# Mozilla Developer Network XSS Vulnerability

**Product:** Mozilla Developer Network (MDN)

**URL:** https://developer.mozilla.org/

**Vulnerability:** Content Sniffing Through Image (XSS attack)

**Severity:** Medium

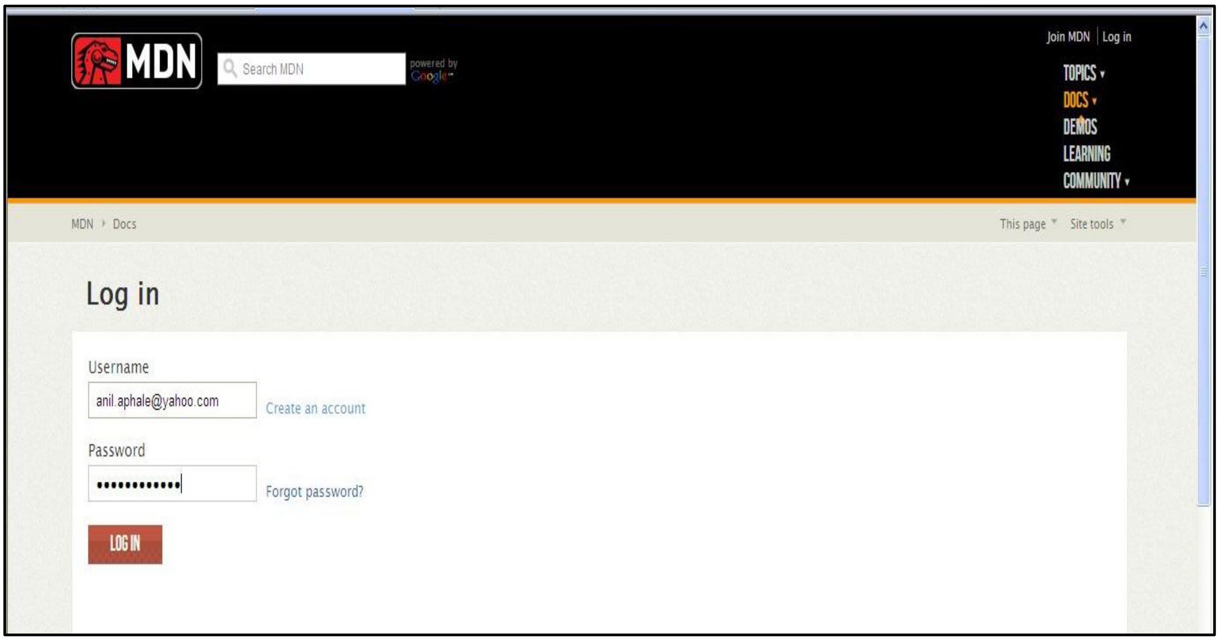
**Tested:** Windows XP SP2 (IE 6 and IE 7)

**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

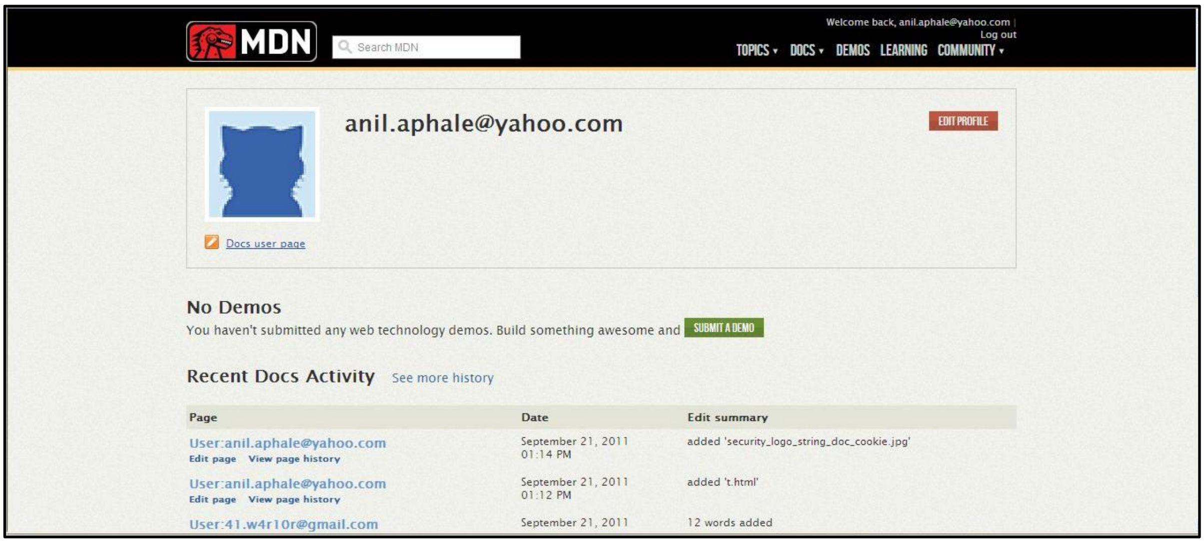


Log in

Username: anil.aphale@yahoo.com

Password: ••••••••••••

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



anil.aphale@yahoo.com

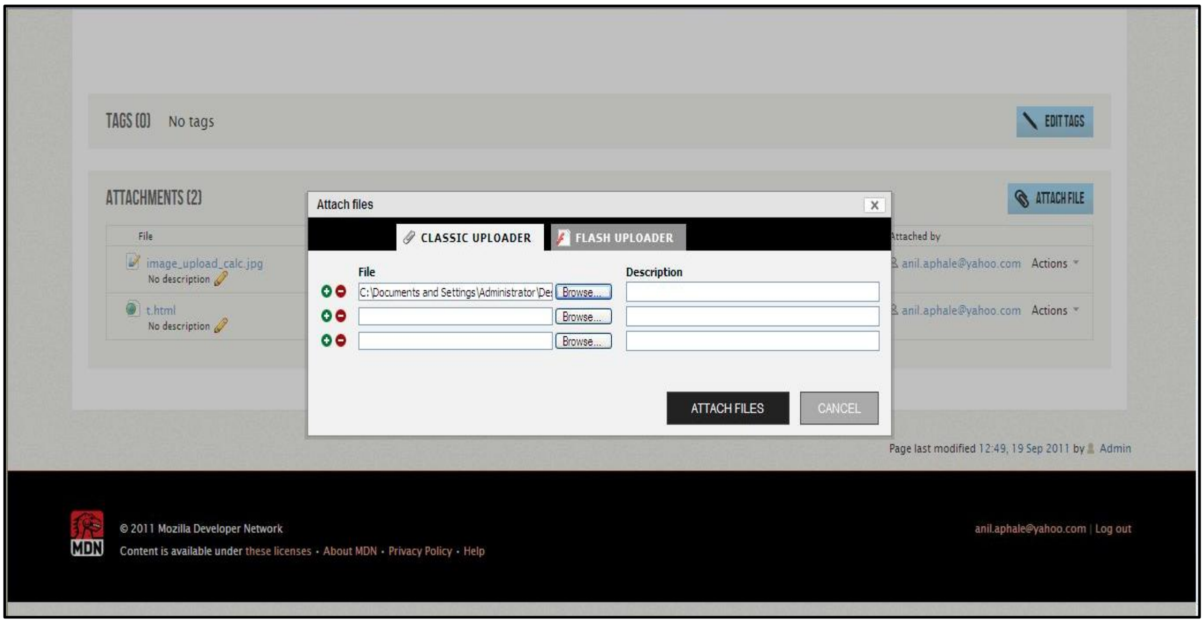
No Demos

You haven't submitted any web technology demos. Build something awesome and

Recent Docs Activity See more history

| Page | Date | Edit summary |
|---|---|---|
| User:anil.aphale@yahoo.com<br>Edit page View page history | September 21, 2011<br>01:14 PM | added 'security_logo_string_doc_cookie.jpg' |
| User:anil.aphale@yahoo.com<br>Edit page View page history | September 21, 2011<br>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)



| File | Attached by |
|---|---|
| image_upload_calc.jpg<br>No description | anil.aphale@yahoo.com |
| t.html<br>No description | anil.aphale@yahoo.com |

| File | Description |
|---|---|
| C:\Documents and Settings\Administrator\De |  |
|  |  |
|  |  |

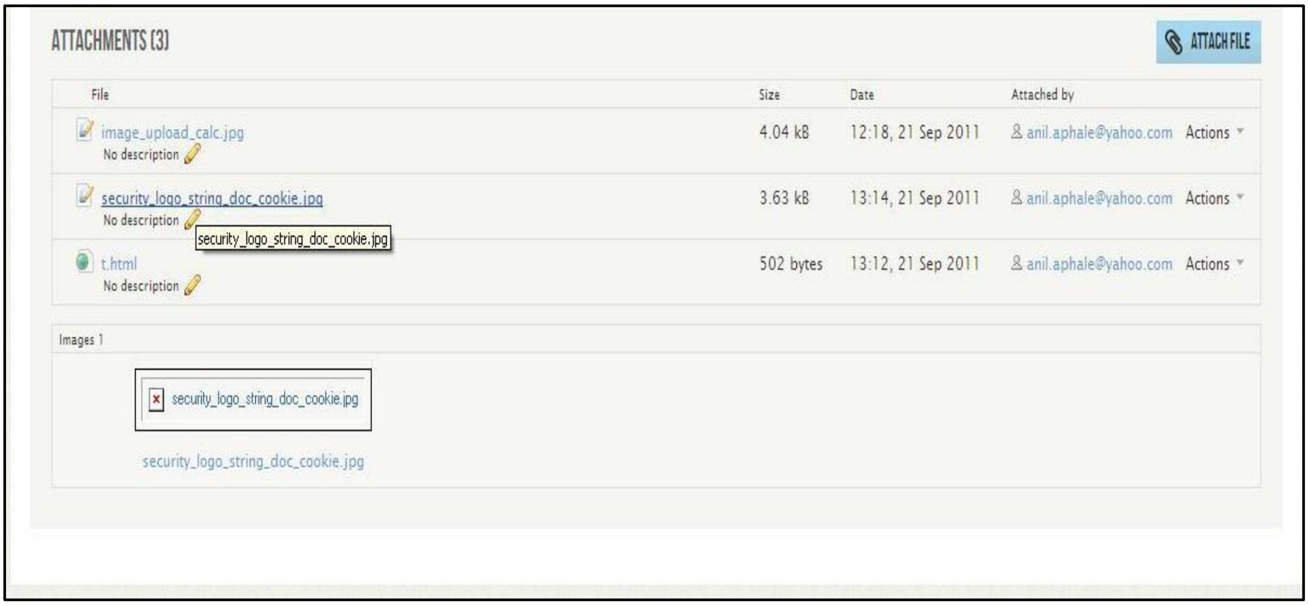
Page last modified 12:49, 19 Sep 2011 by Admin

© 2011 Mozilla Developer Network

Content is available under these licenses • About MDN • Privacy Policy • Help

anil.aphale@yahoo.com | Log out

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



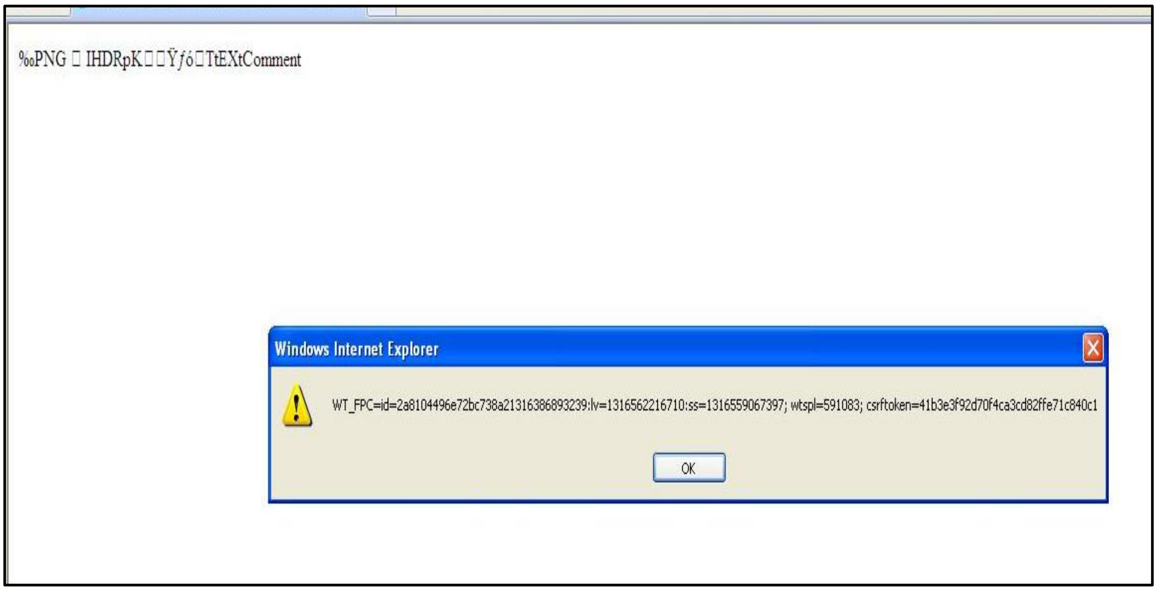
ATTACHMENTS (3)

| File | Size | Date | Attached by | |
|---|---|---|---|---|
| image_upload_calc.jpg<br>No description | 4.04 kB | 12:18, 21 Sep 2011 | anil.aphale@yahoo.com | Actions |
| security_logo_string_doc_cookie.jpg<br>No description | 3.63 kB | 13:14, 21 Sep 2011 | anil.aphale@yahoo.com | Actions |
| t.html<br>No description | 502 bytes | 13:12, 21 Sep 2011 | anil.aphale@yahoo.com | Actions |

Images 1

security_logo_string_doc_cookie.jpg

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



```
‰PNG  IHDRpK  Ÿƒó TtEXtComment
```

Windows Internet Explorer

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

**Contact:** 41.w4r10r@gmail.com