Bugzilla XSS Vulnerability

Product: Bugzilla

URL: https://bugzilla.mozilla.org/

Vulnerability: Content Sniffing Through any file type (XSS attack)

Severity: Medium

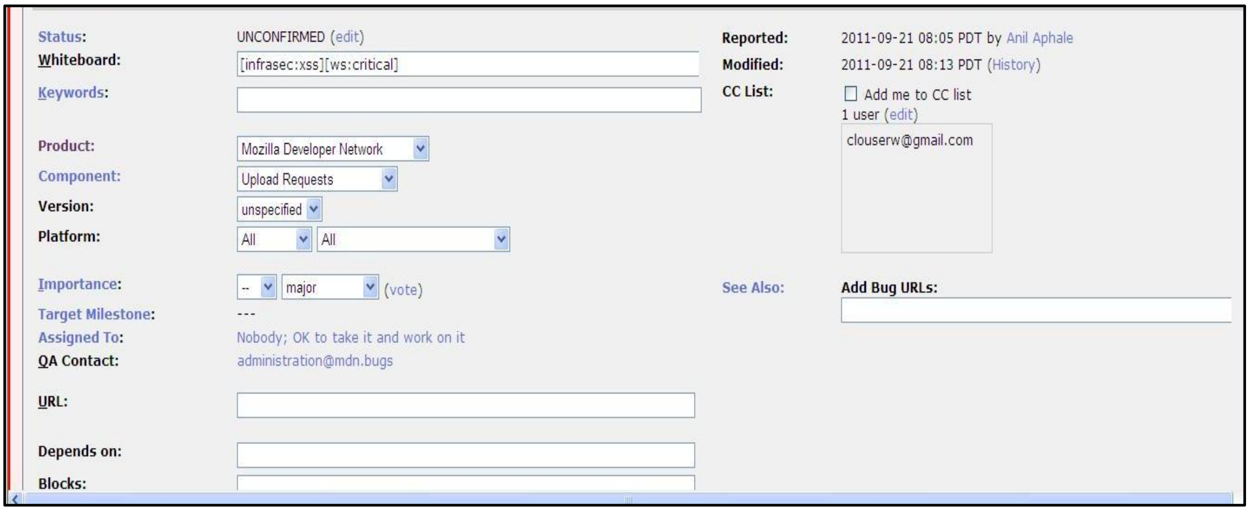
Tested: Windows7 (IE 9 and FireFoz 6.2)

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:

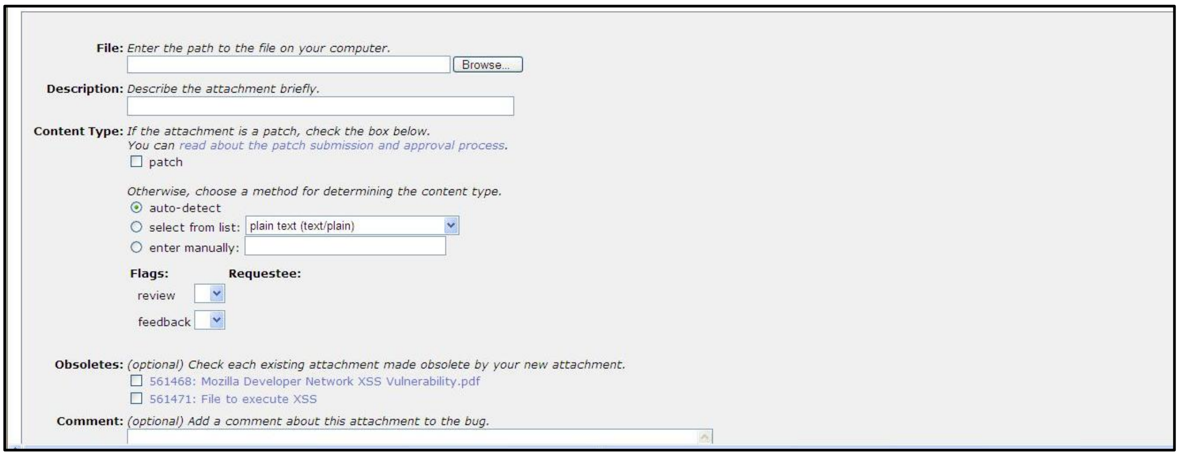
Step1: Login into application Create new bug



Status: UNCONFIRMED (edit)
Whiteboard: [infrasec:xss][ws:critical]
Keywords:
Product: Mozilla Developer Network
Component: Upload Requests
Version: unspecified
Platform: All All
Importance: -- major (vote)
Target Milestone: ---
Assigned To: Nobody; OK to take it and work on it
QA Contact: administration@mdn.bugs
URL:
Depends on:
Blocks:

Reported: 2011-09-21 08:05 PDT by Anil Aphale
Modified: 2011-09-21 08:13 PDT (History)
CC List: □ Add me to CC list
1 user (edit)
clouserw@gmail.com
See Also: Add Bug URLs:

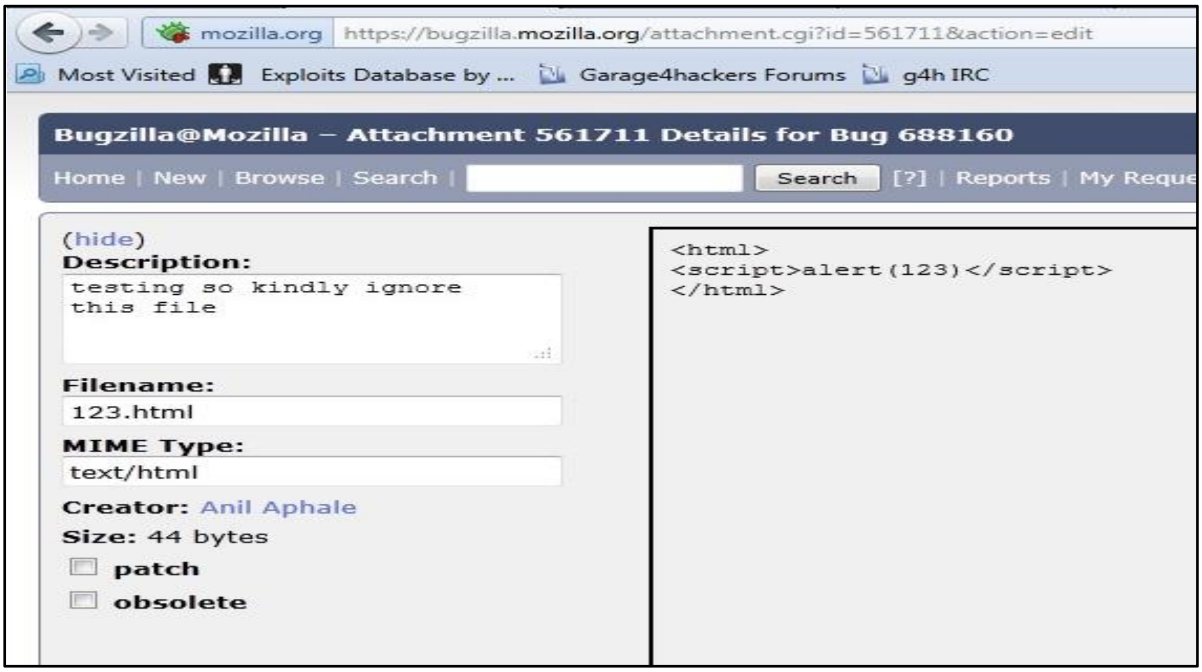
Step2: Click on attach test cases and attach the image created for content sniffing



File: Enter the path to the file on your computer.

Description: Describe the attachment briefly.
Content Type: If the attachment is a patch, check the box below.
You can read about the patch submission and approval process.
□ patch
Otherwise, choose a method for determining the content type.
● auto-detect
○ select from list: plain text (text/plain)
○ enter manually:
Flags: Requestee:
review
feedback
Obsoletes: (optional) Check each existing attachment made obsolete by your new attachment.
□ 561468: Mozilla Developer Network XSS Vulnerability.pdf
□ 561471: File to execute XSS
Comment: (optional) Add a comment about this attachment to the bug.

Step3: Click on Attached and click on Edit Details and and change the content type to text/html and submit



Bugzilla@Mozilla – Attachment 561711 Details for Bug 688160

(hide)

Description: testing so kindly ignore this file

Filename: 123.html

MIME Type: text/html

Creator: Anil Aphale

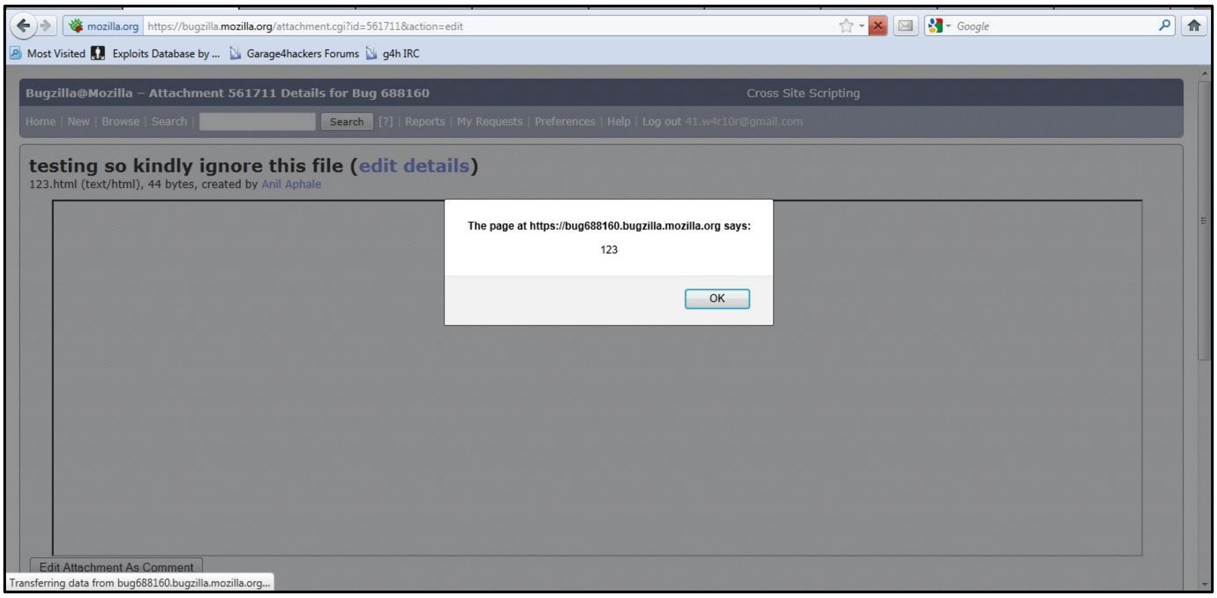
Size: 44 bytes

□ patch

□ obsolete

```
<html>
<script>alert(123)</script>
</html>
```

Step4: Click on attachment file to execute javascript



mozilla.org
https://bugzilla.mozilla.org/attachment.cgi?id=561711&action=edit
Google
Most Visited
Exploits Database by ...
Garage4hackers Forums
g4h IRC

Bugzilla@Mozilla – Attachment 561711 Details for Bug 688160 Cross Site Scripting

Home | New | Browse | Search |
Search
[?] | Reports | My Requests | Preferences | Help | Log out 41.w4r10r@gmail.com

testing so kindly ignore this file (edit details)

123.html (text/html), 44 bytes, created by Anil Aphale

The page at https://bug688160.bugzilla.mozilla.org says:

123

OK
Edit Attachment As Comment

Transferring data from bug688160.bugzilla.mozilla.org...

Contact: 41.w4r10r@gmail.com