{{ project.name }}

# 1.0 Penetration Test Report

## 1.1 Introduction

This penetration test report contains all efforts that were conducted to test Robert Half’s public ip space (can be found at the appendix A) publicly accessible RobertHalf subdomains, and perimeter internet facing web applications. Sub domains and virtual host routed sites were enumerated with OSINT tools and then tested against. The purpose of this report is to explain what the Security Analyst has exploited with the full understanding of penetration testing methodologies as well as the technical knowledge to test the effectiveness of the people, processes and technology of Robert Half’s current security posture.

## 1.2 Objective

The objective of this assessment is to perform a penetration test against Robert Half’s public ip space, publicly accessible Robert Half subdomains, and internet facing web applications. The Rules of Engagement (ROE) were to do recon, and limited exploits that would not impact or interrupt services on the site and assess recommended remediation if any are deemed necessary. Owner of shunning system would be contacted and a temporary whitelisting rule for the shunned system would be requested Any sensitive data discovered will be noted, but not exfiltrated. Proof of data will be presented in the form of a screen shot with sensitive data redacted if applicable. The Red Team is to showcase how a threat actor could exploit external facing webapps to potentially steal PHI/PII or use the webapp’s security vulnerabilities to gain access to the server.

# 2.0 High-Level Executive Summary

{% for finding in findings %}

1. During our penetration testing, we looked at {{ totals.scope }} different IP addresses
2. We found the following amount of findings: {{ totals.findings }}, those being: {{ finding.title }} from our targets (list can be found in Apendix B)
3. We recommend the following mitigations:

{{p finding.recommendation\_rt}}

{% endfor %}

# 3.0 Findings

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Finding | DESCRIPTION | | |  | MITIGATION | | | Severity |
| {%tr for finding in findings %} | |  |  | | | |  | |
| {{ finding.title }} | {{finding.description|replace(“<p>”,””)|replace(“</p>”,””)}} | | |  | | {{p finding.recommendation\_rt}} | | {% cellbg finding.severity\_color %}{{ finding.severity }}  {{ finding.cvss\_score }} |
| {%tr endfor %} | |  |  | | | |  | |

## 4.0 Recommendations

Robert Half EIS Security Red Team recommends upgrading the affected web applications to respective new versions, patching it to the latest available security update, and looking over permissions and access controls. A review of the web application security patches and updates will potentially prevent an attacker from exploiting these systems in the future.

# 5.0 Methodologies

We utilized a widely adopted approach when performing penetration testing that is effective in testing how well the Robert Half environment is secured. Below is a breakdown of how we were able to exploit various public web applications, and how those things could be utilized for more sophisticated attacks.

## 5.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying an attack surface within the scope of the penetration test. During this phase we quickly scanned the target web application of the as per the Rules Of Engagement (ROE). We crawled for pages and files, looked for attack vectors, and found some potential things we can leverage.

## 5.2 Penetration test

The penetration testing portions of the assessment focus heavily on testing external perimeter for security vulnerabilities and what could be done with those to enable discussion on implementing possible improvements if deemed necessary by Robert Half.

## 4 Appendix A : SCOPE

|  |  |  |
| --- | --- | --- |
| NAME | LIST OF IPS |  |
|  | {%tr for s in scope %} | |
| {{s.name}} | {{s.scope|replace(“’”,””)|replace(“[”,””)|replace(“]”,””)}} | |
|  | {%tr endfor %} | |

## 5 Appendix B : TARGETS

|  |  |  |
| --- | --- | --- |
| IP | DOMAIN |  |
| {%tr for t in targets %} |  | |
| {{t.ip\_address}} | {{t.hostname}} | |
| {%tr endfor %} |  | |