Penetration Test
Final Report

April 30, 2024

Prepared By:

Richard Handley

Manager, Cybersecurity

This document contains proprietary and confidential information of CyberGuard Compliance, LLP. ("CyberGuard Compliance") and highly sensitive confidential information of iRely. This document may not be distributed by the recipient without the express permission of CyberGuard Compliance.

Testing Information

Client:	iRely	
Test Type:	Annual	
Purpose:	Web Application Test	
Engagement Dates:	Testing Dates:	04/09/24 to 04/19/24
	Reporting:	04/19/24 to 04/30/24
	Retest Dates:	08/17/24 to 08/19/24
	Reporting:	08/19/24
Active Assets:	Web Application	Total
	1	1
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

Table of Figures

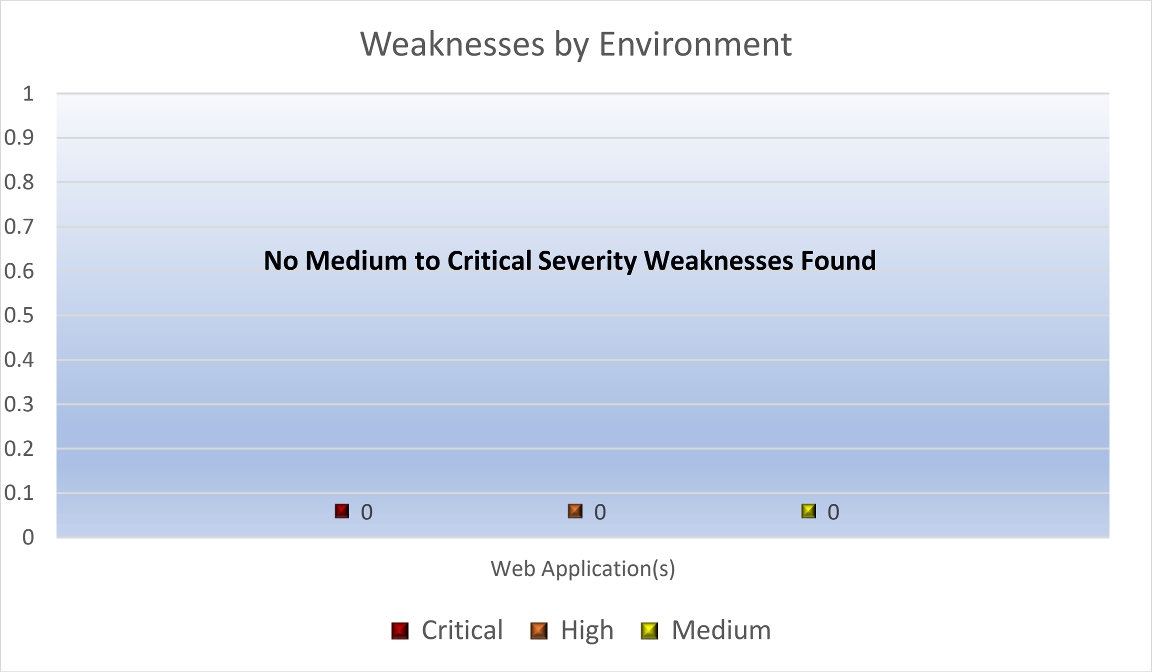
This document contains proprietary and confidential information of CyberGuard Compliance, LLP. ("CyberGuard Compliance") and highly sensitive confidential information of iRely. This document may not be distributed by the recipient without the express permission of CyberGuard Compliance.

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:

- 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
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 does have missing security patches and should review their Security Patch Management program to ensure security patches are applied in a timely manner.

Configuration Management Findings and Recommendations

Applications and technologies that are not configured securely are another leading cause of security breach. 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 does have configuration related weaknesses and should review their Configuration Management program to ensure applications and technologies are configured securely.

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.

Web Application Name	Target URL	Credentials
i21	https://pentesting.irelyapp.com/PenTesting	Client Provided Securely
Modules Tested in Depth:	**Dashboard** • https://pentesting.irelyapp.com/PenTesting/#menu/DB • https://pentesting.irelyapp.com/PenTesting/#/DB/TabSetup?menuId=160&moduleMenuId=156 • https://pentesting.irelyapp.com/PenTesting/#/DB/Connection?menuId=162&moduleMenuId=156 • https://pentesting.irelyapp.com/PenTesting/#/DB/PanelSettings?showSearch=true&menuId=161&moduleMenuId=156 **System Manager** • https://pentesting.irelyapp.com/PenTesting/#menu/SM • https://pentesting.irelyapp.com/PenTesting/#/SM/EntityUser?showSearch=true&menuId=2&moduleMenuId=1 • https://pentesting.irelyapp.com/PenTesting/#/SM/UserRole?showSearch=true&menuId=3&moduleMenuId=1 • https://pentesting.irelyapp.com/PenTesting/#/SM/PortalRole?showSearch=true&menuId=170&moduleMenuId=1 • https://pentesting.irelyapp.com/PenTesting/#/SM/SecurityPolicy?showSearch=true&menuId=171&moduleMenuId=1 • https://pentesting.irelyapp.com/PenTesting/#/SM/CompanyPreference/SystemManager?menuId=6&moduleMenuId=1 • https://pentesting.irelyapp.com/PenTesting/#/SM/LockedRecord?menuId=172&moduleMenuId=1	

- https://pentesting.irelyapp.com/PenTesting/#/SM/EntityUser?action=new&menuId=184&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/ScreenDesigner?showSearch=true&menuId=173&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/FileFieldMapping?showSearch=true&menuId=174&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/LanguageTranslation?showSearch=true&menuId=179&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/Language?menuId=175&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/Letters?showSearch=true&menuId=176&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/ReportLabels?showSearch=true&menuId=177&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/ScreenLabel?menuId=178&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/StartingNumbers?menuId=7&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/CRM/CustomerLicense?showSearch=true&searchCommand=CustomerLicense&menuId=188&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/License?showSearch=true&menuId=186&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/LicenseType?menuId=187&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/AnnouncementType?menuId=181&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/Announcement?menuId=180&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/RapidDeployment?strModule=System%20Manager&menuId=189&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/FileDownloads?menuId=182&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/OriginConversion?menuId=11&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/SM/PerformanceRuntimeLogReport?showSearch=true&menuId=183&moduleMenuId=1

Common Info

- https://pentesting.irelyapp.com/PenTesting/#menu/CI

- https://pentesting.irelyapp.com/PenTesting/#/SM/CompanyLocation?showSearch=true&menuId=197&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/RecurringTransaction?menuId=198&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/BatchPosting?menuId=199&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Calendar?menuId=200&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/NotificationList?menuId=219&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Currency?menuId=16&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/CurrencyExchangeRate?menuId=201&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/CurrencyExchangeRateType?menuId=202&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/OnlineUsers?menuId=221&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/ApprovalList?showSearch=true&menuId=215&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Approval?menuId=212&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/ApproverConfiguration?showSearch=true&menuId=213&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/ApproverGroup?showSearch=true&menuId=214&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/FreightTerm?showSearch=true&menuId=204&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/GeographicalZone?menuId=210&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/LineOfBusiness?menuId=205&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Country?showSearch=true&menuId=14&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/AR/MarketZone?menuId=137&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/PaymentMethod?menuId=18&moduleMenuId=13

- https://pentesting.irelyapp.com/PenTesting/#/SM/PurchasingGroup?menuId=206&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/RecentlyViewedList?menuId=220&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/DocumentMaintenance?showSearch=true&menuId=207&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Term?showSearch=true&menuId=19&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Territory?menuId=211&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/Truck?showSearch=true&menuId=208&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/AuditLogHistory?menuId=229&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/EmailHistory?showSearch=true&menuId=230&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/ExportLog?menuId=231&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/EM/EntityGroup?showSearch=true&menuId=222&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/AR/EntitySalesperson?showSearch=true&menuId=223&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/EntityShipVia?showSearch=true&menuId=224&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/EM/EntityVeterinary?showSearch=true&menuId=225&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/TaxClass?menuId=216&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/TaxCode?showSearch=true&menuId=217&moduleMenuId=13
- https://pentesting.irelyapp.com/PenTesting/#/SM/TaxGroup?showSearch=true&menuId=218&moduleMenuId=13

Scheduling

- https://pentesting.irelyapp.com/PenTesting/#menu/SCH

This document contains proprietary and confidential information of CyberGuard Compliance, LLP. ("CyberGuard Compliance") and highly sensitive confidential information of iRely. This document may not be distributed by the recipient without the express permission of CyberGuard Compliance.

- https://pentesting.irelyapp.com/PenTesting/#/SCH/ReportDistribution?showSearch=true&menuId=1044&moduleMenuId=1042
- https://pentesting.irelyapp.com/PenTesting/#/SCH/ReportDistributionGroup?showSearch=true&menuId=1046&moduleMenuId=1042
- https://pentesting.irelyapp.com/PenTesting/#/SCH/Schedule?showSearch=true&menuId=1047&moduleMenuId=1042

General Ledger

- https://pentesting.irelyapp.com/PenTesting/#menu/GL
- https://pentesting.irelyapp.com/PenTesting/#/GL/GeneralJournal?showSearch=true&menuId=28&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/GLAccountDetail?showSearch=true&menuId=29&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AuditAdjustment?showSearch=true&menuId=243&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/SM/BatchPosting?module=General%20Ledger&menuId=30&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/RevalueCurrency?showSearch=true&menuId=238&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/Consolidate?menuId=239&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/OriginAuditLog?showSearch=true&menuId=240&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/EliminateEntry?showSearch=true&menuId=241&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AccountMapping?showSearch=true&menuId=242&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/ChangeCategory?showSearch=true&menuId=245&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AccountClone?menuId=43&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/FiscalYear?showSearch=true&menuId=44&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/IntraCompanyConfig?showSearch=true&menuId=244&moduleMenuId=26

- https://pentesting.irelyapp.com/PenTesting/#/GL/Ledger?showSearch=true&menuId=246&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/Reallocation?showSearch=true&menuId=46&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/SM/RecurringTransaction?type=General%20Journal&menuId=47&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AccountStructure?menuId=38&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/BuildAccounts?menuId=41&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/ChartOfAccounts?menuId=37&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/SM/RapidDeployment?strModule=System%20Manager&menuId=189&moduleMenuId=1
- https://pentesting.irelyapp.com/PenTesting/#/GL/SegmentAccounts?menuId=40&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/ImportLogs?showSearch=true&menuId=35&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/ImportFromCSV?menuId=34&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AccountGroup?showSearch=true&menuId=250&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AuditorTransactionsByAccountId?menuId=1147&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/AuditorTransactionsByTransactionId?menuId=1148&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/OutOfBalanceReport?showSearch=true&menuId=248&moduleMenuId=26
- https://pentesting.irelyapp.com/PenTesting/#/GL/TrialBalanceReport?showSearch=true&menuId=249&moduleMenuId=26

Financial Reports

- https://pentesting.irelyapp.com/PenTesting/#menu/FRD
- https://pentesting.irelyapp.com/PenTesting/#/FRD/FinancialReports?menuId=50&moduleMenuId=49

- https://pentesting.irelyapp.com/PenTesting/#/FRD/FinancialReportsGenerator?menuId=51&moduleMenuId=49
- https://pentesting.irelyapp.com/PenTesting/#/FRD/Budget?showSearch=true&menuId=257&moduleMenuId=49
- https://pentesting.irelyapp.com/PenTesting/#/FRD/ReportBuilder?showSearch=true&menuId=55&moduleMenuId=49
- https://pentesting.irelyapp.com/PenTesting/#/FRD/FinancialReportGroup?showSearch=true&menuId=258&moduleMenuId=49
- https://pentesting.irelyapp.com/PenTesting/#/FRD/ReportHierarchy?showSearch=true&menuId=259&moduleMenuId=49
- https://pentesting.irelyapp.com/PenTesting/#/FRD/Templates?menuId=56&moduleMenuId=49

Figure 1 – Web Application(s) In-Scope

Penetration Test Results

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, HTM 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

Target URL	https://pentesting.irelyapp.com/PenTesting
Policy	iRely Custom Policy
Scope	Limit at or below URL hostname
Initiated Date	04/17/24
Authentication	Selenium Script
Testing Type	Dynamic Code Analysis

Figure 2 – Web Application Testing Parameters

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

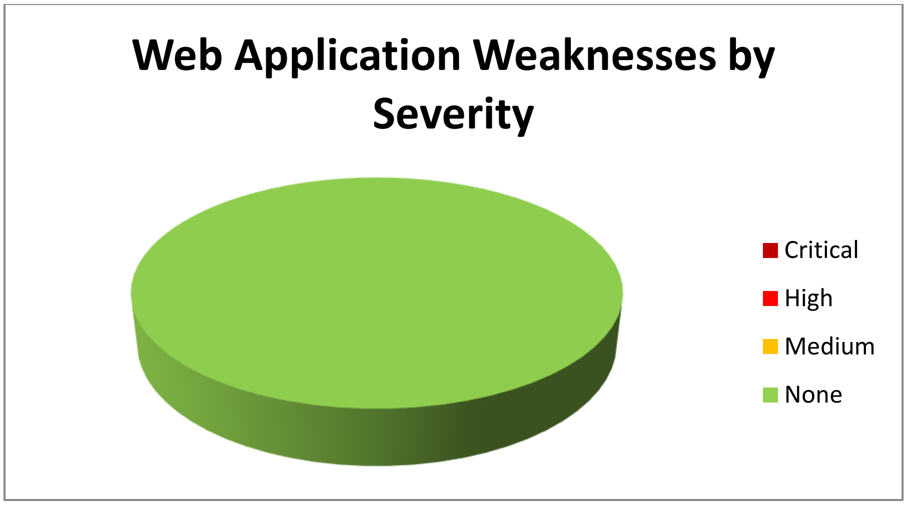


Figure 3 – Web Application Weaknesses by Severity

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 Web Application - Weaknesses (Critical to Medium Severity)

Severity	Weakness	Description	Weakness Instances
			Total Active Count
None			

Web Application Exploitations

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	

This document contains proprietary and confidential information of CyberGuard Compliance, LLP. ("CyberGuard Compliance") and highly sensitive confidential information of iRely. This document may not be distributed by the recipient without the express permission of CyberGuard Compliance.

Web Application High Risk Weaknesses

Weakness	Not Applicable
Severity	**Not Applicable**
Threat	Not Applicable
Impact	Not Applicable
Remediation Guidance	Not Applicable
Detection Parameters	Not Applicable
Access Path:	Not Applicable
Request:	Not Applicable
Response:	Not Applicable

Appendix A: Weakness Severity Levels

Weakness Severity Description

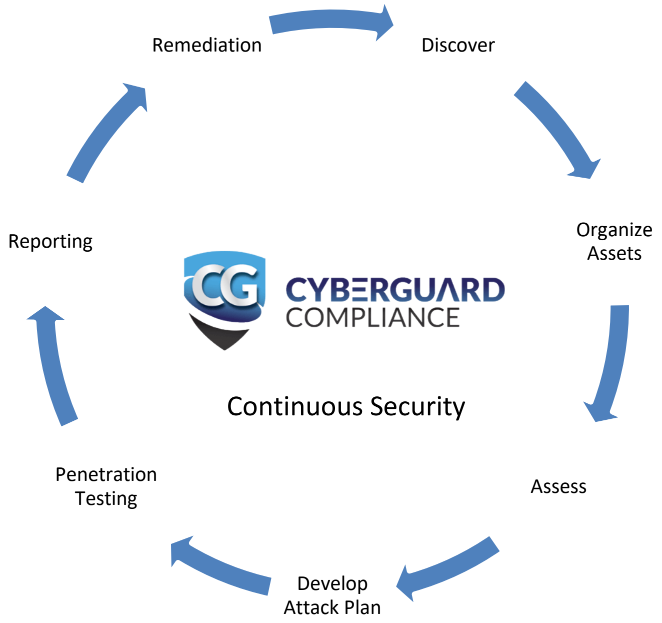
CyberGuard Compliance assigns every weakness a severity level, which is determined by the security risk associated with its exploitation. The possible consequences related to each weakness severity level are described below. The guidance below is followed for all weaknesses. In addition to this broad 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



This document contains proprietary and confidential information of CyberGuard Compliance, LLP. ("CyberGuard Compliance") and highly sensitive confidential information of iRely. This document may not be distributed by the recipient without the express permission of CyberGuard Compliance.

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 is 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