Name : Rukmal Hewawasam
Index: MS14961304

Microsoft education remote code execution

I found the time to hunt some bugs. I recently discovered that Microsoft also launched a bug bounty program so I decided to have a look there. I actually wanted to research on one of their sites that is eligible for a monetary reward, just to challenge myself.

I ended up on a Microsoft subdomain education.microsoft.com and it seemed pretty secure at first.

XSS in data input fields

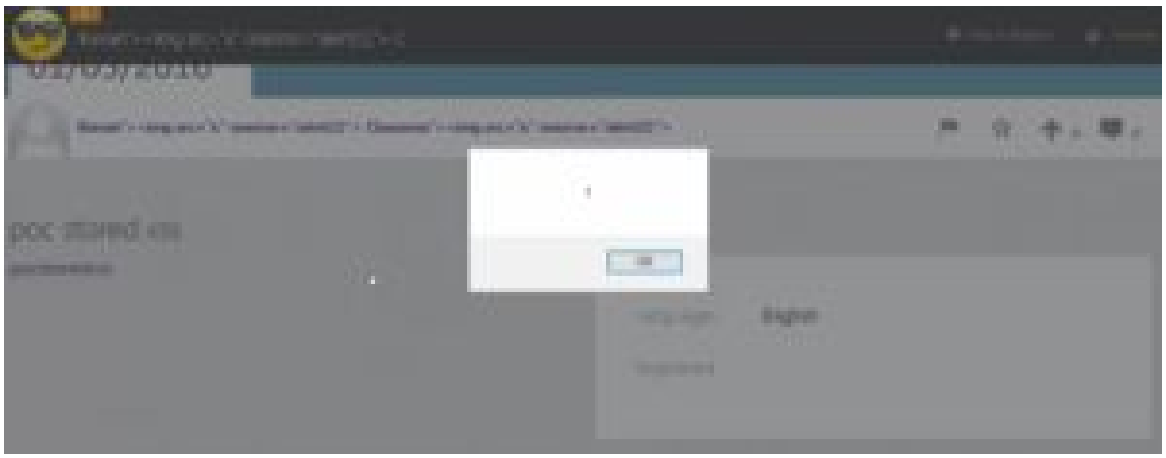
There was xss protection on all inputs, and csrf tokens were in place.

I then discovered a feature to build my own course page, the editor looked a bit like these website builders, it seemed a cool target so I started fiddling with it.

It didn’t take long before the first stored XSS popped up.

There were several stored xss, but this one was the most trivial.

I simply put a javascript:alert(‘xss’); in the URL field, and bet what?



It worked!

XSS image uploader

The uploaded files are stored somewhere on the server and I wasn't able to find out where.

But I wanted to be sure, so I looked for another upload functionality.

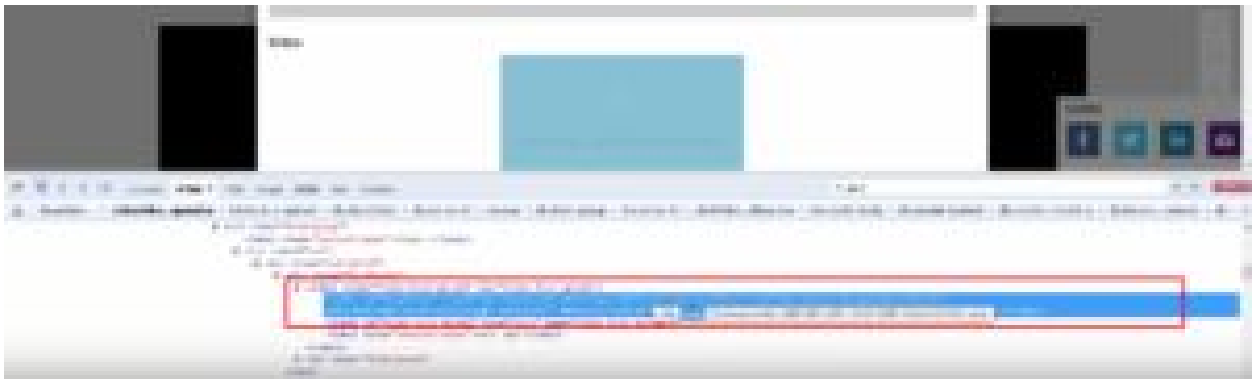
I found out I could upload videos, and that's where it got interesting.

I uploaded a file, video.php, and got the following screen:

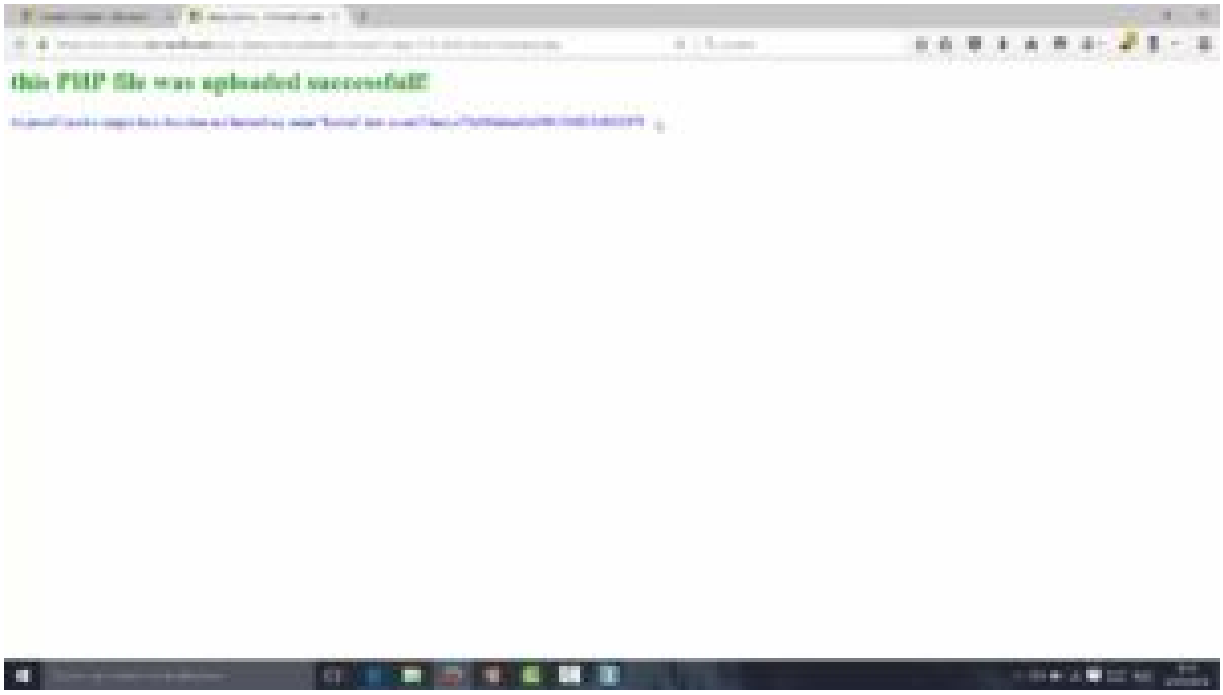
It's stating that the mime-type of the uploaded file was not supported.

I looked at the source and saw the link to a php file.

Well This could turn out to be nothing but hey, you've read the title so you know how it goes from here. 



I pasted the link in my browser and I got the PHP file presented that I uploaded.



I reported it to Microsoft the same day.