



The First Payload Challenge Writeup

Category : Web Security

Difficulty: Basic

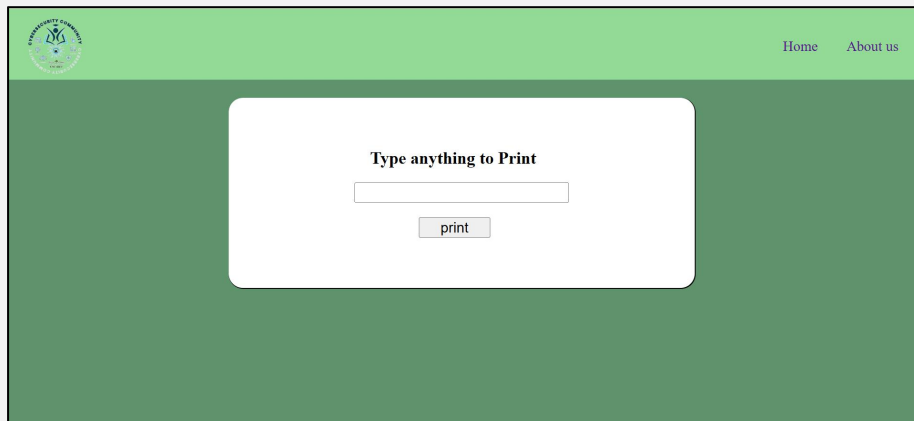
Author: Baraa Sabbah

Hello, and welcome to our community!

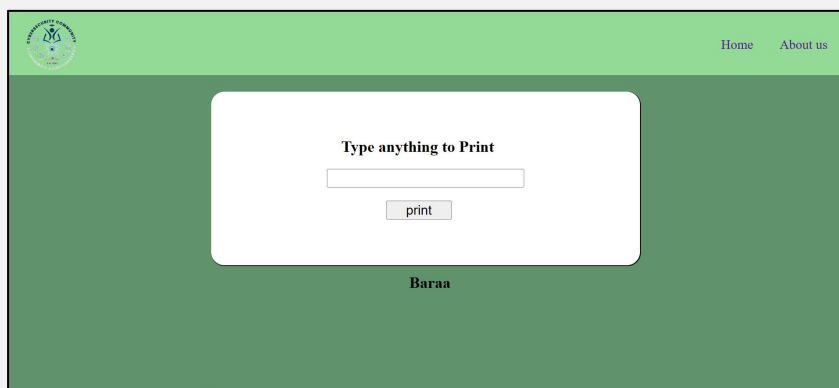
We hope you enjoy participating in the first CTF we've created.

Here is the write-up for the **"The First Payload"** challenge.

Let's Start !!



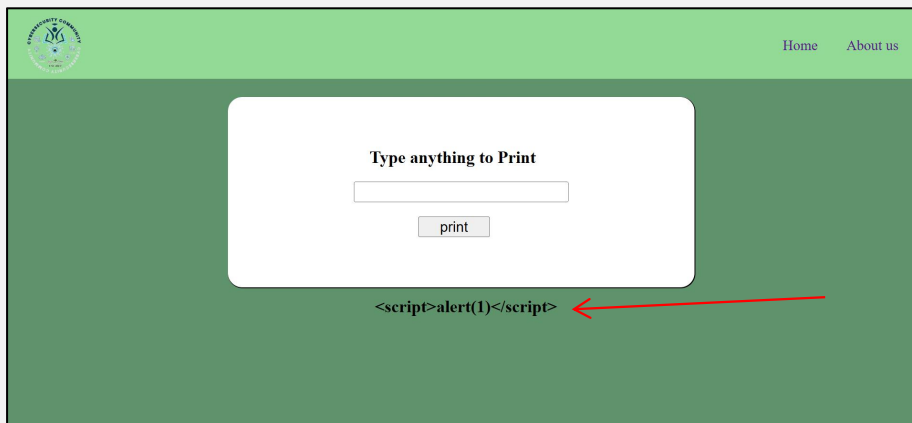
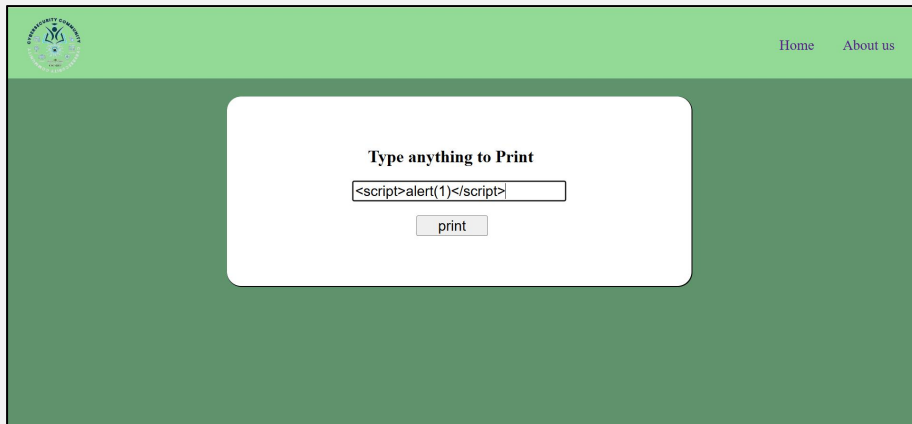
As we see it a simple web page that provide a functionality for printing any text you type
Lets try this



As we see it just print what you type in the input , so the first thing we may think is to check the xss

We can use simple JavaScript code to check if there an xss

I'll try `<script>alert(1)</script>`



It doesn't work the browser simply prints our payload instead of executing it.

```
<div class="result">
  <h2>&lt;script&gt;alert(1)&lt;/script&gt;</h2>
</div>
```

As we can see this is shown in the source code and that tell us the programmer impalement a filter for xss , the application escaping < and > characters instead of letting the browser interpret them as real tags.

Suppose we stop testing ??

No

Let's check the source code maybe we can find something.

```

1  <!-- src -->
2  <!-- src -->
3  <!-- src -->
4  <!-- src -->
5  <!-- src -->
6  <!-- src -->
7  <!-- src -->
8  <!-- src -->
9  <!-- src -->
10 <!-- src -->
11 <!-- src -->
12 <!-- src -->
13 <!-- src -->
14 <!-- src -->
15 <!-- src -->
16 <!-- src -->
17 <!-- src -->
18 <!-- src -->
19 <!-- src -->
20 <!-- src -->
21 <!-- src -->
22 <!-- src -->
23 <!-- src -->
24 <!-- src -->
25 <!-- src -->
26 <!-- src -->
27 <!-- src -->
28 <!-- src -->
29 <!-- src -->
30 <!-- src -->
31 <!-- src -->
32 <!-- src -->
33 <!-- src -->
34 <!-- src -->
35 <!-- src -->
36 <!-- src -->
37 <!-- src -->
38 <!-- src -->
39 <!-- src -->
40 <!-- src -->
41 <!-- src -->
42 <!-- src -->
43 <!-- src -->
44 <!-- src -->
45 <!-- src -->
46 <!-- src -->
47 <!-- src -->
48 <!-- src -->
49 <!-- src -->
50 <!-- src -->
51 <!-- src -->
52 <!-- src -->
53 <!-- src -->
54 <!-- src -->
55 <!-- src -->
56 <!-- src -->
57 <!-- src -->
58 <!-- src -->
59 <!-- src -->
60 <!-- src -->
61 <!-- src -->
62 <!-- src -->
63 <!-- src -->
64 <!-- src -->
65 <!-- src -->
66 <!-- src -->
67 <!-- src -->
68 <!-- src -->
69 <!-- src -->
70 <!-- src -->
71 <!-- src -->
72 <!-- src -->
73 <!-- src -->
74 <!-- src -->
75 <!-- src -->
76 <!-- src -->
77 <!-- src -->
78 <!-- src -->
79 <!-- src -->
80 <!-- src -->
81 <!-- src -->
82 <!-- src -->
83 <!-- src -->
84 <!-- src -->
85 <!-- src -->
86 <!-- src -->
87 <!-- src -->
88 <!-- src -->
89 <!-- src -->
90 <!-- src -->
91 <!-- src -->
92 <!-- src -->
93 <!-- src -->
94 <!-- src -->
95 <!-- src -->
96 <!-- src -->
97 <!-- src -->
98 <!-- src -->
99 <!-- src -->
100 <!-- src -->

```

There is Nothing actually, ok as we see in the home page before there is another page called About us

The screenshot shows the top of a web page with a green header. On the left is a circular logo. On the right are links for 'Home' and 'About us'. Below the header, the text reads 'Cybersecurity Community - Birzeit University' and 'we are here to help you all for develop Your skills in Cybersecurity'. In the center is a white rounded rectangle titled 'Contact Us'. It contains an 'Email :' label with an empty text box, a 'Message :' label with an empty text area, and a 'send' button at the bottom.

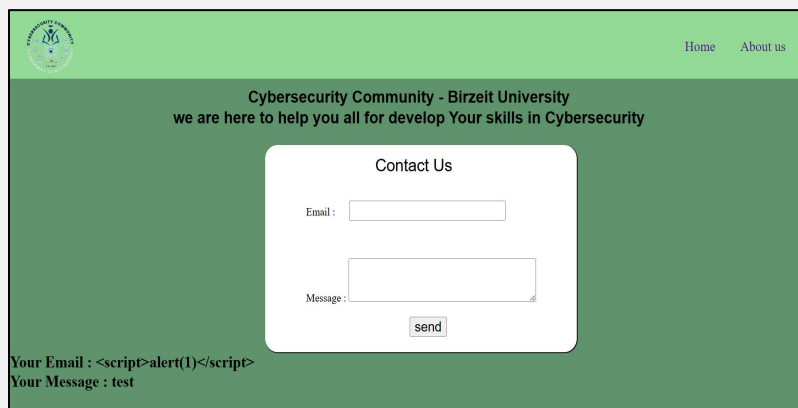
It a Contact Us form , lets try what this do

This screenshot shows the same contact form as before, but with the submitted data displayed at the bottom left: 'Your Email : baraa@gmail.com' and 'Your Message : hello'. The form fields and 'send' button are still visible in the center.

We can inject a JavaScript code to see if there an xss

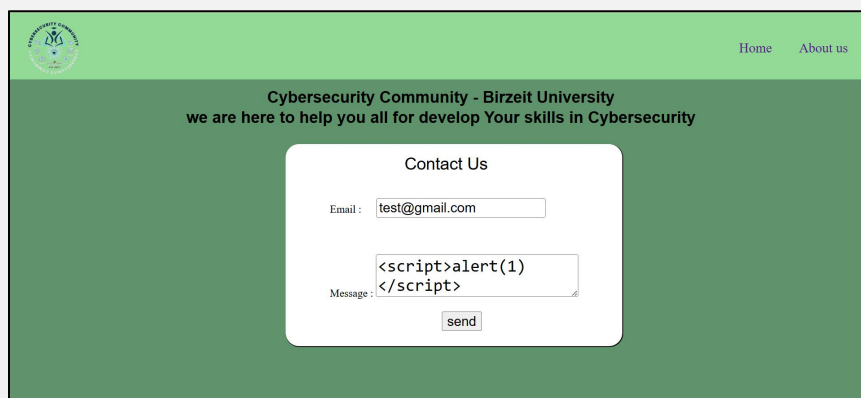
Let's try

This screenshot shows the contact form with a JavaScript payload injected into the email field. The 'Email :' label is followed by a text box containing the code '<script>alert(1)</script>'. The 'Message :' label is followed by a text box containing the word 'test'. The 'send' button remains at the bottom of the form.

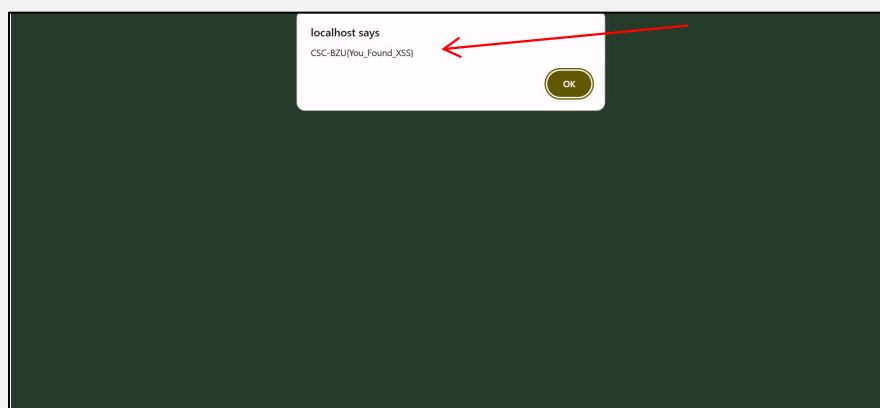


The screenshot shows a web application with a green header and a dark green background. The header contains a logo on the left and 'Home' and 'About us' links on the right. The main content area has the text 'Cybersecurity Community - Birzeit University' and 'we are here to help you all for develop Your skills in Cybersecurity'. In the center is a white 'Contact Us' form with an 'Email' field and a 'Message' field, both with 'send' buttons. Below the form, the text 'Your Email : <script>alert(1)</script>' and 'Your Message : test' is displayed.

Email field also protected , maybe the programmer forget to protect the message field , who's know?



This screenshot shows the same 'Contact Us' form as the previous one, but with the 'Email' field filled with 'test@gmail.com' and the 'Message' field filled with the JavaScript payload '<script>alert(1)</script>'. The 'send' button is visible below the message field.



It worked! The browser successfully executed the payload