COQUINA SYSTEMS

("co-keen-ah")

coquinasystems.com

Penetration Testing Services

IDENTIFY GAPS AND WEAKNESSES IN SYSTEMS BEFORE THREAT ACTORS DO

Penetration testing (pen-testing) mimics a real cyber-attack by inviting a third party to actively search for and exploit vulnerabilities within an organization's digital environment. The goal is to proactively identify weaknesses, ensure protocols are effective, and detect bugs in the software and applications. Pen testing also helps to protect against social engineering tactics by validating how cyber-aware employees are when it comes to information protection best practices. After executing the penetration test, the team reports its findings and recommendations for risk mitigation.

Our Approach

LOWERING THE RISK OF FUTURE ATTACKS

Implementing a comprehensive security and penetration testing strategy not only keeps you one step ahead of cybercriminals but also keeps you compliant with new or expanded regulations such as FedRAMP and SOC 2. At Coquina Systems, we identify vulnerabilities and misconfigurations in your cloud platforms, networks, and applications as well as provide you with the real-world business impact of those issues.

Each set of penetration tests varies based on the goals to be achieved. However, the most common methodology has three phases: ***Discovery***, ***Execution***, and ***Post-execution***.

RANSOMWARE STATISTICS

- U.S. ransomeware attacks cost an estimated $623.7M in 2021 (Emisoft)
- 495 million ransomware attacks occurred in the first nine months of 2021 representing a 148% increase on the previous year. (SonicWall)
- A ransomware attack in early 2020 on the New Orleans city government cost the city upwards of $7 million. (SC Magazine)
- In February 2020, a ransomware attack cost Denmark-based company ISS upwards of $50 million. (GlobeNewswire)
- In 2020, 92 individual ransomware attacks cost US healthcare organizations an estimated $21 billion. (Comparitech)
- One out of five Americans has dealt with a ransomware attack. (The Harris Poll)
- Ransomware is involved in around 17% of malware security incidents, down from 27% in 2020. (Verizon 2021 Data Breach Investigations Report)
- Ransomware payments finally began to decline Q4 2020. In Q3 2021, the average sits at $139,739 which is up 2.3% over the previous quarter. (Coveware's Q3 2021 Ransomware Marketplace report)
- The average downtime due to a ransomware attack was 22 days in Q3 of 2021 compared to 19 days in Q3 2020. (Coveware's Q3 2021 Ransomware Marketplace report)
- 89% of MSPs state that ransomware is the most common threat to SMBs

DISCOVERY

Gathering information, identifying the assets most likely to be targeted by threats, and developing the rules of engagement with the client

EXECUTION

Perform the tests, identify critical and non-critical vulnerabilities, and validates which of those vulnerabilities could result in an attack

POST-EXECUTION

Identify root causes of vulnerabilities to establish recommendations for overall findings. Test common and uncommon exploits used by attackers such as brute-forcing and others.

Getting Results

SOLUTIONS TO REMEDIATE FUTURE THREATS

Through our customer engagement, Coquina Systems identifies multiple moderate and severe vulnerabilities. If left exposed, these could result in dire consequences for the organizations, its members, and the larger public.

While results and findings vary across organizations, we are able to pinpoint issues such as XSS vulnerabilities, CSRF vulnerabilities, issues within authorization controls, and weaknesses that could arise from brute force, SQL injections, and cross-site request forgery.

All pen-testing clients receive a detailed and easy to understand report of our findings. The report not only educates the organization on the vulnerabilities found but also offers solutions on the best ways to remediate them. With penetration testing, these organizations and the many others working with us can more accurately maintain security oversight of their digital environments.

OUR PENETRATION TESTING SERVICES INCLUDE:

- Cloud security testing (AWS, Azure)
- Network penetration testing (internal & external)
- Dark web and open-source intelligence
- Web application penetration testing
- Mobile application penetration testing
- Static application security testing (SAST)
- Dynamic application security testing (DAST)

COMPLETE SOLUTIONS YOU CAN SELL

A Trusted Partner for Your Success

Coquina Systems delivers the highest quality, vetted technology services professionals matched to the specific requirements of each project. Our Services Marketplace™ allows you to tap into IT talent from an extensive library of high-demand practice areas including:

- IT Resources & Residency Services
- Cloud Services
- Security and Cyber Risk
- Data Center Automation
- DevOps and SecOps
- Migration Services
- Managed Services
- Technology Upgrades
- Project Management
- Troubleshooting
- Knowledge Transfer
- Emerging Technologies

EXECUTIVE SUMMARY

The Web Application Pen Test was tested from the perspective of an Authenticated External attacker. The testing team identified **9 (nine)** vulnerabilities as categorized below. An unautenthicated external attacker, with the vulnerabilities we found in this report, would have administrative privileges to the database connected to the application and would have the power to manipulate content, and scripts reflected on the web server.

Critical	High	Medium	Low	Informational
0	3	2	4	3

Finding Name	Risk Level
High Risk Findings	
Credential Enumeration and Brute Forcing	High
Cross-site scripting (reflected)	High
Insufficient Authorization Controls	High
Medium Risk Findings	
Cross-Site Request Forgery (CSRF)	Medium
SQL Injection	Medium
Low Risk Findings	
Backup Files Disclosure	Low
Breached Company Credentials	Low
Browsable Web Directories	Low
Content Sniffing not disabled	Low
Informational Risk Findings	
Application Version Number Displayed	Informational
Similar Domain	Informational
User Interface (UI) Redress (Clickjacking)	Informational

TABLE OF CONTENTS

TESTING AREA RATINGS

Testing was performed across several categories as show below with an associated status. The relevance of each testing category is directly related to the level of access and visibility the testing was performed at a point in time constrained to the allocated time and resources. These results should not be taken as a comprehensive.

External Open Source Intelligence (OSINT) Categories	Status
DNS Registration	Good
Exposed IoT Devices	Good
Google Hacking	Good
Breached Data Sources	Average
Public S3 Buckets	Good
Exposed Email Addresses	Good
Sensitive File Exposure	Good
Threat Intelligence	Good
Public Code Repositories	Good
Social Media Profiles	Good

Web Application and API Testing Categories	Status
Injection	Average
Broken Authentication	Average
Sensitive Data Exposure	Average
XML External Entities (XXE)	Good
Broken Access Control	Average
Security Misconfiguration	Average
Cross Site Scripting	Poor
Insecure Deserialization	Good
Using Components with Known Vulnerabilities	Good
Insufficient Logging & Monitoring	N/A
Broken Object Level Authorization	Good
Excessive Data Exposure	Good

RECOMMENDATIONS SUMMARY

Based on the results of the Web Application Pen Test, the testing team has some high-level recommendations.

- **Limit Data Returned** - Ensure queries only return data to users that the user owns, and that the server will only respond with generic messages thatdo not help enumerate usernames.
- **Data Input Validation** – Ensure data is strictly validated server side and all unsafe characters should be replaced with safe references instead.

For detailed recommendations, please see the Recommendations section in each associated finding.

COQUINA SYSTEMS ("co-keen-ah")

Coquina Systems
PO Box 514
Waynesville, OH 45068

www.coquinasystems.com
info@coquinasystems.com
linkedin.com/company/coquinasystems