External Vulnerability Scan - IT URLS

Redacted

Customer Information	
Company Name:	
Address:	
URL:	

Customer Contact Information	
Contact Name:	
Title:	
Telephone:	
E-mail:	

Consultant Information	
Company Name:	CyberCrowd
Contact Name:	
Title:	Penetration Tester
Telephone:	
E-mail:	
Address:	Unit 2 The Pentangle Park Street Newbury Berkshire RG14 1EA
URL:	hiips://www.cybercrowd.co.uk

Table of Contents

Contents

1. Document Control

1.1 Document Information

Creation Date	30/06/2021
Owner/Author	
Internal/External Audience	External
Document Classification	Commercial in Confidence

1.2 Revision History

Version	Revision Details	Revised By	Date
1.0	Release		06/07/2021

1.3 Document Review/Approval

Reviewer	Position	Date
	Penetration Tester	06/07/2021

2. Executive Summary

The purpose of this document is to provide in-depth analysis of the external vulnerability scan that was conducted on the Redacted external network on the 28/06/2021. Within this document, discovered vulnerabilities and associated CVSS scores will be enumerated along with CVEs and remediation advice. CyberCrowd highly recommend actioning all remediation advice as per section 2 where possible to move towards a more secure external network environment.

2.1 Details

The table below outlines the structure for CVSS (Common Vulnerability Scoring System) scoring as well as a high-level summary from the scan results. Please see the CVSS appendix for risk evaluation against each CVSS score.

CVSS	Risk	Confirmed	Comment
7.0 – 10.0	High/Critical	0	Critical in nature, remediate with priority.
4.0 – 6.9	Medium	3	Assess and remediate with priority.
0.0 – 3.9	Low	0	Assess and remediate.
Informational	N/A	0	Information only.

3. Structure of this Report

This document sets out our findings from the vulnerability assessment and penetration test carried out for Redacted.

It begins with an Executive Summary, above, in Section 2.

Section 3 is this summary of the report structure.

Next, in Section 4, we describe the scope of the engagement.

Section 5, Methodology, briefly describes the testing carried out to deliver the engagement.

Vulnerabilities discovered follows, in Section 6.

4. Scope

The scope of this engagement was to carry out a vulnerability assessment and penetration test of the following targets:

Targets
Redacted

5. Methodology

The testing necessary to deliver the engagement was carried out primarily using industry-standard vulnerability assessment tools:

Nessus Pro from Tenable, is a very widely used professional vulnerability assessment platform that has been developed over nearly 20 years. Nessus includes tens of thousands of test "plugins" each of which tests for a particular kind of security issue. The plugin set is updated daily which means each test uses the absolute latest security knowledge from one of the world's top vendors of security testing technology.

6. Vulnerabilities

Our testing uncovered apparent vulnerabilities on the website. The full detailed list of vulnerabilities is set out as **Appendix A** at the end of this report.

.

IP Address	Vulnerability Title	CVSS Score	Port	Protocol	Remediation Effort
Critical Risk Findings					
High-Risk Findings					
Moderate-Risk Findings					
	Web Application Potentially Vulnerable to Clickjacking	4.3	443	TCP	Quick
	JQuery 1.2 < 3.5.0 Multiple XSS	6.1	443	TCP	Quick
	SSL Medium Strength Cipher Suites Supported (SWEET32)	7.5	443	TCP	Quick
Low-Risk Findings					

6.1 Critical Findings

The following are all of the Critical Findings from the assessment.

6.2 High Risk Findings

The following are all of the High Risk Findings from the assessment.

6.3 Other Findings

The following are the rest of the Findings from the assessment.

Web Application Potentially Vulnerable to Clickjacking

Risk	MODERATE

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Affected Hosts

Proof

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

-