MICROSOFT BUG REPORT

NAME:JAYATEERTHA G

I have done the usual recon process and found a subdomain of microsoft (imagineacademy.microsoft.com) ,which faced XSS(cross side scripting) bug.

I had reported the same following responsible disclosure measures to secure@microsoft.com,in the month of march and continued to be in contact with the Microsoft security team continuously till the bug is fixed.

On may 1 , I received a confirmation mail from Microsoft stating that a –" A fix was confirmed for the issue you presented. Microso would like to recognize your efforts on our public security researcher acknowledgement page: "Security Researcher Acknowledgments for Microso Online Services". "

This was my first bug report and achievement from Microsoft.

I further continued my research and also reported few more bugs in other Microsoft services such as outlook,bing etc.

The outlook bug which I presented , had some serious bug which I am not allowed to disclose until its fixed, But they agreed to offer me a swag for all my efforts and assistance.

I attach all the supporting documents of the bug,email conversations etc in this letter .

Thanks

REGARDS

JAYATEERTHA G

MICROSOFT BUG POC

***case:* MSRC Case 44430 CRM:0461041554**

email:jayateertha043@gmail.com

Hello microsoft security team,

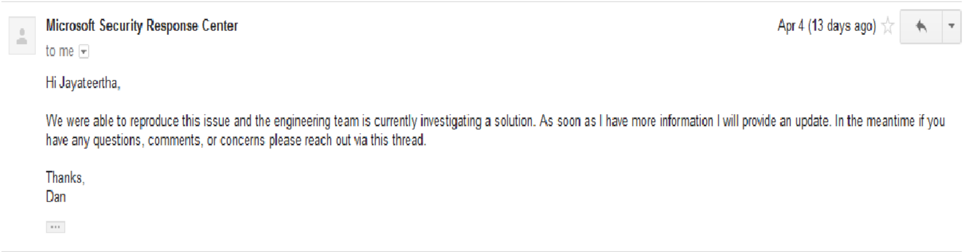
This is a written poc for the xss bug i found in **imagineacademy.microsoft.com** *website.*

Alternately you could also watch for the poc in video format in the previous emails or a

link in youtube: ***www.youtu.be/tgKLrGDhYu8***

For more information on what a xss vulnerability is and remediation follow up owasp guide or email me:*https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).*

I have already recieved a email that the bug is reproducable and the engineering team is investigating on a fix for this.Hope this would be helpful to fix it soon.



Microsoft Security Response Center

to me

Apr 4 (13 days ago)

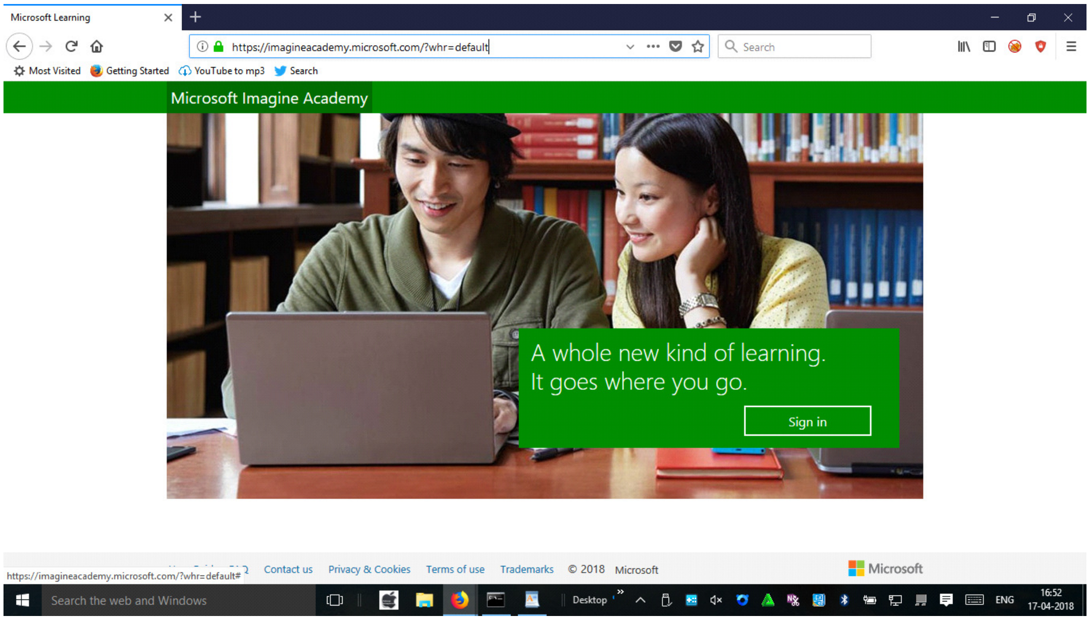
Hi Jayateertha,

We were able to reproduce this issue and the engineering team is currently investigating a solution. As soon as I have more information I will provide an update. In the meantime if you have any questions, comments, or concerns please reach out via this thread.

Thanks,
Dan

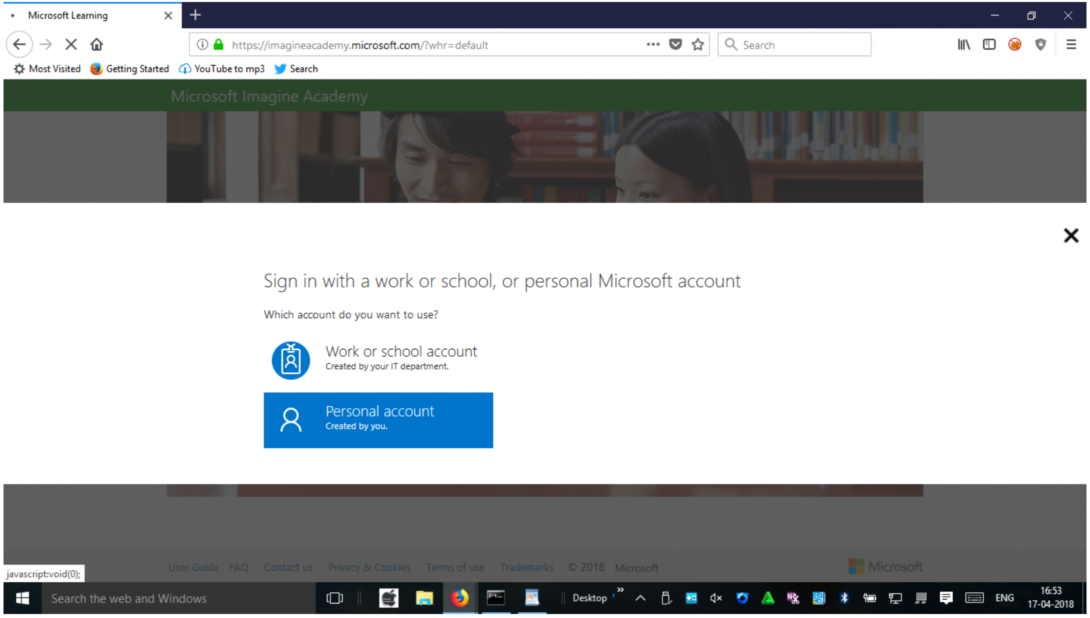
Steps to reproduce the bug:

step 1: goto https://imagineacademy.microsoft.com



A whole new kind of learning.
It goes where you go.

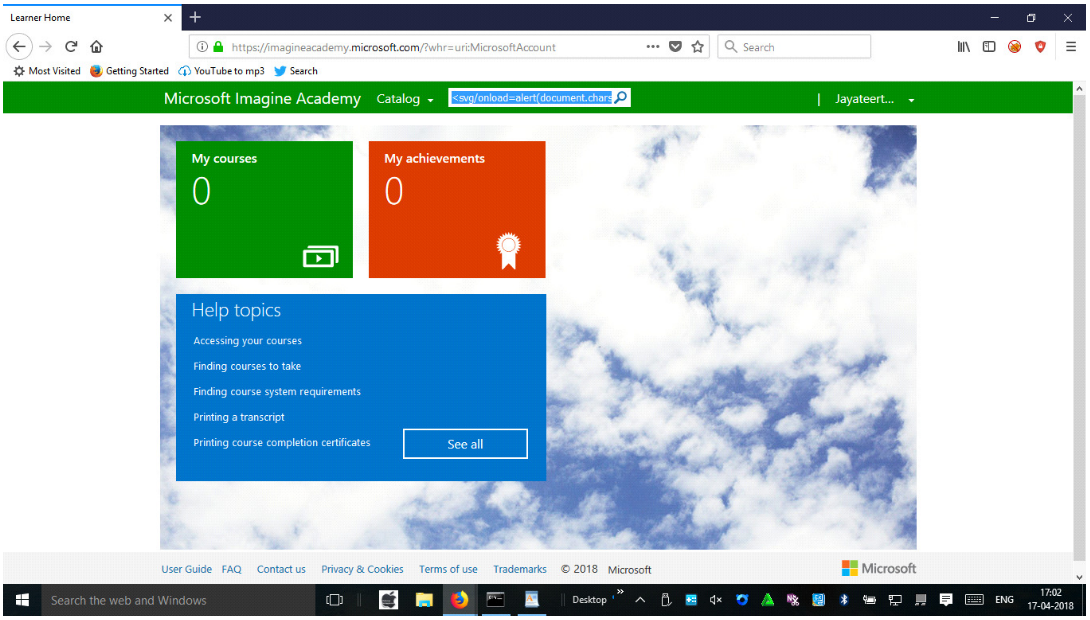
step 2:click sign in and then chose your account and sign in.



Sign in with a work or school, or personal Microsoft account

Which account do you want to use?

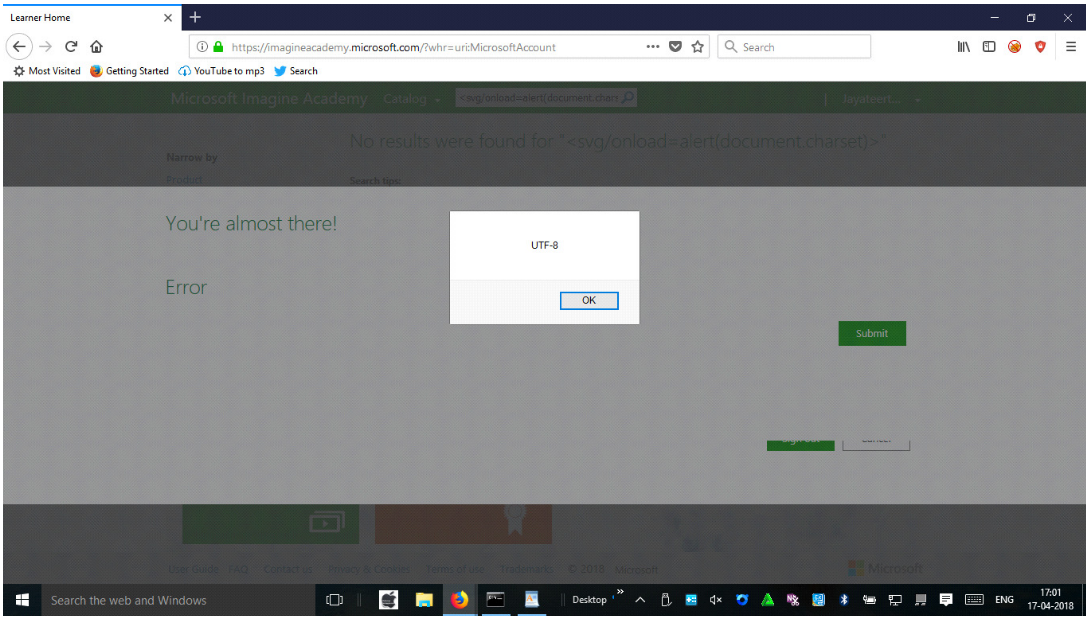
step 3: In the search bar enter the following payload : <svg/onload=alert(document.charset)>



https://imagineacademy.microsoft.com/?whr=uri:MicrosoftAccount

<svg/onload=alert(document.chars

step 4:press enter or click search button ,a classic xss pop up would appear telling the character set used ,which proves existence of xss vulnerability.



https://imagineacademy.microsoft.com/?whr=uri:MicrosoftAccount

No results were found for "<svg/onload=alert(document.charset)>"

You're almost there!

Error

UTF-8

Hope it would be fixed soon.

Thank you

REGARDS

JAYATEERTHA G

jayateertha guruprasad <jayateertha043@gmail.com>

RE: Xss bug status CRM:0461046525

Microsoft Security Response Center <secure@microsoft.com> Tue, May 1, 2018 at 3:33 AM
To: Microsoft Security Response Center <secure@microsoft.com>, Jayateertha Guruprasad <jayateertha043@gmail.com>

Hello Jayateertha,

A fix was confirmed for the issue you presented. Microsoft would like to recognize your efforts on our public security researcher acknowledgement page:
"Security Researcher Acknowledgments for Microsoft Online Services"
<https://technet.microsoft.com/-us/security/cc308589>

If you would like to be acknowledged please provide the following:
Name
If it is an Individual or Company Name
URL to Twitter or online profile

We have resolved the issue you reported, and closed this case.

If you have any questions, or additional information related to this report, please reply on this case thread.

Thank you very much for working with us.

Regards,
Kamuran
MSRC

Link to Bounty Program Terms: https://technet.microsoft.com/en-us/security/dn800983
Link to Privacy Statement: https://technet.microsoft.com/en-us/security/dn425050
Link to Coordinated Vulnerability Disclosure Policy: https://technet.microsoft.com/en-us/security/dn467923.aspx

------------------ Original Message ------------------
From: Jayateertha Guruprasad
[Quoted text hidden]
[Quoted text hidden]

Gmail **jayateertha guruprasad <jayateertha043@gmail.com>**

RE: Xss bug status CRM:0461046525

Microsoft Security Response Center <secure@microsoft.com> Tue, May 1, 2018 at 3:33 AM
To: Microsoft Security Response Center <secure@microsoft.com>, Jayateertha Guruprasad <jayateertha043@gmail.com>

Hello Jayateertha,

A fix was confirmed for the issue you presented. Microsoft would like to recognize your efforts on our public security researcher acknowledgement page:
"Security Researcher Acknowledgments for Microsoft Online Services"
<https://technet.microsoft.com/-us/security/cc308589>

If you would like to be acknowledged please provide the following:
Name
If it is an Individual or Company Name
URL to Twitter or online profile

We have resolved the issue you reported, and closed this case.

If you have any questions, or additional information related to this report, please reply on this case thread.

Thank you very much for working with us.

Regards,
Kamuran
MSRC

Link to Bounty Program Terms: https://technet.microsoft.com/en-us/security/dn800983
Link to Privacy Statement: https://technet.microsoft.com/en-us/security/dn425050
Link to Coordinated Vulnerability Disclosure Policy: https://technet.microsoft.com/en-us/security/dn467923.aspx

------------------ Original Message ------------------
From: Jayateertha Guruprasad
[Quoted text hidden]
[Quoted text hidden]

Microsoft swag:

T-SHIRT(with msrc bug bounty programme mentioned as emblem),pen, tote bag,stickers(white hat verified written on them).BADGE