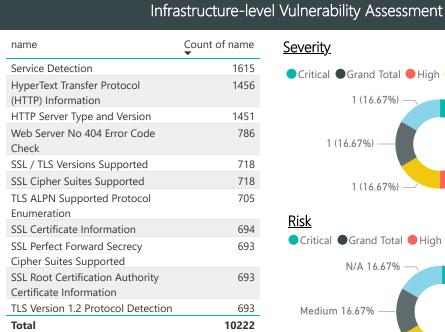
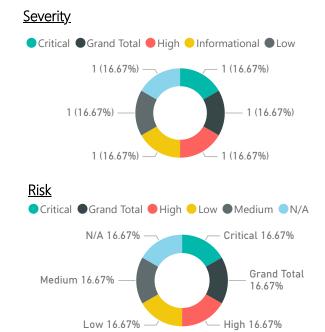
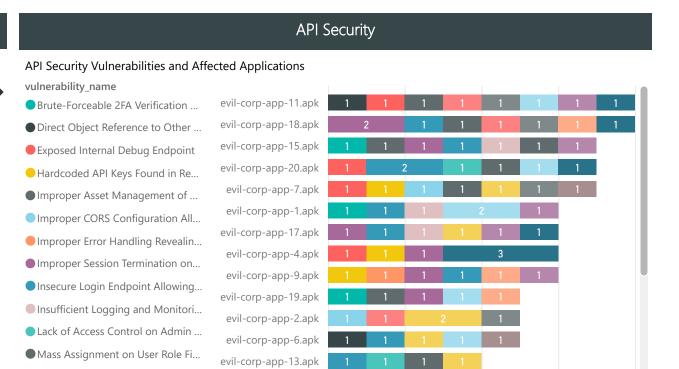
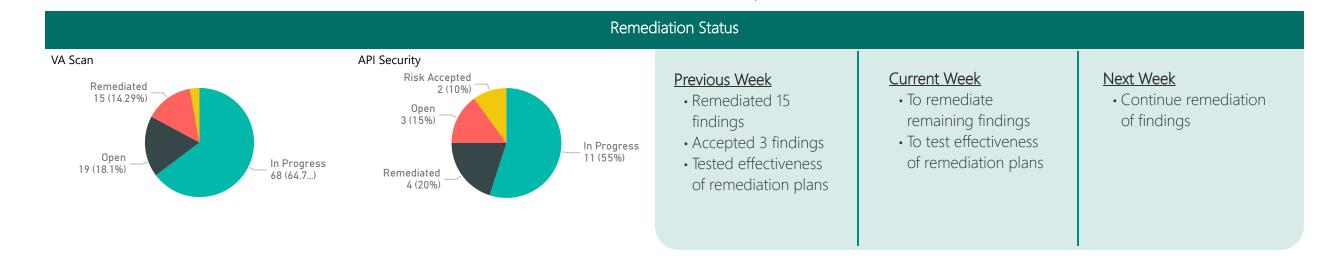
## Weekly Vulnerability and Remediation Status Update

March 30th, 2025



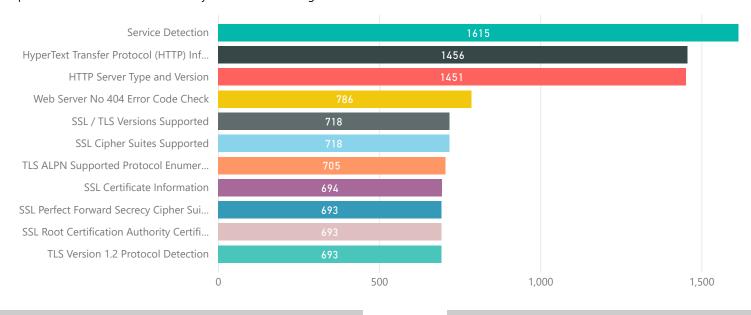






## Infrastructure-level Vulnerability Assessment

## Top 10 Infrastructure-levl Vulnerability Assessment Findings



Severity

Medium 1 (16.67%)

Low
1 (16.67%)

Informational
1 (16.67%)

High 1 (16.67%)

N/A 1 (16.67%)

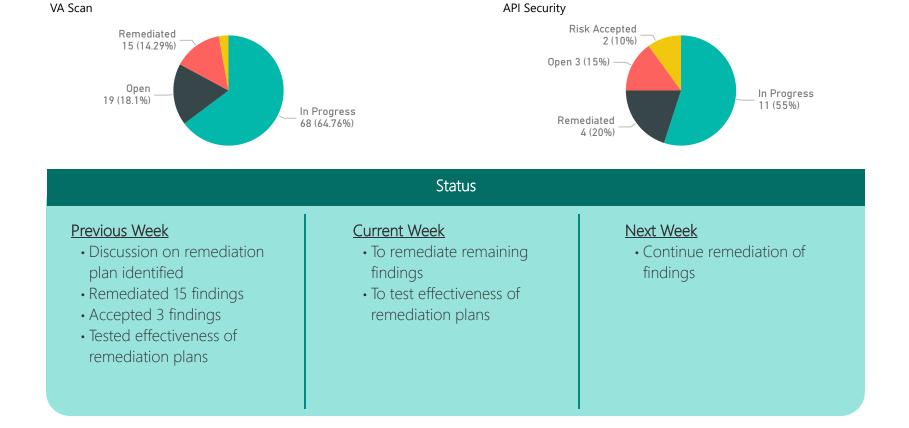
Medium
1 (16.67%)

Low 1 (16.67%)

High 1 (16.67%)

Risk

## **API Security** API Security Vulnerabilities and Affected Applications vulnerability\_name evil-corp-app-11.apk Brute-Forceable 2FA Verification Endpoint evil-corp-app-18.apk ● Direct Object Reference to Other Users' Invoi... evil-corp-app-15.apk Exposed Internal Debug Endpoint evil-corp-app-20.apk Hardcoded API Keys Found in Response evil-corp-app-7.apk Improper Asset Management of Deprecated ... evil-corp-app-1.apk Improper CORS Configuration Allowing Wild... evil-corp-app-17.apk Improper Error Handling Revealing Stack Trace evil-corp-app-4.apk Improper Session Termination on Logout evil-corp-app-9.apk ● Insecure Login Endpoint Allowing Credential ... evil-corp-app-19.apk Insufficient Logging and Monitoring evil-corp-app-2.apk Lack of Access Control on Admin Functions evil-corp-app-6.apk Mass Assignment on User Role Field evil-corp-app-13.apk Missing Authorization Check on User Setting... evil-corp-app-16.apk No Rate Limiting on Feedback Submission En... evil-corp-app-12.apk Overexposed Admin Reports with Unfiltered ... evil-corp-app-14.apk Sensitive User Data Returned in API Response evil-corp-app-3.apk evil-corp-app-8.apk SQL Injection in Product Filtering Endpoint evil-corp-app-10.apk ■ SQL Injection via Unsanitized Search Paramet... evil-corp-app-5.apk Token Refresh Endpoint Missing Session Vali... Unrestricted File Upload in Profile Update 0



Remediation Progress