Information Gathering and Exploitation

By

Yemula Varnith

Submitted in partial Fullfillment of the Requirements
for the Course in cyber security from 1STOP in association with
TALAKUNCHI

April 2022

DECLARATION

I hereby declare that the contents presented in the project entitled "Information Gathering and Exploitation", submitted in partial fulfillment for the course in cyber security from 1STOP in association with TALAKUNCHI, is a record of original work investigated by me.

ACKNOWLEDGEMENT

We sincerely thank all the teaching and non-teaching support staff of the 1stop and Talakunchi. We also like to thank all our college faculty members for their timely suggestions and motivation during the course of our project work. We thank our parents, who were the backbone behind our deeds.

Finally, we express our immense gratitude with pleasure to all individuals who have either directly or indirectly contributed to our needs at the right time for the development and success of our project work.

ABSTRACT

We are more vulnerable to the dangers of cyberspace because we live in an era where most tasks can be digitized. Our presence in the digital domain has exploded, from simple operations like placing a phone call to complicated processes like financial transactions via online banking. We put our information out there before, after, and during these activities, and if it isn't secure, we are vulnerable to cyberattacks. Cyber security is a branch of study that deals with these issues. Cyber security is the protection of our computer network and systems from hostile activity that can harm people, software, and hardware.

TASK 1

Entering into the admin panel using SQL Injections of some random websites

List of Tools used

Kali Linux

Kali Linux is a security Linux distribution based on Debian that was created with computer forensics and advanced penetration testing in mind. It was created by Mati Aharoni and Devon Kearns of Offensive Security, who rewrote BackTrack. Kali Linux comes with a large number of tools that are well-suited to a variety of information security tasks, including penetration testing, security research, computer forensics, and reverse engineering.

SQL Injection

SQL injection is a technique that involves injecting SQL commands as statements into web page inputs in order to exploit user data. In essence, malicious users can use these statements to manipulate the application's web server.

- A SQL injection is a type of code injection that has the potential to completely ruin your database.
- One of the most frequent web hacking tactics is SQL injection.
- SQL injection is when malicious code is injected into SQL statements via web page input.

Burp Suite

Burp, often known as Burp Suite, is a package of tools for web application penetration testing. It is created by the firm Portswigger, whose founder Dafydd Stuttard goes by the alias of the same name. BurpSuite aspires to be an all-in-one toolkit, and its capabilities can be expanded by installing BApps, or add-ons.

Among professional web app security researchers and bug bounty hunters, it is the most widely used tool. Its simplicity makes it a better choice than free alternatives like OWASP ZAP.

Google Hacking database

Attacks that employ Google or another search engine to locate weak web servers and websites are referred to as Google hacking, Google hacks, or Google dorking.

To identify poorly configured web servers and web pages that disclose sensitive information, Google hackers create custom search queries, frequently employing wildcards and complex search operators (such as intitle, inurl, intext, filetype, and more). A search for site:*/signup/password.php, for example, may return all pages with login gateways.

STEP1: Checking for Vulnerability

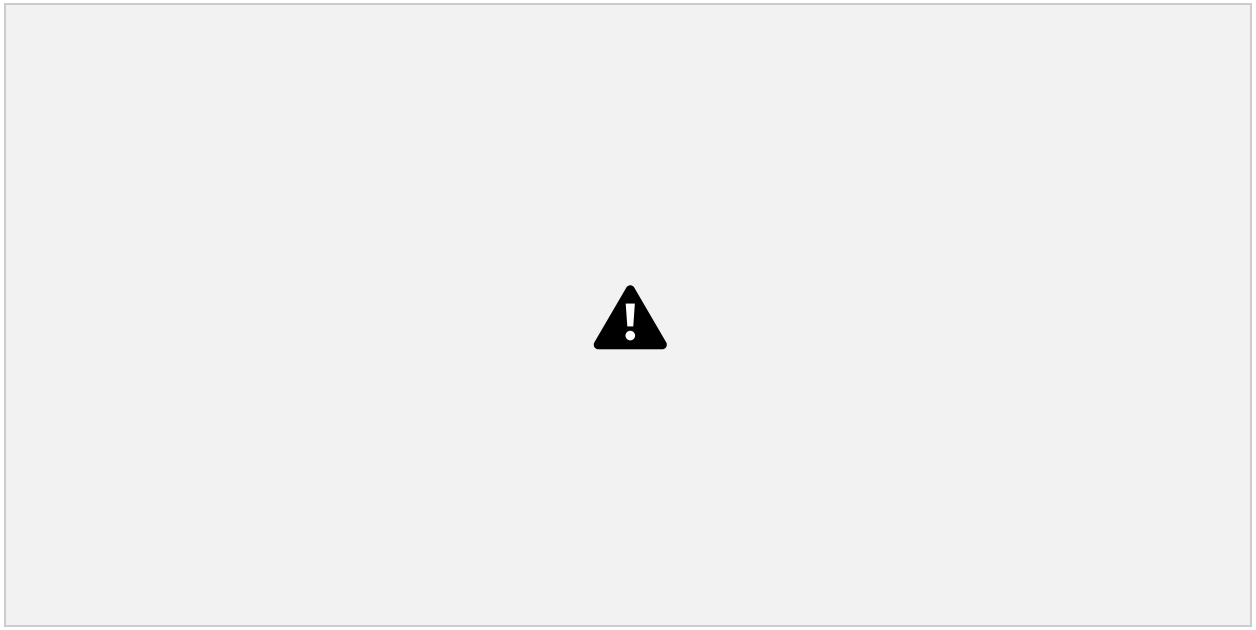
Before attempting to bypass any login authentication, check to see if the website is vulnerable to SQL injection. Putting (') at the username or password is the simplest approach to check for the vulnerable. If the server responds with any form of SQL error, the website is most likely vulnerable to a SQL Injection attack.

(This step isn't essential; it only works on some websites, not all.)

STEP2:Configure Your Attack Browser for Burp Suite

The browser must then be configured to work with Burp Suite, which acts as a proxy to intercept and modify requests. I'm using Firefox to demonstrate this, but most browsers will work similarly.

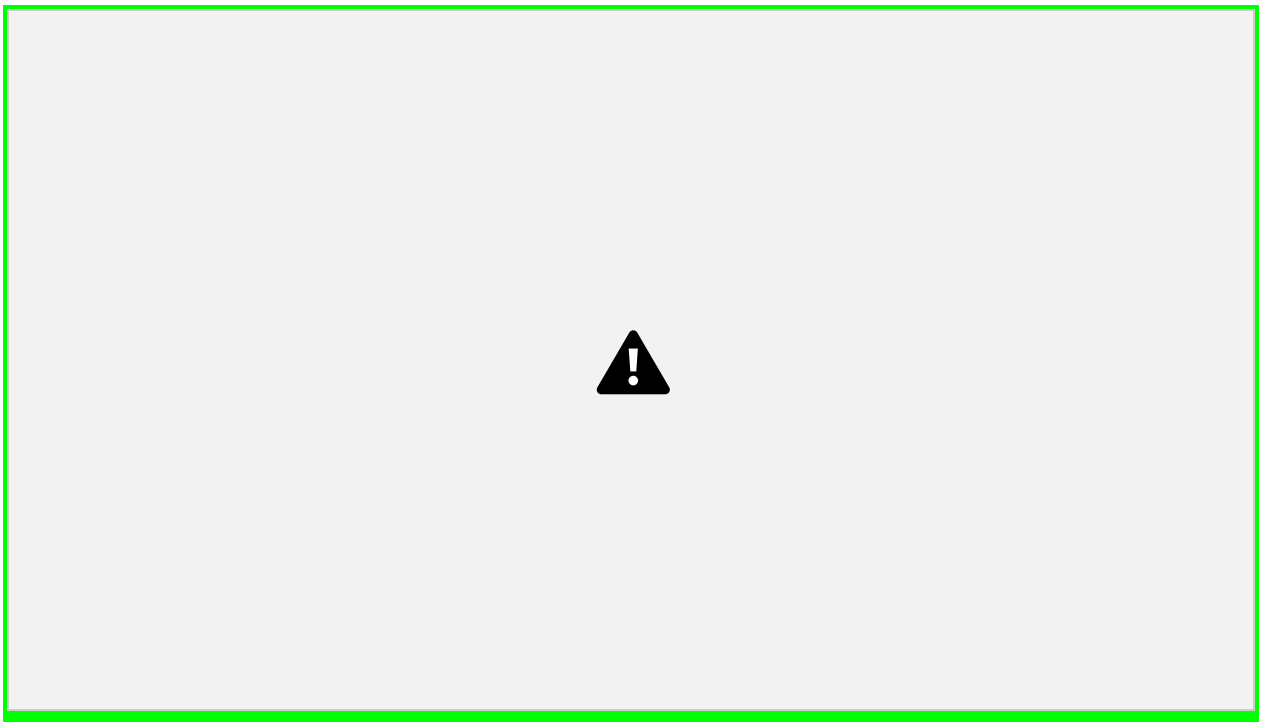
Click "Settings," then Click "Settings," then at the bottom of "General," click on "Network Settings." , then "Manual proxy configuration" and enter 127.0.0.1 and 8080 as the HTTP Proxy and Port, respectively. Next, check "Use this proxy server for all protocols," double-check that "No Proxy for" isn't checked, and then click "OK."



Now it's time to start Burp Suite.

STEP3:Intercept the Request with Burp Suite

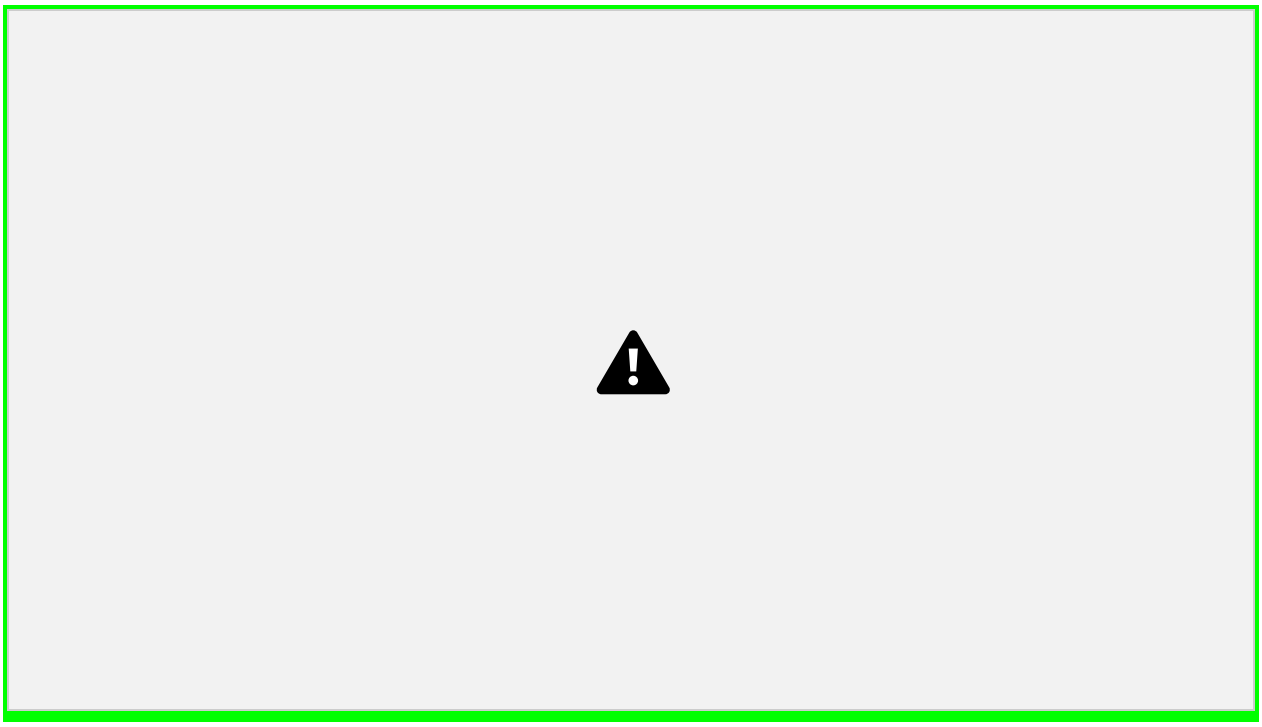
In Kali, open the Burp Suite app, create a new project, and then go to the "Proxy" page and make sure "Intercept is on" is selected. This will allow us to change the request from the webpage and test for SQL injection by inserting different values. I returned to the login page and attempted to log in with a random username. You can see the entire request, including arguments, headers, and even hex data.



We're mostly interested in the username field because that's what we'll change to see if there are any SQL injection problems. Then select "Send to Intruder" from the "Action" menu. Alternatively, you can accomplish the same thing by right-clicking anywhere in the request area.

STEP4:Configure Positions & Payloads in Burp Suite

Then, under the "Intruder" menu, select "Positions." When a request is submitted to intruder, Burp Suite automatically configures the spots where payloads are injected, but since we're only interested in the username field, we can erase all positions by hitting "Clear" on the right. Click the "Add" button after selecting the username value you want to use. We'll use the "Sniper" attack type, which will go through a list of payload values and attempt each one one by one.



Now our position is set, and we're ready to configure the payload. SQL queries work by interacting with data in the database through the use of statements. The SELECT statement is used to retrieve data, so a login query would look like:

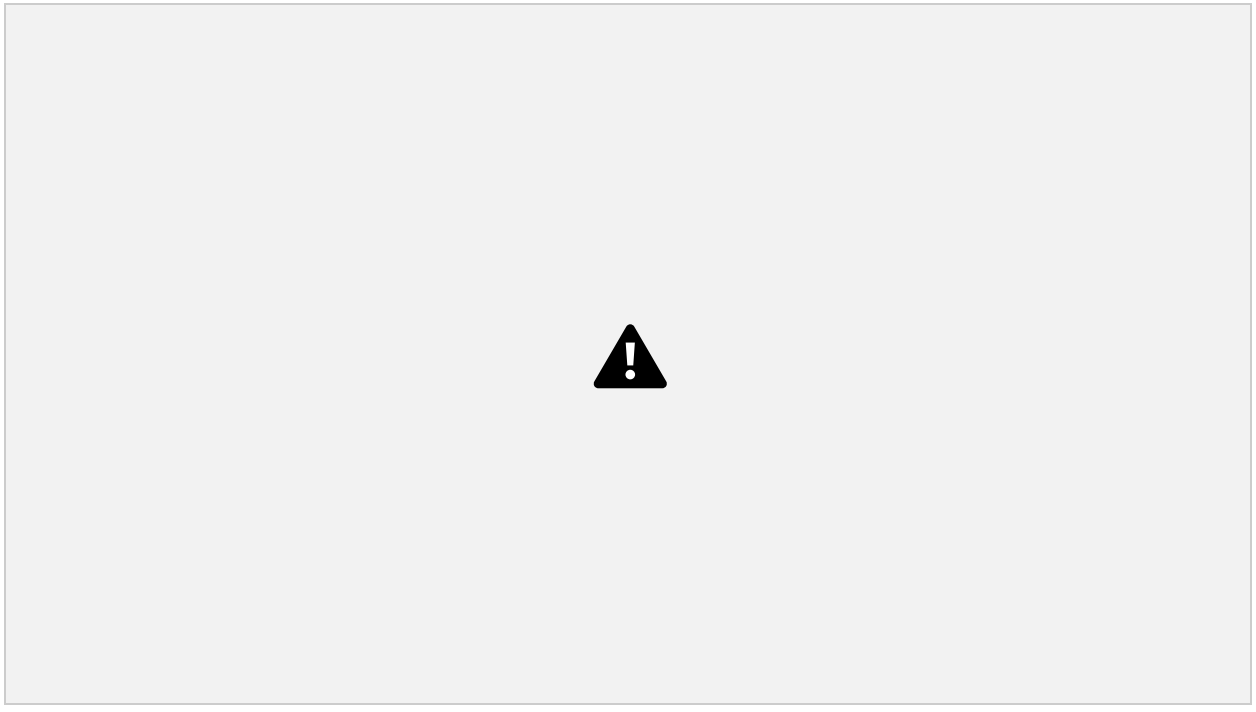
```
SELECT username, password FROM users WHERE username='myname' AND password='mypassword';
```

let's look at the classic SQL injection command **' or 1=1--**. Here is what the SQL statement looks like when entered into the login field:

```
SELECT username, password FROM users WHERE username='' or 1=1-- AND password='';
```

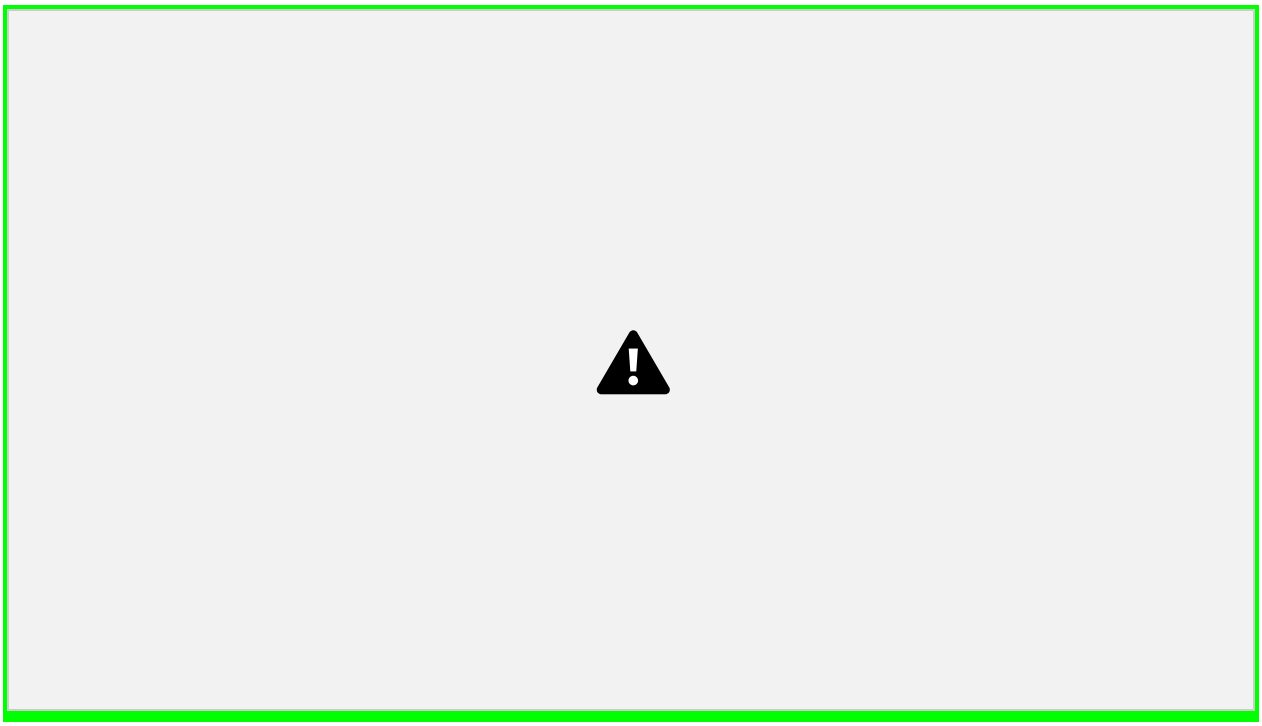
Because 1=1 always evaluates to true, the username query will now return "blank" or "true." The password field is ignored since the double dashes comment out the rest of the query. The database will return account data because "blank" or "true" is always true and the password field is ignored.

Go to "Payload Options'' under the "Payloads'' tab; we may keep all of the default settings for now. Here, we can either add our payloads one by one or load an existing list to create a simple list. Kali includes a number of wordlists, including one for testing SQL injection vulnerabilities. Go to /usr/share/wordlists/wfuzz/injection/SQL.txt and click "Load." We are now ready to start our attack.

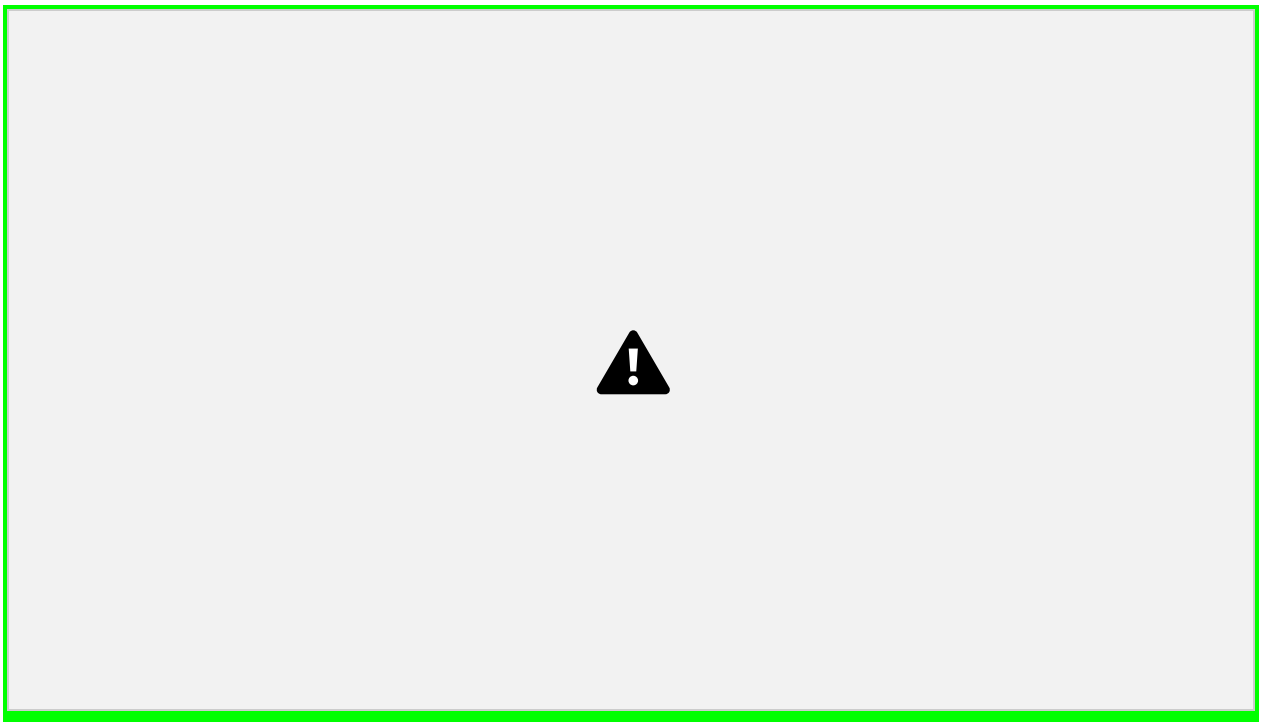


STEP5:Run an Intruder Attack in Burp Suite

When you press the "Start attack" button, a new window will appear, displaying the invader attack. You can see the requests' progress, as well as their payload and status, here. Be patient, as depending on the length of the list, this could take a long time to complete.



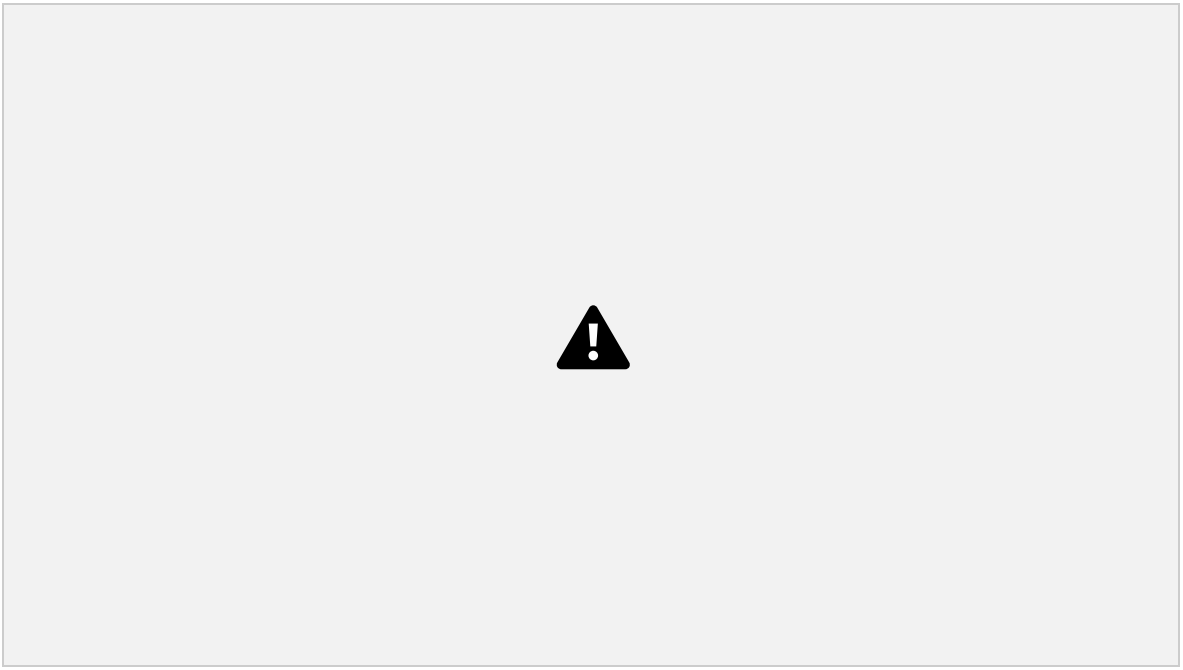
When intruder is finished, simply click on any request to get the specifics.



STEP6:Analyze the Results

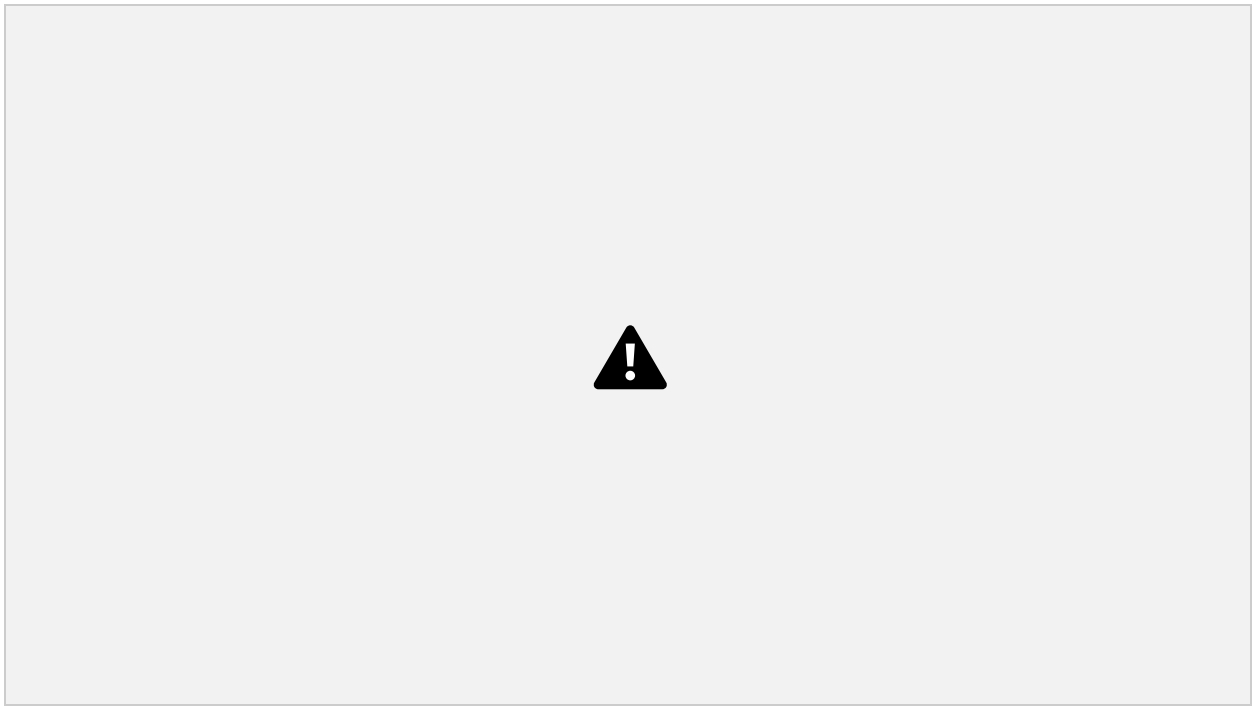
The response is what we're looking for. Every request received a status code of 200, however when a payload is successful, you may get a different code. Another method to know if a query was successful is if the response length differs considerably from the others. I chose the request that contained the SQL query 'or 1=1 or "=' since I had manual

tested this injection and knew it would work.



Burp Suite is important since it allows you to render the webpage that is returned in the response by clicking "Render" on the "Response" tab. Our SQL injection was successful, and we now have users and passwords, as seen below. We could log in with the admin credentials and cause all kinds of havoc if this was an administration panel

anything similar.



Task 2: Show some live cameras using Google hacking database.

Google Hacking database

Attacks that employ Google or another search engine to locate weak web servers and websites are referred to as Google hacking, Google hacks, or Google dorking.

To identify poorly configured web servers and web pages that disclose sensitive information, Google hackers create custom search queries, frequently employing wildcards and complex search operators (such as intitle, inurl, intext, filetype, and more). A search for site:*/signup/password.php, for example, may return all pages with login gateways.

Google hacking, also known as google dorking, is a data collection method that makes advantage of advanced Google search tactics. It may be used to find security flaws in online applications, gather information for arbitrary or specific targets, find error messages containing sensitive information, and find files containing credentials and other sensitive data if utilized properly.

Google's specialized search operators

Before you begin with Google Dorks, you should have a basic understanding of a few unique Google search operators as well as how they work.

1. **intitle**: This instructs Google to display pages with the term in their html title.

2. **inurl**: Searches the URL for a specific phrase. inurl:register.php is an example of a URL.

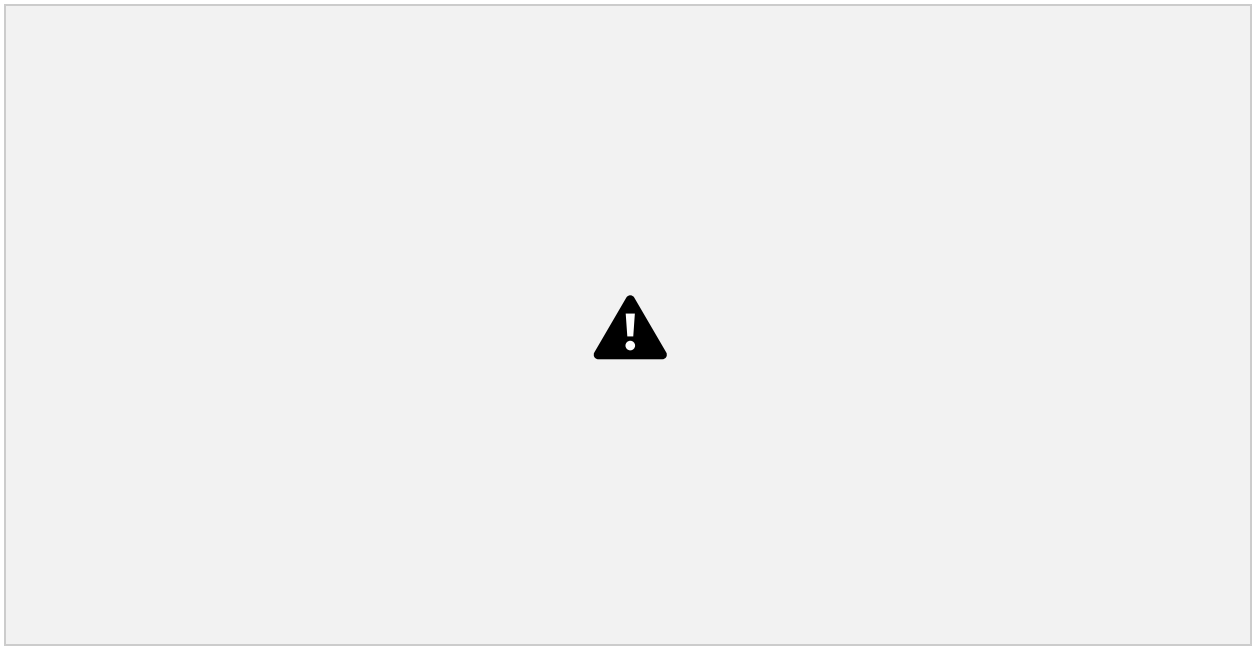
3. **filetype**: I was looking for a specific file type. For instance, filetype:pdf will look for all pdf files on a website.

4. **ext**: It functions in the same way as filetype. ext:pdf, for example, locates files with the pdf extension.

5. **intext**: This will search the page's content. This works in a similar way to a standard Google search.

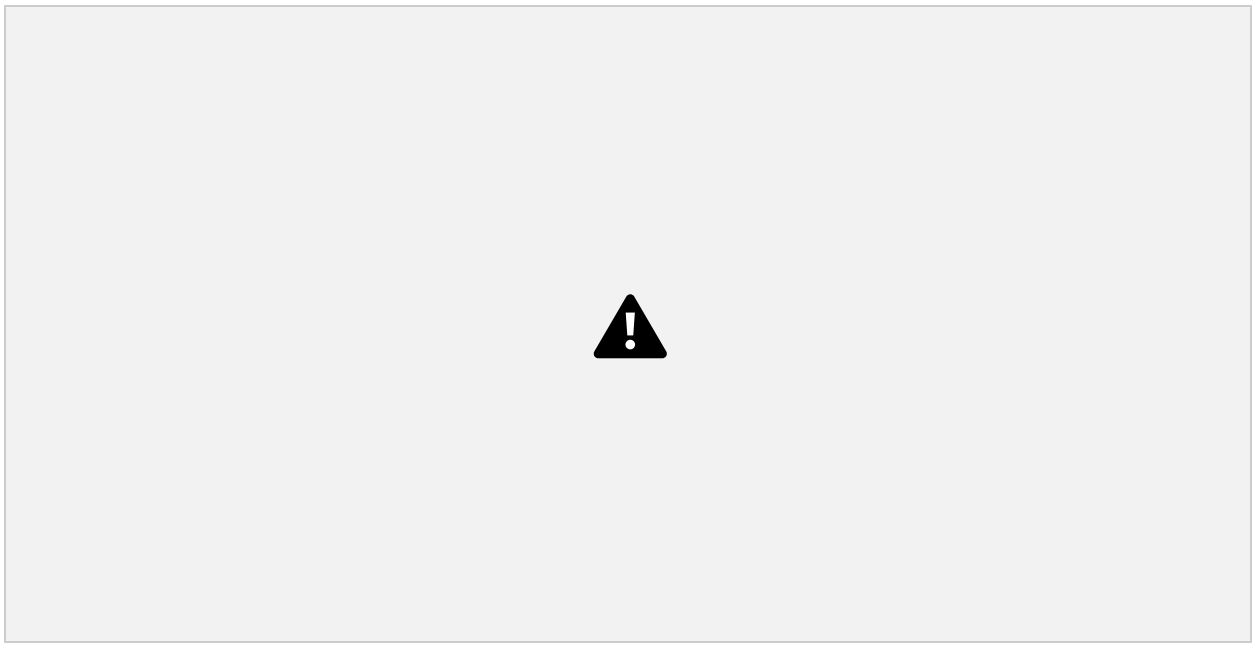
STEP1: Go To Google Hacking Database(GHDB)

You can either search in google for google hacking database or go to link , https://www.exploit-db.com which looks like this

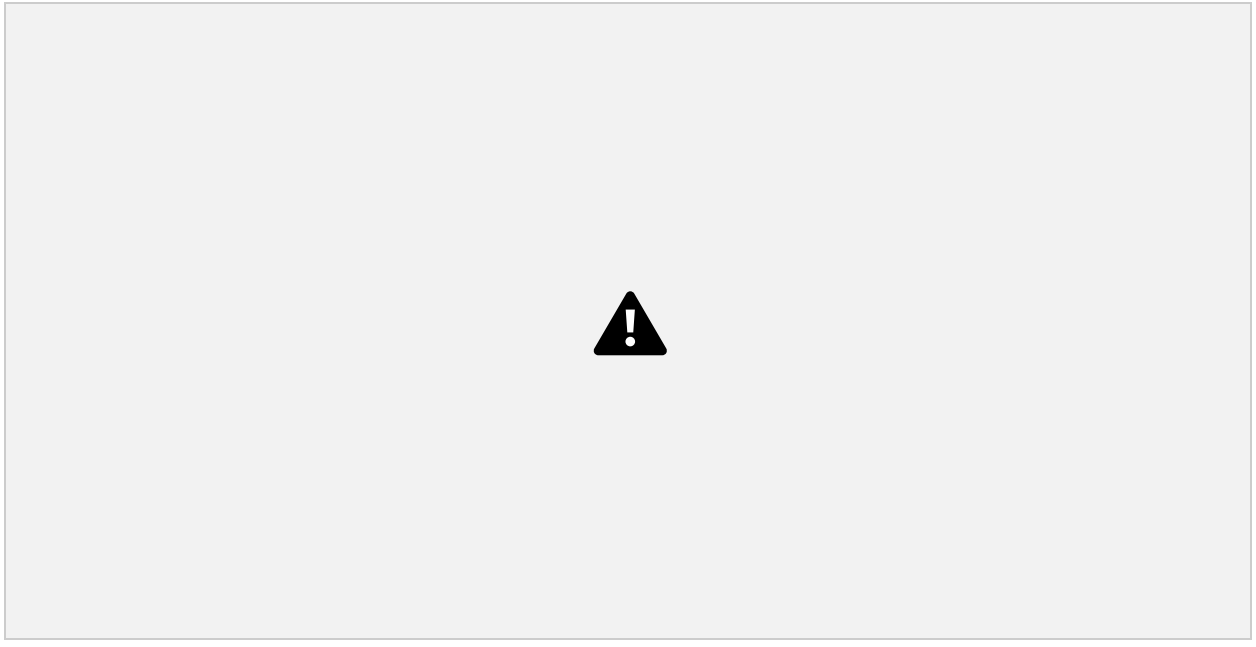


STEP2: Finding webcams

Now click on the search icon as shown in the picture below

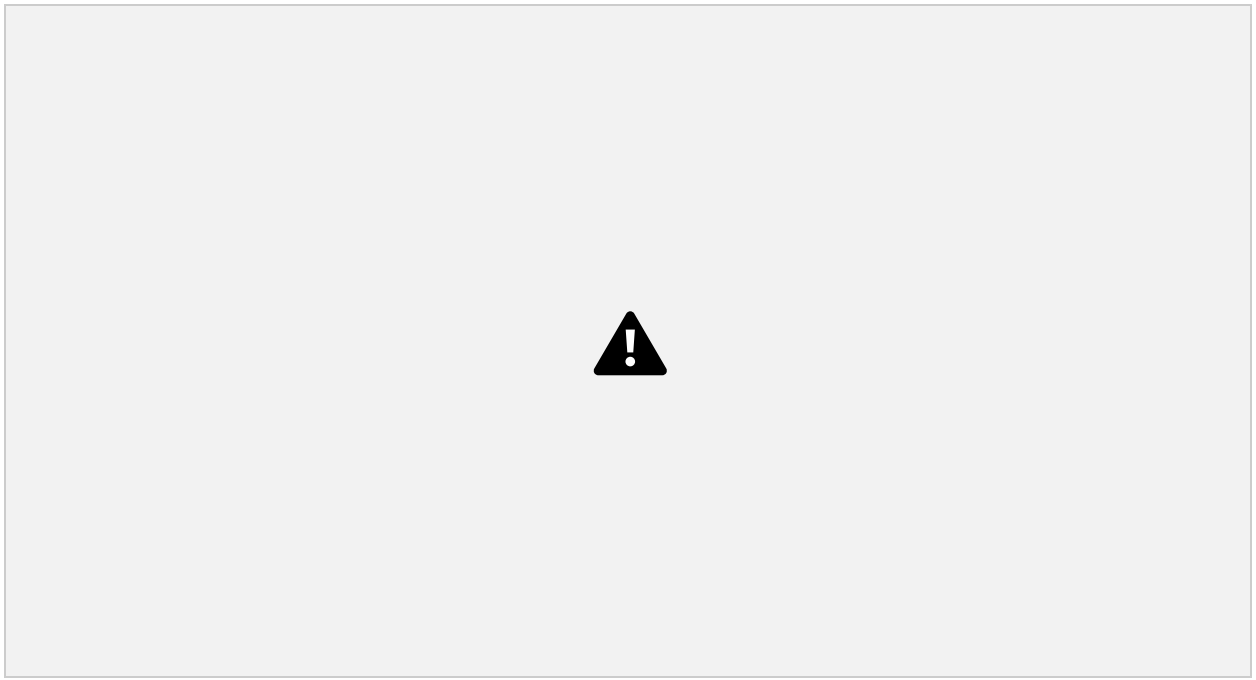


Now in the search box try finding live webcams by typing webcam

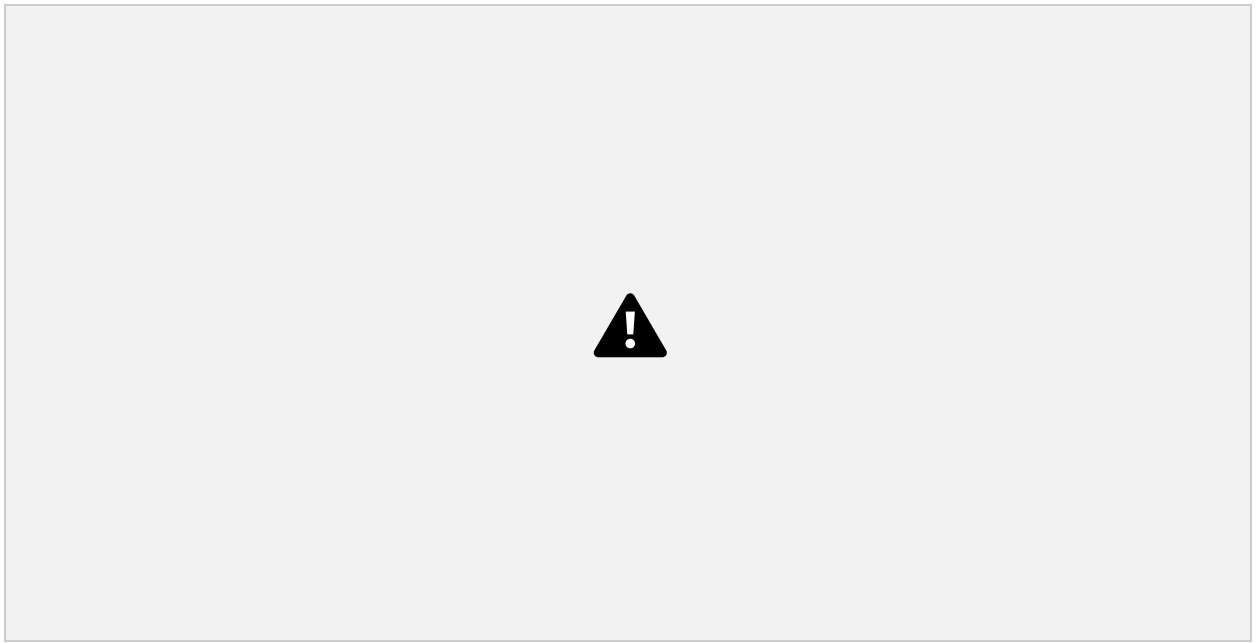


STEP3: Opening Dorks

Select your desired Dorks , copy the Dork and paste it in google



then open the website to watch the live webcam.



Here are few other webcams we found out using GHDB