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 WARANTIES, 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://tyac2.afmc.gov.tw/
Date:	Oct 30, 2020 18:16:47
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
1 High	**0**
2 Medium	**0**
3 Low	**0**
4 Informational	**9**

3.3. Scan Session Statistics

Total Duration:	00 hours 04 minutes
Number of Pages (URLs):	66 pages
Total Requests:	386 requests
Total Bytes In:	3,846,296 bytes
Total Bytes Out:	111,892 bytes
Average Response Time:	0 ms
Average Transfer Rate:	1,178,893.00 KB/s
Average Page Size:	203,673 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 trough 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)

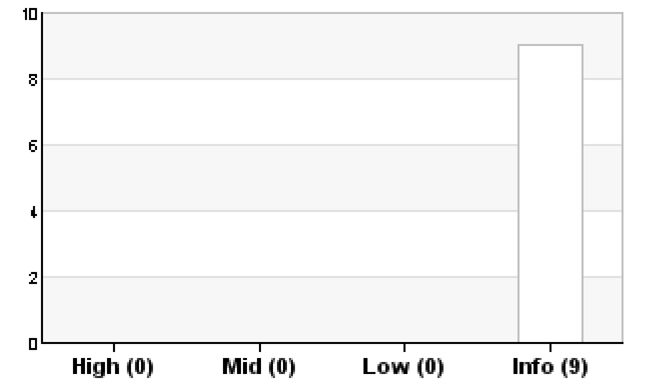
  ? Search for suspicious hidden values in Web Forms

? **Attack Modules**

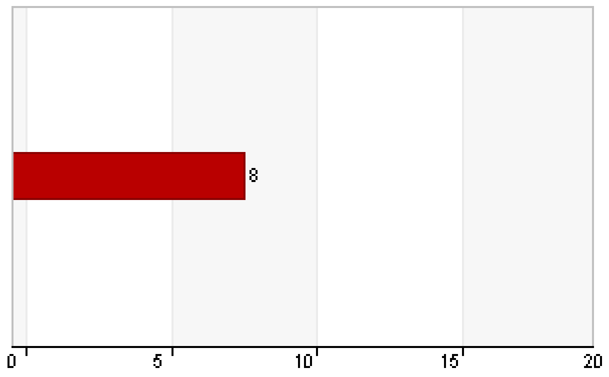
  ? Cross-Site Scripting Assessment

4. Graphical Details

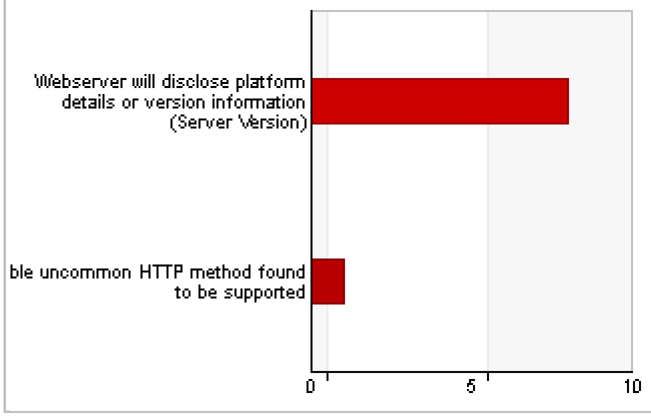
Issues by Severity Level



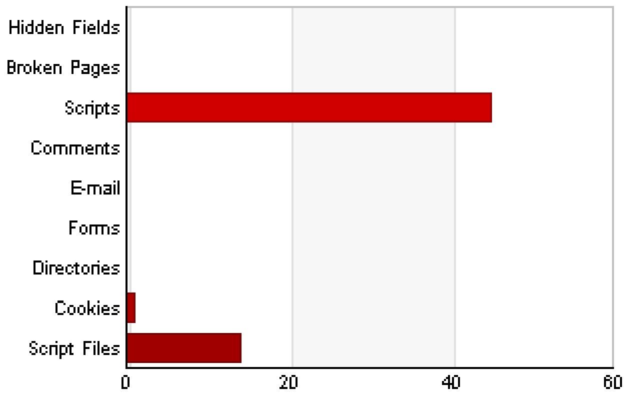
Issues by Threat Type



Issues by Title



Objects Distribution



5. Items that require your attention

5.1. Infrastructure Issues

4 Informational	Webserver will disclose platform details or version information (Server Version)
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.

4 Informational	Webserver will disclose platform details or version information (Platform Details and Version)
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.

4 Informational	Webserver will disclose platform details or version information (HTTP Information)
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
Your webserver is exposing information about its version and platform details that might assist an attacker while assessing an effective attack against your infrastructure.

4 Informational	Found SSL/TLS certificate information
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
N-Stalker provides a full set of common attack signatures to detect vulnerable web server infrastructure and 3rd-party components. By running a set of HTTP requests crafted by well-known signatures, N-Stalker may detect if a vulnerability is present in a particular server. You must consider assessing the issue to define if it represents a real problem to your application.

4 Informational	**SSL/TLS Ciphers supported by this webserver**
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
N-Stalker provides a full set of common attack signatures to detect vulnerable web server infrastructure and 3rd-party components. By running a set of HTTP requests crafted by well-known signatures, N-Stalker may detect if a vulnerability is present in a particular server. You must consider assessing the issue to define if it represents a real problem to your application.

4 Informational	**Webserver is enforcing its own SSL/TLS cipher order**
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
N-Stalker provides a full set of common attack signatures to detect vulnerable web server infrastructure and 3rd-party components. By running a set of HTTP requests crafted by well-known signatures, N-Stalker may detect if a vulnerability is present in a particular server. You must consider assessing the issue to define if it represents a real problem to your application.

4 Informational	**Webserver is supporting SSL/TLS Forward Secrecy Cipher (PFS)**
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?

Instead of using the RSA method for exchanging session keys, you should use the Elliptic Curve Diffie-Hellman (ECDHE) key exchange. Note that you can still use the RSA public-key cryptosystem as the encryption algorithm, just not as the key exchange algorithm. ECDHE is much faster than ordinary DH (Diffie-Hellman), but both create session keys that only the entities involved in the SSL connection can access. Because the session keys are not linked to the server key pair, the server private key alone cannot be used to decrypt any SSL session.

4 Informational	**Default SSL/TLS protocol version**
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?

This security check will inspect the default SSL/TLS protocol version offered by the webserver. See details to obtain additional information.

5.2. Application Issues

4 Informational	Possible uncommon HTTP method found to be supported
Target Server	https://tyac2.afmc.gov.tw/
# of Occurences	1

Why is it an issue ?
HTTP methods are like action verbs/commands that are issued against a particular Web Server. Common methods like GET/POST are vital to any Web Application and usually secure for common transactions. Uncommon HTTP methods are verbs/commands that will be interpreted by your web server but does not necessary carry any importance to your application. By allowing your web server to intepret and respond to uncommon HTTP methods, you are allowing attackers to: ? Remotely identify the version of your HTTP server ? Waste server resources by forcing web servers to interpret and respond useless requests ? Tamper with your web server to obtain additional information (TRACE attacks)

5.3. Confidentiality Issues

No Issues found.