Synack

Cloudfix Pentest report

Date Generated:
March 22, 2023

Table of Contents

Executive Overview **3**
Testing Methodology **4**
Synack Red Team **6**
Synack Red Team Vetting Process 6
Synack Red Team Certifications 6
Synack Red Team Insights **7**
Researcher Effort for Web Assessment of Cloudfix Application 7
Summary of Discovered Vulnerabilities **8**
Vulnerability Distribution By Severity 8
Vulnerability Distribution By Category 8
Vulnerability Distribution By Status 9
Vulnerability Distribution By Status & Severity 10
Vulnerability Count over Time 11
About Synack **12**

Executive Overview

Aurea Software engaged Synack, Inc. to perform a penetration test for their applications. The testing was performed on the targets reported under scope section.

This report reflects testing done between March 08, 2023 - March 16, 2023.

Scope

Web Assessment of Cloudfix
Application

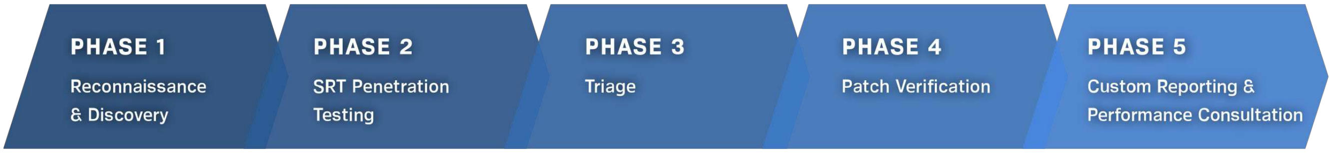
Vulnerabilities Summary

3 **Total Vulnerabilities**	1 Critical Severity	0 High Severity	2 Medium Severity	0 Low Severity

Testing Methodology

Synack offers a replacement to ordinary penetration testing that uses better minds, processes, and analytics to deliver security testing for a new era. Modern digital environments require scalable, dynamic testing, not just point-in-time reports, to proactively find vulnerabilities before the adversary can. Over 100 organizations worldwide have chosen Synack, including some of the largest F500/G500 enterprise organizations across banking and financial services, healthcare, consumer goods and retail, manufacturing, technology, and the U.S. Government.

Each Synack engagement includes five key phases



Phase One — Reconnaissance & Discovery

Synack's approach is the same used by organized adversarial organizations—perform automated recon for weak points on a target. Synack's Hydra software is designed to decrease vulnerability discovery time finding all security issues that a machine can recognize. That information becomes available to Synack's penetration testers—the Synack Red Team (SRT)—so they can begin hunting.

Phase Two — SRT Penetration Testing

The SRT utilize a variety of tools and techniques that closely mimic adversarial tradecraft, but in an identified, protected environment. Each security expert has been extensively checked, interviewed, tested and put on probation before becoming a full-fledged member of the SRT, which admits < 10% of applicants.

All of their hunting traffic is routed through Synack's secure gateway, LaunchPoint, and is continuously monitored and analyzed for patterns. Clients recognize SRT activity through two whitelisted IP addresses. For web application engagements, the SRT uses a range of testing methodologies which address a variety of web-based attacks. Issues such as: configuration management, business logic, authentication, authorization, session management, data validation, web services, client-side code, OWASP Top 10 Project and CWE/ SANS Top 25 Most Dangerous Software Errors are probed.

Phase Three — Triage

All findings from the SRT are submitted to your force multiplier, Synack Mission Operations, which reproduces, validates, and prioritizes all submitted vulnerabilities to filter out any invalid or duplicate reports. The result is that clients only see meaningful, well-written, clear reports about proven exploits, not theoretical weaknesses.

Phase Four — Patch Verification

Once a patch has been released, the client can request Patch Verification. This request is sent directly to the researcher that discovered the original vulnerability. This researcher will then re-test the patch to ensure that the vulnerability has been closed. As a result, Synack clients close vulnerabilities for real.

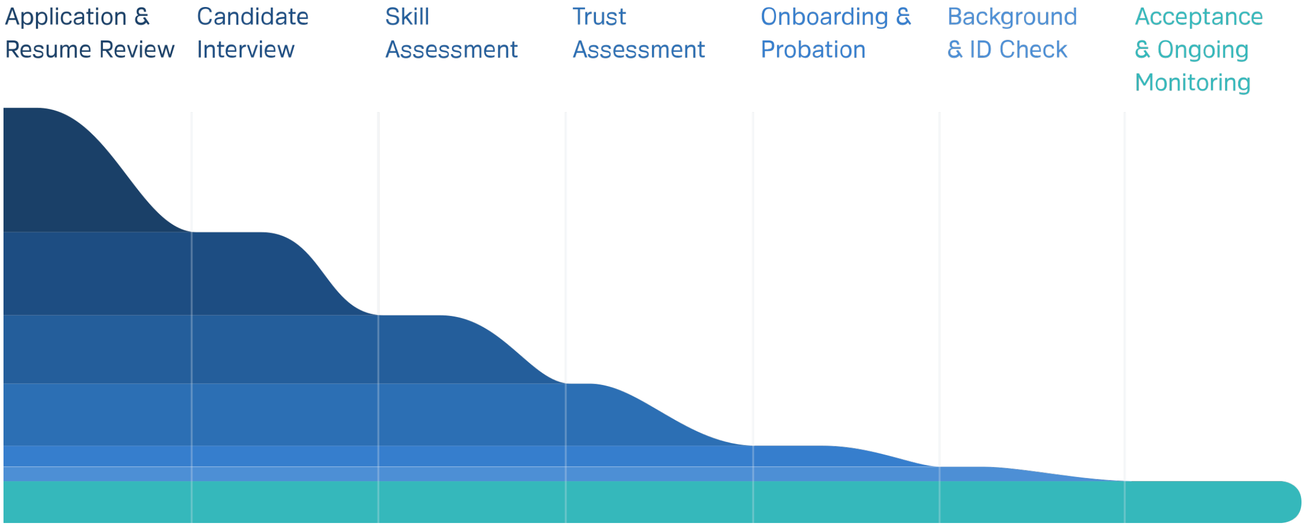
Phase Five — Custom Reporting & Performance Consultation

Throughout the engagement, the clients have access to real-time security analytics and custom reporting on demand, such as time on target, the number of researchers, and coverage in additional to vulnerability reports. Synack Mission Operations constantly tracks a program's performance to ensure the client's objectives are met and that the attack surface is fully covered. At the end of the assessment, your dedicated program management team will provide an outbrief on the program's findings and performance.

Synack Red Team

Synack rigorously vets all new SRT candidates through a 5-step process. Each candidate is tested for both skill and trust, ensuring that only the most qualified and trustworthy individuals are approved to engage in testing activities on Synack's platform. Historically, less than 10% of applicants have been accepted into the SRT, as we strive to add only those trusted individuals who will contribute positive results without excess noise to the platform. To ensure professional behavior, Synack monitors and polices online behavior from SRT members, and removes SRT members immediately when required. Synack maintains a common standard and reward level across the SRT. All of our clients benefit from the clear understanding and agreement between SRT members and Synack for what constitutes a good report deserving of a high reward.

Synack Red Team Vetting Process



As a result, the SRT is a diverse group of highly skilled security experts, which includes top researchers from academia, government, and the private sector. The SRT represents 40+ countries around the world, with incredible diversity of TTP (tactics, techniques and procedures). Many Synack researchers regularly speak at industry events such as Def Con, AppSec, and Black Hat. They have collectively earned millions of dollars and have found thousands of vulnerabilities for Synack clients.

Synack Red Team Certifications

CISSP — Certified Information Systems Security Professional
GCIH SANS — Certified Incident Handler
CISM — Certified Information Security Manager
CISA — Certified Information Systems Auditor
CEH — Certified Ethical Hacker
GSNA, GCFA, GWAPT, GCED, GCUX, etc. — Various SANS GIAC Certifications

Synack Red Team Insights

This section reflects the number of active Researchers and total testing time on the assessment(s).

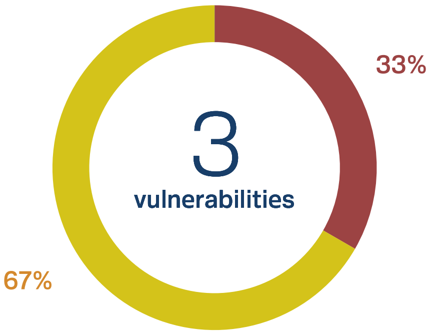
Researcher Effort for Web Assessment of Cloudfix Application

111 Active Synack Red Team	142 Hours Spent on Assessment

Summary of Discovered Vulnerabilities

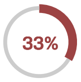
Vulnerability Distribution By Severity

All vulnerabilities are rated using the Common Vulnerability Scoring System (CVSS) 10-point scale. The vulnerabilities discovered during this engagement have been placed into critical, high, medium, low severity tiers based on their CVSS score.

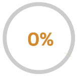


3 Total Vulnerabilities

- ● Critical Severity — 1 vulnerability
- ● High Severity — 0 vulnerability
- ● Medium Severity — 2 vulnerabilities
- ● Low Severity — 0 vulnerability

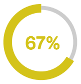


Critical Severity
1 Vulnerabilities

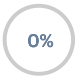


High Severity
0 Vulnerabilities

- 🟥 SQL Injection (1)



Medium Severity
2 Vulnerabilities

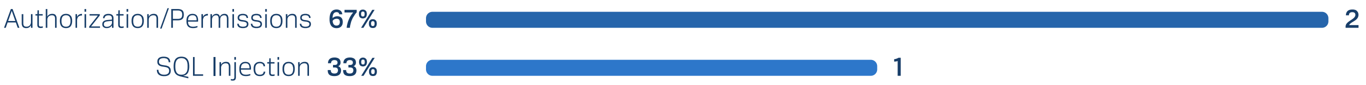


Low Severity
0 Vulnerabilities

- 🟨 Authorization/Permissions (2)

Vulnerability Distribution By Category

This section describes the categorization of vulnerabilities based on the vulnerability category.



Vulnerability Distribution By Status

This section describes the distribution of vulnerabilities based on the vulnerability status at the time of the report generation.

3
vulnerabilities
Closed: 3 (100%)

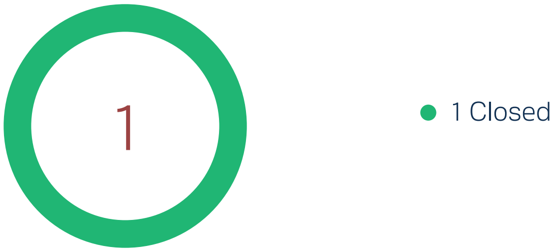
3 Total Vulnerabilities

- ● Closed (100%) - 3

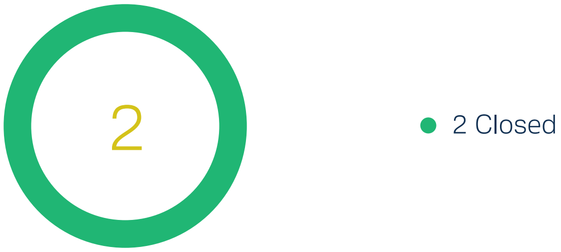
Vulnerability Distribution By Status & Severity

This section describes the distribution of vulnerabilities based on the vulnerability status by severity at the time of report generation. The intent of this section is to provide breakout of vulnerability by severity and status.

Critical Severity Vulnerabilities

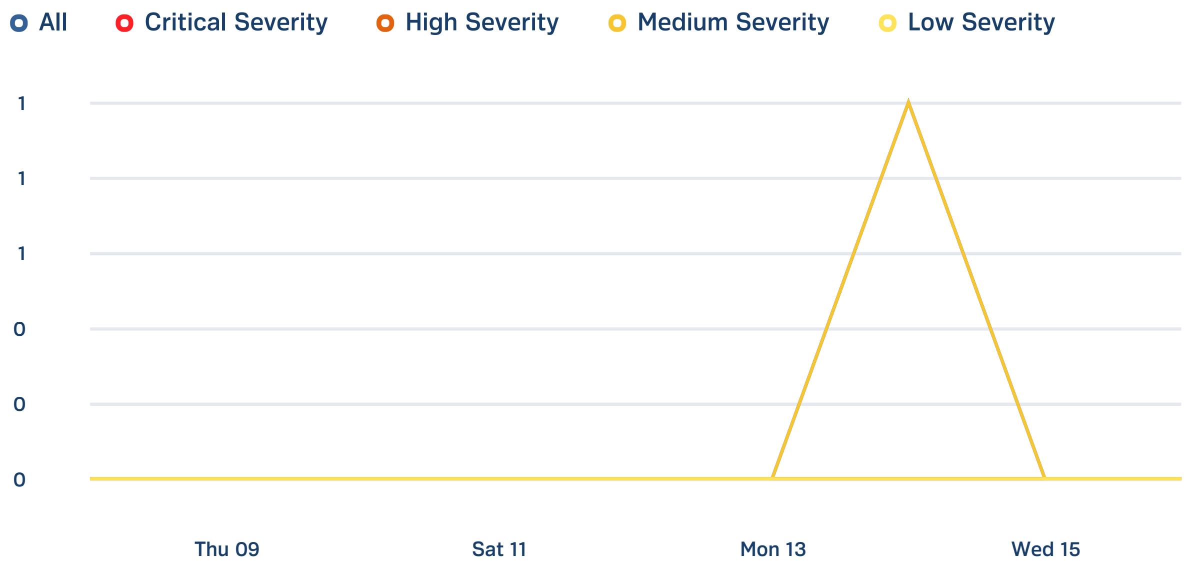


Medium Severity Vulnerabilities



Vulnerability Count over Time

This graph displays a daily count of newly discovered vulnerabilities. Invalid vulnerabilities are excluded from this count.



About Synack

Based in Redwood City, California, Synack is a security company revolutionizing how enterprises view cybersecurity: through a hacker’s eyes. Synack’s private, managed crowdsourced security solution arms clients with hundreds of the world’s most skilled, highly vetted ethical hackers who provide a truly adversarial perspective of clients’ IT environments. Synack’s confidential client base is comprised of some of the largest F500/G500 enterprise organizations across banking and financial services, healthcare, consumer goods and retail, manufacturing, technology and the U.S. Federal Government. All engagements are conducted by Synack’s vetted skilled professionals and are treated with absolute privacy. Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.