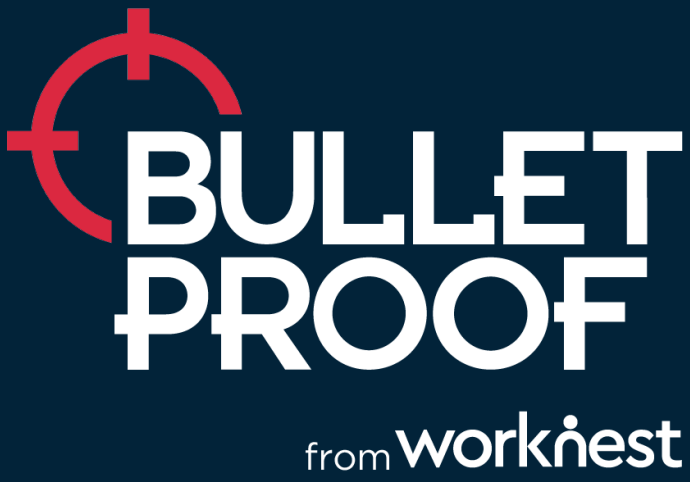


SYNTHETIC USERS - PENETRATION TESTING (FULL REPORT)

CONFIDENTIAL

DOCUMENT CONTROL

CLASSIFICATION	CONFIDENTIAL
DATE	12/09/2025 - 12/09/2025
APPROVED BY	Piyush Paliwal
DOCUMENT REFERENCE	PT83573-9361
DELIVERED	18/09/2025

VERSION	DATE	DESCRIPTION
0.1	12/09/2025	Document Creation
0.2	17/09/2025	Report Completed - Aedan Taylor
0.3	18/09/2025	QA Approved - Piyush Paliwal
1.0	18/09/2025	Delivered - Piyush Paliwal

Your penetration test report is delivered through our cyber security SaaS product, Defense.com™ by Bulletproof penetration testers. Bulletproof/Target Defence penetration testers are independently qualified by industry-recognised bodies such as CREST and can be found on the following CREST member companies list https://service-selection-platform.crest-approved.org/member_companies/bulletproof-cyber-serverchoice/.

TABLE OF CONTENTS

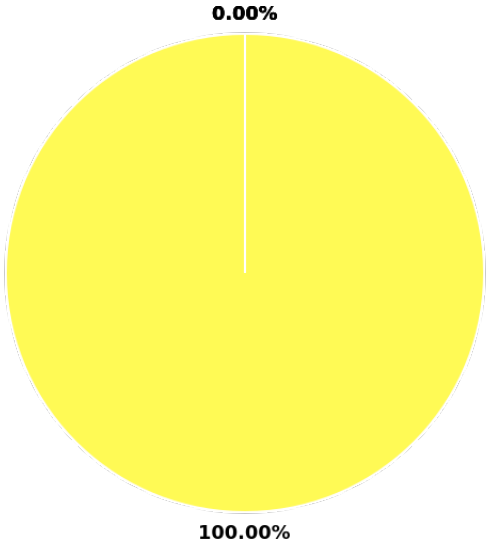
1. EXECUTIVE SUMMARY

1.1 TEST PARAMETERS

DOCUMENT REFERENCE	PT83573-9361
TEST START	12/09/2025
TEST END	12/09/2025
TEST TIME	Office Hours (08:00 - 17:30 UTC)
TEST TYPE	External Infrastructure
TEST TECHNIQUE	Grey box
LIMITATIONS	Assessing and exploiting vulnerabilities that could lead to a denial of service., Social engineering is excluded as way for granting access to an application., There will be no re-test included with this service.
PERSONNEL	Aedan Taylor

1.2 RESULTS SUMMARY

RISK LEVEL	RISKS FOUND
Critical	0
High	0
Medium	0
Low	1
Recommendations	0
TOTAL	1



1.3 RISK RATING TABLE

AREA	DESCRIPTION	RATING
Configuration	Overall security level of service and device configurations.	Strong
Authentication	User authentication methods used.	Strong
Patching	Vulnerable software versions.	Strong
Segmentation	External infrastructure segmentation.	Strong
Encryption	Encryption methods and protocols used.	Strong

1.4 TEST TARGETS

TYPE	TARGET
Hostname	api.syntheticusers.com

2. ASSESSMENT OVERVIEW

2.1 ENVIRONMENT OVERVIEW

Scope

An unauthenticated external infrastructure penetration test was performed on behalf of Synthetic Users.

The aim of the assessment was to uncover any weaknesses that affect the confidentiality, integrity and availability of the services offered by Synthetic Users and was carried out in accordance with the agreed Scope of Work. The assessment was carried out from a grey-box perspective and was conducted in-line with security best practices. No accounts were provided to facilitate testing. No assessment of vertical and horizontal access controls was performed.

The security assessment started by performing automated scans and manual checks in order to gather all the necessary information concerning the in-scope target, current patch levels, improper configurations and security controls. Manual verification and further testing based on observed results were then performed.

The targets for the external infrastructure test were the following domain:

- `api.syntheticusers.com`

Overview

Overall, the security posture of the organisation was found to be nearly optimal. One low risk finding was discovered over the course of the test. This should be mitigated in order to strengthen the security posture of the organisation. Additionally, a recommendation has been provided in line with industry best practice.

The low-risk issue found on the test pertains to SHA-1 being found to be in use on the one available web server's TLS settings. This should be disabled to prevent sufficiently resourced attackers from intercepting and decrypting traffic or spoofing content.

Overall, mitigation is expected to be of low difficulty. Remediation advice has been provided for each issue.

It is important that Synthetic Users are aware that the vulnerabilities identified in this document are dependent on the time and test limitations given for this penetration test. Other issues may come to light after this test, which is why it is recommended to carry out regular vulnerability assessments.

Caveats

There were no caveats or restrictions encountered by the team during the engagement.

2.2 BUSINESS RISK SUMMARY

The recommendations set forth in this report are the result of the shortcomings identified from the unauthenticated external infrastructure penetration testing activities that have been carried out against the pre-defined scope. Overall, the test results indicate very low business risk exposure that is a threat to key business operations requiring resolution. The issues that were identified within the environment are likely to affect the wider organization.

An issue was raised concerning the standard of encryption utilized for data during transit. Decrypted data that is intercepted during transmission by an attacker can disclose a plethora of information, such as credentials and business data. Efforts should be made to ensure that all data within the estate is encrypted during transit using a secure configuration of TLS/SSL to reduce the likelihood of data exposure to suitably positioned attackers.

To conclude, it is strongly advised that a re-test be planned once remediation is applied. It is recommended that Synthetic Users resolve all issues found to better improve its stance. Remediation advice has been provided along with the breakdown of each issue found.

2.3 RISK RESULTS

DESCRIPTION	RISK RATING	REFERENCE
TLS/SSL Misconfigurations	LOW	PT83573-9361-R4329

2.4 CRITICALITY INDEX

Findings have been measured in-line with the CVSS scoring system.

RISK LEVEL	DESCRIPTION	RECOMMENDATION
CRITICAL SCORE: 9-10	A critical risk indicates serious and immediate risk to systems and data being compromised.	Critical rated issues need to be addressed and resolved immediately.
HIGH SCORE: 7-9	High risk indicates that a serious weakness or exposure exists.	High rated issues need to be addressed and resolved immediately.
MEDIUM SCORE: 4-7	Medium risk indicates that a significant issue needs to be addressed.	Actions need to be taken once high risks have been addressed.
LOW SCORE: 1-4	Low-risk indicates minor issues that generally are harmless but can be used when profiling an organisation.	No immediate action is required but should be addressed through the remediation phase.
RECOMMENDATION SCORE: N/A	Recommendations are included for improvements purposes only as they pose an indirect risk to current environment.	N/A

3. ASSESSMENT RESULTS

3.1 EXTERNAL INFRASTRUCTURE

3.1.1 TLS/SSL MISCONFIGURATIONS

REFERENCE	PT83573-9361-R4329
AFFECTED TARGETS	api.syntheticusers.com
PASS / FAIL	FAILED
SEVERITY	LOW
LIKELIHOOD	LOW
EFFORT TO FIX	LOW
DESCRIPTION	

TLS/SSL technology is commonly used in websites and web applications together with the HTTP protocol. To secure the transfer of data, TLS/SSL uses one or more cipher suites - which is a combination of authentication, encryption, and message authentication code (MAC) algorithms.

The following security flaws were identified in relation to the TLS/SSL configuration of the affected hosts:

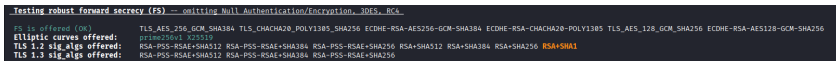
SHA-1 Supported (Low)

SHA-1 is considered insecure as it is vulnerable to collision attacks. Use of SHA-1 is deprecated by NIST in 2011.

EVIDENCE

TLS FINDINGS

SHA-1 was found to be in use on the target server. This can potentially be abused by a sufficiently positioned and resourced attacker in decrypting or spoofing content.



SHA-1 enabled

REMEDIATION

The following TLS/SSL configurations are considered best practice in terms of security:

• Weak or obsolete ciphers such as SHA-1 based ciphers should not be supported

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

https://www.ssllabs.com/projects/best-practices/

https://www.ssl.com/guide/ssl-best-practices/

https://ssl-config.mozilla.org/

4. APPENDIX

4.1 NMAP SCAN RESULTS

Open TCP and UDP ports were scanned on the targets in scope. The open ports and discovered services are summarised below.

TYPE	TARGET	OPEN PORTS	DESCRIPTION
Hostname	api.syntheticusers.com	80/TCP 443/TCP	http https

4.2 TESTING METHODOLOGY

This Bulletproof Cyber Limited penetration test used the CREST framework as an overarching methodology, into which the required frameworks are embedded, such as the Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP).

The below "test highlights" listed for each assessment category describe some of the most important areas that will be covered as part of the engagement. These objectives are primarily achieved by assessing aspects such as the design, configuration, deployment, operational security and direct/indirect risks of all assets in scope. The assessments carried out, checks performed and security best practice recommendations are all in line with industry approved standards and methodologies. Furthermore, our bespoke engagements often include additional custom checks and attack scenarios that are tailored against the target environment and customer.

EXTERNAL INFRASTRUCTURE ASSESSMENT

- Enumerate all running services and open ports on each individual system, network or application component.
- Assess the services and any associated components/dependencies for their patch levels.
- Assess and exploit known vulnerabilities using automation and manual exploitation, prioritised on the criticality of each system.
- Assess and identify misconfigurations based on common attack vectors that are used widely in real life scenarios.
- Assess the authentication mechanisms in place using a variety of different techniques such as access control configuration enforcement, default accounts, authentication bypass vulnerabilities etc.
- Assess the cryptographic protocols and ciphers that are used by each individual service.

• Review the network design and ensure that sufficient segmentation/segregation is in place.

• Assess the infrastructure for any sensitive information disclosure or resources such as databases/network shares storing sensitive data.