CREDSHIELDS

SEPT 2022

SECURITY AUDIT PROPOSAL

SHASHANK
CO-FOUNDER
CREDSHIELDS TECHNOLOGIES PTE. LTD.

20A TANJONG PAGAR ROAD
SINGAPORE (088443)

OVERVIEW

Companies and their executives today recognize the degree of risks cybersecurity and related threats possess. What they are not sure of is how to create a strategy that helps them understand and address the threats, in all their forms, today and in the years ahead. And they're asking for such a strategy every day.

Our experience working to protect some of the world's largest and most sophisticated companies, and our proprietary research, have revealed three broad mandates that can help organizations transform their cybersecurity efforts. This compendium offers a comprehensive series of articles describing how companies can make these mandates a reality and help their leaders sleep more soundly.

OUR PROCESS

Schedule A Meeting

Scope Assessment And Timeline

Payment for Services

Security Audit

Draft Report

Retesting Of Bugs

Final Audit Report

Summary

ASSET MANTLE MODULES

AUDIT METHODOLOGIES

- Source Code Audit
- Business Logic Errors
- Components with Known Vulnerabilities.
- Data and State Storage.
- Database and state integrity
- RPC security
- Insecure communications
- Transaction Fee Mechanism Security Transaction Congestion Attack Protection
- Tokenization Reward Mechanism
- Default Configuration Security
- Economic attacks
- Access Control
- Logical DOS attacks
- Code/Command execution
- Predefined Function Security
- Security Misconfigurations
- Input Validation

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

The team performs gray box penetration test of the web application to assess its risk posture and identify security issues that could negatively affect the company's data, systems, or reputation. The scope of the assessment may cover and include credentials for various levels of privilege within the applications. The pentesters perform the below checklist but not limited to it.

Phase 1
Recon and OSINT

- Whois information discovery
- IP and IP range enumeration
- DNS enumeration
- Subdomain enumeration
- Certificate information gathering
- Fingerprinting of Web Services and Technologies
- Enumerating open ports and services
- Credential Stuffing for leaked Employee data
- GitHub leak detection for sensitive information
- Information exposed through archived data
- Conduct Search Engine Discovery Reconnaissance for Information Leakage

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Input validation
  - Testing for Reflected Cross Site Scripting
  - Testing for Stored Cross Site Scripting
  - Testing for HTTP Verb Tampering
  - Testing for HTTP Parameter Pollution
  - Testing for SQL Injection
  - Testing for LDAP Injection
  - Testing for XML Injection
  - Testing for SSI Injection
  - Testing for XPath Injection
  - Testing for IMAP SMTP Injection
  - Testing for Code Injection
  - Testing for Local and Remote File Inclusion
  - Testing for Command Injection
  - Testing for Format String Injection
  - Testing for HTTP Splitting Smuggling
  - Testing for HTTP Incoming Requests
  - Testing for Host Header Injection
  - Testing for Server-side Template Injection
  - Testing for Server-Side Request Forgery
  - Testing for serialization/deserialization related vulnerabilities

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Configuration and Deployment Management Testing
    - Test Network Infrastructure Configuration
    - Test Application Platform Configuration
    - Test File Extensions Handling for Sensitive Information
    - Review Old Backup and Unreferenced Files for Sensitive Information
    - Enumerate Infrastructure and Application Admin Interfaces
    - Test HTTP Methods
    - Test HTTP Strict Transport Security
    - Test RIA Cross Domain Policy
    - Test File Permission
    - Test for Subdomain Takeover
    - Test Cloud Storage

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Authentication Testing
  - Testing for Credentials Transported over an Encrypted Channel
  - Testing for Default Credentials
  - Testing for Weak Lock Out Mechanism
  - Testing for Bypassing Authentication Schema
  - Testing for Vulnerable Remember Password
  - Testing for Browser Cache Weaknesses
  - Testing for Weak Password Policy
  - Testing for Weak Security Question Answer
  - Testing for Weak Password Change or Reset Functionalities
  - Testing for Weaker Authentication in Alternative Channel

- Authorization Testing
  - Testing Directory Traversal File Include
  - Testing for Bypassing Authorization Schema
  - Testing for Privilege Escalation
  - Testing for Insecure Direct Object References

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Session Management Testing
  - Testing for Session Management Schema
  - Testing for Cookies Attributes
  - Testing for Session Fixation
  - Testing for Exposed Session Variables
  - Testing for Cross Site Request Forgery
  - Testing for Logout Functionality
  - Testing Session Timeout
  - Testing for Session Puzzling
  - Testing for Session Hijacking

- Identity Management Testing
  - Test Role Definitions
  - Test User Registration Process
  - Test Account Provisioning Process
  - Testing for Account Enumeration and Guessable User Account
  - Testing for Weak or Unenforced Username Policy
  - Testing for KYC integrations

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Session Management Testing
  - Testing for Session Management Schema
  - Testing for Cookies Attributes
  - Testing for Session Fixation
  - Testing for Exposed Session Variables
  - Testing for Cross Site Request Forgery
  - Testing for Logout Functionality
  - Testing Session Timeout
  - Testing for Session Puzzling
  - Testing for Session Hijacking

- Identity Management Testing
  - Test Role Definitions
  - Test User Registration Process
  - Test Account Provisioning Process
  - Testing for Account Enumeration and Guessable User Account
  - Testing for Weak or Unenforced Username Policy
  - Testing for KYC integrations

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Business Logic Testing
    - Test Business Logic Data Validation
    - Test Ability to Forge Requests
    - Test Integrity Checks
    - Test for Process Timing
    - Test Number of Times a Function Can Be Used Limits
    - Testing for the Circumvention of Work Flows
    - Test Defenses Against Application Misuse
    - Test Upload of Unexpected File Types
    - Test Upload of Malicious Files
    - Test for round off errors

- Testing for Error Handling
    - Testing for Improper Error Handling
    - Testing for Stack Trace

- Testing for Weak Cryptography
    - Testing for Weak Transport Layer Security
    - Testing for Padding Oracle
    - Testing for Sensitive Information Sent via Unencrypted Channels
    - Testing for Weak Encryption

WEB APPLICATION SECURITY

AUDIT METHODOLOGIES

Phase 2
Application Security Audit

- Information Disclosure
    - Client Side Data protection
    - Hard-coded sensitive information

- Client-Side Testing
    - Testing for DOM-Based Cross Site Scripting
    - Testing for JavaScript Execution
    - Testing for HTML Injection
    - Testing for Client-side URL Redirect
    - Testing for CSS Injection
    - Testing for Client-side Resource Manipulation
    - Testing Cross Origin Resource Sharing
    - Testing for Cross Site Flashing
    - Testing for Clickjacking
    - Testing WebSockets
    - Testing Web Messaging
    - Testing Browser Storage
    - Testing for Cross Site Script Inclusion

EXTERNAL NETWORK

AUDIT METHODOLOGIES

Reconnaissance and Information Gathering

- Whois information discovery
- IP and IP range enumeration
- DNS enumeration
- Subdomain enumeration
- Certificate information gathering
- Fingerprinting of Web Services and Technologies
- Enumerating open ports and services
- Credential Stuffing for leaked Employee data
- GitHub leak detection for sensitive information
- Information exposed through archived data
- Search Engine Discovery Reconnaissance for Information Leakage

Vulnerability Scanning and Exploitation

- Using open-source, commercial, and internally developed tools to identify and confirm well-known vulnerabilities
- Spidering the in-scope network device(s) to effectively build a map of each of the operating systems, open ports and services, and areas of interest

EXTERNAL NEWORK

AUDIT METHODOLOGIES

Vulnerability Scanning and Exploitation

- Use various open-source and commercial tools to exploit the vulnerable services discovered in the above steps. Escalate privileges to find out the maximum impact
- Using discovered sections, features, and capabilities to establish threat categories to be used for more manual/rigorous testing (i.e., default admin credentials, session hijacking, known vulnerabilities in out-of-date components)
- Building the network's threat model using the information gathered in this and the previous phase to be used as a plan of attack for later phases of the assessment

SERVICE DESCRIPTION

SCOPE

- Comdex Modules

- Web Application + External Networks

DETAILED SCOPE

COMDEX AND GOVERNANCE CONTRACTS

https://github.com/AssetMantle/modules/tree/master/modules

- *.assetmantle.one

SERVICE DESCRIPTION

TIMELINE FOR AUDIT

- Audit time - 20 days
- Bug retest time period - 3 months after the audit end date
- Audit Report - 2 days after audit ends date

TOS

- Pentest time does not include weekends.
- There will be additional charges for retest after three (3) months.
- Retest will be performed in batches. Repetitive retest after three (3) requests will be chargeable.
- Retest will be performed in 4 business days upon request.
- The final audit will be made available as soon as the bugs are fixed or the retest time period expires.

SERVICE CHARGES

TOTAL

Assel Mantle Modules	- 11,000 USD
Web Application + External Network	- 4000 USD
GRAND TOTAL.	- 15,000 USD

TOS

- 50% of the services charges are expected to be paid before the pentest begins.
- The final audit report will be delivered after full payment.
- Additional retest time period - 200$ for one (1) month retest time period.
- GST will not be charged as the payment will be made to the Singapore entity.

SERVICE CHARGES

For and on behalf of the Company

Name: AssetMantle

Representative:

Title:

Address:

Signature:

Date:

For and on behalf of Service Provider

Name: Creshields Technology Pte. Ltd

Representative: Shashank

Title: CEO

Address: 20A TANJONG
PAGAR ROAD
SINGAPORE (088443)

Signature: shashank

Date: 12th Sept 2022