

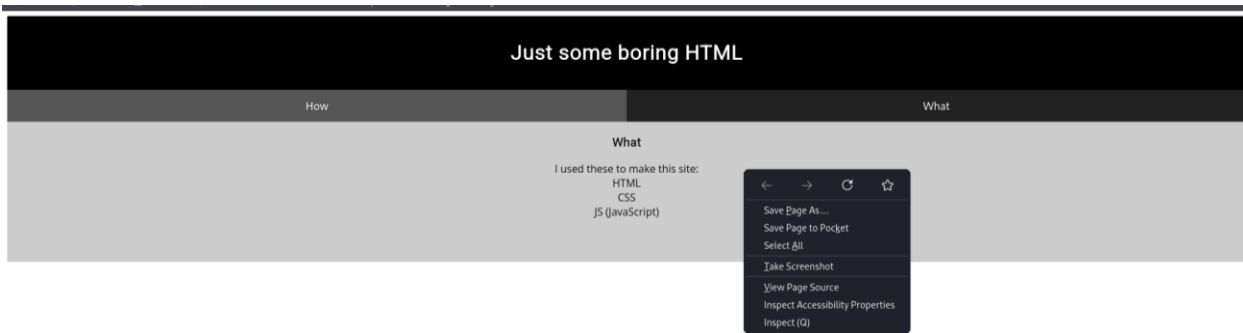
Write up Assignment 3 : Intro to Web Exploit

Mutiara Setya Rini

Daftar Isi

Scavenger Hunt	1
Cookies	4
Where are the robots.....	7
GET aHEAD	8

Scavenger Hunt



Lihat source code dari web yang diberikan dengan klik kanan>view page source.

```
1 <!doctype html>
2 <html>
3 <head>
4   <title>Scavenger Hunt</title>
5   <link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
6   <link rel="stylesheet" type="text/css" href="mycss.css">
7   <script type="application/javascript" src="myjs.js"></script>
8 </head>
9
10 <body>
11   <div class="container">
12     <header>
13       <h1>Just some boring HTML</h1>
14     </header>
15
16     <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen">How</button>
17     <button class="tablink" onclick="openTab('tababout', this, '#222')">What</button>
18
19     <div id="tabintro" class="tabcontent">
20       <h3>How</h3>
21       <p>How do you like my website?</p>
22     </div>
23
24     <div id="tababout" class="tabcontent">
25       <h3>What</h3>
26       <p>I used these to make this site: <br/>
27         HTML <br/>
28         CSS <br/>
29         JS (JavaScript)
30       </p>
31       <!-- Here's the first part of the flag: picoCTF{t -->
32     </div>
33
34   </div>
35
36 </body>
37 </html>
38
```

Dalam page source tersebut terdapat string flag bagian pertama, yaitu picoCTF{t

```
<head>
<title>Scavenger Hunt</title>
<link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
<link rel="stylesheet" type="text/css" href="mycss.css">
<script type="application/javascript" src="myjs.js"></script>
</head>
```

Terdapat link embedded yang refer ke laman lain, coba dicek satu per satu.

mycss.css :

```
div.container {
  width: 100%;
}

header {
  background-color: black;
  padding: 1em;
  color: white;
  clear: left;
  text-align: center;
}

body {
  font-family: Roboto;
}

h1 {
  color: white;
}

p {
  font-family: "Open Sans";
}

.tablink {
  background-color: #555;
  color: white;
  float: left;
  border: none;
  outline: none;
  cursor: pointer;
  padding: 14px 16px;
  font-size: 17px;
  width: 50%;
}

.tablink:hover {
  background-color: #777;
}

.tabcontent {
  color: #111;
  display: none;
  padding: 50px;
  text-align: center;
}

#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }

/* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_10 */
```

Terlihat di dalam page source ini terdapat flag part 2, yaitu h4ts_4_10

myjs.js :

```
function openTab(tabName,elmnt,color) {
  var i, tabcontent, tablinks;
  tabcontent = document.getElementsByClassName("tabcontent");
  for (i = 0; i < tabcontent.length; i++) {
    tabcontent[i].style.display = "none";
  }
  tablinks = document.getElementsByClassName("tablink");
  for (i = 0; i < tablinks.length; i++) {
    tablinks[i].style.backgroundColor = "";
  }
  document.getElementById(tabName).style.display = "block";
  if(elmnt.style != null) {
    elmnt.style.backgroundColor = color;
  }
}

window.onload = function() {
  openTab('tabintro', this, '#222');
}

/* How can I keep Google from indexing my website? */
```

Dalam source page ini terdapat satu clue yaitu “How can I keep Google from indexing my website” yang berarti bahwa bagaimana Google bisa dicegah untuk mengindeks website. Untuk melakukan hal ini, bisa menggunakan file robots.txt. Jadi coba kita buka [viewsource:http://mercury.picoctf.net:27278/robots.txt](http://mercury.picoctf.net:27278/robots.txt)

```
User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

dalam page source robots.txt tersebut ditemukan flag part 3, yaitu `t_0f_pl4c`. Selain itu, dalam page ini juga ditemukan sebuah clue baru, yaitu “# I think this is an apache server... can you Access the next flag?”. Dari clue ini kita bisa mengunjungi [viewsource:http://mercury.picoctf.net:27278/.htaccess](http://mercury.picoctf.net:27278/.htaccess)

```
# Part 4: 3s_2_l00k
# I love making websites on my Mac, I can Store a lot of information there.
```

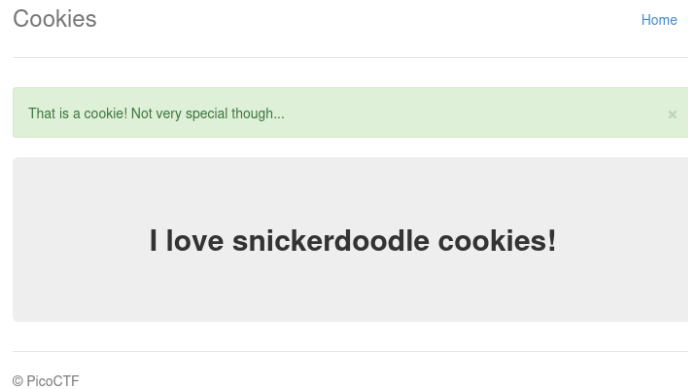
Dari source page ini kita mendapatkan string flag part 4, yaitu `3s_2_l00k`. Selain itu, juga mendapatkan clue baru, yaitu “I love making websites on my Mac, I can Store a lot of information there.” yang artinya pada step selanjutnya kita bisa memanfaatkan `.DS_Store`, di mana file tersebut menyimpan metadata direktori yang secara otomatis dibuat oleh macOS. Berikut adalah hasilnya :

```
Congrats! You completed the scavenger hunt. Part 5: _a69684fd}
```

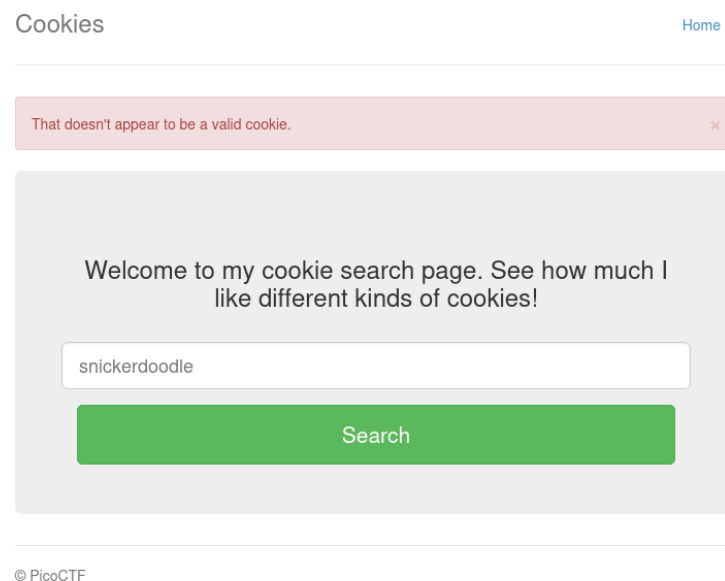
Jadi flag komplit yang telah berhasil didapatkan adalah `picoCTF{th4ts_4_10t_of_pl4c3s_2_l00k__a69684fd}`

Cookies

Ketika kita memasukkan snickerdoodle ke dalam search box maka akan muncul respons seperti ini dan url berubah menjadi mercury.picoctf.net:<port>/check.



Tetapi ketika kita memasukkan string lain, contohnya adalah 'miaw' maka akan muncul seperti ini :



Dan url pun tidak berubah, tetap mercury.picoctf.net:<port>

Coba kita menggunakan burpsuite untuk menyelesaikan challenge ini.

```
Request
Pretty Raw Hex
1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:21485
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Referer: http://mercury.picoctf.net:21485/
9 Accept-Encoding: gzip, deflate, br
10 Cookie: name=7
11 Connection: keep-alive
12
13
```

Kita dapatkan name cookie dalam burp suite. Kemudian send to intruder dan setting payloadnya menjadi seperti ini :

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101

Payload type: Numbers Request count: 0

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 0

To: 100

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples

1

321

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Tidak lupa juga setting Grep Match dengan menambahkan picoCTF{ yang merupakan awalan dari string flag.

? Grep - Match

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

Load...

Remove

Clear

picoCTF{

Add

picoCTF{

Match type: ☒ Simple string

☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Start attack dan menunggu attack selesai.

2. Intruder attack of http://mercury.picoctf.net:21485

Attack Save

2. Intruder attack of http://mercury.picoctf.net:21485

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	picoCTF{	Comment
15	14	200	255			1931		
16	15	200	261			1937		
17	16	200	264			1935		
18	17	200	260			1932		
19	18	200	262			1265	1	
20	19	200	262			1935		
21	20	200	265			1934		
22	21	200	262			1934		
23	22	200	263			1933		
24	23	200	258			1938		

Request Response

Pretty Raw Hex Render

33

</div>

34

<div class="jumbotron">

35

<p class="lead">

36

</p>

37

<p style="text-align:center; font-size:90px;">

38

39

Flag

40

41

: <code>

42

picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}

43

</code>

44

</p>

45

</div>

46

<div class="footer">

47

<p>

48

© PicoCTF

49

</p>

50

</div>

51

</body>

52

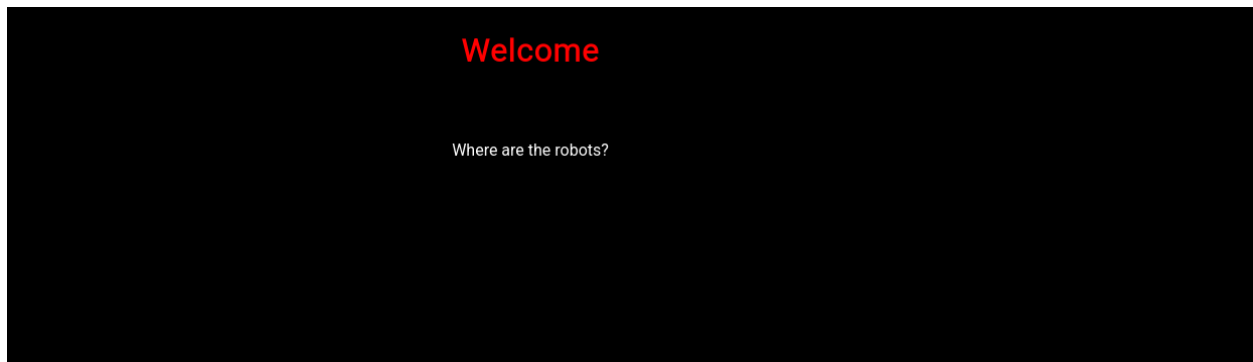
</html>

0 highlights

Cari line yang memiliki indeks picoCTF{ berupa 1, yang juga berarti bahwa line tersebut mengandung string flag. Didapatkan flag, yaitu picoCTF{3v3ry1_l0v3s_c00k135_94190c8a}

6

Where are the robots



Dari page ini, kita bisa menemukan clue, yaitu “Where are the robots?”. Clue ini kemungkinan merujuk pada robots.txt. Mari kita coba membuka laman <https://jupiter.challenges.picoctf.org/problem/<port>/robots.txt>

```
User-agent: *  
Disallow: /1bb4c.html
```

Didapatkan output seperti ini, yang menjadi clue selanjutnya. Kemudian kita coba buka <https://jupiter.challenges.picoctf.org/problem/<port>/1bb4c.html>

```
Guess you found the robots  
picoCTF{ca1cu1at1ng_Mach1n3s_8028f}
```

Flag berhasil ditemukan.

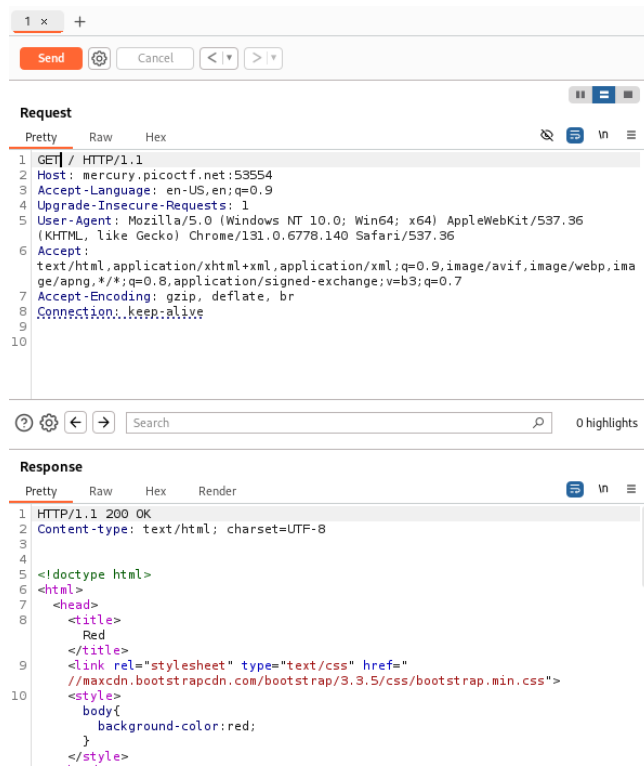
GET aHEAD



Kita dihadapkan pada 2 pilihan, yaitu red dan blue. Ketika dicoba keduanya, hasil dari klik button hanyalah bergantinya warna background. Selanjutnya coba lihat page sourcenya dan ternyata tidak ada sesuatu yang janggal seperti di bawah ini :

```
1
2 <!doctype html>
3 <html>
4 <head>
5   <title>Red</title>
6   <link rel="stylesheet" type="text/css" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
7   <style>body {background-color: red;}</style>
8 </head>
9 <body>
10   <div class="container">
11     <div class="row">
12       <div class="col-md-6">
13         <div class="panel panel-primary" style="margin-top:50px">
14           <div class="panel-heading">
15             <h3 class="panel-title" style="color:red">Red</h3>
16           </div>
17           <div class="panel-body">
18             <form action="index.php" method="GET">
19               <input type="submit" value="Choose Red"/>
20             </form>
21           </div>
22         </div>
23       </div>
24       <div class="col-md-6">
25         <div class="panel panel-primary" style="margin-top:50px">
26           <div class="panel-heading">
27             <h3 class="panel-title" style="color:blue">Blue</h3>
28           </div>
29           <div class="panel-body">
30             <form action="index.php" method="POST">
31               <input type="submit" value="Choose Blue"/>
32             </form>
33           </div>
34         </div>
35       </div>
36     </div>
37   </div>
38 </body>
39 </html>
40
```

Selanjutnya kita coba analisis menggunakan burpsuite karena hint dari challengenya sendiri adalah *“Check out tools like Burpsuite to modify your requests and look at the responses”*. Hint tersebut secara tidak langsung memberi tahu bahwa kita harus mengubah sesuatu pada request dan melihat responsnya.

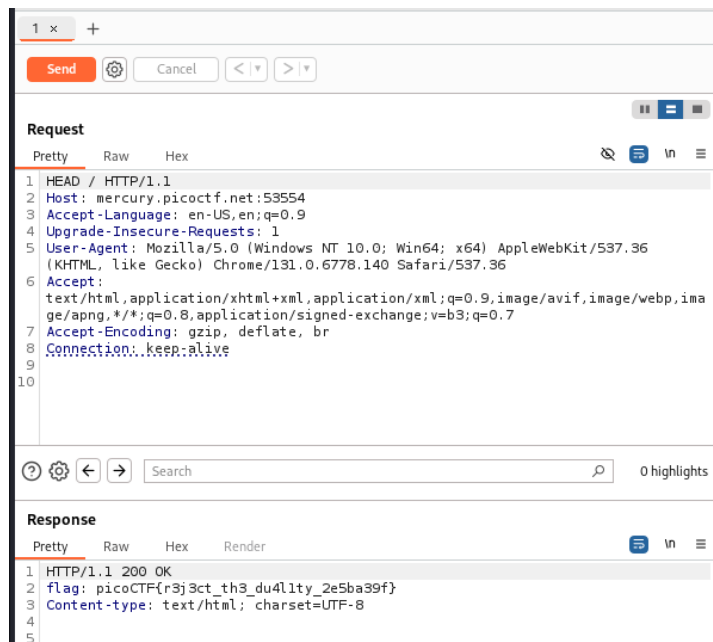


The screenshot shows a web browser's developer tools with the 'Request' tab selected. The request is a GET to `mercury.picoctf.net:53554`. The response is an HTTP 200 OK with `Content-type: text/html; charset=UTF-8`. The response body is an HTML document with a red background and a title 'Red'.

```
1 GET / HTTP/1.1
2 Host: mercury.picoctf.net:53554
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

```
1 HTTP/1.1 200 OK
2 Content-type: text/html; charset=UTF-8
3
4
5 <!doctype html>
6 <html>
7   <head>
8     <title>
9       Red
10    </title>
    <link rel="stylesheet" type="text/css" href="
      //maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
    <style>
      body{
        background-color:red;
      }
    </style>
```

Sesuai nama challengenya, sepertinya kita harus mencoba mengganti GET dengan HEAD yang memungkinkan kita bisa mengambil header https tanpa load bodynya.



The screenshot shows a web browser's developer tools with the 'Request' tab selected. The request is a HEAD to `mercury.picoctf.net:53554`. The response is an HTTP 200 OK with `Content-type: text/html; charset=UTF-8`. The response body is an HTML document with a red background and a title 'Red'.

```
1 HEAD / HTTP/1.1
2 Host: mercury.picoctf.net:53554
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

```
1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4l1ty_2e5ba39f}
3 Content-type: text/html; charset=UTF-8
4
5
```

String flag berhasil ditemukan, yaitu `picoCTF{r3j3ct_th3_du4l1ty_2e5ba39f}`