

Hungry Monkey

In this challenge we were given a website which contained a monkey and three options:

- orange
- pineapple
- apple

When one of the three options were selected the monkey would say a different phrase depending on the option.

1. To get the flag in this challenge it was necessary to modify the http request such that it gave "banana" instead of one of the three options.
2. This can be done by using the Repeater option in BurpSuite.
3. Using this we can change the input manually instead of relying on the three options.
4. To change the input manually we enter the website using the browser in BurpSuite.
5. When we access the website within this browser and submit one of the three options a POST request appears in the intercept section in BurpSuite that shows the option given along with the response.

The screenshot displays the Burp Suite interface with the 'Target' tab selected. The URL bar shows 'https://ctf1.gmstctf.com'. The 'Intercept' tab is active, showing a list of intercepted requests. The selected request is a POST to '/php/monkey-cuB26xTx/index.php' with a status of 200 and a length of 786. The 'Request' pane shows the raw HTTP request, and the 'Response' pane shows the raw HTTP response.

Request:

```
POST /php/monkey-cuB26xTx/index.php HTTP/2
Host: ctf1.gmstctf.com
Content-Length: 11
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://ctf1.gmstctf.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://ctf1.gmstctf.com/php/monkey-cuB26xTx/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
food=orange
```

Response:

```
HTTP/2 200 OK
Server: nginx/1.20.1
Date: Mon, 05 Dec 2022 23:24:53 GMT
Content-Type: text/html
X-Powered-By: PHP/5.4.16
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains

<!DOCTYPE HTML>
<html>
<head>
</head>
<body>
<div style="text-align: center">

<form method="POST" action="/php/monkey-cuB26xTx/index.php">
  <p>
    Please <b>FEED ME!</b>
  </p>
  <input type="radio" name="food" value="orange">
    Orange<br>
  <input type="radio" name="food" value="apple">
    Apple<br>
  <input type="radio" name="food" value="pineapple">
    Pineapple<br>
  <br>
  <input type="submit" value="Submit">
</form>
  <br>
  Your input: orange
</div>
  <br>
  Really? An orange? That's doesn't rhyme with anything!<br>
</div>
</body>
</html>
```

6. We then send this POST request to the Repeater and change the option to banana.

The screenshot shows the Burp Suite Repeater interface. The target is `https://ctf1.gmstctf.com`. A POST request is being sent to `/php/monkey-cuB26xTx/index.php`. The request body contains the following data:

```
1 POST /php/monkey-cuB26xTx/index.php HTTP/2
2 Host: ctf1.gmstctf.com
3 Content-Length: 11
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://ctf1.gmstctf.com
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
12 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
13 Safari/537.36
14 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=0.9
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Referer: https://ctf1.gmstctf.com/php/monkey-cuB26xTx/index.php
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 food=banana
```

The response is an HTTP 200 OK with the following HTML content:

```
1 HTTP/2 200 OK
2 Server: nginx/1.20.1
3 Date: Mon, 05 Dec 2022 23:27:17 GMT
4 Content-Type: text/html
5 X-Powered-By: PHP/5.4.16
6 X-Frame-Options: SAMEORIGIN
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8
9 <!DOCTYPE HTML>
10 <html>
11 <head>
12 </head>
13 <body>
14 <div style="text-align: center">
15 
16 <form method="POST" action="/php/monkey-cuB26xTx/index.php">
17 <p>
18 Please <b>
19 FEED ME!
20 </b>
21 </p>
22 <input type="radio" name="food" value="orange">
23 Orange<br>
24 <input type="radio" name="food" value="apple">
25 Apple<br>
26 <input type="radio" name="food" value="pineapple">
27 Pineapple<br>
28 <input type="submit" value="Submit">
29 </form>
30 <br>
31 Your input: banana
32 <h3>
33 Yes! A banana! Thanks!!
34 </h3>
35 <font color=blue>
36 A flag for you: Z84uy7HjzegMxUX3
37 </font>
38 </div>
39 </body>
40 </html>
```

The response body shows the rendered HTML, including a form with radio buttons for "orange", "apple", and "pineapple", and a submit button. The response also displays the user's input "banana" and a confirmation message "Yes! A banana! Thanks!!". A flag is provided: `Z84uy7HjzegMxUX3`.

7. With this we acquire the flag.