

Mozilla Developer Network XSS Vulnerability

Product: Mozilla Developer Network (MDN)

URL: <https://developer.mozilla.org/>

Vulnerability: Content Sniffing Through Image (XSS attack)

Severity: Medium

Tested: Windows XP SP2 (IE 6 and IE 7)

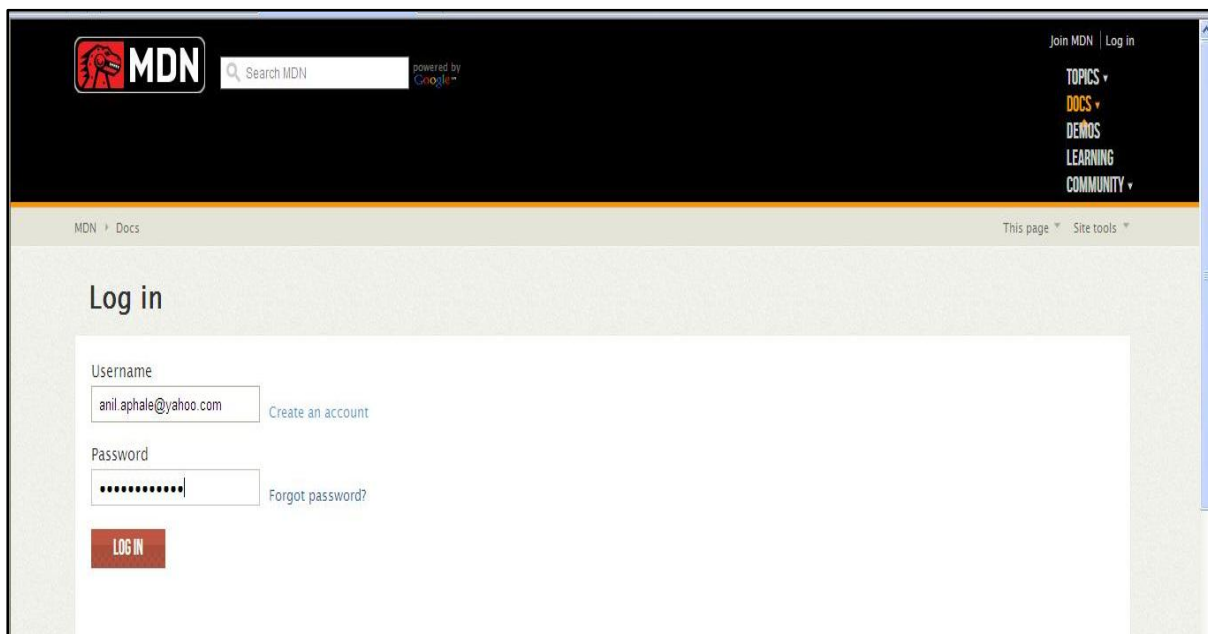
Author: 41.w4r10r (<http://garage4hackers.com/>)

Discription:

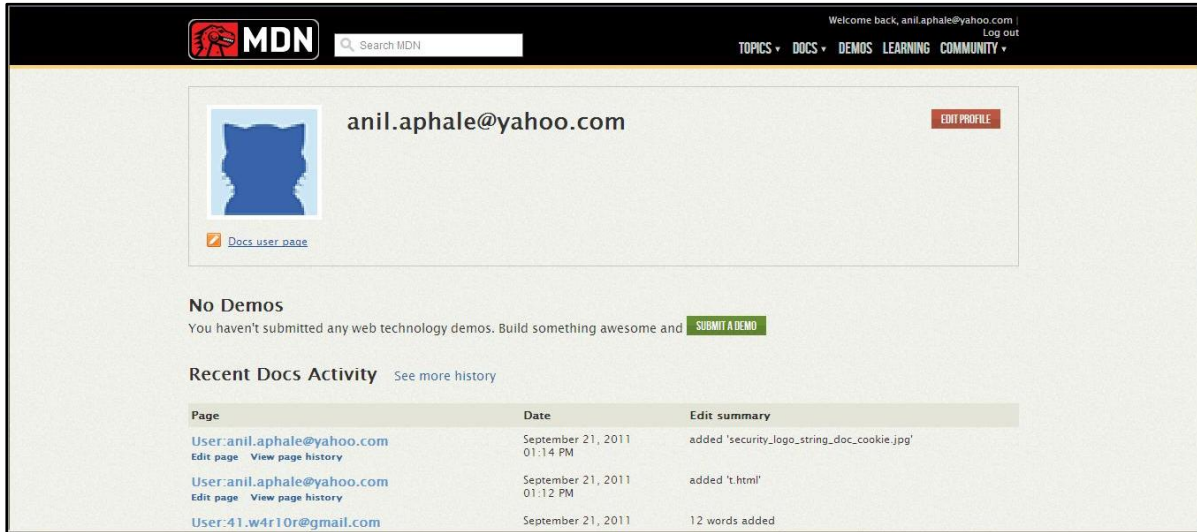
Mozilla Developer Network (MDN) Also known by its project name, "Devmo" (short for "DEVELOper.Mozilla.Org"), this site has been designed to be a comprehensive, usable, accurate, and valuable resource for web developers.

Steps to reproduce vulnerability:

Step1: Login into application



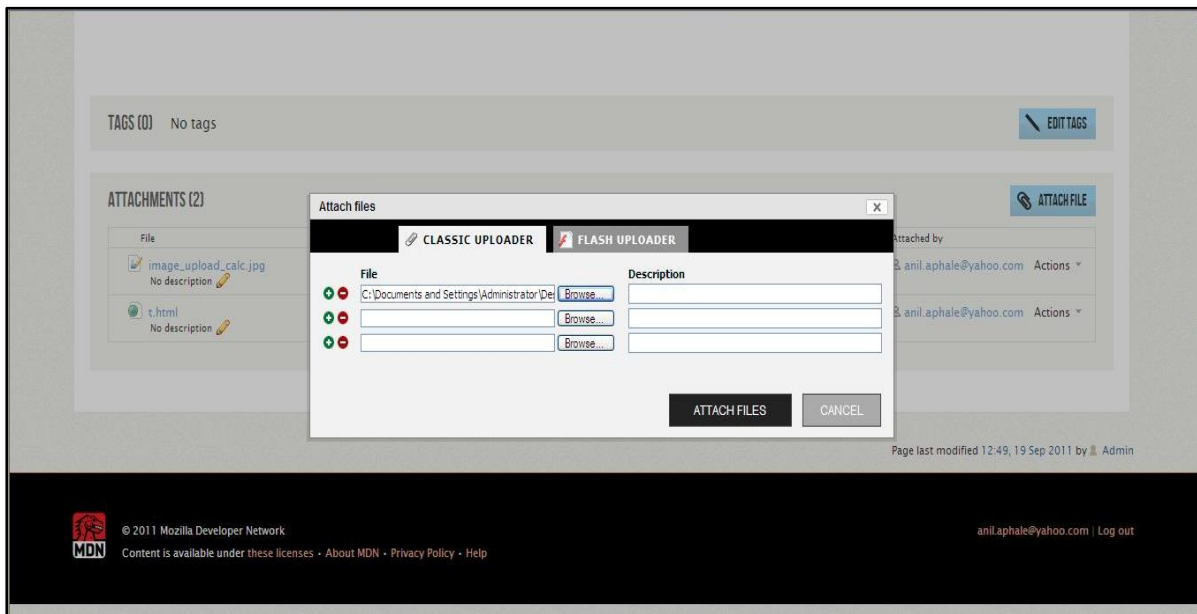
Step2: Click on “Docs User page” (located at below avatar of profile)



The screenshot shows the MDN user profile page for 'anil.aphale@yahoo.com'. At the top, there is a navigation bar with the MDN logo, a search bar, and links for 'TOPICS', 'DOCS', 'DEMOS', 'LEARNING', and 'COMMUNITY'. The user's profile information includes a blue silhouette avatar, the email address 'anil.aphale@yahoo.com', and an 'EDIT PROFILE' button. Below the profile, there is a 'Docs user page' checkbox which is checked. A section titled 'No Demos' indicates that no web technology demos have been submitted, with a 'SUBMIT A DEMO' button. The 'Recent Docs Activity' section shows a table of recent edits:

Page	Date	Edit summary
User:anil.aphale@yahoo.com Edit page View page history	September 21, 2011 01:14 PM	added 'security_logo_string_doc_cookie.jpg'
User:anil.aphale@yahoo.com Edit page View page history	September 21, 2011 01:12 PM	added 't.html'
User:41.w4r10r@gmail.com	September 21, 2011	12 words added

Step3: Click on Attach File and upload the file created for content sniffing (located Below tag button)

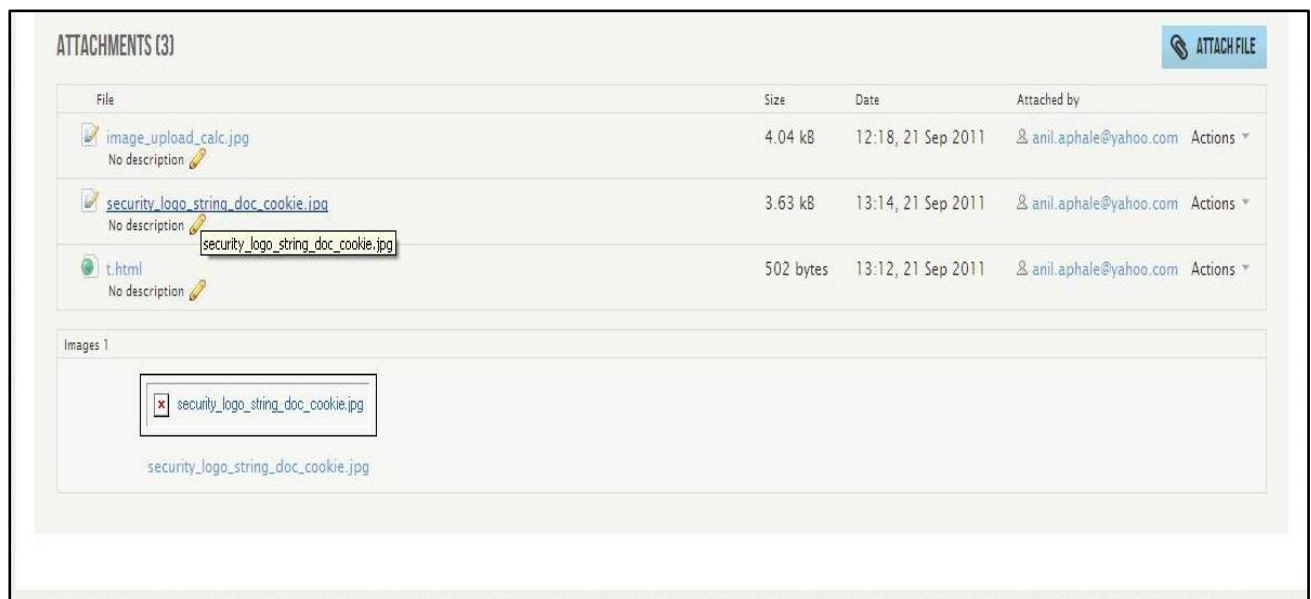


The screenshot shows the MDN page with an 'Attach files' dialog box open. The dialog box has two tabs: 'CLASSIC UPLOADER' and 'FLASH UPLOADER'. It contains a table for adding files:

File	Description
C:\Documents and Settings\Administrator\Del... Browse...	
Browse...	
Browse...	


At the bottom of the dialog are 'ATTACH FILES' and 'CANCEL' buttons. The background page shows a 'TAGS (0) No tags' section and an 'ATTACHMENTS (2)' section with files 'image_upload_calc.jpg' and 't.html'. An 'ATTACH FILE' button is visible in the top right of the page. The footer of the page includes the MDN logo, copyright information for 2011 Mozilla Developer Network, and the user's name 'anil.aphale@yahoo.com' with a 'Log out' link.

Step4: Locate uploaded file and click on it to execute the XSS script

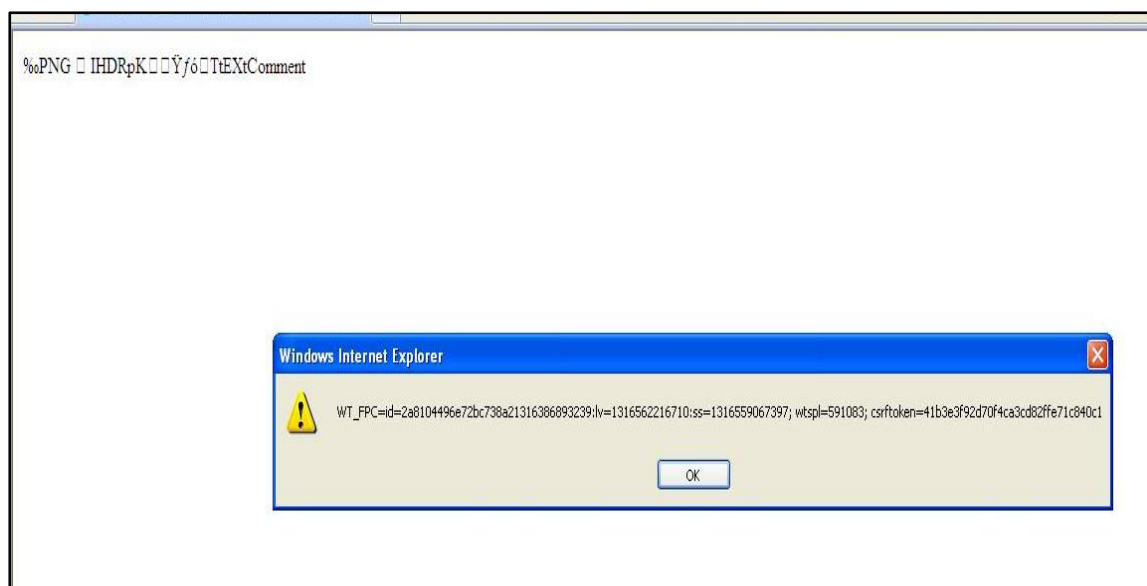


File	Size	Date	Attached by
No description	4.04 kB	12:18, 21 Sep 2011	anil.aphale@yahoo.com
No description	3.63 kB	13:14, 21 Sep 2011	anil.aphale@yahoo.com
No description	502 bytes	13:12, 21 Sep 2011	anil.aphale@yahoo.com

Images 1



Step5: Access the uploaded file (This Execute XSS script available in image file)



Warning from Windows Internet Explorer:

WT_FPC=id=2a8104496e72bc738a21316386893239;lv=1316562216710:ss=1316559067397;wtspl=591083;csrftoken=41b3e3f92d70f4ca3cd82ffe71c840c1

Contact: 41.w4r10r@gmail.com