



Penetration Test Final Report

March 16, 2023

Prepared By:

Richard Handley

Manager, Cybersecurity



Testing Information

Client:	iRely			
Test Type:	External / Internal			
Purpose:	External Network and Systems Penetration Testing Internal Network and Systems Penetration Testing Web Application Testing API Testing			
Engagement Dates:	Testing Dates:	02/10/23 to 03/10/23		
	Reporting:	03/10/23 to 03/16/23		
	Retest and Reporting:	04/26/23 to 05/04/23		
Active Assets:	External	Internal	Web Application	Total
	2	1	1	4
Technical Resources:	Richard Handley Manager, Cybersecurity C/ +1 626.393.5272 T/ +1 866.480.9485 x272 E/ Richard.Handley@CGCompliance.com			

Disclaimer

This document contains confidential and proprietary information. It is intended for the exclusive use of iRely. Unauthorized use or reproduction of this document is prohibited.

The current penetration test report has been conducted by CyberGuard Compliance's security experts. This Penetration Test is a point in time assessment that reveals all identified weaknesses known up to the date of this report. As new weaknesses continue to be found, the computer system environment changes, and the introduction of new security threats, CyberGuard Compliance recommends that a Penetration Test be conducted annually and after every major change in the Information System. CyberGuard Compliance recommends Vulnerability Assessments be performed at least quarterly. This Penetration Test report is not a guarantee of any regulatory compliance or security of the entire network, as security is a continual process.

CyberGuard Compliance is only able to test hosts, workstations, and web applications that are within the defined scope, powered on, attached to the network, and accessible during the testing. CyberGuard Compliance is not responsible for validating every host within scope has been tested. This must be done by the Client as CyberGuard Compliance is often provided with network segments or ranges without specific host details. CyberGuard Compliance is not responsible for any breaches the Client experiences as security testing is only one component of developing and maintaining a secure environment.

CyberGuard Compliance is providing recommendations, which may not have been thoroughly evaluated for functionality, business feasibility, or system stability (including network performance). Before the implementation of any recommendation provided via this documentation or discussions, it is advised that a thorough test of the functionality, associated security implications, and the risk/benefit ratio be assessed in a non-production environment. As with most security implementations, when increasing security, system performance usually decreases as does the ease of use. However, with good security design and architecture, these reductions can be minimized while providing an environment for new services utilizing security as a business-enabling tool.

Table of Contents

Disclaimer.....	3
Table of Figures.....	6
Executive Summary.....	7
Recommendations	8
Remediation Recommendations	8
Cybersecurity Testing and Training Recommendations	8
Security Patch Management Findings and Recommendations	8
Configuration Management Findings and Recommendations	8
Scope.....	9
Penetration Test Results	10
External Network(s) and System(s) Penetration Test Results	10
Summary of External - Weaknesses (Critical to Medium Severity)	11
External Network Penetration Test Results Summary.....	12
Externally Exploited Assets	12
Internal Network(s) and System(s) Penetration Test Results.....	13
Summary of Internal - Weaknesses (Critical to Medium Severity).....	14
Internal Penetration Test Results Summary	15
Internally Exploited Assets.....	15
Web Application Test Results	16
Summary Results - i21.....	16
Summary of Web Application - Weaknesses (Critical to Medium Severity) - i21.....	17
Web Application Exploitations - i21.....	17
High Risk Weaknesses - i21	18
API Test Results.....	19
Summary Results - i21 API	19
Summary of Web Application - Weaknesses (Critical to Medium Severity) - i21 API	20
Web Application Exploitations - i21 API	20
High Risk Weaknesses - i21 API.....	20
Appendix A: Weakness Severity Levels.....	21
Weakness Severity Description.....	21

Appendix B: Penetration Methodology	22
Penetration Testing Lifecycle	22
Discover.....	23
Organize Assets.....	23
Assess.....	23
Develop Attack Plan	24
Penetration Testing.....	24
Reporting.....	24
Remediation.....	24
Appendix C: Glossary of Terms	25
Appendix D: References.....	26

Table of Figures

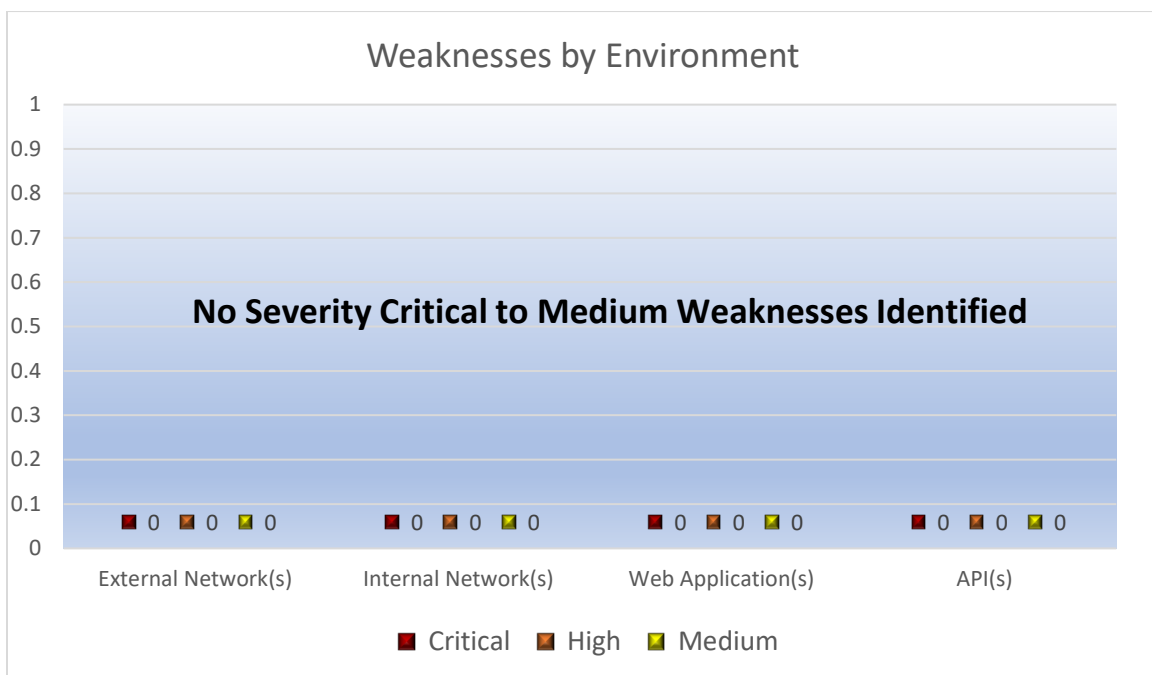
Figure 1 – Network(s) and System(s) In-Scope	9
Figure 2 – Network(s) and System(s) Out-of-Scope.....	9
Figure 3 – Web Application(s) In-Scope.....	9
Figure 4 – External Network(s) and System(s) - Weaknesses by Severity	10
Figure 5 – Externally Exploited Assets	12
Figure 6 – Internal Network(s) and System(s) - Vulnerabilities by Severity	13
Figure 8 – Internally Exploited Assets	15
Figure 8 – Web Application Testing Parameters - i21.....	16
Figure 9 – Web Application Weaknesses by Severity - i21	16
Figure 10 – Web Application Testing Parameters - i21 API	19
Figure 11 – Web Application Weaknesses by Severity - i21 API.....	19

Executive Summary

CyberGuard Compliance has completed a comprehensive Penetration Test for iRely (“iRely”, “Company”, or “Client”) to evaluate the design and adequacy of its current cybersecurity controls. Testing was performed at a threat level equivalent to an experienced hacker without malicious intent or impact. For this Penetration Test, CyberGuard Compliance performed the following services:

- ◆ External and Internal Network and Systems Penetration Testing
- ◆ Web Application Testing

CyberGuard Compliance performed Penetration Testing according to the scoping section of this document. The following is a summary of the identified Critical, High, and Medium severity weaknesses discovered during the Penetration Test:



A series of exploitation attempts were performed on all assets within the scope of this engagement. The goals of the exploitation attempts are to attempt to gain access and elevate access to the network and systems. The following is a summary of assets exploited during the Penetration Test:

Testing Area	Assets Exploited
External Network(s) and System(s)	0
Internal Network(s) and System(s)	0
Web Application(s)	0
Total	0

Any exploited assets are detailed in the report below including exploit steps, evidence of exploit, and remediation guidance.

Recommendations

Remediation Recommendations

CyberGuard Compliance recommends remediating any exploited weaknesses that are of Critical severity within 30 days, High severity within 60 days, and Medium severity within 90 days.

Cybersecurity Testing and Training Recommendations

Based on industry best practices and well-established compliance frameworks, CyberGuard Compliance recommends, at a minimum, iRely perform the following:

- ◆ External and internal network and systems penetration testing should be performed at least annually and when major changes to the environment are introduced.
- ◆ External and internal vulnerability scanning should be performed at least quarterly between penetration tests to ensure new vulnerabilities are identified and addressed in a timely manner to maintain the security posture of the organization.
- ◆ Credentialed web application and API testing using dynamic code analysis should be performed at least annually and before major code releases into production.
- ◆ Security Awareness Training program implemented that is required at hire and at least annually for all employees and contractors.

Security Patch Management Findings and Recommendations

Missing security patches are a leading cause of security breaches. Security Patch Management is a strategy for managing security patches or upgrades for software applications and technologies. CyberGuard Compliance has determined that iRely appears to have a strong Security Patch Management program based on the results of our assessment.

Configuration Management Findings and Recommendations

Configuration Management is a strategy for defining a security configuration standard and managing software applications and technologies to that standard. CyberGuard Compliance has determined that iRely appears to have a strong Configuration Management program based on the results of our assessment.

Scope

The scope for this Penetration Test is limited to the Client’s network(s) and system(s) listed below. All other networks, devices, servers, and web applications hosted externally or internally for the Client are specifically outside the scope of this engagement and were not tested. CyberGuard Compliance only tested devices that were within this scope, powered on, attached to the in-scope network(s), and accessible during the assessment. Amazon AWS does not permit testing of Small, Micro, and Nano instances. CyberGuard Compliance, if applicable, did not test these assets in accordance with Amazon AWS Customer Support Policy for Penetration Testing.

IP Address / Range	Type	Description	Estimated Active Hosts within Range	Time Range When Assets Available
20.221.209.24	External	Typical customer install for i21	1	24/7
10.0.1.4	Internal	Typical customer install for i21	1	24/7
74.208.26.189	External	PowerBI Test Server (internal)	1	24/7
74.208.26.189	Internal	PowerBI Test Server (internal)	1	24/7

Figure 1 – Network(s) and System(s) In-Scope

IP Address / Range	Type	Description	Out of Scope Reason
Not Applicable	Not Applicable	Not Applicable	Not Applicable

Figure 2 – Network(s) and System(s) Out-of-Scope

Web Application Name	Target URL	Credentials
i21	https://irelypentesting.irelyapp.com/iRelyProd	Client Provided Securely
i21 API	https://irelypentesting.irelyapp.com/irelyapi	Client Provided Securely

Figure 3 – Web Application(s) In-Scope

Penetration Test Results

External Network(s) and System(s) Penetration Test Results

Reconnaissance of the External environment was performed, and two (2) active hosts were identified. Reconnaissance data was leveraged to develop an attack plan. During the attack phase of the penetration test all new findings were utilized to adjust the attack plan for deeper penetration. The following weaknesses by severity were identified:

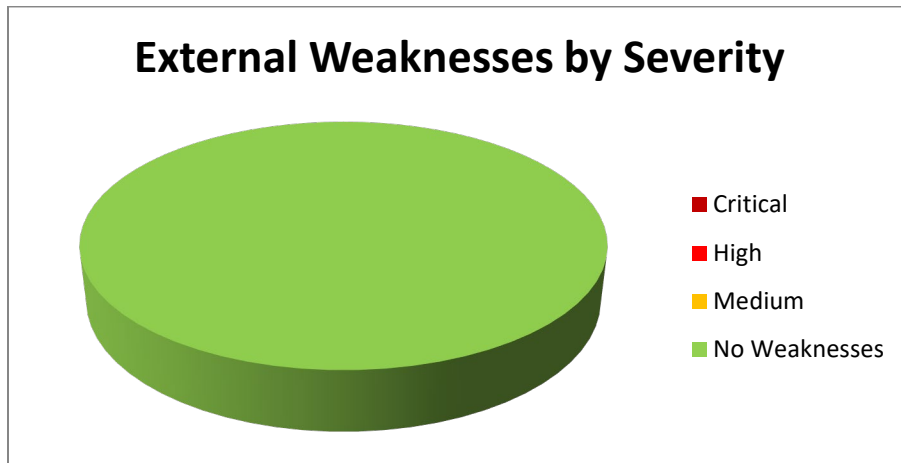


Figure 4 – External Network(s) and System(s) - Weaknesses by Severity

CyberGuard Compliance leverages industry best practices and well-established compliance standards with a focus on Critical, High, and Medium severity weaknesses. CyberGuard Compliance advises the Client to follow the remediation guidance provided in the *Recommendations* section of this document. Below is a summary of the Critical, High, and Medium severity weaknesses identified during the Penetration Test.

Summary of External - Weaknesses (Critical to Medium Severity)

Severity	Weakness	Description	Weakness Instances
			Total Active Count
None			

External Network Penetration Test Results Summary

CyberGuard Compliance performed penetration testing against the firewall and assets with the Client’s protection systems fully active. The penetration test consisted of modules and tools that were specifically selected for the identified hosts. The modules and tools are designed to simulate the actions of an actual hacker with the knowledge gained during the reconnaissance phase. The modules and tools are specifically selected during the design of the attack plan based on the footprint of each host within scope. *Figure 6 – Externally Exploited* is a summary of assets exploited during the penetration testing.

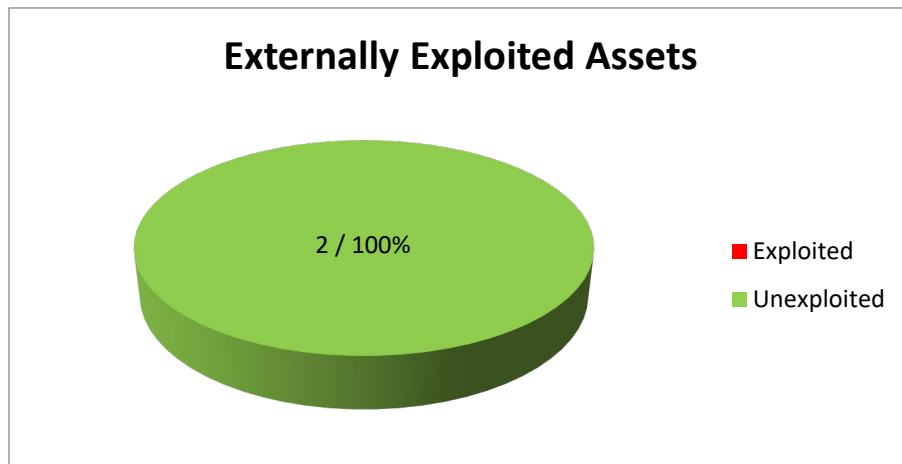


Figure 5 – Externally Exploited Assets

Externally Exploited Assets

Weakness	Not Applicable		
Severity	Not Applicable		
Description	Not Applicable		
Assets Exploited	Not Applicable		
Exploitation Method	Not Applicable		
Additional Attacks	Not Applicable		
Remediation Guidance	Not Applicable		
Exploitation Evidence Listed Below			
Not Applicable			

Internal Network(s) and System(s) Penetration Test Results

Reconnaissance of the Internal environment was performed, and one (1) active host was identified. Reconnaissance data was leveraged to develop an attack plan. During the attack phase of the penetration test all new findings were utilized to adjust the attack plan for deeper penetration. The following weaknesses by severity were identified:

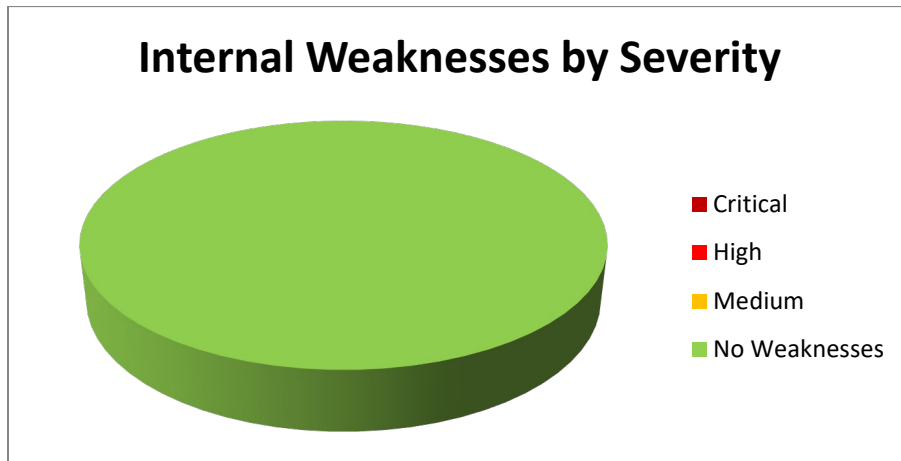


Figure 6 – Internal Network(s) and System(s) - Vulnerabilities by Severity

CyberGuard Compliance leverages industry best practices and well-established compliance standards with a focus on Critical, High, and Medium severity weaknesses. CyberGuard Compliance advises the Client to follow the remediation guidance provided in the *Recommendations* section of this document. Below is a summary of the Critical, High, and Medium severity weaknesses identified during the Penetration Test

Summary of Internal - Weaknesses (Critical to Medium Severity)

Severity	Weakness	Description	Weakness Instances
			Total Active Count
None			

Internal Penetration Test Results Summary

CyberGuard Compliance performed penetration testing against the configuration of the firewall and assets with the testing environment whitelisted on the Client’s protection systems. The penetration test consisted of modules and tools that were specifically selected for the identified hosts. The modules and tools are designed to simulate the actions of an actual hacker with the knowledge gained during the reconnaissance phase. The modules and tools are specifically selected during the design of the attack plan based on the footprint of each host within scope. *Figure 8 – Internally Exploited Assets* is a summary of assets exploited during the penetration testing.

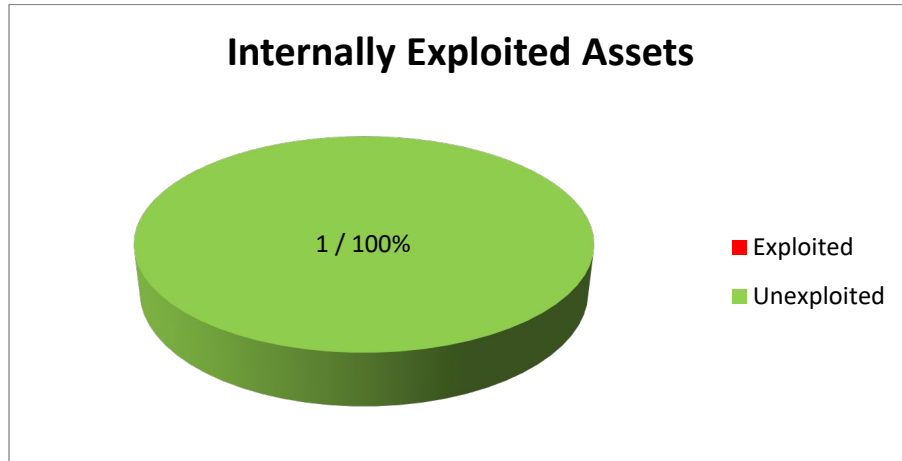


Figure 7 – Internally Exploited Assets

Internally Exploited Assets

Weakness	Not Applicable		
Severity	Not Applicable		
Description	Not Applicable		
Assets Exploited	Not Applicable		
Exploitation Method	Not Applicable		
Additional Attacks	Not Applicable		
Remediation Guidance	Not Applicable		
Exploitation Evidence Listed Below			
Not Applicable			

Web Application Test Results

CyberGuard Compliance leverages many different tools to perform web application testing along with manual testing methods. Each URL tested within this report is scanned to detect every accessible web page and web service. Credentialed testing allows access to a larger set of web pages and services. Non-credentialed testing limits access to boundary web pages and services. Access to the source code is not required with our proprietary methodology and there is no agent that needs to be installed. Once the entire website and all services are mapped, a scan is performed to identify any weaknesses.

Weakness identification can be performed on any custom or modern application platform including, but not limited to, HTML 5, .NET, Ruby on Rails, PHP, jQuery, JavaScript, and countless others. Regardless of the technology the website is built on, our proprietary methodology will scan the site and identify weaknesses. Weaknesses are then exploited using safe read only methods, which generates proof of exploitation. Proof of exploitation confirms the identified weaknesses and eliminates false positives.

Summary Results - i21

Target URL	https://irelypentesting.irelyapp.com/iRelyProd
Policy	iRely Custom
Scope	Limit at or below URL hostname
Initiated Date	04/26/23
Authentication	Selenium Script
Testing Type	Dynamic Code Analysis

Figure 8 – Web Application Testing Parameters - i21

A web application test of the above web application was performed. The web application test identified the following zero (0) web application weaknesses:

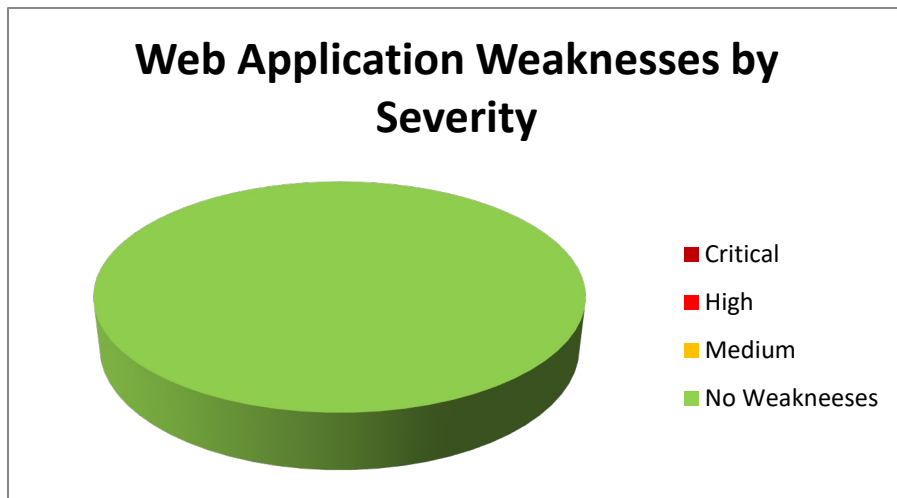


Figure 9 – Web Application Weaknesses by Severity - i21

CyberGuard Compliance leverages industry best practices and well-established compliance standards with a focus on Critical, High, and Medium severity weaknesses. CyberGuard Compliance advises the Client to follow the remediation guidance provided in the *Recommendations* section of this document. Below is a summary of the Critical, High, and Medium severity weaknesses identified during the Penetration Test.

Summary of Web Application - Weaknesses (Critical to Medium Severity) - i21

Severity	Weakness	Description	Weakness Instances
			Total Active Count
None			

Web Application Exploitations - i21

Weakness	None
Severity	None
Threat	None
Impact	None
Detection Parameters	None
Access Path:	None
Additional Attacks	Not Applicable
Remediation Guidance	Not Applicable
Exploitation Evidence Listed Below	
Not Applicable	

High Risk Weaknesses - i21

Weakness	None
Severity	None
Threat	None
Impact	None
Detection Parameters	None
Access Path:	None
Remediation Guidance	Not Applicable

API Test Results

CyberGuard Compliance incorporates several automated tools to perform API testing along with manual testing methods. These tools support various API platforms including SOAP and REST API's. Each API tested within this report is scanned to detect every accessible API call. Access to the source code is not required with our proprietary dynamic code analysis methodology and there is no agent that needs to be installed. Once the API call sets are mapped, testing is performed to identify any vulnerabilities.

API testing was performed on thirty-eight (38) endpoints of the Open Deal Exchange API environment. The API testing identified no application related vulnerabilities:

Summary Results - i21 API

Target URL	https://irelypentesting.irelyapp.com/irelyapi
Policy	iRely Custom
Scope	Limit at or below URL hostname
Initiated Date	02/28/23
Authentication	Selenium Script
Testing Type	Dynamic Code Analysis

Figure 10 – Web Application Testing Parameters - i21 API

A web application test of the above web application was performed. The web application test identified the following zero (0) web application weaknesses:

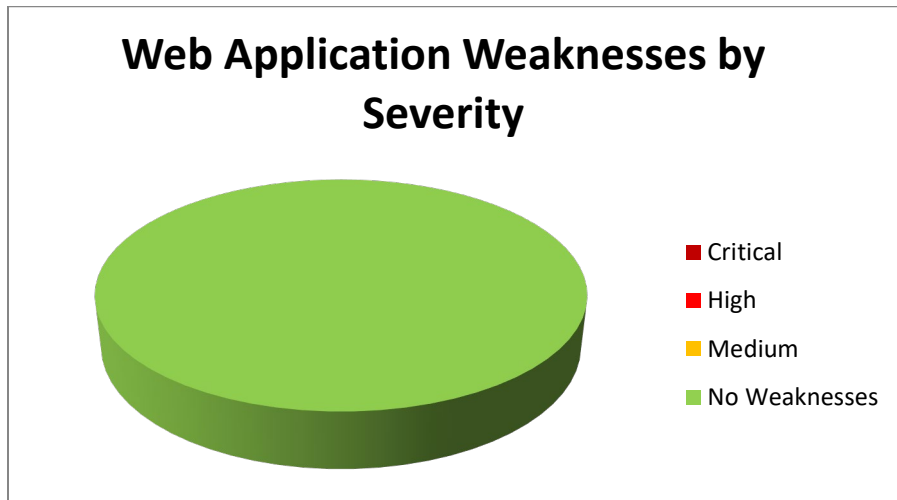


Figure 11 – Web Application Weaknesses by Severity - i21 API

CyberGuard Compliance leverages industry best practices and well-established compliance standards with a focus on Critical, High, and Medium severity weaknesses. CyberGuard Compliance advises the Client to follow the remediation guidance provided in the *Recommendations* section of this document. Below is a summary of the Critical, High, and Medium severity weaknesses identified during the Penetration Test.

Summary of Web Application - Weaknesses (Critical to Medium Severity) - i21 API

Severity	Weakness	Description	Weakness Instances
			Total Active Count
None			

Web Application Exploitations - i21 API

Weakness	None
Severity	None
Threat	None
Impact	None
Detection Parameters	None
Access Path:	None
Additional Attacks	Not Applicable
Remediation Guidance	Not Applicable
Exploitation Evidence Listed Below	
Not Applicable	

High Risk Weaknesses - i21 API

Weakness	None
Severity	None
Threat	None
Impact	None
Detection Parameters	None
Access Path:	None
Remediation Guidance	Not Applicable

Appendix A: Weakness Severity Levels

Weakness Severity Description

CyberGuard Compliance assigns every weakness a severity level, which is determined by the security risk associated with its exploitation. The possible consequences related to each weakness severity level are described below. The guidance below is followed for all weaknesses. In addition to this broad guidance, the service also takes into consideration factors like complexity of the exploit and likelihood of the exploit to work under normal conditions.

Severity	Description
Critical	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, weaknesses at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
High	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, weaknesses at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
Medium	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, weaknesses at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Appendix B: Penetration Methodology

This test used a set of specialized methodologies derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) (“NIST SP 800-115”) - “Technical Guide to Information Security Testing and Assessment”, the Open-Source Security Testing Methodology Manual (“OSSTMM”) – authored by the Institute for Security and Open Methodologies (“ISECON”), and the Open Web Application Security Project (“OWASP”) testing methodologies. These methodologies were then augmented by CyberGuard Compliance proprietary Penetration Testing Methodology.

Penetration Testing Lifecycle



Discover

The first pass in discovering assets within the scope of this engagement is to perform DNS Reconnaissance using industry standard tool such as:

- Domain Lookup <whois> (identifies DNS servers)
- DNS Zone Transfer (collects host records from DNS database)
- DNS Brute Force
- Reverse DNS Lookups (based on IPs already discovered/known)

The DNS Reconnaissance provides a preliminary mapping of the Information System environment that is not comprehensive enough to provide a detailed Penetration Test. A second pass in discovering assets is required to gain more details to the environment. A live host sweep is performed using ICMP, TCP, and UDP probes. The live host sweep completes the discovery mapping picture and provide an overall view of the assets within the scope of the Penetration Test.

Discovery Mapping is the foundation for proper asset management as it identifies known asset within scope and unknown assets. Unknown assets or rogue assets can range from assets that were not properly decommissioned, test assets, or malicious assets that are not owned by the organization. The Discover phase of the Penetration Testing Lifecycle is used to confirm the scope of the Penetration Test.

Organize Assets

Once the scope of the Penetration Testing has been confirmed the assets are organized within CyberGuard Compliance's system based on the organization, asset type, priority or criticality, geographic location, and operating system. These groups or organizational methods are used to track the assets within the Penetration Test and provide a deeper level of reporting over time.

Assess

The assets are assessed using an inference-based scanning engine that intelligently launches modules specific to each unique host that provides for optimal performance and accuracy. The modules are responsible for collecting data from the hosts. Modules are launched based on information collected during the Discover and Organize Assets phases of the Vulnerability Management Lifecycle. Hundreds of modules can coexist during a single scan to collect information about operating systems, open ports, active services, and installed applications. Weaknesses are detected using template-based weakness signatures. The tests for almost all detections are active, but non-intrusive. Specially crafted requests are initiated to distinguish between patched and un-patched versions.

Develop Attack Plan

The assessment step provides key details about each host and its weaknesses. This information is used to develop an attack plan that focuses the maximum amount of effort on critical systems with weaknesses that can be exploited. Hosts with no known weaknesses are given lower priority but are still examined manually to confirm there is no possibility of manual exploitation. Our Attack Plans are meticulously created so we have the highest probability for penetrating the hosts and expanding our attack plan.

Penetration Testing

Our security experts start each Penetration Test by reviewing the Attack Plan to ensure it is fully understood and to determine if additional steps can be added to the plan for maximum attack. The attack plan is followed much like a roadmap until an exploit occurs. Once an exploit occurs the attack plan is revisited to determine if further updates, based on the exploit, are needed to fully expand the attack plan. At each step of the penetration testing the security team documents their efforts, collects evidence, documents remediation recommendations, and ensures a proper audit trail for the entire test.

Reporting

A report is created for each host identified as “active” within the scope of the Penetration Test. The report contains the details about weaknesses. The details can include the severity and classification of the weakness, a description of the threat, information related to the impact of the weakness, information related to a solution for the weakness, any compliance related information, a description of any exploit that exists for the weakness, and other technical details related to the weakness.

Remediation

It is industry best practice and our recommendation to remediate weaknesses identified in this Penetration Testing Report by Severity Level. Weaknesses that have been exploited are the highest priority and should be remediated immediately. Weaknesses that have not been exploited but have been identified as security impacting should be addressed next as they pose a high risk to the organization.

Appendix C: Glossary of Terms

CVE	Common Vulnerabilities and Exposures is a dictionary of common names for publicly known information security vulnerabilities.
DNS	The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.
Exploit	An exploit is the use of software, data, or commands that exploit a vulnerability in a computer system or program to carry out some form of malicious intent.
Host	A network host is a computer or other device connected to a computer network.
IP	An Internet Protocol address (IP address) is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.
Penetration Test	A penetration test is an attempt to evaluate the security of an IT infrastructure by safely performing exploits on identified vulnerabilities within the infrastructure.
Risk Tolerance	An organization's limit for risk, that is, how far an organization is willing to go about accepting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
Rules of Engagement (ROE)	The ROE defines how the testing is to be performed in a Penetration Test.
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.
Ubuntu	Ubuntu is a Debian-based Linux operating system.
Vulnerability/Weakness	A vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.
Vulnerability Assessment	A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer network or communications infrastructure.

Appendix D: References

FIPS 140-2 – “Security Requirements for Cryptographic Modules” -

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

NIST SP 800-39 – “Managing Information Security Risk” -

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

NIST SP 800-115 – “Technical Guide to Information Security Testing and Assessment” -

<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

OSSTMM - <http://www.isecom.org/research/osstmm.html>

OWASP - https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf