NetEnt CTF 2016 write-up

Challenge 1

You are presented with an image of Yoda, with the text "May the source be with you".

Solution

Use "View Source" on your browser and inspect the source code of the page. Towards the bottom of the page you will find:

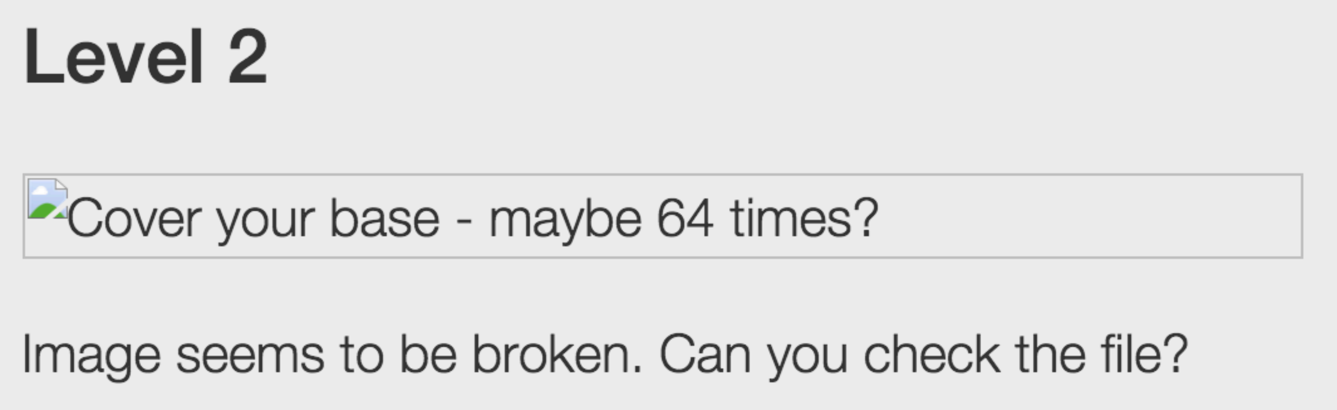
```
<p>
    <img src="/static/img/yoda.png" alt="May the source be with you" style="width: 50%; height: 50%"/>
    <!-- the_flag_is_ctfnetent -->
</p>
```

Flag

The flag is: ctfnetent

Challenge 2

You are presented with a page that has a broken image with a hint:



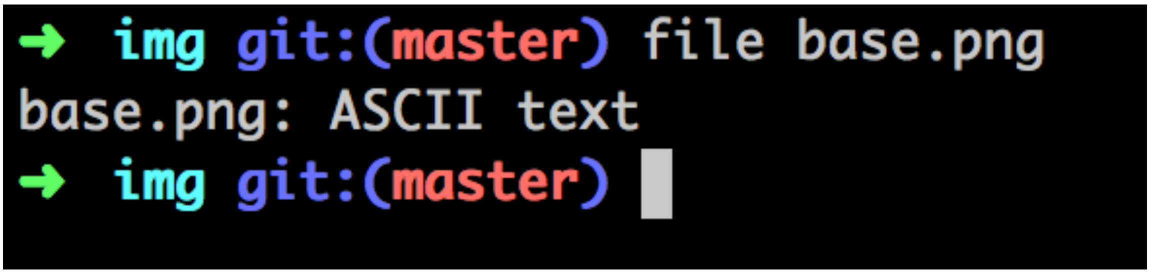
Level 2

Cover your base - maybe 64 times?

Image seems to be broken. Can you check the file?

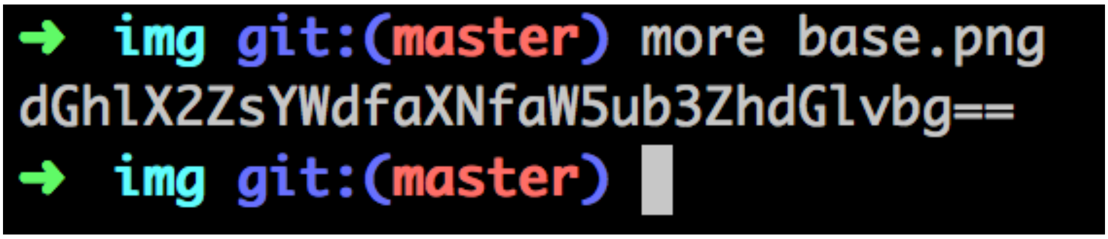
Solution

Download the image and insect it:



```
➜  img git:(master) file base.png
base.png: ASCII text
➜  img git:(master)
```

This is not the proper answer for an image file, so open up the image with a text editor:



```
➜  img git:(master) more base.png
dGhlX2ZsYWdfaXNfaW5ub3ZhdGlvbg==
➜  img git:(master) 
```

The string is unreadable, but the 2 equal signs at the end signal that the string is Base64 encoded.

Run the string via any online Base64 decoder and you get the answer

Flag

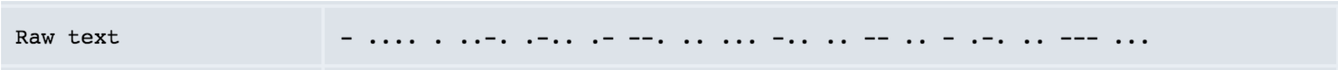
The flag is: innovation

Challenge 3

The page presents you with a QR image.

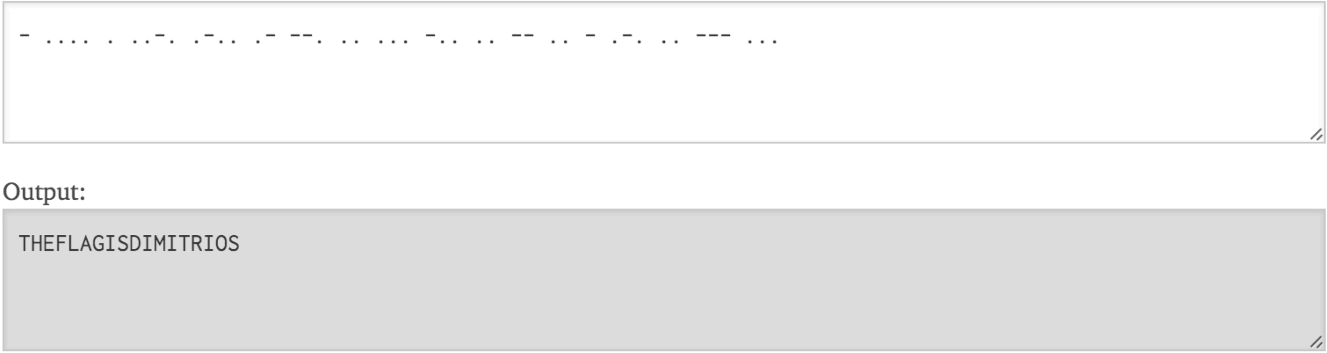
Solution

Run the image through any QR code reader application and you will be presented with a series of dots (.) and underscores (_):



Raw text	- ....-. .-.. .- --. .. ... -.. .. -- .. - .-. .. --- ...

The dots and underscores are Morse code, so you run the string via an online Morse code decoder:



```
- .... . ..-. .-.. .- --. .. ... -.. .. -- .. - .-. .. --- ...
```

Output:

```
THEFLAGISDIMITRIOS
```

Flag

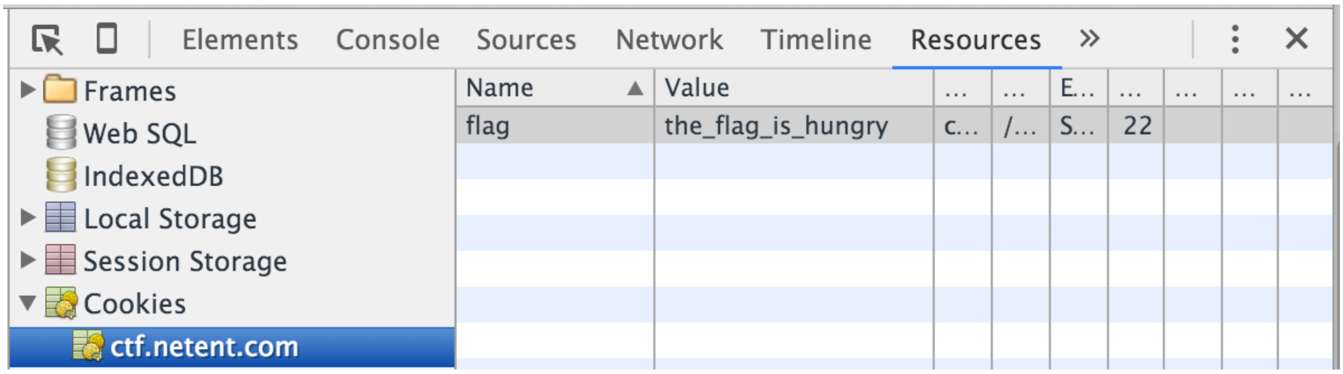
The flag is: Dimitrios

Challenge 4

The page presented you with an image that reads: "Gimme the cookies"

Solution

Use your browser to review the cookies on the page:



Name ▲	Value	…	…	E…	…	…	…	…
flag	the_flag_is_hungry	c…	/…	S…	22			

Flag

The flag is: hungry

Challenge 5

The page presented you with a picture with the text Look Deeper

Solution

Download the file and use steghide to extract the hidden message (no passphrase needed)

Flag

The flag is: hidden

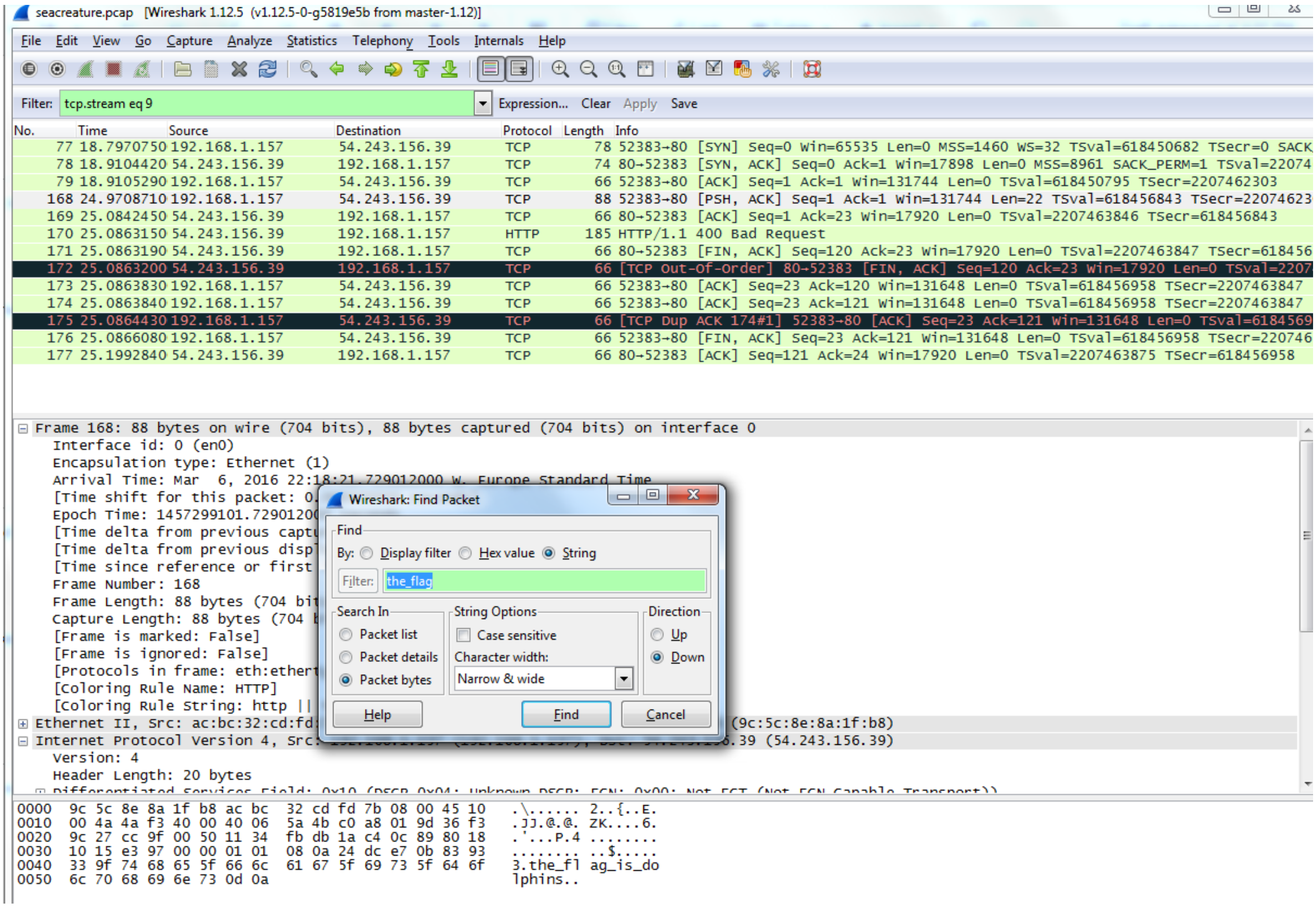
Challenge 6

The page presented you with a link to download a file and a text Download file and spend some time looking into it

Solution

Download and use Wireshark to open the packet capture file

Use the Find Packet functionality to search for a string



seacreature.pcap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp.stream eq 9

```
No.   Time       Source          Destination     Protocol Length Info
   77 18.7970750 192.168.1.157   54.243.156.39   TCP      78 52383→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=618450682 TSecr=0 SACK
   78 18.9104420 54.243.156.39   192.168.1.157   TCP      74 80→52383 [SYN, ACK] Seq=0 Ack=1 Win=17898 Len=0 MSS=8961 SACK_PERM=1 TSval=22074
   79 18.9105290 192.168.1.157   54.243.156.39   TCP      66 52383→80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=618450795 TSecr=2207462303
  168 24.9708710 192.168.1.157   54.243.156.39   TCP      88 52383→80 [PSH, ACK] Seq=1 Ack=1 Win=131744 Len=22 TSval=618456843 TSecr=22074623
  169 25.0842450 54.243.156.39   192.168.1.157   TCP      66 80→52383 [ACK] Seq=1 Ack=23 Win=17920 Len=0 TSval=2207463846 TSecr=618456843
  170 25.0863150 54.243.156.39   192.168.1.157   HTTP    185 HTTP/1.1 400 Bad Request
  171 25.0863190 54.243.156.39   192.168.1.157   TCP      66 80→52383 [FIN, ACK] Seq=120 Ack=23 Win=17920 Len=0 TSval=2207463847 TSecr=618456
  172 25.0863200 54.243.156.39   192.168.1.157   TCP      66 [TCP Out-Of-Order] 80→52383 [FIN, ACK] Seq=120 Ack=23 Win=17920 Len=0 TSval=2207
  173 25.0863830 192.168.1.157   54.243.156.39   TCP      66 52383→80 [ACK] Seq=23 Ack=120 Win=131648 Len=0 TSval=618456958 TSecr=2207463847
  174 25.0863840 192.168.1.157   54.243.156.39   TCP      66 52383→80 [ACK] Seq=23 Ack=121 Win=131648 Len=0 TSval=618456958 TSecr=2207463847
  175 25.0864430 192.168.1.157   54.243.156.39   TCP      66 [TCP Dup ACK 174#1] 52383→80 [ACK] Seq=23 Ack=121 Win=131648 Len=0 TSval=6184569
  176 25.0866080 192.168.1.157   54.243.156.39   TCP      66 52383→80 [FIN, ACK] Seq=23 Ack=121 Win=131648 Len=0 TSval=618456958 TSecr=220746
  177 25.1992840 54.243.156.39   192.168.1.157   TCP      66 80→52383 [ACK] Seq=121 Ack=24 Win=17920 Len=0 TSval=2207463875 TSecr=618456958
```

```
⊟ Frame 168: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  6, 2016 22:18:21.729012000 W. Europe Standard Time
    [Time shift for this packet: 0.
    Epoch Time: 1457299101.72901200
    [Time delta from previous captu
    [Time delta from previous displ
    [Time since reference or first
    Frame Number: 168
    Frame Length: 88 bytes (704 bit
    Capture Length: 88 bytes (704 b
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethert
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http ||
⊞ Ethernet II, Src: ac:bc:32:cd:fd:                              (9c:5c:8e:8a:1f:b8)
⊟ Internet Protocol Version 4, Src:                             .39 (54.243.156.39)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
```

```
0000  9c 5c 8e 8a 1f b8 ac bc  32 cd fd 7b 08 00 45 10   .\...... 2..{..E.
0010  00 4a 4a f3 40 00 40 06  5a 4b c0 a8 01 9d 36 f3   .JJ.@.@. ZK....6.
0020  9c 27 cc 9f 00 50 11 34  fb db 1a c4 0c 89 80 18   .'...P.4 ........
0030  10 15 e3 97 00 00 01 01  08 0a 24 dc e7 0b 83 93   ........ ..$.....
0040  33 9f 74 68 65 5f 66 6c  61 67 5f 69 73 5f 64 6f   3.the_fl ag_is_do
0050  6c 70 68 69 6e 73 0d 0a                            lphins..
```

Wireshark: Find Packet

Find

By: ○ Display filter ○ Hex value ● String

Filter: the_flag

Search In: ○ Packet list ○ Packet details ● Packet bytes

String Options: ☐ Case sensitive

Character width: Narrow & wide

Direction: ○ Up ● Down

Flag

The flag is: dolphins

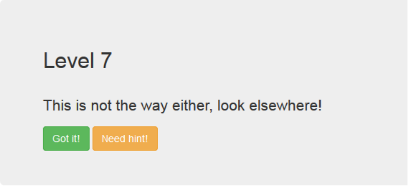
Challenge 7

The link from the Challenges page was intentionally broken leading to a 404 page with the text "This is not the path young Padowan"

Solution

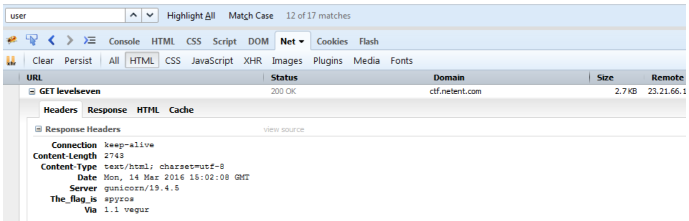
Navigate to http://ctf.netent.com/levelseven

Inspect the HTTP Response headers



Level 7

This is not the way either, look elsewhere!



URL	Status	Domain	Size	Remote
GET levelseven	200 OK	ctf.netent.com	2.7 KB	23.21.66.1

Response Headers

```
    Connection keep-alive
Content-Length 2743
  Content-Type text/html; charset=utf-8
          Date Mon, 14 Mar 2016 15:02:08 GMT
        Server gunicorn/19.4.5
   The_flag_is spyros
           Via 1.1 vegur
```

Flag

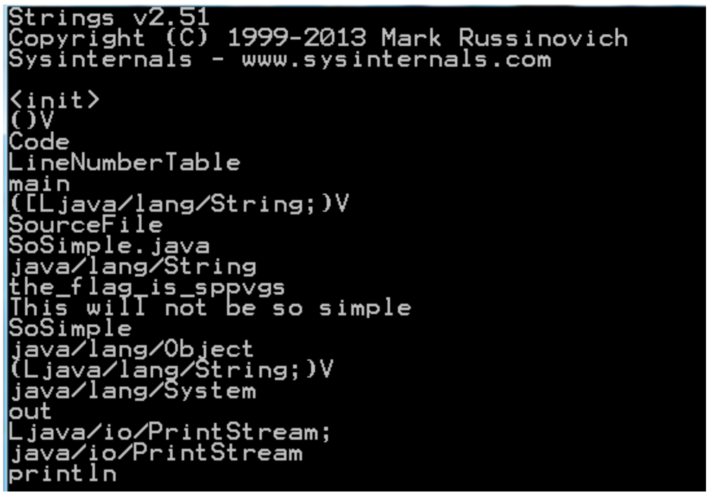
The flag is: spyros

Challenge 8

The page presented you with a link to download a file and a text Download file and see if this class can teach you anything!

Solution

Download the file and extract ASCII-readable strings from it



```
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

<init>
()V
Code
LineNumberTable
main
([Ljava/lang/String;)V
SourceFile
SoSimple.java
java/lang/String
the_flag_is_sppvgs
This will not be so simple
SoSimple
java/lang/Object
(Ljava/lang/String;)V
java/lang/System
out
Ljava/io/PrintStream;
java/io/PrintStream
println
```

Flag

The flag is: sppvgs

Challenge 9

The page presented you with a login form and a banner "CISCO CNR Login System"

Solution

Use Google to search for Cisco CNR default credentials

Flag

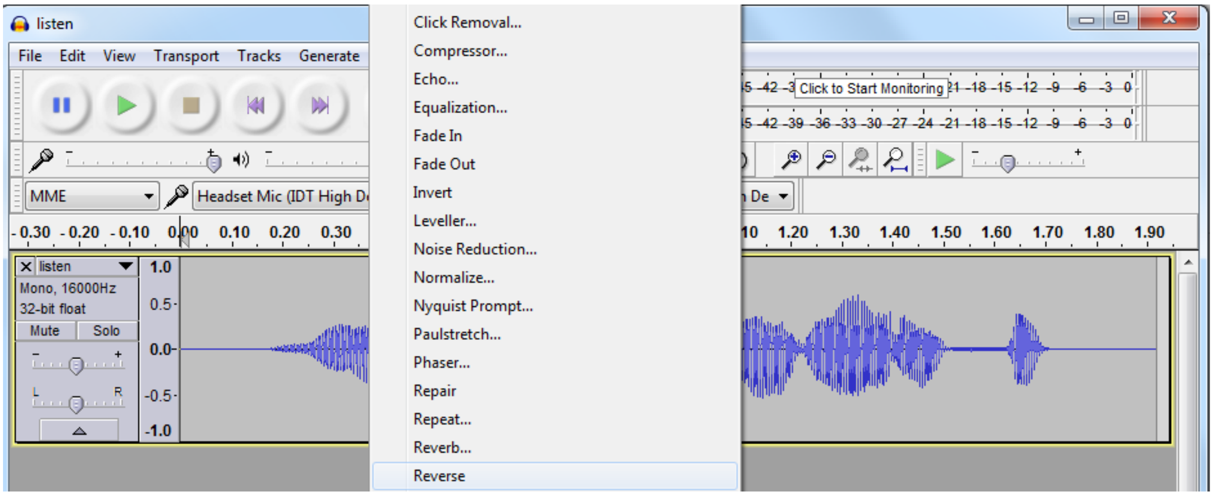
The flag is: lego

Challenge 10

The page presented you with a picture with the word "Listen" and a link to download a wav file

Solution

Download the audio file and play it in reverse (e.g. with Audacity)



Flag

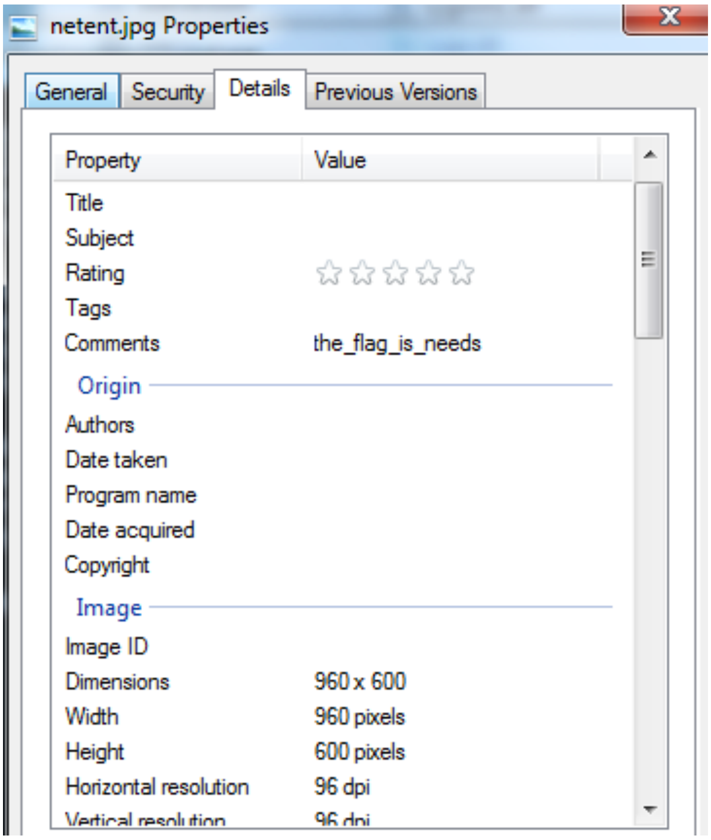
The flag is: magical

Challenge 11

The page presented you with a picture depicting the Guns 'n' Roses logo

Solution

Download the image file and check the file's properties



netent.jpg Properties

Property	Value
Title	
Subject	
Rating	☆☆☆☆☆
Tags	
Comments	the_flag_is_needs
Origin	
Authors	
Date taken	
Program name	
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	960 x 600
Width	960 pixels
Height	600 pixels
Horizontal resolution	96 dpi
Vertical resolution	96 dpi

Flag

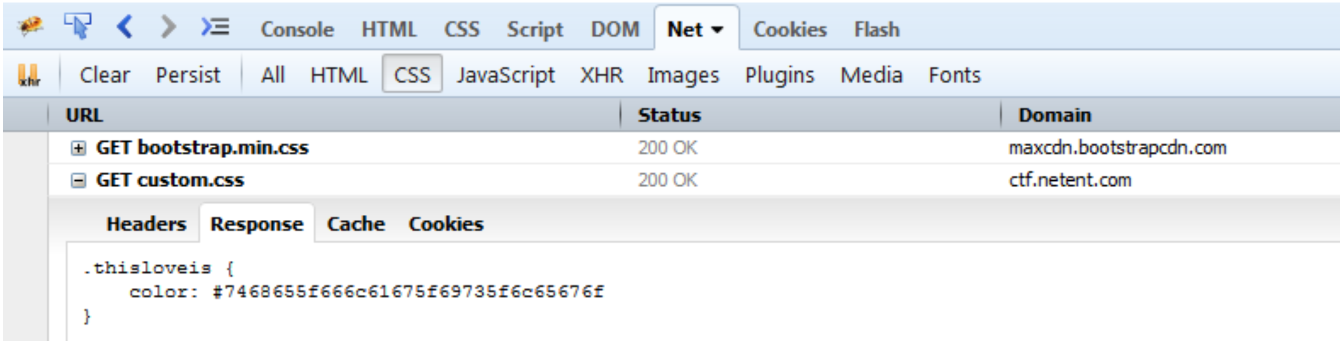
The flag is: needs

Challenge 12

The page presented you with a picture containing the word 'CSS'

Solution

Use your browser to inspect the resources loaded by the page.



URL	Status	Domain
GET bootstrap.min.css	200 OK	maxcdn.bootstrapcdn.com
GET custom.css	200 OK	ctf.netent.com

```
.thisloveis {
    color: #7468655f666c61675f69735f6c65676f
}
```

and use a hex to string converter

Flag

The flag is: lego

Challenge 13

The page presented you with the text "**Oh no!** It seems we lost this level - can you find a backup file to save the level? "

Solution

Browse to http://ctf.netent.com/levelthirteen.old

and examine the returned text

Flag

The flag is: gdk

Challenge 14

The page presented you with the text "We managed to extact a database dump from the victim. Maybe you will find it interesting"

and a link to a text file

Solution

Examine the file and locate the line

```
INSERT INTO `user` VALUES
(1,1,'simplerisk','victim','Victim','victim@example.com','sAbwTbIFywWKcheyQw9a','\u0074\u0068\u0065\u005f\u
0066\u006c\u0061\u0067\u005f\u0069\u0073\u005f\u0074\u0061\u0063\u006f\u0073','2015-07-29
08:46:16','all',NULL,1,1,1,1,1,1,1,1,1,1,1,1);
```

Use a UTF-8 decoder for

```
'\u0074\u0068\u0065\u005f\u0066\u006c\u0061\u0067\u005f\u0069\u0073\u005f\u0074\u0061\u0063\u006f\u0073'
```

Flag

The flag is: tacos

Challenge 15

The page presented you with the text

DNS Resolution

DNS resolution is helpful, but was this implemented correctly?
Maybe it does more than it should!

and an input field

Solution

Perform a command injection by sending an input like

www.google.com; ls -la

Flag

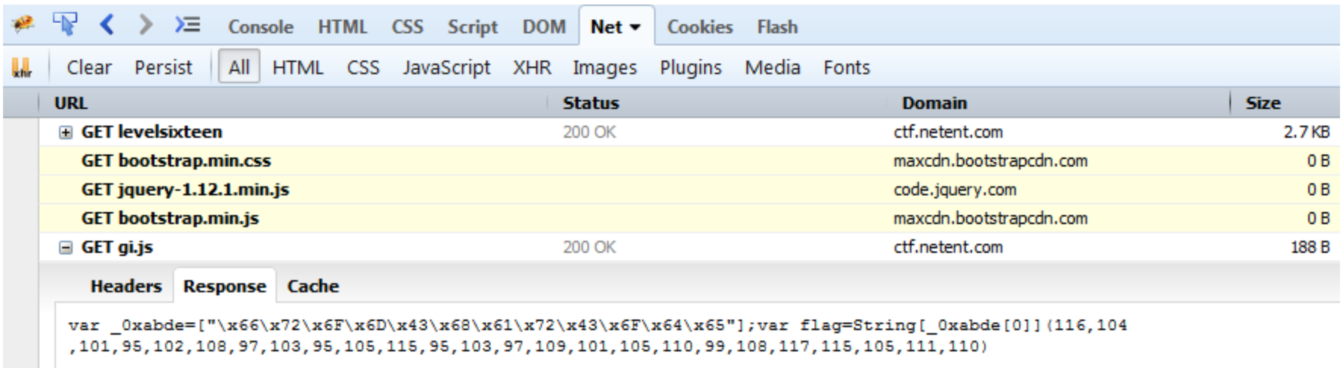
The flag is: wolverine

Challenge 16

The page presented you with the text "The client holds the secret"

Solution

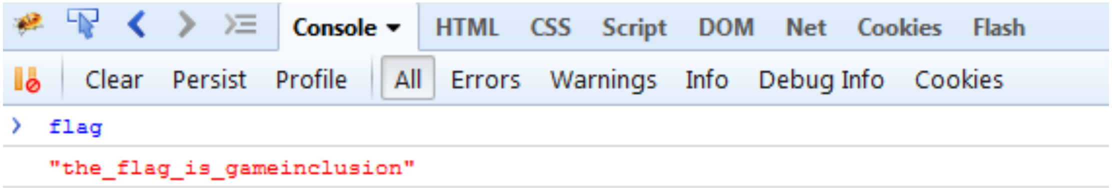
Use your browser to inspect the resources loaded by the page.



URL	Status	Domain	Size
⊞ GET levelsixteen	200 OK	ctf.netent.com	2.7 KB
GET bootstrap.min.css		maxcdn.bootstrapcdn.com	0 B
GET jquery-1.12.1.min.js		code.jquery.com	0 B
GET bootstrap.min.js		maxcdn.bootstrapcdn.com	0 B
⊟ GET gi.js	200 OK	ctf.netent.com	188 B

```
var _0xabde=["\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65"];var flag=String[_0xabde[0]](116,104
,101,95,102,108,97,103,95,105,115,95,103,97,109,101,105,110,99,108,117,115,105,111,110)
```

Use the console to display the value of the flag variable



```
> flag
  "the_flag_is_gameinclusion"
```

Flag

The flag is: gameinclusion

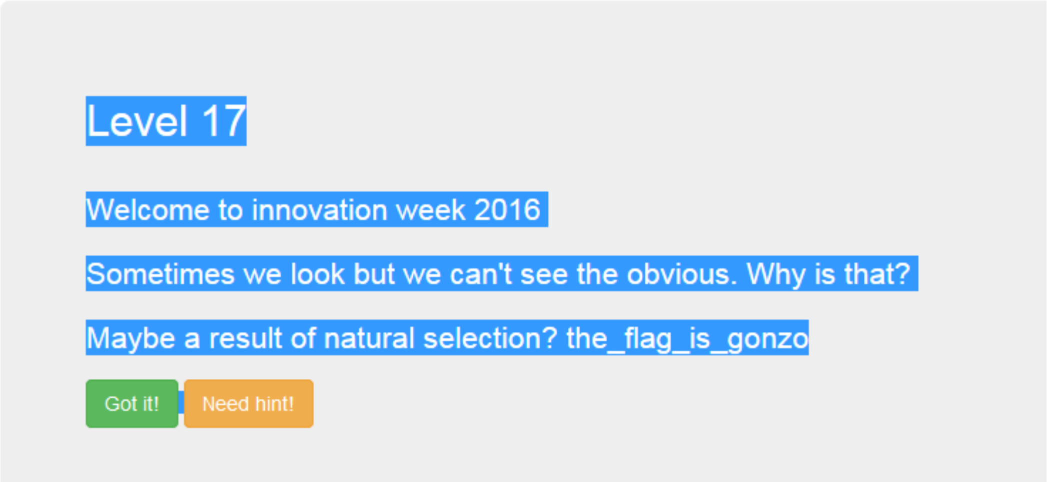
Challenge 17

The page presented you with the text

"Welcome to innovation week 2016
Sometimes we look but we can't see the obvious. Why is that?
Maybe a result of natural selection"

Solution

Press Ctrl+A to select all text on the page



Level 17

Welcome to innovation week 2016

Sometimes we look but we can't see the obvious. Why is that?

Maybe a result of natural selection? the_flag_is_gonzo

Flag

The flag is: gonzo

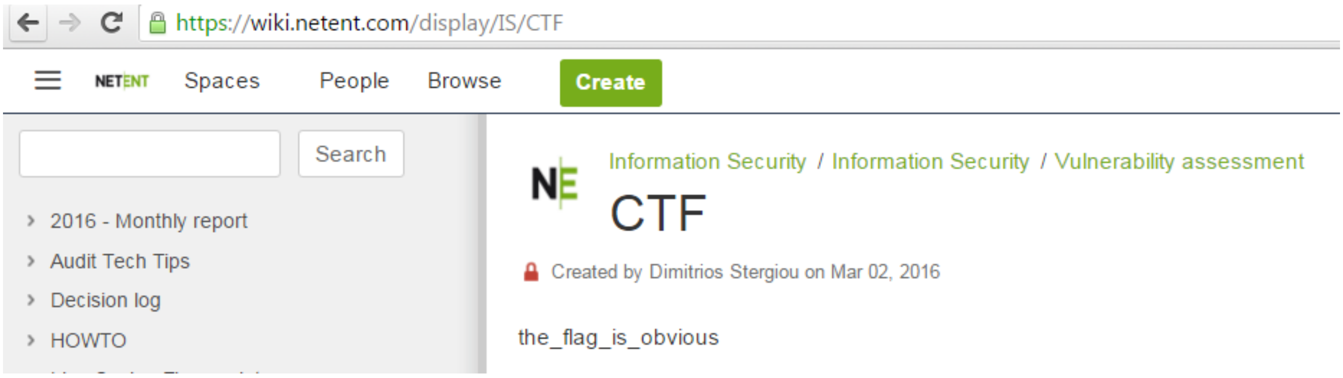
Challenge 18

The page presented you with the text

"This flag is not really well hidden. If you know where to look for knowledge you will be able to find it easily!"

Solution

The ultimate source of knowledge is the Wiki and more specifically the Information Security pages



https://wiki.netent.com/display/IS/CTF

Information Security / Information Security / Vulnerability assessment

CTF

Created by Dimitrios Stergiou on Mar 02, 2016

the_flag_is_obvious

Flag

The flag is: obvious

Challenge 19

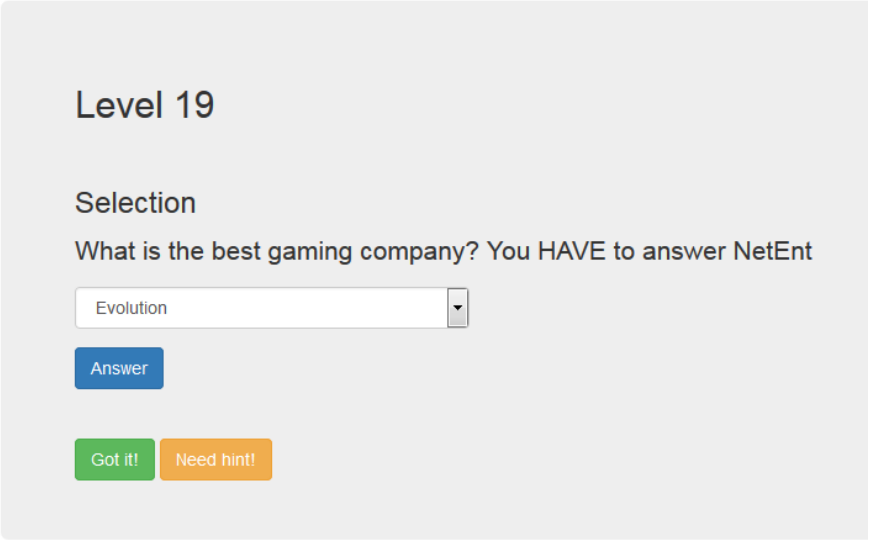
The page presented you with the text

"What is the best gaming company? You HAVE to answer NetEnt " and a dropdownlist that didn't contain the option NetEnt

Solution

Use your browser to inspect the HTML code of the page.

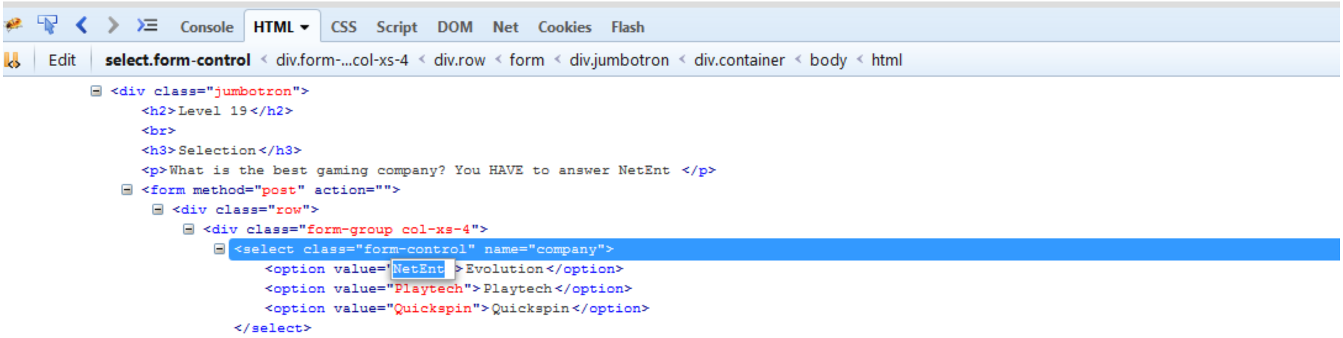
You can use Browser tools like Firebug to inspect and edit the HTML code at the client



Level 19

Selection

What is the best gaming company? You HAVE to answer NetEnt



Console
HTML
CSS
Script
DOM
Net
Cookies
Flash
Edit
select.form-control < div.form-...col-xs-4 < div.row < form < div.jumbotron < div.container < body < html

```
<div class="jumbotron">
    <h2>Level 19</h2>
    <br>
    <h3>Selection</h3>
    <p>What is the best gaming company? You HAVE to answer NetEnt </p>
    <form method="post" action="">
      <div class="row">
        <div class="form-group col-xs-4">
          <select class="form-control" name="company">
              <option value="NetEnt >Evolution</option>
              <option value="Playtech">Playtech</option>
              <option value="Quickspin">Quickspin</option>
          </select>
```

Change the value to NetEnt and click on the Answer button

Flag

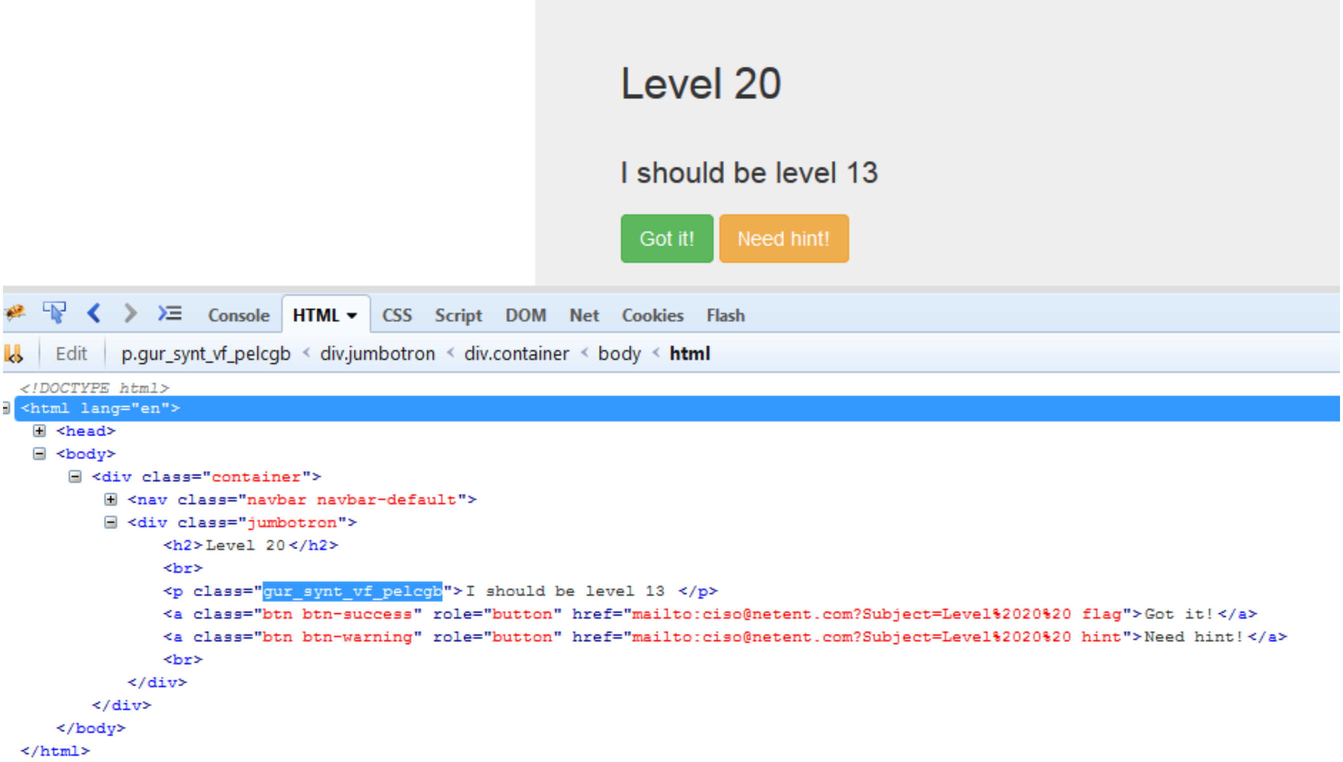
The flag is: yeahbaby

Challenge 20

The page presented you with the text
I should be level 13

Solution

Use your browser to inspect the HTML code of the page.



Level 20

I should be level 13

Got it!
Need hint!
Console
HTML
CSS
Script
DOM
Net
Cookies
Flash
Edit
p.gur_synt_vf_pelcgb < div.jumbotron < div.container < body < html

```
<!DOCTYPE html>
<html lang="en">
  <head>
  <body>
    <div class="container">
      <nav class="navbar navbar-default">
      <div class="jumbotron">
          <h2>Level 20</h2>
          <br>
          <p class="gur_synt_vf_pelcgb">I should be level 13 </p>
          <a class="btn btn-success" role="button" href="mailto:ciso@netent.com?Subject=Level%2020%20 flag">Got it!</a>
          <a class="btn btn-warning" role="button" href="mailto:ciso@netent.com?Subject=Level%2020%20 hint">Need hint!</a>
          <br>
      </div>
    </div>
  </body>
</html>
```

Use an online ROT13 decryptor to get the message of the strangely-looking class attribute value

Flag

The flag is: crypto

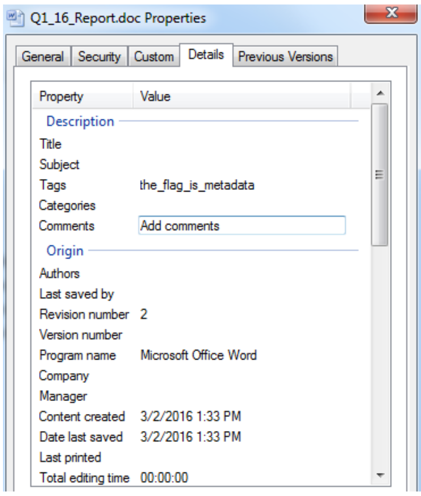
Challenge 21

The page presented you with the text

"Data...data...more data" and a link to download a doc file "Q1_16_Report.doc"

Solution

Examine the file's properties


Q1_16_Report.doc Properties

Property	Value
Description	
Title	
Subject	
Tags	the_flag_is_metadata
Categories	
Comments	Add comments
Origin	
Authors	
Last saved by	
Revision number	2
Version number	
Program name	Microsoft Office Word
Company	
Manager	
Content created	3/2/2016 1:33 PM
Date last saved	3/2/2016 1:33 PM
Last printed	
Total editing time	00:00:00

Flag

The flag is: metadata

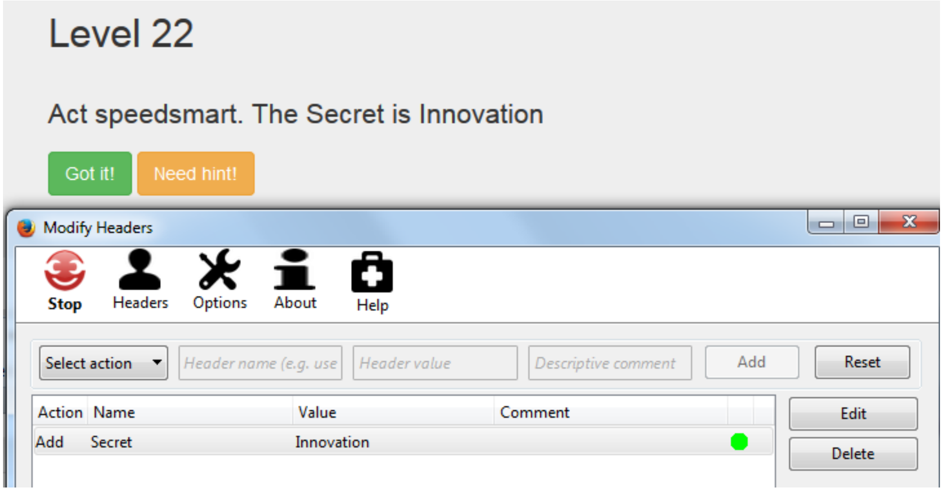
Challenge 22

The page presented you with the text

"Act speedsmart. The Secret is Innovation"

Solution

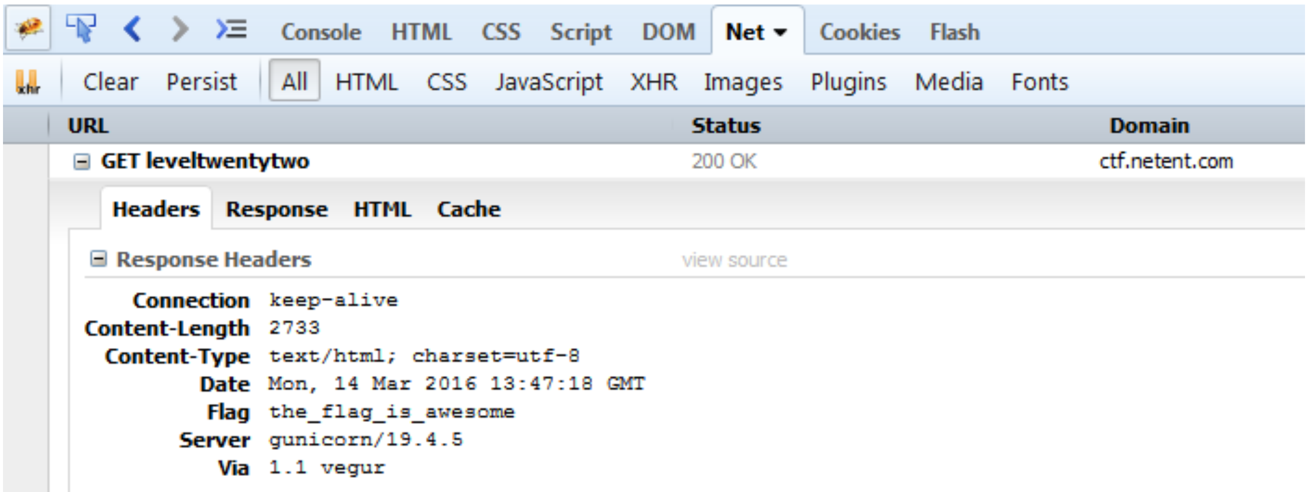
Use a browser add-on or proxy tool in order to modify the HTTP headers sent in the request


Level 22

Act speedsmart. The Secret is Innovation

Action	Name	Value	Comment	
Add	Secret	Innovation		●

Inspect the HTTP Response Headers



URL	Status	Domain
GET leveltwentytwo	200 OK	ctf.netent.com

Response Headers

```
    Connection  keep-alive
Content-Length  2733
  Content-Type  text/html; charset=utf-8
          Date  Mon, 14 Mar 2016 13:47:18 GMT
          Flag  the_flag_is_awesome
        Server  gunicorn/19.4.5
           Via  1.1 vegur
```

Flag

The flag is: awesome

Challenge 23

The page presented you with an image depicting robots

Solution

Request the http://ctf.netent.com/robots.txt URL

Flag

The flag is: ultron

Challenge 24

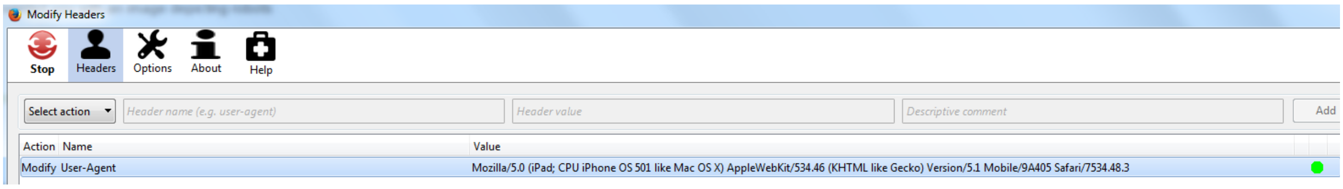
The page presented you with the text

"Sometime is not simple to get the correct viewpoint.
What can change how this page looks?"

Solution

For non-iPhone users

Use a browser add-on or proxy tool in order to modify the HTTP User-Agent request parameter to one matching an iPhone device and visit the page



Action	Name	Value
Modify	User-Agent	Mozilla/5.0 (iPad; CPU iPhone OS 501 like Mac OS X) AppleWebKit/534.46 (KHTML like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

Flag

The flag is: ironman

Challenge 25

The page presented you with the text
"Hope you enjoyed the game. For the last flag, give us a valid credit card number "

and an text input field

Solution

Submit your credit card number 😀😀😀

Alternatively use an online credit card number generator to generate a valid credit card serial

Flag

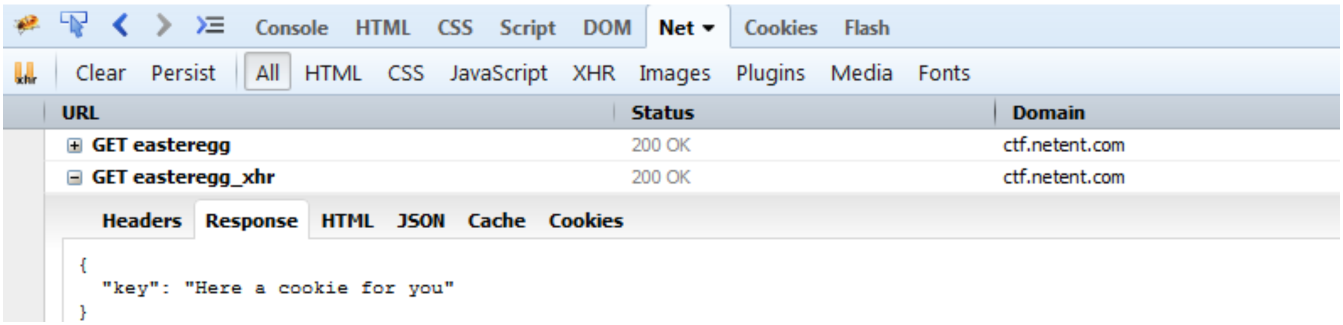
The flag is: money

Easter Egg

Browse to http://ctf.netent.com/easteregg

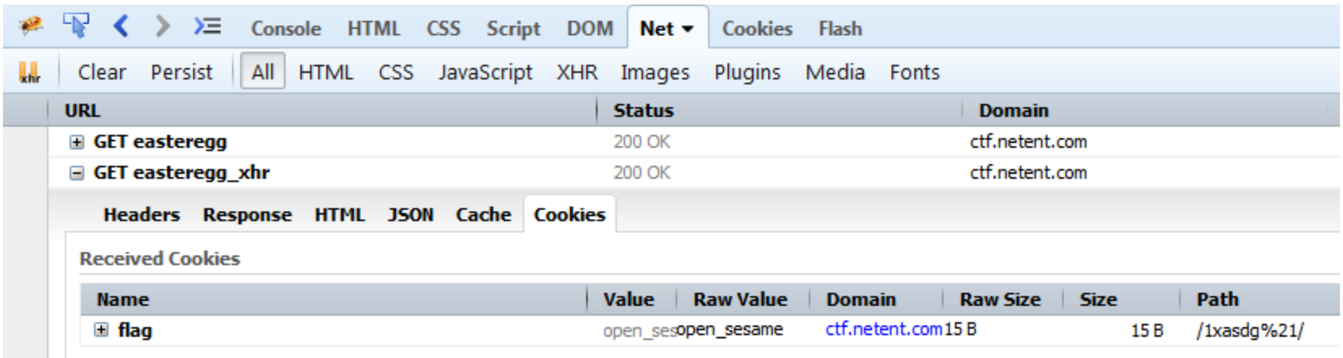
Solution

Inspect the XHR requests that your browser is making



URL	Status	Domain
GET easteregg	200 OK	ctf.netent.com
GET easteregg_xhr	200 OK	ctf.netent.com

```
{
  "key": "Here a cookie for you"
}
```



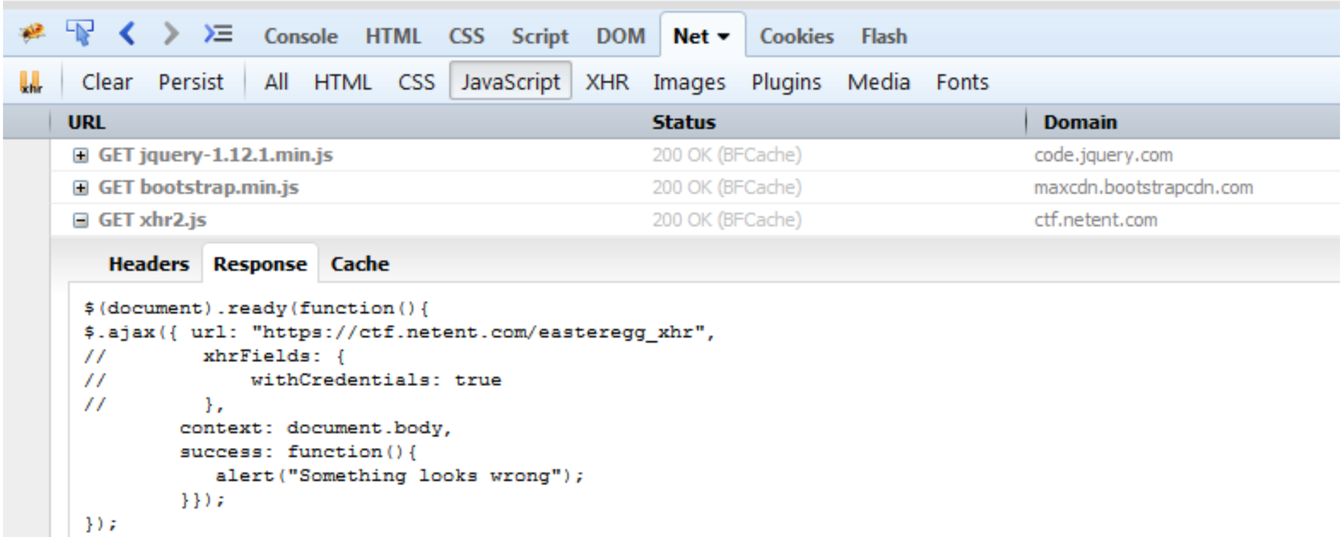
Console HTML CSS Script DOM Net Cookies Flash
Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts
Headers Response HTML JSON Cache Cookies

URL	Status	Domain
⊞ GET easteregg	200 OK	ctf.netent.com
⊟ GET easteregg_xhr	200 OK	ctf.netent.com

Received Cookies

Name	Value	Raw Value	Domain	Raw Size	Size	Path
⊞ flag	open_ses	open_sesame	ctf.netent.com	15 B	15 B	/1xasdg%21/

Notice that the cookie that the XHR response is sending is not actually installed on the browser's cookie jar due to the XHR's configuration in the respective script

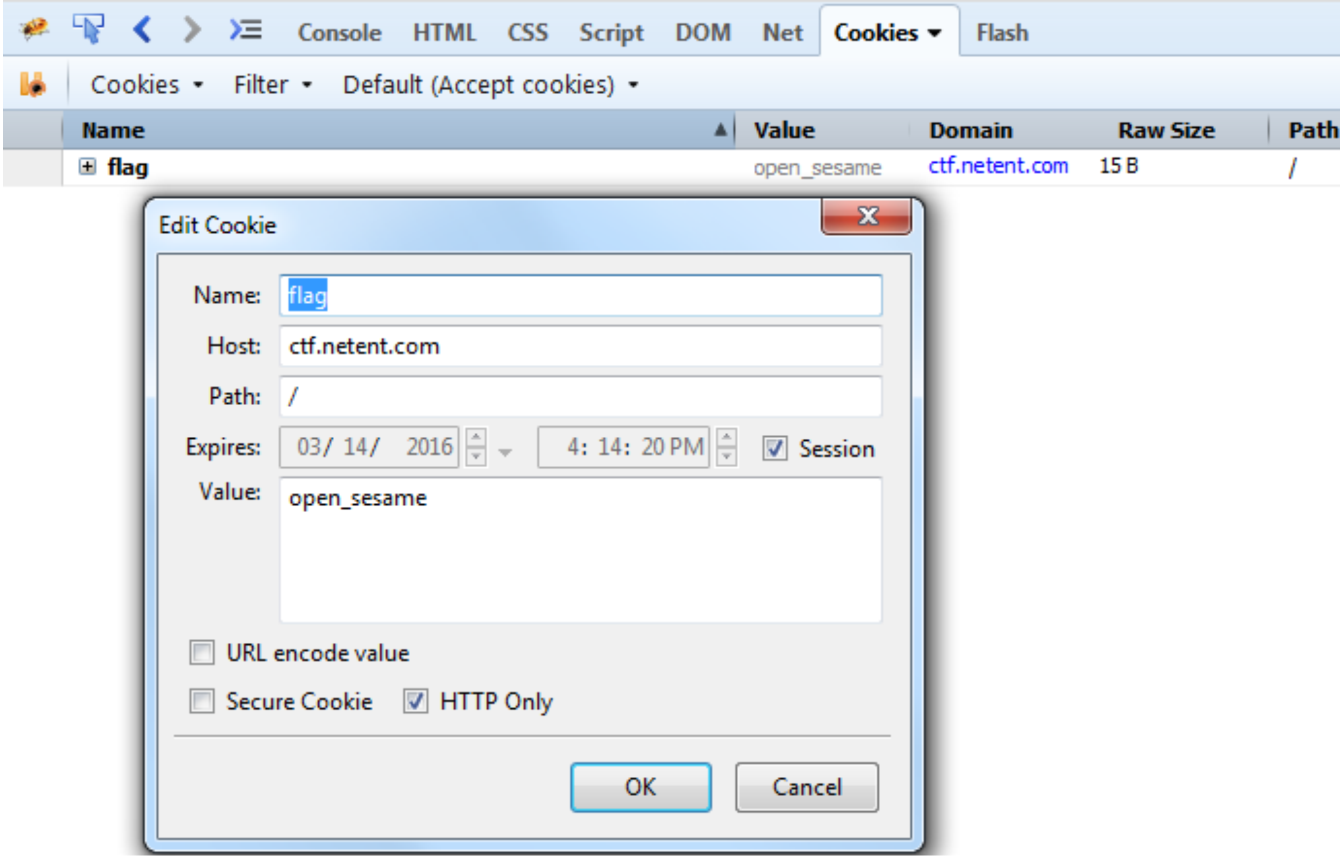


Console HTML CSS Script DOM Net Cookies Flash
Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts
Headers Response Cache

URL	Status	Domain
⊞ GET jquery-1.12.1.min.js	200 OK (BFCache)	code.jquery.com
⊞ GET bootstrap.min.js	200 OK (BFCache)	maxcdn.bootstrapcdn.com
⊟ GET xhr2.js	200 OK (BFCache)	ctf.netent.com

```
$(document).ready(function(){
$.ajax({ url: "https://ctf.netent.com/easteregg_xhr",
//        xhrFields: {
//            withCredentials: true
//        },
        context: document.body,
        success: function(){
           alert("Something looks wrong");
        }});
});
```

Install manually the cookie on your browser



Name	Value	Domain	Raw Size	Path
⊞ flag	open_sesame	ctf.netent.com	15 B	/

Edit Cookie

Name: flag

Host: ctf.netent.com

Path: /

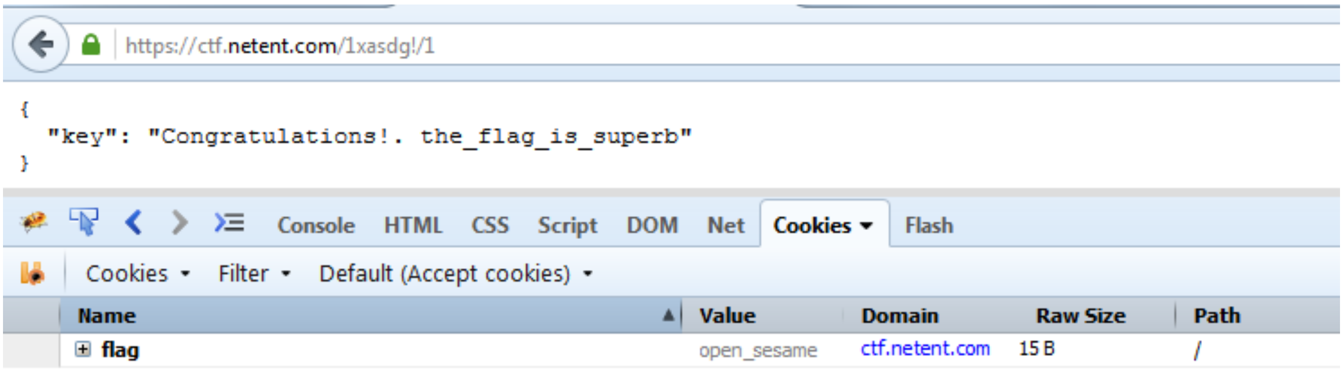
Expires: 03/ 14/ 2016 4: 14: 20 PM ☑ Session

Value: open_sesame

□ URL encode value

□ Secure Cookie ☑ HTTP Only

Navigate to a random page under the URL path that the cookie indicated


https://ctf.netent.com/1xasdg!/1

```
{
  "key": "Congratulations!. the_flag_is_superb"
}
```

Name	Value	Domain	Raw Size	Path
⊞ flag	open_sesame	ctf.netent.com	15 B	/

Flag

The flag is: superb