IT - Security, Mandatory II

Rasmus Carlsen, Lucas Modin

November 2025

Problem 1: SQL Injection (Software Security)

SQLI are a way to insert malicious query code in a input field in apps, so one can manipulate the app to show the data in the database or altering the database, eg. deleting the whole database or rows/columns, adversaries would maybe have some reason for altering. In the Portswigger.net under the learning path for academy and in the sql path, we can find information on the sql injection attacks. Here labs are provided for exercising sql attacks.

A Using the 'Union select NULL...' command

To use the

```
UNION SELECT NULL, NULL, NULL;
```

sql attack, we need to use the websites url for injection. Here we would go around the site to see what queries the website does normally, here we can see "web-security-academy.net/filter?category=Gifts" if we click on the Gifts category, now we know that if we can input ' in after the ?category=' and get internal server error that it is vulnerably to sql injections. We now only need to do: UNION SELECT NULL, NULL, NULL... until we get the number of rows/columns that is in the table. So the correct sql injection would be: `?category=Gifts'+UNION+SELECT+NULL,+NULL,+NULL--`, now we know the number of columns/rows in the table, and we can now try to insert to see what datatype each row/column takes, here we try for strings and try with each NULL to set to eg. 'abc', for seing which takes a string:

`?category=Gifts'+UNION+SELECT+'abc',+NULL,+NULL--`
`?category=Gifts'+UNION+SELECT+'NULL',+abc,+NULL--`
`?category=Gifts'+UNION+SELECT+'NULL',+NULL,+abc--`

Pros with union is: that we know that that we can find the number of columns, we can find the specific datatype for each column, and we know that if it works that union is permitted.

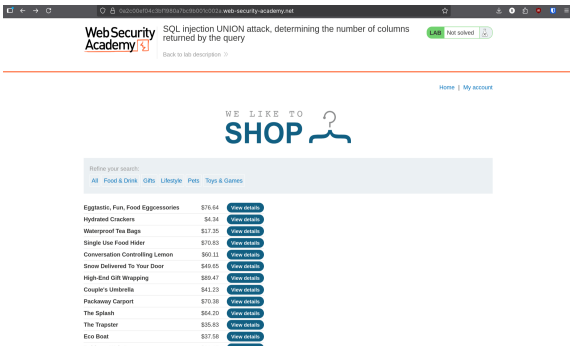

Figure 1: Websites main products site

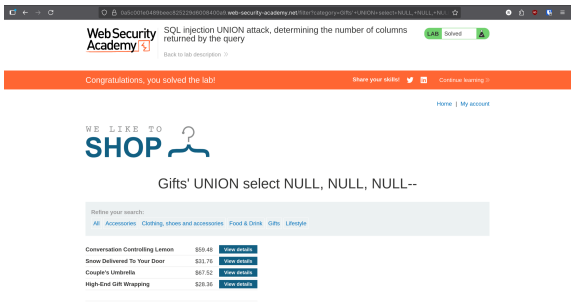

Figure 2: After using UNION

B Using the 'Order by' command

To use the (n == number)

```
ORDER BY n;
```

sql attack, we nned to use the websites url for injection as before. This time we would instead in the url type:

```
category=Gifts'+ORDER+BY+1--
category=Gifts'+ORDER+BY+2--
category=Gifts'+ORDER+BY+3--
```

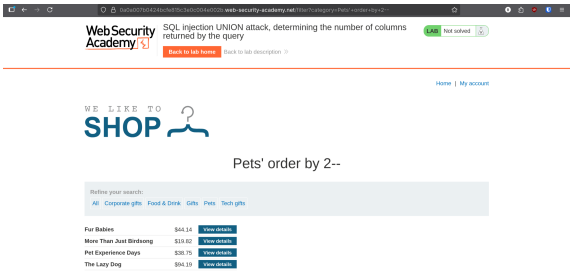

Figure 3: Order by 2, for the string column(ascending alphabetically)

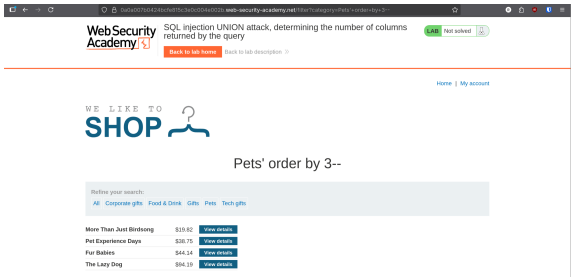

Figure 4: Order by 3, for the price column(ascending numerically)

Pros with order by, is that it is very fast to get a idea of how many columns the table has, instead of writing a bunch of NULL's in the union. Plus order by may not be restricted in the WAF[1]

C Using 'ORDER BY' & 'UNION' To retrive data from other tables

We will now use both methods to retrive data from another table, which is hidden in the database. First we will use the 'ORDER BY 2 ...' query to see how many colums that the table has, and after we would use the 'UNION select NULL, NULL' to see how many of the columns are string/varchar values.

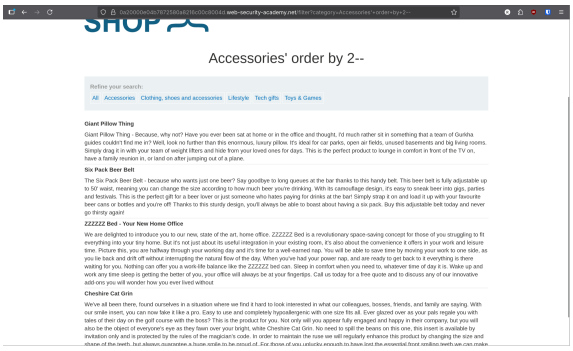

Figure 5: Order by 2;

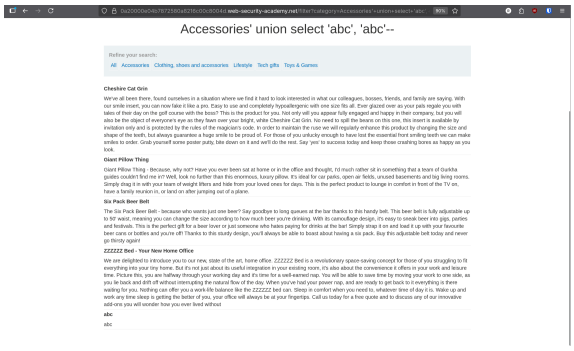

Figure 6: Union SELECT 'abc', 'abc';

We now know that the site is vulnerable to sql injections, with unions and we also now know the number of columns and which columns take strings as inputs.
The lab gave us hints of what the other tables names was: `users` & that the column name was: `username` & `password`.
Now we will use this info combined with the knowledge that there is 2 colums, and we know we can use 'UNION' on the website.

```
UNION SELECT username, password FROM users--;
```

This sqli will show us the table users, where username and password are shown:

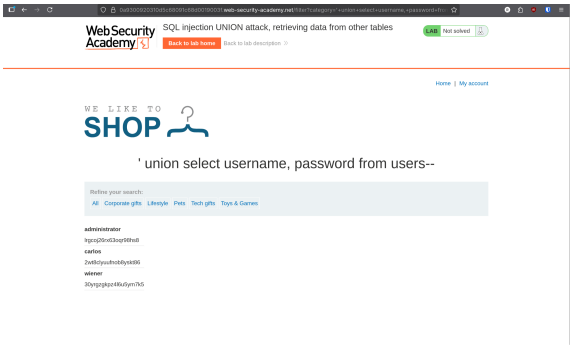

Figure 7: Using the UNION to get another tables dataimage

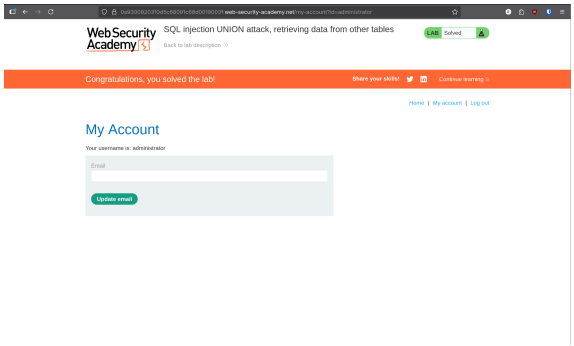

Figure 8: Logged successfully into the administrator account

References

[1] Cloudflare. Web application firewall (waf). Accessed: 2025-11-14.