Stickman Penetration Testing Sample Report

Subtitle Text

Prepared for:

Company Logo

stickman

CYBER SECURITY BY DESIGN

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

Table of Contents

1. Executive Brief

Stickman Consulting conducted a penetration test against the <Testing activities in scope> of <Client name>from <date> until <Date>.

Stickman Consulting launched the penetration test against the in-scope assets (see Appendix – Scope) and identified the following vulnerabilities:

- <Number of issues found> Critical vulnerability.
- <Number of issues found> High vulnerability.
- <Number of issues found> medium vulnerabilities.
- <Number of issues found> low vulnerabilities.
- <Number of issues found> informative issue.

The test was conducted as a <type of testing> approach for the <Testing activities in scope> provided to the Stickman testing team.

For the in-scope <Testing activities in scope>, Stickman conducted a thorough analysis by making use of various manual (e.g. BurpSuite[1]) and other techniques and identified the presented vulnerabilities. OWASP ASVS v4.0[2] and OWASP API Security Top 10 were adopted as the testing approach for the tests conducted.

The identified issues should be remediated, within 24 hours for the Critical issue, two (2) weeks for the high issues, and one (1) month for medium and low vulnerabilities (as highlighted by the Australian Signal Directorate (ASD)[3]). For the informative issue reported, it is recommended that XYZ perform an internal risk assessment and address the issue based on the organisation's risk strategy.

[1] https://portswigger.net/burp/pro
[2] https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
[3] https://www.cyber.gov.au/node/83

2. Vulnerability List

The following vulnerabilities were detected during the penetration test:

ID	Vulnerability	Risk	Status	Reported Date	Retest Date
C1	production Web Server (ProdWebServer) Path Traversal Vulnerability	Critical	Open	<date>	<date>
C2	MS17-010 Eternal Blue - SMB Remote Windows Kernel Pool Corruption	Critical	Open	<date>	<date>
C3	Blind SQL Injection	Critical	Open	<date>	<date>
C4	Out-of-band XML External Entity (OOB-XXE)	Critical	Open	<date>	<date>
C5	Broken Access Control Leading Access to the User's Sensitive Data and Site Wide Account Takeover	Critical	Open	<date>	<date>
H1	Cisco ASA/FTD Web Services Read-Only Path Traversal Vulnerability (CVE-2020-3452)	High	Open	<date>	<date>
H2	Information Disclosure in .js File	High	Open	<date>	<date>
H3	Stored Cross Site Scripting	High	Open	<date>	<date>
H4	Anonymous FTP Server Login enabled	High	Open	<date>	<date>
H5	CSRF to change password Leading to Account Takeover	High	Open	<date>	<date>
H6	Reflected Cross Site Scripting - Customer to Any Account	High	Open	<date>	<date>
H7	Host Header Injection in Password Reset Lead to Reset Token Leakage	High	Open	<date>	<date>
M1	TLS 1.0 Protocol Detection	Medium	Open	<date>	<date>
M2	SSL/TLS Server Supports RC4 Ciphers	Medium	Open	<date>	<date>
M3	SSL/TLS server supports short block sizes (SWEET32 attack)	Medium	Open	<date>	<date>
M4	SMB Signing Disabled or Not Required	Medium	Open	<date>	<date>
M5	SNMP Agent Default Community Name (public)	Medium	Open	<date>	<date>
L1	Weak Cache Policy	Low	Open	<date>	<date>
L2	External SSRF	Low	Open	<date>	<date>
L3	Exif Data Not Stripped From Uploaded Images	Low	Open	<date>	<date>
I1	Server Banner Disclosure	Informative	Open	<date>	<date>
I2	Information Disclosure	Informative	Open	<date>	<date>
I3	Weak Password Policy	Informative	Open	<date>	<date>

3. Detailed Findings

4.1 Critical

C1	production Web Server (ProdWebServer) Path Traversal Vulnerability
Description	Stickman identified that the Example Web Server on port 80 is vulnerable to an exploit which would allow an attacker to read arbitrary files on the remote host outside the web server's document directory using a specially crafted URL. An unauthenticated attacker may be able to exploit this issue to access sensitive information to aid in subsequent attacks. During the time of our engagement, we were not able to find/identify any CVE allocated to this issue, therefore we believe that this could potentially be an undisclosed security issue and might require immediate vendor attention.
CVSSv3.1 Base Score	Critical 9.1
CVSSv3.1 Base Vectors	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-23: Relative Path Traversal
OWASP Top Ten 2017	-
Affected URL/IP	http://<target-ip>/../../../../../../../../etc/passwd
Test Reproduction	During the time of our engagement, we were able to retrieve the affected host's password file (/etc/passwd), host file (/etc/hosts) and/or any internal system files. Approach 1: Send a GET request to the path '../../../../../../../../etc/passwd' using a proxy tool like Burpsuite and you should be able to see the system file "/etc/passwd" **<Screenshot#1>** Approach 2: Send a GET request to the path using either netcat (nc) or telnet as highlighted on the image below. You should be presented with the internal system file "/etc/passwd" **<Screenshot#2>**

Appendix – Scope

Web Applications

- http://target.com/

APIs

- http://target.com/

Tools

- BurpSuite.
- Postman.
- Nikto.
- Nmap.
- Google Chrome (*various developer tools*).

Confidentiality & Copyright Agreement

stickman
CYBER SECURITY BY DESIGN

Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

P: 1800 785 626
E: sales@stickman.com.au
www.stickman.com.au