

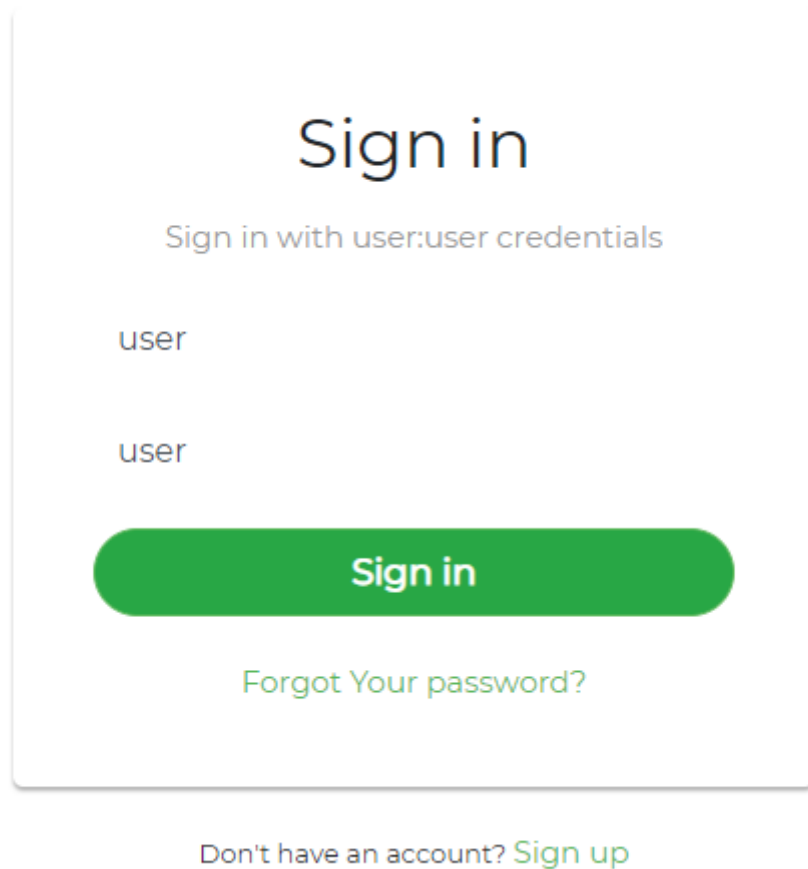
Union Based SQLi Report - 17.6.3 - 17

Tester's name: Stanley Ford

Lab 17.6.3 "Union Based SQLi":

- General information:
 - Testing period: 15.02.2023
 - Test object: <http://51.250.73.193:5009/>
- Description of actions:

After clicking on the site, I roughly figured out its functionality, what redirects where. Next, I additionally looked and inspected the code of the page, where I did not find anything.



The image shows a web form for signing in. At the top, the text "Sign in" is displayed in a large, dark font. Below it, a smaller line of text reads "Sign in with user:user credentials". There are two input fields, both containing the text "user". Below the input fields is a prominent green button with the text "Sign in" in white. Underneath the button is a link that says "Forgot Your password?". At the bottom of the form, there is a link that says "Don't have an account? Sign up".

So, the start page with authorization offers to log in as user:user, which I did.

SALE

New Arrivals Collection 2019

Categories

[All](#)
[Women](#)
[Men](#)
[Accessories](#)

Filters

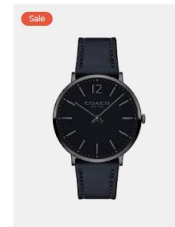
Price

Range: \$50 - \$200

Color

Search Products...

Showing 10 results

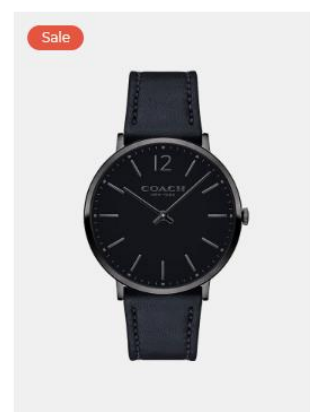
Herschel supply co 25l
\$75.00Denim jacket blue
\$92.50Coach slim easton black
~~\$165.90~~ \$120.30

There is a search form on the site, the first possible entry point. You can try to type something like HTML injection `<alert>` but it didn't lead to anything. It just gave away that no such items were found. You can try SQL injection by inserting something in quotation marks into the form, thus trying to go beyond them. I typed in 'hahaha' (with brackets) for the test and it didn't lead to anything either. I tried it with double brackets ("hahaha") and that's it resulted in a 500 Internal Server Error, which may mean that this type of request was processed failed.

I'll introduce a simple SQL injection of the form: `" or 1=1 --` which should return TRUE, because 1 always equals 1.

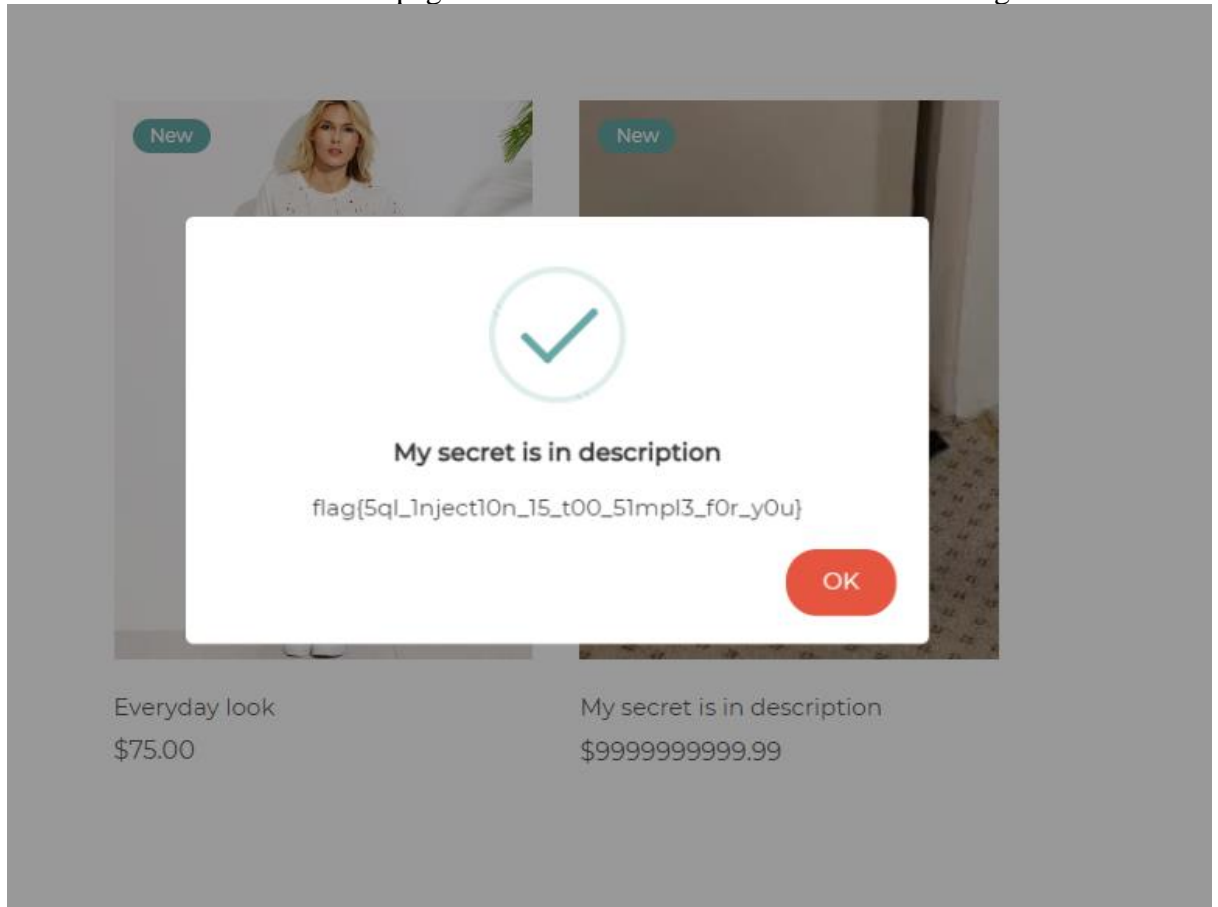
`" or 1=1 --`

Showing 11 results

Herschel supply co 25l
\$75.00Denim jacket blue
\$92.50Coach slim easton black
~~\$165.90~~ \$120.30

Now 11 items are displayed, although there were 10.

I scrolled to the bottom of the page and saw this "secret" element with the flag:



Lab Done!

Self-Assessment Questions:

- List the tools (programs and utilities) you used to solve this lab: Web browser (Google Chrome);
- List the vulnerabilities you discovered: Union Based SQL Injection
- Give advice on how to improve security:

Check forms for the ability to enter special characters such as quotation marks, equal signs, and various parentheses. This should not be the case.