

Burpsuite

Target: Mapeo del sitio

The screenshot shows the Burp Suite Community Edition v2023.9.3 interface. The 'Site map' tab is active, displaying a list of discovered URLs. The 'Request' tab is selected, showing the details of a GET request to the root of the target site.

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time request...
https://0a63007c0480b90d8287261000800c	GET	/		200	8098	HTML	SQL injection vulnerabil...		16:33:44 31 A...
https://0a7a04303023ad582085146009500	GET	/filter?category=Accesso...		200	4888	HTML	SQL injection vulnerabil...		16:31:10 31 A...
https://0a9001904b183bb8090e2f0082006	GET	/filter?category=Gifts		200	4888	HTML	SQL injection vulnerabil...		16:32:24 31 A...
https://accounts.google.com	GET	/product?productId=10		200	4035	HTML	SQL injection vulnerabil...		16:33:11 31 A...
https://adservice.google.com	GET	/product?productId=15		200	3959	HTML	SQL injection vulnerabil...		16:31:32 31 A...
https://analytics.google.com	GET	/product?productId=20		200	4362	HTML	SQL injection vulnerabil...		16:31:41 31 A...
https://analytics.ticketmaster.com.mx	GET	/resources/labheader/im...		200	707	XML			16:38:15 31 A...
https://apis.google.com	GET	/resources/labheader/js/...		200	175	script			16:38:15 31 A...
https://beacons.gcp.gvt2.com	GET	/academyLabHeader		504	309	HTML	Server Error: Gateway TL...		16:49:35 31 A...

The 'Request' tab shows the following details:

Request

1 GET / HTTP/2

2 Host: 0a63007c0480b90d8287261000800c.web-security-academy.net

3 Cookie: session=DCR84MY3Jkygv9rcBGXYNmcJvKNtqYNH

4 Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "Windows"

Response

1 HTTP/2 200 OK

2 Content-Type: text/html; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 8098

5

6 <!DOCTYPE html>

7 <html>

8 <head>

9 <link href=/resources/labheader/css/academyLabHeader.css rel=

Proxy: Intercepción de peticiones

The screenshot shows the Burp Suite Community Edition v2023.9.3 interface. The 'Proxy' tab is active, displaying a list of intercepted requests. The 'Request' tab is selected, showing the details of a GET request to the root of the target site.

Request to https://portswigger.net:443 [34.240.117.4]

Forward Drop Intercept is on Action Open browser

Comment this item HTTP/2

1 GET /web-security/sql-injection/lab-login-bypass HTTP/2

2 Host: portswigger.net

3 Cookie: AWSALBAPP-0=_remove_; AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_; AWSALBAPP-3=_remove_; stg_traffic_source_priority=4; Authenticated_UserVerificationId=5486F95B5C42FDEF0EC6FB7B23129999; t=LUKVryPZJtZrQJYLjG1Gyw%3D%3D; __stripe_mid=d34035c4-0b63-4cd3-90b2-576247ac712fbb0d63; stg_externalReferrer=https://0a63007c0480b90d828726100080080c.web-security-academy.net/; SessionId=CfDj8I8mhUzb%2F5xBAi3J%2BxXV0heex7WsBIdZsBAusRIP%2BZE0dXbu%2Box54Tv0tR3RkV0pnEG4%2B404NUP6PAC8K6uWxY5SoV2aL0yxMz04X61cxaLD2bm8XvyL0c7NLqDClnZiXyW1b0RRgKpeYfICiBet9xa9IU3tjuk3CixuKzwa1Sx3; __pk_ses.287552c2-4917-42e0-8982-ba994a2a73d7.1467=*; __pk_id.287552c2-4917-42e0-8982-ba994a2a73d7.1467=497eab2199521786.1693519011.2.1693523365.1693523359.; stg_last_interaction=Thu%2C%2031%20Aug%202023%2023:36:26%20GMT; stg_returning_visitor=Thu%2C%2031%20Aug%202023%2023:36:26%20GMT

4 Cache-Control: max-age=0

5 Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"

6 Sec-Ch-Ua-Mobile: ?0

7 Sec-Ch-Ua-Platform: "Windows"

8 Upgrade-Insecure-Requests: 1

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/

Repeater: Copiar una intercepción y probarla.

The screenshot shows the Burp Suite Repeater tab. The Request pane displays a GET request to `/filter?category=Gifts'or 1=1--` with various headers including `Host: 0a63007c0480b90d828726100008008c.web-security-academy.net`, `Cookie: session=DCR84MY3Jkygv9rcBGXYNmcJvKNtqYNH`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36`. The Response pane shows an HTTP 200 OK response with headers `Content-Type: text/html; charset=utf-8` and `Content-Length: 13510`. The body contains HTML code with a link to `/resources/labheader/css/academyLabHeader.css` and a title `SQL injection vulnerability in WHERE clause allowing retrieval of hidden data`. The Inspector pane on the right shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.

Intruder: Ataques de fuerza bruta.

The screenshot shows the Burp Suite Intruder tab. The Payload sets section allows defining one or more payload sets. The first set is named '1' and has a 'Simple list' type. The 'Payload set' dropdown is open, showing options like 'Simple list', 'Runtime file', 'Custom iterator', 'Character substitution', 'Case modification', 'Recursive grep', 'Illegal Unicode', 'Character blocks', 'Numbers', 'Dates', 'Brute forcer', 'Null payloads', 'Character frotter', 'Bit flipper', and 'Username generator'. The 'Add' button is visible. The Payload processing section allows defining rules to perform various processing tasks on each payload before it is used. The 'Add' button is visible.