# {{ 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 {{ server.ip\_address }}/20, {{ server.ip\_address }}/20, 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 {{ server.ip\_address }}/{{ server.ip\_address }}/20, 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

1. During our penetration testing, we looked at {{ totals.scope }}
2. We found the following findings: {{ totals.findings }}
3. We thoroughly recommend the following mitigations: {{p finding.recommendation\_rt }}

## 

## 2.1 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.

# 3.0 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.

## 3.1 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.

## 3.2 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.

This template is an example of how Jinja2 variables can be used in a Word template to dynamically drop-in information and generate tables. The following output is based on the Ghostwriter project: {{ client.name }} ({{ client.short\_name }}) {{ project.type }} (generated on {{ report\_date }})

The “raw” (JSON) report will show you the data accessible from your template. Some of this data is chopped-up into smaller bits to make it easy to reassemble in different ways. For example, the project’s start and end dates are accessible as pre-formatted dates based on your date format configuration:

{{ project.start\_date }} – {{ project.end\_date }}

Perhaps you want to reference only pieces (e.g., day, month, and year) of these dates to present them in different ways. Here is one option for dynamically assembling a date range:

{% if project.start\_year == project.end\_year %}{% if project.start\_month == project.end\_month %}{{ project.start\_month }} {{ project.start\_day }}–{{ project.end\_day }}, {{ project.end\_year }}{% else %}{{ project.start\_day }} {{ project.start\_month }} to {{ project.end\_day }} {{ project.end\_month }} {{ project.end\_year }}{% endif %}{% else %}{{ project.start\_day }} {{ project.start\_month }} {{ project.end\_year }} to {{ project.end\_day }} {{ project.end\_month }} {{ project.end\_year }}{% endif %}

That looks kind of complicated, but it outputs several different date formats based on the months and years involved. You can add newlines to break-up the statements to make them easier to read. We write Jinja2 statements in one line so we don’t end up with blank lines and extra whitespace.

You can also pull in some pre-calculated values for various parts of your project and perform calculations:

Table 1 – Assessment Results

|  |  |  |
| --- | --- | --- |
| Value | Total | Math |
| **Objectives** | {{ totals.objectives }} |  |
| **Completed Objectives** | {{ totals.objectives\_completed }} | {% if totals.objectives > 0 %}{{ totals.objectives\_completed / totals.objectives }}{% else %}100{% endif %}% |
| **Findings** | {{ totals.findings }} |  |
| **Team Members** | {{ totals.team }} |  |
| **Targeted Hosts** | {{ totals.targets }} |  |
| **Scope** | {{ totals.scope }} |  |

## Assessment Points of Contact & Stakeholders

You can also create tables with loops:

Table 2 – {{ client.name }} Points of Contact

|  |  |  |
| --- | --- | --- |
| Name | Role | Email |
| {%tr for poc in client.contacts %} | | |
| {{ poc.name }} | {{ poc.job\_title }} | {{ poc.email }} |
| {%tr endfor %} | | |

Table 3 – {{ company.name }} Points of Contact

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Email |  |
| {%tr for member in team %} | | | |
| {{ member.name }} | {{ member.role }} | {{ member.email }} | {{ member.phone }} |
| {%tr endfor %} | | | |

Table 4 – Domain Names Used for Assessment Activities

|  |  |
| --- | --- |
| Domain Name | Role |
| {%tr for domain in infrastructure.domains %} | |
| {{ domain.domain }} | {{ domain.activity }} |
| {%tr endfor %} | |

Table 5 – Servers Used for Assessment Activities

|  |  |  |
| --- | --- | --- |
| IP Address | Purpose | Role |
| {%tr for server in infrastructure.servers %} | | |
| {{ server.ip\_address }} | {{ server.activity }} | {{ server.role }} |
| {%tr endfor %} | | |
| {%tr for server in infrastructure.cloud %} | | |
| {{ server.ip\_address }} | {{ server.activity }} | {{ server.role }} |
| {%tr endfor %} | | |

Table 6 – Summary of Findings

|  |  |
| --- | --- |
| Finding | Severity |
| {%tr for finding in findings %} | |
| {{ finding.title }} | {% cellbg finding.severity\_color %}{{ finding.severity }} |
| {%tr endfor %} | |

There are numerous Jinja2 filters available within templates. Ghostwriter also has some custom filters (see the wiki). The above template looks like this with the filter\_severity filter:

|  |  |
| --- | --- |
| Finding | Severity |
| {%tr for finding in findings|filter\_severity([“Critical”, “High”]) %} | |
| {{ finding.title }} | {% cellbg finding.severity\_color %}{{ finding.severity }} |
| {%tr endfor %} | |

Here is that table again with the filter\_type filter:

|  |  |
| --- | --- |
| Finding | Severity |
| {%tr for finding in findings|filter\_type([“Network”, “Web”]) %} | |
| {{ finding.title }} | {% cellbg finding.severity\_color %}{{ finding.severity }} |
| {%tr endfor %} | |

Findings–and some other objects–include special versions of their content called *RichText* objects. These objects have the same name as the normal object with “\_rt” at the end. For example, a finding has a *Description* field that you access with finding.description. There is also a finding.description\_rt version that drops into a Word document fully formatted and styled.

Check the wiki for more and look at the following section.

{% for finding in findings %}

{{ finding.title }}

**Severity – {{ finding.severity\_rt }}**

#### Affected Entities

{{p finding.affected\_entities\_rt }}

#### Description

{{p finding.description\_rt }}

#### Impact

{{p finding.impact\_rt }}

#### Mitigation

{{p finding.recommendation\_rt }}

#### Replication Steps

{{p finding.replication\_steps\_rt }}

#### References

{{p finding.references\_rt }}

{% endfor %}