**Secure Programming Assignment 1: Vulnerable Web Application**

This group consists of:

* Daniel Mocek (B00152633)
* Shahenwaz Muzahid (B00155676)
* Kenert Salm (B00153878)

**The Task and Deliverables:**

The purpose of this assignment is to secure vulnerable source code in the web application provided and provide a report on how you achieved this. You will be supplied with a simple Web application. The app is coded using Python Flask and connects to an SQLite backend database.

There are 3 parts to the assignment:

* Demonstrate 10 exploits in the code using screenshots and a description on how the application is vulnerable in the source code. We should aim for 5 exploits we have learned in the labs and 5 we have not.
* Fix the 10 exploits in the code. 5 fixes we have learned in the labs and 5 we have not.
* Demonstrate that the 10 exploits are no longer possible (again use screenshots and a description).

The final code must still run properly with the changes and remain as close as possible to the original code.

Marking Rubric goes as follows:

**Identifying and exploiting vulnerabilities (50%):**

• Lab vulnerabilities - 20%

• Non-lab vulnerabilities - 30%

**Fixing the vulnerabilities (50%)**

• Lab vulnerabilities - 20%

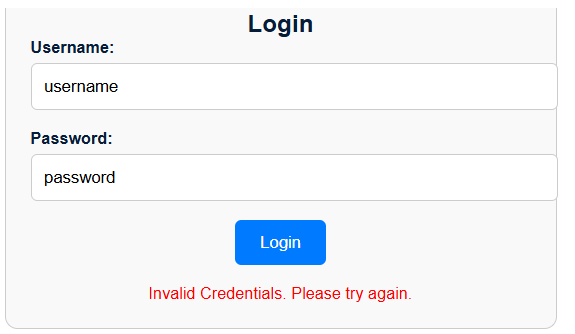
• Non-lab vulnerabilities - 30%

**Section 1: Identifying and Exploiting Vulnerabilities**

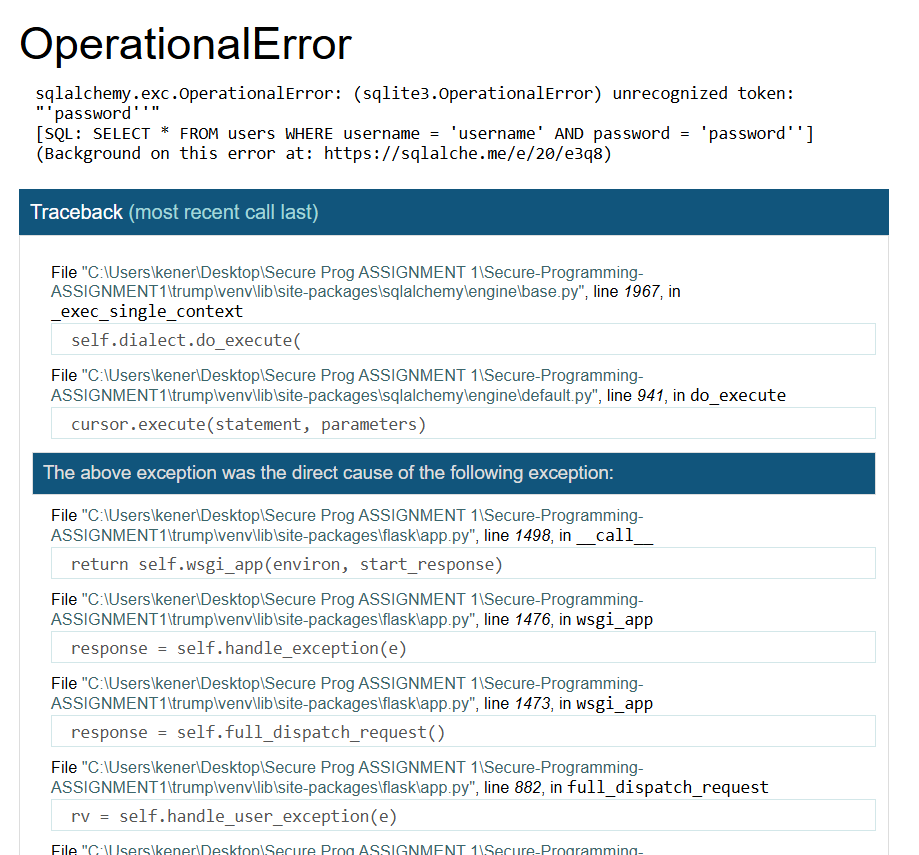
**(Kenert Salm)**

1. SQL Injection Attacks

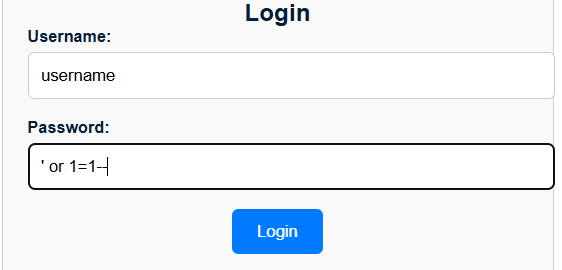
Looking at the Login section first, we can see there are prompts for a username and password. When trying to enter random details it will say its invalid



However, if we add a quote character ( ‘ ) to the end of password we get this error.



This means that the quote character is significant to the code that runs the login form and adding one caused the whole process to crash. Exploiting this fact, we can try to write this in the password section:



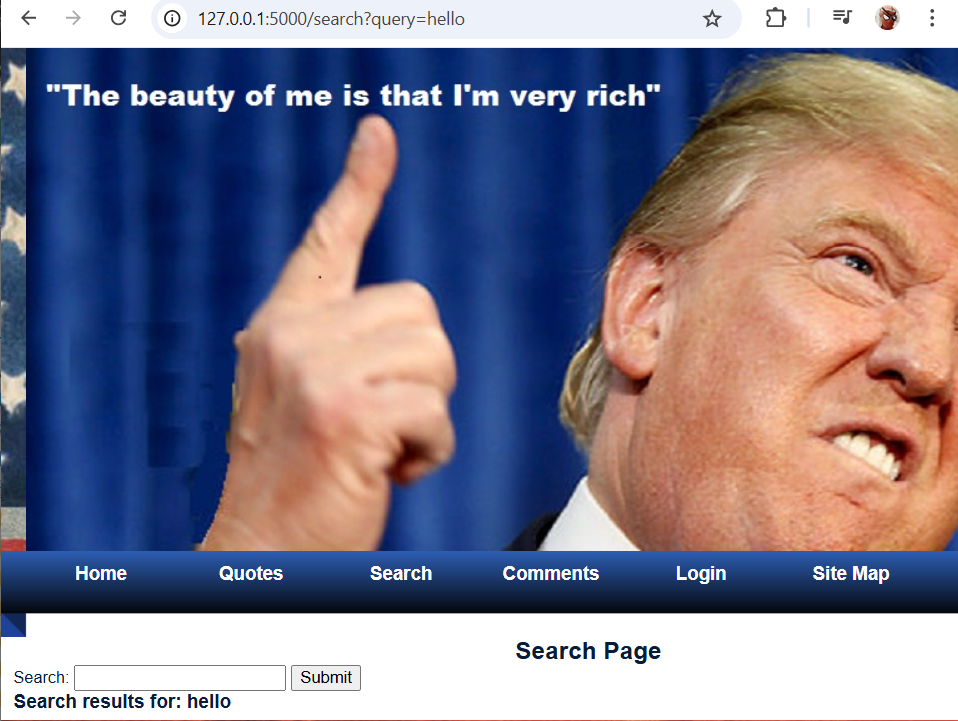
Once we press login, details of a user knows as Holmes show up including very sensitive details such as his email and card details.



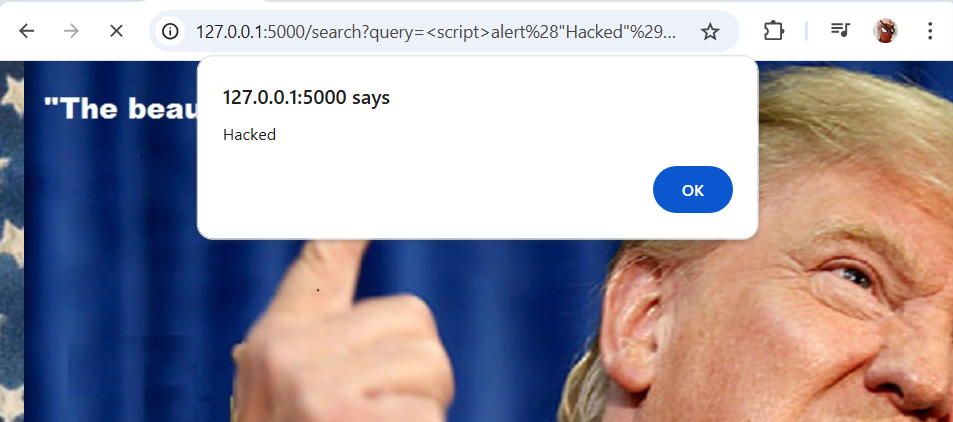
Since 1=1 is always true, the entered password will exploit the database into ignoring any security protocols allowing hackers to bypass any need for a password to get access to details.

1. Reflected XSS Vulnerability

When we write anything into the search function of this website, we can see that the entered term is displayed in the URL of the website.



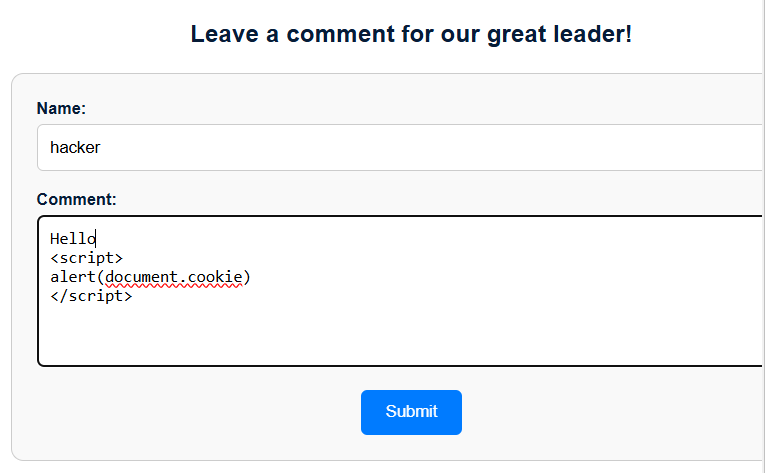
Knowing this, we can make the page display a banner like the following:



Hackers can exploit this vulnerability by redirecting victims and their authentication cookies to their own server and then steal the cookies for impersonation.

1. Stored XSS Vulnerability

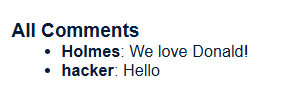
Since users can leave comments on this website, attackers might be able to inject their own JavaScript into the website database. We will write a comment with a basic script like this for example.



Once we submit the comment , whenever anyone visits the comment section on the website, a banner prompt shows up.



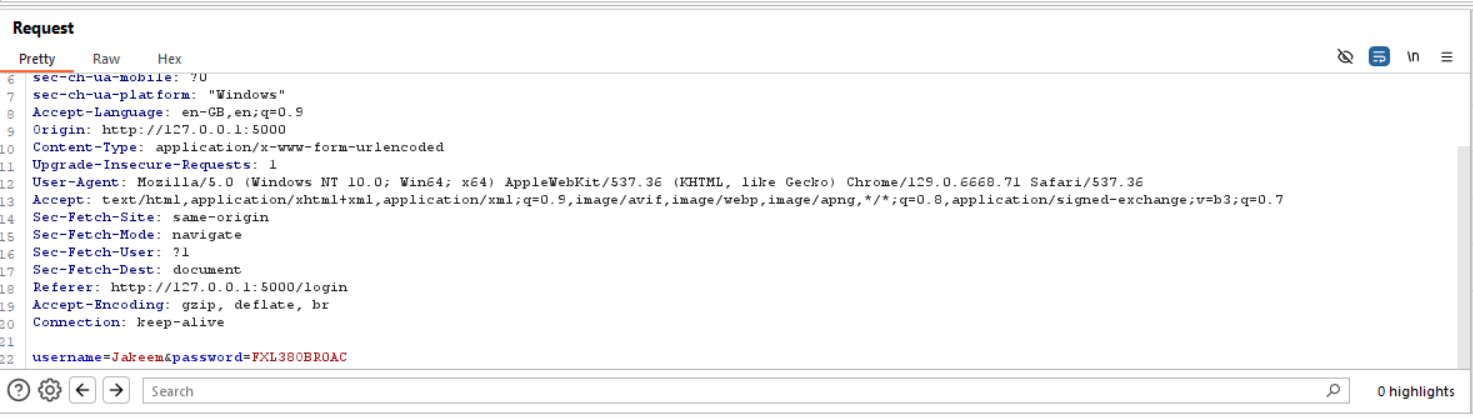
While in our instance, the banner says nothing, this vulnerability could be exploited if the hacker decides to write a more in-depth script that will show the users cookies on the hackers server if they enter this part of the website. The code itself will also be hidden on the page so only the message “Hello” will be displayed.



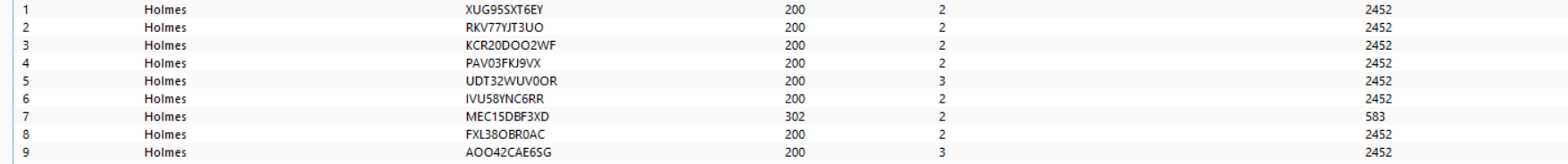
1. Brute-force Authentication Attack

Let’s say that a hacker wanted access to a certain account, for this instance we want to find out the password for Holmes. The hacker has a list of passwords but the website has a limit to how many attempts to login. The hacker can use Burpsuite to brute-force attempts and find out which password is Holmes’.

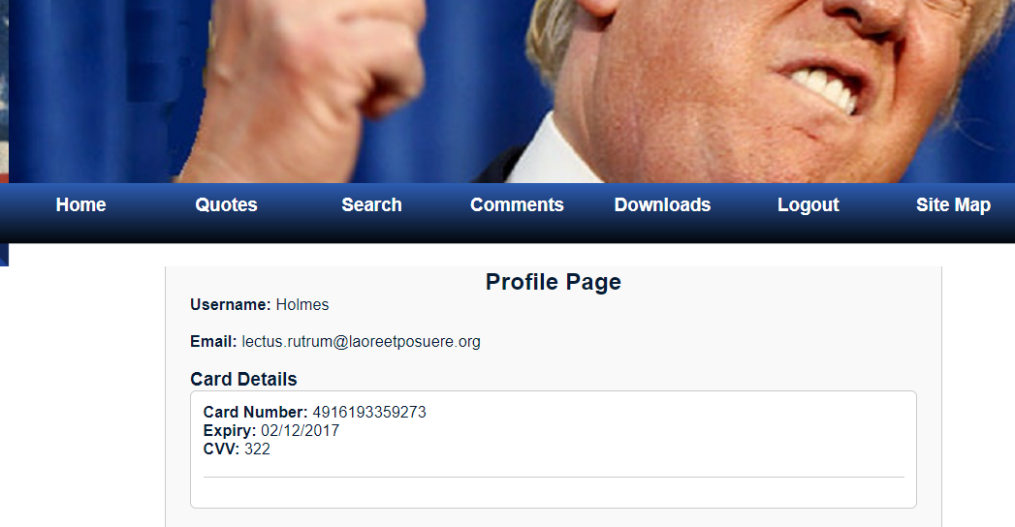
Using Burpsuite, the hacker can get something like this to display by using another account.



After the hacker follows a process of setting up a “Cluster Bomb” attack with two payloads, one being the username Holmes and the other being passwords, they can start attack and Burpsuite will give back the results.



We can see that the status code and length for the 7th password is different from the rest, this indicates that the password could be correct. This can be then tested if we see the response in browser. As we can see the Authentication Brute-Force attack has worked.

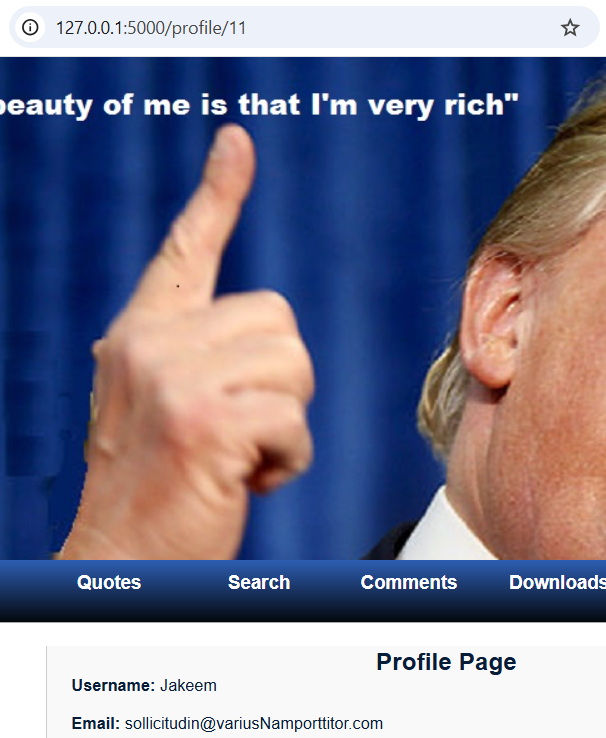


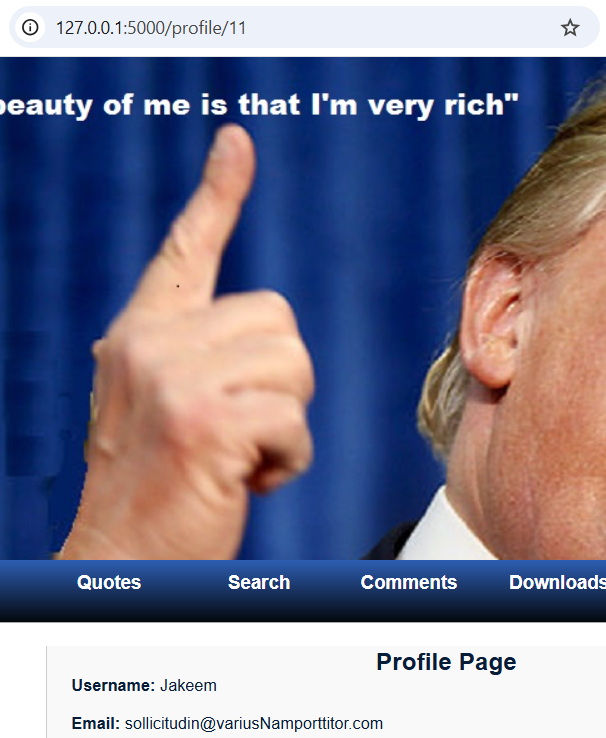
1. Command Injection

As the port of the website is 5000, the hacker an create a reverse shell on a netcat session which will allow them to execute commands remotely on the server. If done correctly they could get access to every users info on the website.

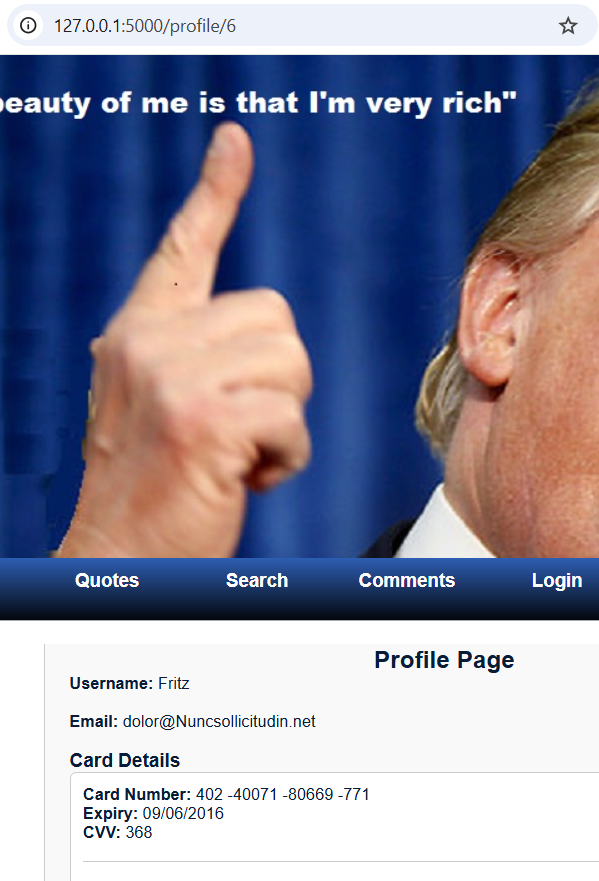
1. Insecure Direct Object Reference

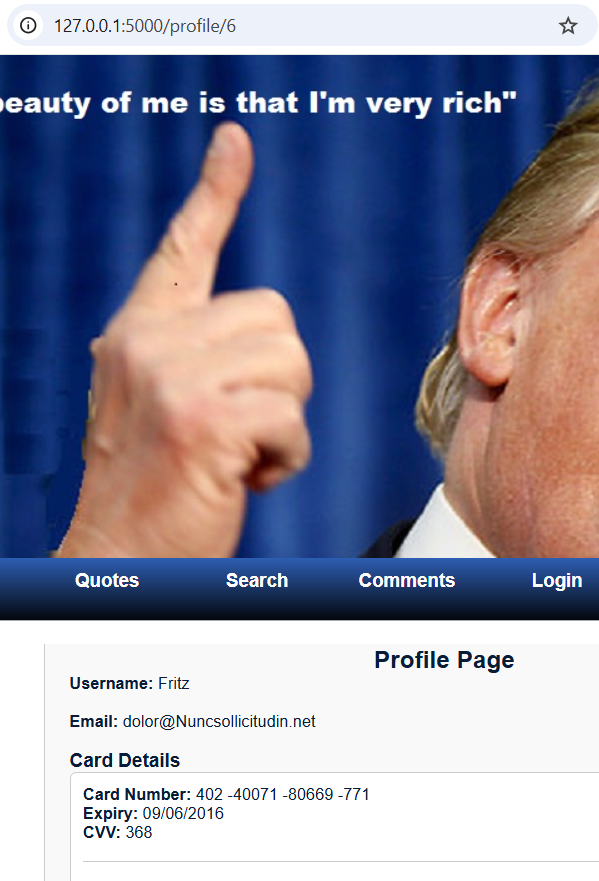
When logging in as Jakeem for example, the URL changes to this:





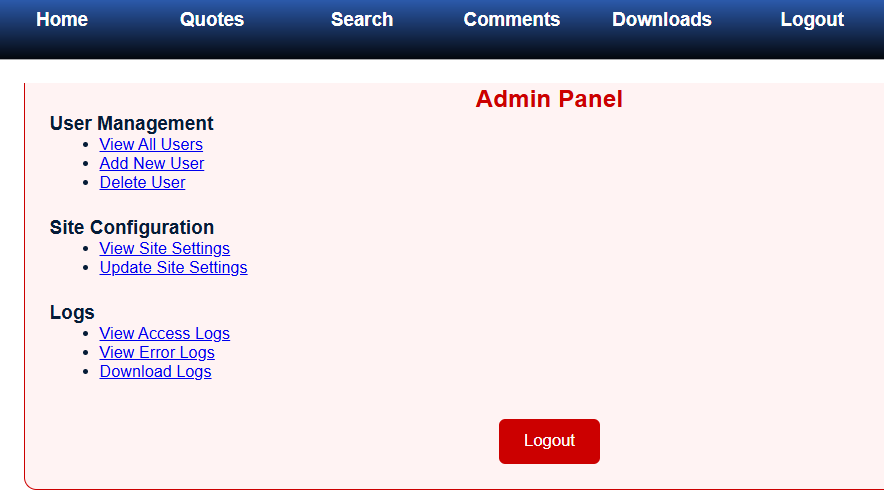
The hacker can now see any profile including their bank details by just changing the profile number. If he wants to see details of profile 6 he can just do this.





1. Broken Access Control

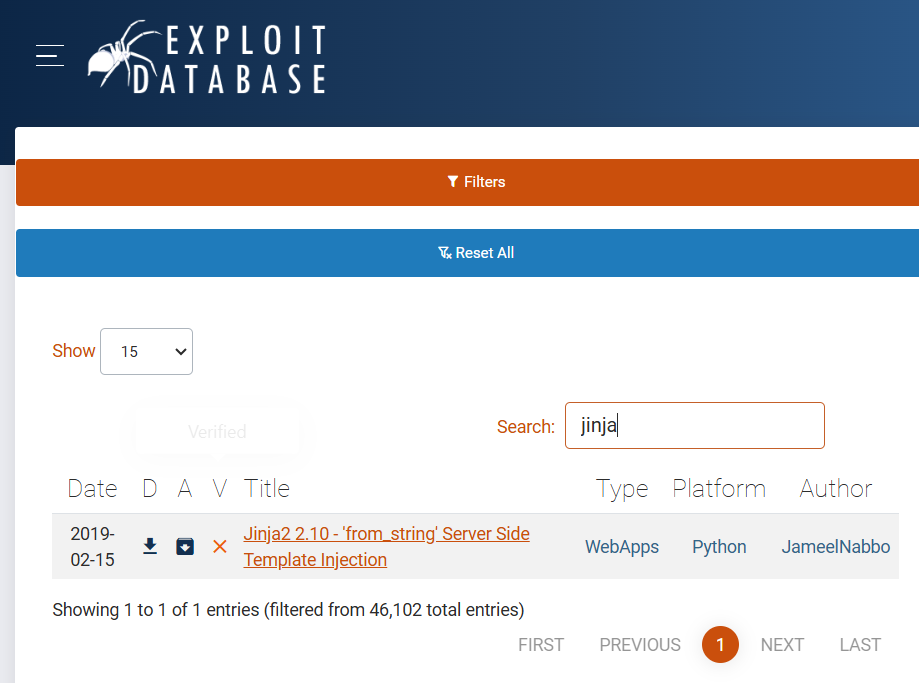
Looking at the code we can see that there is an admin panel on this website. By changing the URL of the site to “127.0.0.1:5000/admin\_panel” we get access to this panel.



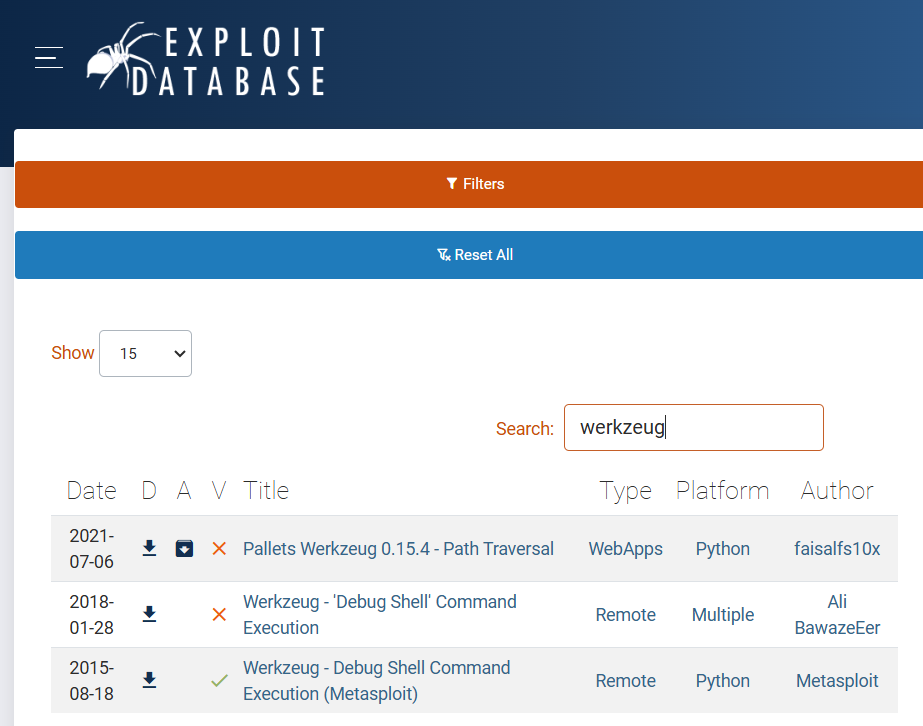
With this panel, the hacker could now do anything with the site such as deleting users, changing setting or checking access/ download logs.

1. Vulnerable and Outdated Components

The code for the website does include some vulnerable components in the lib folder. Two components “Jinja2” and “Werkzeug” display vulnerabilities on exploit-db.com



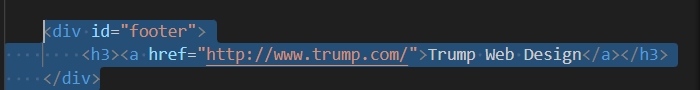
We can see that Jinja is vulnerable to a Server-Side Template injection. This essentially puts users at risk as the hacker could take complete control over the server.



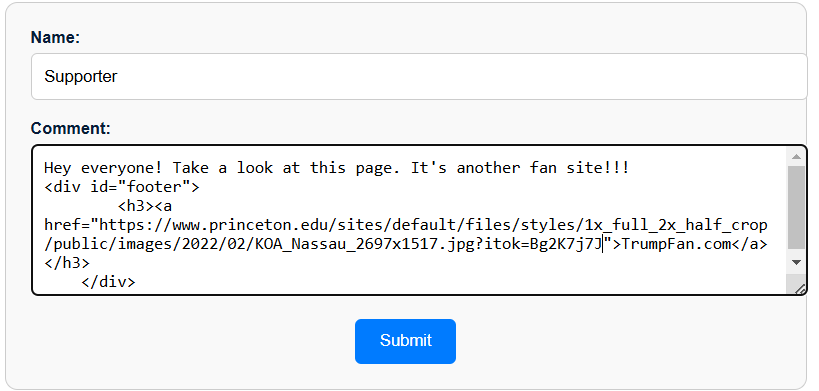
Werkzeug has 2 vulnerabilities here. Path Traversal and Debug Shell Command Execution.

1. Cross-Site Request Forgery

Looking at the code used in the Quotes section, we can see that there is a link made to the trump website.



A hacker can exploit this link in the Quotes section by going into the Comments section and then writing something like this



The hacker can put any href link that they want and when submitted, the page will only display the comment and fake URL added as a clickable link.



Let’s say that this could be an inline frame link, the hacker could use an oblivious users cookies if they clicked on the link. They could then issue commands such as account deletion etc.

**Section 2: Fixing The Vulnerabilities**

**(Daniel Mocek)**

**Section 3: Demonstrating the Fixed Vulnerabilities**

**(Shahenwaz Muzahid)**