# VULNERABILITY ASSESSMENT REPORT.

maxPROTECT | maxapex

# Table of Content

# Vulnerability Assessment Report

## Statement of Confidentiality

The contents of this document have been developed by Information Security Team at MaxAPEX Cloud for Client Talal Elsaqqa for finc.app. MaxAPEX Cloud considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Client Talal Elsaqqa. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Client Talal Elsaqqa.

## Engagement Contacts

| Client Contacts | |
|---|---|
| **Primary Contact** | **Primary Contact Email** |
| Talal Elsaqqa | telsaqqa@gmail.com |

| Assessor Contacts | |
|---|---|
| **Primary Contact** | **Primary Contact Email** |
| MaxAPEX Support | support@maxapex.com |

## Scope

The scope of this security assessment was strictly limited to the server identified as: finc.app

Our testing efforts were focused exclusively on evaluating the security posture of this single server, encompassing its system configurations, network services, and associated security protocols.

No other systems, networks, or services outside of this specified server were included in this assessment. The aim was to perform a detailed and focused analysis on finc.app to identify potential vulnerabilities and assess its resilience against security threats.

## Executive Summary

This security assessment report presents the findings from a comprehensive security scan conducted on the server finc.app. The server was assessed for various security vulnerabilities across multiple service vectors.

The assessment identified a total of several vulnerabilities that need attention to mitigate potential risks.

| Risk Assessment | Number of Vulnerability Classes |
|---|---|
| Critical | 3 |
| High | 3 |
| Medium | 0 |
| Low | 0 |
| Informational | 1 |
| Total | 7 |

## Key Findings

### CRITICAL

**OpenSSL Vulnerability:** The installed OpenSSL 1.1.1.x version is no longer supported, so it won't get security updates. Apply the latest January 2026 Critical Patch Units to resolve these issues.

**Oracle Database Server Multiple Vulnerabilities:** The versions of Oracle Database Server installed on the remote host are affected by multiple vulnerabilities as referenced in the January 2026 CPU advisory. Apply the appropriate patch according to the January 2026 Oracle Critical Patch Update advisory.

**Oracle Java SE Multiple Vulnerabilities:** The version of Java installed on the remote host is affected by multiple vulnerabilities as referenced in the January 2026 CPU advisory. Apply the appropriate patch according to the January 2026 Oracle Critical Patch Update advisory.

## HIGH

**Apache Tomcat Vulnerabilities:** The Apache Tomcat installation on the remote host is outdated and affected by multiple vulnerabilities. To resolve this, update to version 9.0.115 or later.

**Apache Commons FileUpload:** The version of Apache Commons FileUpload is affected by a denial of service vulnerability. Update ORDS to the latest stable version.

**RockyLinux 8 kernel:** The Rocky Linux 8 host is affected by multiple kernel vulnerabilities that could affect system stability. Updated kernel packages are installed, but a reboot is required to load the new kernel.

## INFO

**Open Port Detection:** Several externally accessible services were identified during testing. These services increase the exposed attack surface and may provide an attacker with additional entry points for reconnaissance or exploitation.

## Recommendations

Immediate actions are required to address the identified vulnerabilities:

- **Critical Patch Updates:** Apply the latest Critical Patch Updates to mitigate OpenSSL, Oracle Database Server and Oracle Java SE component Vulnerabilities.
- **Reboot the System:** Perform a system reboot to fully apply kernel updates.
- **Update Apache Tomcat:** Update the Apache Tomcat service to version 9.0.115 or later.
- **Update ORDS:** Update to the latest stable ORDS version.
- **Review and manage open ports:** Ensure only necessary services are exposed and accessible and apply IP filtering as needed.

These measures will significantly enhance the security of the server and protect against potential cyber-attacks.

# Detailed Analysis

**Host Information**
DNS Name: finc.app
IP: 37.27.49.243

## Vulnerabilities

## 1. OpenSSL Vulnerability and SEoL

**Synopsis**
An unsupported version of OpenSSL is affected by multiple vulnerabilities.

**Description**
According to its version, OpenSSL is 1.1.1.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

**Solution**
Apply the latest January 2026 CPU for Database and components to resolve these issues.

**Risk Factor**
Critical

**CVSS v3.0 Base Score**
10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

**Proof of Concept**

```
Path : /opt/oracle/product/21c/dbhome_1/python/bin/openssl
Installed version : 1.1.1k
Security End of Life : September 11, 2023
Time since Security End of Life (Est.) : >= 2 years

Path : /opt/oracle/product/21c/dbhome_1/python/lib/libcrypto.so
Installed version : 1.1.1k
Security End of Life : September 11, 2023
Time since Security End of Life (Est.) : >= 2 years

Path : /opt/oracle/product/21c/dbhome_1/python/lib/libcrypto.so.1.1
Installed version : 1.1.1k
Security End of Life : September 11, 2023
Time since Security End of Life (Est.) : >= 2 years
```

```
Path : /opt/oracle/product/21c/dbhome_1/python/lib/libssl.so
Installed version : 1.1.1k
Security End of Life : September 11, 2023
Time since Security End of Life (Est.) : >= 2 years

Path : /opt/oracle/product/21c/dbhome_1/python/lib/libssl.so.1.1
Installed version : 1.1.1k
Security End of Life : September 11, 2023
Time since Security End of Life (Est.) : >= 2 years
```

## 2. Oracle Database Server Multiple Vulnerabilities

**Synopsis**

The remote host is affected by multiple vulnerabilities

**Description**

The versions of Oracle Database Server installed on the remote host are affected by multiple vulnerabilities as referenced in the January 2026 CPU advisory.

- Vulnerability in the Oracle Spatial and Graph (OpenJPEG) component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.0. Easily exploitable vulnerability allows low privileged attacker having None privilege with logon to the infrastructure where Oracle Spatial and Graph (OpenJPEG) executes to compromise Oracle Spatial and Graph (OpenJPEG). Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Spatial and Graph (OpenJPEG). (CVE-2025-54874)

- Vulnerability in the Fleet Patching and Provisioning (Eclipse Jersey) component of Oracle Database Server.
Supported versions that are affected are 23.4.0-23.26.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Fleet Patching and Provisioning (Eclipse Jersey). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Fleet Patching and Provisioning (Eclipse Jersey) accessible data as well as unauthorized access to critical data or complete access to all Fleet Patching and Provisioning (Eclipse Jersey) accessible data. (CVE-2025-12383)

- Vulnerability in the SQLcl component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.0. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where SQLcl executes to compromise SQLcl. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability

can result in takeover of SQLcl. (CVE-2026-21939)

- Vulnerability in the RDBMS (Python) component of Oracle Database Server. Supported versions that are affected are 21.3-21.20 and 23.4.0-23.26.0. Easily exploitable vulnerability allows high privileged attacker having Authenticated User privilege with logon to the infrastructure where RDBMS (Python) executes to compromise RDBMS (Python). Successful attacks of this vulnerability can result in takeover of RDBMS (Python). (CVE-2025-13836, CVE-2025-13837, CVE-2025-6069, CVE-2025-6075, CVE-2025-8194, CVE-2025-8291, CVE-2025-8869)

- Vulnerability in the Oracle Graal Development Kit for Micronaut (Nimbus JOSE+JWT) component of Oracle Database Server. Supported versions that are affected are 19.3-19.29 and 23.4.0-23.26.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Graal Development Kit for Micronaut (Nimbus JOSE+JWT). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Graal Development Kit for Micronaut (Nimbus JOSE+JWT) accessible data as well as unauthorized read access to a subset of Oracle Graal Development Kit for Micronaut (Nimbus JOSE+JWT) accessible data. (CVE-2025-67735)

**Solution**

Apply the appropriate patch according to the January 2026 Oracle Critical Patch Update advisory.

**Risk Factor**

Critical

**CVSS v3.0 Base Score**

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**Proof of Concept**

```
Oracle Home : /opt/oracle/product/21c/dbhome_1
Component : RDBMS
Installed version : 21.0.0.0.0
Fixed version : 21.21.0.0.260120
```

## 3. Oracle Java SE Multiple Vulnerabilities

**Synopsis**

The remote host is affected by multiple vulnerabilities

**Description**

The version of Java installed on the remote host is affected by multiple vulnerabilities as referenced in the January 2026 CPU advisory.

- Vulnerability in Oracle Java SE (component: JavaFX (libxslt)). Supported versions that are affected are Oracle Java SE: 8u471-b50. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Java SE. (CVE-2025-7425)

- Vulnerability in Oracle Java SE (component: JavaFX (WebKitGTK)). Supported versions that are affected are Oracle Java SE: 8u471-b50. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Java SE. (CVE-2025-43368)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. (CVE-2026-21945)

**Solution**

Apply the appropriate patch according to the January 2026 Oracle Critical Patch Update advisory.

**Risk Factor**

Critical

**CVSS v3.0 Base Score**

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**Proof of Concept**

```
Path : /opt/oracle/product/21c/dbhome_1/jdk/
Installed version : 8.0.291.09 / build 8.0.291
Fixed version : Upgrade to version 8.0.481 or greater
```

## 4. Apache Tomcat Vulnerabilities

**Synopsis**

The remote Apache Tomcat server is affected by a vulnerability

**Description**

The version of Tomcat installed on the remote host is prior to 9.0.115. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.115_security-9 advisory.

- Improper Input Validation vulnerability in Apache Tomcat Native, Apache Tomcat. When using an OCSP responder, Tomcat Native (and Tomcat's FFM port of the Tomcat Native code) did not complete verification or freshness checks on the OCSP response which could allow certificate revocation to be bypassed. This issue affects Apache Tomcat Native: from 1.3.0 through 1.3.4, from 2.0.0 through 2.0.11; Apache Tomcat: from 11.0.0-M1 through 11.0.17, from 10.1.0-M7 through 10.1.51, from 9.0.83 through 9.0.114. The following versions were EOL at the time the CVE was created but are known to be affected: from 1.1.23 through 1.1.34, from 1.2.0 through 1.2.39. Older EOL versions are not affected. Apache Tomcat Native users are recommended to upgrade to versions 1.3.5 or later or 2.0.12 or later, which fix the issue. Apache Tomcat users are recommended to upgrade to versions 11.0.18 or later, 10.1.52 or later or 9.0.115 or later which fix the issue. (CVE-2026-24734)

**Solution**

Update to Apache Tomcat version 9.0.115 or later.

**Risk Factor**

High

**CVSS v3.0 Base Score**

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

**Proof of Concept**

```
Path : /opt/tomcat
Installed version : 9.0.106
Fixed version : 9.0.115
```

## 5. Apache Commons FileUpload

**Synopsis**

A package installed on the remote host is affected by a denial of service vulnerability

**Description**

The version of Apache Commons FileUpload on the remote host is 1.6 , 2.0.0-M1 2.0.0-M4. It is, therefore, affected by a denial of service vulnerability due to allocation of resources for multipart headers with insufficient limits.

**Solution**

Since the Apache Commons FileUpload library is bundled within ORDS, update ORDS to the latest stable, supported version to fix the vulnerability.

**Risk Factor**

High

**CVSS v3.0 Base Score**

7.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

**Proof of Concept**

```
Path : /opt/tomcat/webapps/apex/WEB-INF/lib/commons-fileupload-1.4.jar
Installed version : 1.4
Fixed version : 1.6

Path : /opt/tomcat/webapps/dev/WEB-INF/lib/commons-fileupload-1.5.jar
Installed version : 1.5
Fixed version : 1.6
```

## 6. RockyLinux 8 kernel

**Synopsis**

The remote RockyLinux host is missing one or more security updates

**Description**

The remote RockyLinux 8 host has packages installed that are affected by multiple vulnerabilities as referenced in the RLSA-2026:3963 advisory.

- kernel: ipv6: BUG() in pskb_expand_head() as part of calipso_skbuff_setattr() (CVE-2025-71085)
- kernel: macvlan: fix possible UAF in macvlan_forward_source() (CVE-2026-23001)

**Solution**

The necessary kernel packages have already been installed on the host. A server reboot is required to load the newly installed kernel and fully remediate these vulnerabilities.

**Risk Factor**
High

**CVSS v3.0 Base Score**
7.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

**Proof of Concept**

```
Package kernel-4.18.0-553.111.1.el8_10 is installed.
However, according to uname -r, the current running kernel level is 4.18.0-
553.58.1.el8_10.
This system requires a reboot to begin using the patched kernel level.

Package kernel-core-4.18.0-553.111.1.el8_10 is installed.
However, according to uname -r, the current running kernel level is 4.18.0-
553.58.1.el8_10.
This system requires a reboot to begin using the patched kernel level.

Package kernel-modules-4.18.0-553.111.1.el8_10 is installed.
However, according to uname -r, the current running kernel level is 4.18.0-
553.58.1.el8_10.
This system requires a reboot to begin using the patched kernel level.

Package kernel-tools-4.18.0-553.111.1.el8_10 is installed.
However, according to uname -r, the current running kernel level is 4.18.0-
553.58.1.el8_10.
This system requires a reboot to begin using the patched kernel level.

Package kernel-tools-libs-4.18.0-553.111.1.el8_10 is installed.
However, according to uname -r, the current running kernel level is 4.18.0-
553.58.1.el8_10.
This system requires a reboot to begin using the patched kernel level.
```

## 7. Open Port Detection

**Synopsis**
It is possible to determine which TCP/UDP ports are open.

**Description**
SYN 'half-open' and UDP port scanner are used. It shall be reasonably quick even against a firewalled target.

**Solution**
Disable these services if they are not needed or restrict access with IP filter to internal hosts only if the services are available externally.

**Proof of Concept**

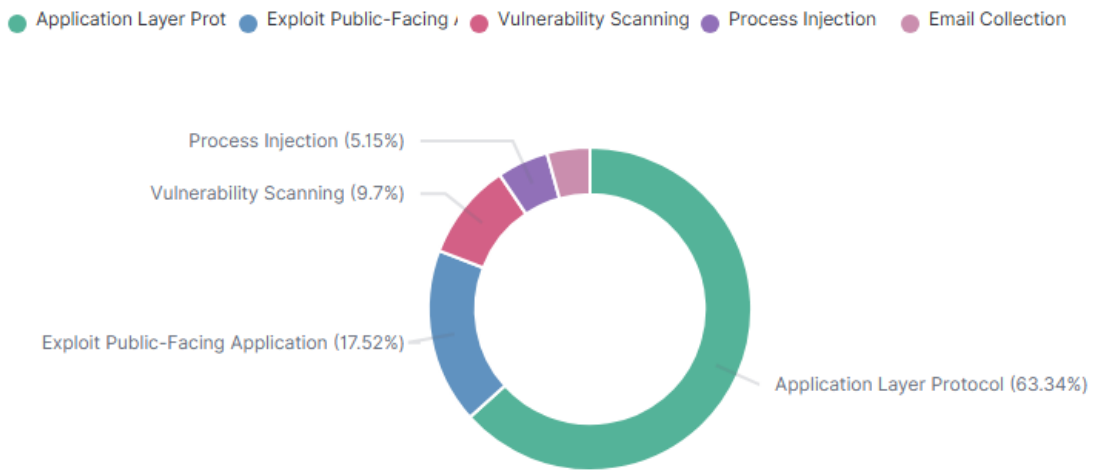
```
PORT       STATE  SERVICE     VERSION
----------------------------------------------------------------------------
PORT       STATE  SERVICE     VERSION
80/tcp     open   http        Apache httpd
443/tcp    open   ssl/http    Apache httpd
465/tcp    open   ssl/smtp    Postfix smtpd
587/tcp    open   smtp        Postfix smtpd
993/tcp    open   ssl/imap    Dovecot imapd
995/tcp    open   ssl/pop3    Dovecot pop3d
9292/tcp   open   ssh         OpenSSH 8.0 (protocol 2.0)
10000/tcp  open   webmin
15220/tcp  open   oracle-tns  Oracle TNS listener 1.5.0.0.0 (unauthorized)
```

# MITRE ATTCK Summary

| Server Name | IP address | Operating system | Last keep alive |
|---|---|---|---|
| finc.app | 37.27.49.243 | Rocky Linux 8.10 | April 06, 2026 |

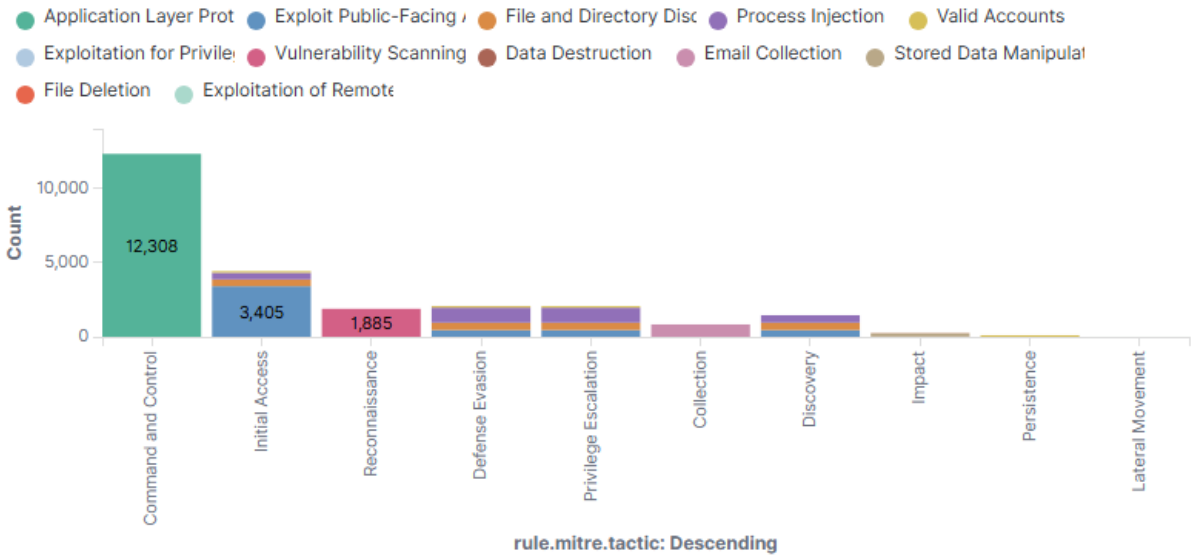
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

## Alerts level by attack



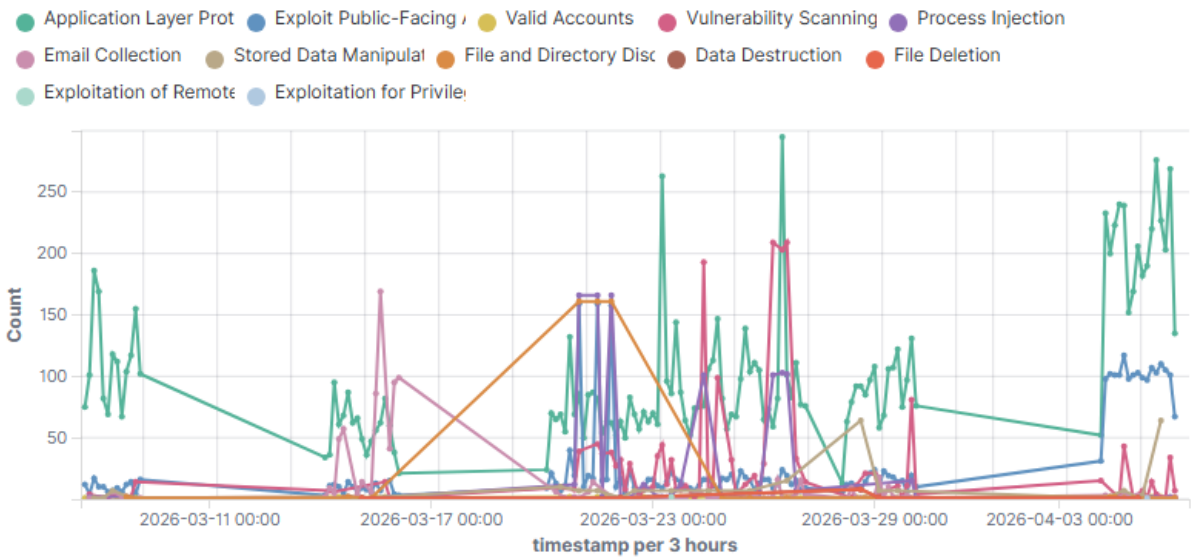

This section presents the distribution and severity of alerts generated due to various attacks detected on the system. Each alert is categorized by its level of importance or potential impact, helping to prioritize responses based on the severity of the threats.

## Top tactics



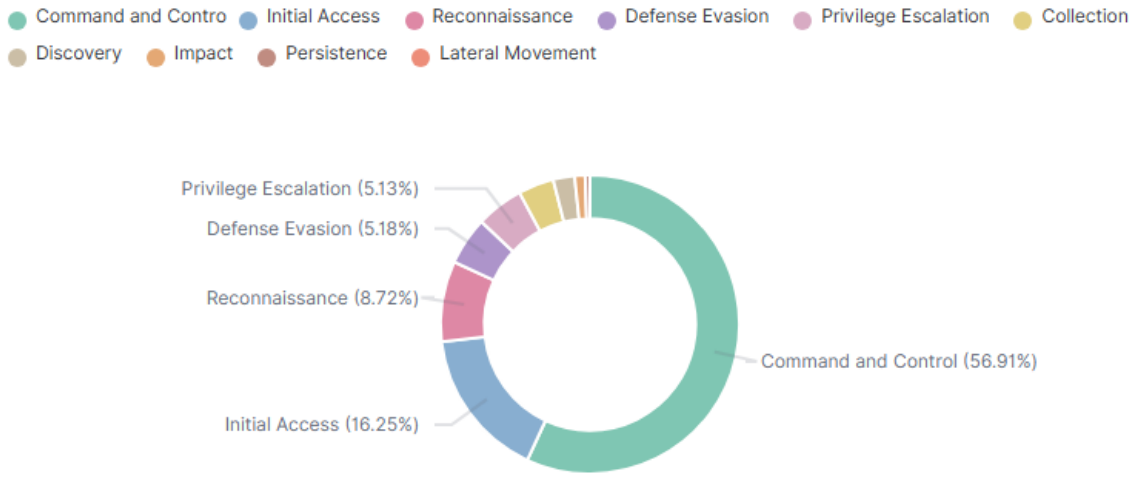

This graph highlights the most frequently used tactics by attackers. It provides a visual representation of the tactics that are most prevalent, indicating common threat vectors and areas where security measures may need reinforcement.

## Mitre alerts evolution




This section shows the trend of alerts over time, mapped against various tactics identified in the MITRE framework. It provides insights into how attack patterns evolve, helping in understanding whether certain attacks are increasing in frequency or severity.

## Top tactics pie




This section features a pie chart that visually represents the proportion of different tactics employed in attacks, as classified by the MITRE ATTCK framework. It provides a quick glance at which tactics are most dominant, enabling security teams to quickly assess the primary methods being used by attackers and adjust their defensive strategies accordingly. This visual helps in understanding the distribution and focus areas of current security threats, assisting in prioritizing security measures and responses.

# Conclusion

The vulnerability assessment conducted provides a clear view of the vulnerabilities impacting the server at finc.app. It is evident that while some areas show robust defenses, others require strategic enhancements to align with best security practices and the evolving threat landscape. Moving forward, we must integrate the insights from this assessment into our broader security strategy, focusing on areas with frequent alerts and adopting proactive defense measures. This will not only mitigate current vulnerabilities but also prepare us for future security challenges.