Logging, right kind, can make lot of difference in the world of security

Application Security is critical, when your security perimeter has shied from usual DMZ and Firewall to web infra and mobile devices, and, a combination of those!

Web Security

Ensuring that your website or open web application is secure is critical.

Mobile Security

Without mobile device security measures, organizations can be vulnerable to malicious software.

API's Security

Focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of Application Programming Interfaces

AppSec Works Coverage Metrics

APP SECURITY

Threat Modeling and Reconnaissance

- Developing a threat model which identifies security flows/zones of application
- Developing a threat model which identifies security boundaries of application
- A document which guides application developer in making design decision
- A document which guides appsec experts in prioritizing pen test cases

Static Pen Testing

- Set of security test cases which are configuration related
- Early testing of the application for quick detections
- Almost 40 test cases out of library of 200
- Identifies all misconfiguration issues in app

Penetration Testing (Full Castellum Labs Library)

- Execution of all test vectors for security vulnerabilities
- A total of 200 test cases and more than 400 scenarios in test cases
- Detects vulnerabilities across all twenty six categories s/w security testing
- Also provides issue detail report for every detected test case (including fixes)

Code Scan for Vulnerabilities (Automated)

- Scan of code to detect hard-coded elements
- Detects hard coding of credentials, IP, secrets, API Keys and more
- Checks for inappropriate inclusion of the author details in production code
- Provides a list of things which need to be removed to sanitize the application

AppSec Works Coverage Metrics

APP SECURITY

Selective Code Review for Vulnerabilities (Manual)

- Detects logical flaws in code which can be exploited by an attacker
- Detects all issues which are not detectable through ten modeled testing
- Finds out improper inclusion of components and libraries in the code construct
- Recommends changes to code logic for key/ sensitive areas of the software code

Software Composition Analysis

- Detection of malicious and vulnerable libraries and component in code
- An inventory of all libraries, components and sub-components in software code
- Analysis of the libraries and components for vulnerable (vulnerabilities which are outstanding)
- Recommending correct versions or remediation's/replacements for the libraries

Remediation Regression Testing

- Testing of the fixes completed by development team
- Assurance that fix is complete and protects against the detected vulnerability
- Ensuring that fix has been rolled out to address all areas of software code, not localized
- Signing off the issue fix in a pre-production release (for PASS/FAIL based certification of code)

Production Security Config review

- Checking the host environment where application is deployed for security misconfigs
- Ensuring that code is signed and pre-production code is released in production env
- Ensuring base OS does not carry a vulnerable version
- This test is done only for one server (not for Dockers) and only when s/w is hosted on host OS

AppSec Works Categories Metrics

APP SECURITY

19 Authentication	14 Access Control	6 Access Token Bypassing	1 Application Logs
6 Business Logic Bypass	13 Code Quality	10 Component Exploitation	6 Cryptography
10 CSRF	4 Data Storage	22 Enumeration	1 Error Handelling
5 File Inclusion	6 File Upload	4 Information Disclosure	16 Injection
16 Input Validation	6 Manifest File Checks	6 Rate Limiting	4 Reverse Engineering
16 Security Misconfiguration	5 Sensitive Data Exposure	12 Session Management	3 SSRF

Secure applications need big budgets,
AppSec experts and more time - always in short supply.
We deliver everything on a platter!

appFORT

Continuous Application Security

watchOUT

Darkweb Monitoring

threatNIXD

Next Gen SOC Monitoring

Castellum Labs

3rd Floor, NYN Arcade,
Lumbini Avenue, Gachibowli,
Hyderabad, India

+91 97009 70397
reach@castellumlabs.com
www.castellumlabs.com