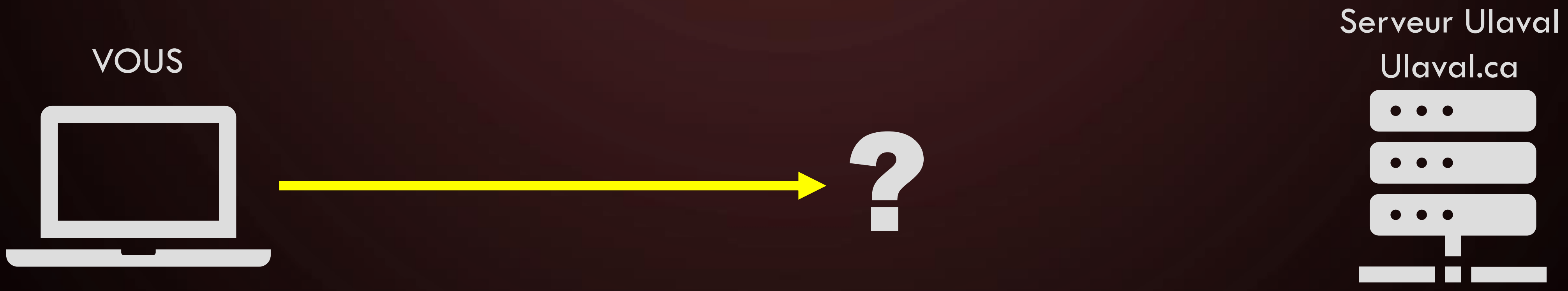
Introduction aux attaques web

CLUB DE SÉCURITÉ INFORMATIQUE (CSIUL)
Automne 2024

Jean-Nicolas Turbis [myDonut]

QU'EST-CE QUE LE WEB?



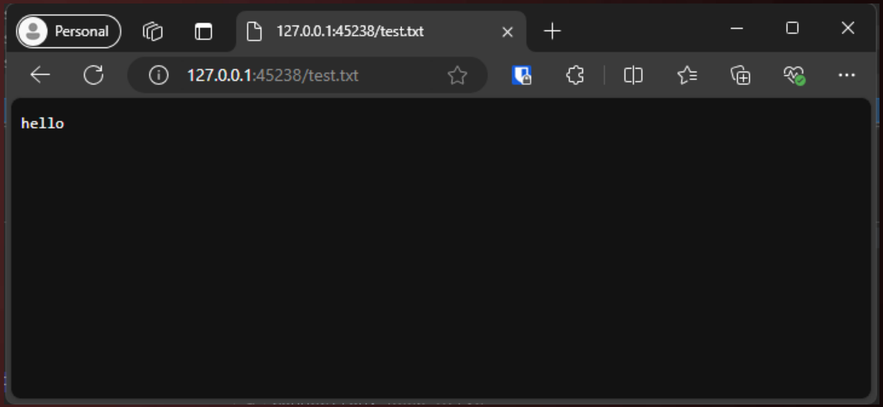
VOUS

?

Serveur Ulaval

Ulaval.ca

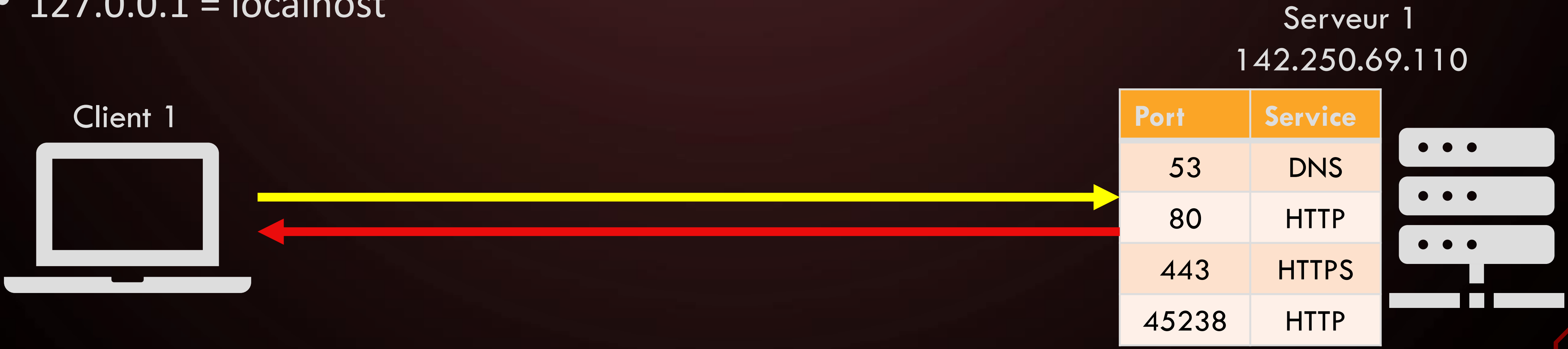
ADRESSE IP ET PORT?



127.0.0.1:45238/test.txt

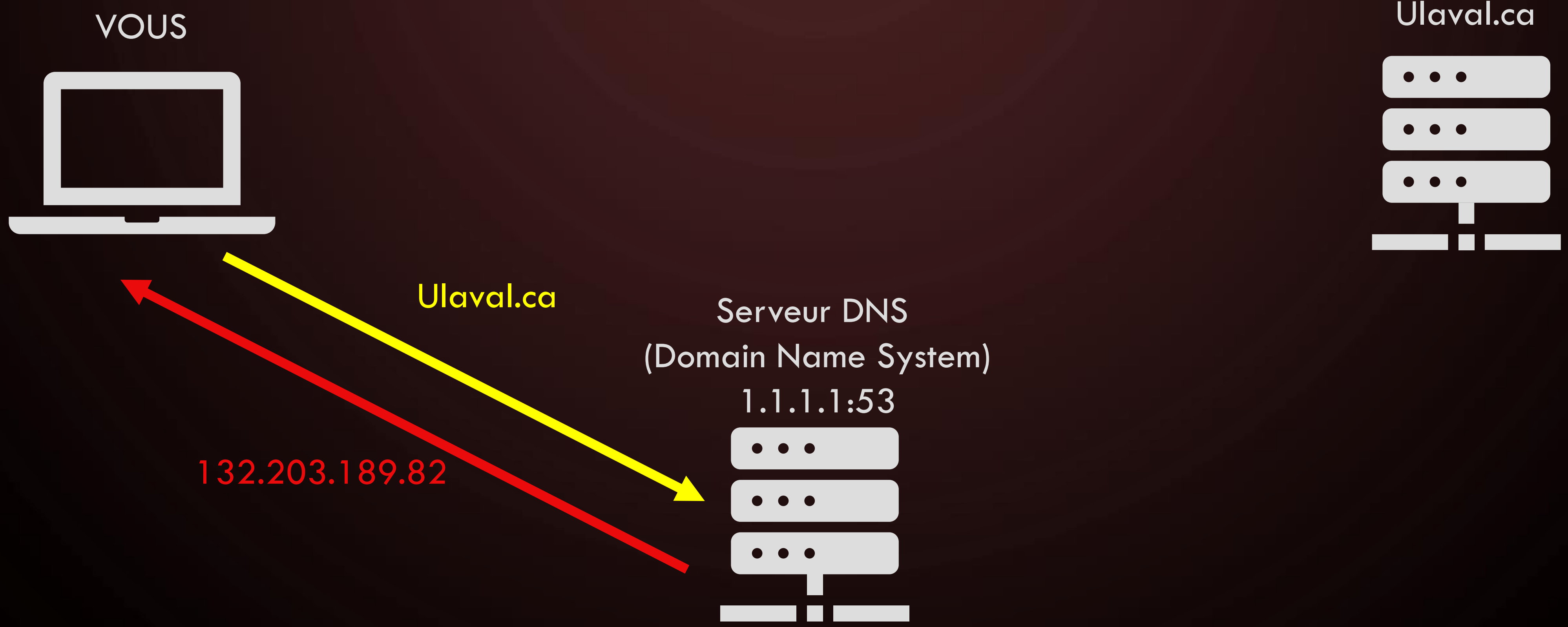
```
hello
```

- IP: 0.0.0.0 à 255.255.255.255
- Port : 0-65535
- 127.0.0.1 = localhost



Port	Service
53	DNS
80	HTTP
443	HTTPS
45238	HTTP

OÙ EST ULAVAL?



VOUS

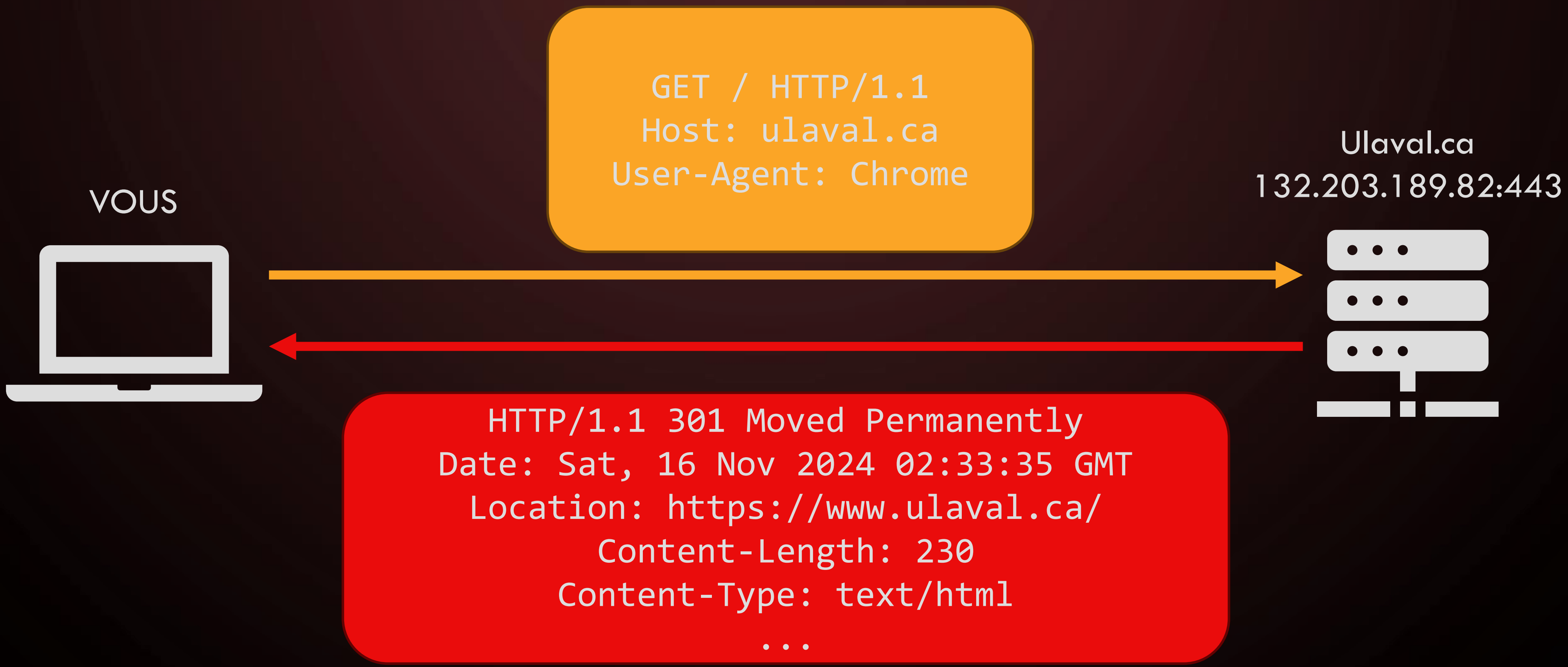
Ulaval.ca

Ulaval.ca

Serveur DNS
(Domain Name System)
1.1.1.1:53

132.203.189.82

PROTOCOLE HTTP



```
GET / HTTP/1.1
Host: ulaval.ca
User-Agent: Chrome
```

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 16 Nov 2024 02:33:35 GMT
Location: https://www.ulaval.ca/
Content-Length: 230
Content-Type: text/html
...
```

VERBES HTTP

```
GET / HTTP/1.1
Host: ulaval.ca
User-Agent: Chrome
```

GET

HEAD

POST

PUT

DELETE

USER-AGENT

```
GET / HTTP/1.1
Host: ulaval.ca
User-Agent: Chrome
```

User-Agent: <product> / <product-version> <comment>

- curl/8.9.1

User-Agent: Mozilla/5.0 (<system-information>) <platform> (<platform-details>) <extensions>

- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
- Mozilla/5.0 (iPhone; CPU iPhone OS 16_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.5 Mobile/15E148 Safari/604.1
- Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

CODE DE RÉPONSE HTTP

```
HTTP/1.1 301 Moved Permanently
Date: Sat, 16 Nov 2024 02:33:35 GMT
Location: https://www.ulaval.ca/
Content-Length: 230
Content-Type: text/html
...
```

Succès

- 200 – OK
- 201 – Created

Redirection

- 301 – Moved Permanently
- 302 – Found

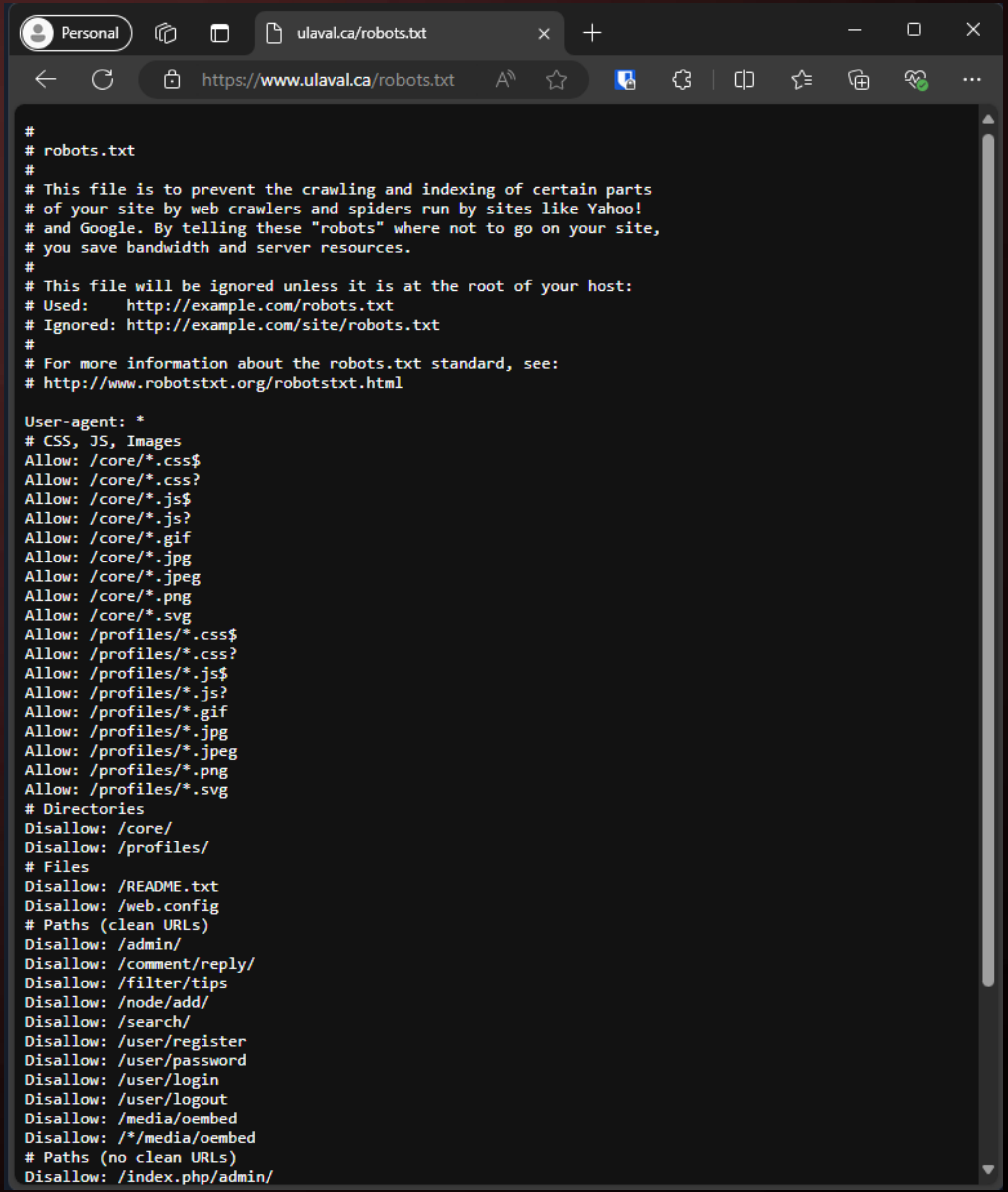
Erreur Client

- 400 – Bad Request
- 401 – Unauthorized
- 404 – Not found
- 418 – I’m a teapot

Erreur Serveur

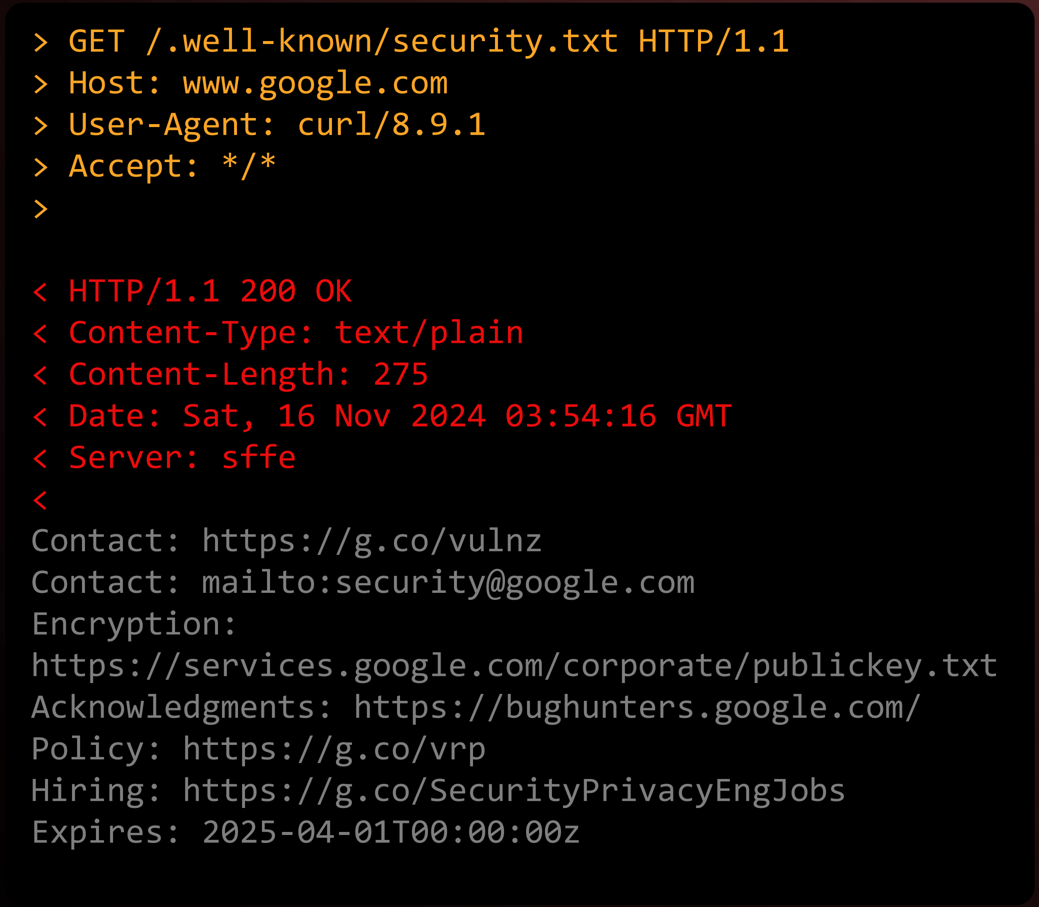
- 500 – Internal Server Error
- 503 – Service Unavailable

/ROBOTS.TXT

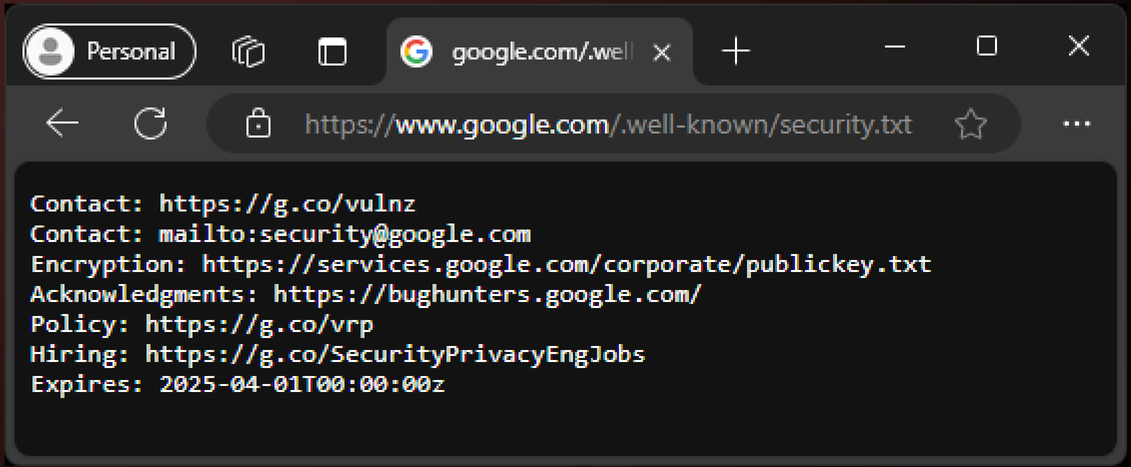


```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
# CSS, JS, Images
Allow: /core/*.css$
Allow: /core/*.css?
Allow: /core/*.js$
Allow: /core/*.js?
Allow: /core/*.gif
Allow: /core/*.jpg
Allow: /core/*.jpeg
Allow: /core/*.png
Allow: /core/*.svg
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /profiles/*.svg
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.txt
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register
Disallow: /user/password
Disallow: /user/login
Disallow: /user/logout
Disallow: /media/oembed
Disallow: /*/media/oembed
# Paths (no clean URLs)
Disallow: /index.php/admin/
```

/.WELL-KNOWN/SECURITY.TXT

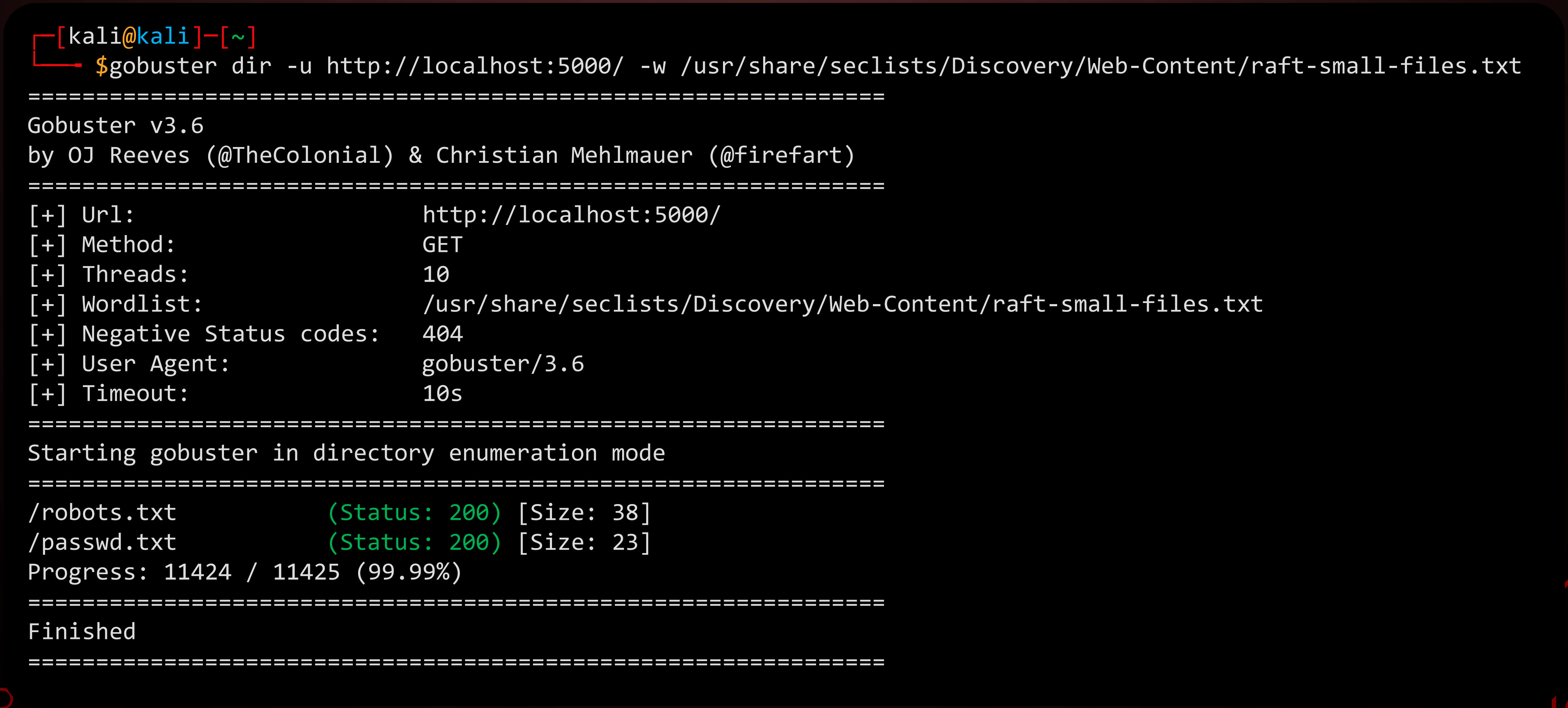


```
> GET /.well-known/security.txt HTTP/1.1
> Host: www.google.com
> User-Agent: curl/8.9.1
> Accept: */*
>

< HTTP/1.1 200 OK
< Content-Type: text/plain
< Content-Length: 275
< Date: Sat, 16 Nov 2024 03:54:16 GMT
< Server: sffe
<
Contact: https://g.co/vulnz
Contact: mailto:security@google.com
Encryption:
https://services.google.com/corporate/publickey.txt
Acknowledgments: https://bughunters.google.com/
Policy: https://g.co/vrp
Hiring: https://g.co/SecurityPrivacyEngJobs
Expires: 2025-04-01T00:00:00z
```



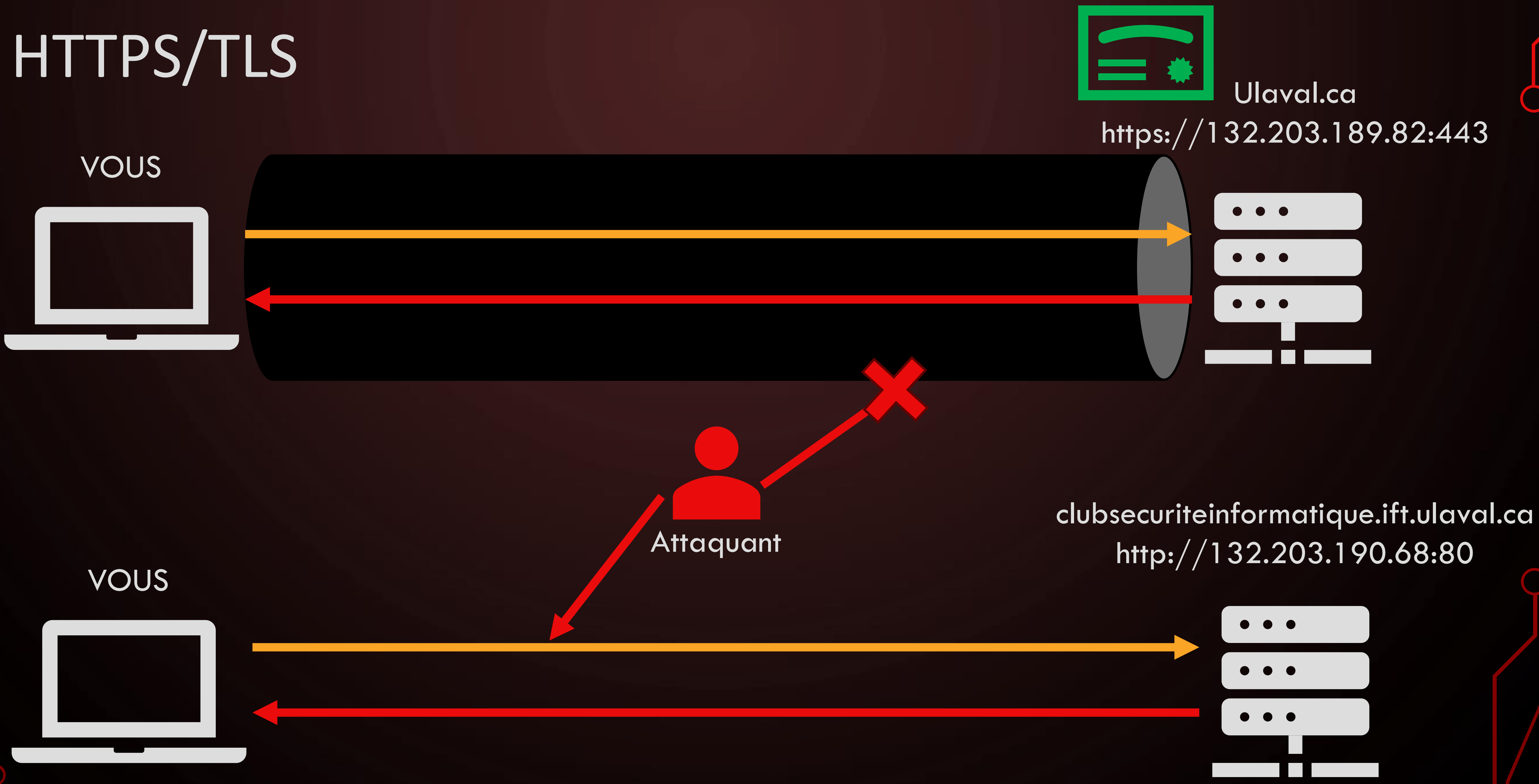
```
Contact: https://g.co/vulnz
Contact: mailto:security@google.com
Encryption: https://services.google.com/corporate/publickey.txt
Acknowledgments: https://bughunters.google.com/
Policy: https://g.co/vrp
Hiring: https://g.co/SecurityPrivacyEngJobs
Expires: 2025-04-01T00:00:00z
```

DIRBUSTING



```
┌─[kali@kali]─[~]
└──╼ $gobuster dir -u http://localhost:5000/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://localhost:5000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/robots.txt           (Status: 200) [Size: 38]
/passwd.txt           (Status: 200) [Size: 23]
Progress: 11424 / 11425 (99.99%)
===============================================================
Finished
===============================================================
```

HTTPS/TLS



VOUS

Ulaval.ca

https://132.203.189.82:443

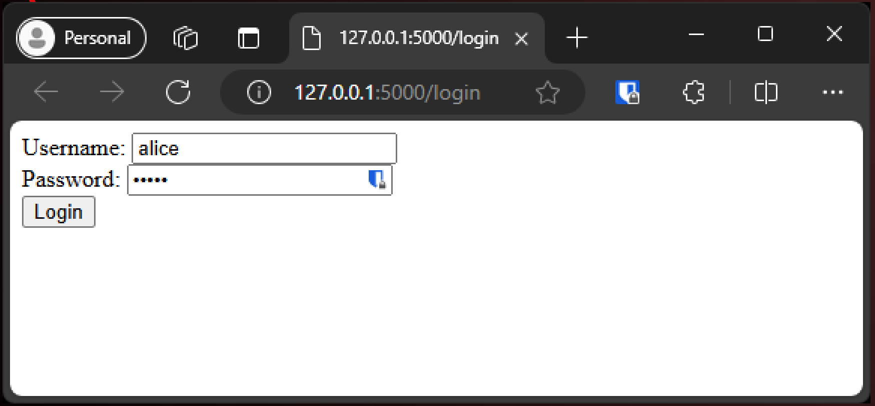
Attaquant

VOUS

clubsecuriteinformatique.ift.ulaval.ca

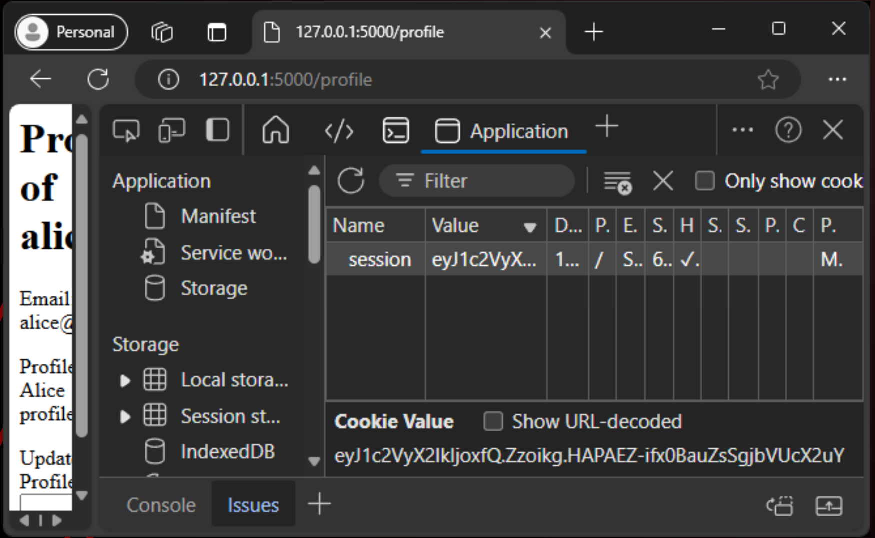
http://132.203.190.68:80

COOKIE



Username: alice
Password: •••••
Login

F12



Name	Value	D...	P.	E.	S.	H	S.	S.	P.	C	P.
session	eyJ1c2VyX...	1...	/	S..	6..	✓.					M.

Cookie Value □ Show URL-decoded

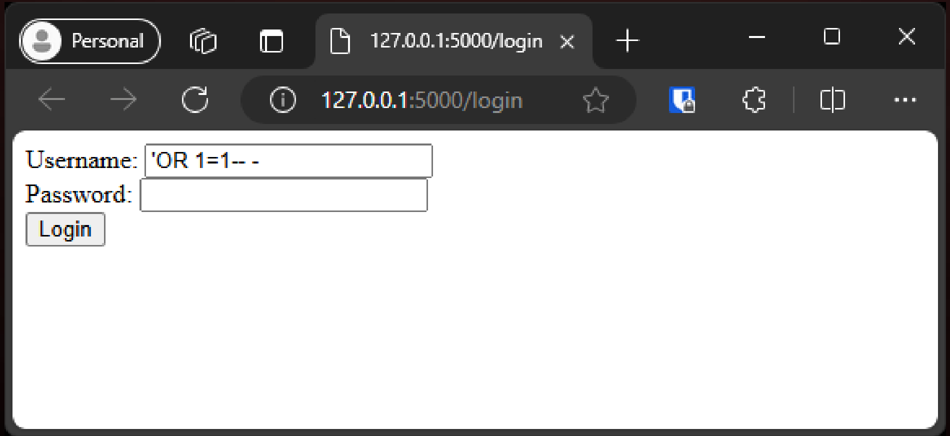
eyJ1c2VyX2lkIjoxfQ.Zzoikg.HAPAEZ-ifx0BauZsSgjbVUcX2uY

```
> POST /login HTTP/1.1
> Host: 127.0.0.1:5000
> User-Agent: curl/8.9.1
> Content-Length: 36
> Content-Type: application/x-www-form-urlencoded
>
username=alice&password=alice
< HTTP/1.1 302 FOUND
< Server: Werkzeug/3.1.3 Python/3.11.9
< Date: Sun, 17 Nov 2024 16:44:36 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 203
< Location: /profile
< Set-Cookie:
session=eyJ1c2VyX2lkIjoxfQ.ZzoddA.jMFLLFn9Xzz5Dk54koEPmvjUR08;
HttpOnly; Path=/
< Connection: close
<
<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a
href="/profile">/profile</a>. If not, click the link.
```

INJECTION SQL

```
# Requête normal
SELECT * FROM users WHERE username = 'alice' AND password = 'motdepassealice'
# Requête malicieuse
SELECT * FROM users WHERE username = 'alice'-- - ' AND password = 'motdepassealice'
SELECT * FROM users WHERE username = ' 'OR 1=1-- - ' AND password = 'motdepassealice'
```

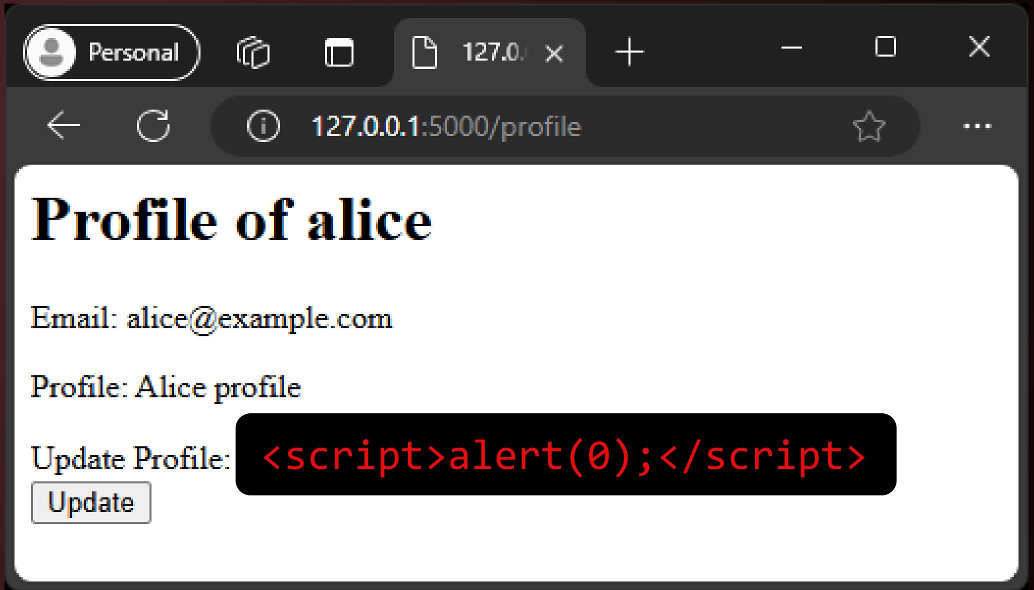
```
# app.py - ligne 56
query = f"SELECT * FROM users WHERE username = '{username}' AND password = '{password}'"
cursor.execute(query)
user = cursor.fetchone()
```



Username: 'OR 1=1-- -
Password:

XSS (CROSS-SITE SCRIPTING)

```
return render_template_string("""
   <h1>Profile of {{ user[1] }}</h1>
   <p>Email: {{ user[3] }}</p>
   <p>Profile: {{ user[4]|safe }}</p>
   <form method="POST">
      Update Profile: <input type="text"
name="profile"><br>
      <input type="submit" value="Update">
   </form>
""", user=user)
```

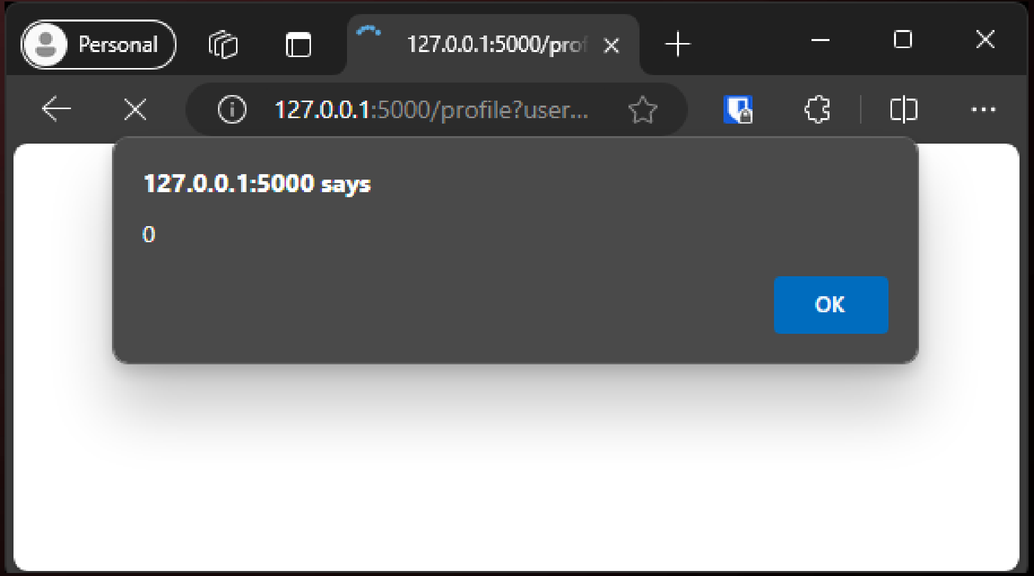


Profile of alice

Email: alice@example.com

Profile: Alice profile

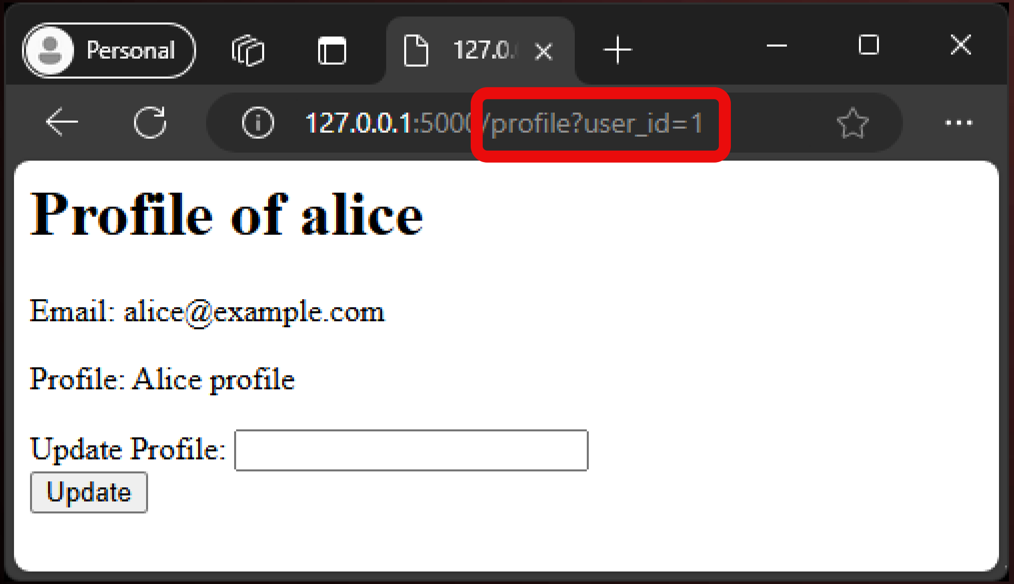
Update Profile: <script>alert(0);</script>



127.0.0.1:5000 says

0

IDOR (INSECURE DIRECT OBJECT REFERENCES)

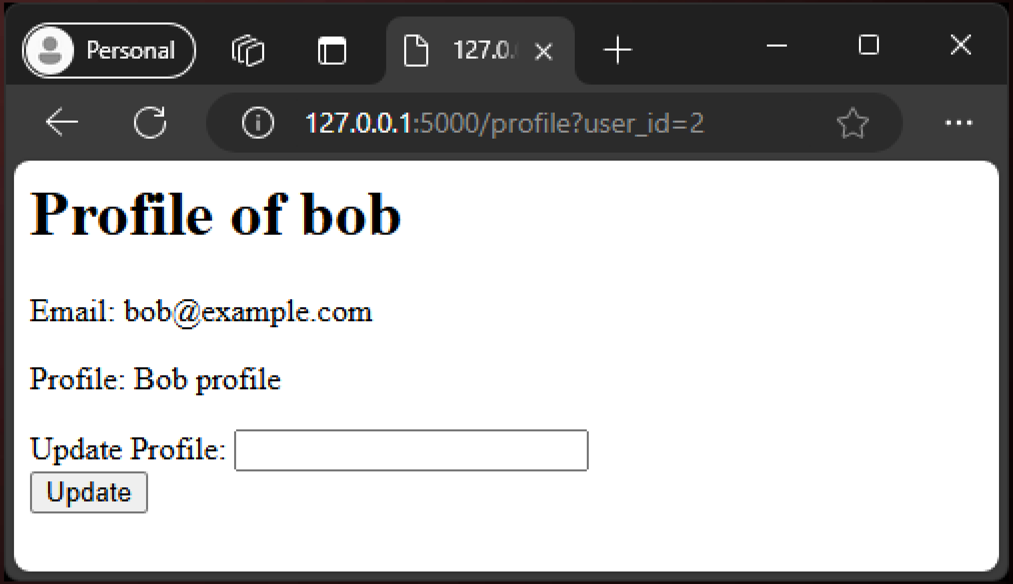


Profile of alice

Email: alice@example.com

Profile: Alice profile

Update Profile:



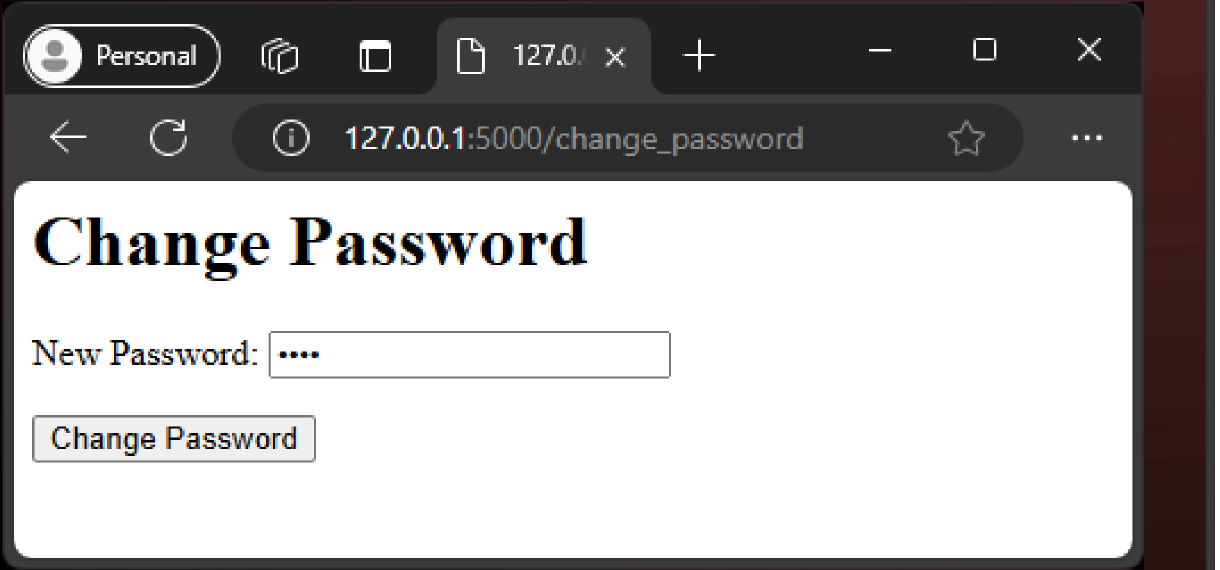
Profile of bob

Email: bob@example.com

Profile: Bob profile

Update Profile:

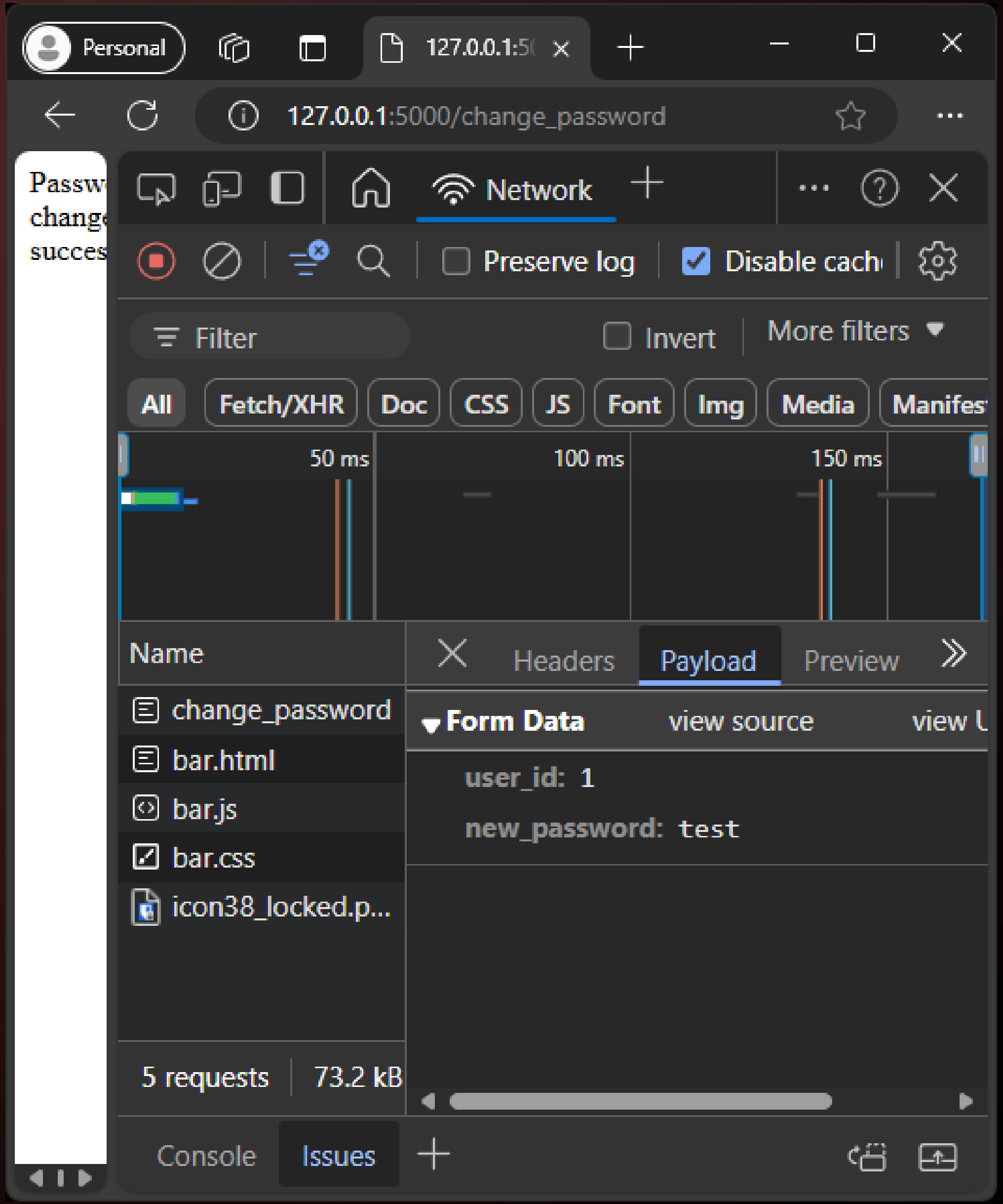
ATO (ACCOUNT TAKEOVER)



127.0.0.1:5000/change_password

Change Password

New Password: ••••



127.0.0.1:5000/change_password

Passw
chang
succes

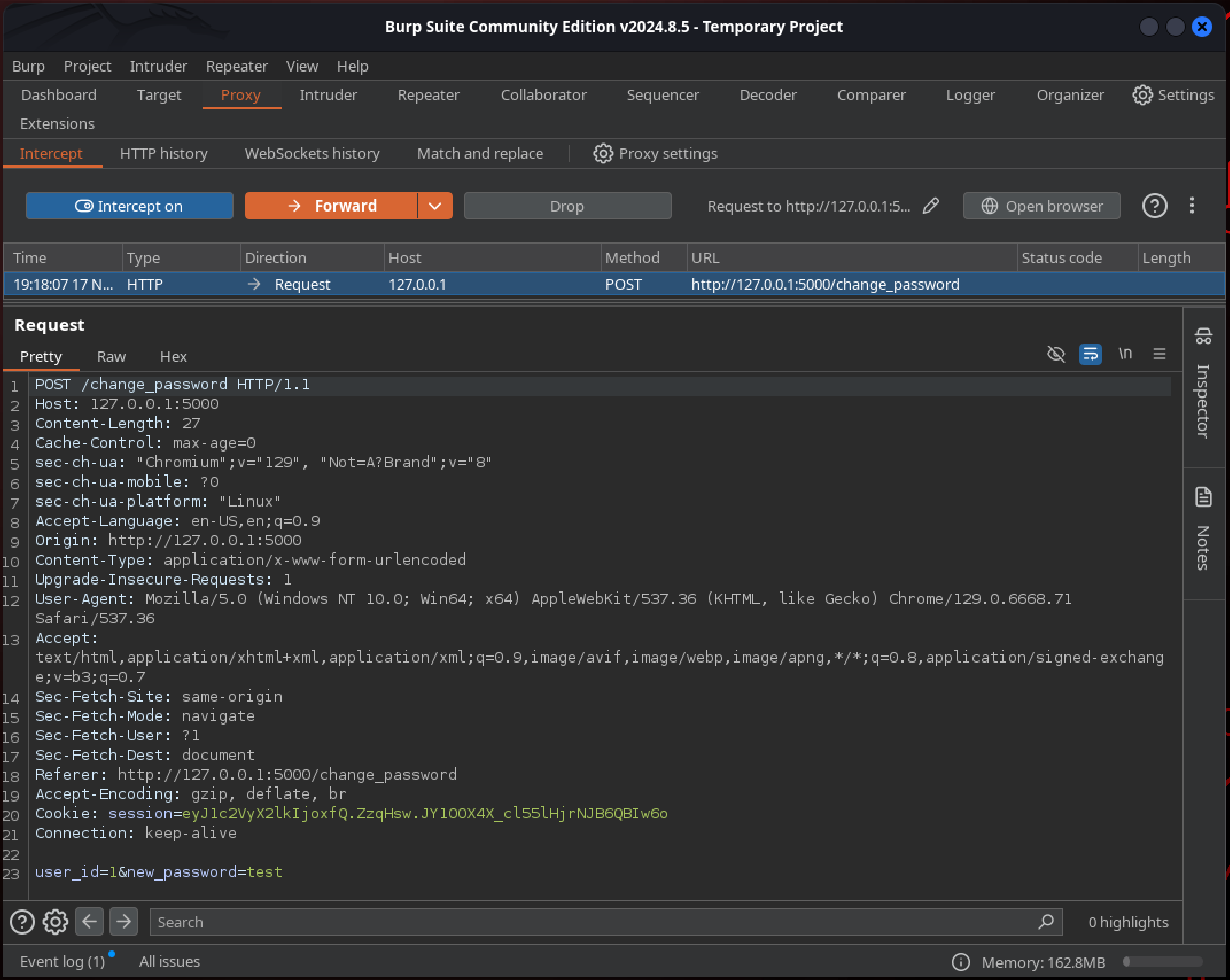
Form Data

user_id: 1
new_password: test

Name
change_password
bar.html
bar.js
bar.css
icon38_locked.p...

5 requests 73.2 kB

BURP SUITE


Burp Suite Community Edition v2024.8.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://127.0.0.1:5...
Open browser
Request
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues
Memory: 162.8MB

Time	Type	Direction	Host	Method	URL	Status code	Length
19:18:07 17 N...	HTTP	→ Request	127.0.0.1	POST	http://127.0.0.1:5000/change_password		

```
POST /change_password HTTP/1.1
Host: 127.0.0.1:5000
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:5000/change_password
Accept-Encoding: gzip, deflate, br
Cookie: session=eyJ1c2VyX2lkIjoxfQ.ZzqHsw.JY1OOX4X_cl55lHjrNJB6QBIw6o
Connection: keep-alive

user_id=1&new_password=test
```

ALLEZ PLUS LOIN

https://github.com/csiul/Formations-A2024/

https://owasp-juice.shop/

https://www.root-me.org/

https://tryhackme.com/

https://www.hackthebox.com/