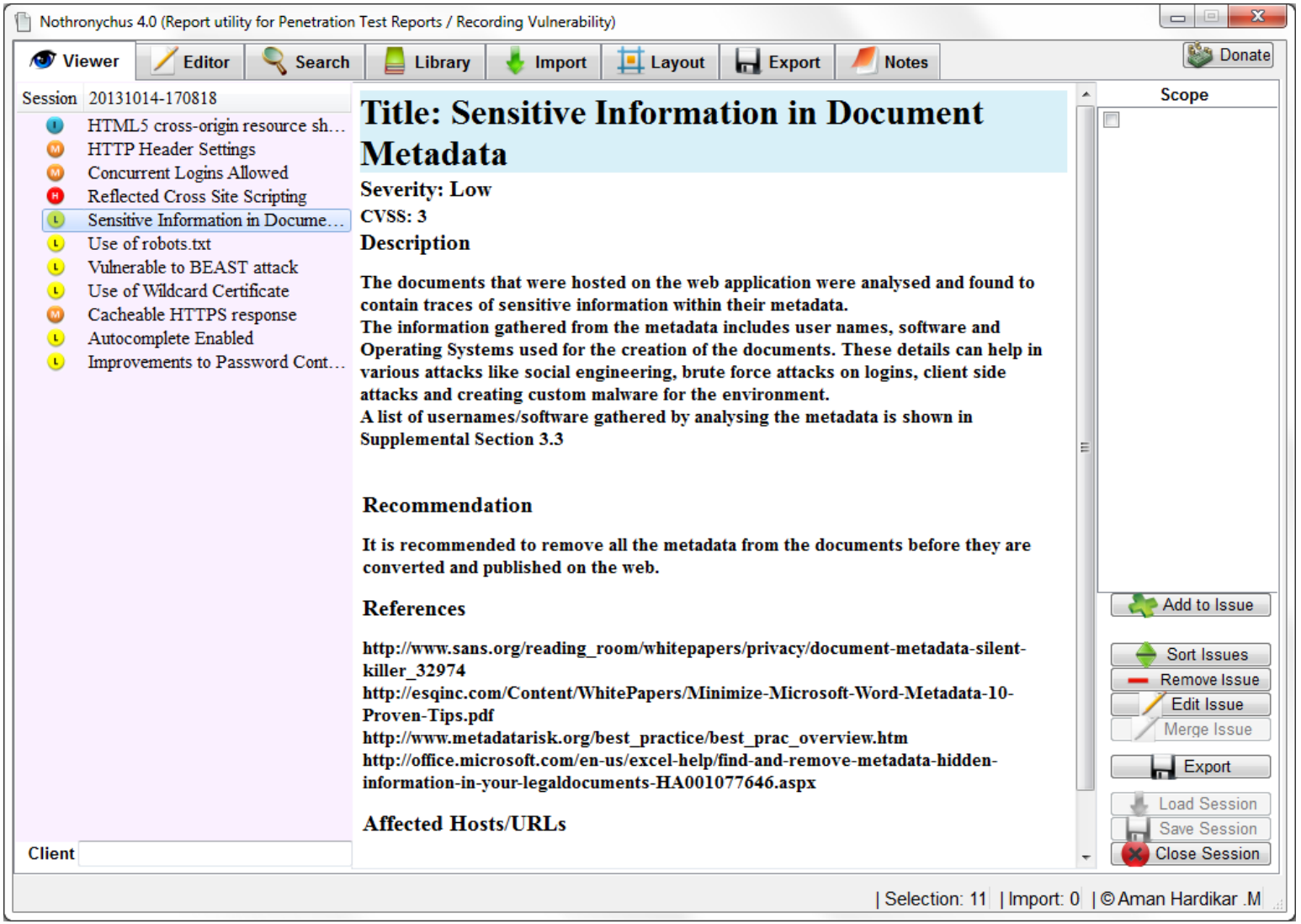
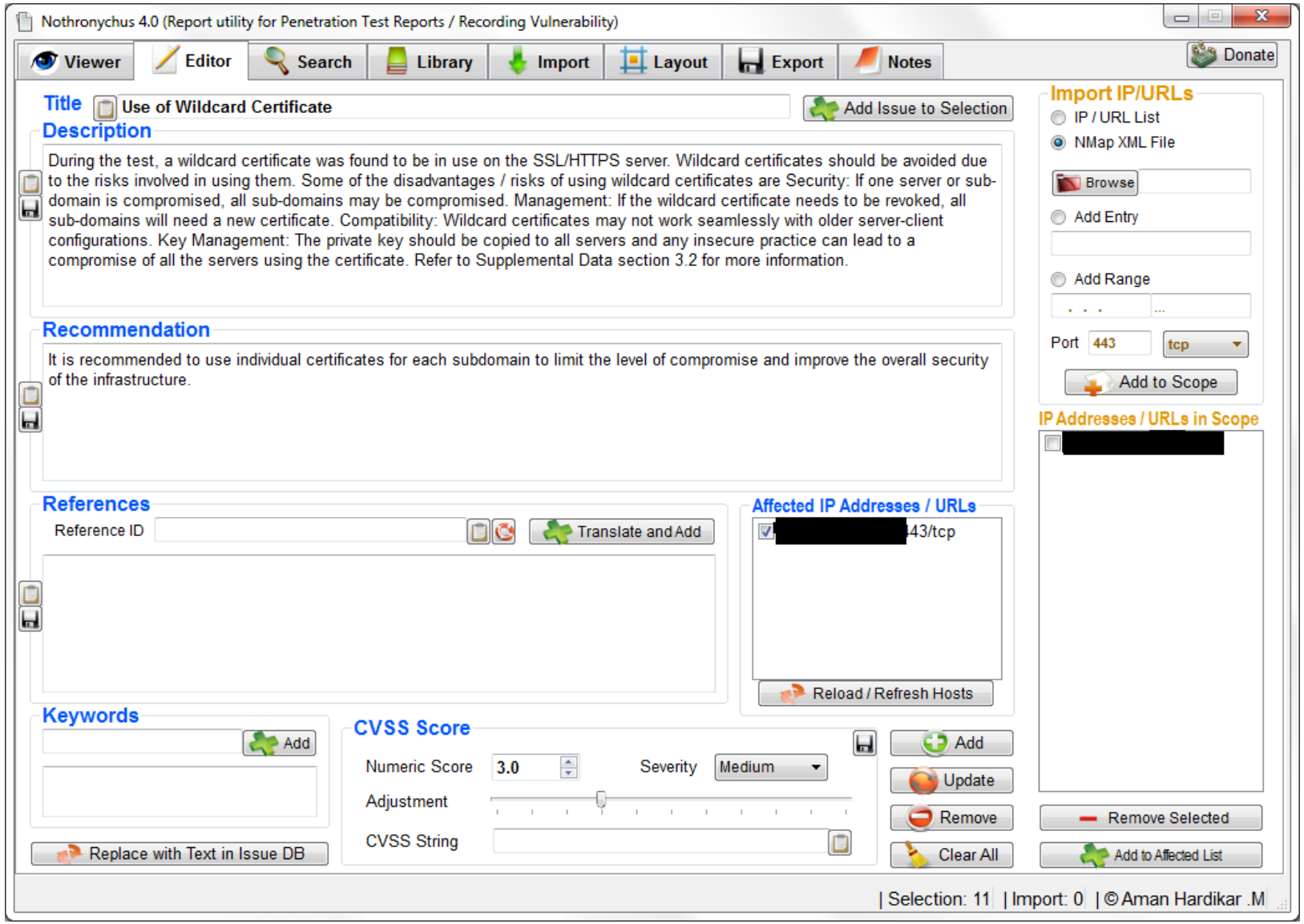
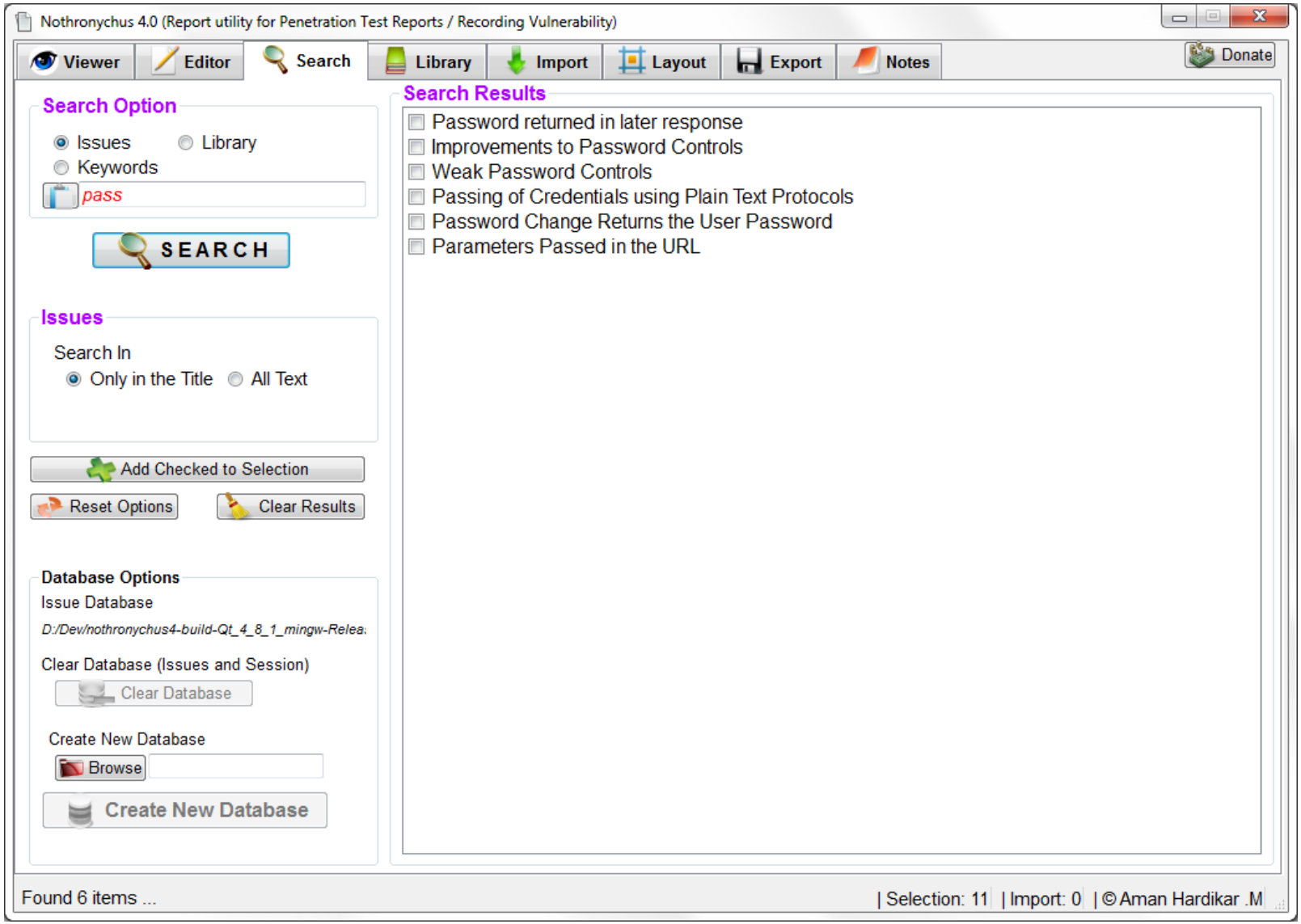
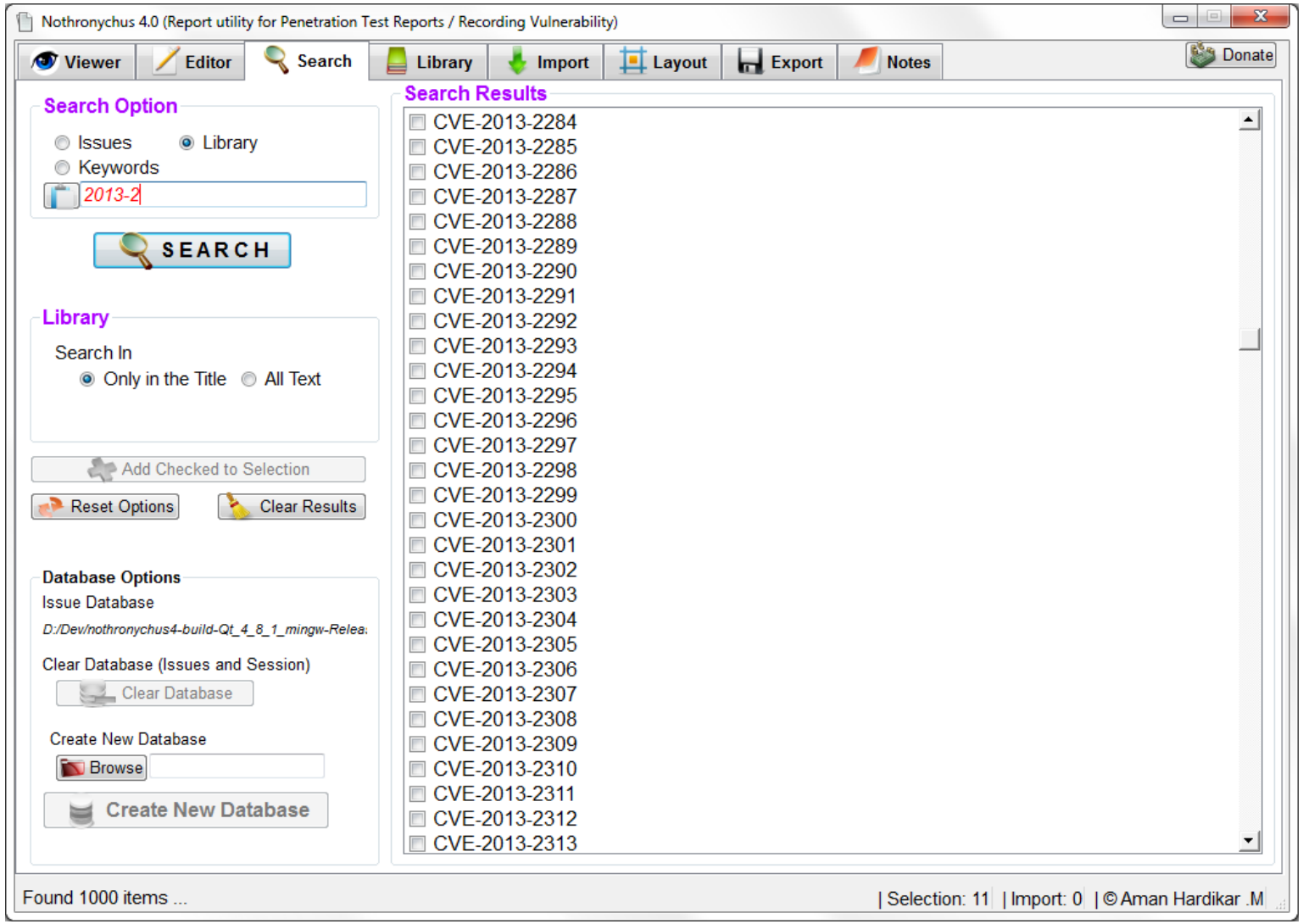
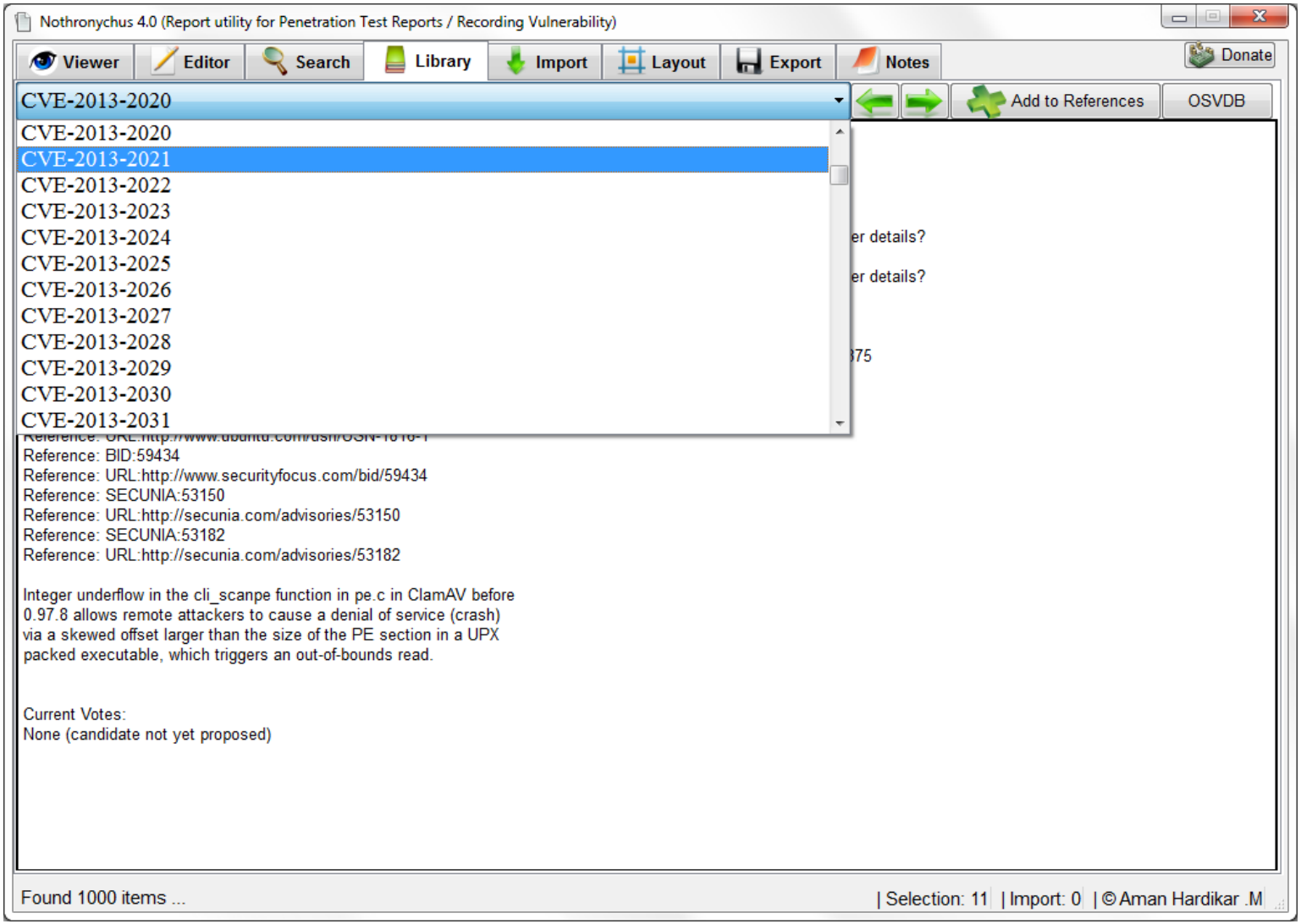
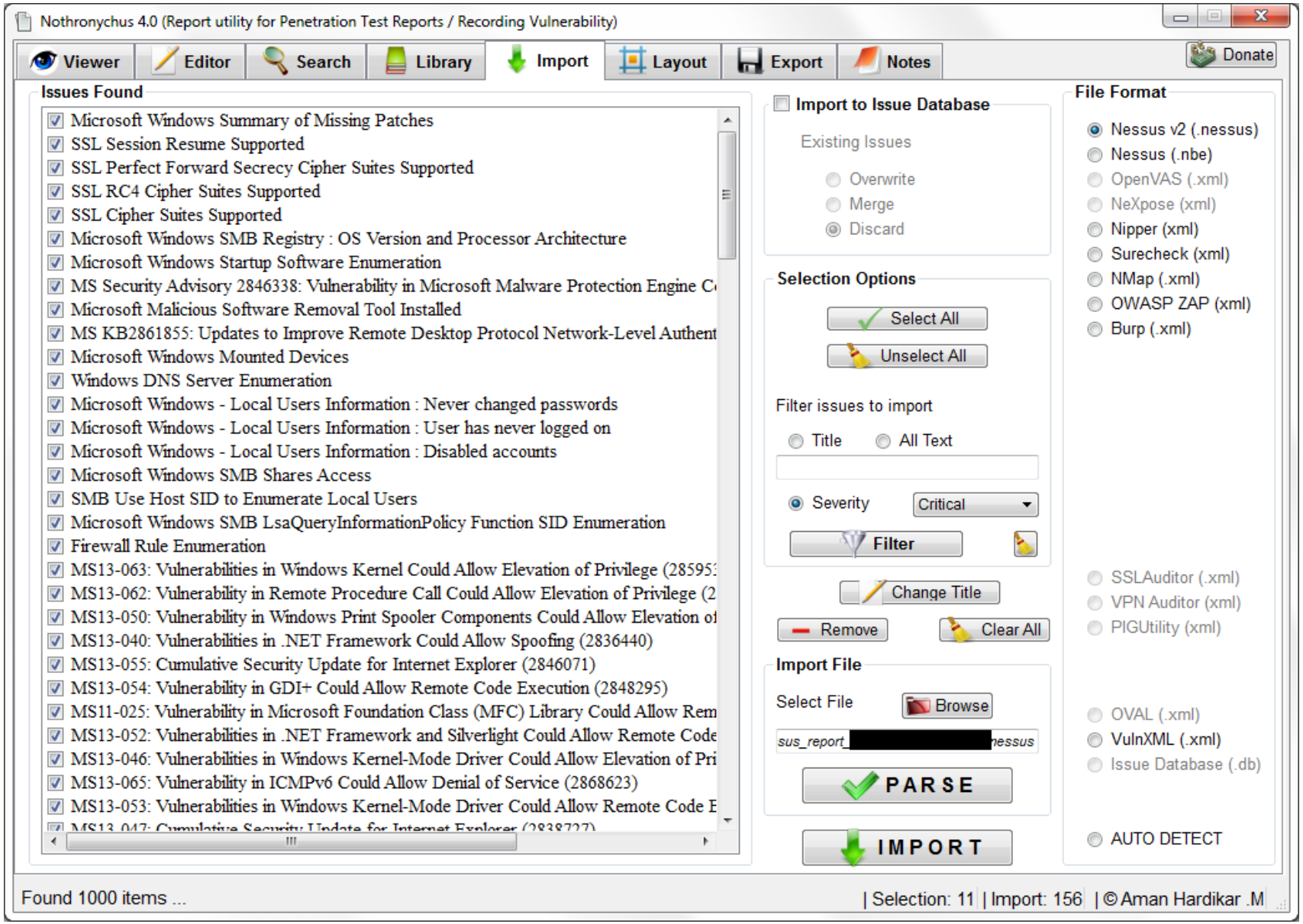

Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Session 20131014-170818
HTML5 cross-origin resource sh…
HTTP Header Settings
Concurrent Logins Allowed
Reflected Cross Site Scripting
Sensitive Information in Docume…
Use of robots.txt
Vulnerable to BEAST attack
Use of Wildcard Certificate
Cacheable HTTPS response
Autocomplete Enabled
Improvements to Password Cont…
Client
Title: Sensitive Information in Document Metadata
Severity: Low
CVSS: 3
Description
The documents that were hosted on the web application were analysed and found to contain traces of sensitive information within their metadata.
The information gathered from the metadata includes user names, software and Operating Systems used for the creation of the documents. These details can help in various attacks like social engineering, brute force attacks on logins, client side attacks and creating custom malware for the environment.
A list of usernames/software gathered by analysing the metadata is shown in Supplemental Section 3.3
Recommendation
It is recommended to remove all the metadata from the documents before they are converted and published on the web.
References
http://www.sans.org/reading_room/whitepapers/privacy/document-metadata-silent-killer_32974
http://esqinc.com/Content/WhitePapers/Minimize-Microsoft-Word-Metadata-10-Proven-Tips.pdf
http://www.metadatarisk.org/best_practice/best_prac_overview.htm
http://office.microsoft.com/en-us/excel-help/find-and-remove-metadata-hidden-information-in-your-legaldocuments-HA001077646.aspx
Affected Hosts/URLs
Scope
Add to Issue
Sort Issues
Remove Issue
Edit Issue
Merge Issue
Export
Load Session
Save Session
Close Session
| Selection: 11 | Import: 0 | © Aman Hardikar .M

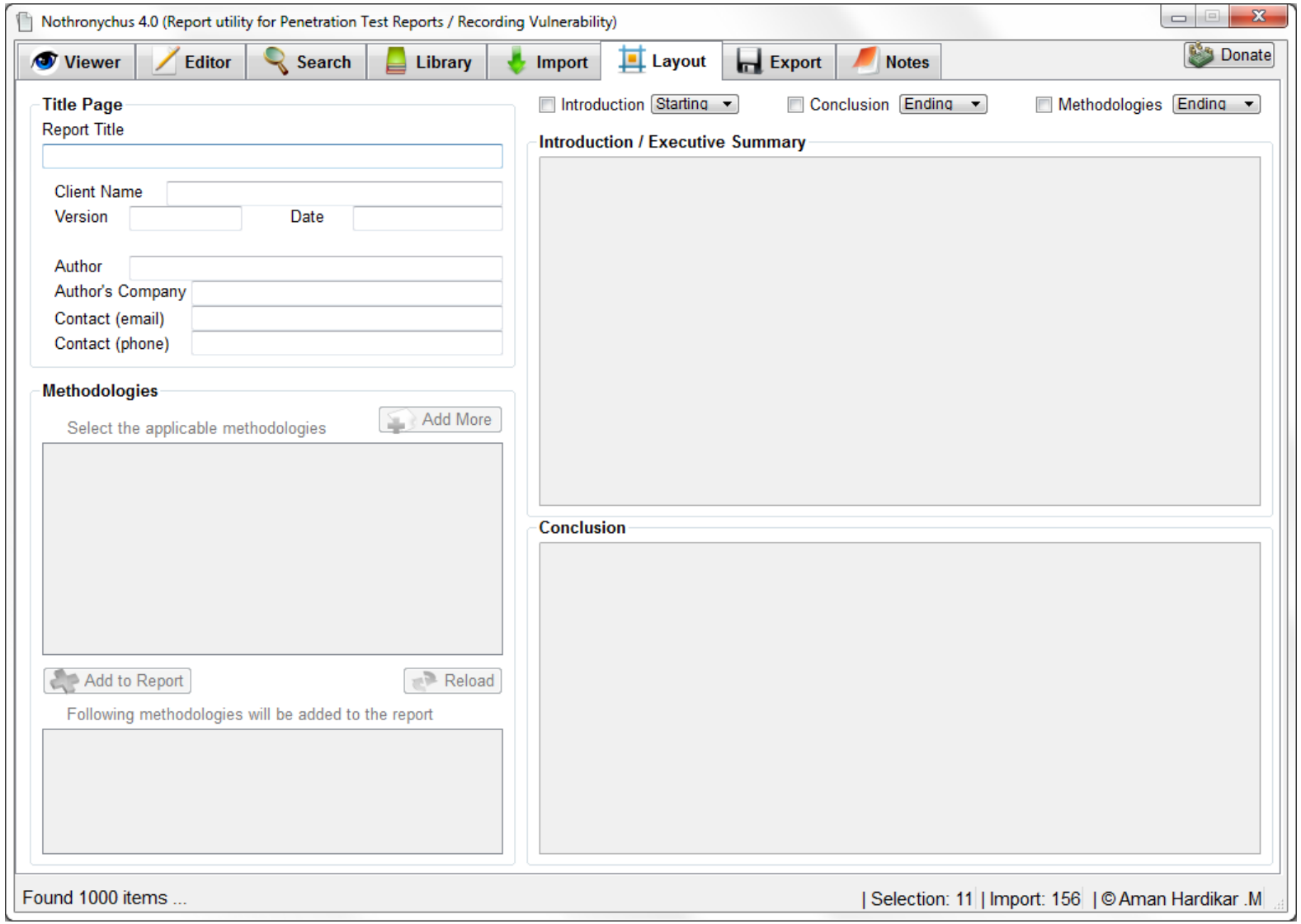

Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Title
Use of Wildcard Certificate
Add Issue to Selection
Description
During the test, a wildcard certificate was found to be in use on the SSL/HTTPS server. Wildcard certificates should be avoided due to the risks involved in using them. Some of the disadvantages / risks of using wildcard certificates are Security: If one server or sub-domain is compromised, all sub-domains may be compromised. Management: If the wildcard certificate needs to be revoked, all sub-domains will need a new certificate. Compatibility: Wildcard certificates may not work seamlessly with older server-client configurations. Key Management: The private key should be copied to all servers and any insecure practice can lead to a compromise of all the servers using the certificate. Refer to Supplemental Data section 3.2 for more information.
Recommendation
It is recommended to use individual certificates for each subdomain to limit the level of compromise and improve the overall security of the infrastructure.
References
Reference ID
Translate and Add
Affected IP Addresses / URLs
[redacted]43/tcp
Reload / Refresh Hosts
Keywords
Add
Replace with Text in Issue DB
CVSS Score
Numeric Score
3.0
Severity
Medium
Adjustment
CVSS String
Add
Update
Remove
Clear All
Import IP/URLs
IP / URL List
NMap XML File
Browse
Add Entry
Add Range
Port
443
tcp
Add to Scope
IP Addresses / URLs in Scope
[redacted]
Remove Selected
Add to Affected List
| Selection: 11 | Import: 0 | © Aman Hardikar .M

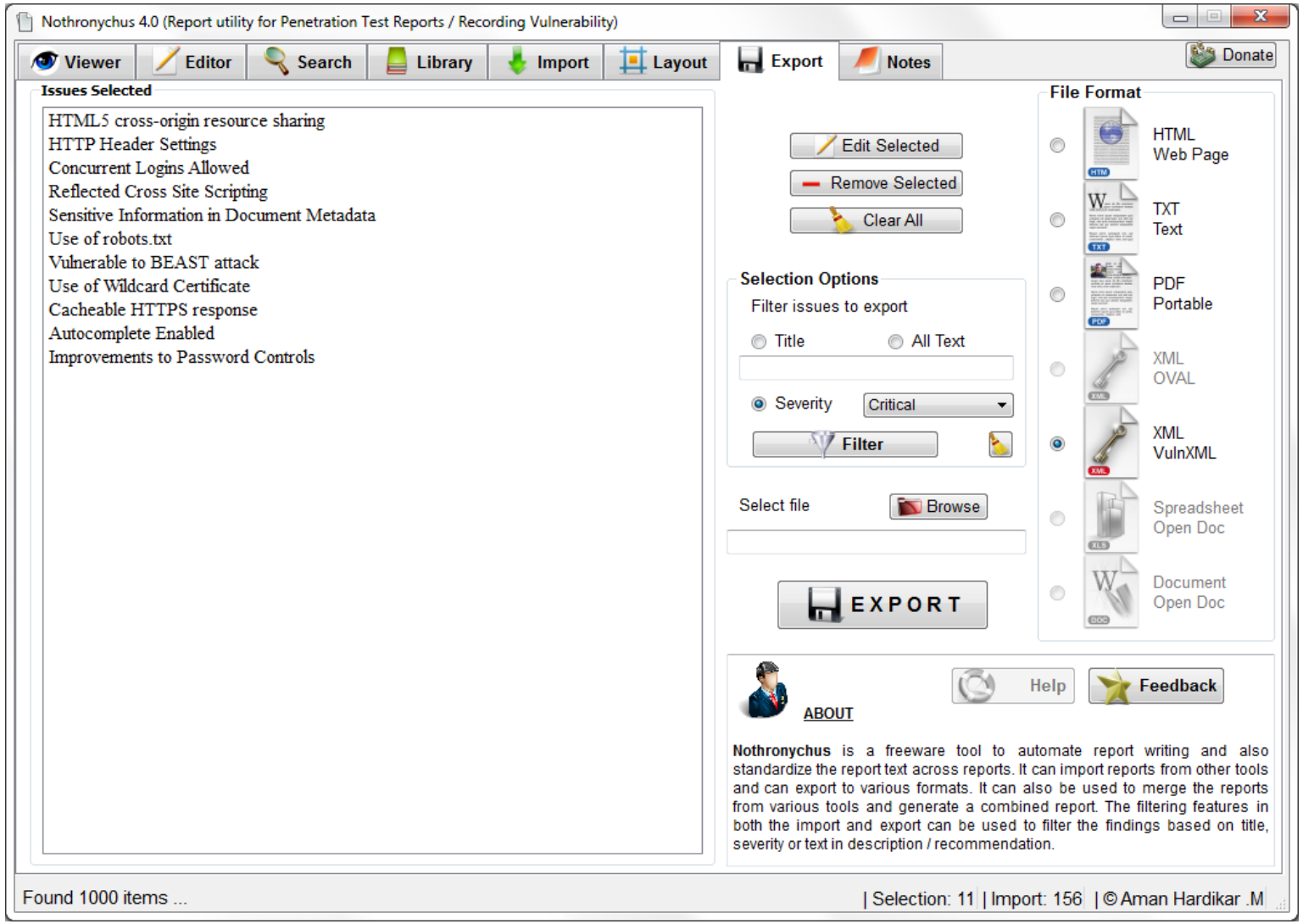

Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Search Option
Issues
Library
Keywords
pass
SEARCH
Issues
Search In
Only in the Title
All Text
Add Checked to Selection
Reset Options
Clear Results
Database Options
Issue Database
D:/Dev/nothronychus4-build-Qt_4_8_1_mingw-Relea
Clear Database (Issues and Session)
Clear Database
Create New Database
Browse
Create New Database
Search Results
Password returned in later response
Improvements to Password Controls
Weak Password Controls
Passing of Credentials using Plain Text Protocols
Password Change Returns the User Password
Parameters Passed in the URL
Found 6 items ...
| Selection: 11 | Import: 0 | © Aman Hardikar .M

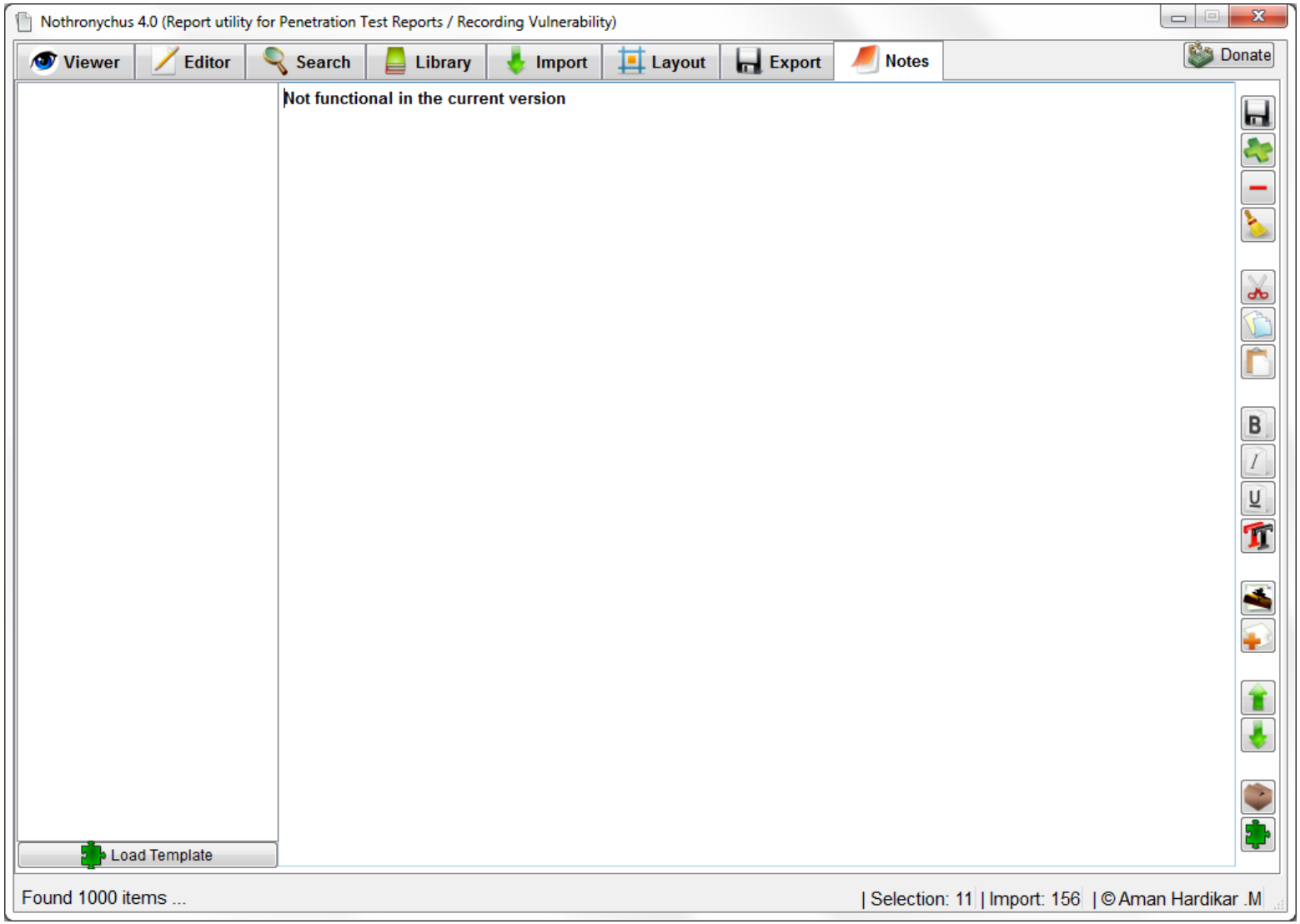

Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Search Option
Issues
Library
Keywords
2013-2
SEARCH
Library
Search In
Only in the Title
All Text
Add Checked to Selection
Reset Options
Clear Results
Database Options
Issue Database
D:/Dev/nothronychus4-build-Qt_4_8_1_mingw-Relea
Clear Database (Issues and Session)
Clear Database
Create New Database
Browse
Create New Database
Search Results
CVE-2013-2284
CVE-2013-2285
CVE-2013-2286
CVE-2013-2287
CVE-2013-2288
CVE-2013-2289
CVE-2013-2290
CVE-2013-2291
CVE-2013-2292
CVE-2013-2293
CVE-2013-2294
CVE-2013-2295
CVE-2013-2296
CVE-2013-2297
CVE-2013-2298
CVE-2013-2299
CVE-2013-2300
CVE-2013-2301
CVE-2013-2302
CVE-2013-2303
CVE-2013-2304
CVE-2013-2305
CVE-2013-2306
CVE-2013-2307
CVE-2013-2308
CVE-2013-2309
CVE-2013-2310
CVE-2013-2311
CVE-2013-2312
CVE-2013-2313
Found 1000 items ...
| Selection: 11 | Import: 0 | © Aman Hardikar .M


Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
CVE-2013-2020
CVE-2013-2020
CVE-2013-2021
CVE-2013-2022
CVE-2013-2023
CVE-2013-2024
CVE-2013-2025
CVE-2013-2026
CVE-2013-2027
CVE-2013-2028
CVE-2013-2029
CVE-2013-2030
CVE-2013-2031
Add to References
OSVDB
er details?
er details?
375
Reference: BID:59434
Reference: URL:http://www.securityfocus.com/bid/59434
Reference: SECUNIA:53150
Reference: URL:http://secunia.com/advisories/53150
Reference: SECUNIA:53182
Reference: URL:http://secunia.com/advisories/53182
Integer underflow in the cli_scanpe function in pe.c in ClamAV before
0.97.8 allows remote attackers to cause a denial of service (crash)
via a skewed offset larger than the size of the PE section in a UPX
packed executable, which triggers an out-of-bounds read.
Current Votes:
None (candidate not yet proposed)
Found 1000 items ...
| Selection: 11 | Import: 0 | © Aman Hardikar .M


Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Issues Found
Microsoft Windows Summary of Missing Patches
SSL Session Resume Supported
SSL Perfect Forward Secrecy Cipher Suites Supported
SSL RC4 Cipher Suites Supported
SSL Cipher Suites Supported
Microsoft Windows SMB Registry : OS Version and Processor Architecture
Microsoft Windows Startup Software Enumeration
MS Security Advisory 2846338: Vulnerability in Microsoft Malware Protection Engine C
Microsoft Malicious Software Removal Tool Installed
MS KB2861855: Updates to Improve Remote Desktop Protocol Network-Level Authent
Microsoft Windows Mounted Devices
Windows DNS Server Enumeration
Microsoft Windows - Local Users Information : Never changed passwords
Microsoft Windows - Local Users Information : User has never logged on
Microsoft Windows - Local Users Information : Disabled accounts
Microsoft Windows SMB Shares Access
SMB Use Host SID to Enumerate Local Users
Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Firewall Rule Enumeration
MS13-063: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (28595
MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2
MS13-050: Vulnerability in Windows Print Spooler Components Could Allow Elevation of
MS13-040: Vulnerabilities in .NET Framework Could Allow Spoofing (2836440)
MS13-055: Cumulative Security Update for Internet Explorer (2846071)
MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)
MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Rem
MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code
MS13-046: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Pri
MS13-065: Vulnerability in ICMPv6 Could Allow Denial of Service (2868623)
MS13-053: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code E
MS13-047: Cumulative Security Update for Internet Explorer (2838727)
Import to Issue Database
Existing Issues
Overwrite
Merge
Discard
Selection Options
Select All
Unselect All
Filter issues to import
Title
All Text
Severity
Critical
Filter
Change Title
Remove
Clear All
Import File
Select File
Browse
sus_report_ [redacted] nessus
PARSE
IMPORT
File Format
Nessus v2 (.nessus)
Nessus (.nbe)
OpenVAS (.xml)
NeXpose (xml)
Nipper (xml)
Surecheck (xml)
NMap (.xml)
OWASP ZAP (xml)
Burp (.xml)
SSLAuditor (.xml)
VPN Auditor (xml)
PIGUtility (xml)
OVAL (.xml)
VulnXML (.xml)
Issue Database (.db)
AUTO DETECT
Found 1000 items ...
| Selection: 11 | Import: 156 | © Aman Hardikar .M


Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Title Page
Report Title
Client Name
Version
Date
Author
Author's Company
Contact (email)
Contact (phone)
Methodologies
Select the applicable methodologies
Add More
Add to Report
Reload
Following methodologies will be added to the report
Introduction
Starting
Conclusion
Ending
Methodologies
Ending
Introduction / Executive Summary
Conclusion
Found 1000 items ...
| Selection: 11 | Import: 156 | © Aman Hardikar .M


Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Issues Selected
HTML5 cross-origin resource sharing
HTTP Header Settings
Concurrent Logins Allowed
Reflected Cross Site Scripting
Sensitive Information in Document Metadata
Use of robots.txt
Vulnerable to BEAST attack
Use of Wildcard Certificate
Cacheable HTTPS response
Autocomplete Enabled
Improvements to Password Controls
Edit Selected
Remove Selected
Clear All
Selection Options
Filter issues to export
Title
All Text
Severity
Critical
Filter
Select file
Browse
EXPORT
File Format
HTML
Web Page
TXT
Text
PDF
Portable
XML
OVAL
XML
VulnXML
Spreadsheet
Open Doc
Document
Open Doc
Help
Feedback
ABOUT
Nothronychus is a freeware tool to automate report writing and also standardize the report text across reports. It can import reports from other tools and can export to various formats. It can also be used to merge the reports from various tools and generate a combined report. The filtering features in both the import and export can be used to filter the findings based on title, severity or text in description / recommendation.
Found 1000 items ...
| Selection: 11 | Import: 156 | © Aman Hardikar .M


Nothronychus 4.0 (Report utility for Penetration Test Reports / Recording Vulnerability)
Viewer
Editor
Search
Library
Import
Layout
Export
Notes
Donate
Not functional in the current version
Load Template
Found 1000 items ...
| Selection: 11 | Import: 156 | © Aman Hardikar .M