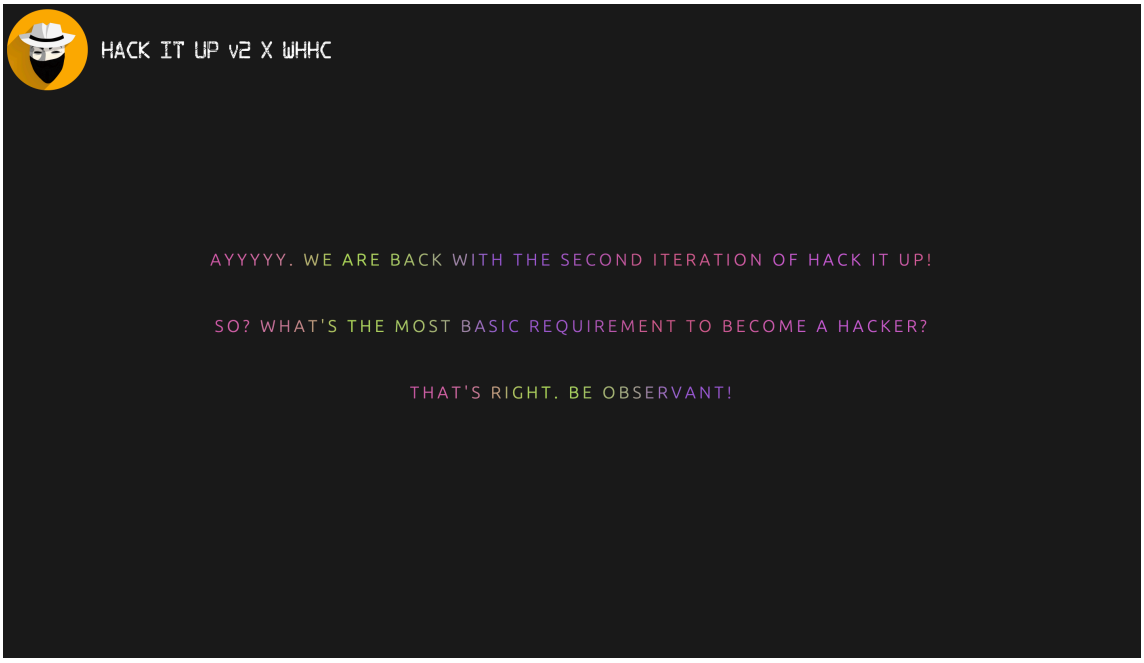
HACK IT UP v2.0

Level 1:



The first step to become a hacker is to know how to check the source code

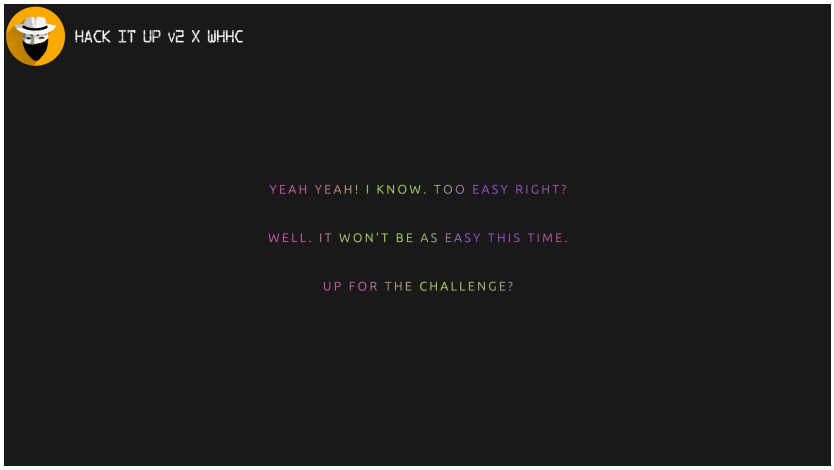
(Left Click and tap on “Source Code”).

Source code shows the working of the webpage.(HTML/CSS)

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Hack It Up v2 | Level 1</title>

<script async src="https://www.googletagmanager.com/gtag/js?id=UA-125937952-1" type="fe784517e512a37015bda22f-text/javascript"></script>
<script type="fe784517e512a37015bda22f-text/javascript">
        window.dataLayer = window.dataLayer || [];
          function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
          gtag('config', 'UA-125937952-1');
    </script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="css/style.css?v=1548736800">
</head>
<body>
<img id="logo" src="../../whhc.png"></div>
<img id="text" src="../../logov2.png"></div>
<div class="container">
<span class="txt anim-text-flow">Ayyyyy. We are back with the second iteration of Hack It Up!</span>
<br>
<span class="txt anim-text-flow">So? What's the most basic requirement to become a hacker?</span>
<br>
<span class="txt anim-text-flow">That's right. Be Observant!</span>
</div>
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js?answer=ZCCyVl" type="fe784517e512a37015bda22f-text/javascript"></script>
<script src="js/index.js" type="fe784517e512a37015bda22f-text/javascript"></script>
<script src="https://ajax.cloudflare.com/cdn-cgi/scripts/2448a7bd/cloudflare-static/rocket-loader.min.js" data-cf-nonce="fe784517e512a37015bda22f-" defer=""></script></body>
</html>
```

Level 2:

Just like Level 1, check for the source code, but this time the **token** was hidden in CSS code. In last level we saw how to check the HTML Source code. This time we have to check the CSS code.
Look at the picture below, You will see the CSS's "<link>" Tag. Click on that.




```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Hack It Up v2 | Level 2</title>

<script async src="https://www.googletagmanager.com/gtag/js?id=UA-125937952-1" type="3409406a329e04ce48f275cf-text/javascript"></script>
<script type="3409406a329e04ce48f275cf-text/javascript">
        window.dataLayer = window.dataLayer || [];
          function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
          gtag('config', 'UA-125937952-1');
    </script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="css/style.css?v=1548737520">
</head>
<body>
<img id="logo" src="../../whhc.png"></div>
<img id="text" src="../../logov2.png"></div>
<div class="container">
<span class="txt anim-text-flow">Yeah Yeah! I know. Too easy right?</span>
<br>
<span class="txt anim-text-flow">Well. It won't be as easy this time.</span>
<br>
<span class="txt anim-text-flow">Up for the challenge?</span>
</div>
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js" type="3409406a329e04ce48f275cf-text/javascript"></script>
<script src="js/index.js" type="3409406a329e04ce48f275cf-text/javascript"></script>
<script src="https://ajax.cloudflare.com/cdn-cgi/scripts/2448a7bd/cloudflare-static/rocket-loader.min.js" data-cf-nonce="3409406a329e04ce48f275cf-"
</html>
```

CSS Source Code -

```
/*
 * Animation module with all animation code
 */
@import url(https://fonts.googleapis.com/css?family=Ubuntu:300);
.anim-text-flow,
.anim-text-flow-hover:hover {
  /*
   * I am right here eSeKaz
   */
  /*
   * Elements settings
   */
  /*
   * Keyframe loop
   */
  /*
   * Element animation delay loop
   */
}
```

Level 3:

Level 3 is easier than level 1 and 2 combined since now you know to check the source code and also what “Tags” in HTML are.

HTML SourceCode

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Hack It Up v2 | Level 3</title>

<script async src="https://www.googletagmanager.com/gtag/js?id=UA-125937952-1" type="f5504213935a87c32ff2c4b1-text/javascript"></script>
<meta></rCVhBr>
<script type="f5504213935a87c32ff2c4b1-text/javascript">
        window.dataLayer = window.dataLayer || [];
          function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
          gtag('config', 'UA-125937952-1');
    </script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="css/style.css?v=1548738946">
</head>
<body>
<img id="logo" src="../../whhc.png"></div>
<img id="text" src="../../logov2.png"></div>
<div class="container">
<span class="txt anim-text-flow">Let's Tag Along</span>
</div>
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js" type="f5504213935a87c32ff2c4b1-text/javascript"></script>
<script src="js/index.js?v=1548738946" type="f5504213935a87c32ff2c4b1-text/javascript"></script>
<script src="https://ajax.cloudflare.com/cdn-cgi/scripts/2448a7bd/cloudflare-static/rocket-loader.min.js" data-cf-nonce="f5504213935a87c32f
</html>
```

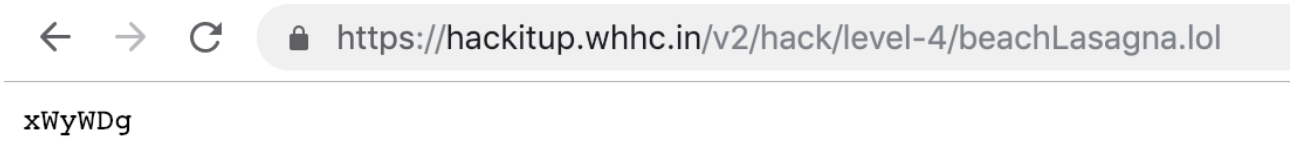
Level 4:

This level focuses more on the “Session/Tokens” stored as Cookies. Cookies are the basic storage used by the websites to store data in the browser eg:- when you login in Facebook, some tokens are stored in cookies which helps you to access the data from Facebook server. Hence having an access to check cookie is essential for the hackers.

You can access cookies by having an extension for your preferred browser. We have used an extension called “Cookie Inspector” for Google Chrome.

Name	Value	Domain	Size	Path	Expires (GMT)	H...	Se...
_gat_gtag_UA_...	1	.whhc.in	25 B	/	Tue Jan 29 201...		
_gid	GA1.2.81691327.1548736741	.whhc.in	29 B	/	Wed Jan 30 20...		
PHPSESSID	uh3vpf0gq4pfkhub70122fvr22	hackitup....	35 B	/	Session		
_ga	GA1.2.1996837459.1544411342	.whhc.in	30 B	/	Thu Jan 28 202...		
__cfduid	d0cb0a7233745dd3d32335270bdf4686d15444...	.whhc.in	51 B	/	Tue Dec 10 20...	True	True
JSESSIONID	beachLasagna.lol	hackitup....	26 B	/v...	Session		

Here a cookies name “JSESSIONID” is the one which will grab the attention due to this value “beachLasagna.lol”. Now since their is an extension to this value which is “.lol”, it indicates that it is a file, so simply access the file by copy pasting the filename in the address bar.



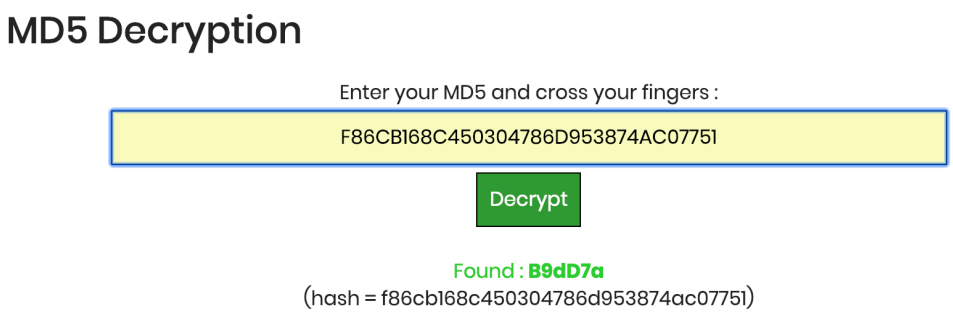
xWyWDg

Level 5:

This level deals with basic hashing algorithms. A hashed value is displayed on the screen. Now just check the source code and you will find the type of hashing as well as the tool required to find the value (De-Hash).

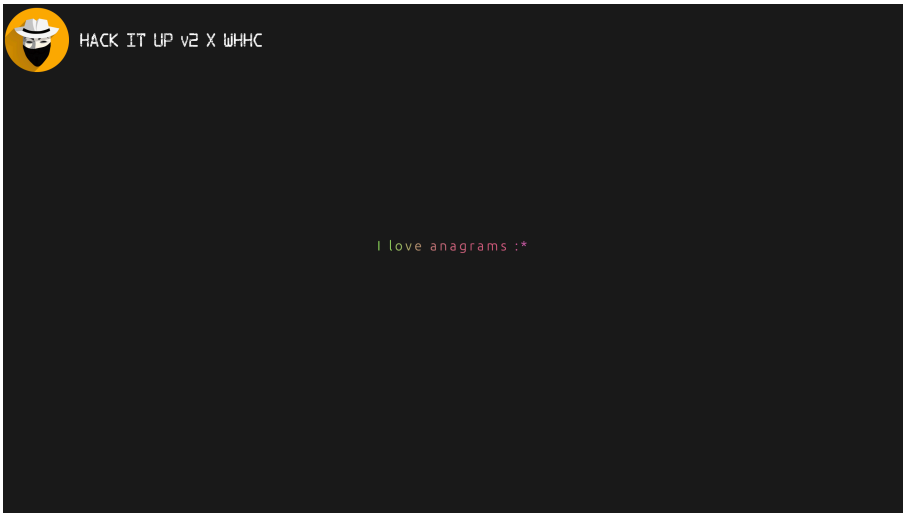

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Hack It Up v2 | Level 5</title>

<script async src="https://www.googletagmanager.com/gtag/js?id=UA-125937952-1" type="32d75103a757d15237b4e91c-text/javascript"></script>
<script type="32d75103a757d15237b4e91c-text/javascript">
        window.dataLayer = window.dataLayer || [];
          function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
          gtag('config', 'UA-125937952-1');
    </script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="css/style.css?v=1548740405">
</head>
<body>
<img id="logo" src="../../whhc.png"></div>
<img id="text" src="../../logov2.png"></div>
<div class="container">
<div class="tryThi">https://passwordsgenerator.net/md5-hash-generator </div>
<span class="txt anim-text-flow">F86CB168C450304786D953874AC07751</span>
<br />
<span class="here"></span>
</div>
<style>
```

Now we know that it is a MD5 hashed value, and our token is about 6 character long, MD5 is not very strong hashing tool for such short value, Hence most of the online tool for De-Hashing the tokens are easily available.



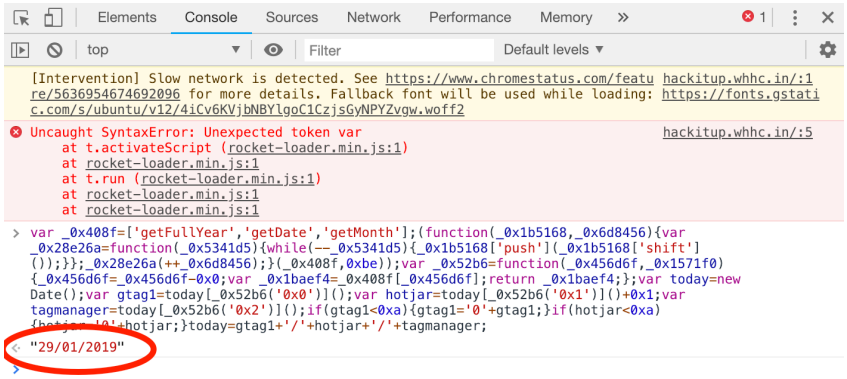
Level 6:

Level 6 is an easy level, Just go to source code and check the clue related to “Anagram”. Anagram is rearranging the letters of a word. You will see a word “notek” which is anagram for “token”, now there is code followed by that word. Which is your next clue. Since it is JS code, you have to run it your browser’s console, which can be accessed by right clicking and tapping on “Inspect”.




```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Hack It Up v2 | Level 6</title>

<script async src="https://www.googletagmanager.com/gtag/js?id=UA-125937952-1" type="ac6fb5ace0cfe64b91ae5f97-text/javascript"></script>
<script type="ac6fb5ace0cfe64b91ae5f97-text/javascript">
        window.dataLayer = window.dataLayer || [];
          function gtag(){dataLayer.push(arguments);}
          gtag('js', new Date());
          gtag('notek', var _0x408f=['getFullYear','getDate','getMonth'];(function(_0x1b5168,_0x6d8456){var _0x28e26a=function(_0x5341d5){while(--_0x5341d5){_0x1b5168['push']
(_0x1b5168['shift']());}};_0x28e26a(++_0x6d8456);}(_0x408f,0xbe));var _0x52b6=function(_0x456d6f,_0x1571f0){_0x456d6f=_0x456d6f-0x0;var _0x1baef4=_0x408f[_0x456d6f];return
_0x1baef4;};var today=new Date();var gtag1=today[_0x52b6('0x0')]();var hotjar=today[_0x52b6('0x1')]()+0x1;var tagmanager=today[_0x52b6('0x2')]();if(gtag1<0xa)
{gtag1='0'+gtag1;}if(hotjar<0xa){hotjar='0'+hotjar;}today=gtag1+'/'+hotjar+'/'+tagmanager;)
          gtag('config', 'UA-125937952-1');
    </script>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="css/style.css?v=1548741538">
</head>
<body>
<img id="logo" src="../../whhc.png"></div>
<img id="text" src="../../logov2.png"></div>
<div class="container">
<span class="txt anim-text-flow">I love anagrams :*</span>
<br />
<span class="here"></span>
</div>
<style>
```

Once you run this code in your console, you will see today’s date, which is your **token**.

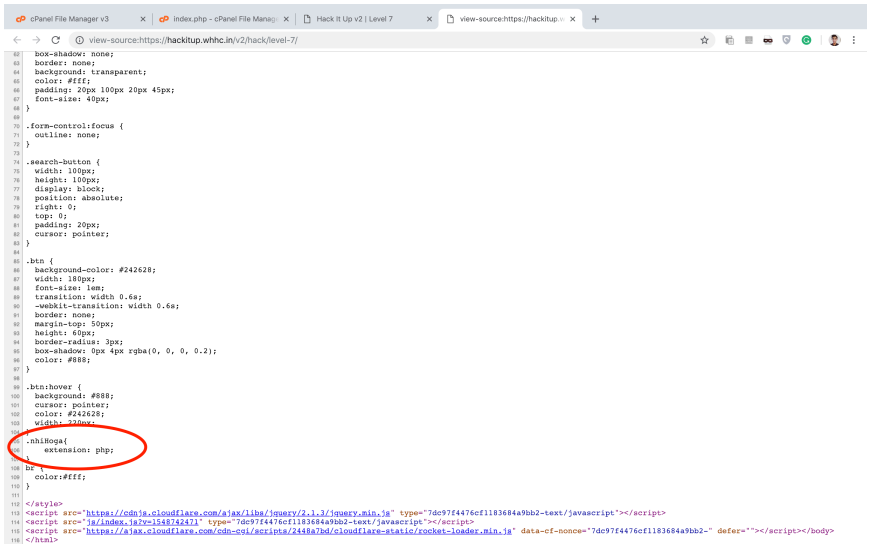


Level 7:

This is most trickiest level till now and it tests your knowledge which you learned in previous levels.

The text shown on the screen is “send as a post”, which means you have to send a **POST** request, hence you have to use **Postman**, But you will require a link on which you have to send a POST request.

Check in source code, you will find an unusual class name “nhiHoga” consisting of an attribute “extension:php” which is the link to which you to send a POST request.



Now when you send the POST request via Postman, the response will be, “Invalid Session”, hacker will check for the headers to see if there is any loophole in host’s system.

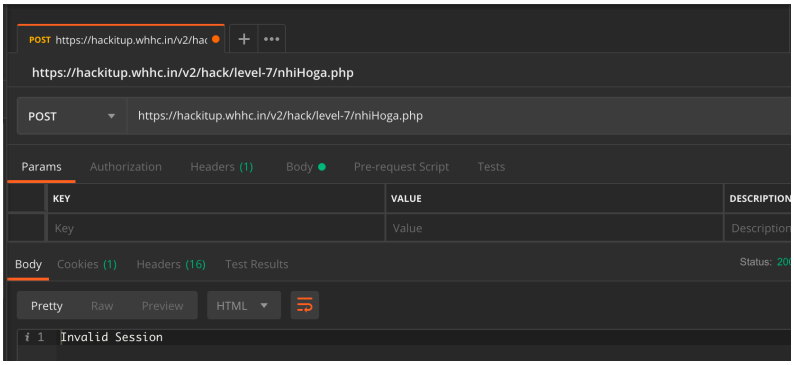
In HEADERS there are multiple clues like the field name session has a value “Of course I need a cookie man. You think i'm gonna let you get pass without it?”, Which means that you have to set a **cookie** and then fire a request. But for setting a cookie requires a **Key** and a **Value**.

When you check the “cookie” field,

The value if “level-current = Encrypted Fish

(Wx3SKXKeQWynsCLcKnzfpr1HYgeG/DFL)”,

which means **Key** is level-current, that is **level-7.**

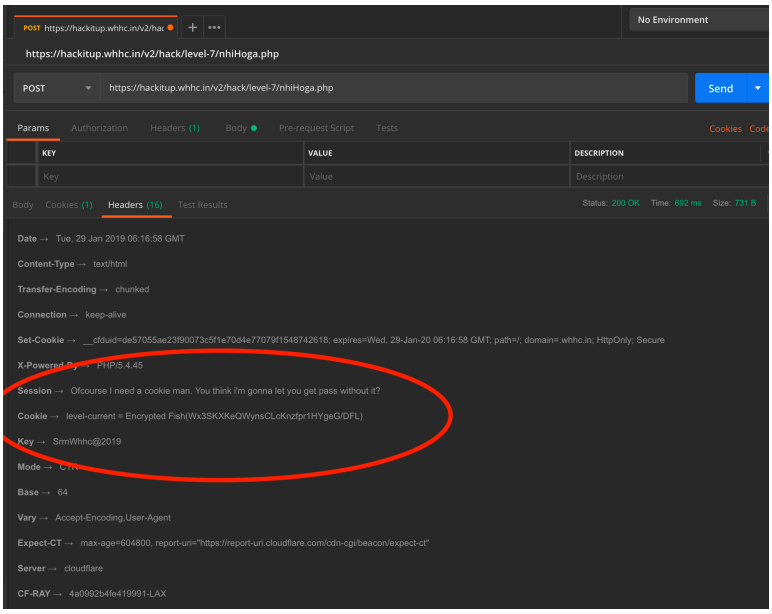


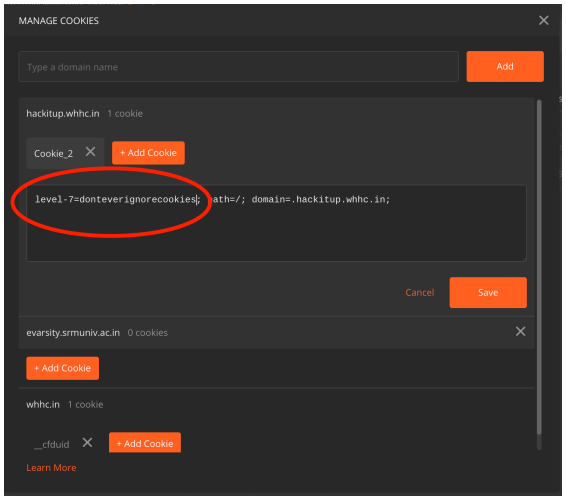
Now for the Value we have a random string encrypted by something called Fish, which indicates the BlowFish Algorithm. So go to any online tool for decrypting the code, and it which ask for a decryption key which is again given in the HEADERS as a filed called ”**Key**” whose value is “**SrmWhhc@2019**”, use that and decrypt it.

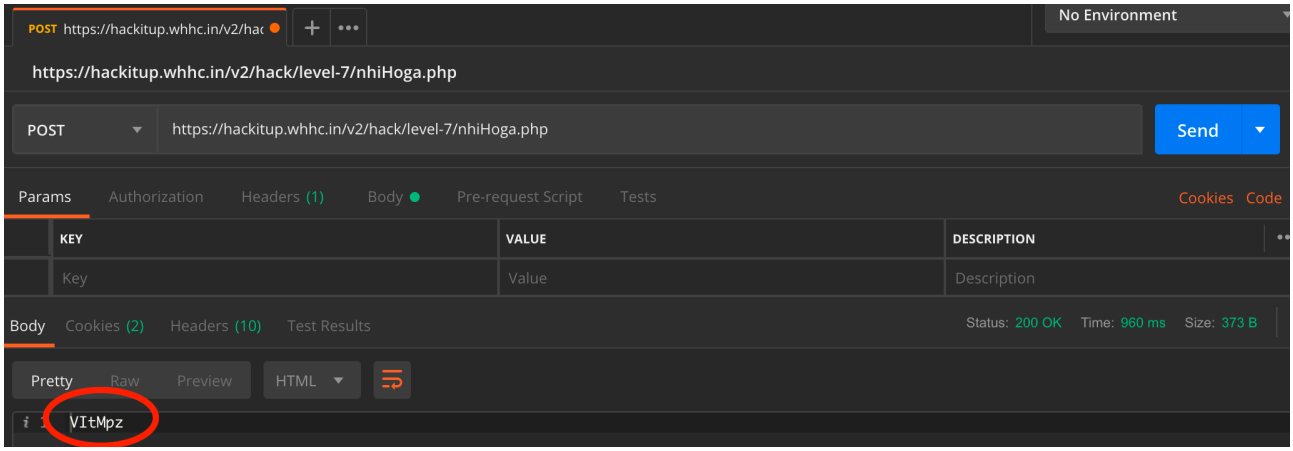
Once you decrypt it, you will receive the value as “**donteverignorecookies**” (which you should).

Now just a click on orange text named “**Cookies**” just below the Send button, and click on “Add Cookie”. Set the key as “**level-7**” and value as “**donteverignorecookies**” and save it.

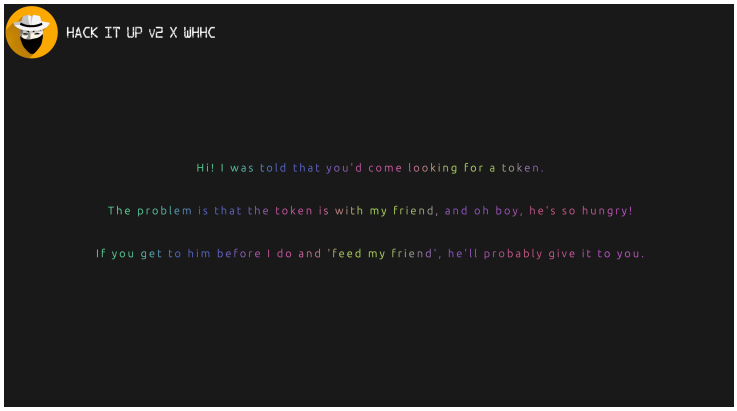
Last step is to send a the same POST request and check the body, there was your token.





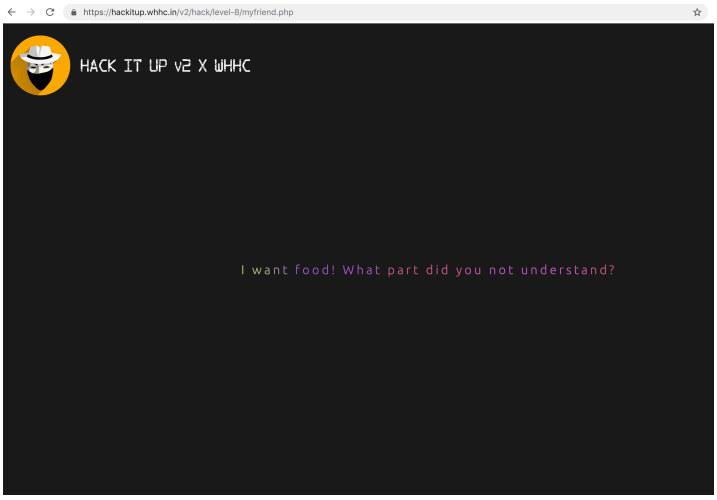


Level 8:



Level 8 is easier in terms of technicality, but hints and clues where hidden in such a way that it was harder for the participants to find them. It starts with massage which says about food, hence it is about he cookie also a hidden message behind it was the GET request mentioned in the third line. Check the second image, you will see a cookie named “food” having a value

“KQxAKtsZUd”.

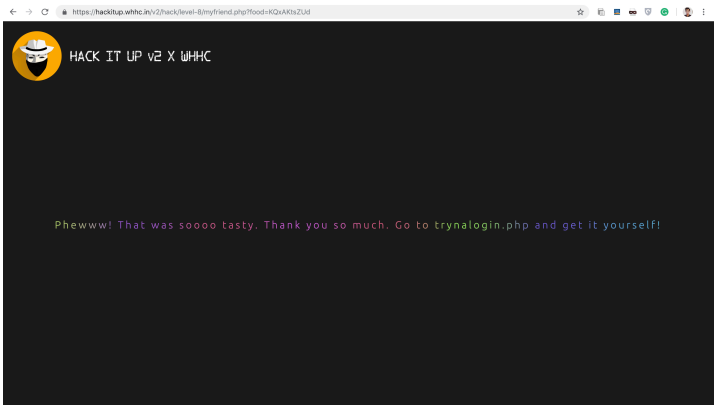


When you send a GET request on the same link it won’t work, read the message again it guide you to the file name on which you have to send a GET request. File name is “myfriend”.

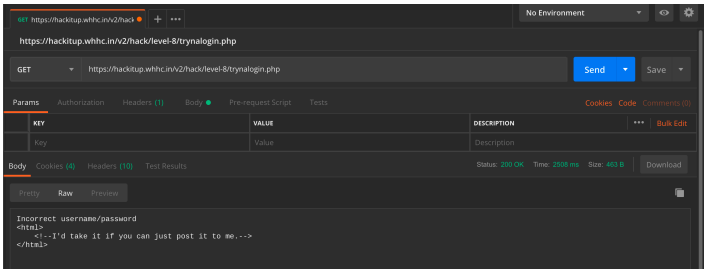
If you send a GET request on myfriend.php”, it will show you the message as “I want food! What part did you not understand?”.

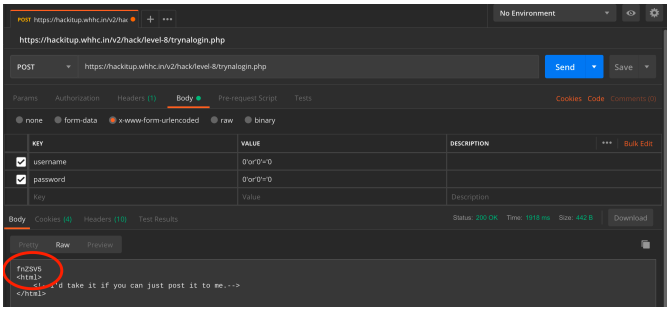
Now send a GET request with a parameter as “food” whose value should be “KQxAKtsZUd”.

This will give you one more file name “trynalogin.php”.



Now this indicates a login page, so goto Postman and hit a GET request on myfriend.php, a message will be displayed, which is “I'd take it if you can just post it to me”, which means that we have to send a POST request. So on firing a POST request we will receive another massage as “Incorrect username/password”, which means we have to pass two params i.e username and password and since we don’t know their value, it should be a SQL-Injection attack. Hence pass two params with any kind of SQL-Injection query and hit the send button, your token will be in the response body.





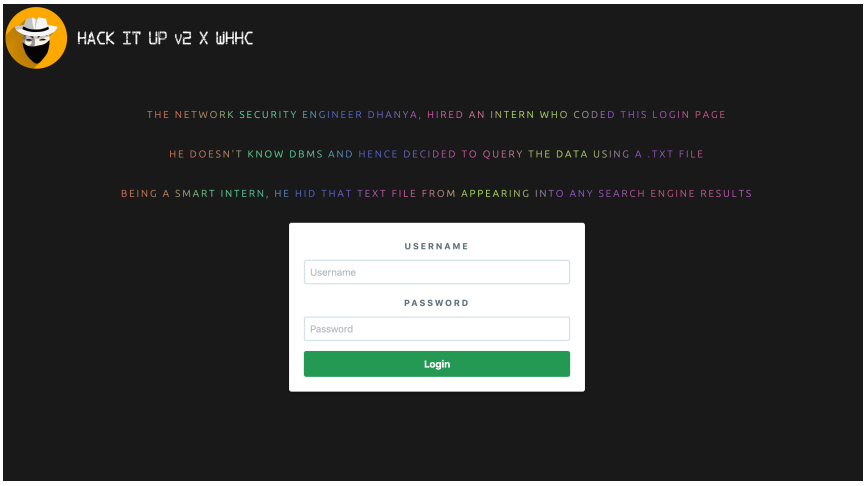
Level 9:

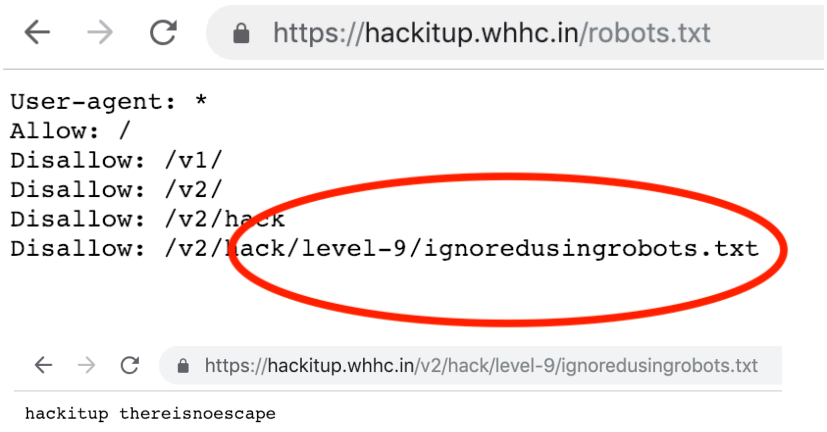
This levels deals with how search engine reads the website. The message displayed on the main page indicates that SQL injection won't work since the password and username is stored in text file.

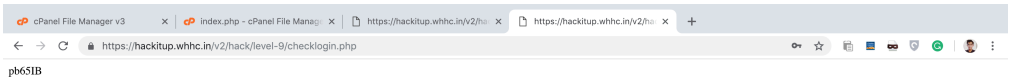
Now a file name "robots.txt" which is stored in the root directory of the website, handles the visibility of the file and directory to be shown in the search results.

So goto to the robots.txt and there you can see the directory of the text file you want to access i.e "**ignoredusingrobots.txt**".Now go to that file and you will see the username and password.

Now username is "hackitup" and password is "thereisnoescape". Once to set them and click on Login, You will receive the token.





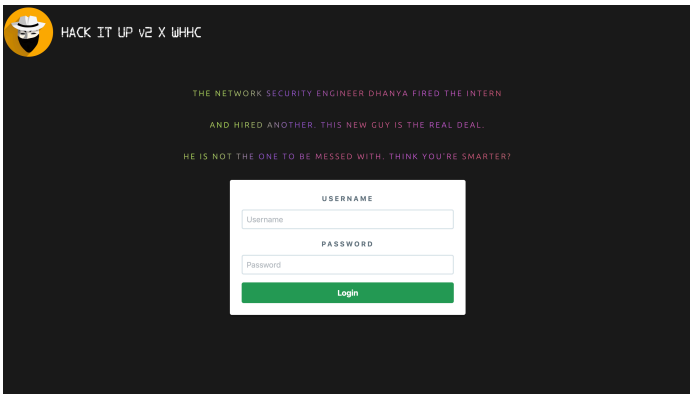


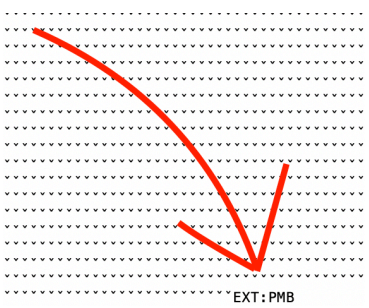
Level 10:

For this level, go to source code, you will find a link to “**level10.txt**” a file will be downloaded.

Once you open the file some gibberish characters will be shown, but at the end of it there was a clue i.e “EXT:PMB”, which indicates that you have to change the extension to bitmap i.e **.bmp** and you will have the login credentials.

Login with those credentials and you would have cleared all the rounds. Cheers!





Username: steganography

Password: isimportant