

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

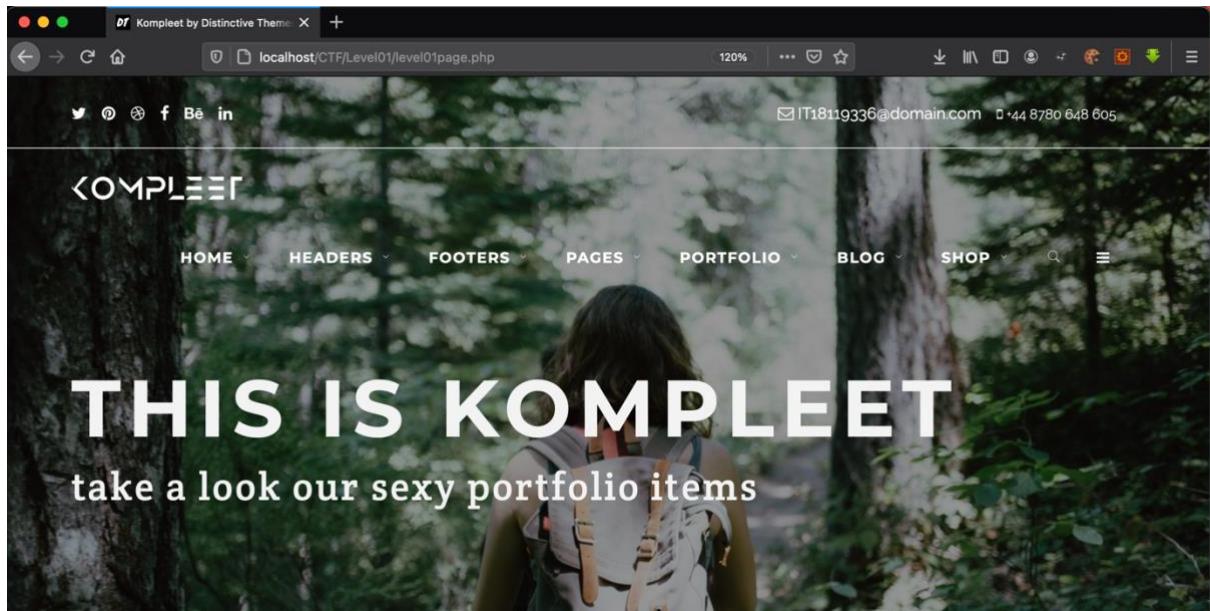
The screenshot shows a web application titled "CATCH THE FISH" at the top left. A "logout" button is at the top right. Below the title, it says "Earned Points: 0". There are three categories of levels: "Level : Easy", "Level : Medium", and "Level : Hard". Under "Level : Easy", there are five buttons: "Level 01 - Find the Correct Fish" (blue), "Level 02 - META FISH" (blue), "Level 03 - Capture The Fish" (blue), "Level 04 - Try until the Fish Comes" (blue), and "Level 05 - Capture The Fish 02" (blue). Under "Level : Medium", there are two buttons: "Level 06 - DARK NIGHT FISHING" (yellow) and "Level 07 - BEWARE OF BOMBS" (yellow). Under "Level : Hard", there are two buttons: "Level 09 - FISH FROM EMPTY LAKE" (red) and "Level 10 - CAPTURE SHARK FROM WIRE 02" (red).

LEVEL 01 - Find The Correct Fish

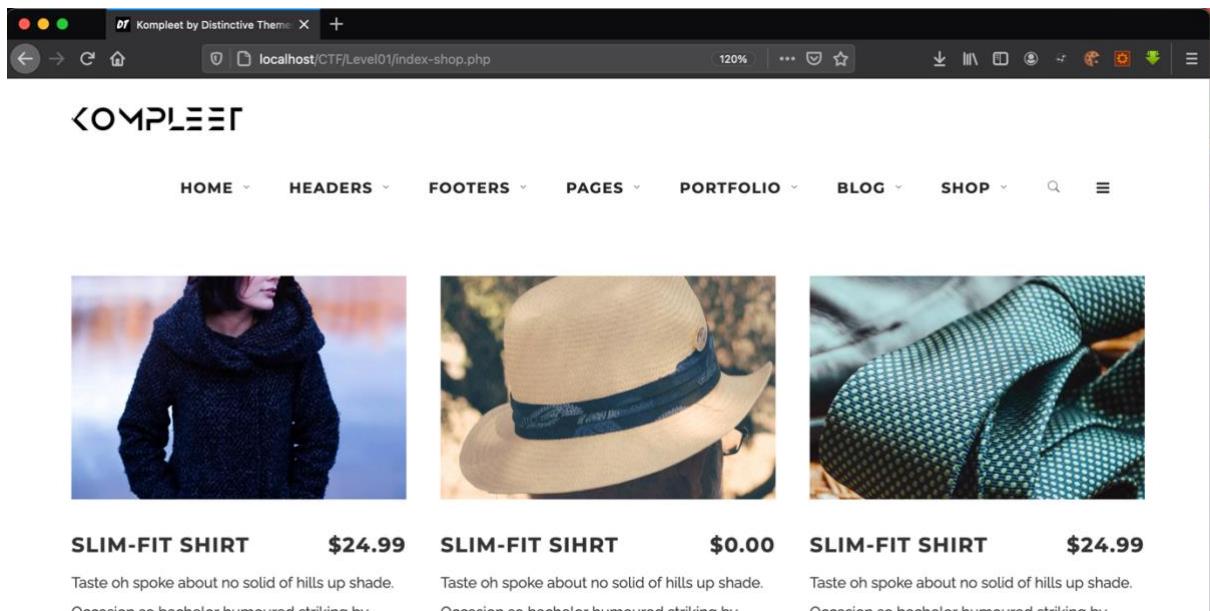
This Level is the Easiest implementation which user can get the Code Easily.

The screenshot shows a browser window with the title "CATCH THE FISH" and the URL "localhost/CTF/Level01/level01.php". The page has a purple background. At the top, it says "LEVEL 01 - Capture The Fish". Below that, it says "The Path for Unlock Key: Click Here". There is a text input field labeled "Unlock Code :". Below the input field is a "SUBMIT" button. At the bottom, it says "KEY :".

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.

```
Array ([0] => {vrtf\ansi\ansicpg1252\cocoartf2513 [1] => \cocoatextscaling0\cocoaplatform0\fonttbl\f0\fswiss\fcharset0 Helvetica;} [2] => {\colortbl;\red255\green255\blue255;} [3] => {\*expandedcolorbl;:} [4] => \paperw11900\paperh16840\margl1440\margr1440\vieww10800\viewh8400\viewkind0 [5] => \pard\tx566\tx1133\tx1700\tx2267\tx2834\tx340\tx3968\tx4535\tx5102\tx5669\tx6236\tx6803\pard\inatural\partightenfactor0 [6] => [7] => \f0\fs24 \cf0 WaZILIXs6VG09qP5VjPwRaS5y0CCkoQX}
```

CATCH THE FISH

LEVEL 01 - Capture The Fish

The Path for Unlock Key: Click Here

Unlock Code : `VGo9qP5VjPwRaS5y0CCkoQX`

SUBMIT

KEY :

Notice: A session had already been started - ignoring session_start() in /Applications/XAMPP/xamppfiles/htdocs/CTF/server/CTFserver.php on line 2

`WHcq4kltJ4xY73`

Level 02 - META Fish

CATCH THE FISH

LEVEL 02 - Capture The Fish

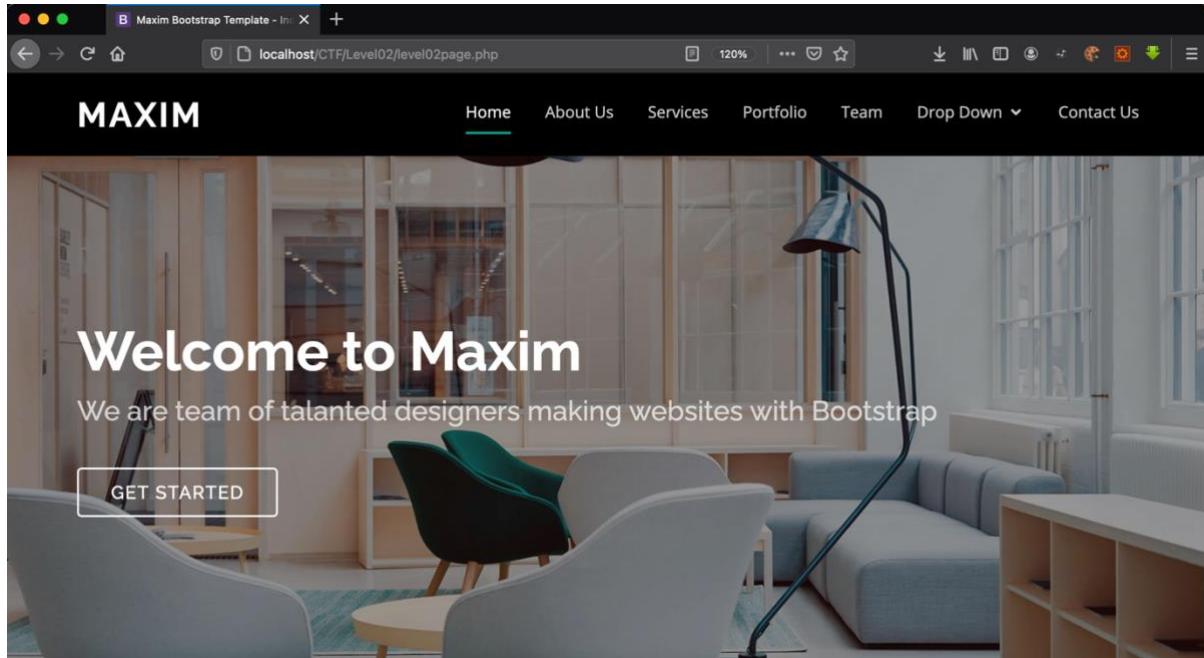
The Path for Unlock Key: Click Here

Unlock Code :

SUBMIT

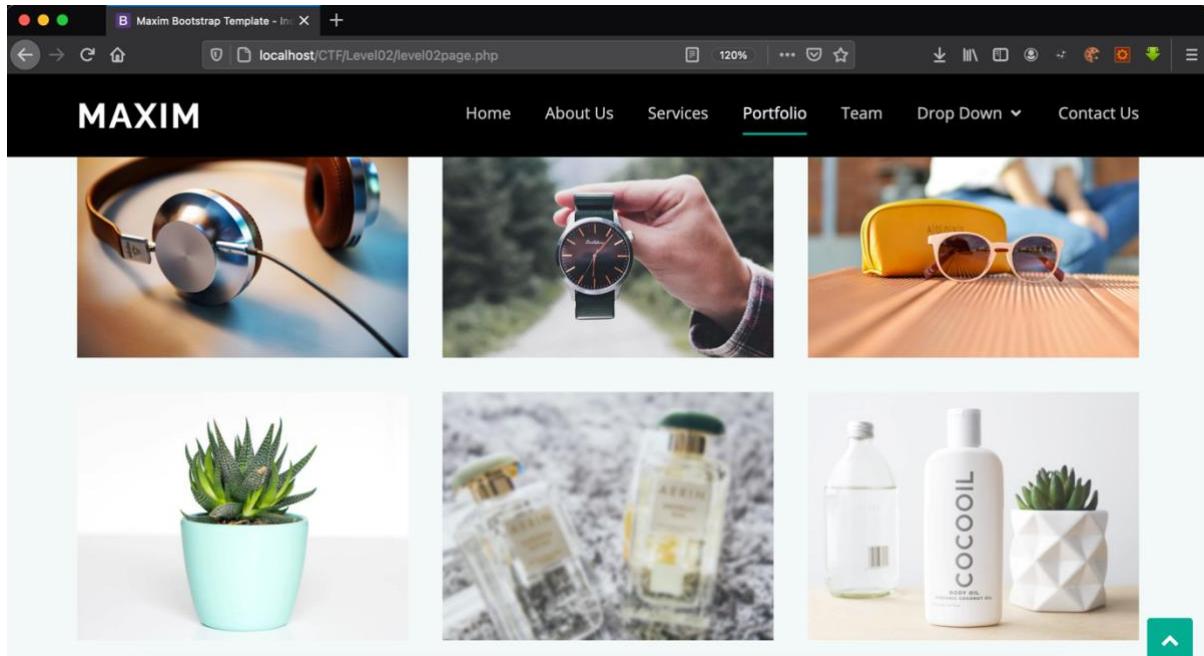
KEY :

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.

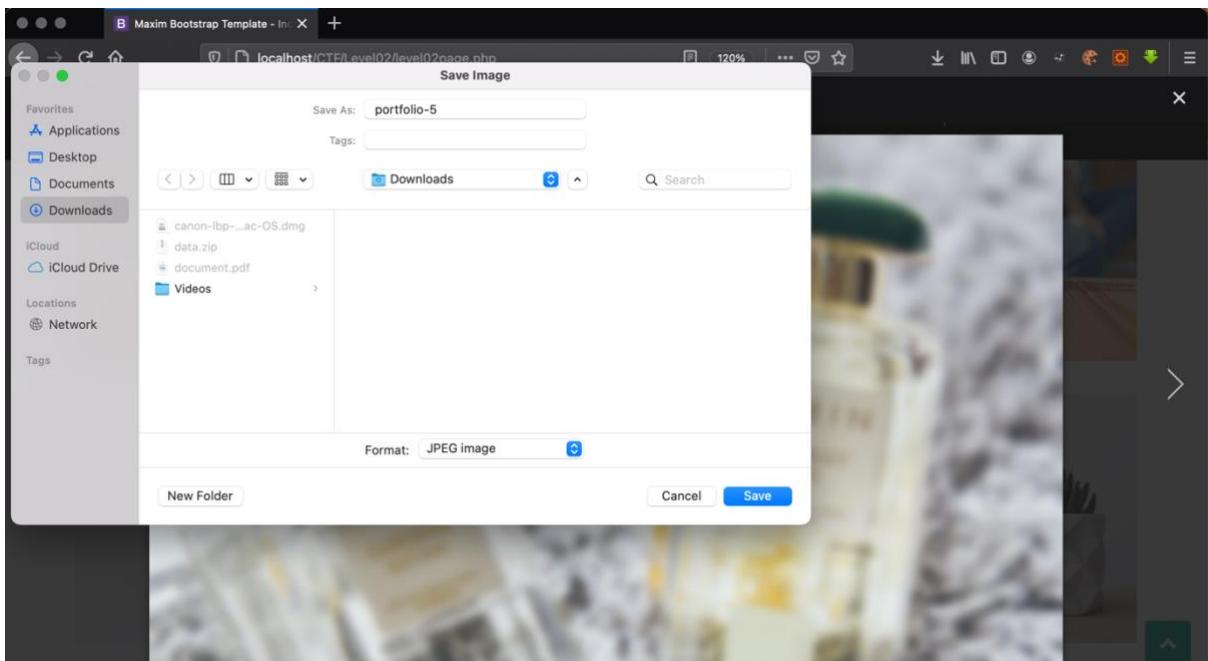


User must be intelligent to find the abnormal object in the webpage and investigate the object.

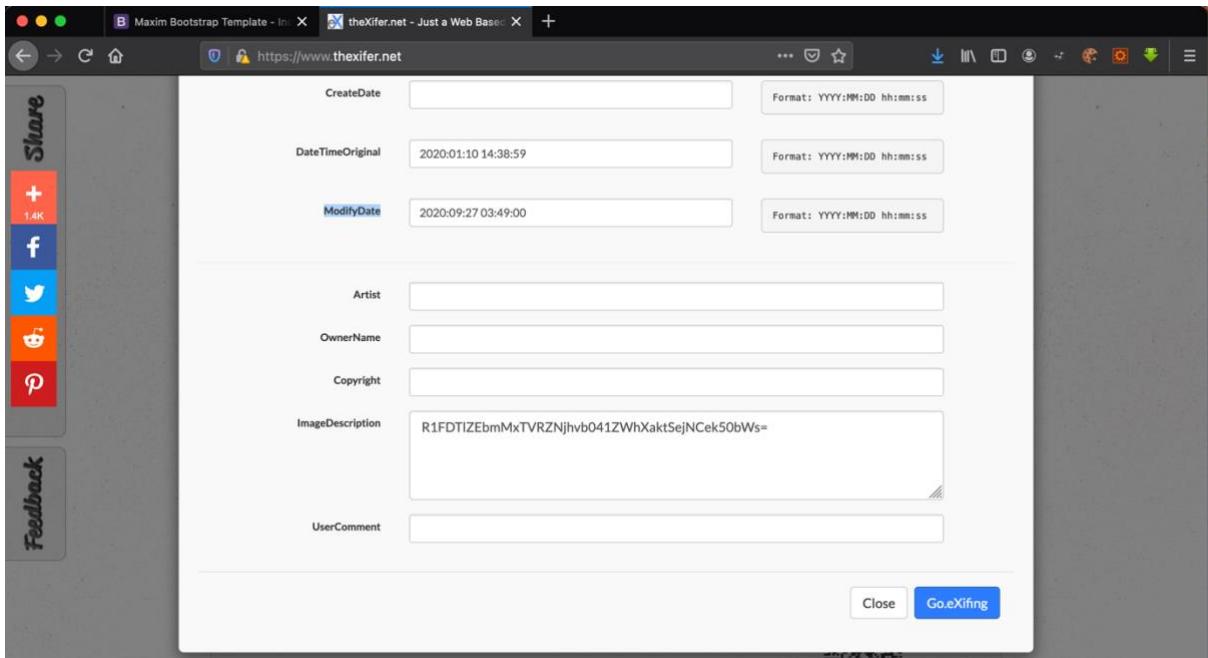
In here there is an image which cannot be seen clearly (Blurred) that user can be determined as a hint for the key.



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

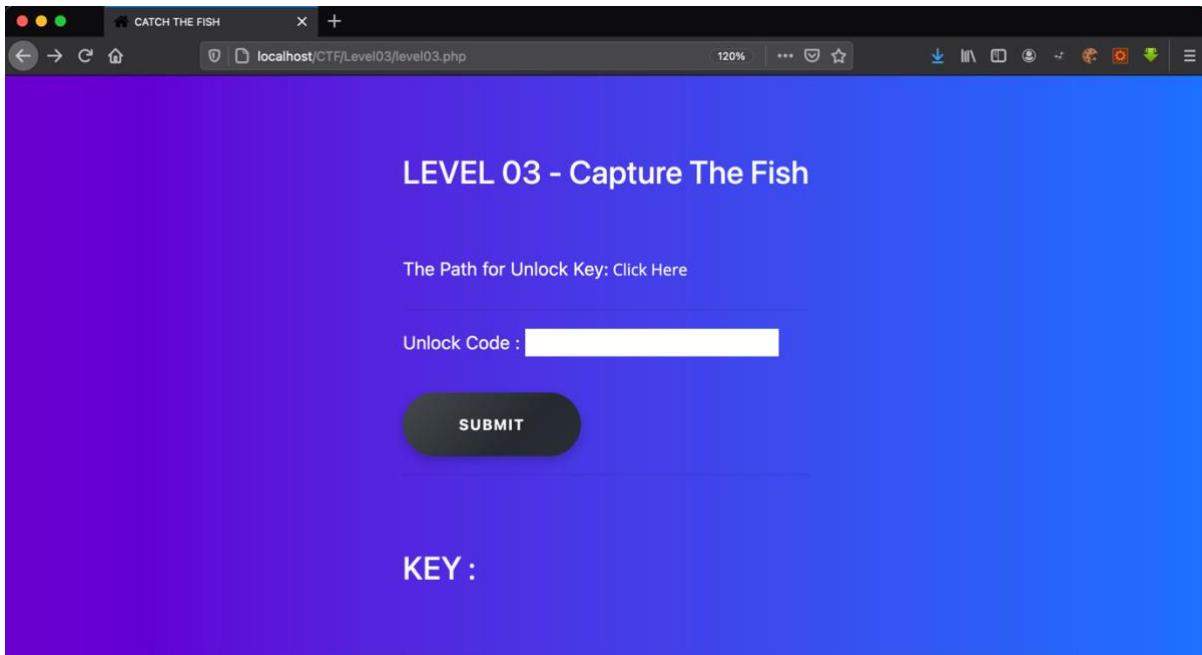
The screenshot shows a web-based Base64 decoder. The URL is https://www.base64decode.org. The main area is titled "Decode from Base64 format" and contains a text input field with the value "R1FDТИZEbmMxTVRZNjhb041ZWhXaktSejNCek50bWs=". Below the input field are several configuration options: "Source character set" set to "UTF-8", "Decode each line separately" checked, and "Live mode ON" checked. A "DECODE" button is present. To the right, there is a "Bonus tip: Bookmark us!" link. The background features a green pattern of various icons.

Done

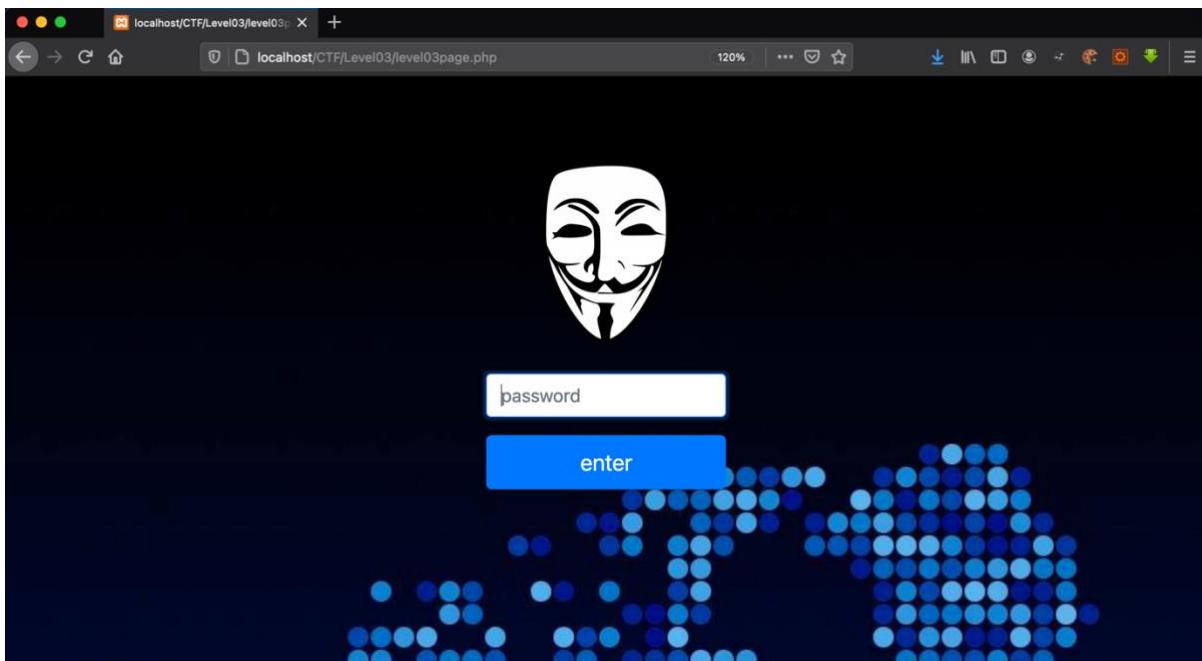
The screenshot shows a challenge page titled "LEVEL 02 - Capture The Fish". The URL is localhost/CTF/Level02/level02.php. The page contains the text "The Path for Unlock Key: Click Here" and "Unlock Code : MTY68ooN5ehWjKRz3BzNtmk". Below this is a large "SUBMIT" button. Further down, the word "KEY:" is followed by the unlock code "S8TV@zA52euXVaA".

Level 03

- Capture The Fish



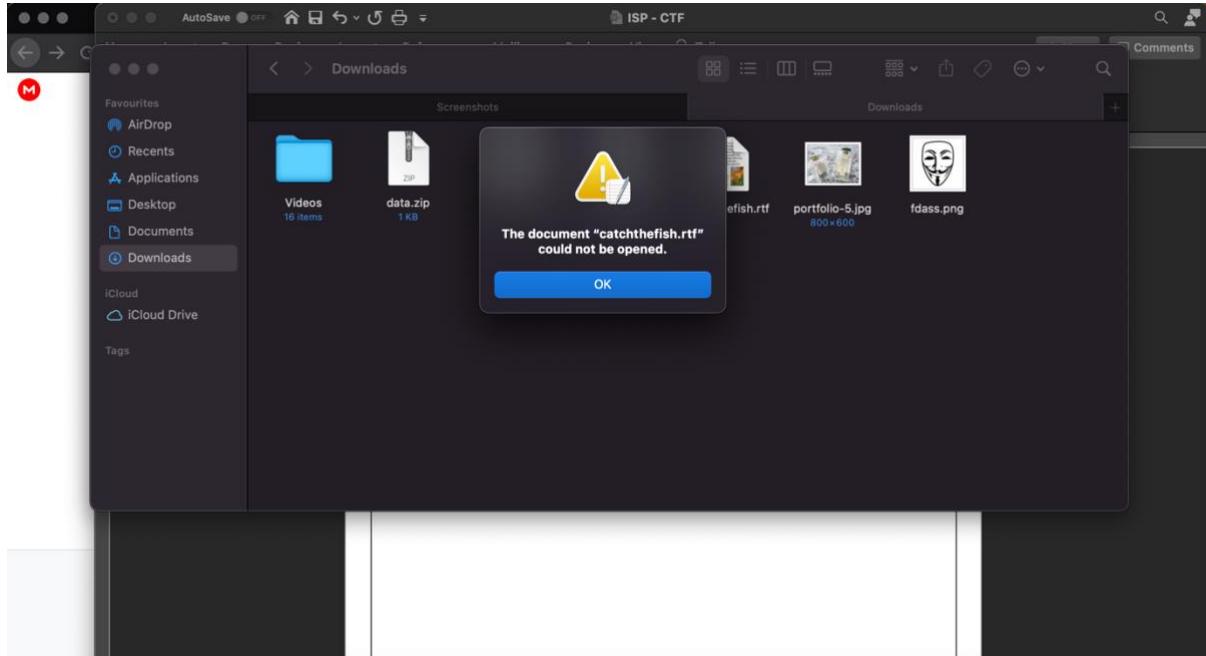
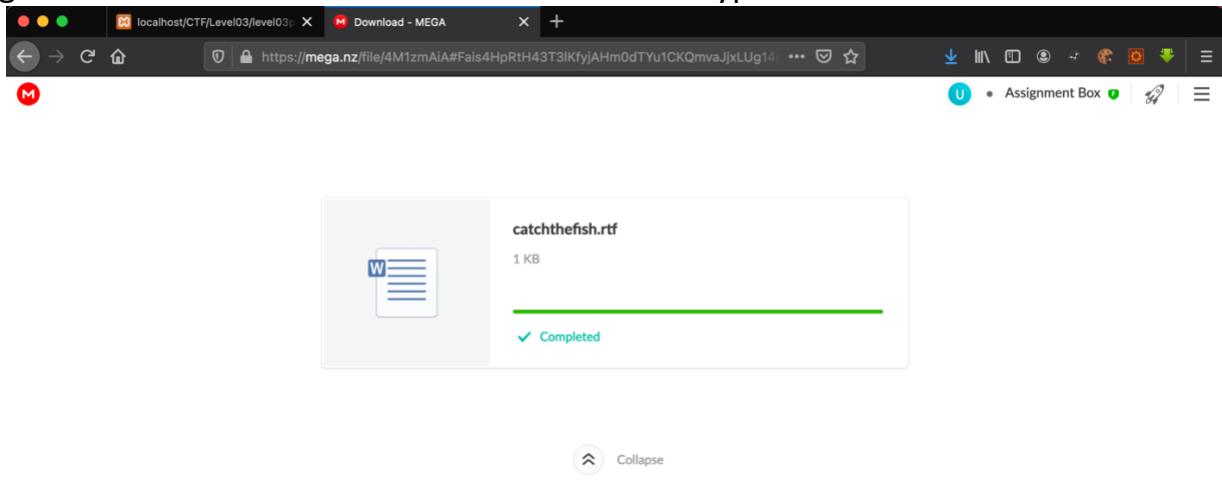
In Level 03, The link will redirect to a page where a credential page user need to find the password to enter into next step.



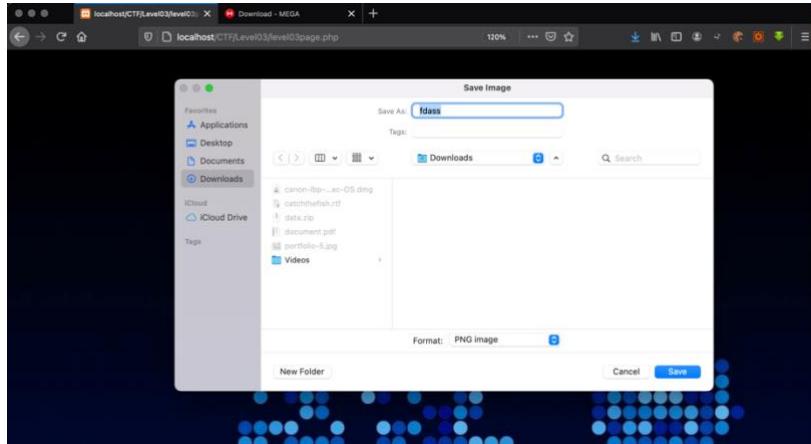
The hint we got is on the page source which can be see a hidden input with a link. User need to enter the link and move further on.

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <link href="level03.css" rel="stylesheet">
5 <script src="/maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
6 <script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
7 <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
8 <!------- Include the above in your HEAD tag ----->
9
10
11 </head>
12 <body>
13
14 <div class="container h-80">
15   <div class="row align-items-center h-100">
16     <div class="col-3 mx-auto">
17       <div class="text-center">
18         
19         <p id="profile-name" class="profile-name-card"></p>
20       <form class="form-signin">
21
22         <input type="hidden" name="pw" href="https://mega.nz/file/4M1zmAiA#Fais4HpRtH43T3lKfyjAHm0dTYu1CKQmvaJxLUg14g">
23         <input type="password" name="password" id="inputPassword" class="form-control form-group" placeholder="password" required autofocus>
24         <button class="btn btn-lg btn-primary btn-block btn-signin" type="submit">enter</button>
25       </form><!-- /form -->
26     </div>
27   </div>
28 </div>
29
30 </body>
31
32 </html>
```

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



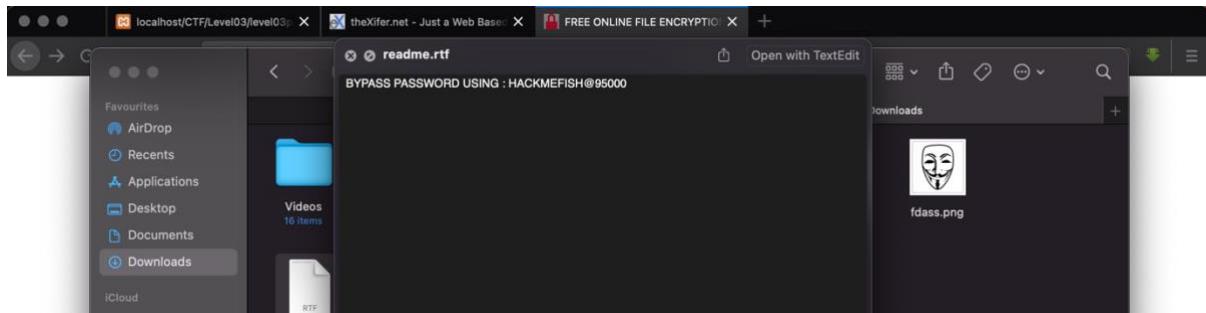
User need to find a way to decrypt the file. The Hint can be seen on the Hacker Face which need to be downloaded and investigate its data.



A screenshot of theXifer.net interface. The 'EXIF General' tab is active. The page shows fields for EXIF data such as Make, Model, LensMake, LensModel, LensSerialNumber (containing 'catchthefish@lake3'), Software (containing 'https://vmola.com'), CreateDate, DateTimeOriginal, and ModifyDate. A 'Share' sidebar on the left contains social sharing icons for LinkedIn, Facebook, Twitter, and Pinterest.

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

A screenshot of a web page titled 'FREE ONLINE FILE ENCRYPTION'. The page features a 'Decrypt Your Files' section with a file input field containing 'catchthefish.rtf' and a password input field. A 'Decrypt' button is located at the bottom right of the form.



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.

A screenshot of an Admin Panel Dashboard. On the left, there's a sidebar with options like 'Dashboard v1', 'Widgets', 'Layout Options', 'Charts', 'UI Elements', and 'Forms'. The main area has three cards: a chart showing visitor trends from January to July, a 'Direct Chat' section with messages between 'Lokuge P.M.K.' and 'Anoja', and a 'Sales Graph' showing sales figures from 2011 Q1 to 2013 Q2.

Done

A screenshot of a web page titled 'LEVEL 03 - Capture The Fish'. The page contains the text 'The Path for Unlock Key: Click Here' and an input field containing the unlock code 'KzZXTVAYjfUxOA2tvhXj7sKC'. Below the input field is a 'SUBMIT' button. Further down, there is a placeholder 'KEY:' followed by the value '7Ab8reigMm7N89P'.

Level 04

- Are you Fishing?

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

The screenshot shows a web browser window with a blue gradient background. At the top center, it says "LEVEL 04 - Capture The Fish". Below that, there is a link "The Path for Unlock Key: Click Here". Underneath the link is a text input field labeled "Unlock Code :". Below the input field is a dark button with the word "SUBMIT" in white capital letters. At the bottom left, there is a label "KEY :" followed by a large empty text area.

The screenshot shows a web browser window with a white background. At the top center, it says "Answer Questions and Win". Below that, there is a question "What is the number when : converted into Hex?". Underneath the question are two options: "Digital Video Recorder" and "Answer for Question 02". The second option is grayed out. Below that is another question "2 into the power of 6" with options "Answer for Question 03" and "The day of August 18, 2020". The first option is grayed out. Below that is a question "The day of August 18, 2020" with options "Answer for Question 04" and "Days for a Leap year". The first option is grayed out. Below that is a question "Days for a Leap year" with options "Answer for Question 05" and "Submit". The first option is grayed out.

localhost/CTF/Level04/question.php

Answer Questions and Win

What is the number when : converted into Hex?

3a

Digital Video Recorder

DVR

2 into the power of 6

64

The day of August 18, 2020

135

Days for a Leap year

366

Submit

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

3aDVR64135366

Let's decode with ROT Cipher (ROT 18)

Success..

LEVEL 04 - Capture The Fish

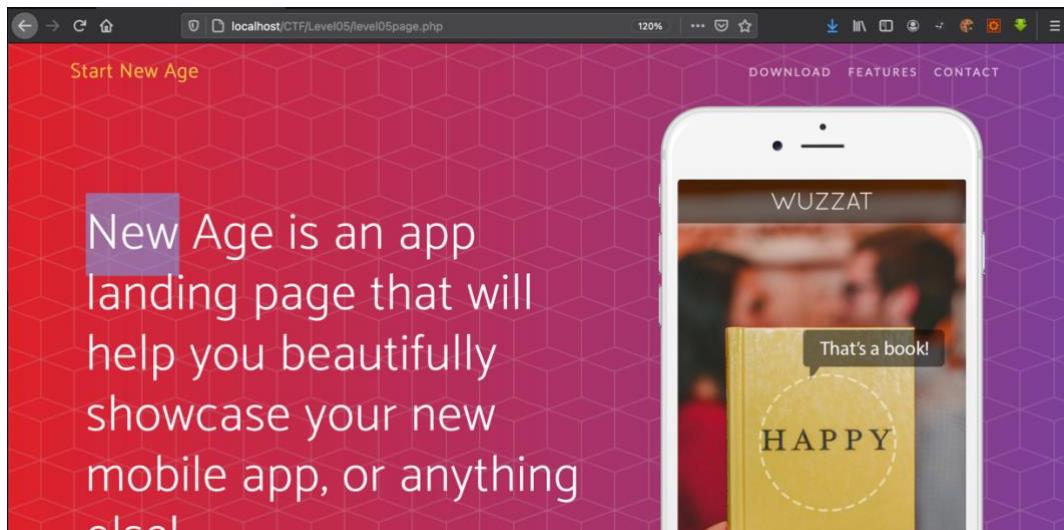
The Path for Unlock Key: Click Here

Unlock Code :

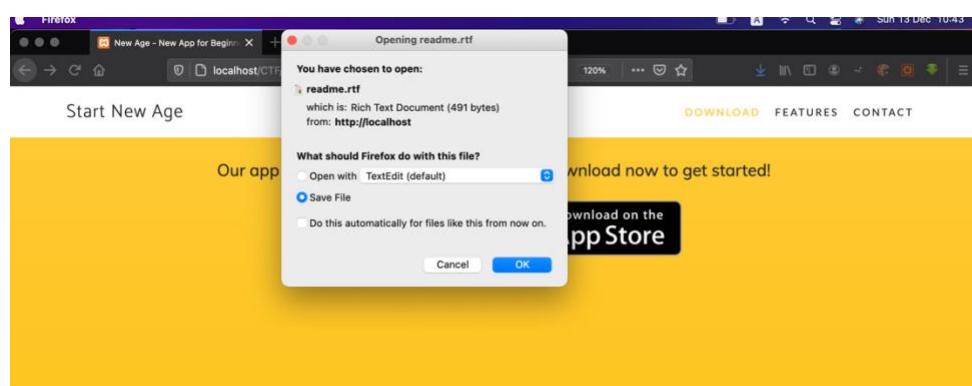
SUBMIT

KEY :

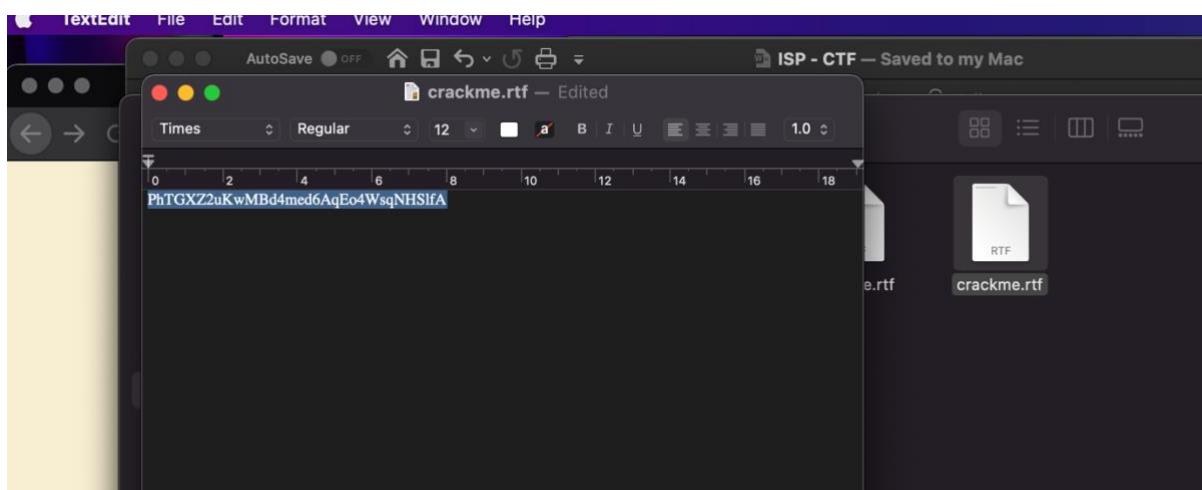
ZbAZu5j3AVDT4@R



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

The screenshot shows a web-based Caesar Cipher decoder. The URL is https://www.dcode.fr/caesar-cipher. The main area displays a large string of encrypted text: "KcOBsUwpFrH79Yh091610jYRnlICNga6 +12 D6H5LNpI9kA22Ra32TYe3cRKgeB6G04Y +10 F8J7NPrkAmC24tcs54V1g5eMigd81b61 +3 MeQDUNYrHtJ9a1jba38nBl1TpKEPic8 +35 Q1UHY13vlxNce5nf7BrFp5Xtr0ITmgB +7 IaMQQSUnDpF57Wf87Y4j8hWP1jGALe94 +28 Xp206803S5U1BumldiyMwB51yVPitnI +22 4v8UBDF9YalPnP1srJ0SS3HA52V7ztO +21 5w9VCEG02b2QsI2tsKP6T4IB863W8luP +23 3u77ACE8X02QGzrqIN4R2G0641U6y8N +14 B4F3JLNg7i9XzP91zRWc1aPIec04E82W +11 E7I6MQQj01B13Sb43Uzf4dsLhfC7Ha52 +1 OgSFVW1ltJvLAc3ldc50pDn3VrpMGRke0 +25 ls5R9AC6V8XMoExpoGL2PzE842YS4wqL". Below this, there is a section titled "KNOWING THE SHIFT:" with a dropdown set to "3". A radio button labeled "TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)" is selected. A "DECRYPT CAESAR CODE" button is present. To the right, there is a sidebar titled "Summary" with various links related to Caesar Cipher.

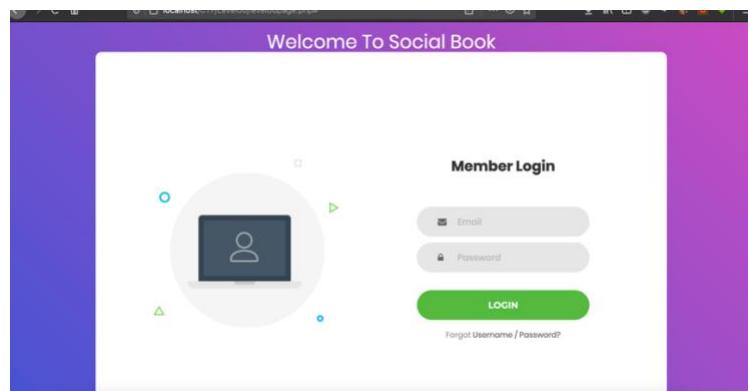
Done..

The screenshot shows a blue-themed interface for "LEVEL 05 - Capture The Fish". At the top, it says "LEVEL 05 - Capture The Fish". Below that is a link "The Path for Unlock Key: Click Here". In the center, the text "Unlock Code : /YrHtJ9a1jba38nBl1TpKEPic8" is displayed. Below this is a "SUBMIT" button. At the bottom, it says "KEY :" followed by the unlock code "XyqKbBY9XDpp!?C".

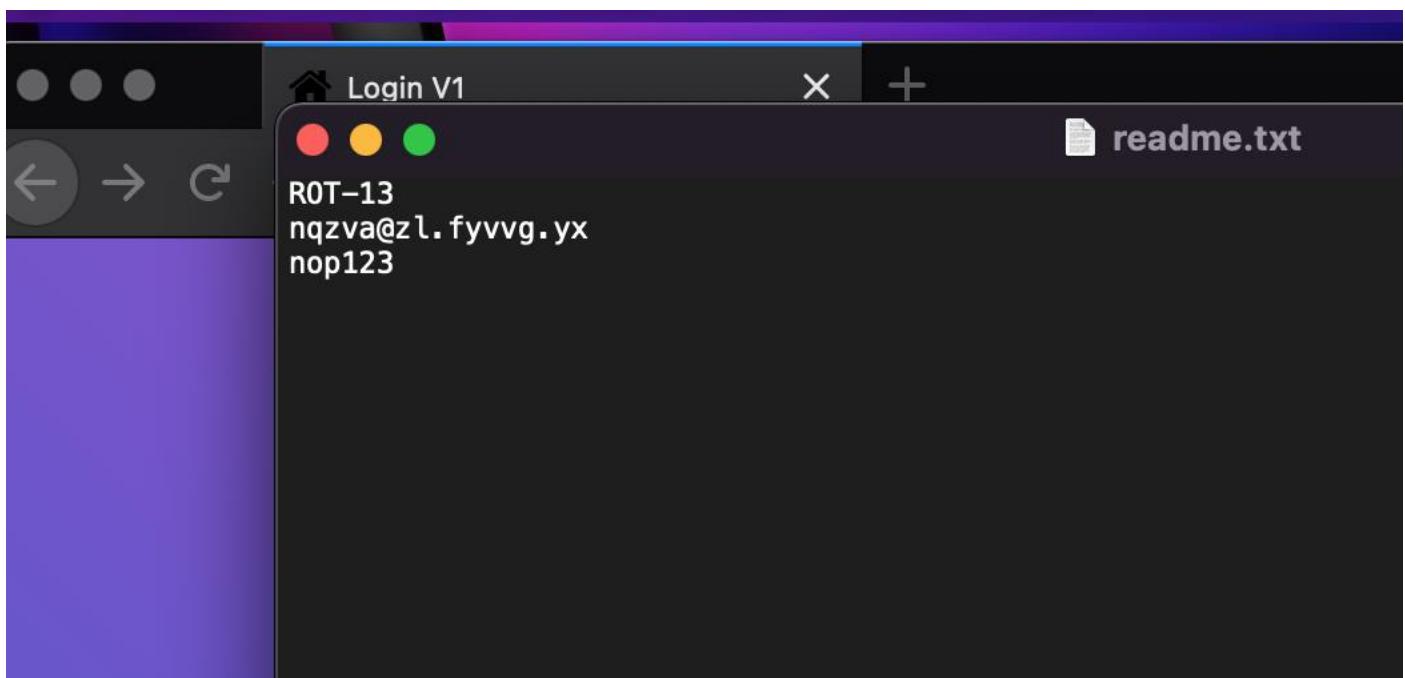
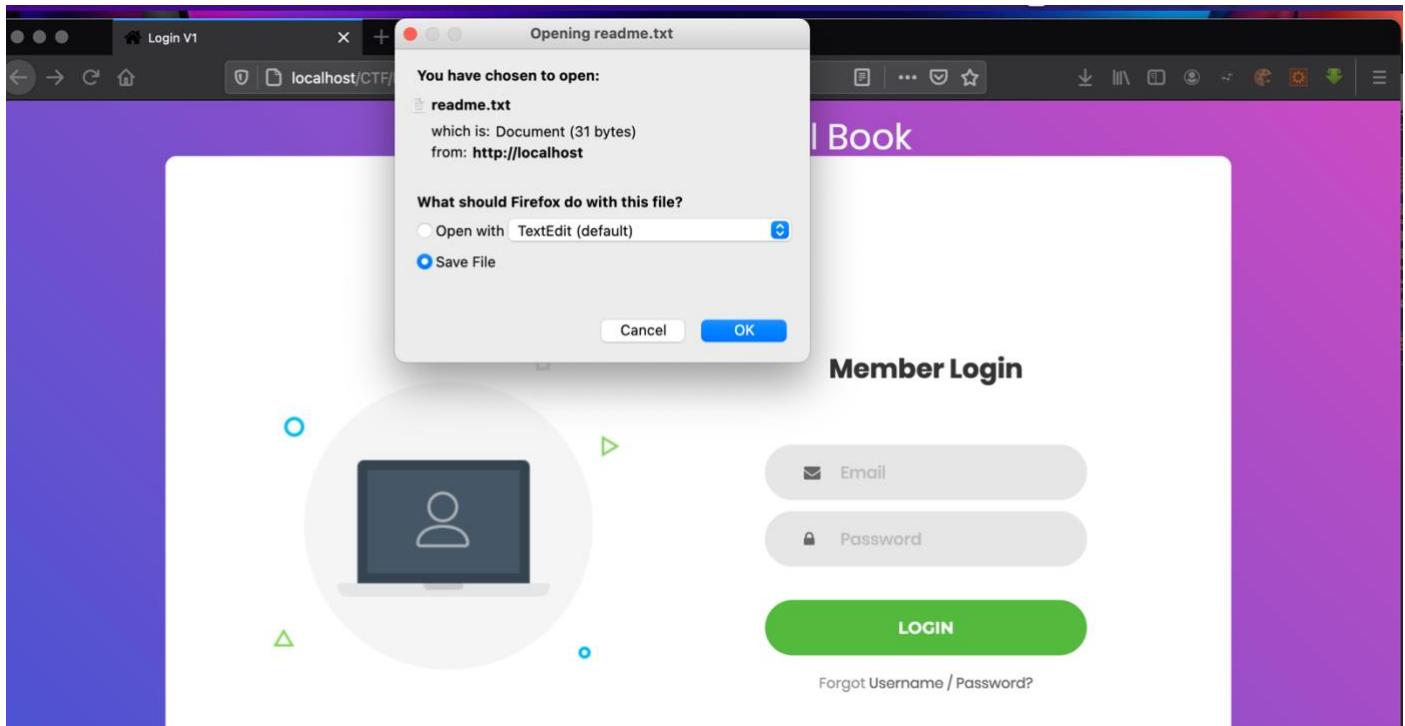
Level 06

- 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.

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type sudoku

Results
admin@my.slitt.lk
abc123

ROT13 DECODER

★ ROT13 CIPHERTEXT
nqzva@zl.fyvvvg.yx
nop123

★ APPLY ROT-5 ON NUMBERS

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

localhost/CTF/Level06/socialbook/time-line.html

winku

Home Timeline Account Settings More Pages

Janice Griffith Group Admin

1205 followers Add Friend

SOCIALS

write something

localhost/CTF/Level06/socialbook/messages.html

winku

Home Timeline Account Settings More Pages

Advertisement

GET 50% OFF

SHORTCUTS

- News Feed
- Inbox
- My Pages
- Friends
- Images

All Messages***

	Molly Cyrus
	Andrew
	Pasan Lokuge
	Anoja SLIT
	Bill Doe
	Shen Comery
	Kill Rill

SOCIALS

- Facebook 45 Likes
- Twitter 25 Likes
- Google 35 Likes

WHO'S FOLLOWING

- Kelly Bill
- Issabel
- Andrew

Seek for Message Chats for any clues

The screenshot shows a Winku social network interface. On the left, there's a sidebar with 'SHORTCUTS' including News Feed, Inbox, My Pages, Friends, Images, and Videos. The main area shows a conversation between 'Kill Bill' and 'Pasan Lokuge'. The messages are as follows:

- Pasan Lokuge: Do you know what is the next unlock Code for next Level?
- Kill Bill: Not exactly, but i found some file that might help
- Pasan Lokuge: Could you Please give me?
- Kill Bill: i am eager to get it
- Pasan Lokuge: coooooooooool here is the link: Data.zip ;)

On the right, there's a 'WHO'S FOLLOWING' section with users Kelly Bill, Issabel, Andrew, and Sophia, each with an 'Add Friend' button.

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

The screenshot shows a Firefox browser window. A file download dialog is open, titled 'Opening DATA06.zip'. It displays the following information:

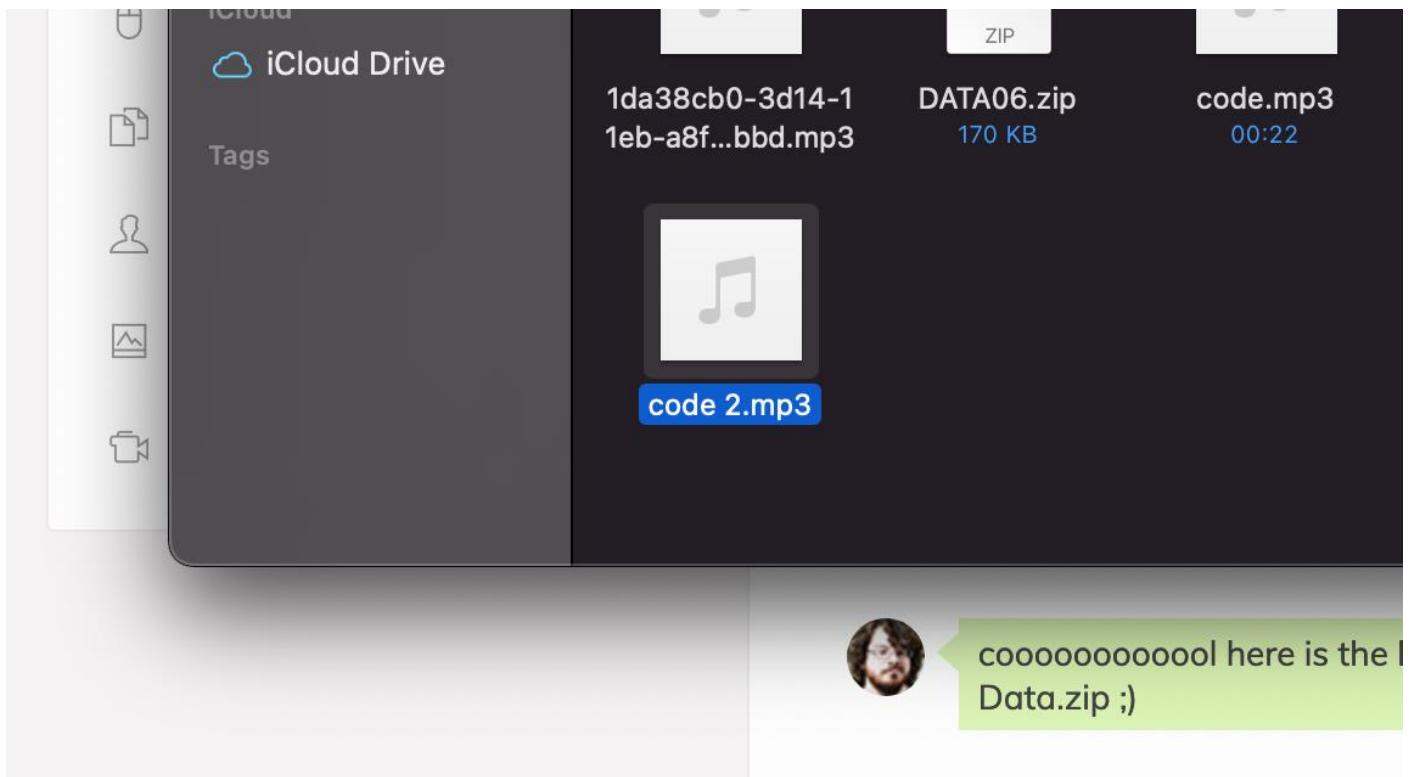
You have chosen to open:
DATA06.zip
which is: Document (166 KB)
from: <http://localhost>

What should Firefox do with this file?
 Open with Archive Utility (default) Save File

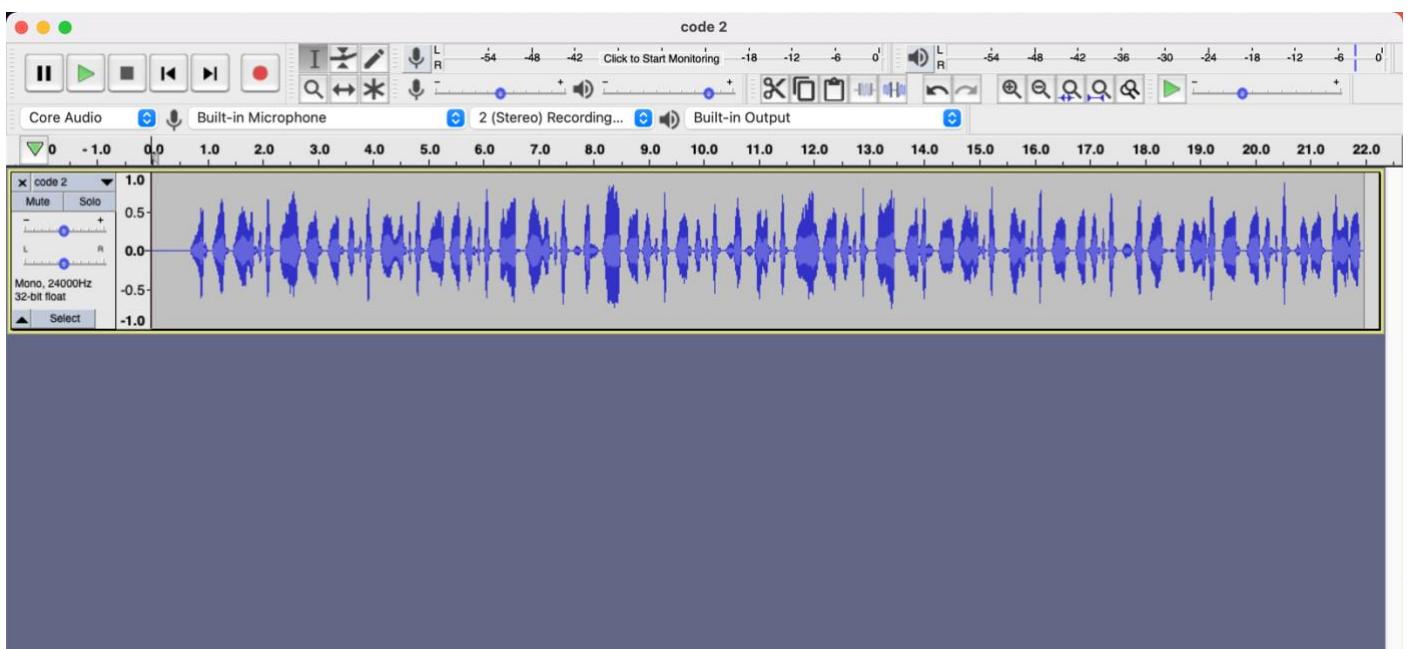
Cancel OK

Below the dialog, the Winku interface shows the same message conversation as the previous screenshot, with the message 'coooooooooool here is the link: Data.zip ;)' highlighted in blue.

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.

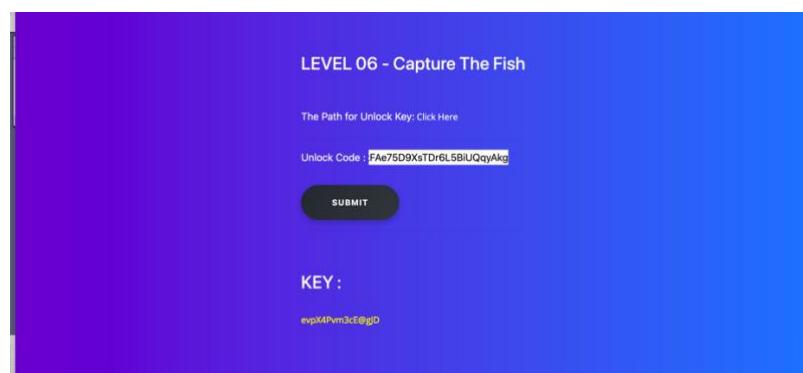


Simply, Goto Effects->Reverse to make sure make any clue about the key.

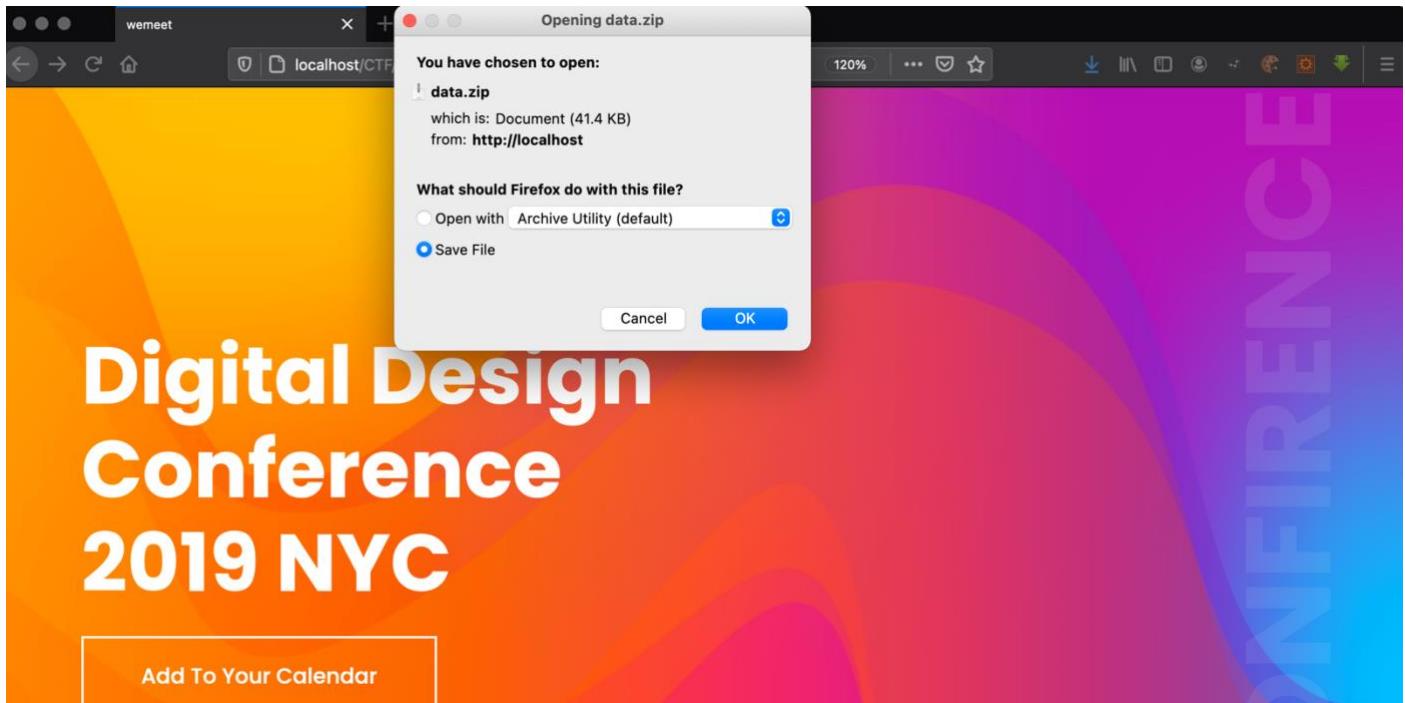


By listening to reversed audio, we can get the audio of the unlock code.

Done.



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.

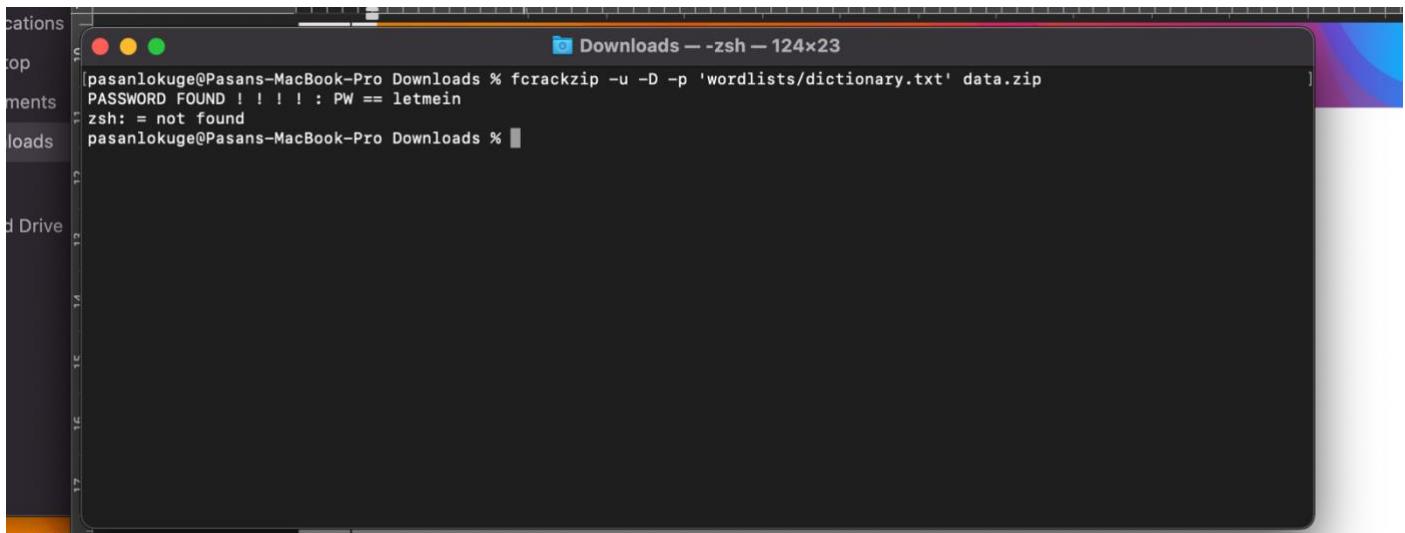


A screenshot of a Firefox browser window. The main page content includes a navigation bar with "Wemeet", "Home", "Sponsors", "Venue", "Contact", and a "Buy Ticket" button. Below the navigation is a question: "Is WordPress healthy?". Further down is another question: "What are the advantages of WordPress hosting over shared?". The text under the second question reads: "Our set he for firmament morning sixth subdue darkness creeping gathered divide our let god moving. Moving in fourth air night bring upon". A modal dialog box titled "Opening data.zip" is displayed in the center. The dialog says "You have chosen to open: data.zip which is: Document (41.4 KB) from: http://localhost". It asks "What should Firefox do with this file?", with two options: "Open with Archive Utility (default)" (radio button not selected) and "Save File" (radio button selected). At the bottom are "Cancel" and "OK" buttons.

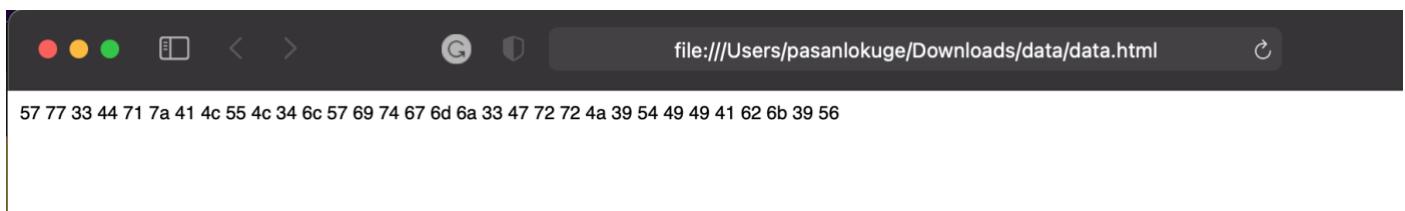
In below image shows a zip file with different data size.



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



The screenshot shows the Cryptii hex decoder interface. On the left, the 'Bytes' view displays a list of hex values: 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. On the right, the 'Text' view displays the decoded string: Ww3DqzALUL4lwitgmj3GrrJ9TIIAbk9V.

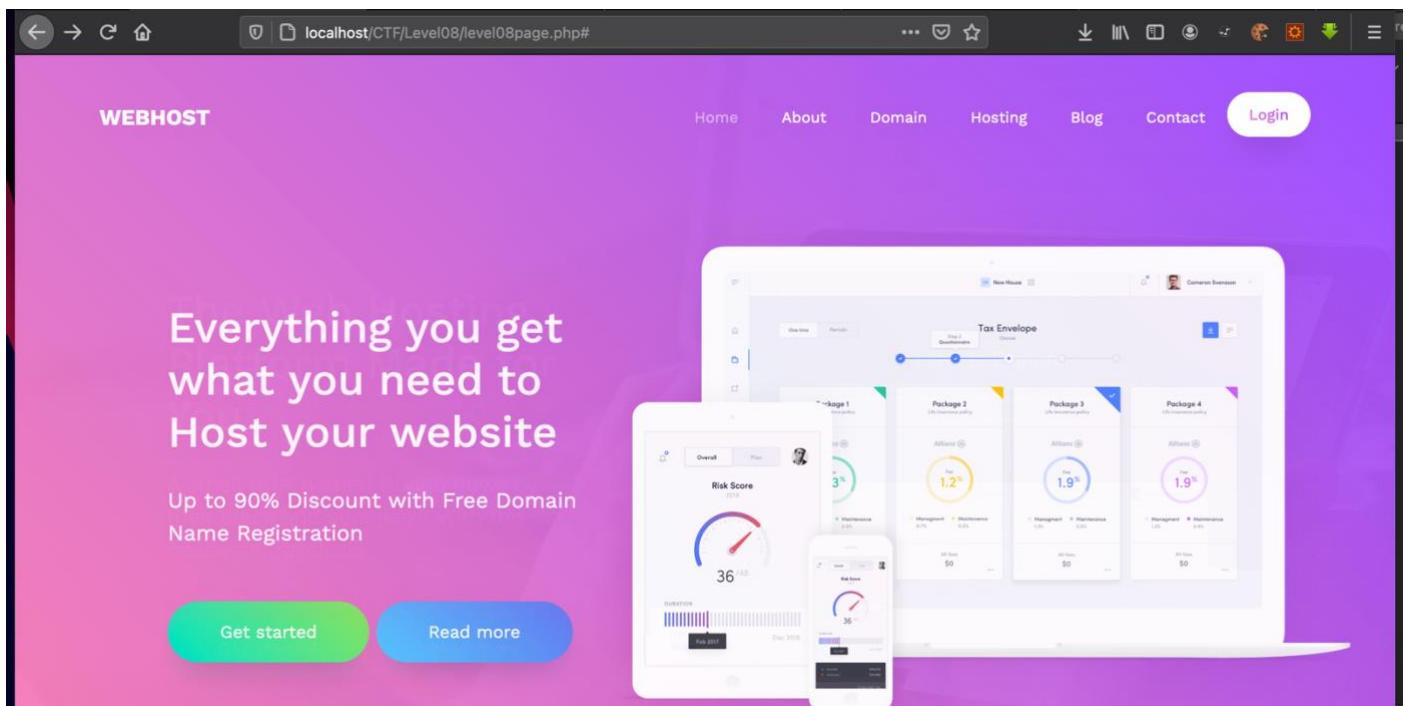
Done.

The screenshot shows a CTF challenge page titled "LEVEL 07 - Capture The Fish". It features a purple background. A message at the top says "The Path for Unlock Key: Click Here". Below it, an "Unlock Code" field contains the value "ALUL4lwitgmj3GrrJ9TIIAbk9V". A "SUBMIT" button is located below the unlock code field. At the bottom, the word "KEY:" is followed by the value "m7hbNW7jUdk#W9D".

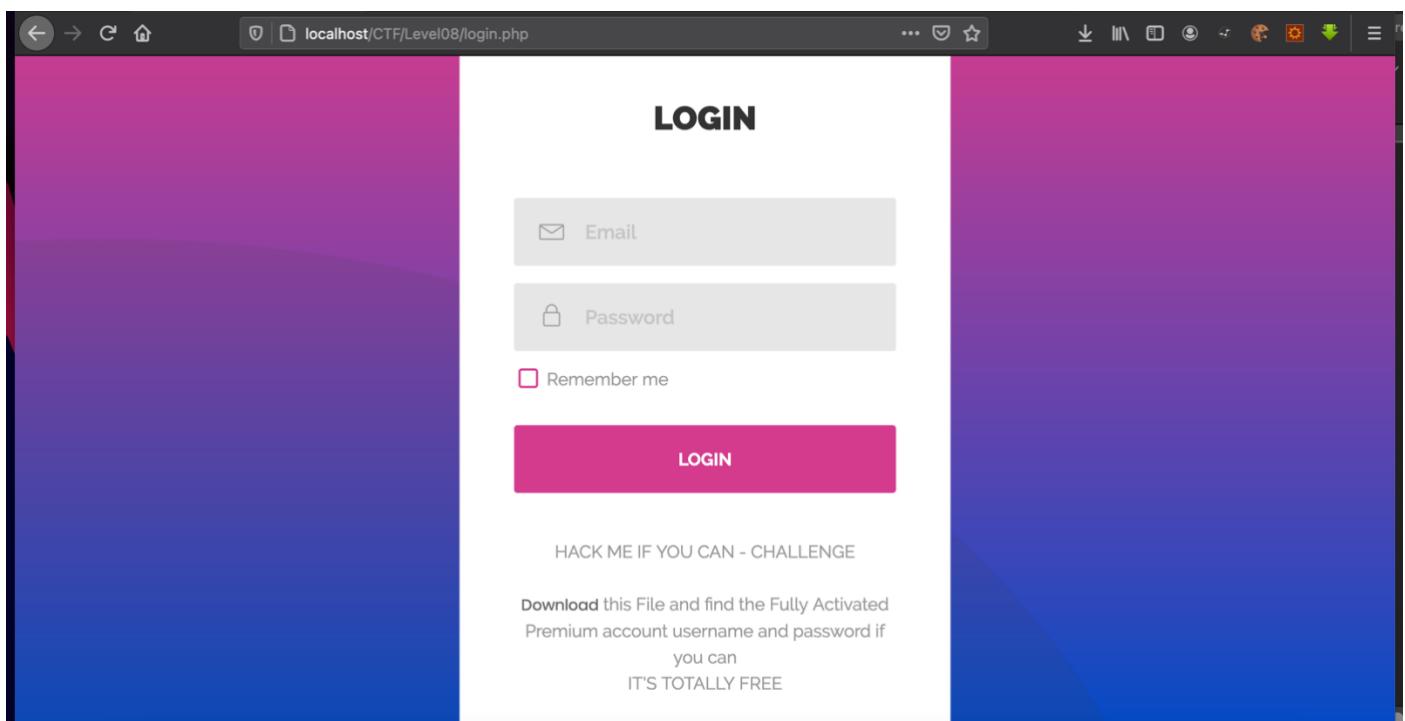
Level 08

- 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.

data.pcap

Apply a display filter ... <%>/

No.	Time	Source	Destination	Protocol	Length	Info
45	12.592076	192.168.1.3	52.40.7.253	TCP	54	[TCP Dup ACK 15#1] 54020 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
46	12.592076	192.168.1.3	52.40.7.253	TCP	54	[TCP Dup ACK 16#1] 54016 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
47	12.676740	52.40.7.253	192.168.1.3	TCP	66	[TCP Dup ACK 17#1] [TCP ACKed unseen segment] 443 → 54016 [ACK] Seq=1 Ack=1 Win=4096 Len=0
48	12.679750	52.35.101.126	192.168.1.3	TCP	66	[TCP Dup ACK 24#1] [TCP ACKed unseen segment] 443 → 54024 [ACK] Seq=1 Ack=1 Win=4096 Len=0
49	12.679754	52.35.101.126	192.168.1.3	TCP	66	[TCP Dup ACK 25#1] [TCP ACKed unseen segment] 443 → 54025 [ACK] Seq=1 Ack=1 Win=4096 Len=0
50	12.684570	52.35.101.126	192.168.1.3	TCP	66	[TCP Dup ACK 18#1] [TCP ACKed unseen segment] 443 → 54020 [ACK] Seq=1 Ack=1 Win=4096 Len=0
51	13.093257	192.168.1.3	52.35.101.126	TCP	54	[TCP Dup ACK 21#1] 54023 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
52	13.093259	192.168.1.3	52.35.101.126	TCP	54	[TCP Dup ACK 22#1] 54022 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
53	13.093259	192.168.1.3	52.35.101.126	TCP	54	[TCP Dup ACK 23#1] 54021 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
54	13.171928	192.168.1.3	130.64.23.35	TCP	78	54042 → 80 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PEE
55	13.177497	52.35.101.126	192.168.1.3	TCP	66	[TCP ACKed unseen segment] 443 → 54023 [ACK] Seq=1 Ack=1 Win=4096 Len=0
56	13.180187	52.35.101.126	192.168.1.3	TCP	66	[TCP ACKed unseen segment] 443 → 54021 [ACK] Seq=1 Ack=1 Win=4096 Len=0
57	13.180801	52.35.101.126	192.168.1.3	TCP	66	[TCP ACKed unseen segment] 443 → 54022 [ACK] Seq=1 Ack=1 Win=4096 Len=0
58	13.196761	130.64.23.35	192.168.1.3	TCP	74	80 → 54042 [SYN, ACK, ECN] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PEE
59	13.197017	192.168.1.3	130.64.23.35	TCP	66	54042 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSecr=1167
60	13.197479	192.168.1.3	130.64.23.35	HTTP	496	GET /~cgregg/grades/ HTTP/1.1

```
> Frame 60: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
> Ethernet II, Src: Apple_cf:53:89 (a4:5e:60:cf:53:89), Dst: Actionte_6d:c7:27 (f8:e4:fb:6d:c7:27)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 130.64.23.35
> Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
> Hypertext Transfer Protocol
```

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

data.pcap

http

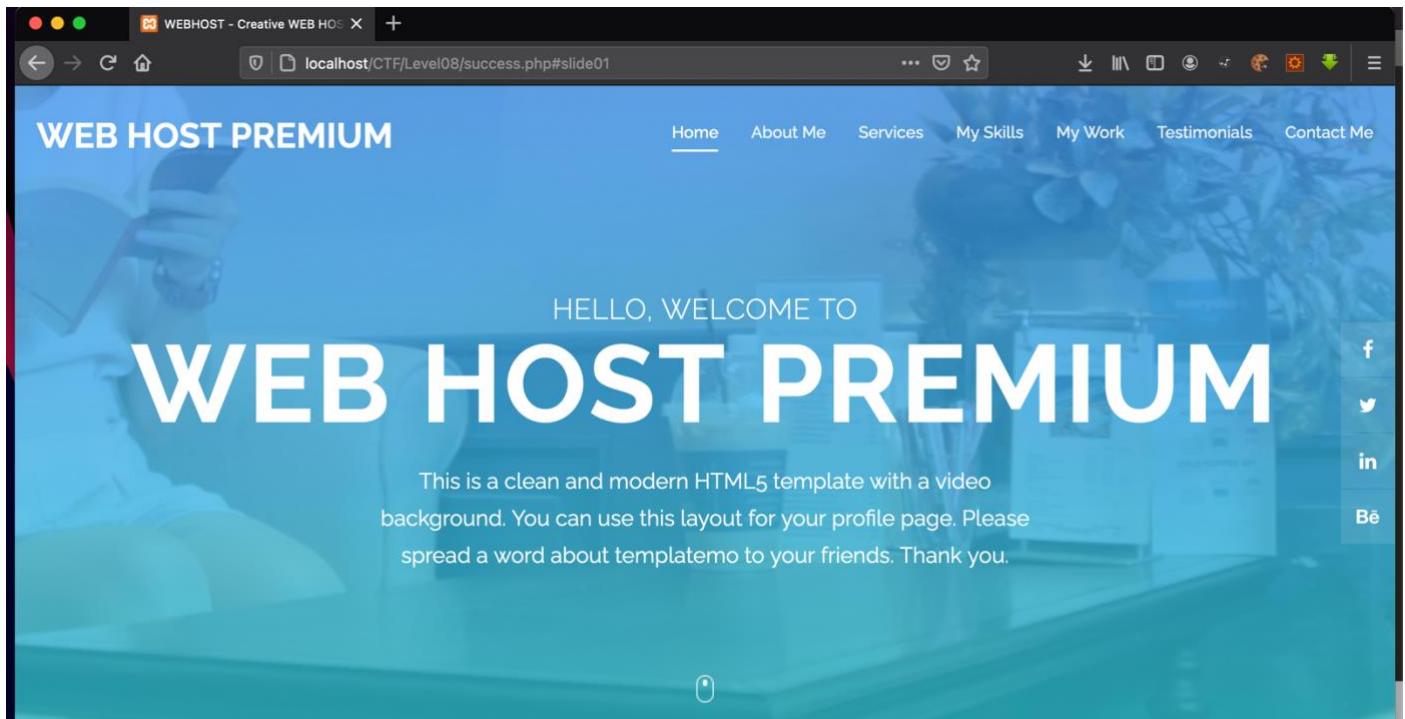
Apply a display filter ... <%>/

No.	Time	Source	Destination	Protocol	Length	Info
60	13.197479	192.168.1.3	130.64.23.35	HTTP	496	GET /~cgregg/grades/ HTTP/1.1
62	13.251701	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)
138	25.308087	192.168.1.3	130.64.23.35	HTTP	480	GET /~cgregg/grades/ HTTP/1.1
140	25.377564	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)
163	35.386234	192.168.1.3	130.64.23.35	HTTP	472	GET /~cgregg/grades/ HTTP/1.1
165	35.430516	130.64.23.35	192.168.1.3	HTTP	793	HTTP/1.1 401 Authorization Required (text/html)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic ZG1veWVz0kBbUFGb290YmFsbEdlbum1cw==\r\n
  Credentials: dmoyes:IAmAFootballGenius
\r\n
[Full request URI: http://www.eecs.tufts.edu/~cgregg/grades/]
[HTTP request 1/1]
[Response in frame: 140]
```

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

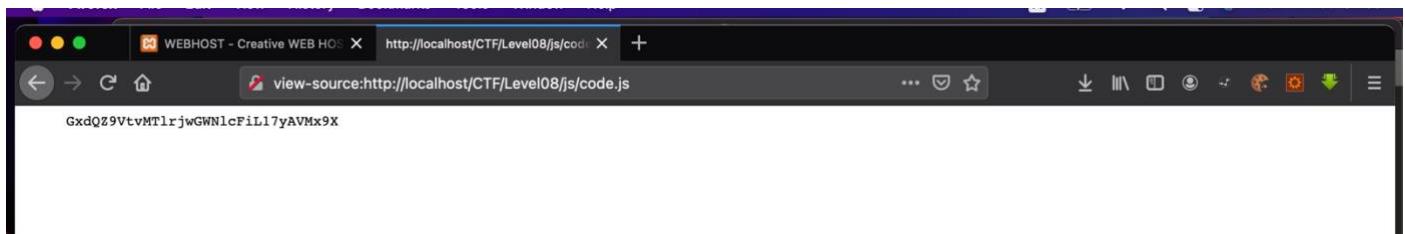
Success we are on the WEBHOST Premium account. Then we need to find the unlock code from this page at somewhere.

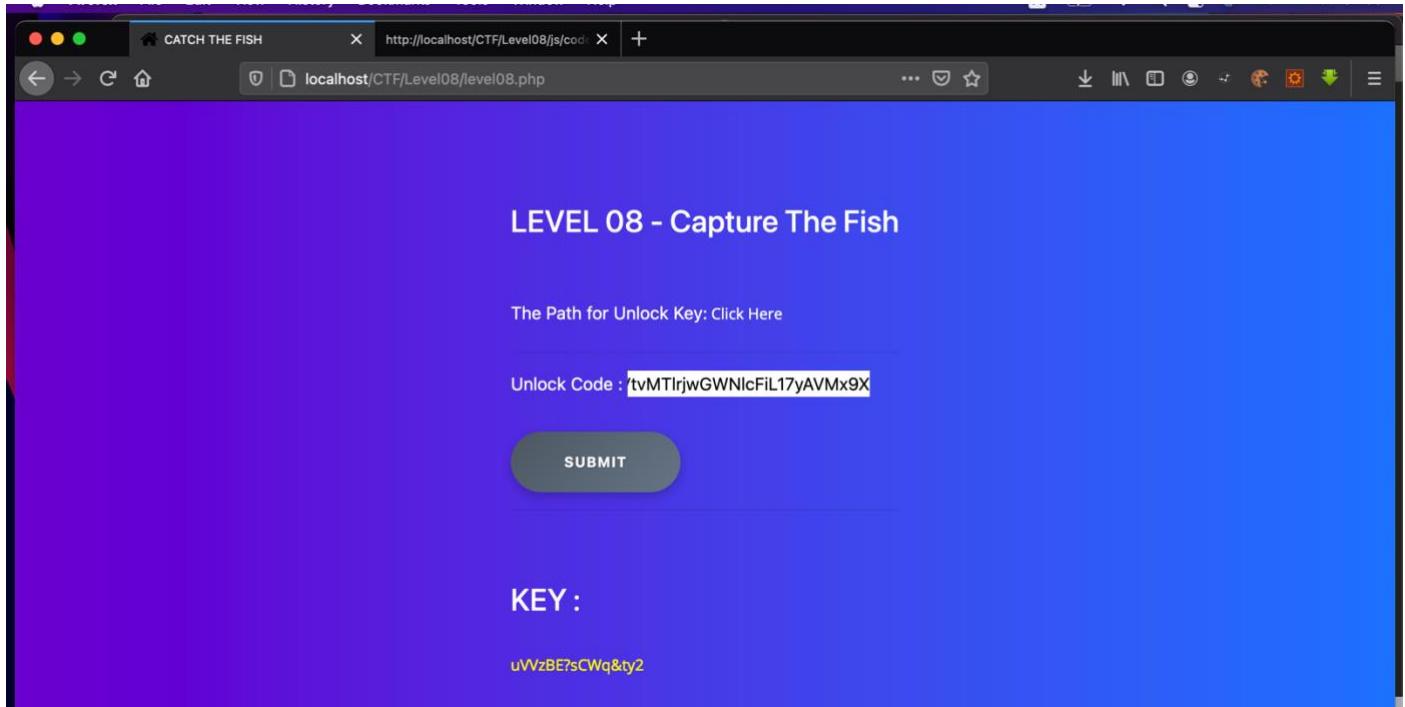


Let's move on to page source for any clue

```
493 <script src="js/fullpage.min.js"></script>
494 <script src="js/scrolloverflow.js"></script>
495 <script src="js/owl.carousel.min.js"></script>
496 <script src="js/jquery.inview.min.js"></script>
497 <script src="js/form.js"></script>
498 <script src="js/custom.js"></script>
499 <script src="js/code.js"></script>
500
501
502
503
504
505
506
507
508 </body>
```

Success.



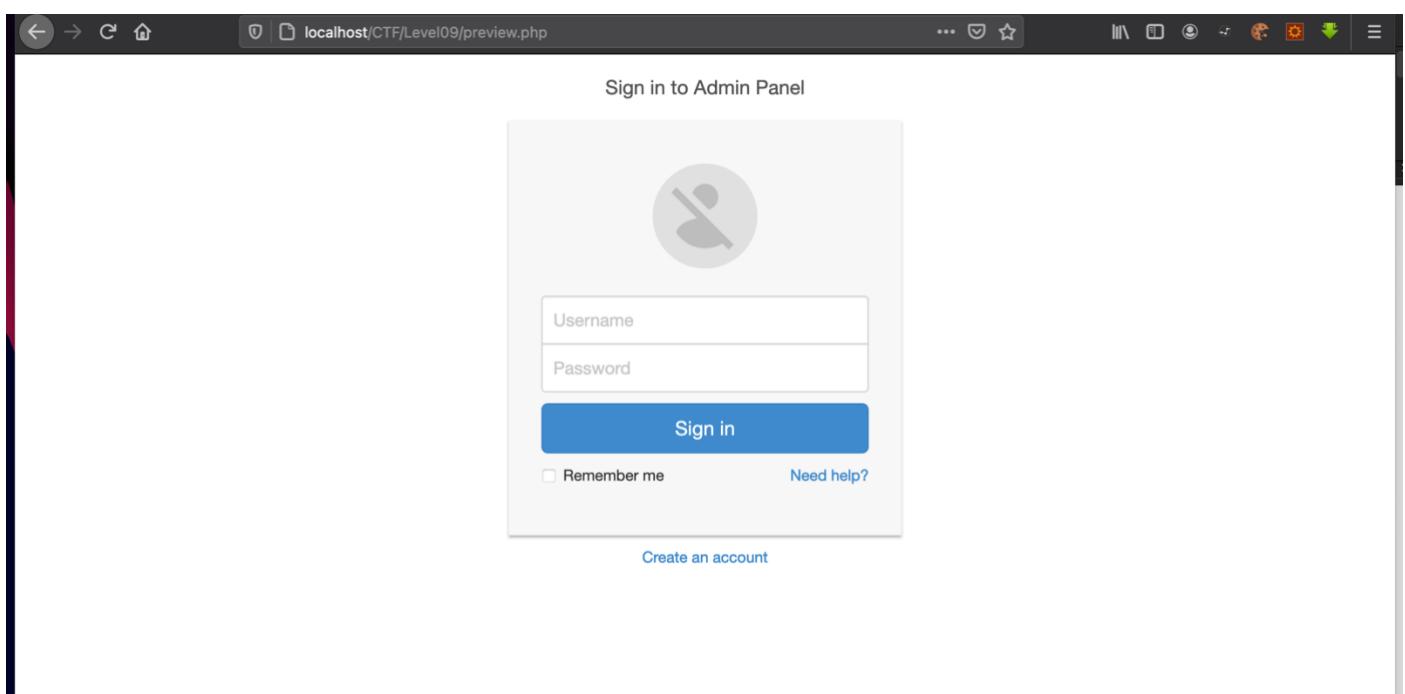
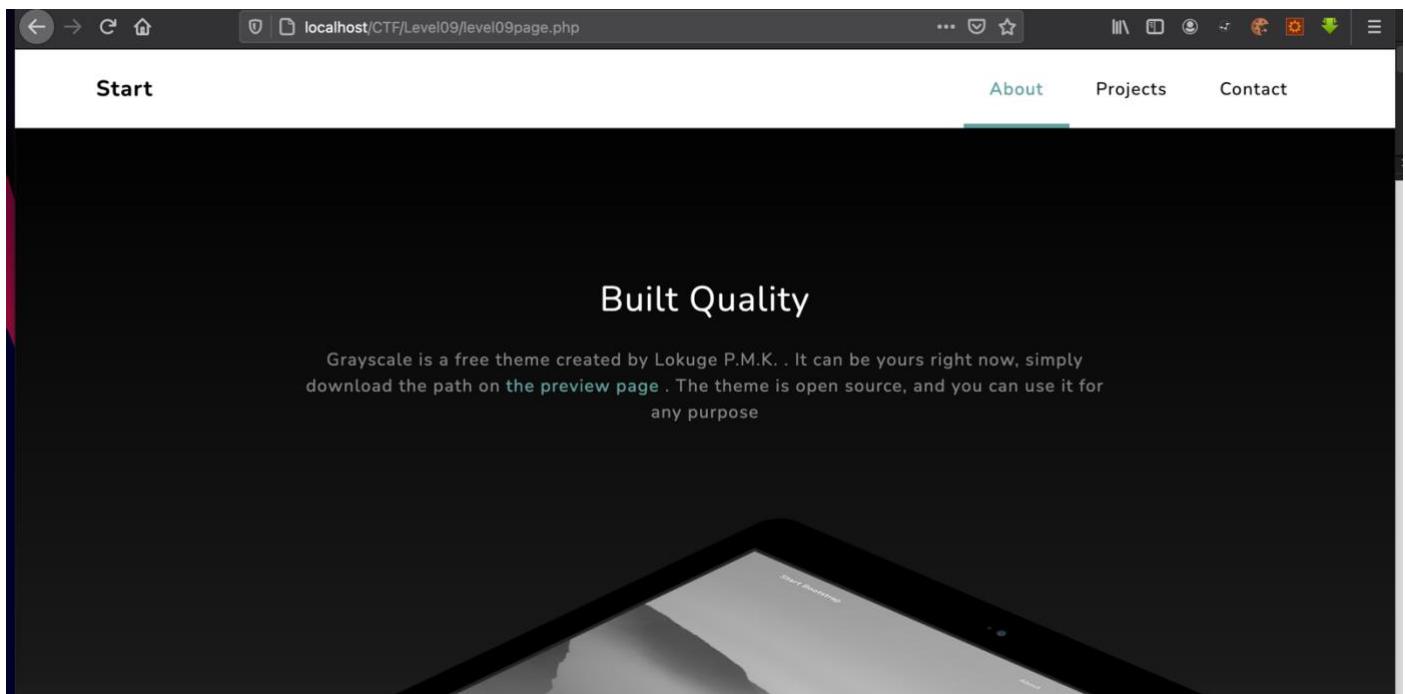


Level 09

- Try Until the Fish Comes

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





```

84 {
85     display: block;
86     margin-top: 10px;
87 }
88
89 </style>
90 </head>
91 <body>
92
93 <div class="container">
94     <div class="row">
95         <div class="col-sm-6 col-md-4 col-md-offset-4">
96             <h1 class="text-center login-title">Sign in to Admin Panel</h1>
97             <div class="account-wall">
98                 
101                    <input name="username" type="text" class="form-control" placeholder="Username" required autofocus>
102                    <input type="password" name="password" class="form-control" placeholder="Password" required>
103                    <button class="btn btn-lg btn-primary btn-block" type="submit" name="log_admin">
104                        Sign in</button>
105                    <label class="checkbox pull-left">
106                        <input type="checkbox" value="remember-me" >
107                        Remember me
108                    </label>
109                    <a href="#" class="pull-right need-help">Need help? </a><span class="clearfix"></span>
110                </form>
111            </div>
112            <a href="#" class="text-center new-account">Create an account </a>
113        </div>
114    </div>
115 </div>
116 </div>
117 </div>
118 </body>
119
120 <script type="text/javascript" src="assets/js/misc/admin.js"></script>
121 <script type="text/javascript" src="assets/js/app/app.js"></script>
122 <script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
123 <script type="text/javascript" src="vendor/bootstrap/bootstrap.min.js"></script>
124 <script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
125 <script type="text/javascript" src="vendor/angular/angular.min.js"></script>
126
127
128 </html>
129

```

```

_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

```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
f25a2fc72690b780b2a14e140ef6a9e  
d8578edf8458ce06fbcb5bb76a58c5ca4  
276f8db0b86edaa7fc805516c852c88  
0d107d09f5bbe40cade3de5c71e9eb7  
38441851393dd6ed4d316af20c6b431e  
84d961568a65073a3bcf0eb216b2a576
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

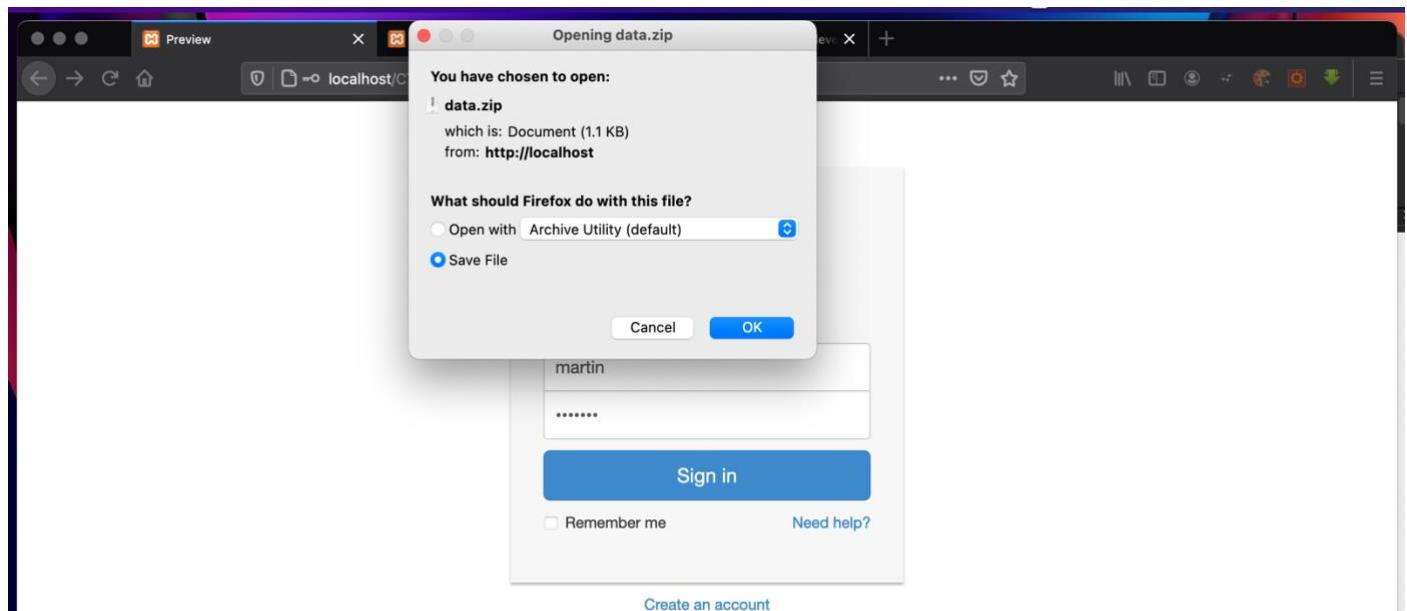
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f25a2fc72690b780b2a14e140ef6a9e	Unknown	Unrecognized hash format.
d8578edf8458ce06fbcb5bb76a58c5ca4	md5	qwerty
276f8db0b86edaa7fc805516c852c88	Unknown	Unrecognized hash format.
0d107d09f5bbe40cade3de5c71e9eb7	md5	letmein
38441851393dd6ed4d316af20c6b431e	Unknown	Not found.
84d961568a65073a3bcf0eb216b2a576	md5	superman

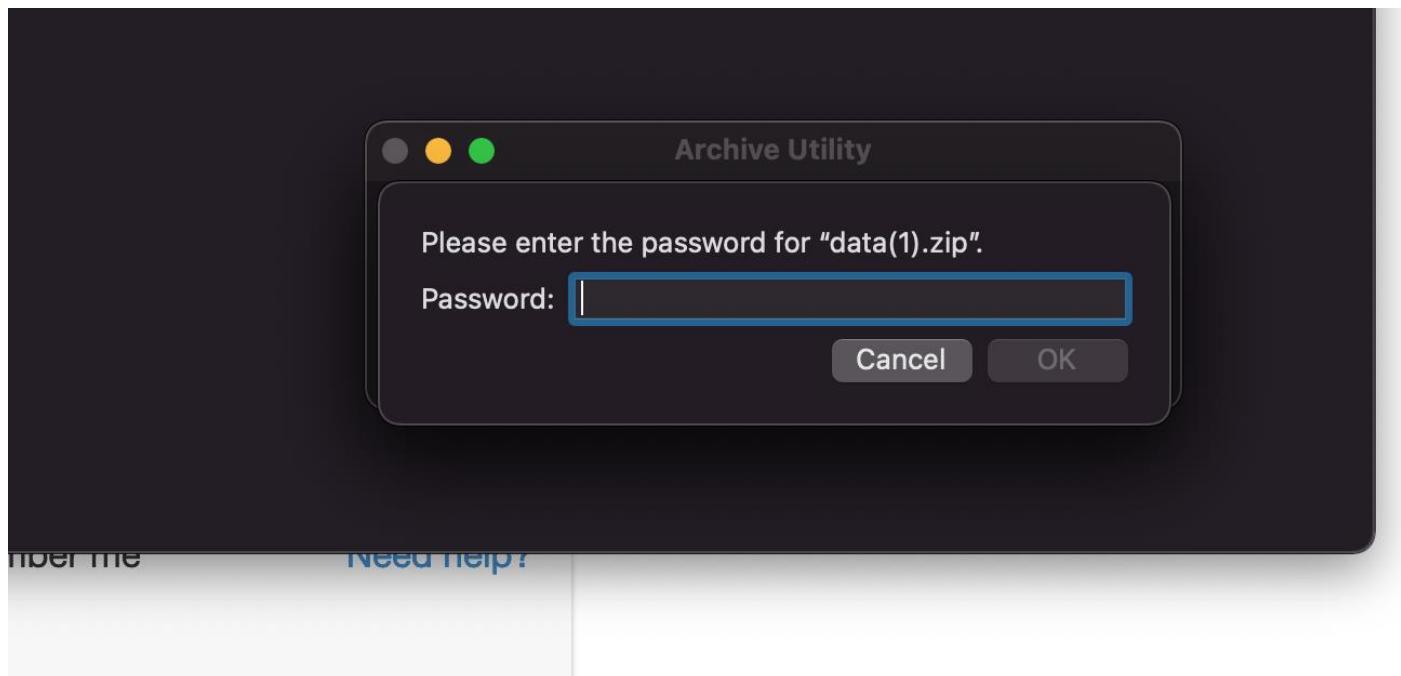
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

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

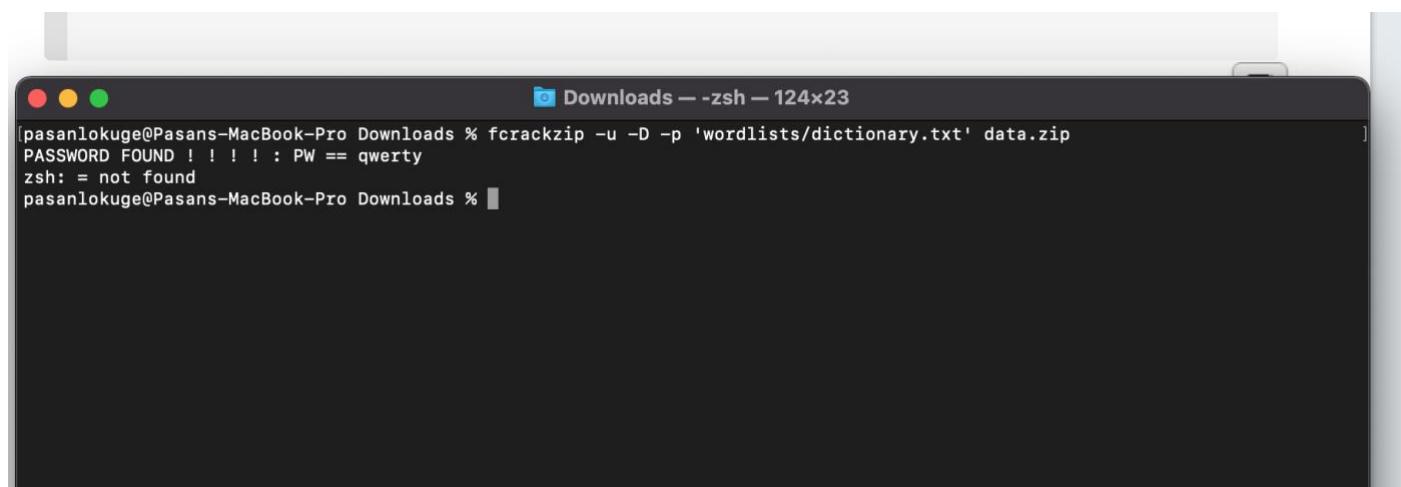
When enter username and password, there is a file which prompt for download gives a hint for the unlock code



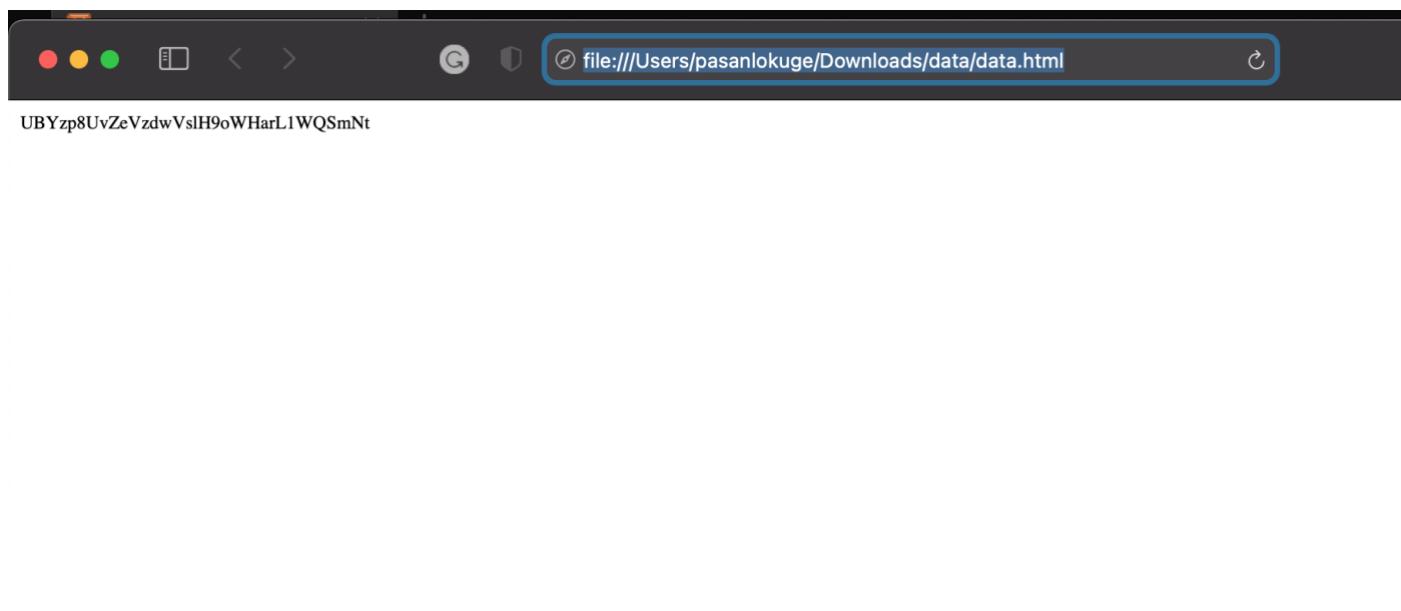
The downloaded zip file is read protected with passcode which needs to be cracked



For demonstration purpose, we have used fcrackzip and got password



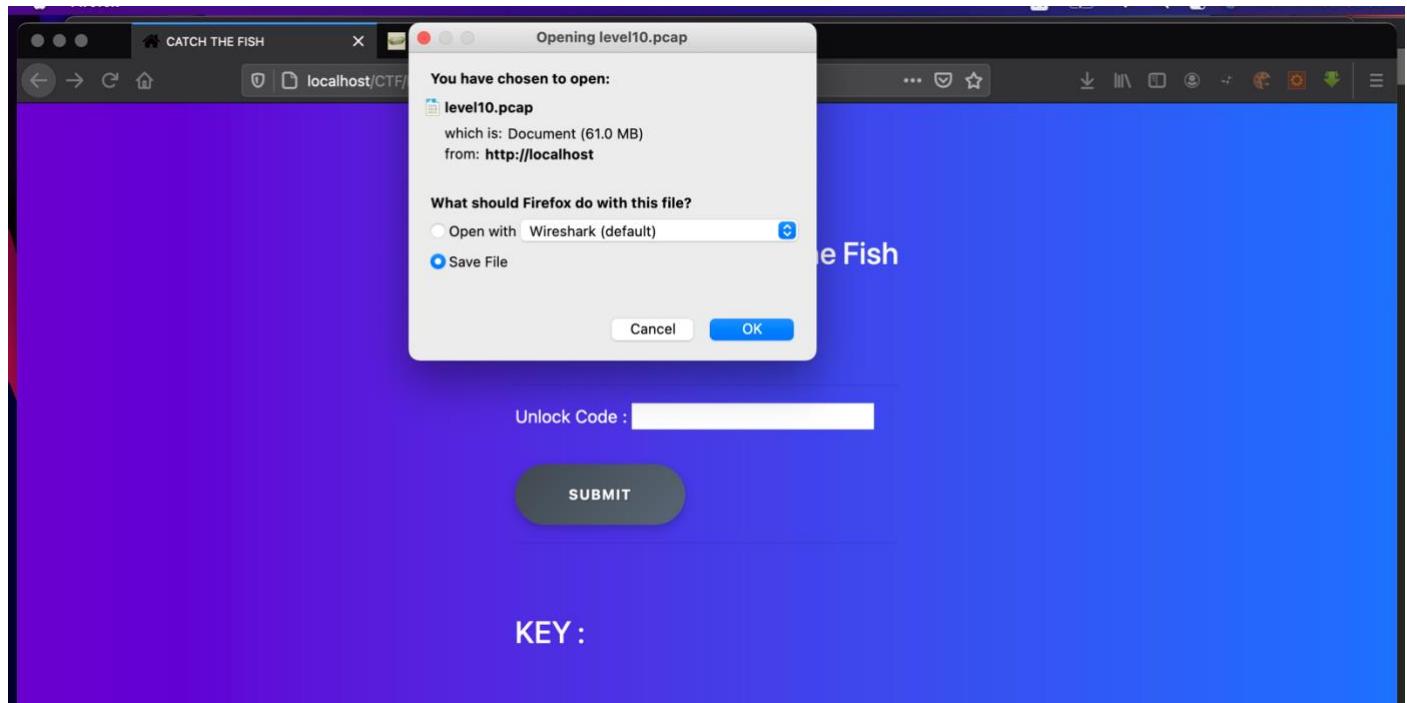
Success..



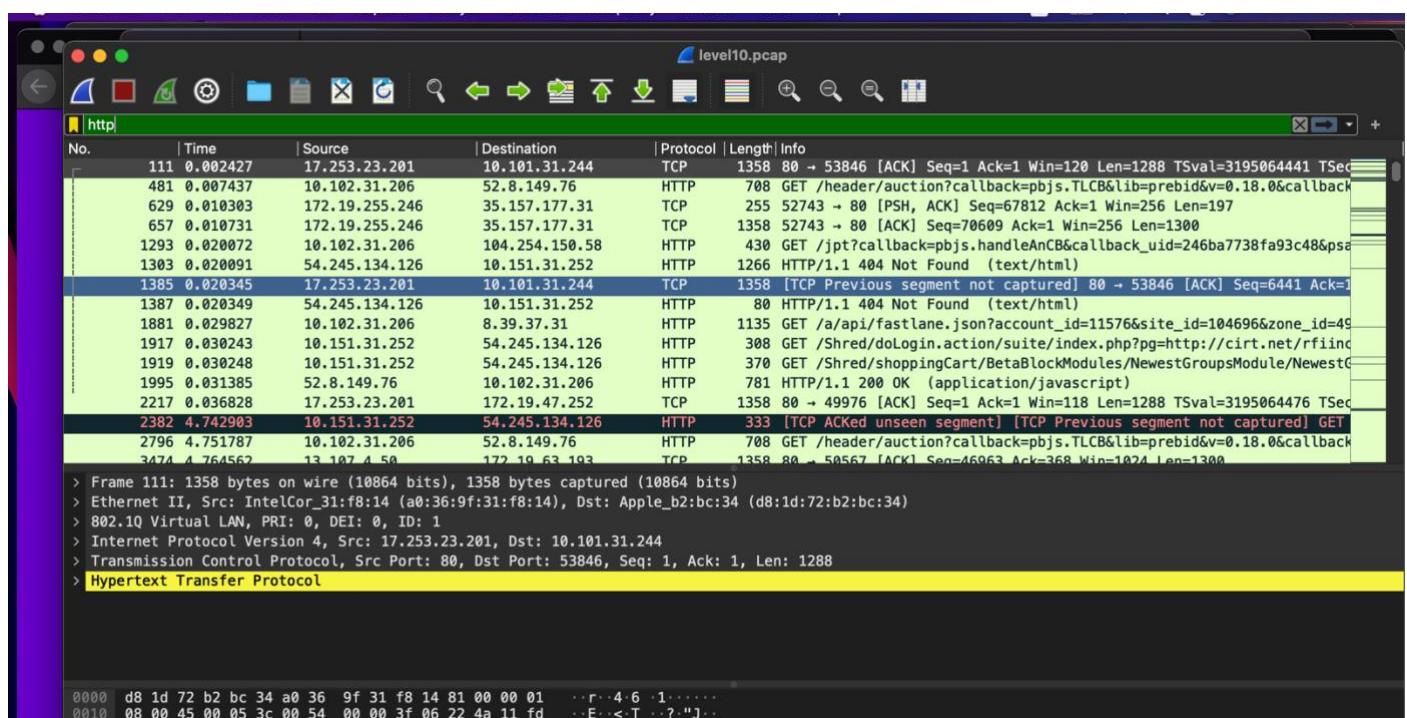
Level 10

- 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.



KEY :



Screenshot of Wireshark showing network traffic for level10.pcap. The selected packet is a GET request to http://wbg-server.se:80/wbg/img/GetAccountPicture.php?email=guest137646@worldboardgames.com. The packet details pane shows the following headers:

```

Connection: keep-alive\r\n
Accept: */*\r\n
User-Agent: YatzyWorld/5181 CFNetwork/811.5.4 Darwin/16.6.0\r\n
Accept-Language: da-dk\r\n
Authorization: Basic d2JnYXBwMzEyMTY6UTgyN3dPNjY1NiFuVzk5X2Ex\r\n
    Credentials: wbapp31216:Q827w06656!nW99_a1
Accept-Encoding: gzip, deflate\r\n
\r\n
[Full request URI: http://utils.wbg-server.se:80/wbg/img/GetAccountPicture.php?email=guest137646@worldboardgames.com]
[HTTP request 2/3]
[Prev request in frame: 5430]

```

The packet bytes pane shows the raw hex and ASCII data of the selected packet.

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

Knowing the PASSWORD as : KEY

Screenshot of a web-based Vigenere cipher tool at <https://www.dcode.fr/vigenere-cipher>. The tool interface includes a search bar, a results section, and a main decoder section. The main section has tabs for "VIGENERE DECODER" and "VIGENERE ENCODER". It features parameters for "PLAINTEXT LANGUAGE" (set to English) and "ALPHABET" (set to ABCDEFGHIJKLMNOPQRSTUVWXYZ). Under "DECRIPTION METHOD", the "KNOWING THE KEY/PASSWORD" option is selected, with "KEY" entered. A "DECRYPT" button is present. To the right, there is a "Summary" sidebar with links related to the Vigenere cipher.

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

Paste text or drop text file

3YVdU91sYpAaCPAWQ56uZT91DfARJu5

Character encoding

ASCII

Output delimiter string (optional)

Space

Convert Reset Swap

33 59 56 64 55 39 31 73 59 70 41 61 43 50 41 57 51 35 36 75
5a 54 39 31 44 66 41 52 4a 75 35

Success..

LEVEL 10 - Capture The Fish

The Path for Unlock Key: Click Here

Unlock Code : **34 39 31 44 66 41 52 4a 75 35**

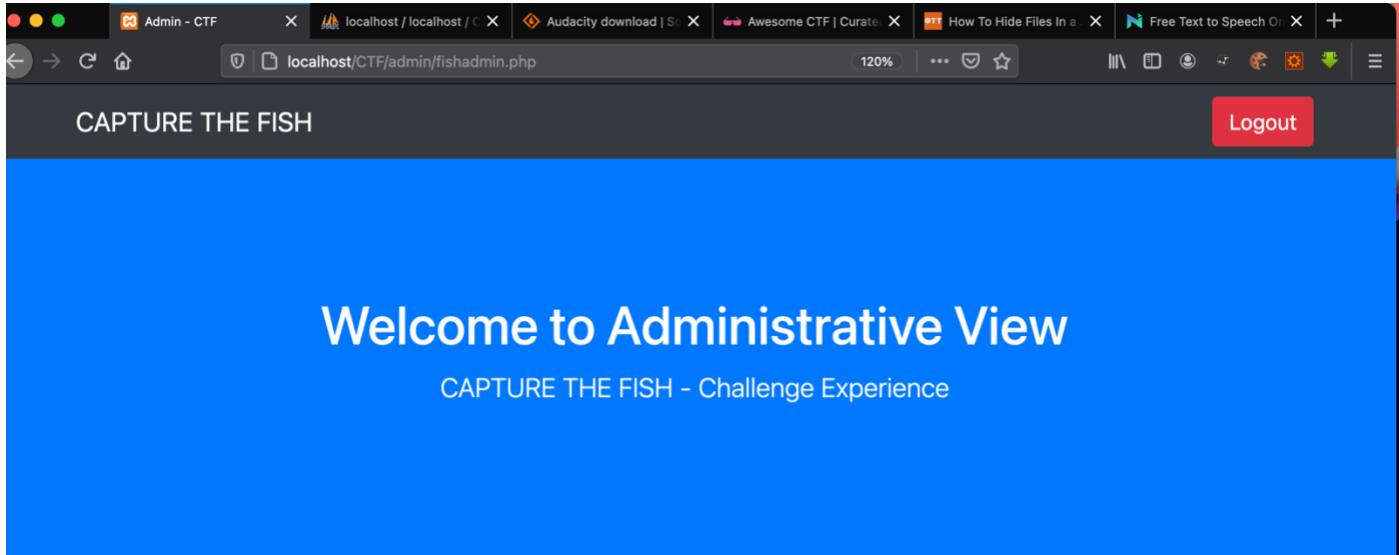
SUBMIT

KEY :

You Are Done!

Administrative View

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

A screenshot of a web browser showing the 'Key Changer' form. The title bar says 'localhost / localhost / CTF / Admin - CTF'. The main content area contains a table with six rows, each for a different level. Each row has two input fields ('Code:' and 'Key:') and a 'Submit' button. The levels are numbered 01 to 06. The table has a light gray background and teal-colored 'Submit' buttons.

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-OBLQ8vu09Rryg3_yX9elsqxQ?e=hfOsOe