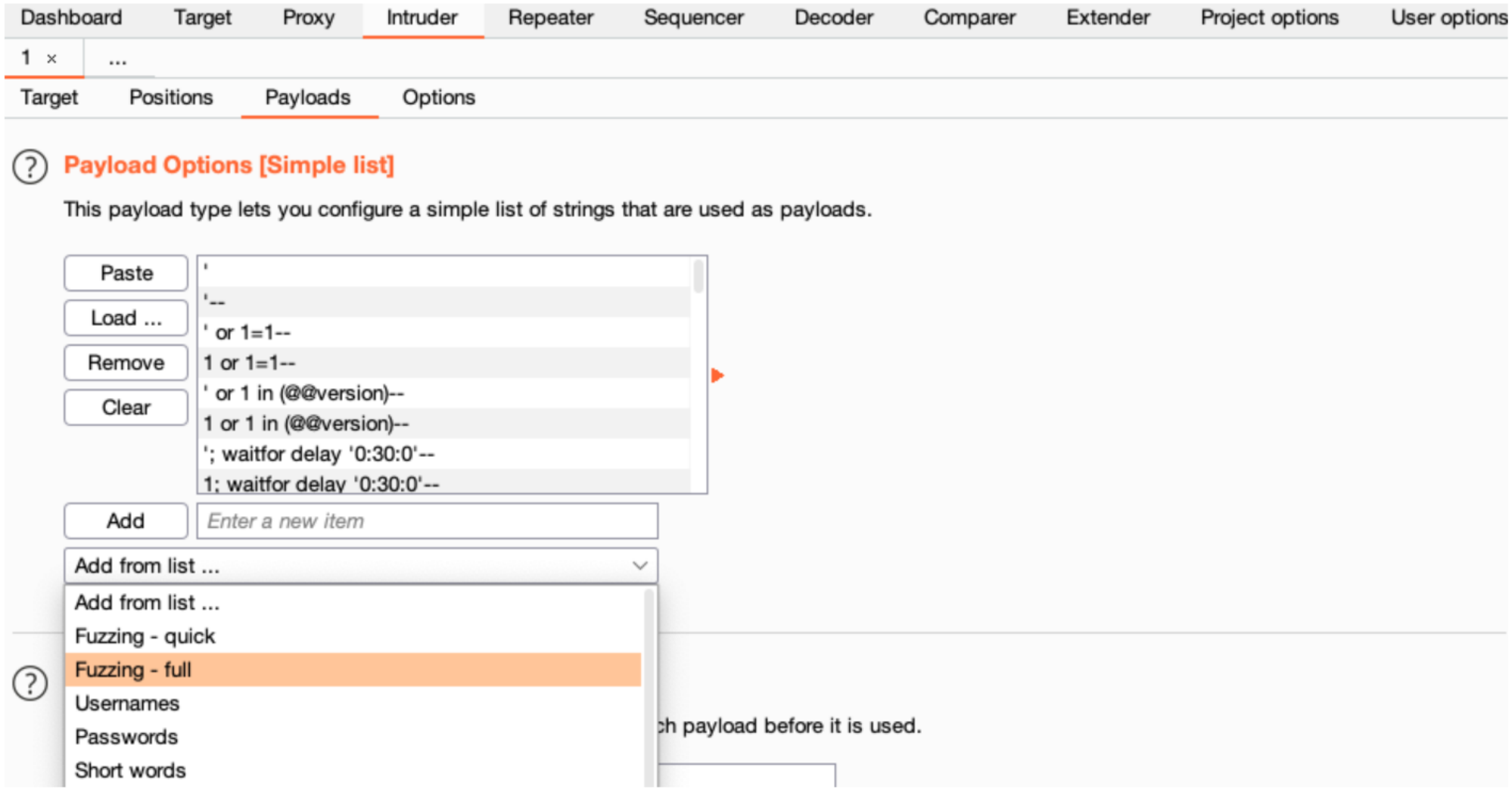
Mode: **In-session**

Duration: **5 minutes**

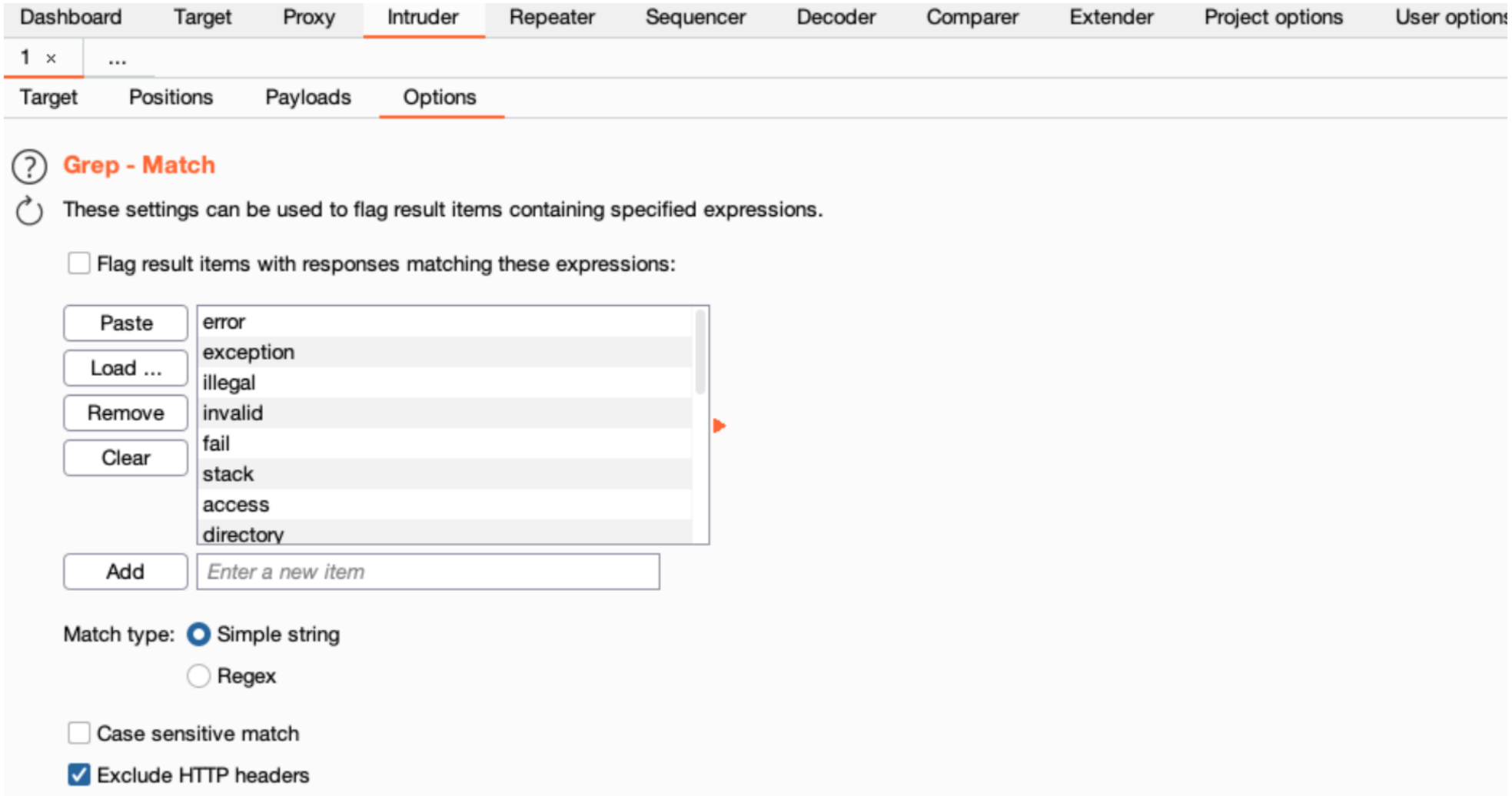
Materials Required: **None**

Explain Harvesting Useful Data

Fuzzing for Vulnerabilities



Fuzzing for Vulnerabilities



Fuzzing for Vulnerabilities

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
6	adm	200	☐	☐	3186	
0		200	☐	☐	3184	
1	root	200	☐	☐	3184	
2	admin	200	☐	☐	3184	
3	test	200	☐	☐	3184	
4	guest	200	☐	☐	3184	
5	info	200	☐	☐	3184	
7	mysql	200	☐	☐	3184	
8	user	200	☐	☐	3184	
9	administrator	200	☐	☐	3184	
10	oracle	200	☐	☐	3184	
11	ftp	200	☐	☐	3184	
12	pi	200	☐	☐	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

- 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

Loading Data into Decoder

- 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

Transformations

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

URL	HTML	Base64	ASCII hex
Hex	Octal	Binary	GZIP

Created by fae frey from Noun Project

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

Transformations

- 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

Work Manually

- 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

Smart Decoding

- 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**

Knowledge Check – Correct or Incorrect

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

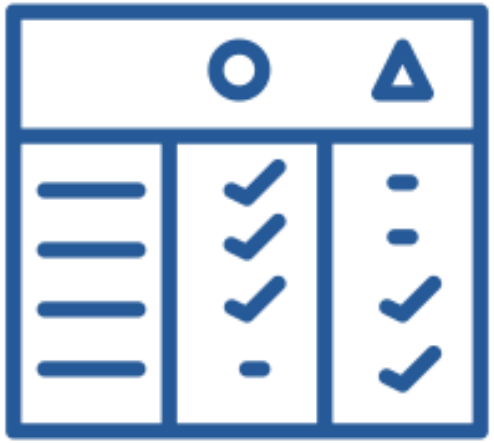
- Burp Comparer is a simple tool for performing a comparison (a visual "diff") between any two items of data
- Some common uses for Burp Comparer are as follows:

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

Loading Data into Comparer

You can load data into Comparer in the following ways:

- Paste it directly form 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

Performing Comparisons

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	Byte 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	• 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

Summary

In this session, you learnt about:

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

What Next?

In this topic, you will further learn about:

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

Source: Pixabay

TATA STRIVE | Right Skills Bright Future

Skill Development Initiative of Tata Trusts

- www.tatastrive.com -