

Burninator Sec

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

Tuesday, April 13, 2021

CVE-2020-29592 and CVE-2020-29593 - Orchard CMS Unrestricted File Upload and XSS

Note: This is fixed in Orchard 1.10, this post is about Orchard 1.8.1.0.

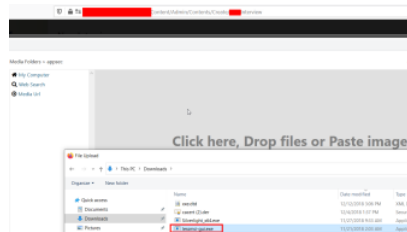
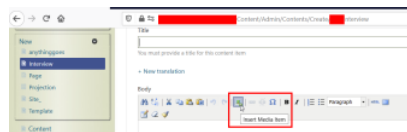
CVE-2029-29592 - Unrestricted File Upload via Media Folder and TinyMCE HTML Editor:



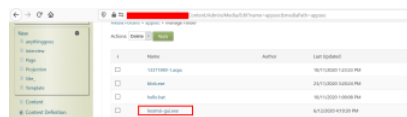
Not allowed because these are the allowed file types:



But we can...



Success!



CVE-2020-29593 - XSS via Media Types Settings



[//cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29592](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29592)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29593>

Posted by burninator at 7:26 PM

Labels: **attack chaining**, **broken access control**, **CVE**, **external libraries**, **unrestricted file upload**, **XSS**

No comments:

Post a Comment

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)

► July (1)

► June (1)

▼ April (6)

CVE-2020-29592 and
CVE-2020-29593 -
Orchard CMS Un...

RCE Using Recaf: an Awesome Java Decompiler/Recomp...

Hash Cracking with Rental AI GPUs

CVE-2020-26885 - XSS in 2SXC

CVE-2021-3163 - Stored XSS Slab Quill JS

Bamboozle D 3 f e n d e r
Effortlessly (BDE) - Fi...

► 2020 (7)

► 2019 (5)

► 2018 (8)

► 2014 (1)

► 2013 (8)

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



[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)
