XSS Vulnerability in PDF Download

January 11th 2007

Douglas Noakes

Younus Rashid

Table Of Contents

PDF XSS Vulnerability

- It is really a cross site scripting vulnerability based on PDF
- http://domain/pdf_file.pdf#anyname=javascript:your_code_here
- Any JavaScript code is executed when the PDF is loaded in the browser
- It is not really a vulnerability with the application but rather an issue with Abode Reader and how certain browser open PDF files
- No write access to the file is required
- According to Google, 317,000,000 sites have this vulnerability
- URL obfuscation (i.e., TinyURL) makes the issue worse

Impact

- Session Hi-Jacking
- Stealing User Credentials
- Cross Site Request Forgery (AJAX Sites)
- Phishing
- Backdoor Access (Trojan)
- Left to the Imagination (scripting)
- Additional Information: http://www.gnucitizen.org/blog/universal-pdf-xss-after-party/

Demo

Are you vulnerable?

Server Side Fixes

- Create a filter
  - OWASP has J2EE filter for J2EE application
- Change Content-disposition
  - Apache

    Add these lines to the httpd.conf file inside the <Directory> tags.

```
AddType application/octet .pdf
<Files *.pdf>
      Header add Content-Disposition "Attachment"
</Files>
```

Server Side Fixes (Continued..)

- IIS

1. Change MIME type to "application/octet":
2. Start > Run > Enter compmgmt.msc. The Computer Management console appears.
3. Right click on the Services and Applications > Internet Information Services (IIS Manager)
4. Select Properties > MIME Types
5. Scroll down to ".pdf". The MIME type should be "application/pdf" which should be changed to "application/octet".
6. Hit OK twice.

7. Add Content-Disposition header (this must be done by directory or for each PDF file individually):
8. In the IIS Management tool (not in Windows Explorer), select a directory with PDF content or an individual PDF file.
9. Right-click on the directory or file.
10. Select Properties.
11. Click the HTTP Headers tab.
12. In the Custom HTTP Headers section, click Add.
13. A dialog appears. In the "Custom-header name" field enter "Content-disposition". In the "Custom-header value field, enter "Attachment".
14. Click OK twice.
15. Restart IIS (command line: iisreset).
16. Check that PDF content from the browser now prompts the user to "download" rather than simply opening the content.

Client Side Fixes

- Disable Java Script
- Upgrade to Adobe Acrobat Reader 8.0
- Upgrade to a Browser that is not susceptible (e.g. IE 6 SP2, IE 7)

Discussion

- Questions related to XSS?
- What is your client response to Best Practice/Academic findings?
  - Are academic findings generally fixed?
  - How do you convince your client to implement academic findings?
- What is the best approach for mitigation?
- When do you decide usability is more important then security or vice versa?