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

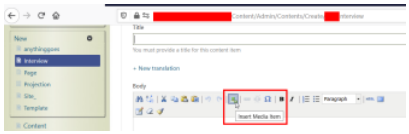
CVE-2020-29592 and CVE-2020-29593 - Orchard CMS Unrestricted File Upload and XSS

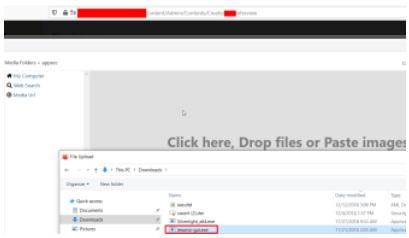
Note: This is fixed in Orchard 1.10, this post is about Orchard 1.8.1.0.

CVE-2929-29592 - 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

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

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

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)