



Executive Security Report

1. Special Notes

This report has been generated using N-Stalker Free Edition 2012. Get your copy at <http://www.nstalker.com/>.

2. Legal Disclaimer

This report and any supplements are CONFIDENTIAL and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. If you are not the intended recipient, any use, disclosure, copying or distribution of the report is UNAUTHORIZED. If you have received this report in error, please destroy it immediately.

N-Stalker Web Application Security Scanner assessments ("Services") are provided on an "As Is, As Available" basis without any warranty of any kind. By accepting this report, you understand that assessing computer security is highly complex and changeable. N-Stalker Web Application Security Scanner makes no warranty that the "Services" will find every vulnerability in your Web Application or Web Server(s), or that the solutions suggested and advice provided in this report will be complete or error-free. N-Stalker Web Application Security Scanner shall be held harmless and free from all liabilities for any use or application of the information provided by aexcea in connection with using the "Services". You use the "Services" at your own risk. You are solely responsible for any damage to your devices as a result of using the "Services".





N-Stalker Web Application Security Scanner MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF THE SERVICES.

3. Technical Summary

3.1. Scan Session Information

URL :	https://www.afmc.gov.tw/
Date:	Oct 30, 2020 17:41:34
Scan Policy:	OWASP Policy
SSL Cipher (Algorithm):	N/A
Server Reported Banner:	Microsoft-IIS/10.0
Server Technology (Banner):	Unknown Server
Server Technology Detected:	Microsoft-IIS/3-4.0 (old versions)
Server-side Technologies:	[ASP], [WinCGI], [.NET], [MS IIS]

3.2. Issues Found

Status	# Found
 High	0
 Medium	0
 Low	0
 Informational	20

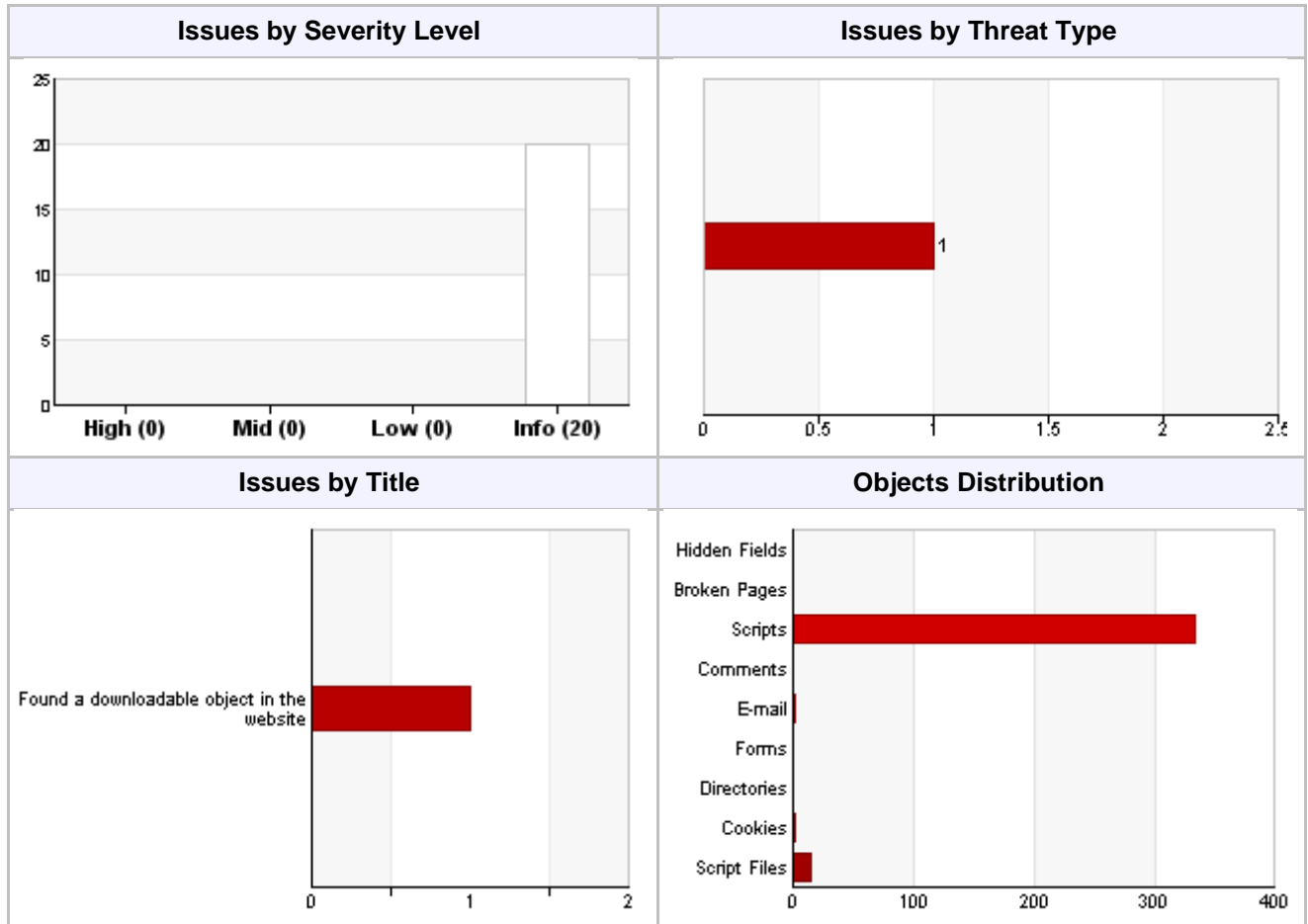
3.3. Scan Session Statistics

Total Duration:	00 hours 16 minutes
Number of Pages (URLs):	358 pages
Total Requests:	567 requests
Total Bytes In:	12,223,508 bytes
Total Bytes Out:	267,726 bytes
Average Response Time:	0 ms
Average Transfer Rate:	1,329,089.00 KB/s
Average Page Size:	207,106 bytes

3.4. Scan Policy Details

- ? **N-Stalker Web Application Security Scanner HTTP Attack Signatures Database**
 - ? Generic HTTP Attacks
 - ? CGI Attacks
- ? **Ataque Common File & Directory**
 - ? Search for Hidden Directories
- ? **Web Server Security**
 - ? Search for Files susceptible to download
 - ? Ensure SSL channel is using strong encryption
 - ? Search for Insecure HTTP Methods
 - ? Identify server technology through HTTP fingerprints
 - ? Search for Web Server software vulnerabilities
 - ? Search for issues in SSL server's certificate
- ? **DOM Security Check**
 - ? Search for Information Exposure on Meta Tags
- ? **Web Form Security**
 - ? Search for Web Forms that allow for password-cache
 - ? Search for information leakage in Web Forms (external action)
 - ? Search for Unprotected Authentication Web Forms (outside SSL)
 - ? Search for suspicious hidden values in Web Forms
- ? **Attack Modules**

4. Graphical Details



5. Items that require your attention

5.1. Infrastructure Issues

No Issues found.

5.2. Application Issues

No Issues found.

5.3. Confidentiality Issues

④ Informational	Found a downloadable object in the website
Target Server	https://www.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
Objects available to download in Web Applications are a critical part of any information security strategy. Usually confidential/private documents end up being exposed because of the lack of controls and manual verification. You should consider evaluating all "downloadable" objects to avoid private information exposure.