Sri Lanka Institute of Information Technology

Information Security Project

Catch The Fish

Walkthrough and Demonstration

IT18119336 - Lokuge P.M.K.

IT18127492 – Somasiri J.P.A.K.

Introduction

A CTF (Capture The Flag) is a competition that takes major disciplines of information security and makes them into smaller, objectively measurable exercises. Participants may attempt to solve challenges by solving, exploiting, or breaking. This CTF event mainly focus on vulnerability assessment and penetration testing skills.

Jeopardy, Attack defend and mixed are the types of CTFs.

In Jeopardy there are puzzles and we have to solve the puzzle to acquire the toke or the flag. The flag may be hidden inside the text file, folders, or images etc. These challenges may include OWASP Top 10 vulnerabilities, or any other misconfiguration.

Attack defend type focuses on either attacking the opposite side or defending the own.
The combination of both attack defend and Jeopardy is known as the mixed type of CTF.

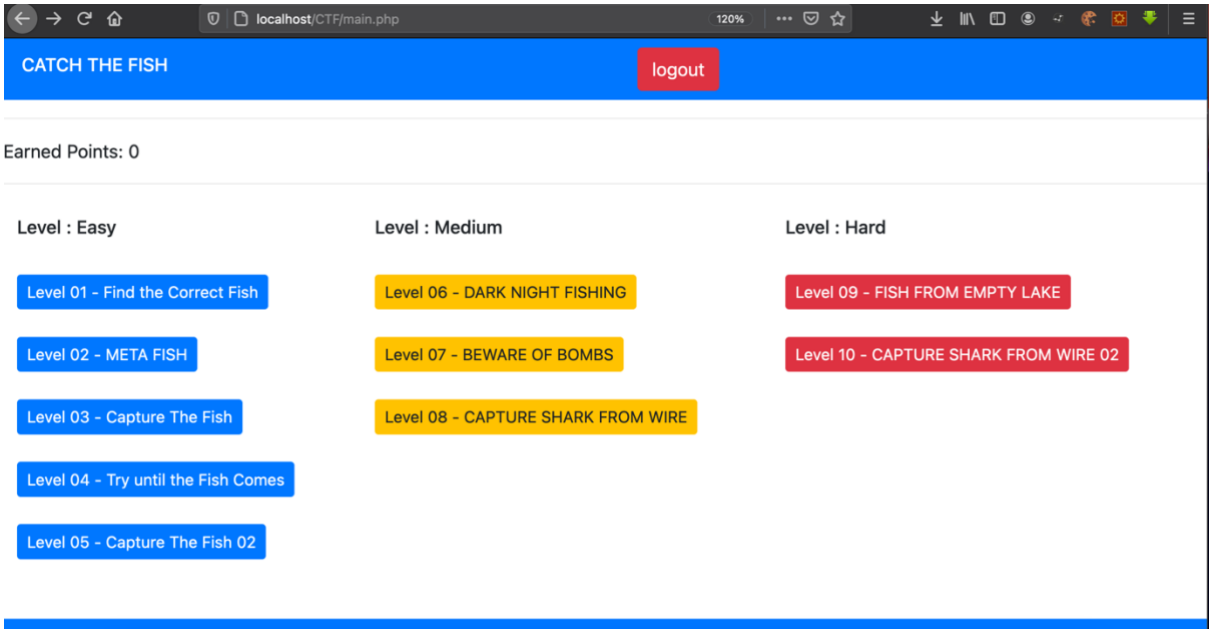
Further we can categorize CTF as web, forensics, miscellaneous, networking, reversing, pwn/exploit. CTF challenges may cover many viewpoints of cyber security such as reverse engineering, binary analysis, mobile security etc.

Computer security students can have benefit from applying security tools and defend vulnerable systems. Working on pre-defined hacking challenges gives common practice on security education. CTF challenges may help us to gain the ability to vulnerability scanning and pen testing.

Requirements

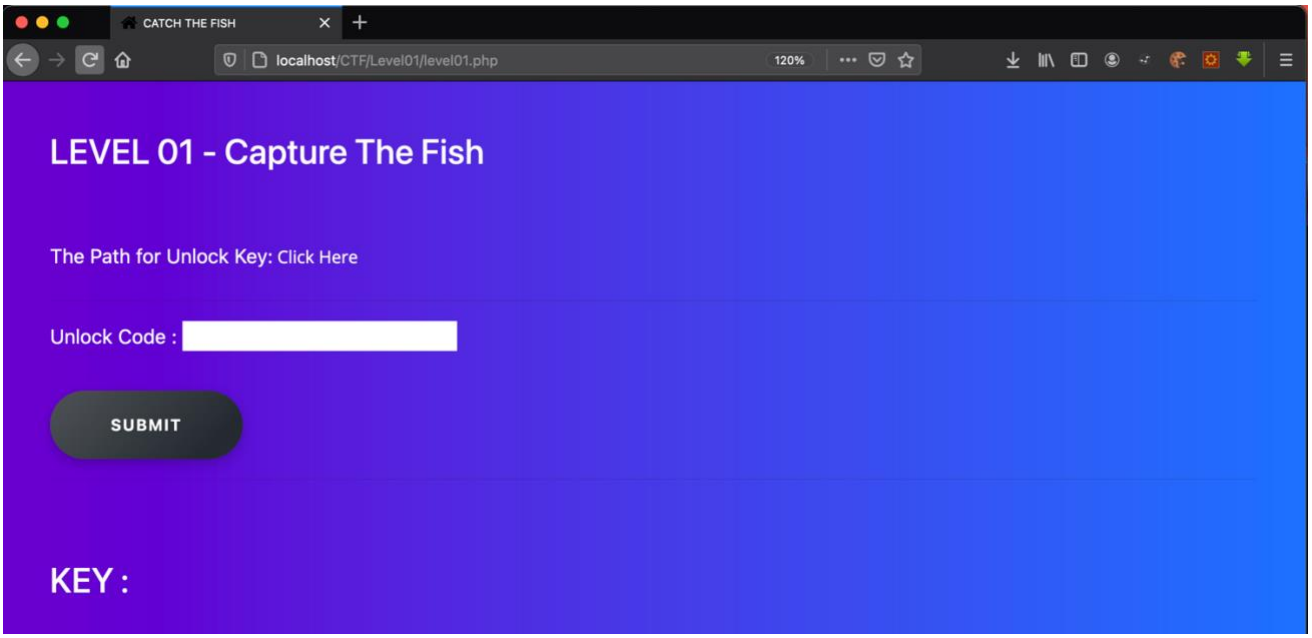
Windows 10 64bit OS / Kali Linux
Internet Connection
Basic ethical hacking knowledge
Stegnography / crypto Tools

Walkthrough

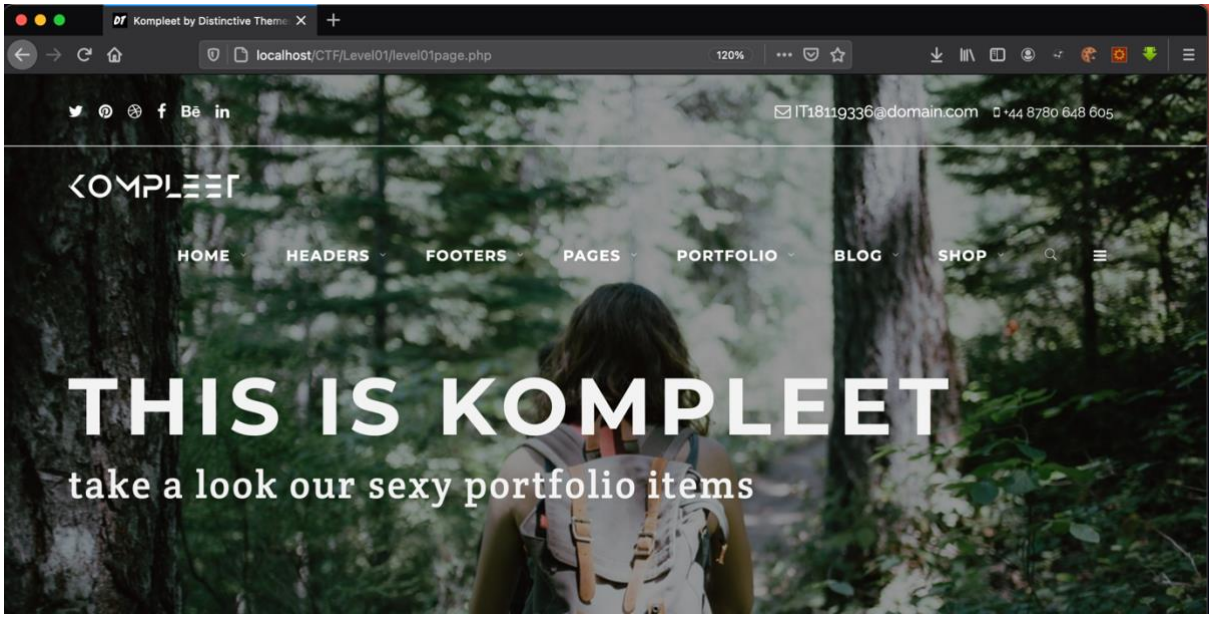


LEVEL 01 - Find The Correct Fish

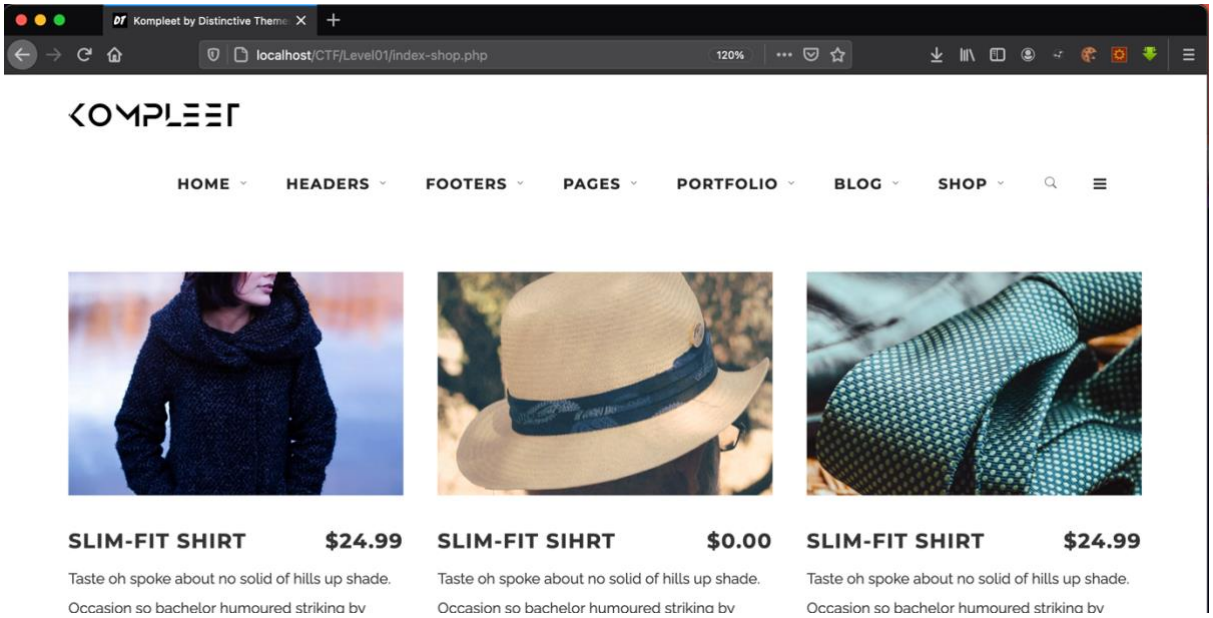
This Level is the Easiest implementation which user can get the Code Easily.



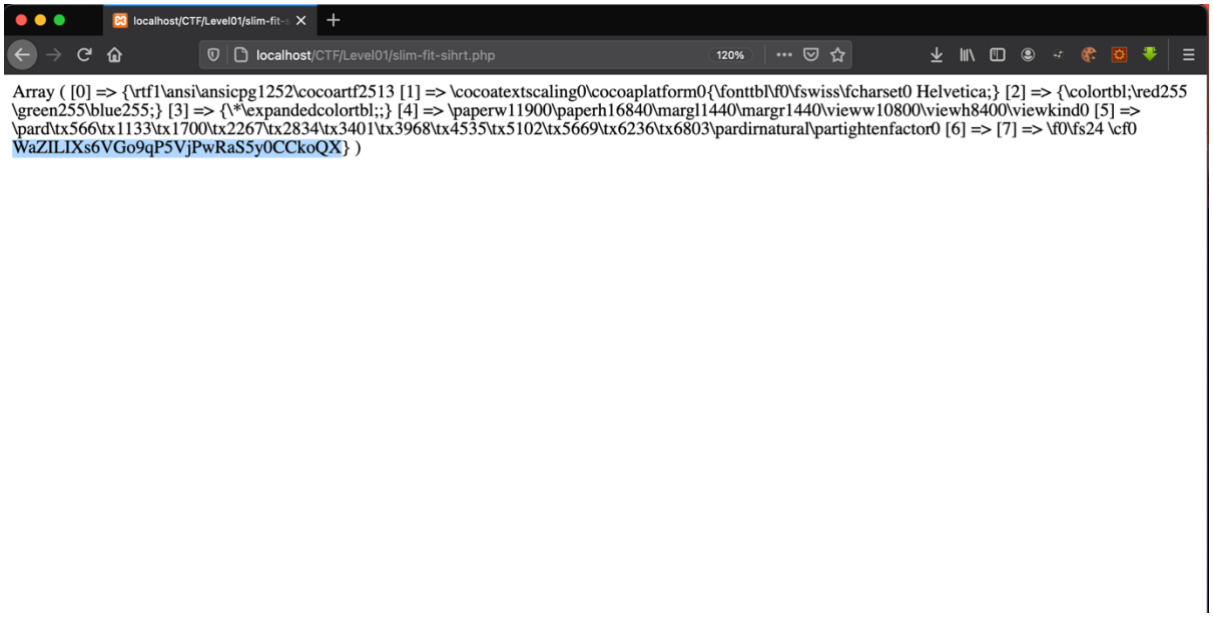
User Need to click here link for the game which the Unlock code is embedded.

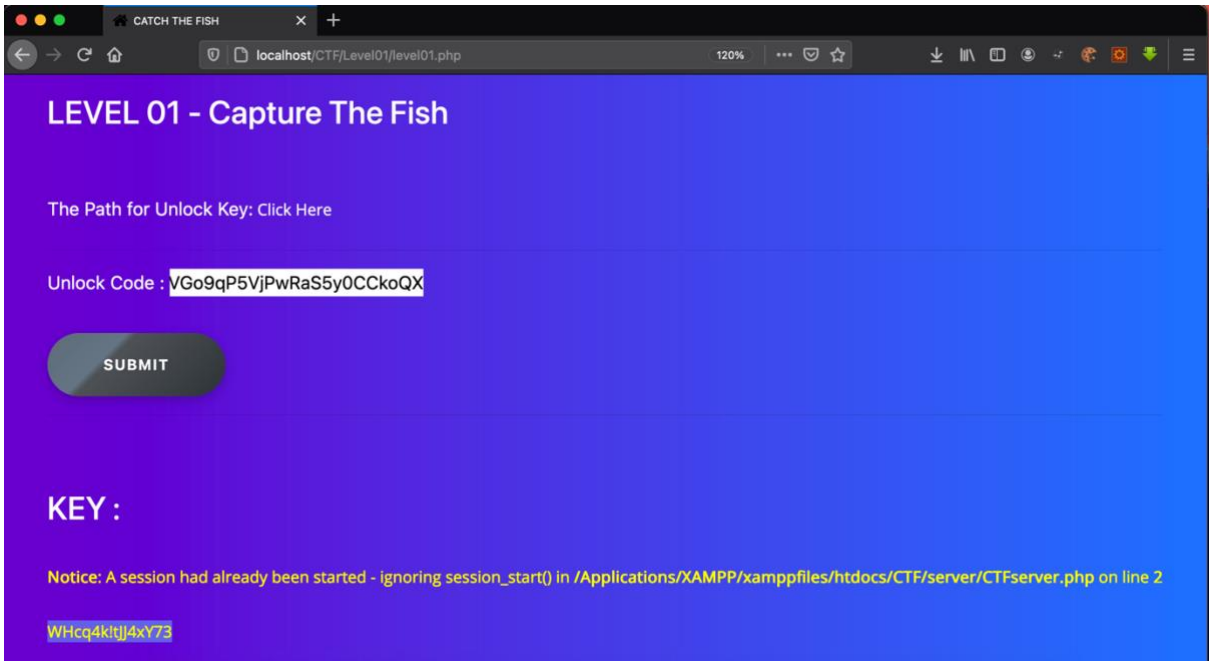


User need to identify the correct different image and open to get the code.

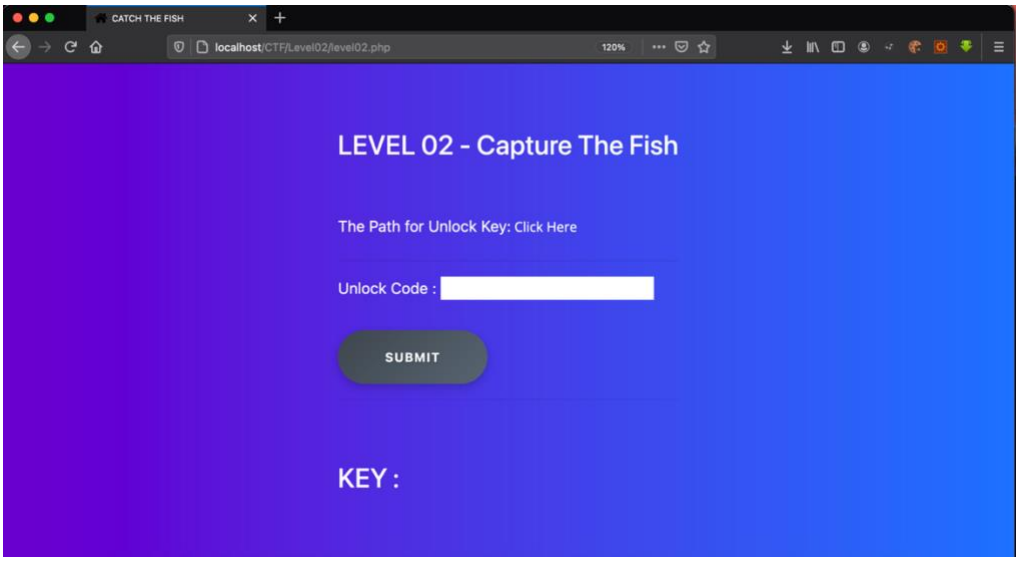


That’s all! You need to enter the correct unlock code to receive secret key for the next Level.

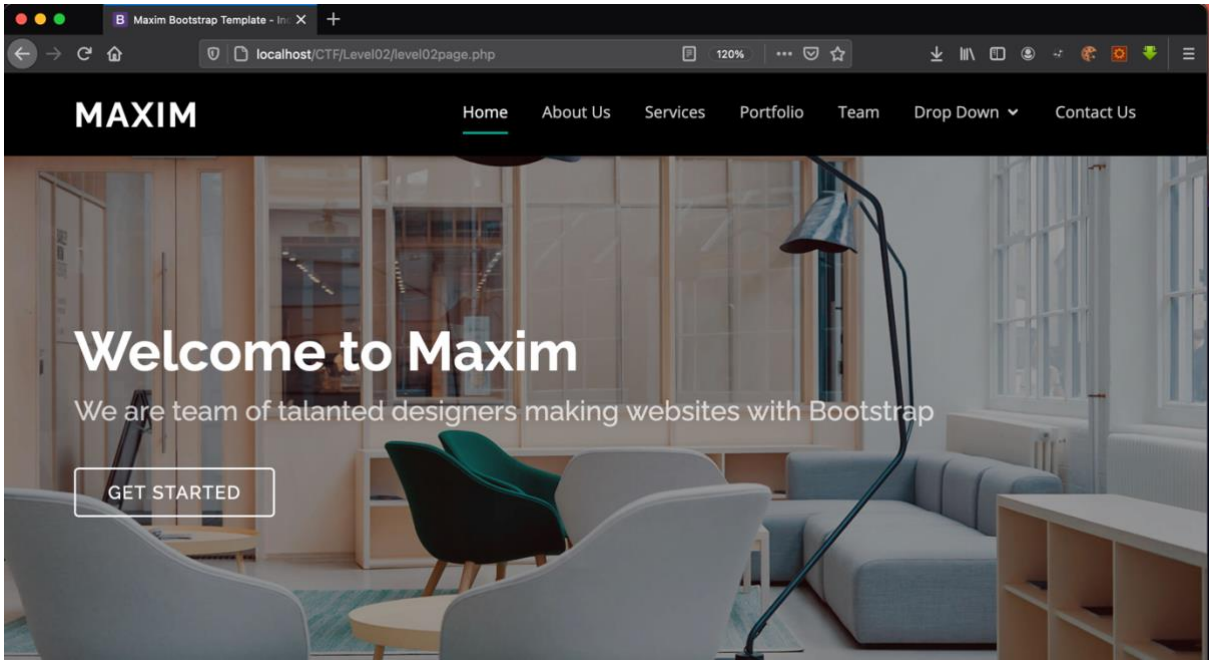




Level 02 - META Fish

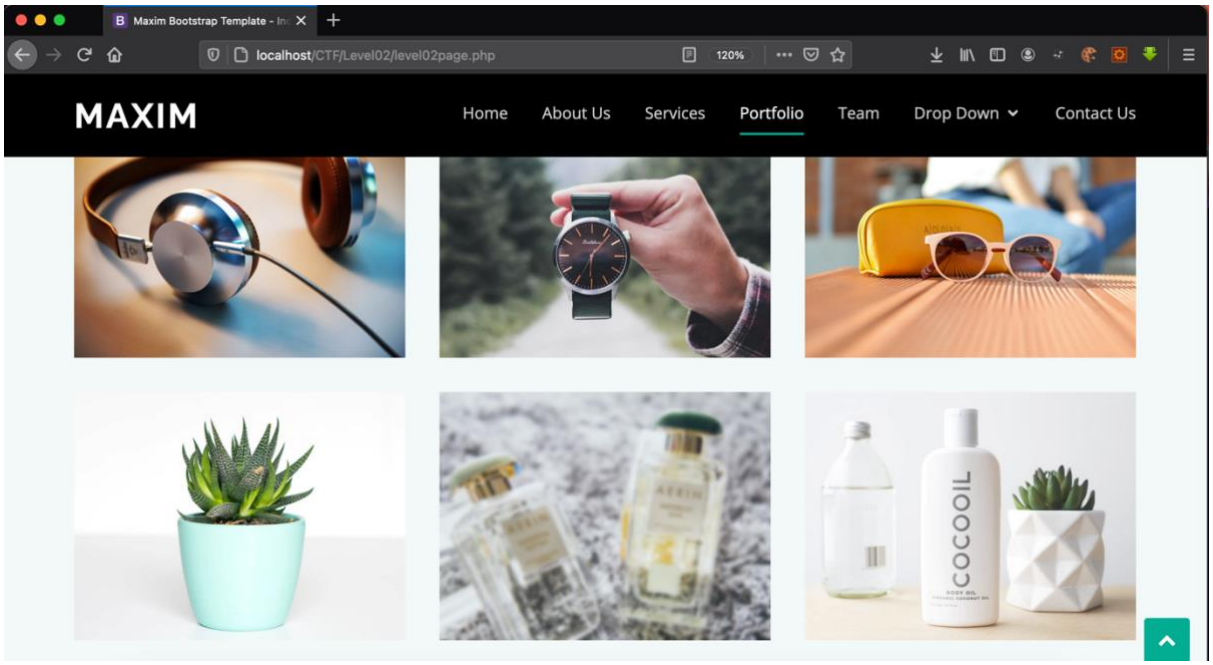


In this Level User need Some knowledge about metadata of image and what are the tools which needs to be get to extract data from unknown sources.

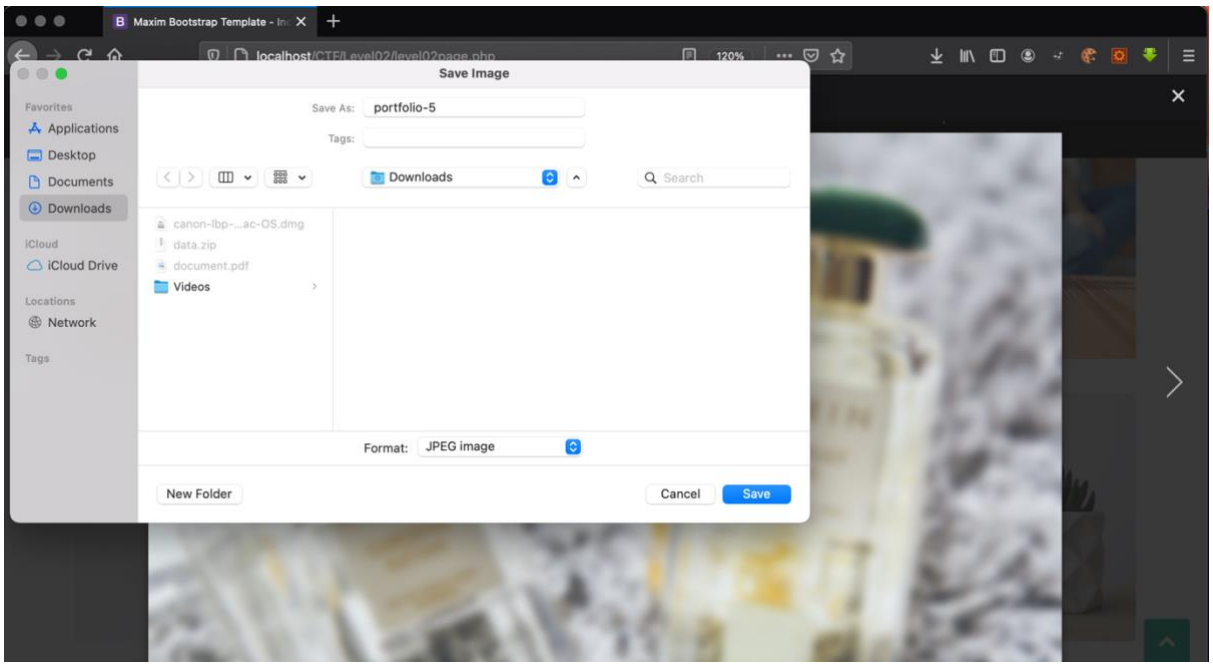


User must be intelligent to find the abnormal object in the webpage and investigate the object.

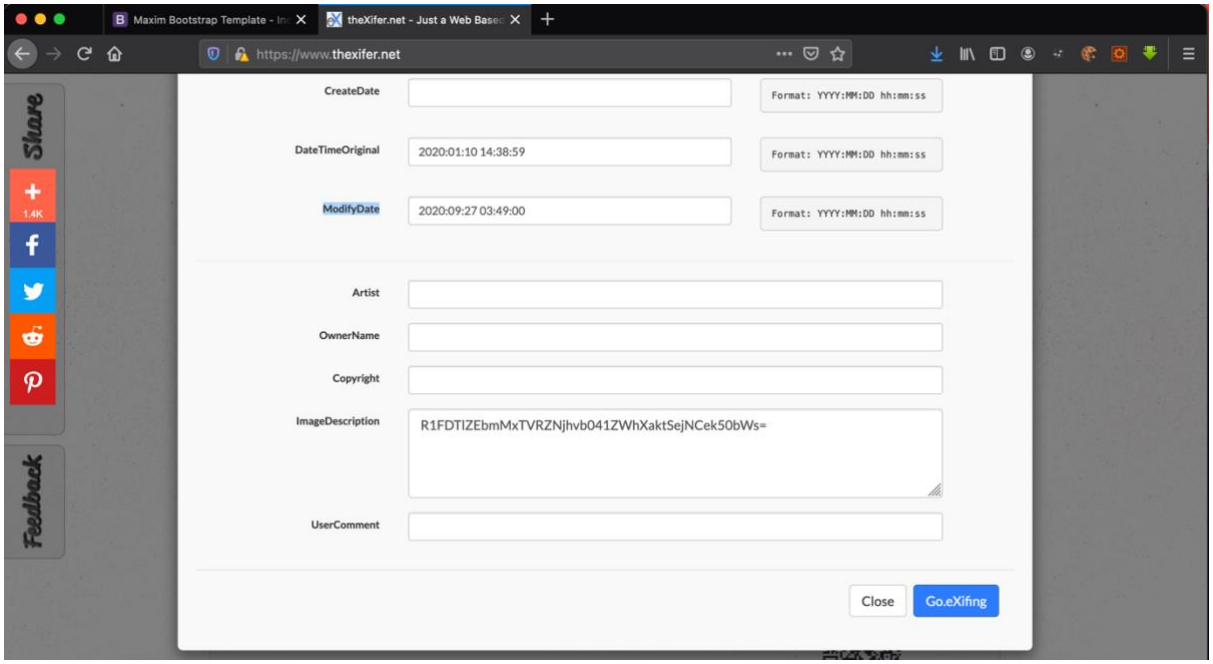
In here there is an image which cannot be seen clearly (Blurred) that user can be determined as a hint for the key.



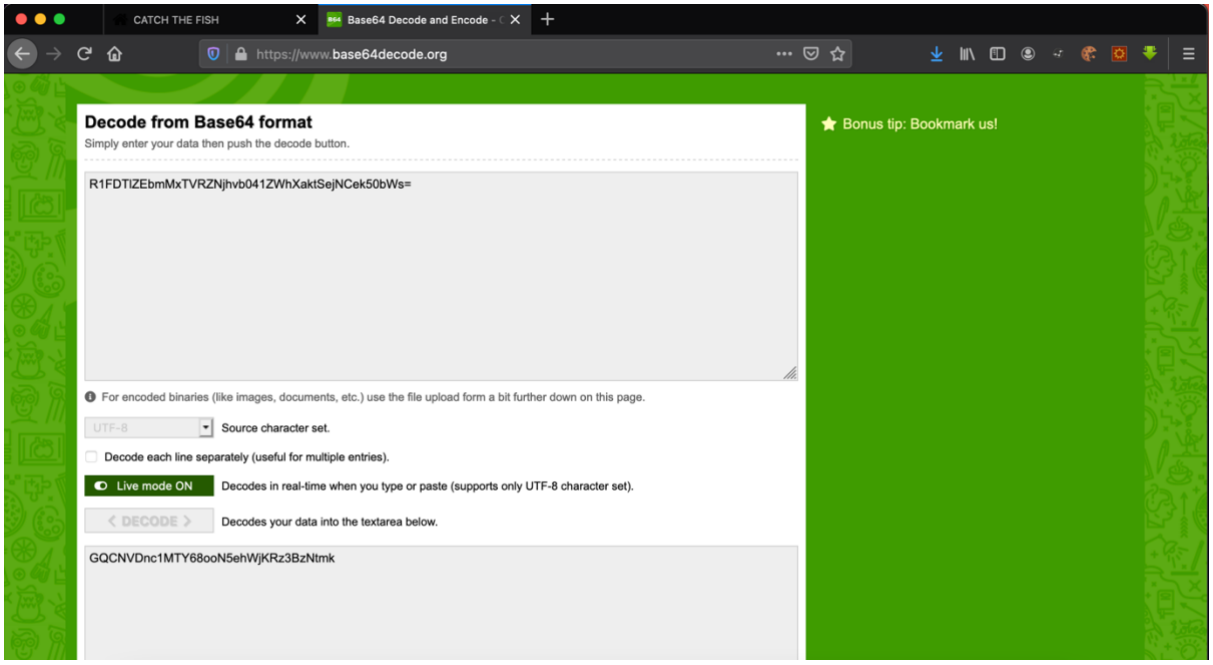
User need to download the relevant image to investigate data.



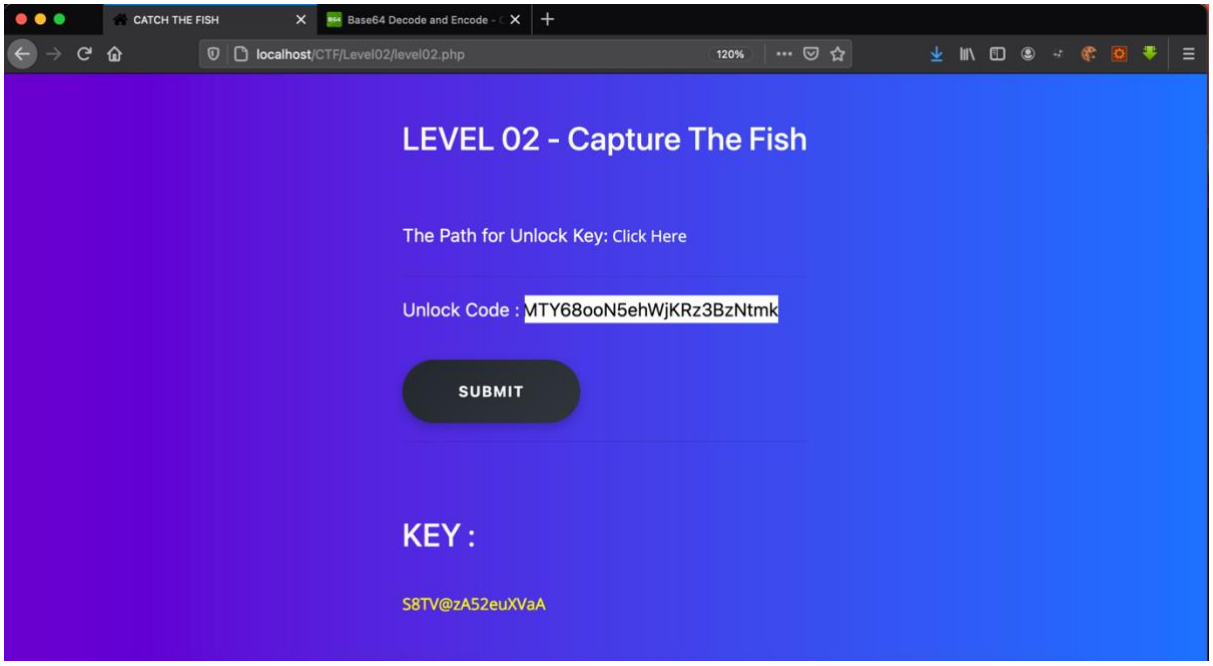
In here, We are using exiftool online for demonstration



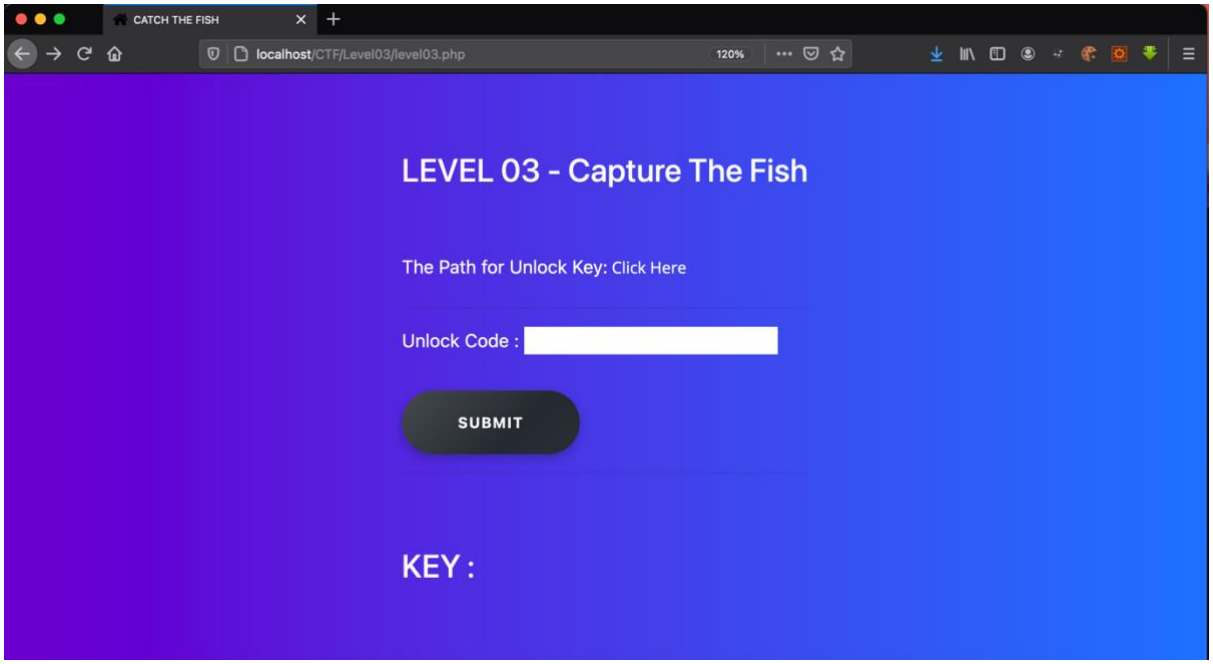
Use Base64 Decoding tool to test whether the code giving unlock code


CATCH THE FISH
Base64 Decode and Encode -
https://www.base64decode.org
Decode from Base64 format
Simply enter your data then push the decode button.
R1FDTlZEbmMxTVRZNjhvb041ZWhXaktSejNCek50bWs=
Bonus tip: Bookmark us!
For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.
UTF-8
Source character set.
Decode each line separately (useful for multiple entries).
Live mode ON
Decodes in real-time when you type or paste (supports only UTF-8 character set).
DECODE
Decodes your data into the textarea below.
GQCNVDnc1MTY68ooN5ehWjKRz3BzNtmk

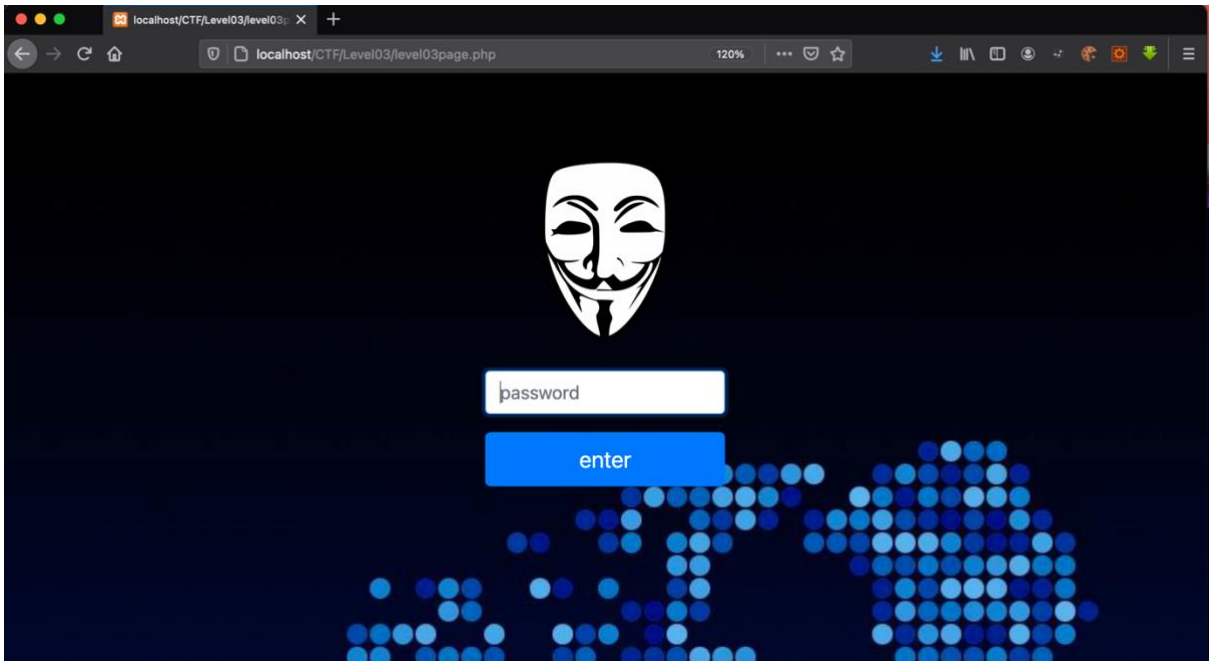
Done


CATCH THE FISH
Base64 Decode and Encode -
localhost/CTF/Level02/level02.php
120%
LEVEL 02 - Capture The Fish
The Path for Unlock Key: Click Here
Unlock Code : MTY68ooN5ehWjKRz3BzNtmk
SUBMIT
KEY :
S8TV@zA52euXVaA

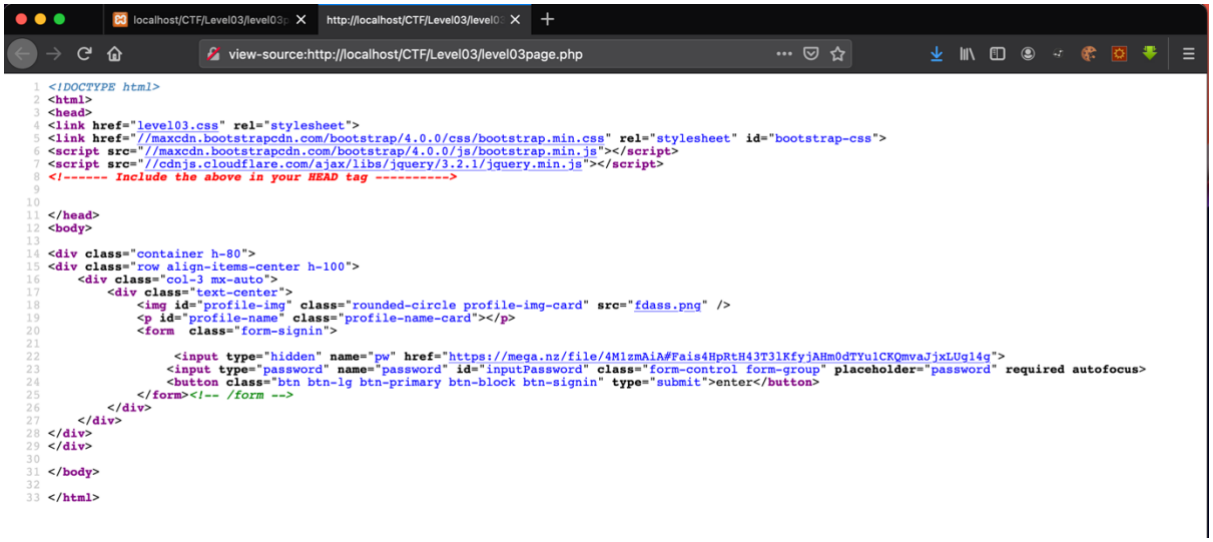
Level 03 - Capture The Fish



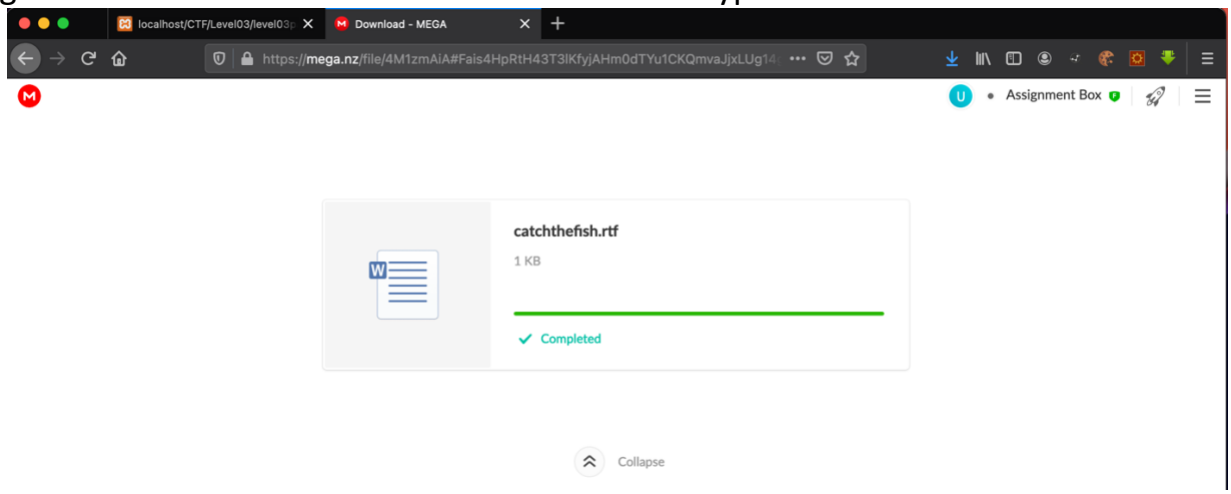
In Level 03, The link will redirect to a page where a credential page user need to find the password to enter into next step.

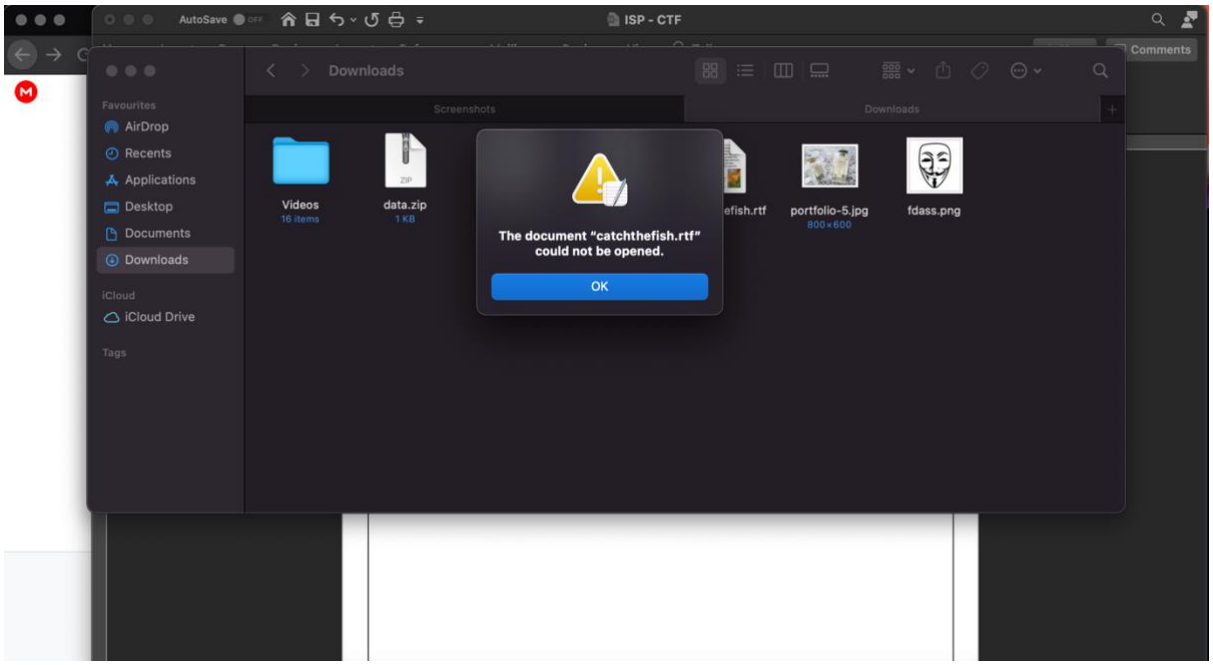


The hint we got is on the page source which can be see a hidden input with a link. User need to enter the link and move further on.

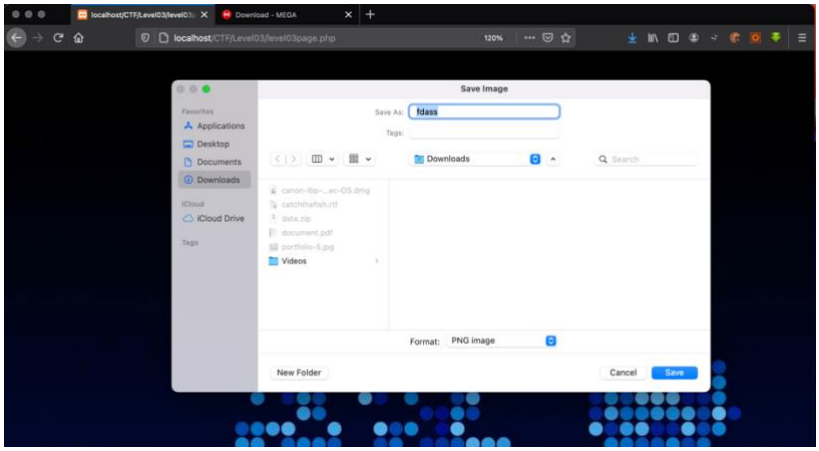


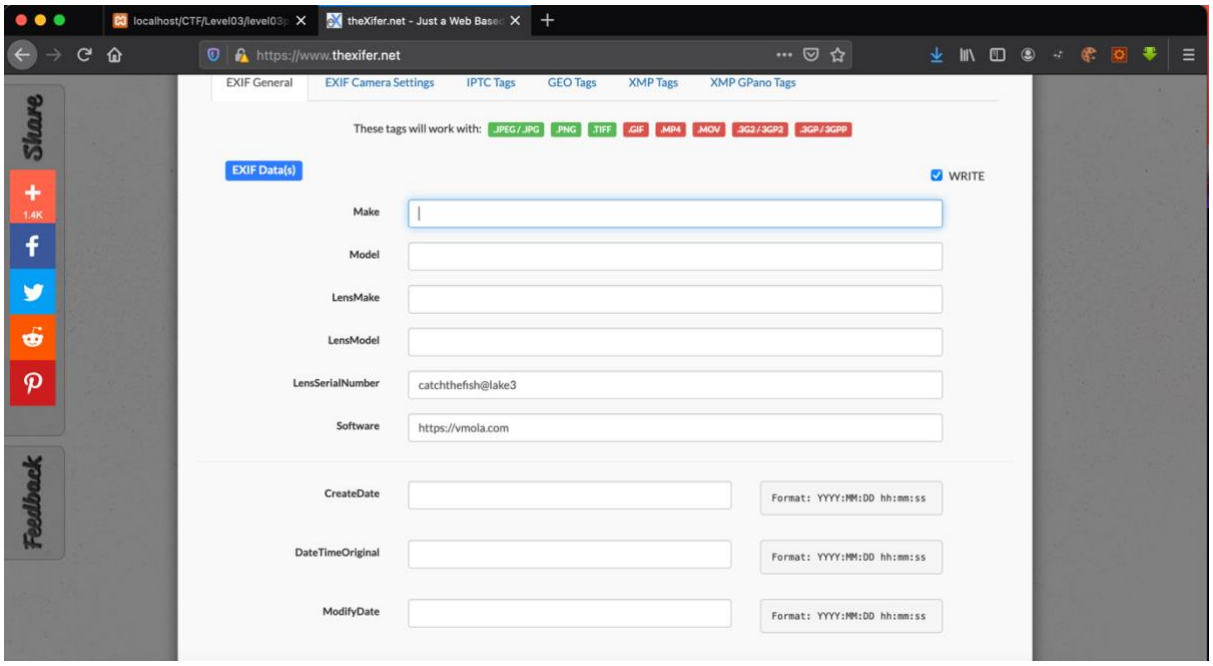
User gets an RTF file to download but the File is encrypted.



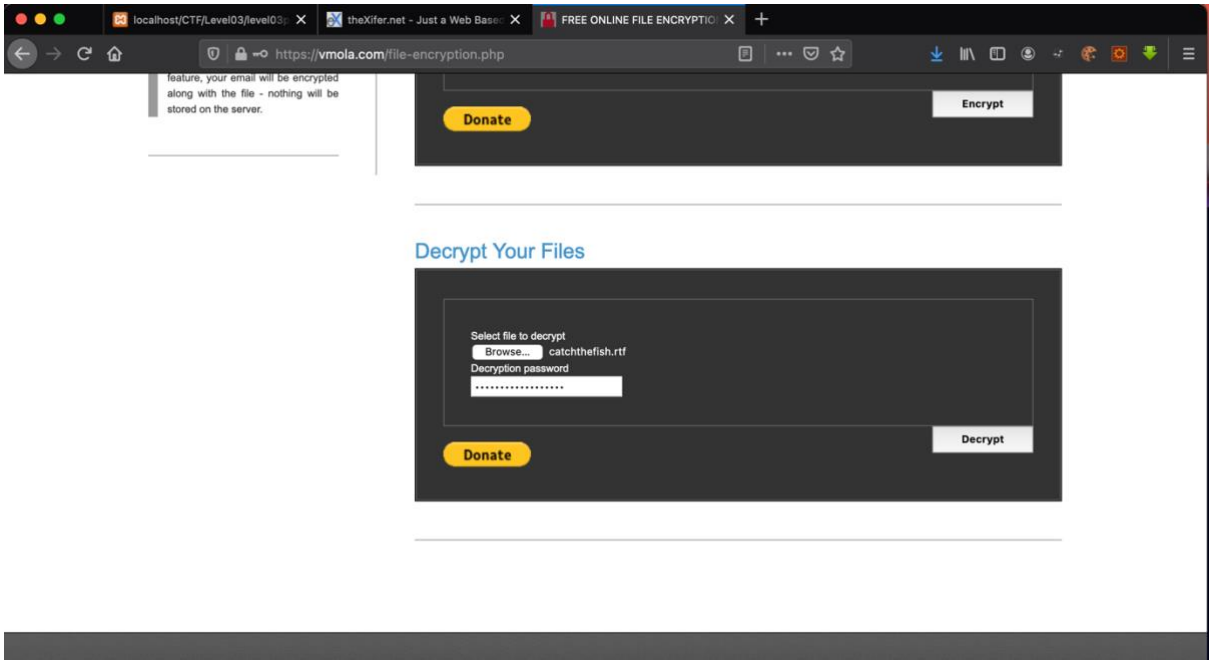


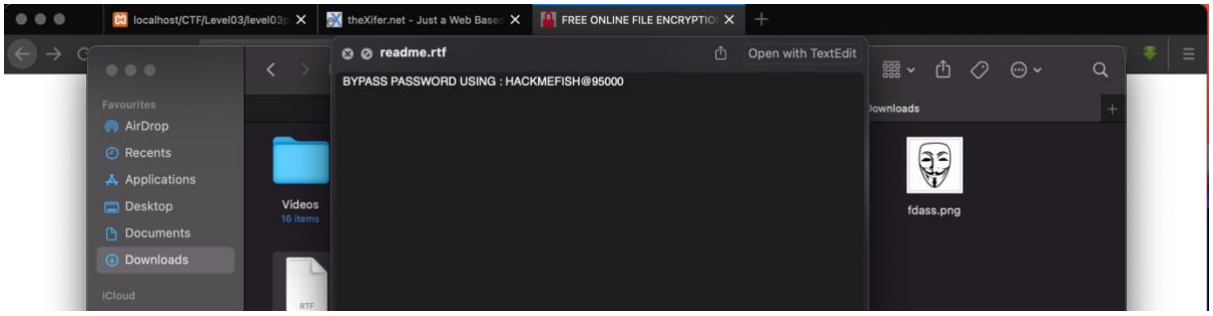
User need to find a way to decrypt the file. The Hint can be seen on the Hacker Face which need to be downloaded and investigate its data.



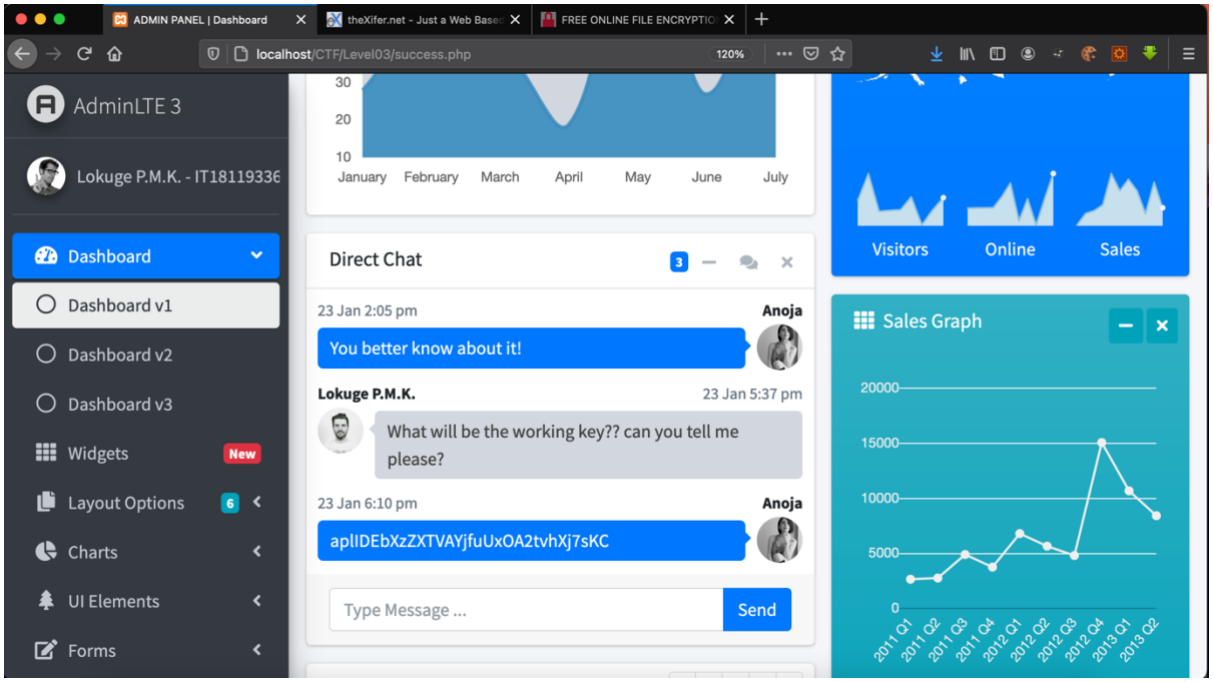


Here we can see a link with Decryption Key to Decrypt the RTF File.

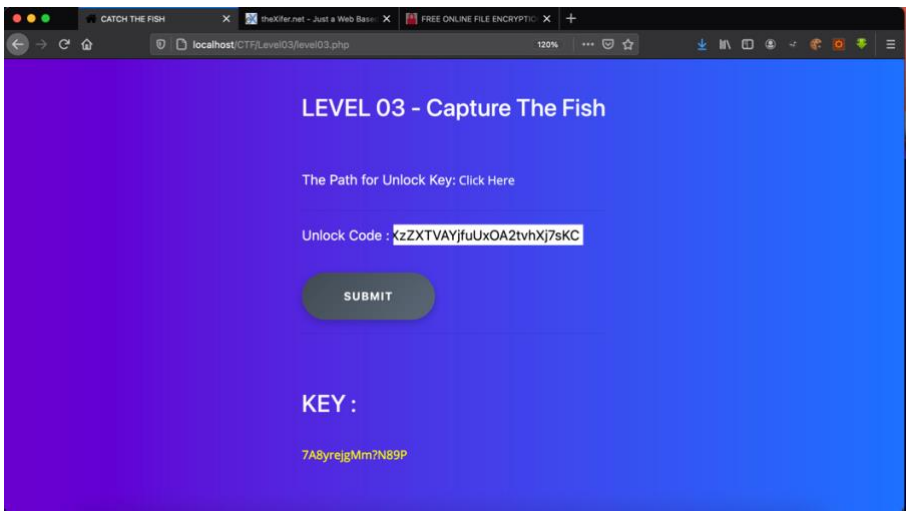




After Entering Password, We can enter into an admin panel view. When user see carefully. We can see a chat which exchanges unlock code between 2 users.

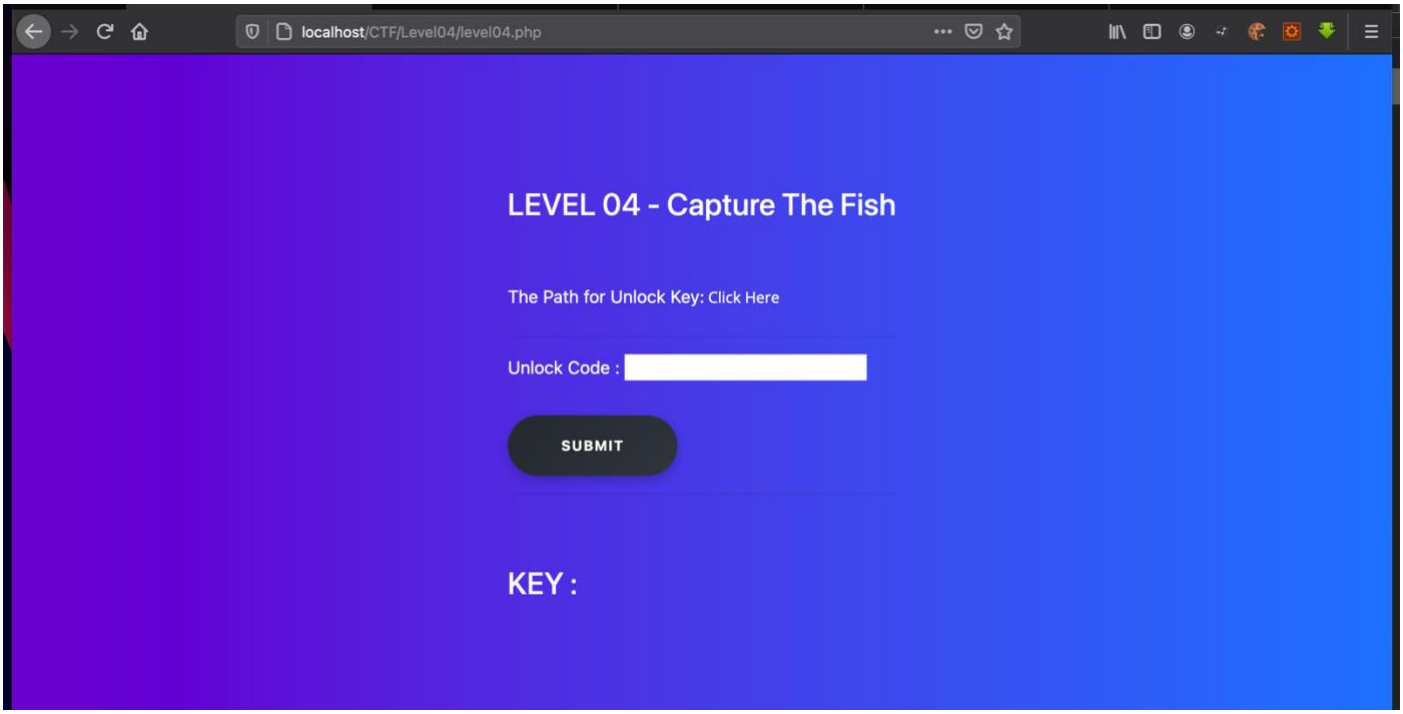


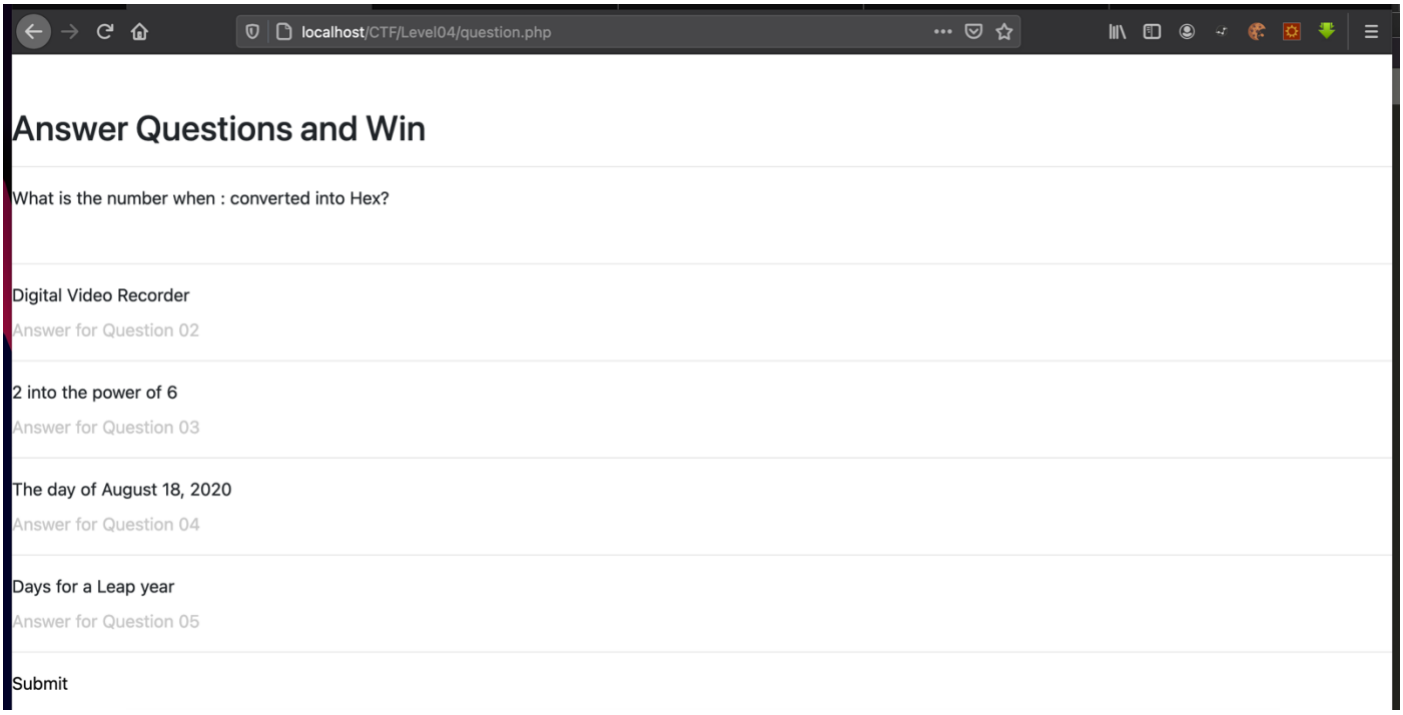
Done

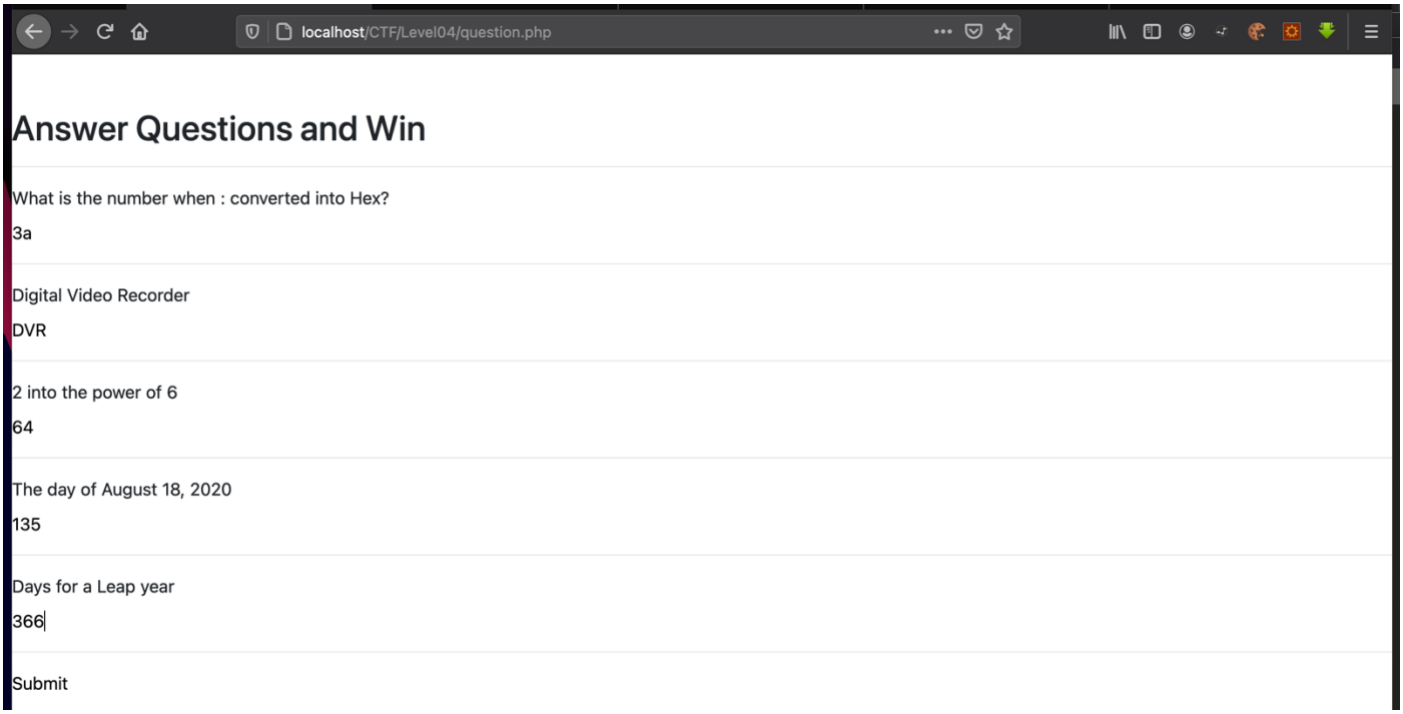


Level 04	-	Are you Fishing?

In this level, user need to answer simple questionnaire and must be intelligent the process of getting unlock code.

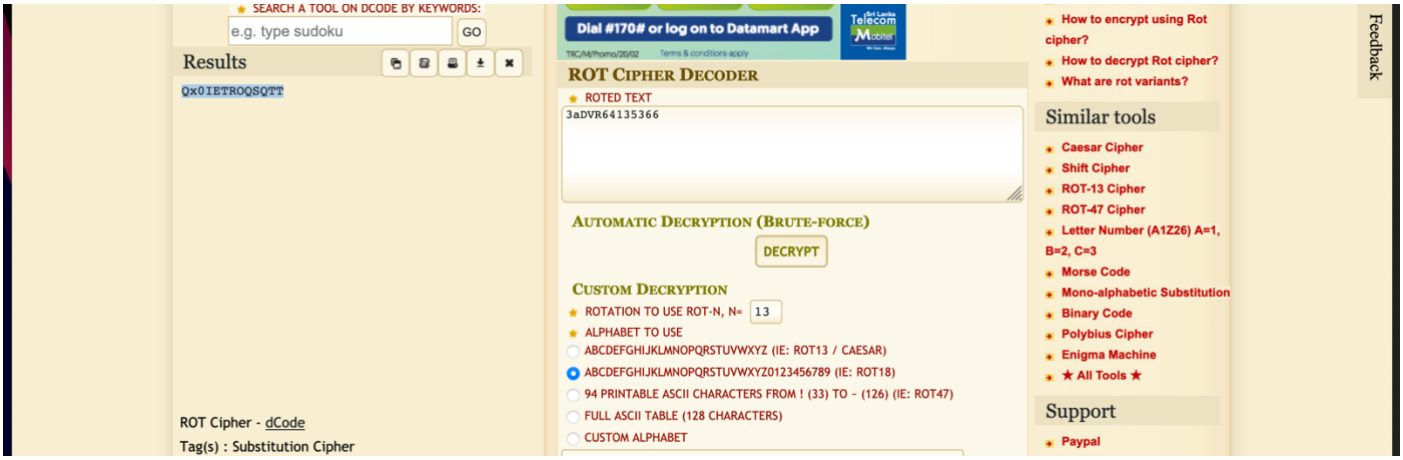




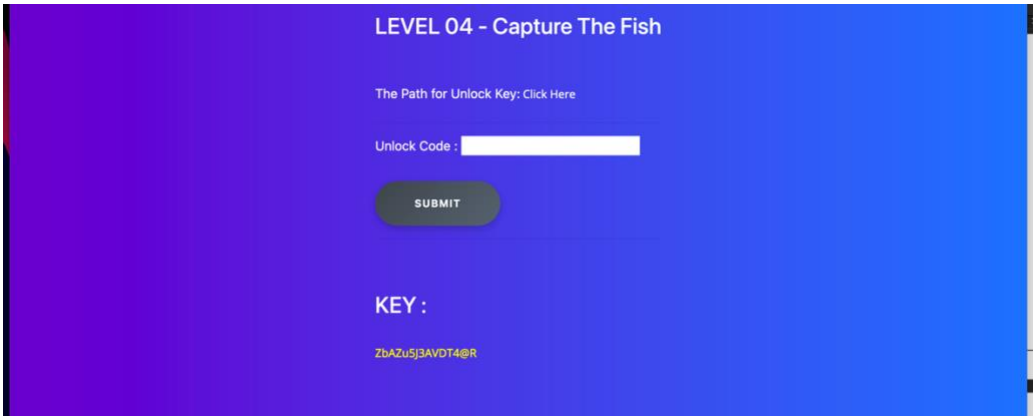


We can see a code can be generated through this answer pattern
3aDVR64135366

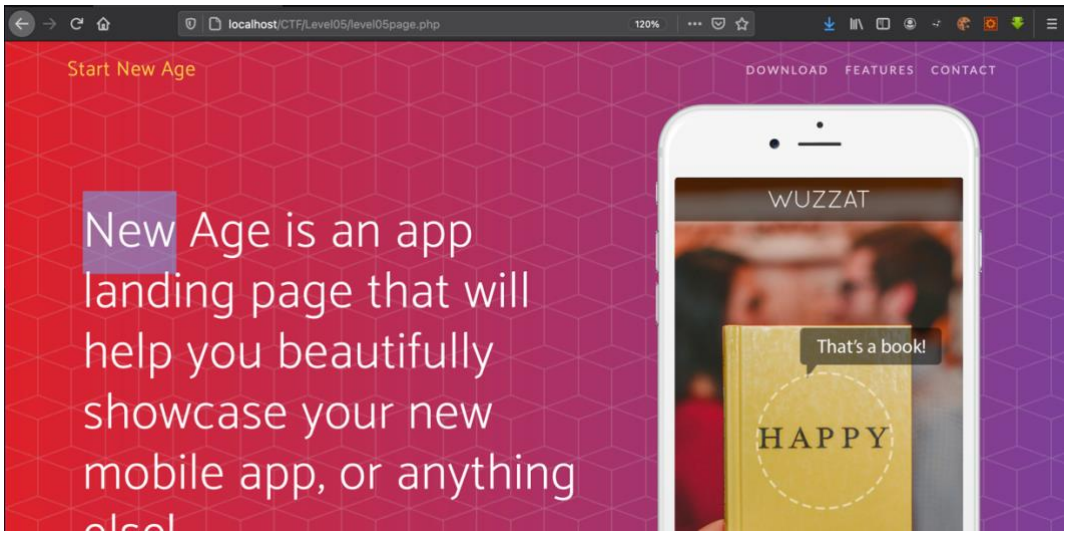
Let's decode with ROT Cipher (ROT 18)



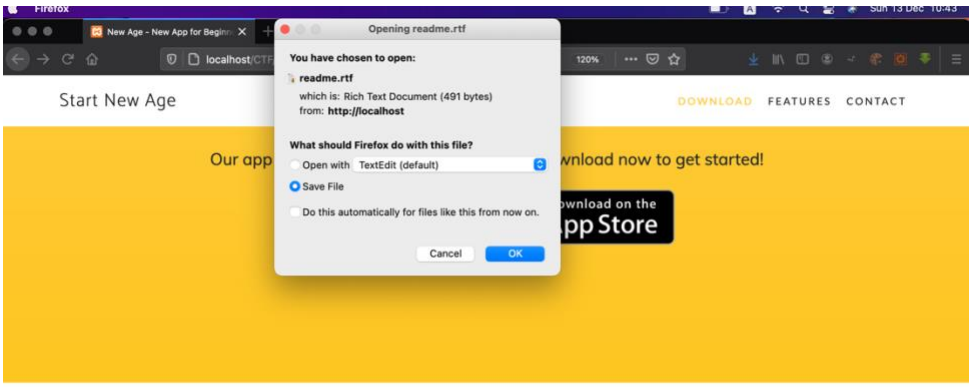
Success..



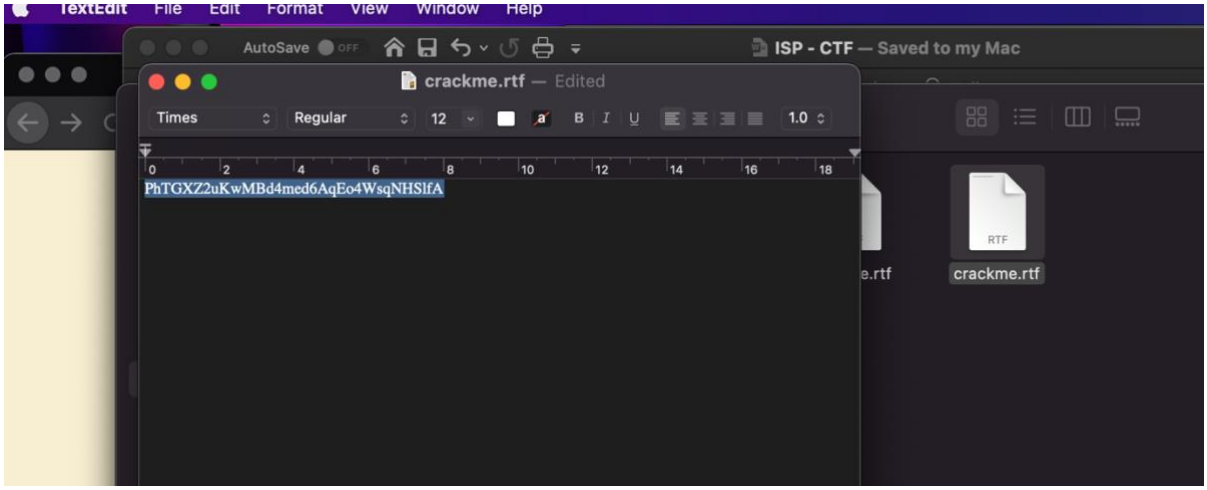
Level 05 - Capture The Fish 2



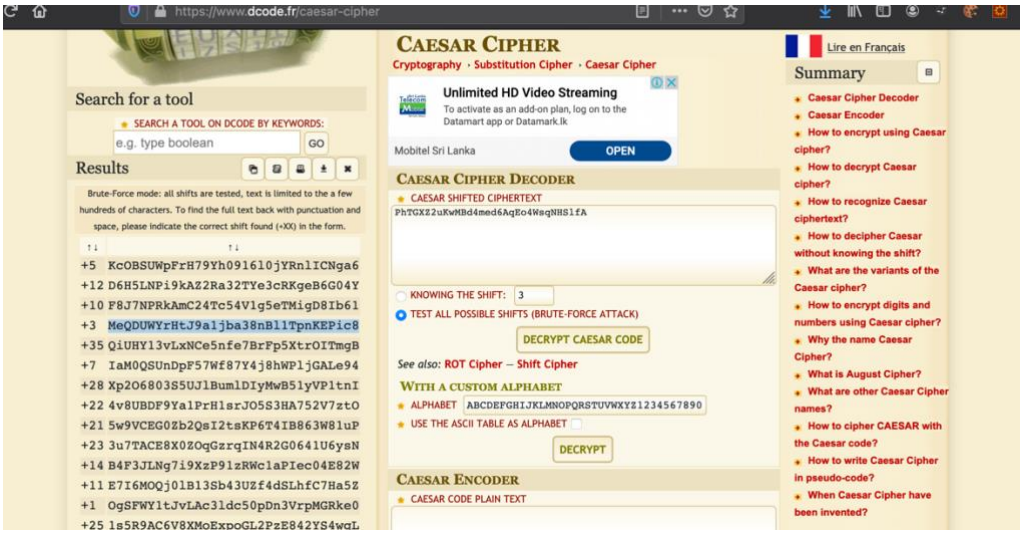
In this level user need to compare each file until capturing the correct fish (file) which is available on a download button.



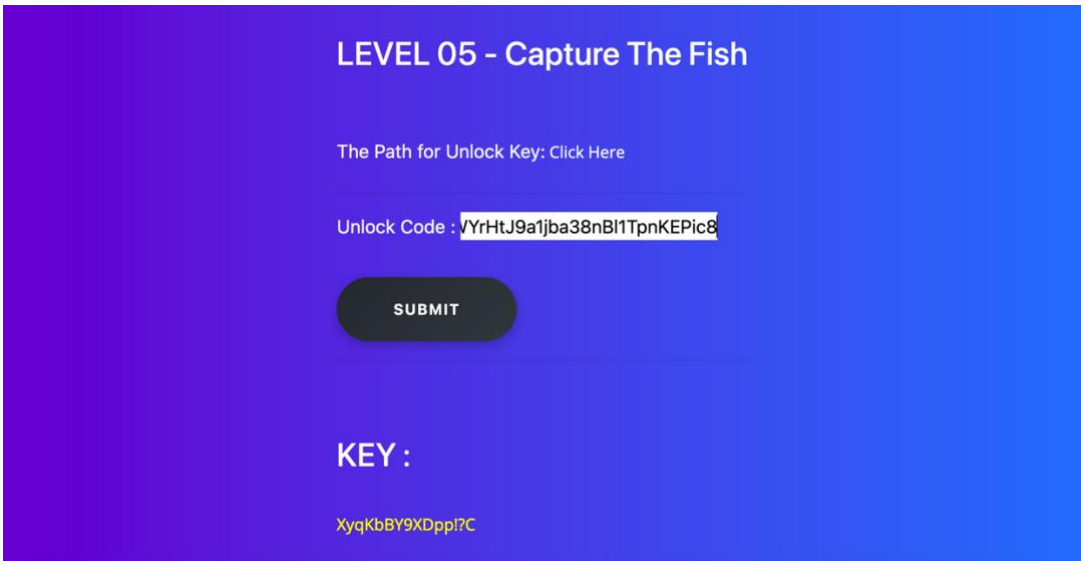
Remember that there are several readme.rtf are available but all those except this one is providing invalid paths. Therefore, user might take some time to capture the correct one.



The giving crackme.rtf file results must be decrypted using caesar Cipher (+3) and get the unlock Code

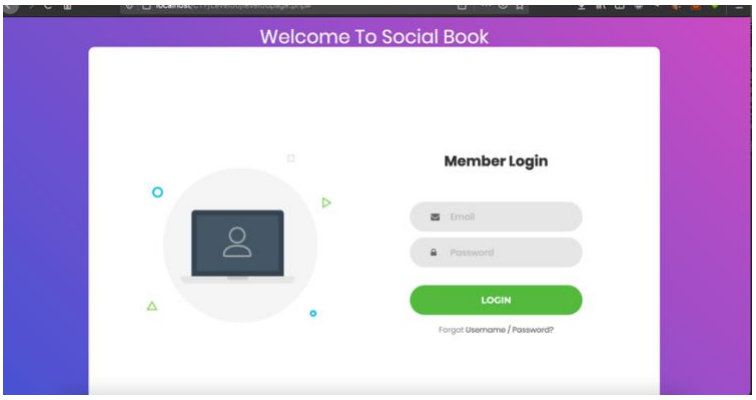


Done..

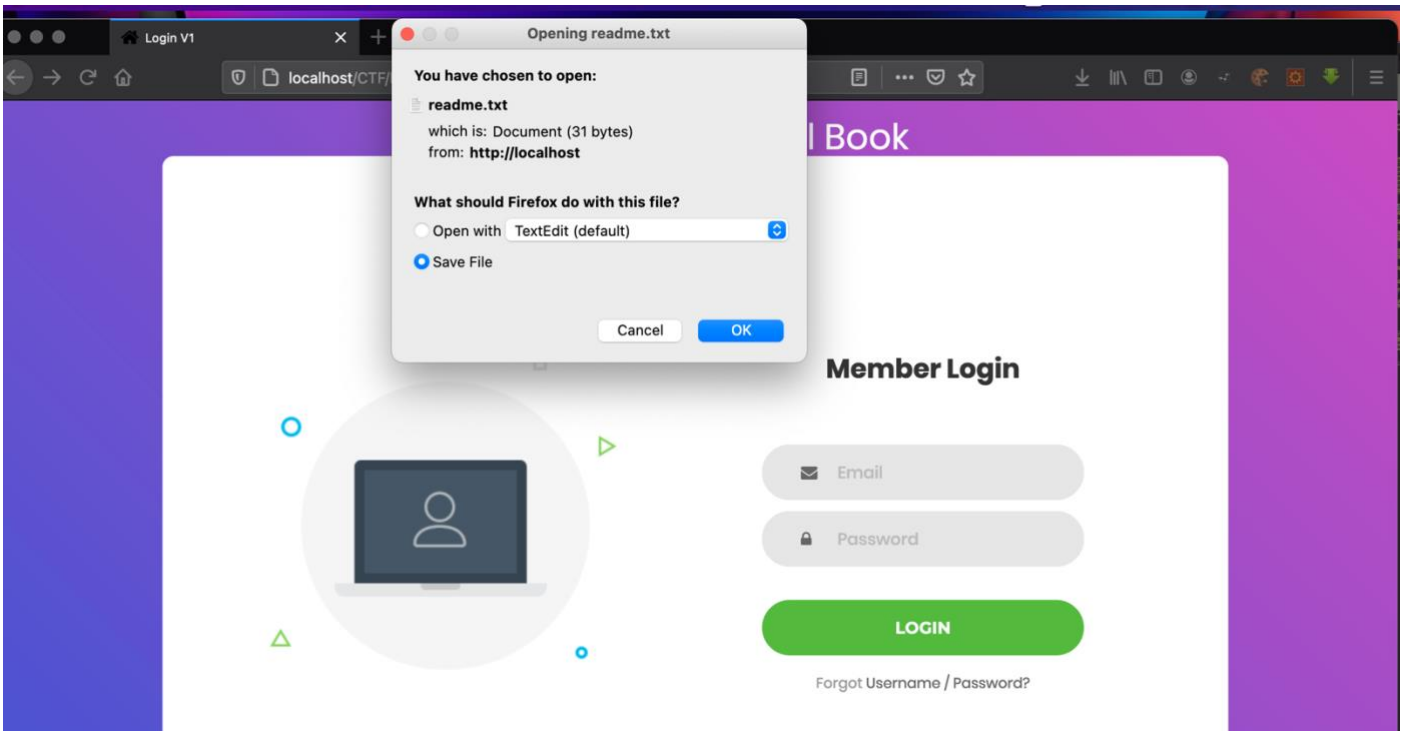


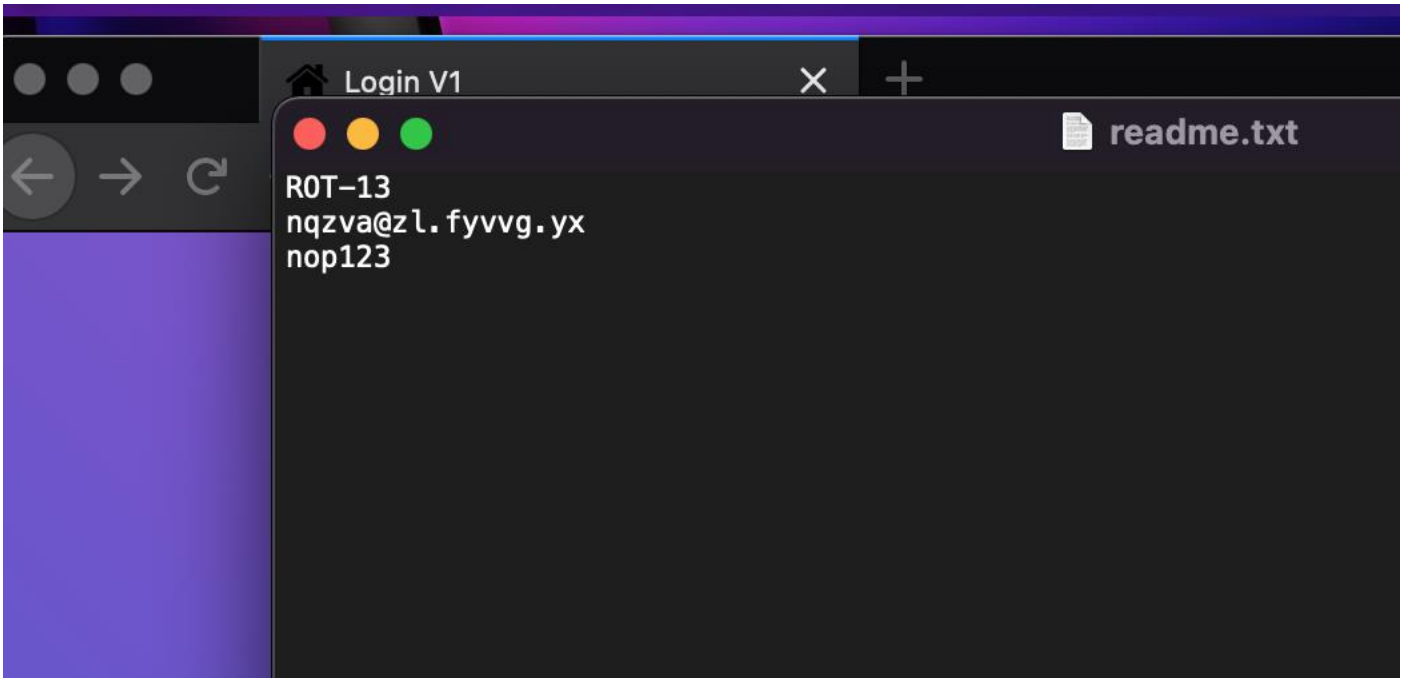
Level 06	-	Dark Knight Fishing (Blind Fishing)

In this level, user gets new experience by getting unlock code through hearing rather than viewing on the screen.

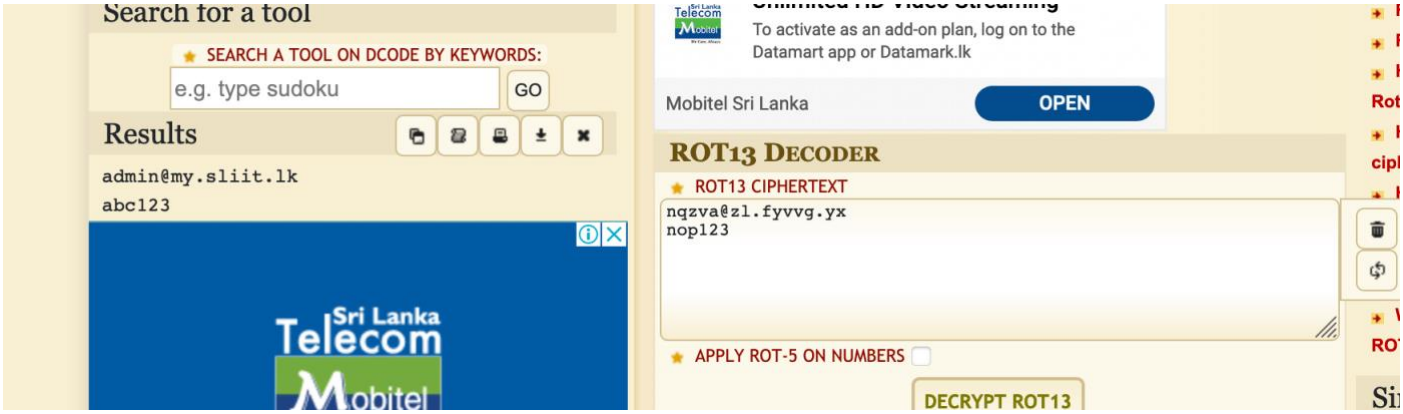


User can get username and password very easily through clicking forgot password link

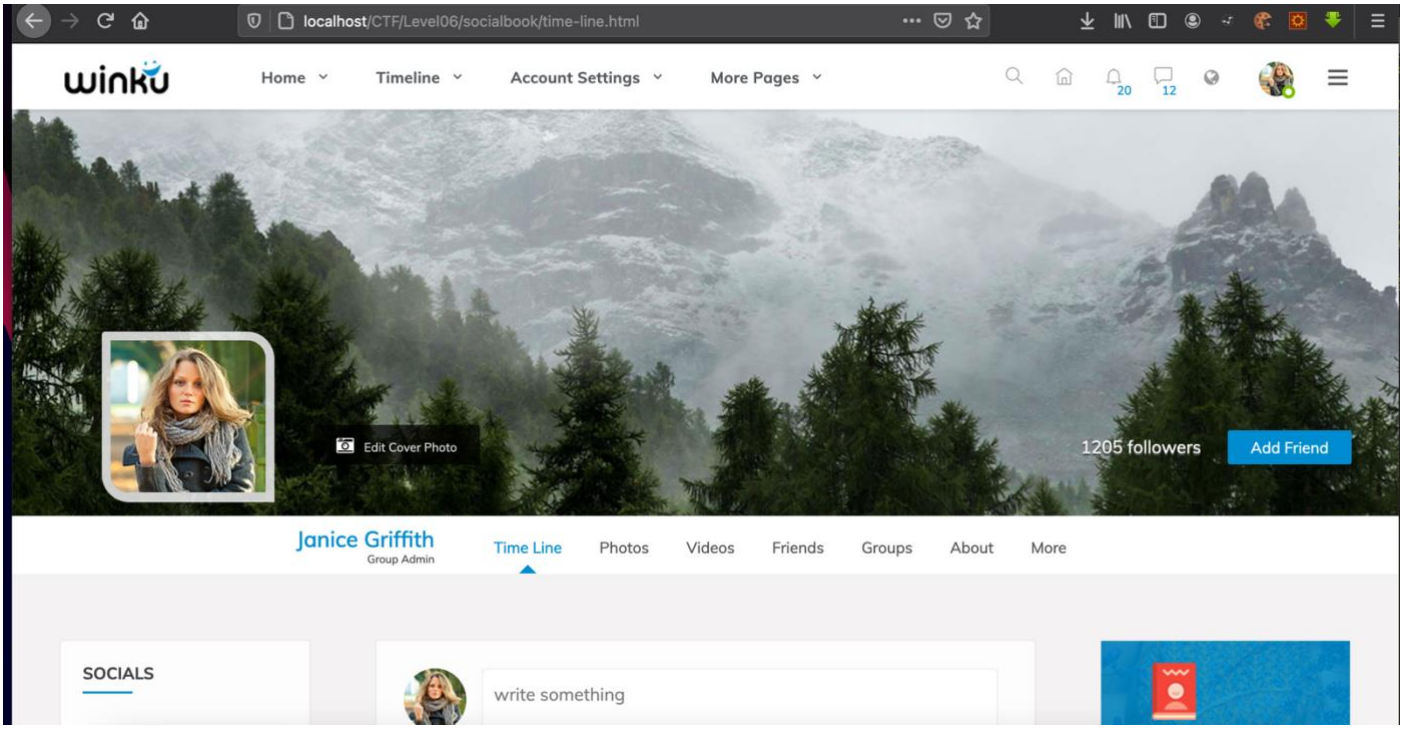


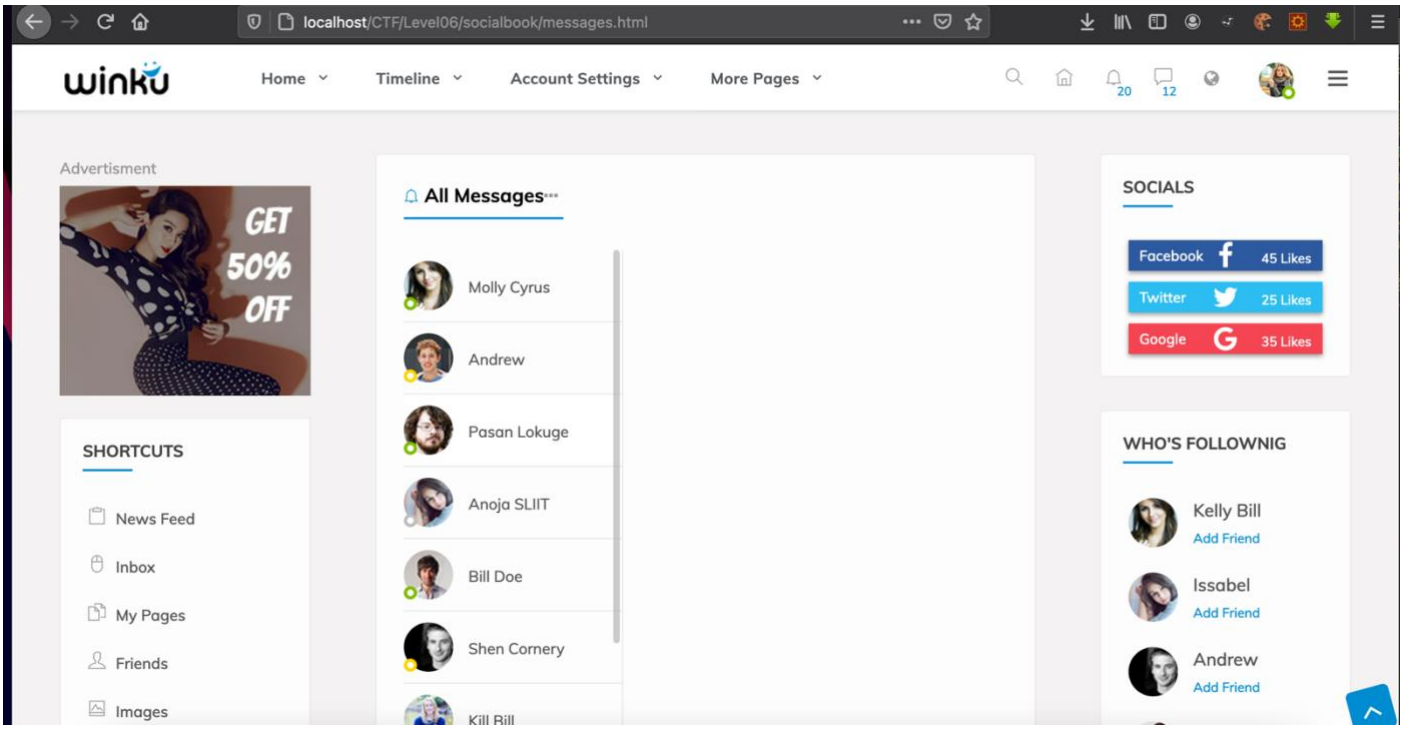


User need to ROT-13 Basic cryptographic decryption to get correct username and password.

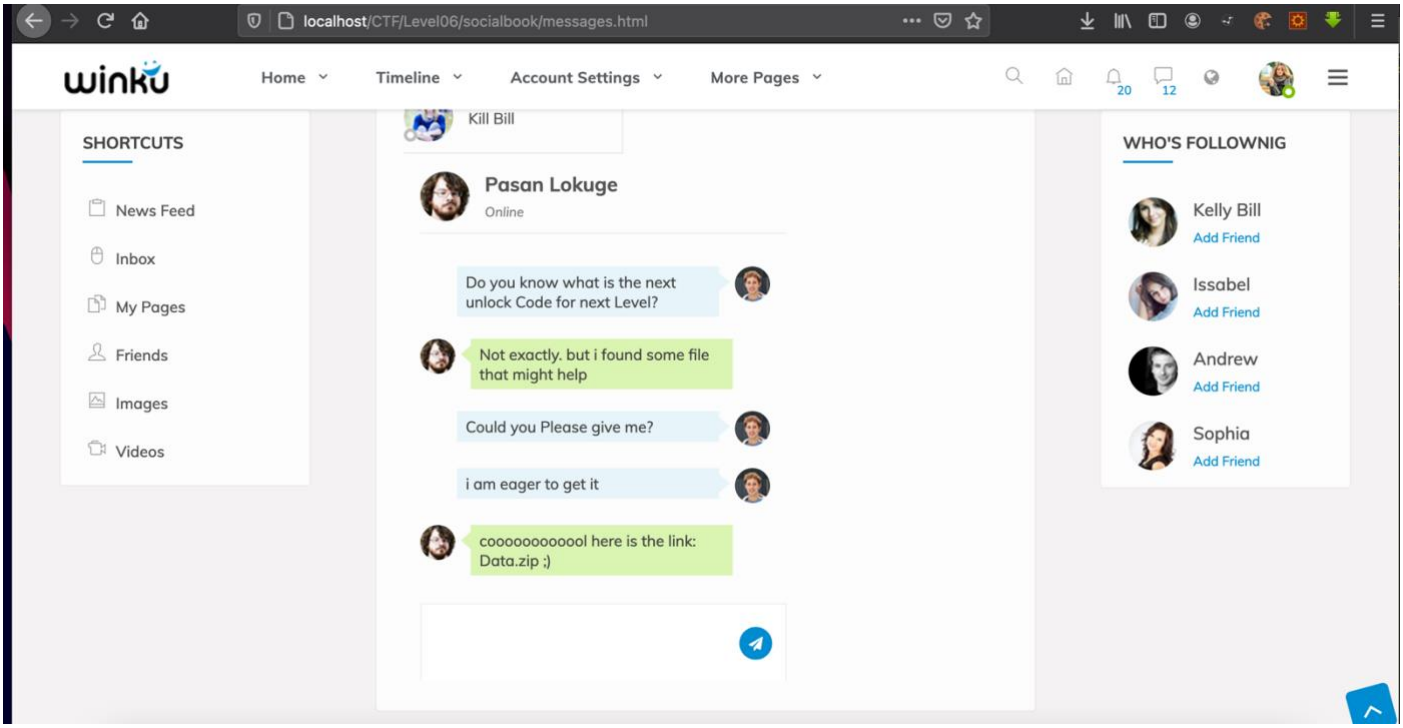


After login, user can see a new social media experience. But user need to find a clue about the unlock code.

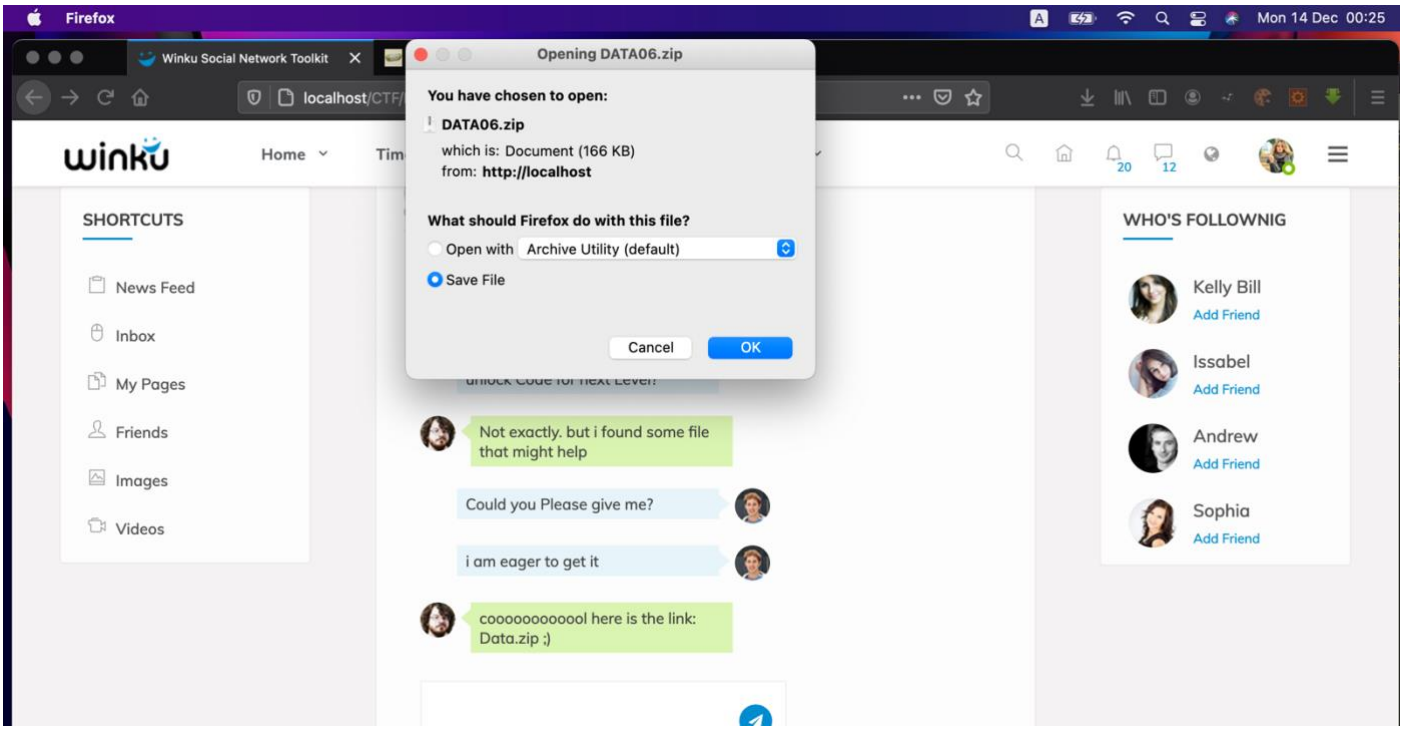




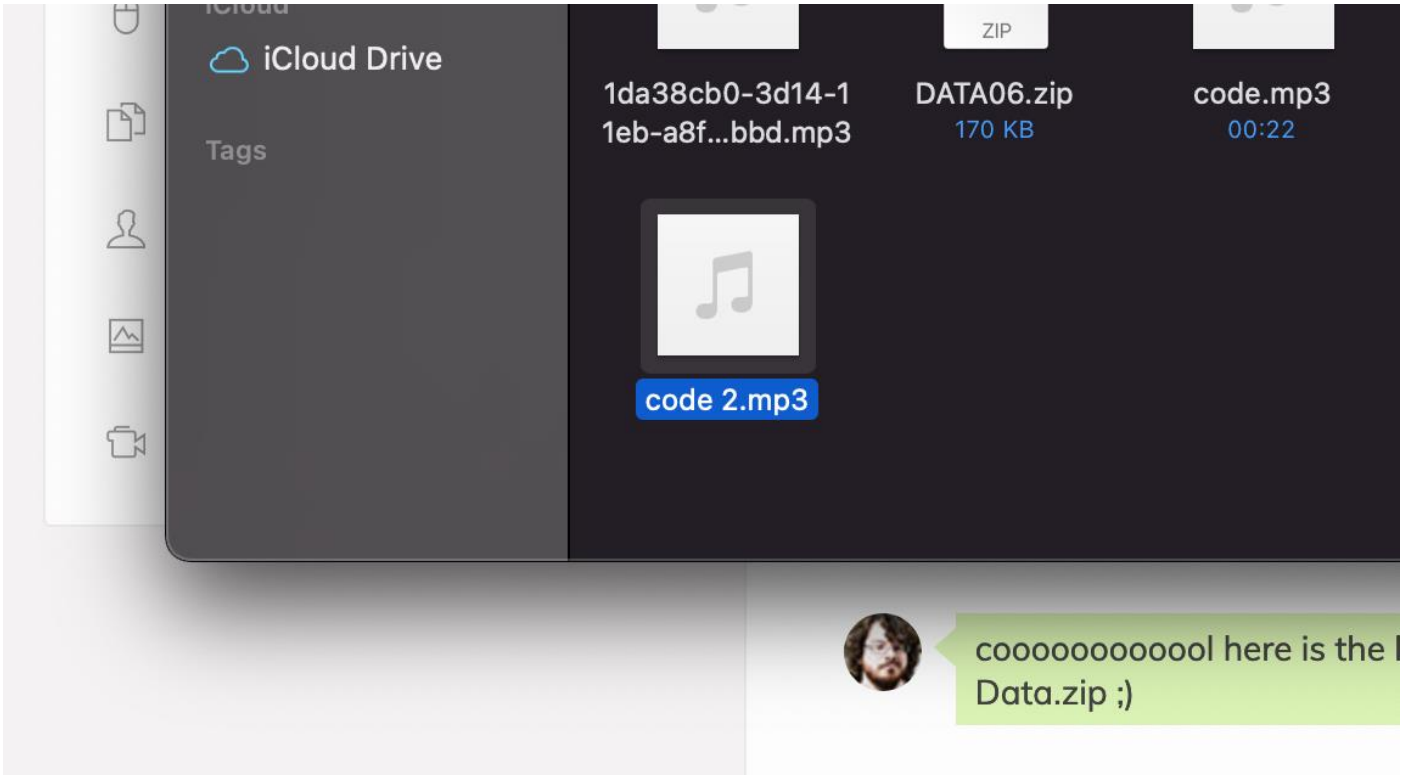
Seek for Message Chats for any clues



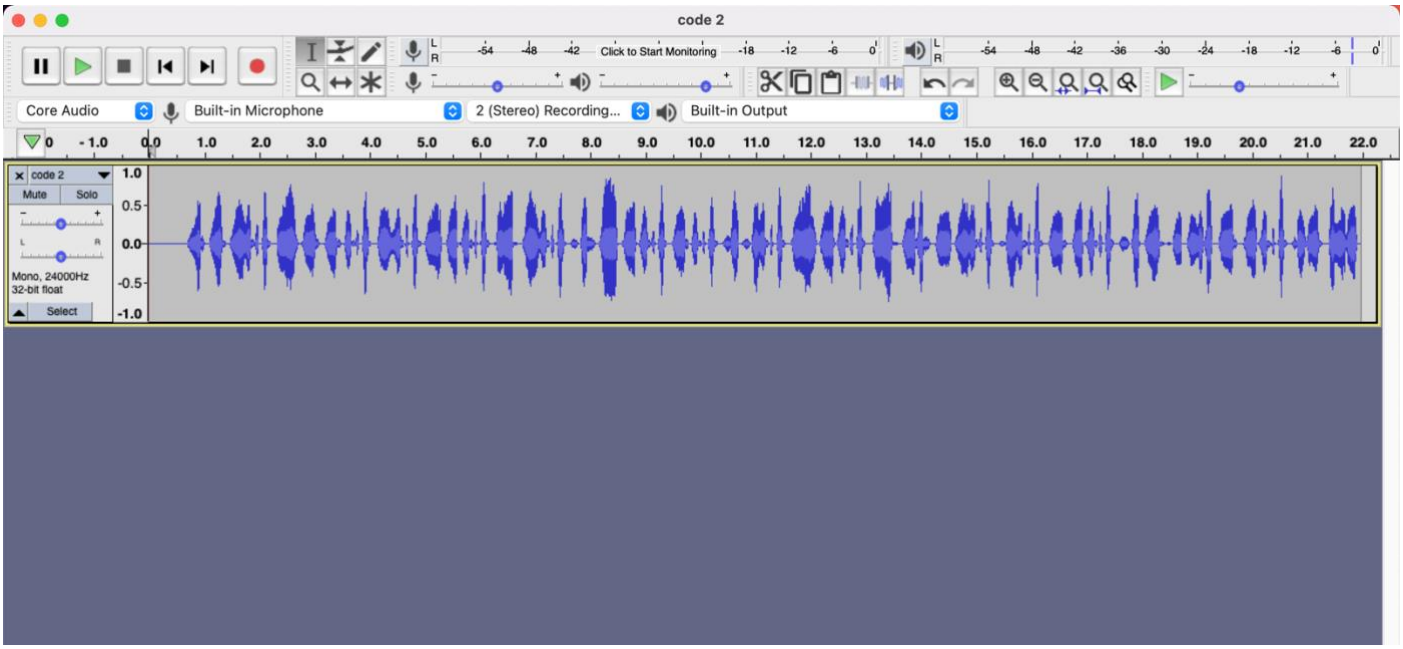
We can see a file which came from a friend that makes a clue about the unlock code.



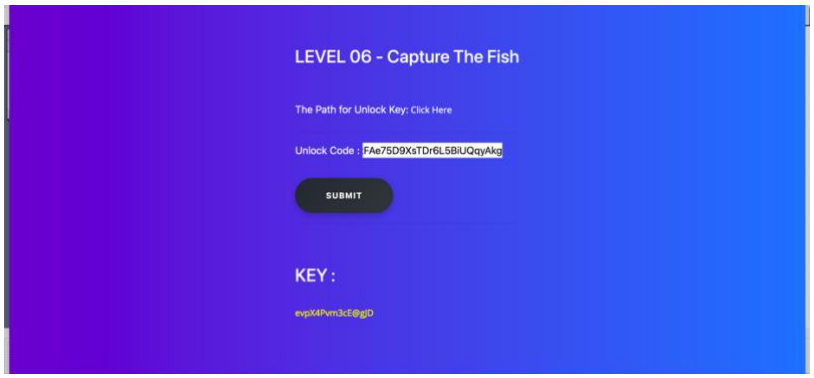
user can see a .mp3 file but audio is cannot be understand. Therefore we need to analyze audio using proper software. For demonstration purpose, we are using audacity.



Simply, Goto Effects->Reverse to make sure make any clue about the key.

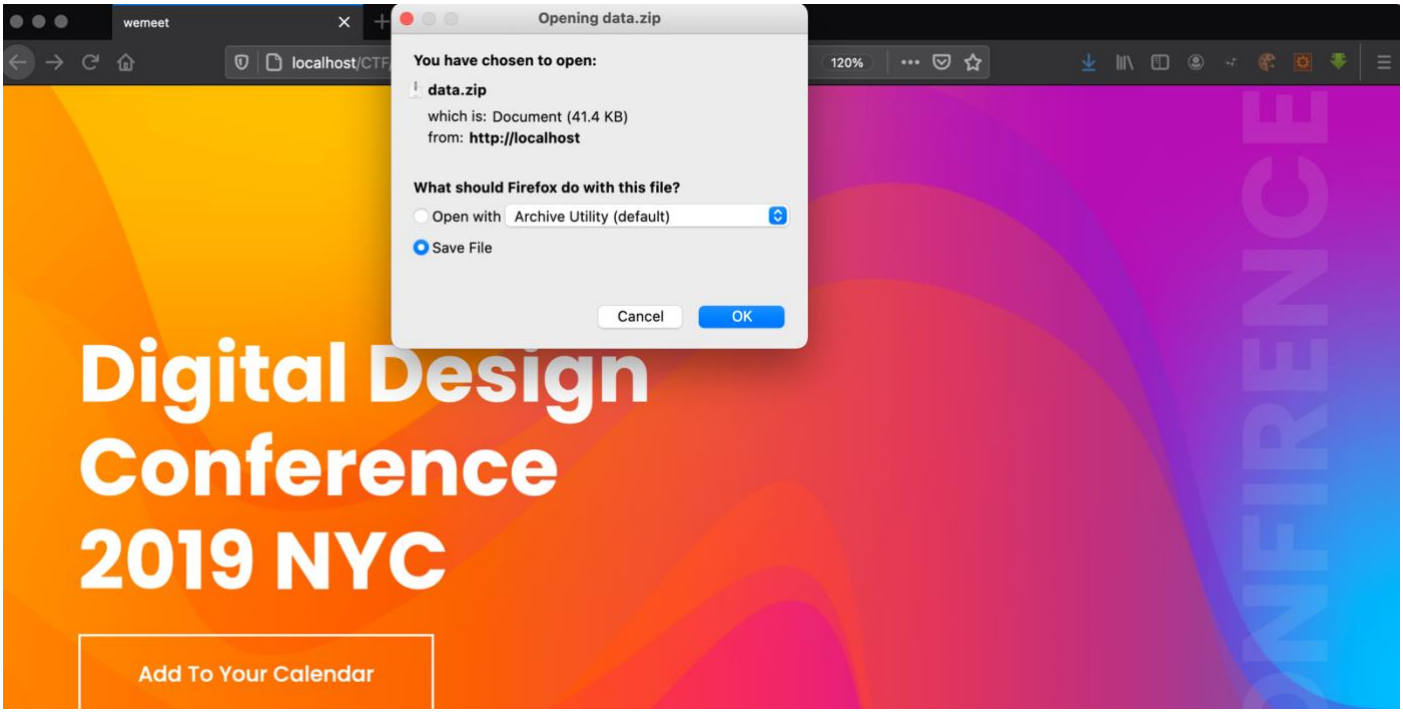


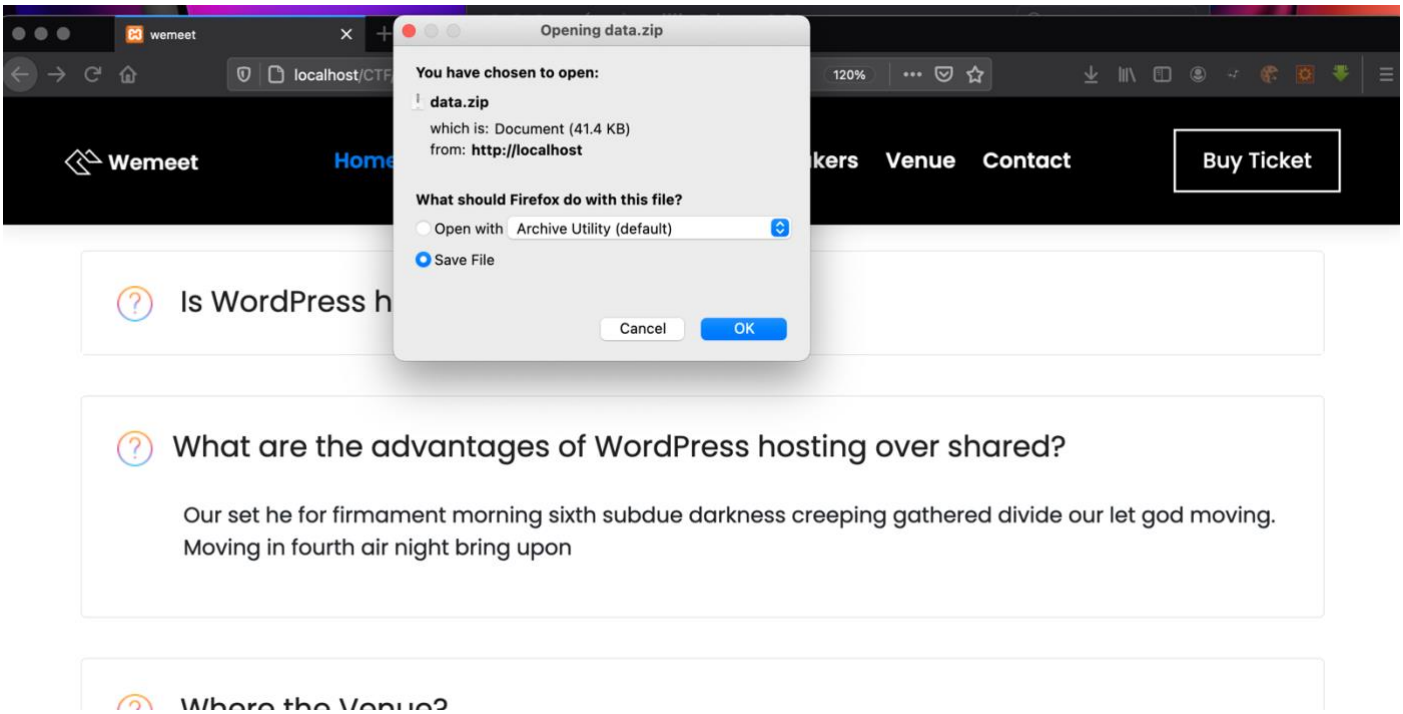
By listening to reversed audio, we can get the audio of the unlock code.
Done.



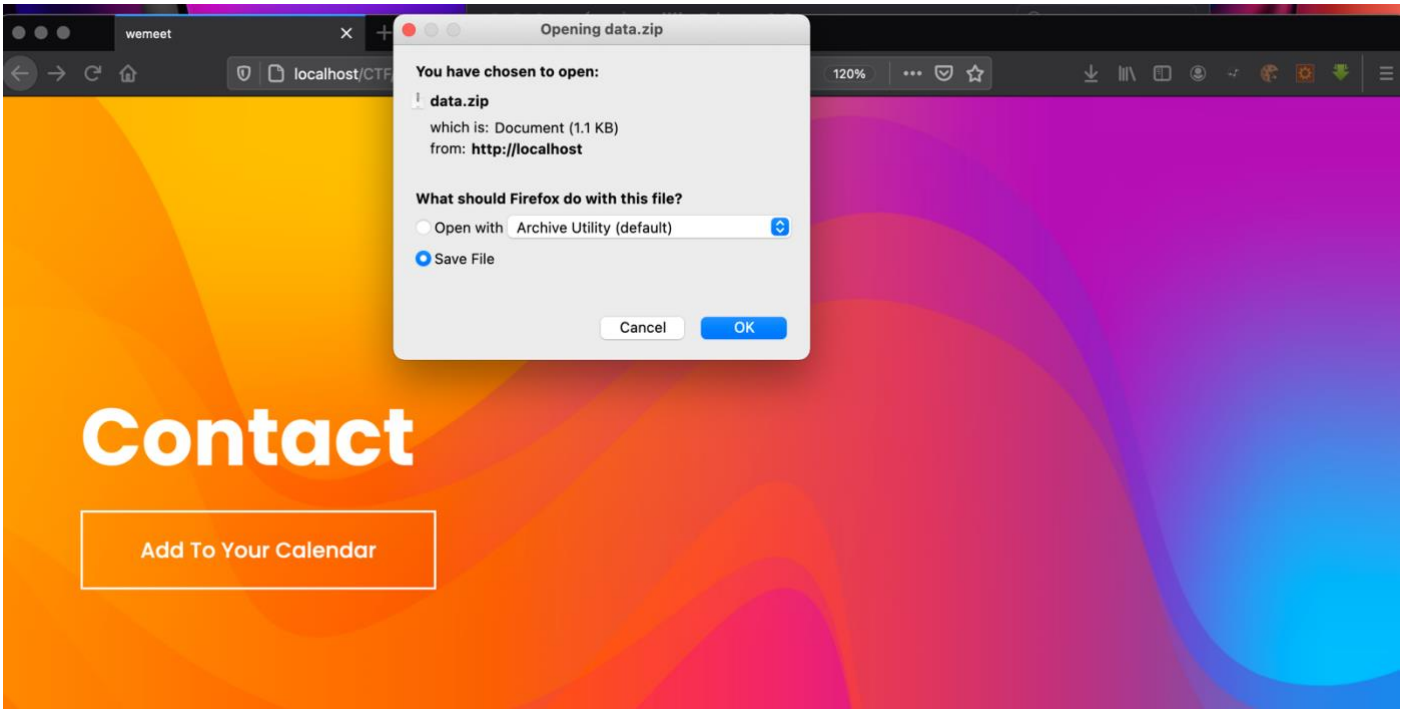
Level 07	- Beware of Bombs

This Level is simply dangerous to user's machines if you catch a bomb. (ZipBomb). There are several zip bomb files planted on many links in the webpage and user need to analyze the file size of the zip files and capture the unlock code.

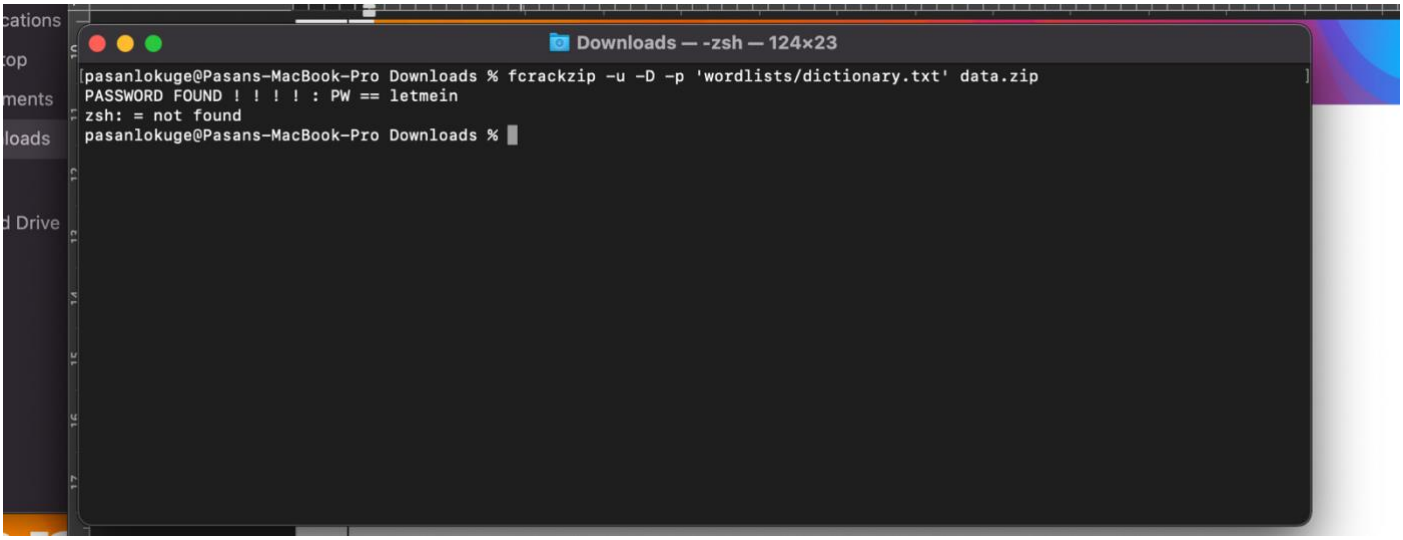




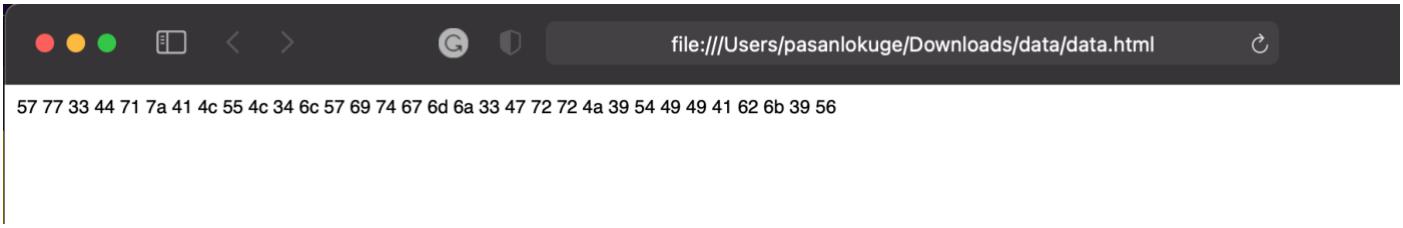
In below image shows a zip file with different data size.

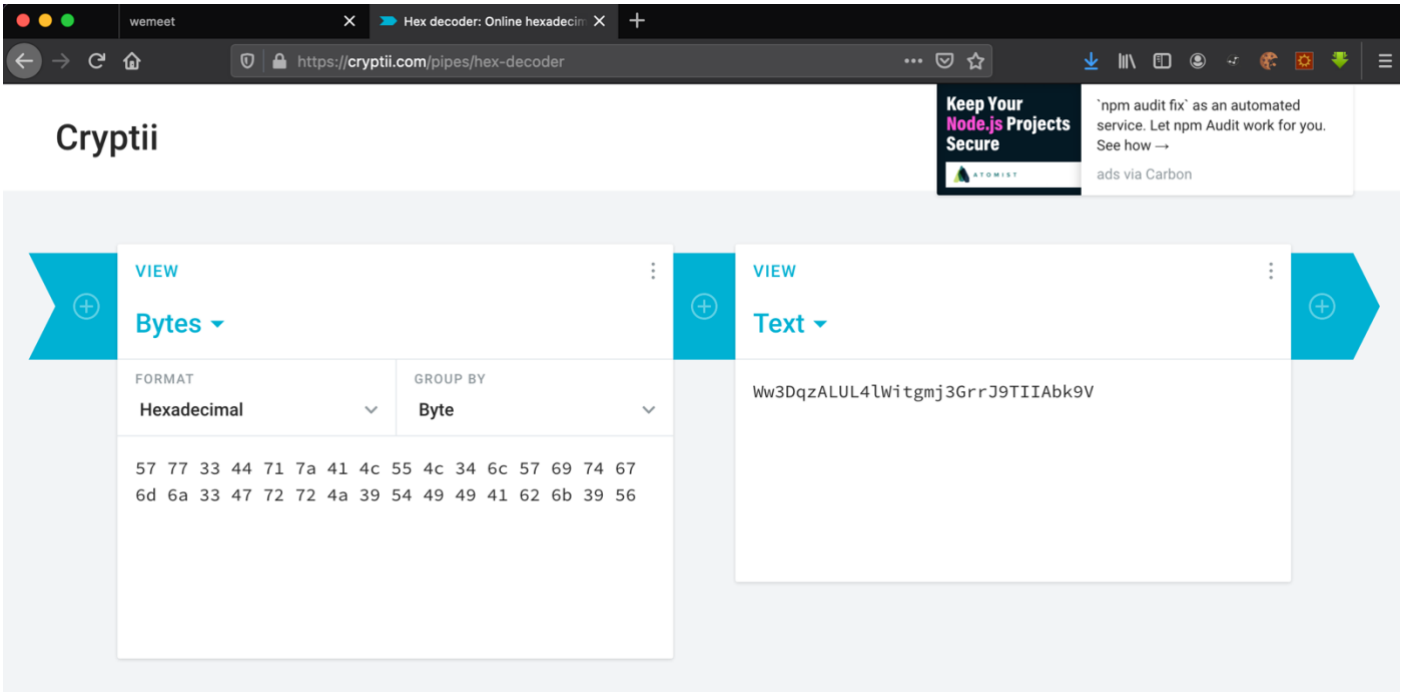


Simply, user will need to brute force zip file to gain access

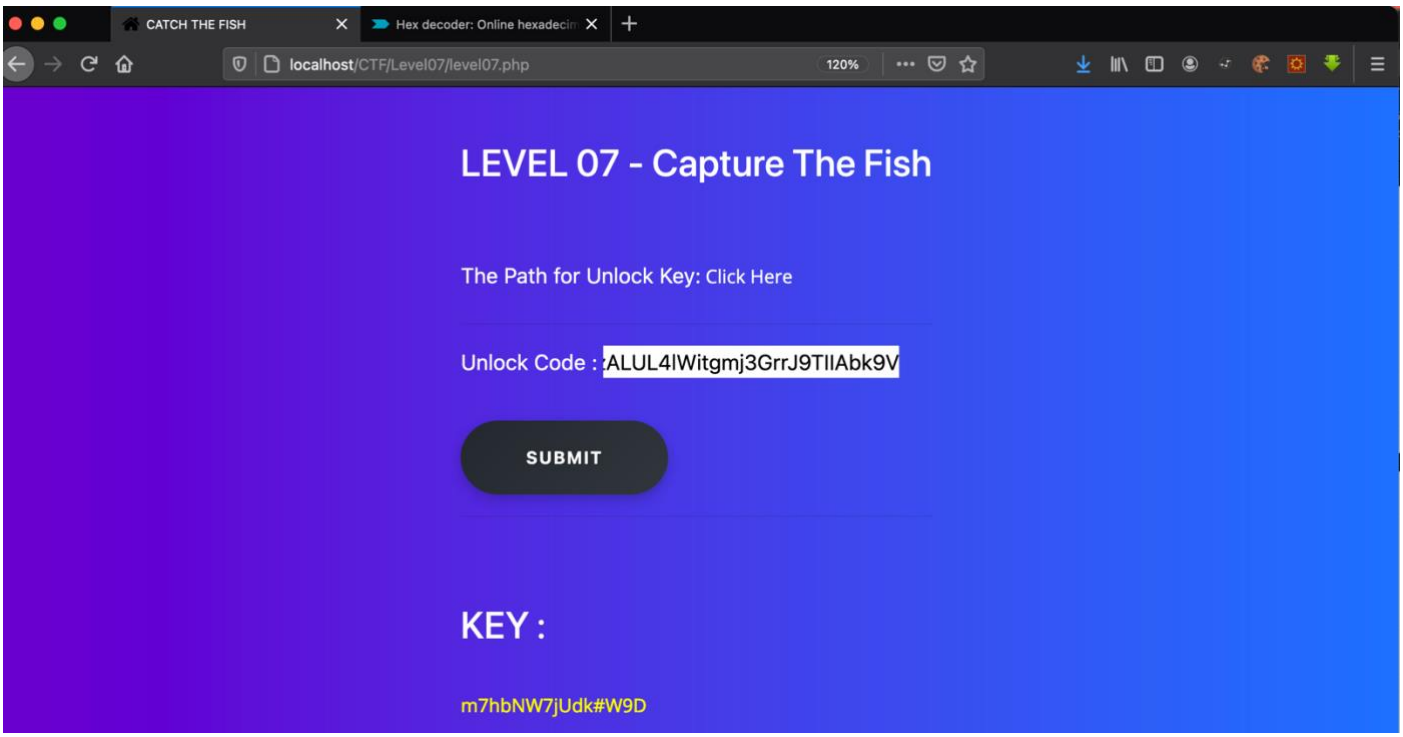


In the zip file we can see only a hex type code which needs to be converted to decimal / ASCII



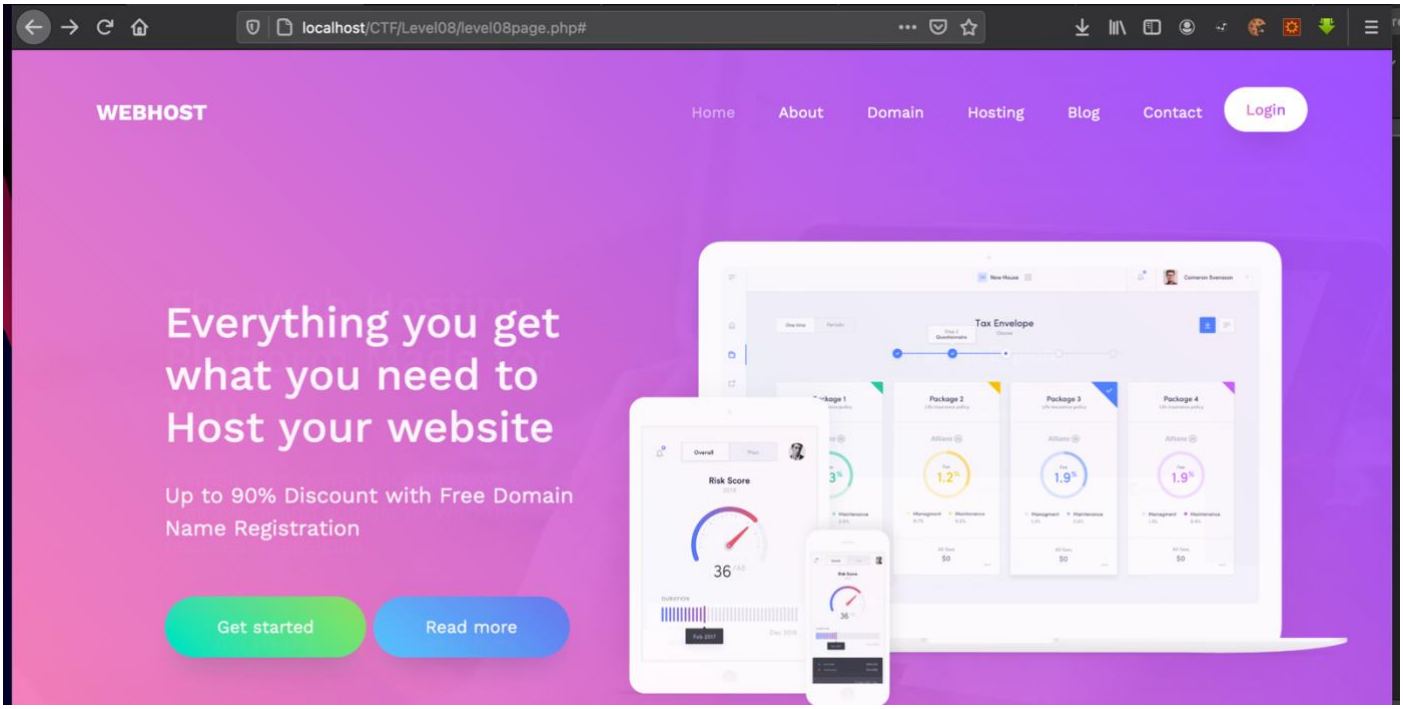

wemeet
Hex decoder: Online hexadecim
https://cryptii.com/pipes/hex-decoder
Cryptii
Keep Your Node.js Projects Secure
`npm audit fix` as an automated service. Let npm Audit work for you. See how →
ads via Carbon
VIEW
Bytes
FORMAT
Hexadecimal
GROUP BY
Byte
57 77 33 44 71 7a 41 4c 55 4c 34 6c 57 69 74 67
6d 6a 33 47 72 72 4a 39 54 49 49 41 62 6b 39 56
VIEW
Text
Ww3DqzALUL4lWitgmj3GrrJ9TIIAbk9V

Done.

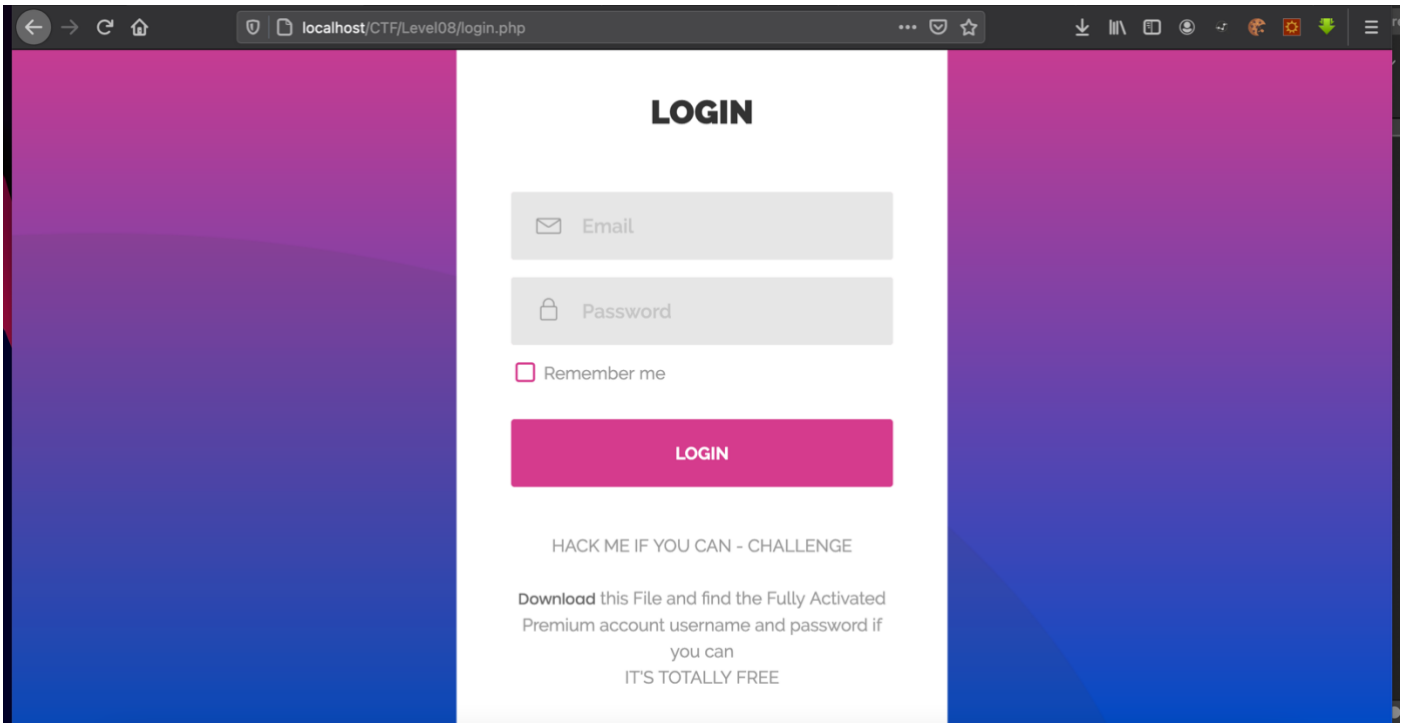

CATCH THE FISH
Hex decoder: Online hexadecim
localhost/CTF/Level07/level07.php
120%
LEVEL 07 - Capture The Fish
The Path for Unlock Key: Click Here
Unlock Code : ALUL4lWitgmj3GrrJ9TIIAbk9V
SUBMIT
KEY :
m7hbNW7jUdk#W9D

Level 08	-	Capture Shark from Wire

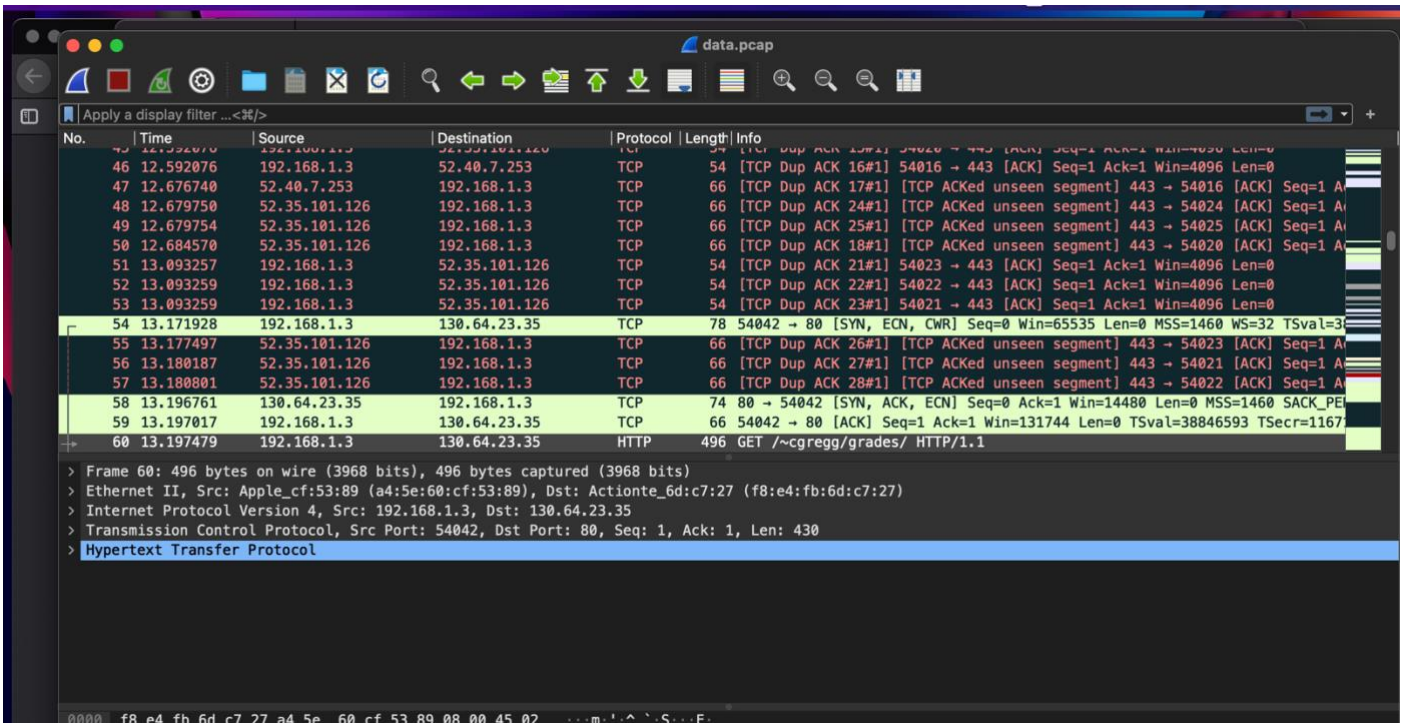
This is an open challenge from WEBHOST service provider which getting premium account for free if user can capture the username and password credentials from given Wireshark scan file.



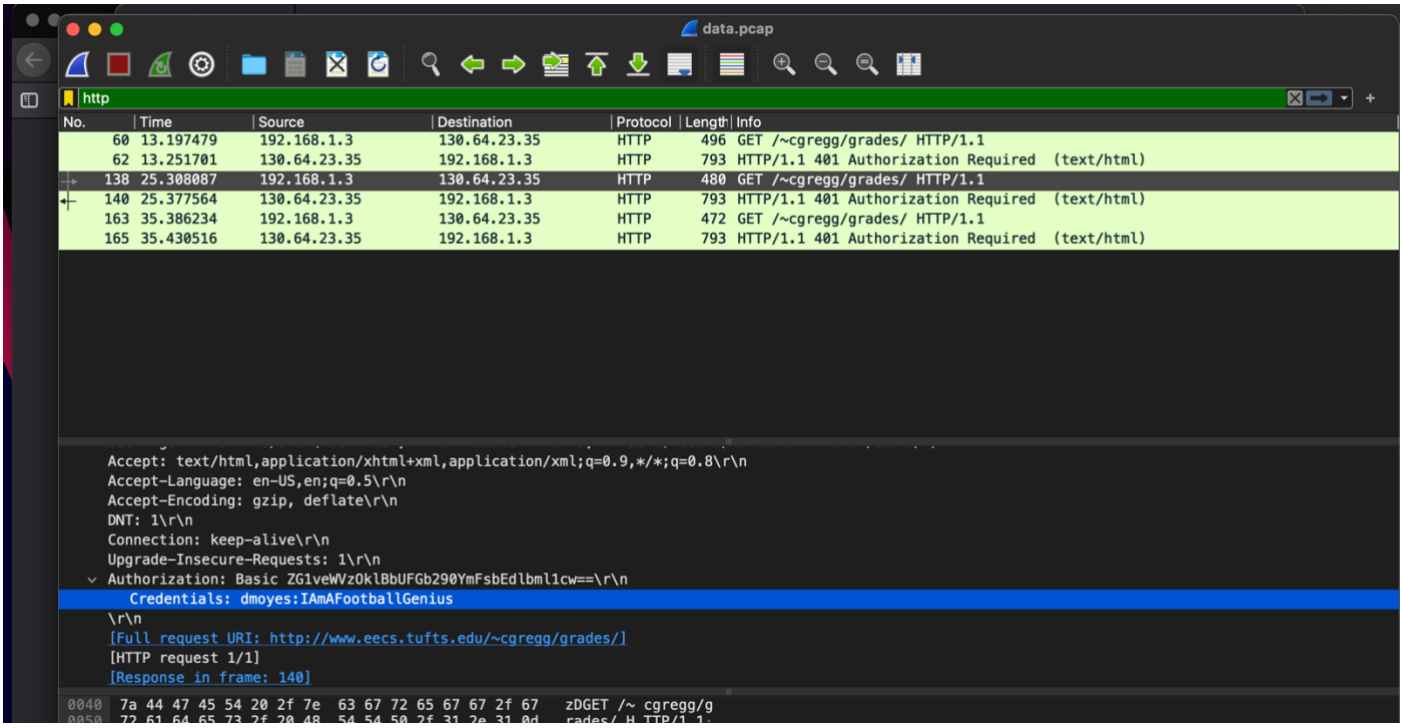
The challenge feature is available on the login form which can be open and examine for every user.



When we open pcap file, there are huge amount packets and details available and user need to find the correct credential details from given pcap file to move further on.

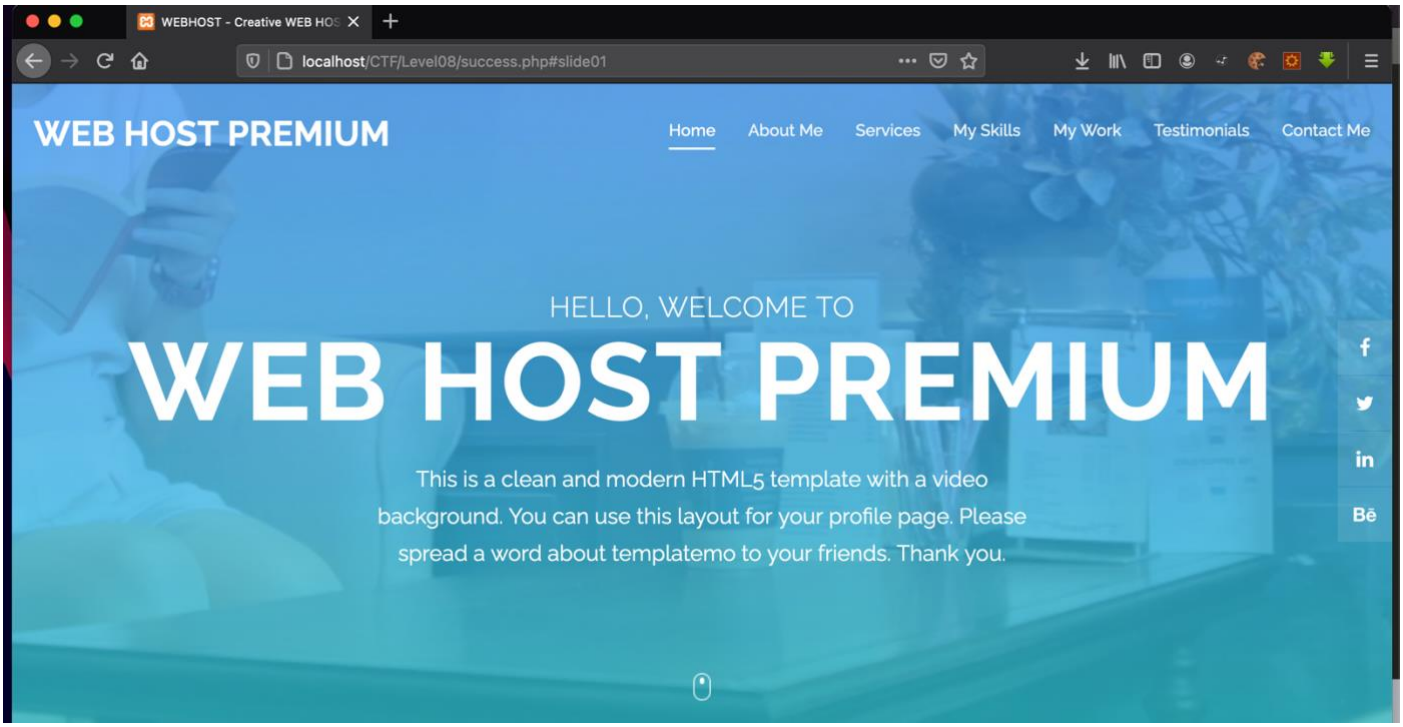


User might can search on http stream to get clue about credential data.



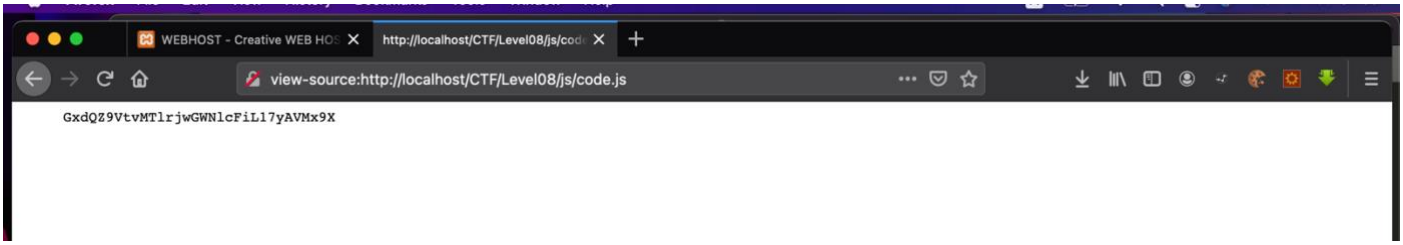
From source 192.168.1.3 , we can get some credential details which might be the webhost premium account credentials.

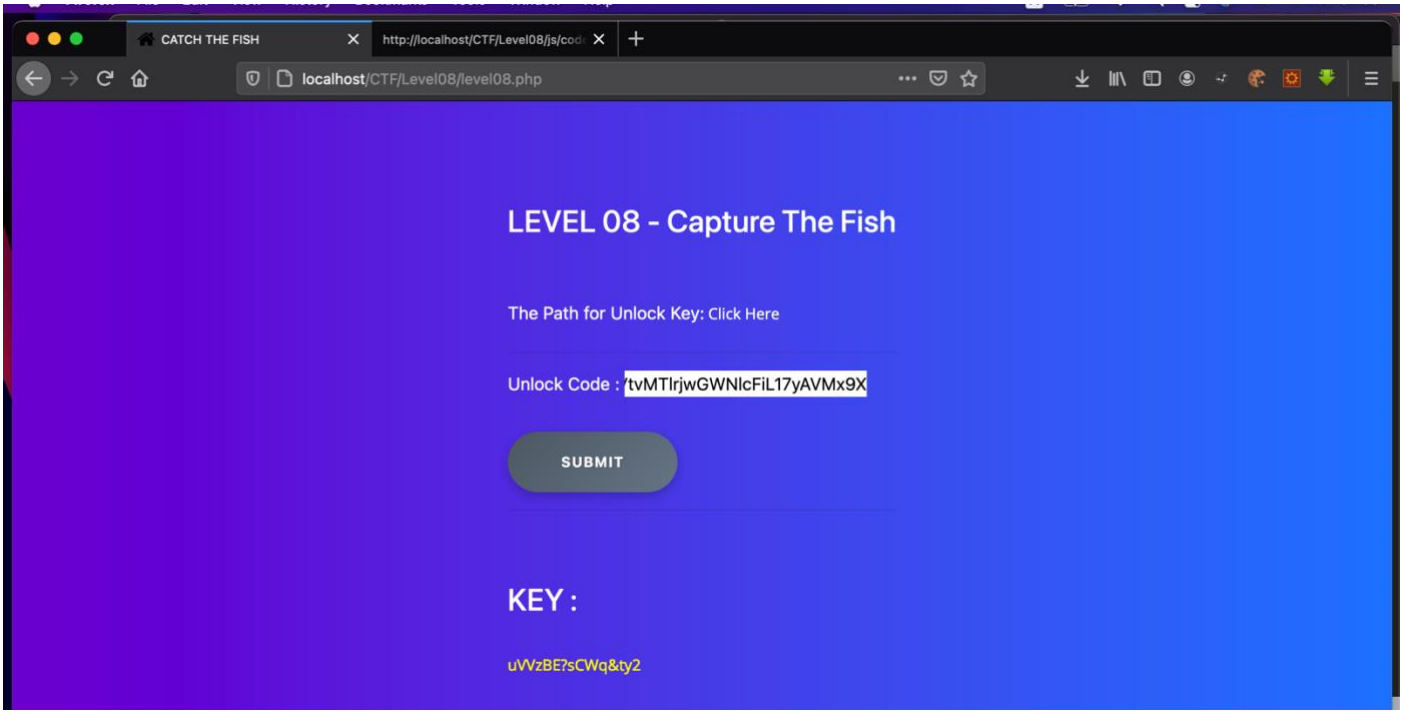
Success we are on the WEBHOST Premium account. Then we need to find the unlock code from this page at somewhere.



Let's move on to page source for any clue

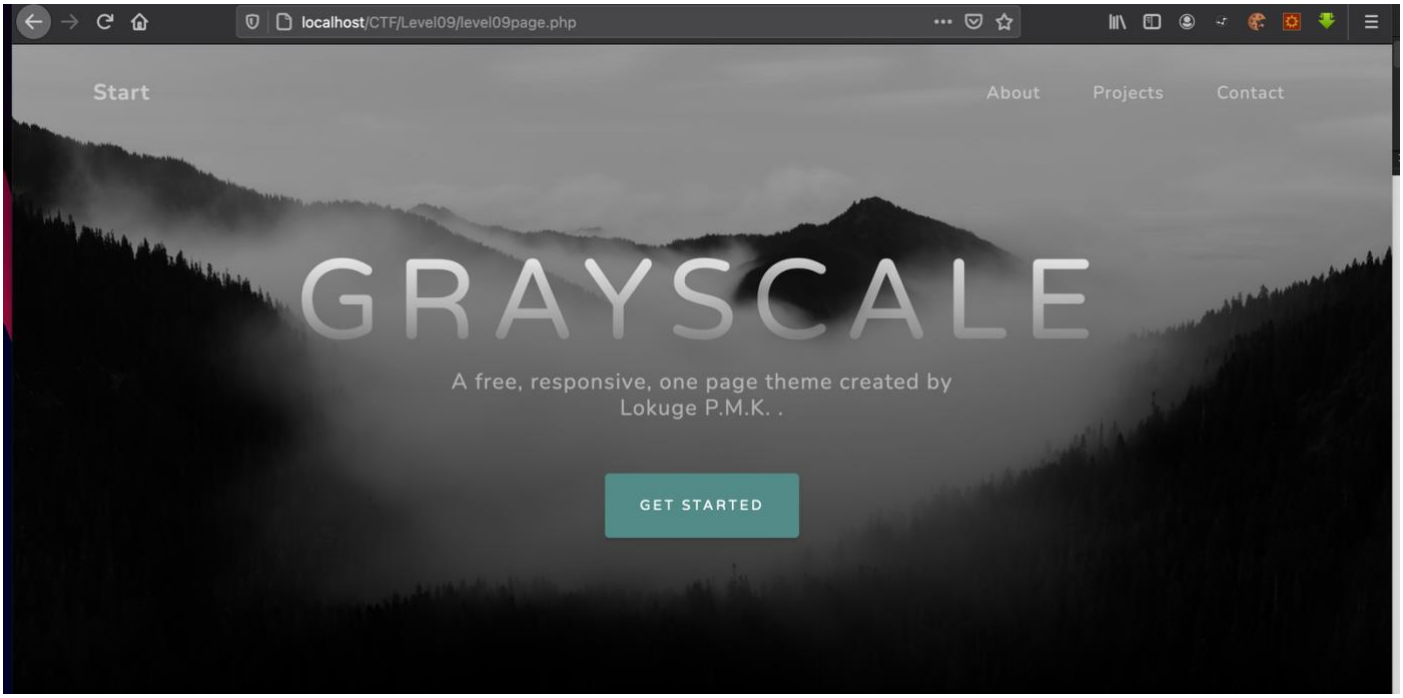
Success.

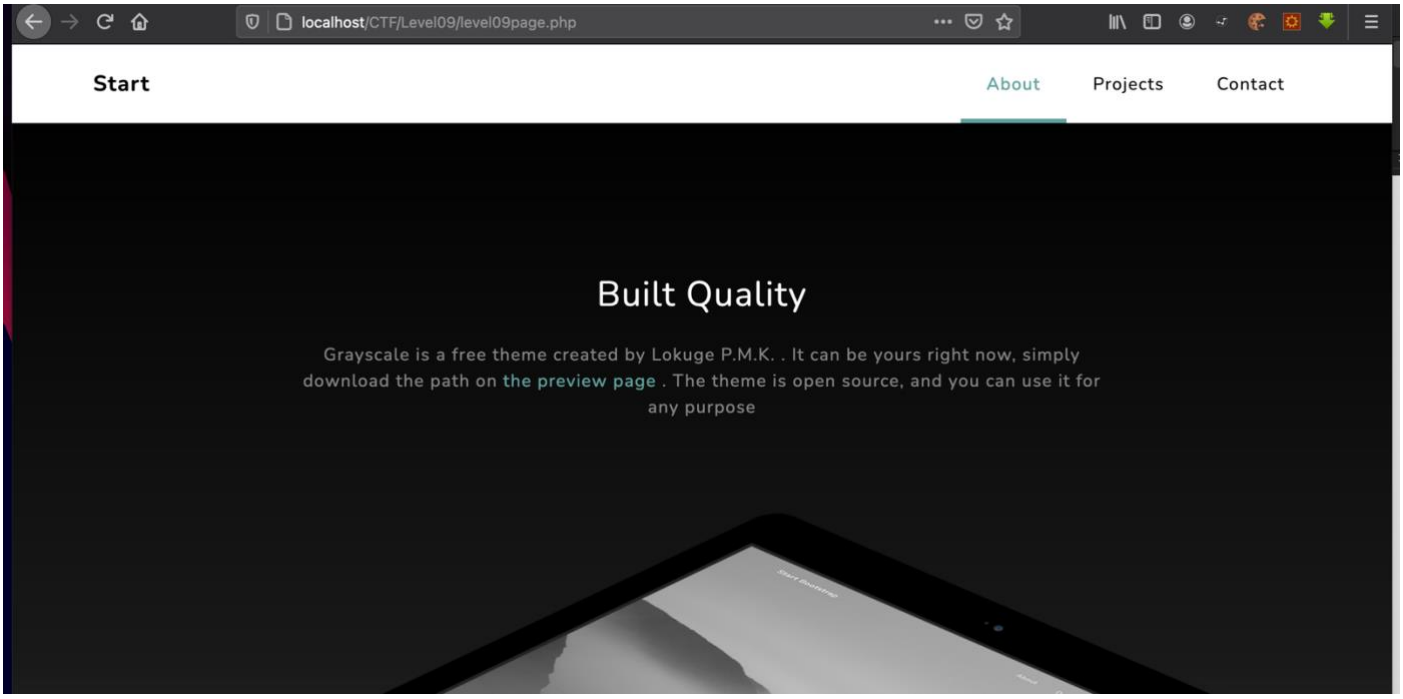


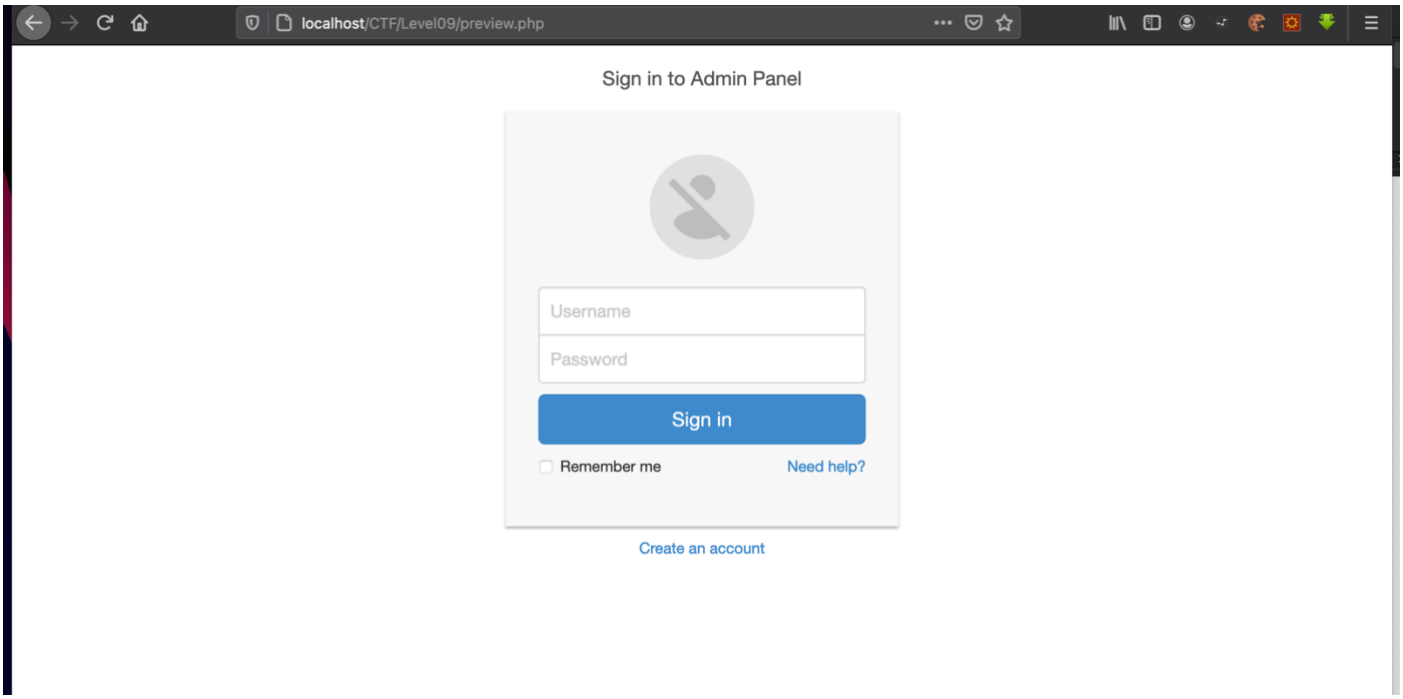


Level 09 - Try Until the Fish Comes

In this level user need to find the correct credentials with admin privileges by brute force / dictionary attack method.

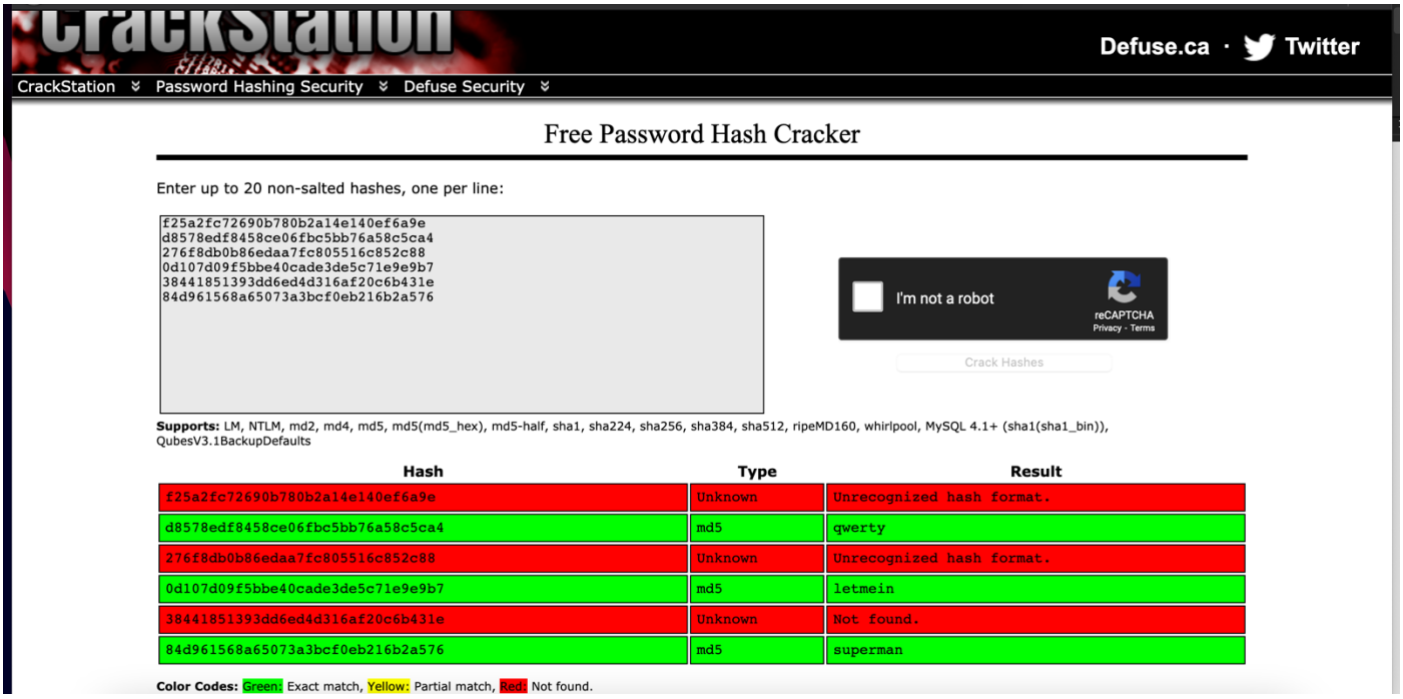



localhost/CTF/Level09/level09page.php
Start
About
Projects
Contact
Built Quality
Grayscale is a free theme created by Lokuge P.M.K. . It can be yours right now, simply download the path on the preview page . The theme is open source, and you can use it for any purpose


localhost/CTF/Level09/preview.php
Sign in to Admin Panel
Username
Password
Sign in
Remember me
Need help?
Create an account

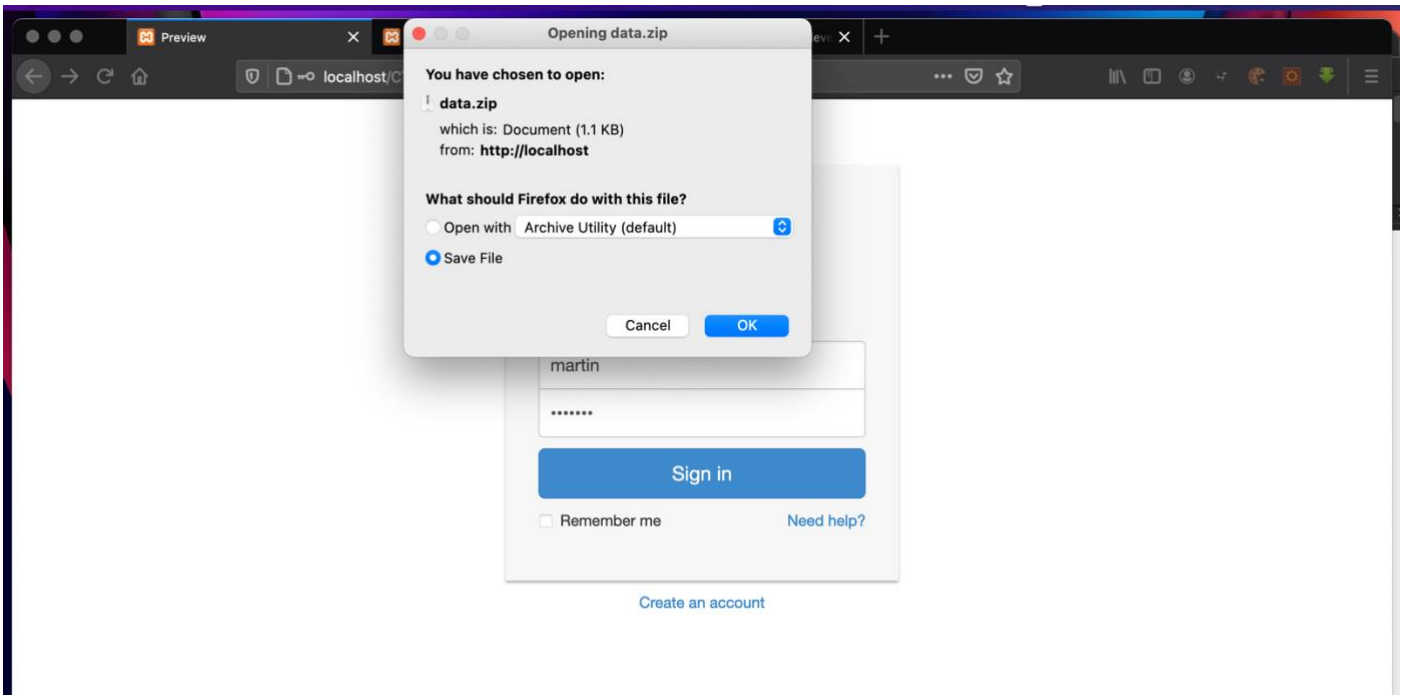
```
{
    display: block;
    margin-top: 10px;
}


</style>

</head>
<body>

<div class="container">
    <div class="row">
        <div class="col-sm-6 col-md-4 col-md-offset-4">
            <h1 class="text-center login-title">Sign in to Admin Panel</h1>
            <div class="account-wall">
                <img class="profile-img" src="https://lh5.googleusercontent.com/-b0-k99FZlyE/AAAAAAAAAAI/AAAAAAAAAAA/eu7opA4byxI/photo.jpg?sz=120"
                    alt="">
                <form class="form-signin" method="POST" action="preview.php" >
                <input name = "username"type="text" class="form-control" placeholder="Username" required autofocus>
                <input type="password" name="password"class="form-control" placeholder="Password" required>
                <button class="btn btn-lg btn-primary btn-block" type="submit" name="log_admin">
                    Sign in</button>
                <label class="checkbox pull-left">
                    <input type="checkbox" value="remember-me">
                    Remember me
                </label>
                <a href="#" class="pull-right need-help">Need help? </a><span class="clearfix"></span>
                </form>
            </div>
            <a href="#" class="text-center new-account">Create an account </a>
        </div>
    </div>
</div>

</body>

<script type="text/javascript" src="assets/js/misc/admin.js"></script>
<script type="text/javascript" src="assets/js/app/app.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
<script type="text/javascript" src="vendor/bootstrap/bootstrap.min.js"></script>
<script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
<script type="text/javascript" src="vendor/angular/angular.min.js"></script>

</html>

```

```
_id: ""
username:"lexar"
password:"5f4dcc3b5aa765d61d8327deb882cf99"
is_admin:false

_id: ""
username:"carl"
password:"f25a2fc72690b780b2a14e140ef6a9e0"
is_admin:false

_id: ""
username:"johnson"
password:"d8578edf8458ce06fbc5bb76a58c5ca4"
is_admin:false

_id: ""
username:"krish"
password:"276f8db0b86edaa7fc805516c852c889"
is_admin:false

_id: ""
username:"martin"
password:"0d107d09f5bbe40cade3de5c71e9e9b7"
is_admin:true

_id: ""
username:"luther"
password:"38441851393dd6ed4d316af20c6b431e"
is_admin:false

_id: ""
username:"marina"
password:"84d961568a65073a3bcf0eb216b2a576"
is_admin:false

_id: ""
username:"william"
password:"8afa847f50a716e64932d995c8e7435a"
is_admin:false
```

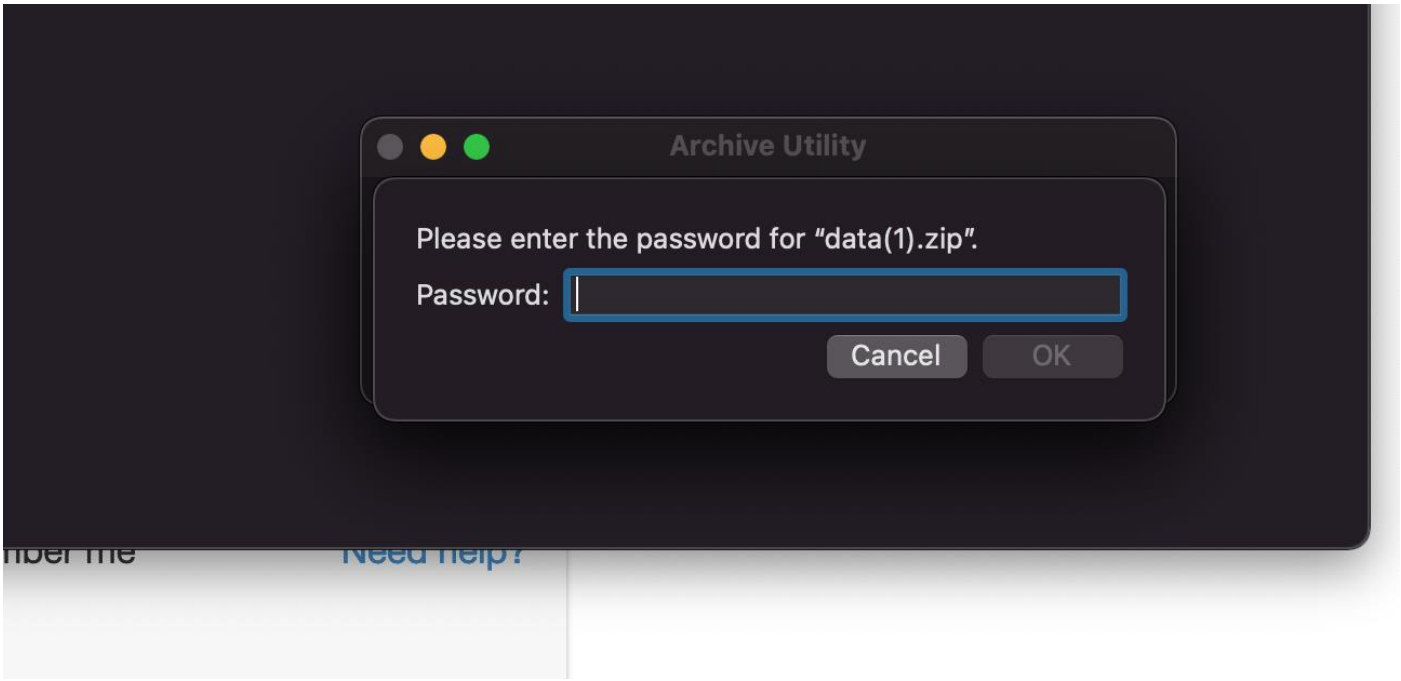


We can identify there is a password extracted by user martin and password letmein which has administrative privileges.

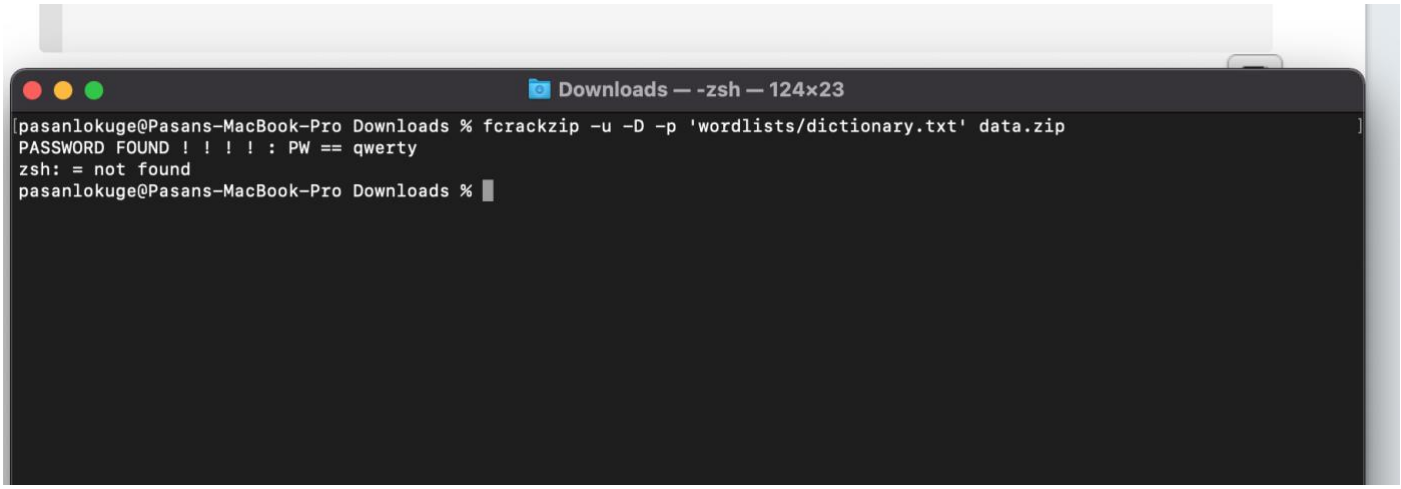
When enter username and password, there is a file which prompt for download gives a hint for the unlock code



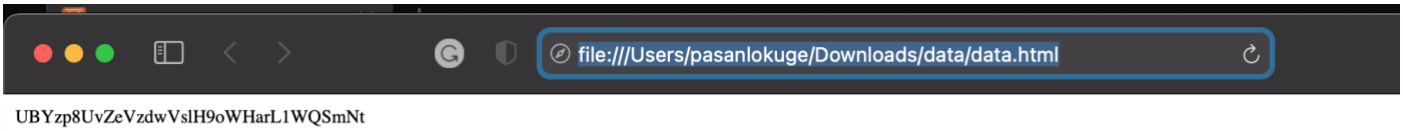
The downloaded zip file is read protected with passcode which needs to be cracked



For demonstration purpose, we have used fcrackzip and got password



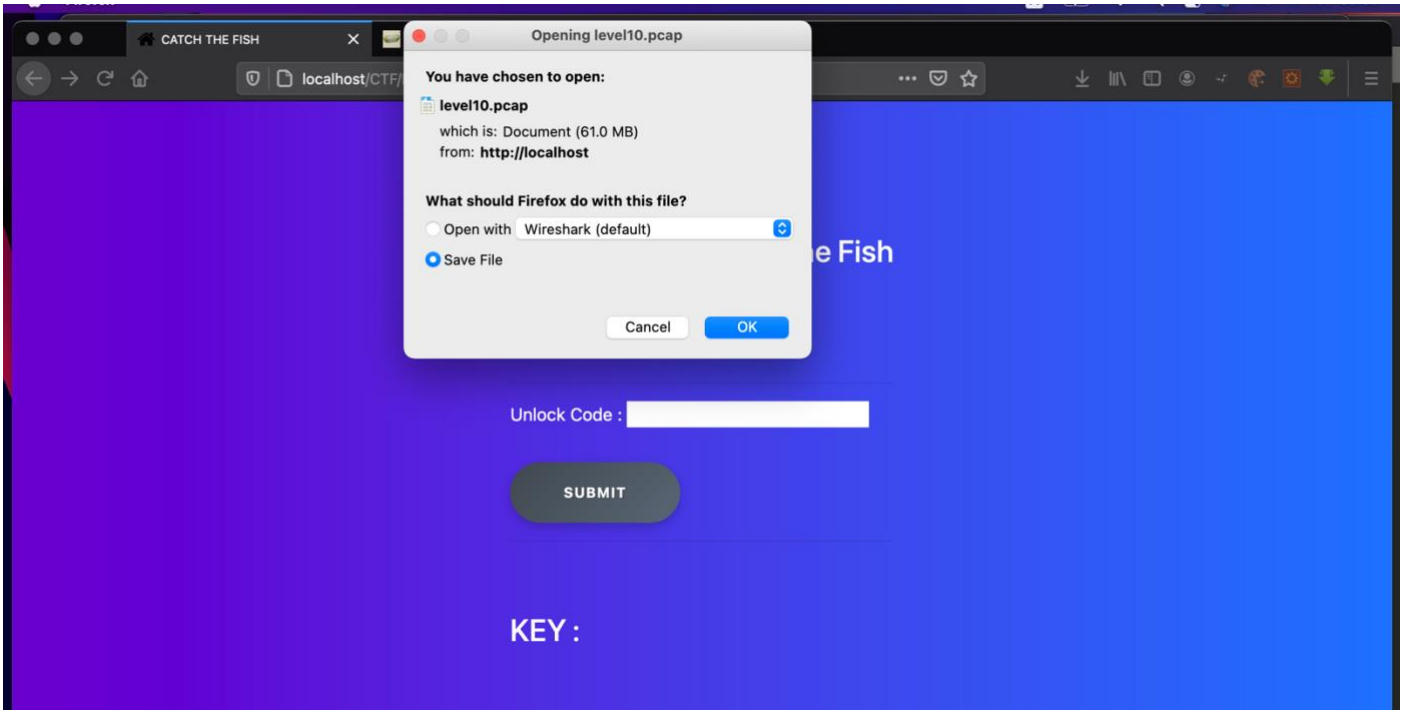
Success..

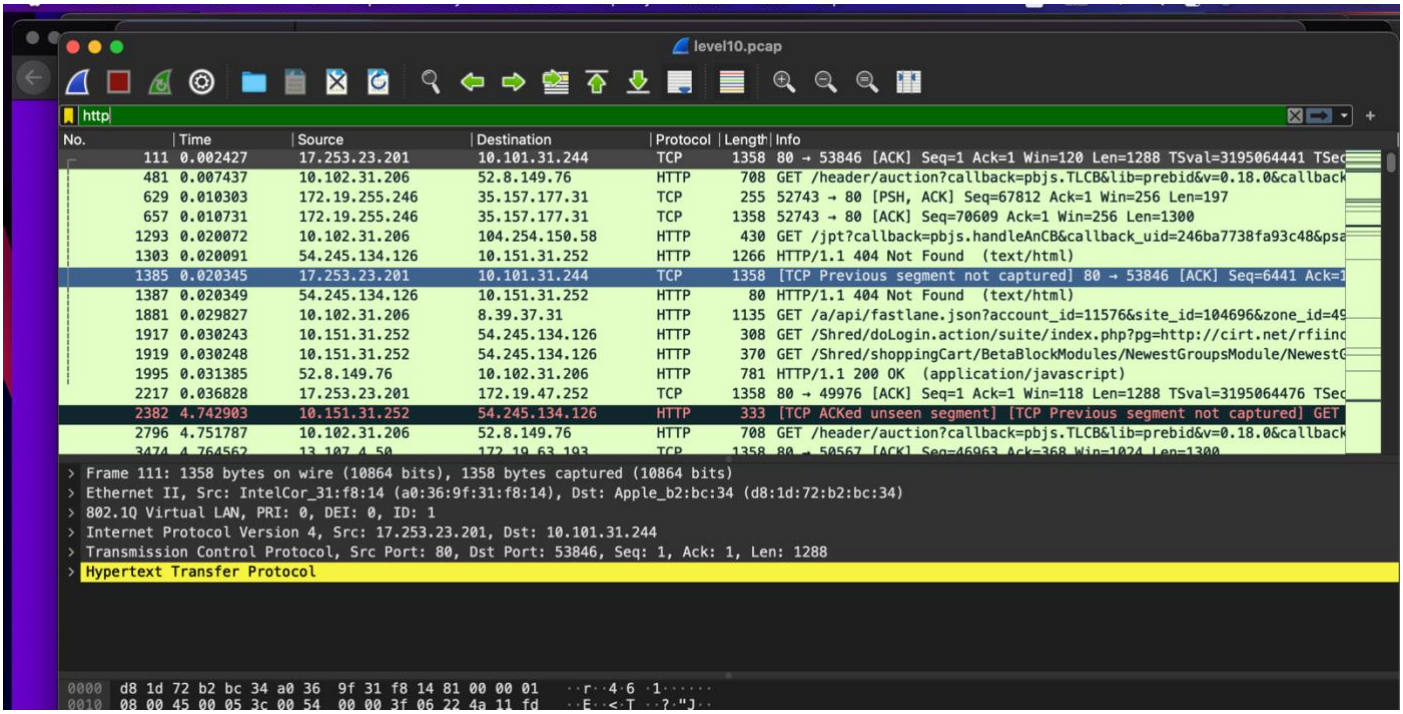


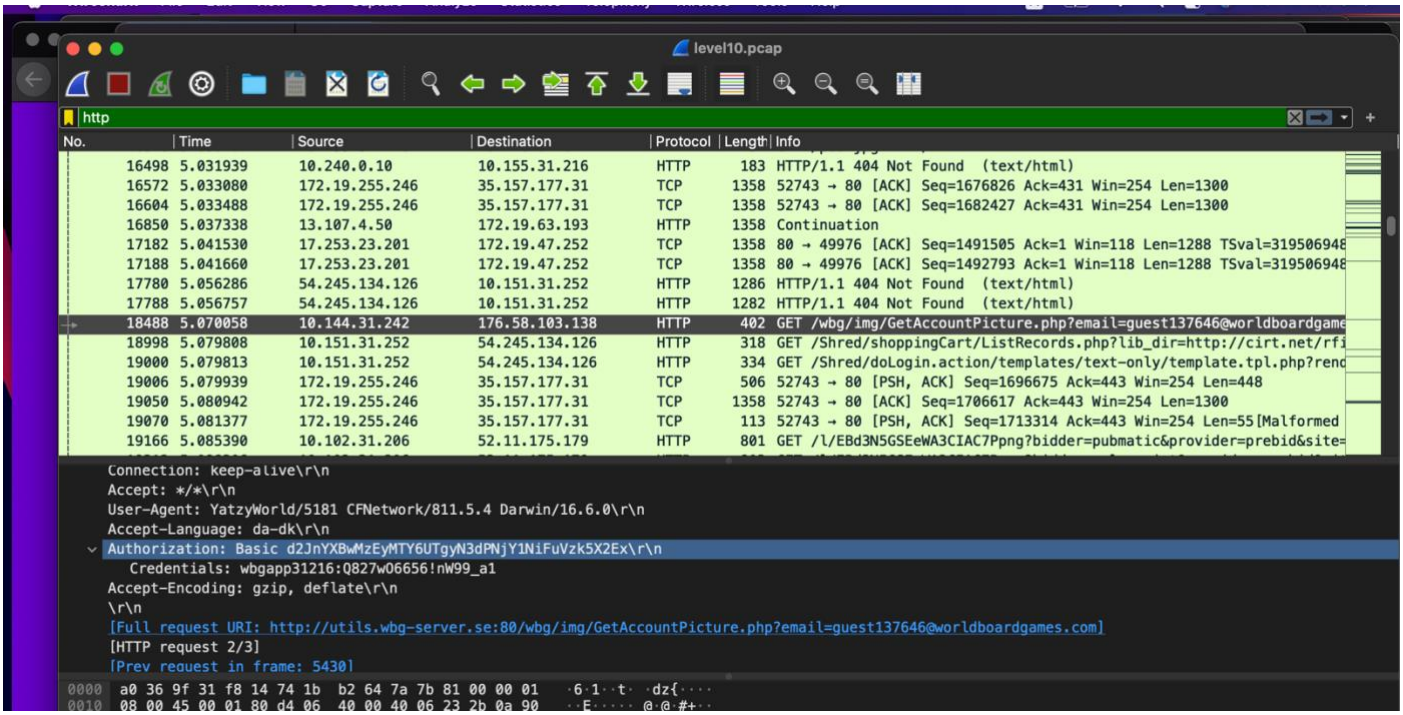
UBYzp8UvZeVzdwVslH9oWHarL1WQSmNt

Level 10	- Capture Shark from Wire 2

In this Level, User has no option to get a clue about the unlock code. When user directly click on the path, a .pcap file will be appeared and user need to investigate and grab correct credential for further modifications.

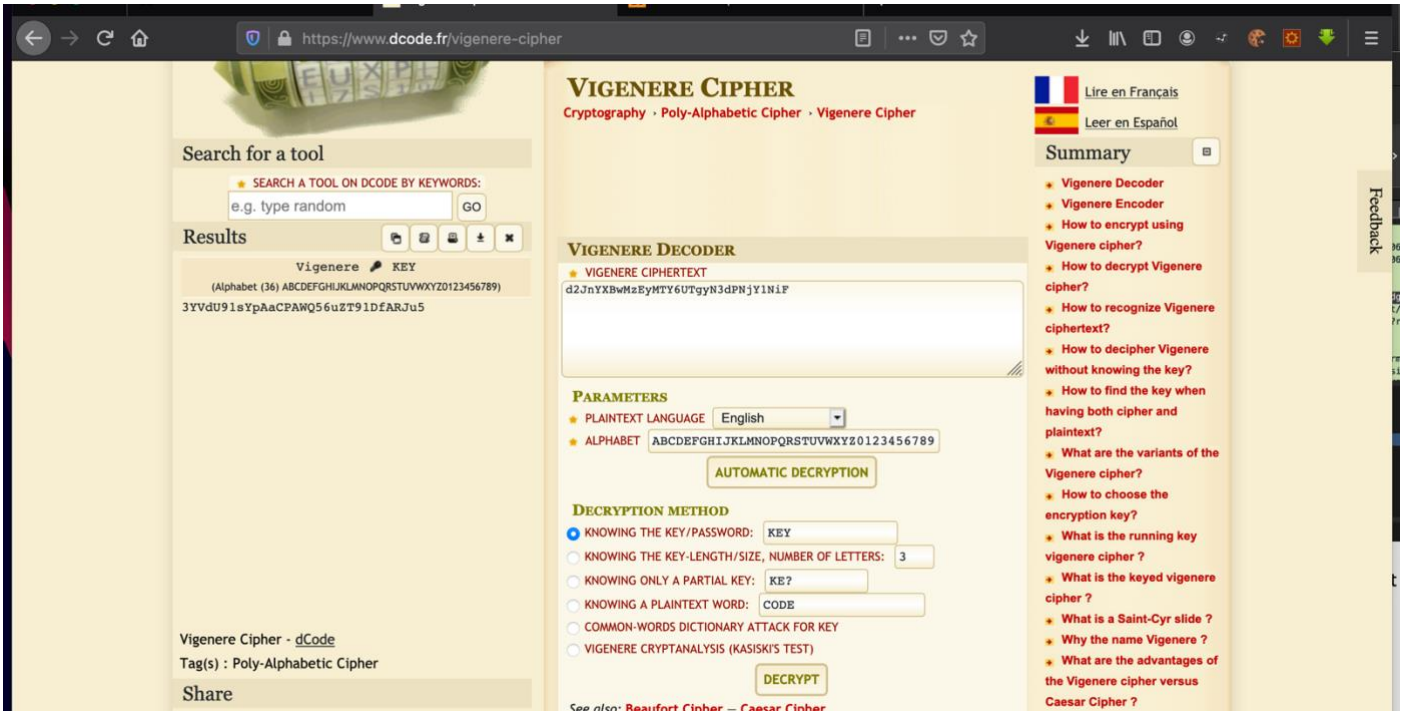




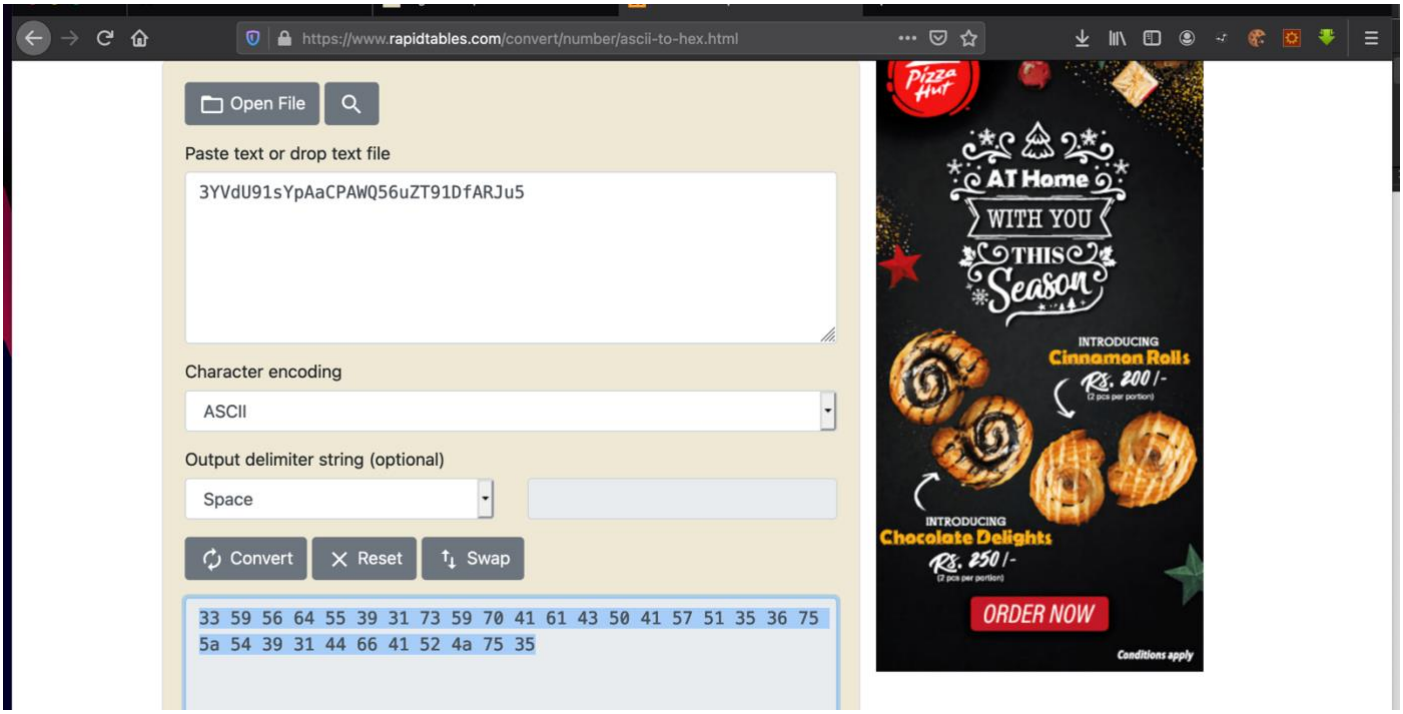


The found Authorization code must be decoded with vegenere cipher to make unlock code in correct format.

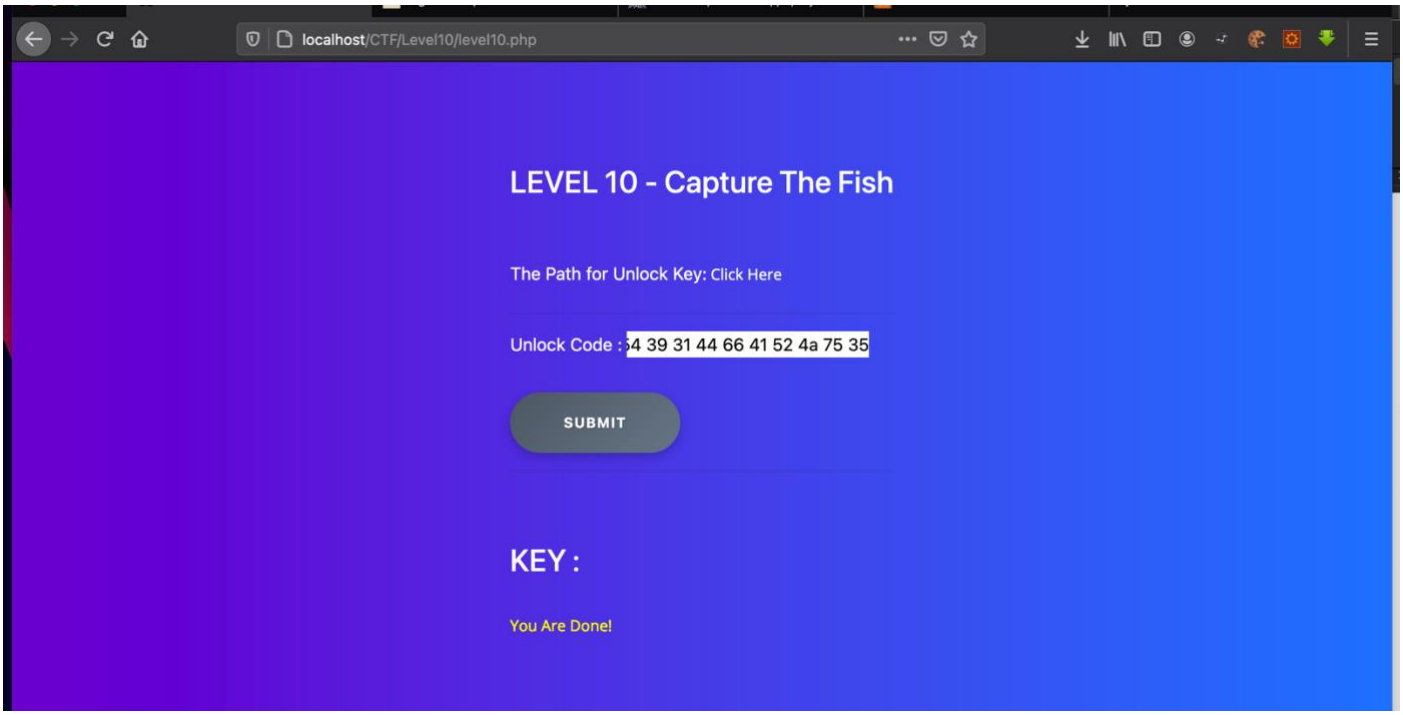
Knowing the PASSWORD as : KEY



Final output must be get out by converting decrypted code to Hex value.

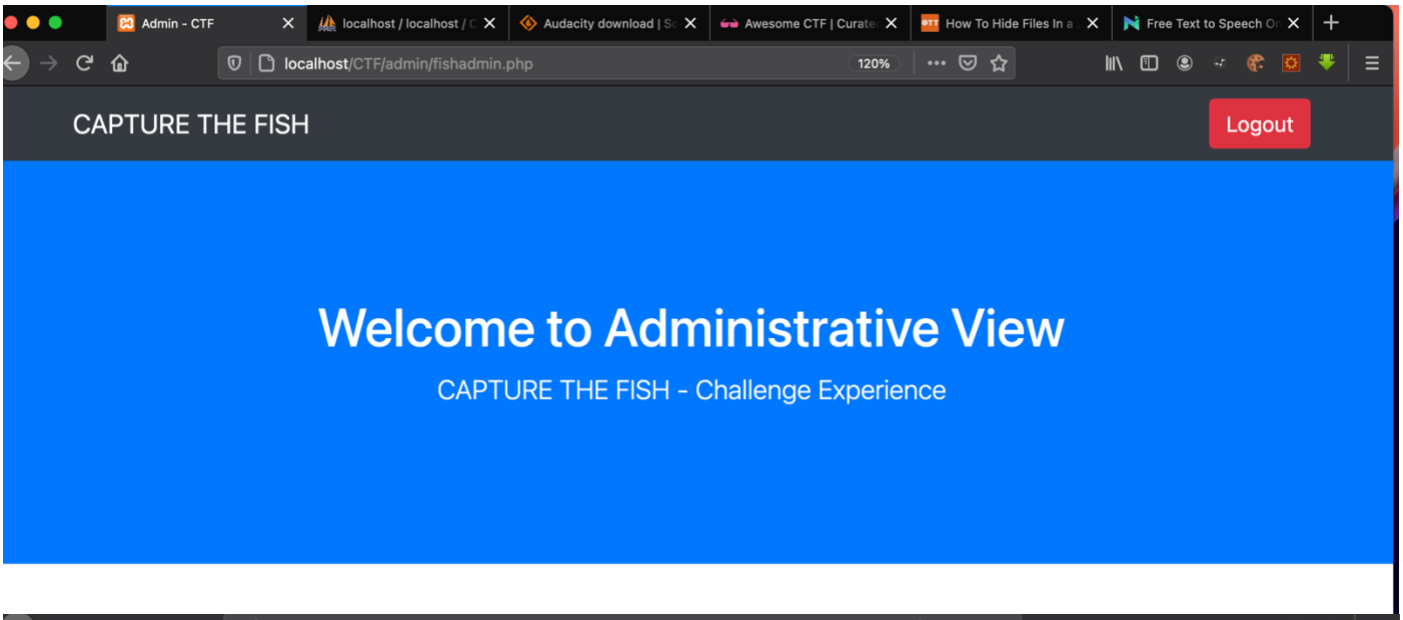


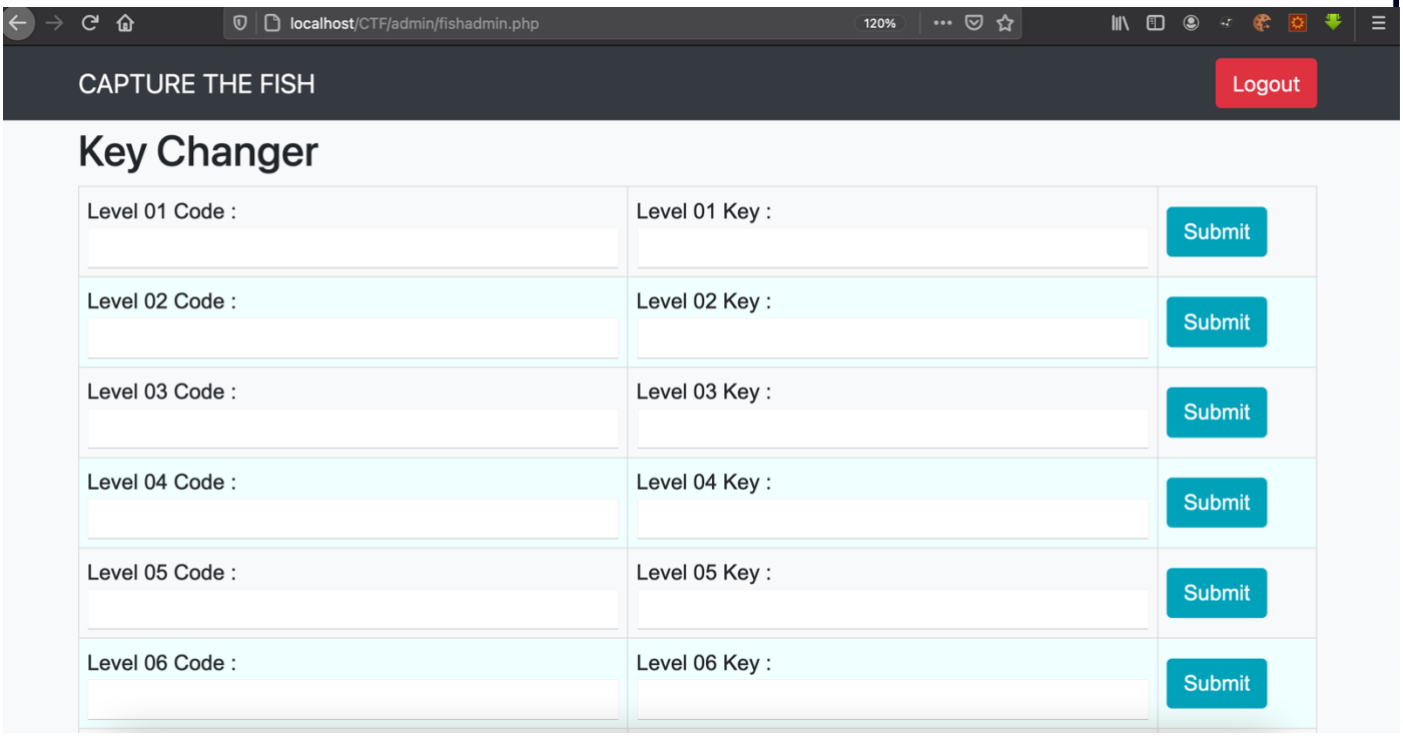
Success..



Administrative View

Administrator in the Catch The Fish Game has interface to change codes and the relavant Key for avoid writeups and spoiler information.





References :

https://www.sneakymonkey.net/2017/03/03/pcap-file-extraction/
https://www.dcode.fr/shift-cipher
https://ctftime.org/writeup/6387
https://book.hacktricks.xyz/forensics/basic-forensics-esp/video-and-audio-file-analysis
https://crackstation.net/
https://www.networkcomputing.com/networking/wireshark-editing-packet?ng_gateway_return=true&full=true

Video Link :
https://mysliit-my.sharepoint.com/:f:/g/personal/it18119336_my_sliit_lk/EkJdW-nJXgREgxx836XG6-0BLQ8vu09Rryg3_yX9elsqxQ?e=hfOsOe