

# Bugzilla XSS Vulnerability

**Product:** Bugzilla

**URL:** <https://bugzilla.mozilla.org/>

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

**Severity:** Medium

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

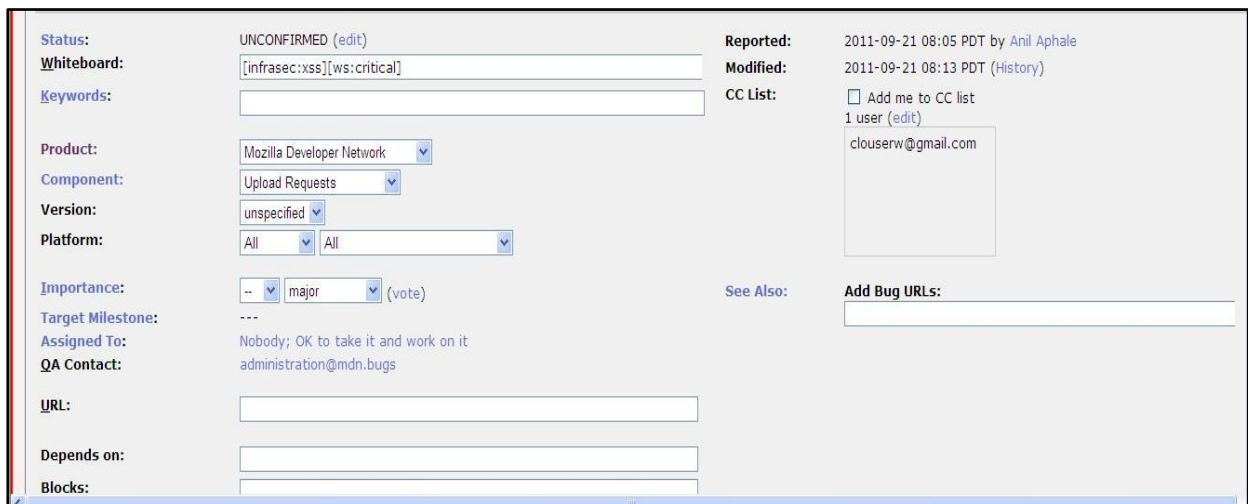
**Author:** 41.w4r10r (<http://garage4hackers.com/>)

## Discription:

**Bugzilla** is site provided by Mozilla to file a bug this contains Content Sniffing (XSS) vulnerability.

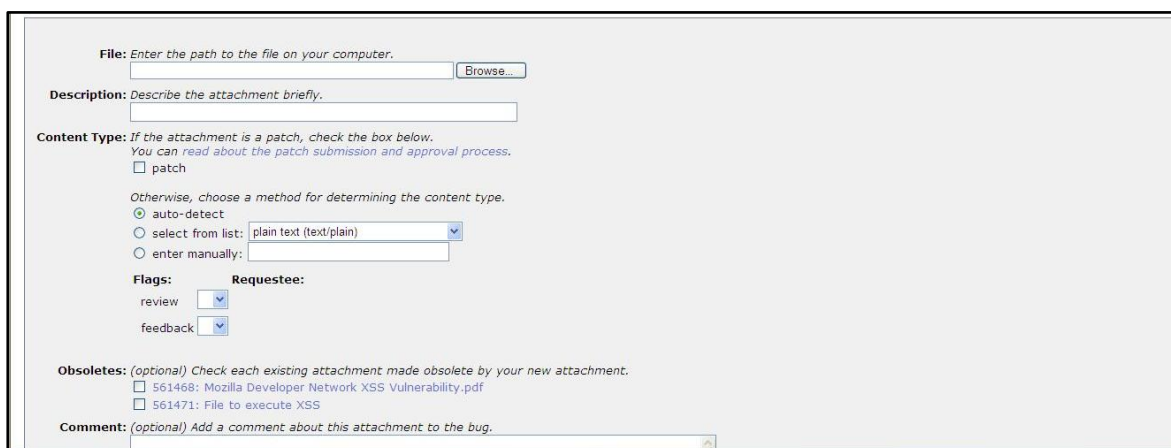
## Steps to reproduce vulnerability:

**Step1:** Login into application



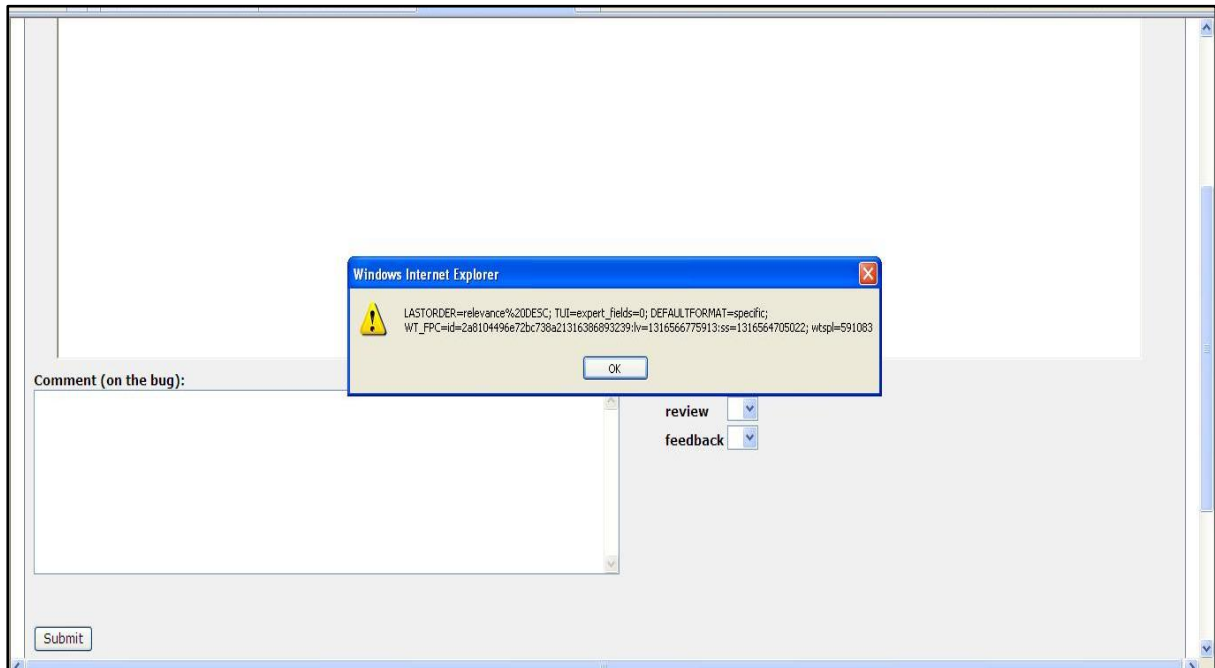
The screenshot shows a Bugzilla bug report page. The status is 'UNCONFIRMED (edit)'. The whiteboard contains '[infrasec:xss][ws:critical]'. The product is 'Mozilla Developer Network', component is 'Upload Requests', and version is 'unspecified'. The importance is set to 'major'. The assigned to is 'Nobody; OK to take it and work on it' and the QA contact is 'administration@mdn.bugs'. The reported date is '2011-09-21 08:05 PDT' by 'Anil Aphale'. The modified date is '2011-09-21 08:13 PDT'. The CC list includes 'clouserw@gmail.com'. There are fields for 'URL:', 'Depends on:', and 'Blocks:'.

**Step2:** Click on attach test cases and attach the image created for content sniffing



The screenshot shows the attachment upload form in Bugzilla. It includes a 'File' field with a 'Browse...' button. The 'Description' field is for a brief description of the attachment. The 'Content Type' section has options for 'patch', 'auto-detect', 'select from list' (with 'plain text (text/plain)' selected), and 'enter manually'. There are 'Flags' and 'Requestee' dropdown menus. The 'Obsoletes' section has checkboxes for existing attachments. The 'Comment' field is for an optional comment about the attachment to the bug.

**Step3:** Click on Attached File or Details available in front of attached file.



Contact: [41.w4r10r@gmail.com](mailto:41.w4r10r@gmail.com)