

 **Matrixforce**[®]
Overwatch[®] **Cybersecurity**

FORTINET[®]

Web Penetration Test
27 October 2021

Executive Summary
Common Criteria Evaluation

FORWARD

This report is an UNCLASSIFIED publication, issued under the authority of the Chief Executive Officer of Matrixforce.

The Information identified in this report, and its associated detail, has been evaluated and approved by a licensed cyberist using the Delta Method established under Matrixforce Overwatch Cybersecurity. This report, and its associated detail, applies only to the identified version and release of the penetration test configuration. The evaluation has been conducted in accordance with the provisions outlined by the Cybersecurity and Infrastructure Security Agency. This report, and its associated detail, are not an endorsement of the tested app or website and no warranty for security is either expressed or implied.

If your department has identified a requirement for this report based on business needs and would like more detailed information, please contact:

Matrixforce Support
support@matrixforce.com | 1-918-622-1167

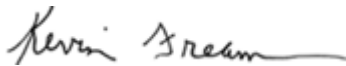
OVERVIEW

Matrixforce provides a third-party evaluation service for determining the trustworthiness of cloud applications or websites. Evaluations are performed by Matrixforce established in 1978 and thoroughly investigated by government and industry authorities for commercial Common Criteria Evaluation

Matrixforce uses a commercial platform that has been approved to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of Vetted IT Support, the General Requirements of Fraud Protection, Intellectual Property, Industry Competency, Published Authority, and Public Compliance.

With a Common Criteria report, the app or website complies with the security requirements specified in the associated security target. A security target is a requirements specification that defines the scope of the evaluation activities. The client should review the security target, in addition to this report, in order to gain an understanding of any assumptions made during the test, the intended environment, the evaluated security functionality, and the testing and analysis conducted.

The cloud penetration report follows along with Matrixforce logo for public notice and proof of client commitment to cybersecurity and privacy for publication on client official website.



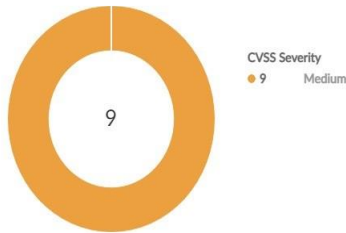
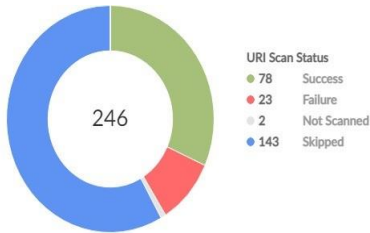
Kevin Fream
CEO
Matrixforce



Security Target Summary

IP/FQDN : <https://matrixforce.com>
 PORT : 443
 UUID : 59f7e6de-a7b8-4c42-9c3c-2b0895f20a28
 Scan Status : 100%
 Completed : 2021-10-27 13:56:59 UTC
 Total Requests sent : 1545

Threat Level :



URI Scan Summary

OWASPCATEGORY	SEVERITY			
	Critical	High	Medium	Low
A1 - Injection	0	0	0	0
A2 - Broken Authentication	0	0	0	0
A3 - Sensitive Data Exposure	0	0	4	0
A4 - XML External Entities	0	0	0	0
A4 2010 - Upload Insecure Files	0	0	0	0
A5 - Broken Access Control	0	0	0	0
A6 - Security Misconfiguration	0	0	5	0
A7 - Cross-Site Scripting	0	0	0	0
A8 - Insecure Deserialization	0	0	0	0
A9 - Using Components with Known Vulnerabilities	0	0	0	0
A10 - Insufficient Logging and Monitoring	N/A			
A10 2013 - Unvalidated Redirects and Forwards	0	0	0	0
Total	0	0	9	0



Top 10 Web Application Security Risks

Leveraging the OWASP Top 10 list of most prominent application security risks, FortiPenTest runs a series of tests and attacks to determine what vulnerabilities a target IP address or Fully Qualified Domain Name (FQDN) is susceptible to, then provides full details on not only the vulnerability, but also what you can do about it.

FortiPenTest leverages the OWASP Top 10 Application Security Risk listing to craft a series of tests designed to verify that a target system has been successfully secured against exploit or penetration. FortiPenTest can also take advantage of a third-party command and control (C&C) server, allowing security modules to carry blind attacks. Full results are displayed and categorized by their CVSS severity score. Based upon these CVSS scores, an overall Threat Score for the target is generated and displayed

1. **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
2. **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
3. **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
4. **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
5. **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it’s not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
6. **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.



7. **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
8. **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
9. **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
10. **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.



Security Vulnerabilities

URI List

URI	STATUS	STARTED	COMPLETED			ISSUES		
nasdaq-vetted-it-support-briefing/		04:40:26.076	13:55:25.606					
https://www.matrixforce.com/phoenix/online-backup/	Success	2021-09-02 04:40:31.774	2021-09-07 13:55:31.112	0	0	0	0	0
https://www.matrixforce.com/orbit/cloud-computing/	Success	2021-09-02 04:40:31.798	2021-09-07 13:55:28.156	0	0	0	0	0
https://www.matrixforce.com/resources/easy-prey/	Success	2021-09-02 04:40:35.782	2021-09-07 13:55:33.622	0	0	0	0	0
https://www.matrixforce.com/overwatch/	Success	2021-09-02 04:40:39.846	2021-09-07 13:55:39.751	0	0	0	0	0
https://www.matrixforce.com/resources/ransomware-prevention-blueprint/	Success	2021-09-02 04:40:39.892	2021-09-07 13:55:47.350	0	0	0	0	0
https://www.matrixforce.com/phoenix/	Success	2021-09-02 04:40:40.272	2021-09-07 13:56:07.927	0	0	0	0	0
https://www.matrixforce.com/resources/service-provider-advisory/	Success	2021-09-02 04:40:45.909	2021-09-07 13:55:41.924	0	0	0	0	0
https://www.matrixforce.com/resources/	Success	2021-09-07 13:55:35.314	-	0	0	0	0	0
https://www.matrixforce.com/support/	Success	2021-09-02 04:40:49.974	2021-09-07 13:55:53.880	0	0	0	0	0
https://www.matrixforce.com/search/	Success	2021-09-02 04:40:58.335	2021-09-07 13:56:04.019	0	0	0	0	0
https://www.matrixforce.com/resources/trusted-advisor-guide/	Success	2021-09-02 04:41:00.044	2021-09-07 13:55:57.479	0	0	0	0	0
https://www.matrixforce.com/kb/active-directory-rogue-account-detection/	Success	2021-09-02 04:41:04.092	2021-09-03 13:38:32.247	0	0	0	0	0
https://www.matrixforce.com/kb/enable-bitlocker/	Success	2021-09-02 04:41:04.397	2021-09-03 13:38:17.820	0	0	0	0	0
https://www.matrixforce.com/kb/azure-ad-connect-setup/	Success	2021-09-02 04:41:04.519	2021-09-03 13:37:56.789	0	0	0	0	0
https://www.matrixforce.com/kb/auditing-account-logon/	Success	2021-09-02 04:41:08.715	2021-09-03 13:38:14.375	0	0	0	0	0
https://www.matrixforce.com/legal/terms	Success	2021-09-02 04:41:10.177	2021-09-03 13:37:56.805	0	0	0	0	0
https://www.matrixforce.com/kb/workstation-setup-guide/	Success	2021-09-02 04:41:11.357	2021-09-03 13:38:13.966	0	0	0	0	0
https://www.matrixforce.com/kb/group-policy-configuration/	Success	2021-09-02 04:41:12.204	2021-09-03 13:38:40.389	0	0	0	0	0
https://www.matrixforce.com/kb/office-365-android-setup/	Success	2021-09-02 04:41:12.621	2021-09-03 13:38:06.654	0	0	0	0	0
https://www.matrixforce.com/legal/privacy	Success	2021-09-03 13:39:02.755	2021-09-07 13:56:37.926	0	0	0	0	0
https://www.matrixforce.com/guardian/it-consulting/	Success	2021-09-02 04:41:20.315	2021-09-03 13:38:49.033	0	0	0	0	0
https://www.matrixforce.com/kb/microsoft-365-group-setup/	Success	2021-09-02 04:41:22.725	2021-09-03 13:38:14.981	0	0	0	0	0
https://www.matrixforce.com/kb/cybersecurity-risk-exam-process/	Success	2021-09-02 04:41:28.426	2021-09-03 13:38:36.014	0	0	0	0	0
https://www.matrixforce.com/kb/office-365-important-urls/	Success	2021-09-02 04:41:30.851	2021-09-03 13:38:24.122	0	0	0	0	0
https://www.matrixforce.com/guardian/managed-services/#benefits	Success	2021-09-02 04:41:31.492	-	0	0	0	0	0
https://www.matrixforce.com/kb/azure-backup-file-restore/	Success	2021-09-02 04:41:34.477	2021-09-03 13:38:09.699	0	0	0	0	0
https://www.matrixforce.com/	Success	2021-09-02	-	0	0	0	0	0



URI	STATUS	STARTED	COMPLETED	ISSUES				
guardian/managed-services/#msp		04:41:38.866						
https://www.matrixforce.com/guardian/it-support/	Success	2021-09-02 04:41:39.280	2021-09-03 13:38:32.246	0	0	0	0	0
https://www.matrixforce.com/guardian/managed-services/#faq	Success	2021-09-02 04:41:39.528	-	0	0	0	0	0
https://www.matrixforce.com/kb/microsoft-secure-score-actions/	Success	2021-09-02 04:41:40.972	2021-09-03 13:38:24.511	0	0	0	0	0
https://www.matrixforce.com/legal	Success	2021-09-02 04:41:44.652	-	0	0	0	0	0
https://www.matrixforce.com/contact	Success	2021-09-02 04:41:49.112	2021-09-07 13:56:04.043	0	0	0	0	0
https://www.matrixforce.com/about	Success	2021-09-02 04:41:49.408	2021-09-07 13:56:06.935	0	0	0	0	0
https://www.matrixforce.com/about/streamlining-technology	Success	2021-09-02 04:41:49.649	2021-09-07 13:56:21.027	0	0	0	0	0
https://www.matrixforce.com/guardian/managed-services/#model	Success	2021-09-02 04:41:51.933	-	0	0	0	0	0
https://www.matrixforce.com/about/microsoft-gold-partner	Success	2021-09-07 13:56:09.179	-	0	0	0	0	0
https://www.matrixforce.com/about/delta-methodology	Success	2021-09-02 04:41:56.369	2021-09-07 13:56:15.611	0	0	0	0	0
https://www.matrixforce.com/resources/revealing-secrets-streamlining-technology	Success	2021-09-02 04:41:59.779	2021-09-07 13:56:31.900	0	0	0	0	0
https://www.matrixforce.com/about/streamline-your-technology	Success	2021-09-02 04:42:01.003	2021-09-07 13:56:30.341	0	0	0	0	0
https://www.matrixforce.com/about/vetted-it-support	Success	2021-09-02 04:42:02.048	2021-09-07 13:56:19.900	0	0	0	0	0
https://www.matrixforce.com/404/?aspxerrorpath=/kb/microsoft-secure-score-actions/	Success	2021-09-02 04:42:04.476	2021-09-07 13:56:53.492	0	0	0	0	0
https://www.matrixforce.com/resources/service-provider-advisory	Success	2021-09-02 04:42:08.333	2021-09-07 13:56:21.937	0	0	0	0	0
https://www.matrixforce.com/resources/easy-prey	Success	2021-09-02 04:42:09.313	2021-09-07 13:56:31.995	0	0	0	0	0
https://www.matrixforce.com/careers	Success	2021-09-02 04:42:10.151	2021-09-07 13:56:07.941	0	0	0	0	0
https://www.matrixforce.com/kb	Success	2021-09-07 13:56:36.810	-	0	0	0	0	0
https://www.matrixforce.com/kb/microsoft-secure-score-actions/	Success	2021-09-07 13:56:37.928	-	0	0	0	0	0
https://www.matrixforce.com/resources/trusted-advisor-guide	Success	2021-09-03 13:36:24.028	2021-09-07 13:56:42.412	0	0	0	0	0
https://www.matrixforce.com/events	Success	2021-09-03 13:36:49.670	2021-09-07 13:56:31.914	0	0	0	0	0
https://www.matrixforce.com/resources/ransomware-prevention-blueprint	Success	2021-09-03 13:36:59.264	2021-09-07 13:56:31.355	0	0	0	0	0
https://www.matrixforce.com/kb/remote-desktop-services-mfa-setup/	Success	2021-09-03 13:38:17.823	-	0	0	0	0	0
https://www.matrixforce.com/overwatch/covid19-cybersecurity/	Success	2021-09-03 13:38:49.037	-	0	0	0	0	0
https://www.matrixforce.com/resources/data-breach-training/	Success	2021-09-03 13:38:55.041	-	0	0	0	0	0
https://www.matrixforce.com/resources	Success	2021-09-03 13:39:03.918	2021-09-07 13:56:22.850	0	0	0	0	0



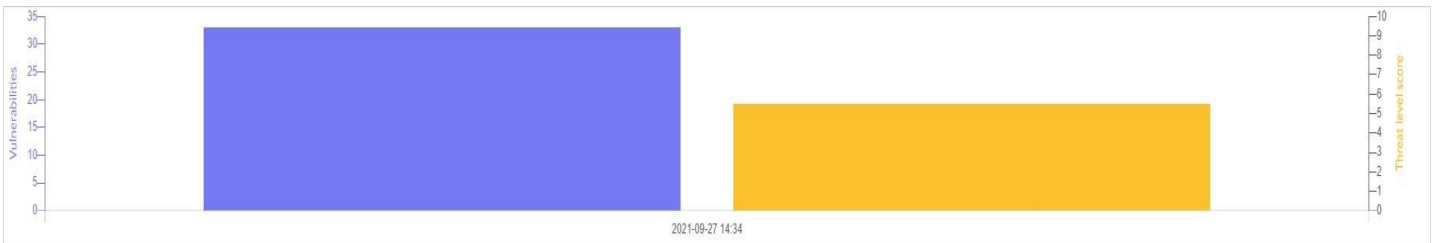
URI	STATUS	STARTED	COMPLETED	ISSUES				
https://www.matrixforce.com/resources#emergency	Success	2021-09-03 13:39:07.306	-	0	0	0	0	0
https://www.matrixforce.com/images/resources.png/	Success	2021-09-03 13:39:11.040	-	0	0	0	0	0

Summary Report generated by FortiPenTest web vulnerability scanner
v21.3.0-build0104(GA), at Wed Oct 27 2021 15:48:23 GMT-0500 (Central Daylight Time)

Remediation Status and Schedule

There are no critical items. Medium items are system URLs that are not reachable for security purposes. Low items are 2 external Apps unrelated to the website. Separate detail report lists remediation by CVE and client has an ongoing program to remediate and re-run the cloud penetration test quarterly.

Compare Threat Mitigation



Date	Critical	High	Medium	Low	Total	Threat Level	Improvement
2021-09-27 14:34	0	1	30	2	33	5.5	

