WWW.DETASECURE.COM

DeTaSECURE

Application Security Program

Every business, knowingly or without knowing has a certain amount of data exposed in public.

We fix that! and improve your data protection without any resistance to your buiness continuity.

contact@detasecure.com

WHO ARE WE?

We are accomplished cyber security experts, with industry experience in leadership roles in enterprises PwC, PayPal, Walmart,Thoughtworks and EY, taking care of cyber security practices and global delivery in sectors like web3, finance, e-commerce, healthcare, insurance and telecom domains. We help companies in discovering their exposed data over the Internet. Post analysis, we score them on the basis of their existing security frameworks and recommend ways to improve their overall security posture. We also provide a threat protection program to make companies ready for any unforeseen future attacks.

Our Clients

Infosys®

Great Learning
POWER AHEAD

ACVISS

isteer®
Linking Expertise. Leading Success.

Certifications

GCIH

E|CSA
EC-COUNCIL CERTIFIED SECURITY ANALYST

C|EH
CERTIFIED ETHICAL HACKER

OFFENSIVE security®

Conferences

black hat®

NULLCON

OWASP
Open Web Application Security Project

contact@detasecure.com

Application Security Program

DeTaSECURE Application Security Program for web and mobile applications is to emulate external and internal directed attacks on the application and identify any weaknesses which may lead to unauthorized access and data breaches. With the help of DeTaSECURE DAST & SAST program run on iOS, Windows and Android platform, you can scale static analysis rapidly and affordably to systematically identify and fix security flaws in source code.

Web Applications Black/Grey Box Testing

- Web application security testing services: black box, grey box approach
- Identifying potential vulnerabilities
- Automated and manual analysis of web application
- Test for OWASP top 10 vulnerabilities
- Specific business logic testing based on sector
- Reporting - findings, recommendations

Source Code Review

A crucial component of application security testing is static analysis. But what if your team is short on the tools or expertise necessary to complete the task across your whole portfolio? DeTaSECURE Source Code Review (SCR) Program is a systematic & Security examination of the Source Code of Application and Software. It looks for Security Loop Holes, Bugs that may have been planted and overlooked during Application and software development.

Mobile Application Testing

Security Assessment of the mobile application on iOS, Windows and Android platform to weaknesses which may lead to unauthorized access to business critical information and data. Undertake an application walkthrough to understand the functionality of the application. Identify the threats hampering the security of a mobile application on the Android, Windows and iOS platform.

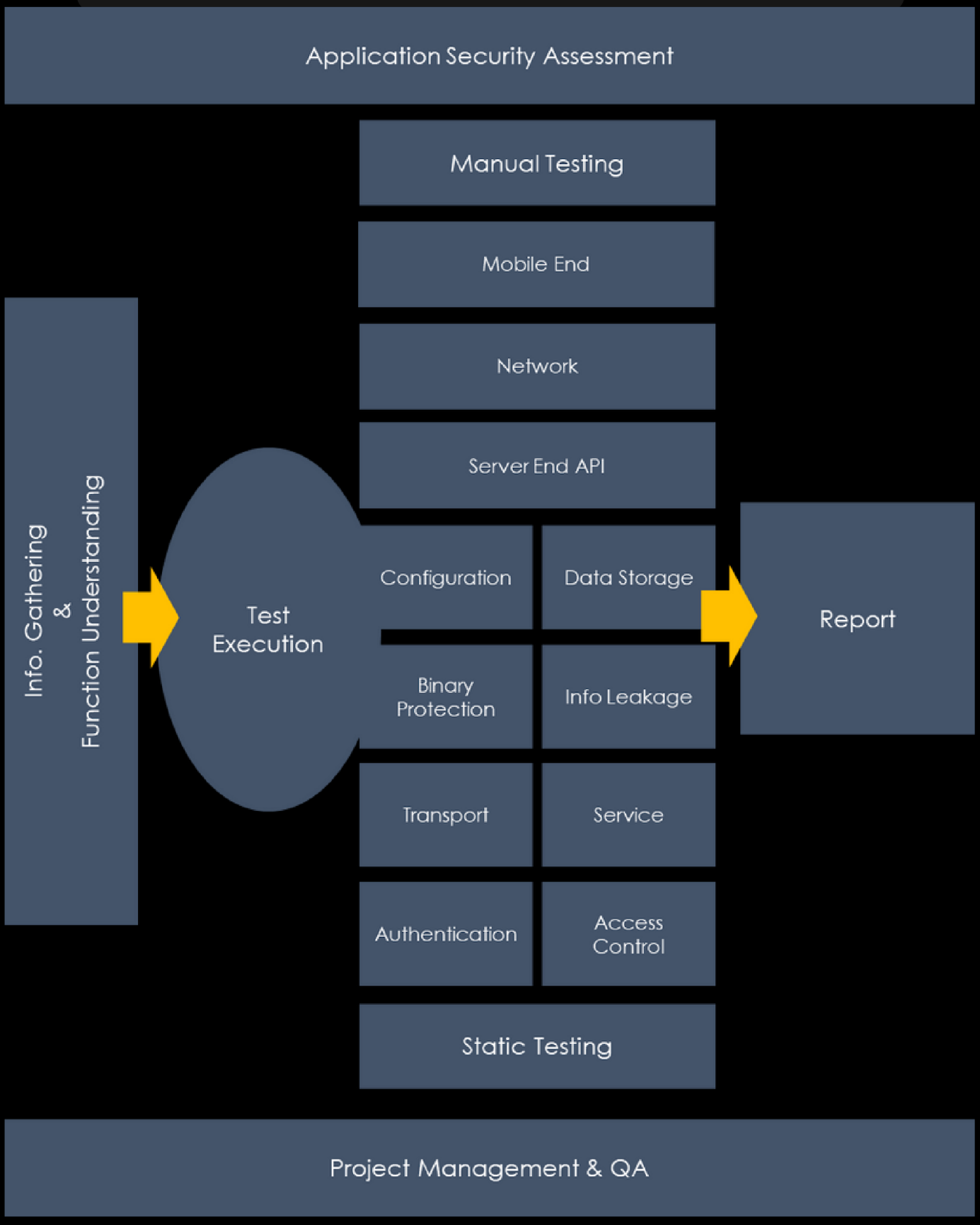
API Security Assessment

Any application that wants to extract and share data in an accessible fashion must have an API layer. Any systems and data connecting to a poorly secured API can be exposed to a significant attack surface, and API abuse commonly leads to significant data breaches for businesses. Finding API-specific vulnerabilities cannot be done using functional testing or web application scans alone.

contact@detasecure.com

OUR PROCESS

APPLICATION SECURITY



contact@detasecure.com

OUR PROCESS

APPLICATION SECURITY METHODLOGY

Phase 1: Target mapping:

- Enumerate/Crawl the application/host to map out the relevant components./ports/services in order to obtain 100% coverage.
- Areas of the application which accept user input are noted for further testing.

Phase 2: Automated Fault injection/Known vulnerability scanning:

- Use automated tools to attempt to exploit vulnerabilities
- Bypassing authentication controls.
- Bypassing validations or manipulation of application business logic.
- Obtaining unauthorized access to the application, the database or the underlying operating system.
- Manual validation of all findings and remove false positives prior to report generation thus minimizing the list of vulnerabilities that have to be verified by the school
- Recommendations and guidance in relation to finding remediation and risk management with Web Application Penetration Testing report

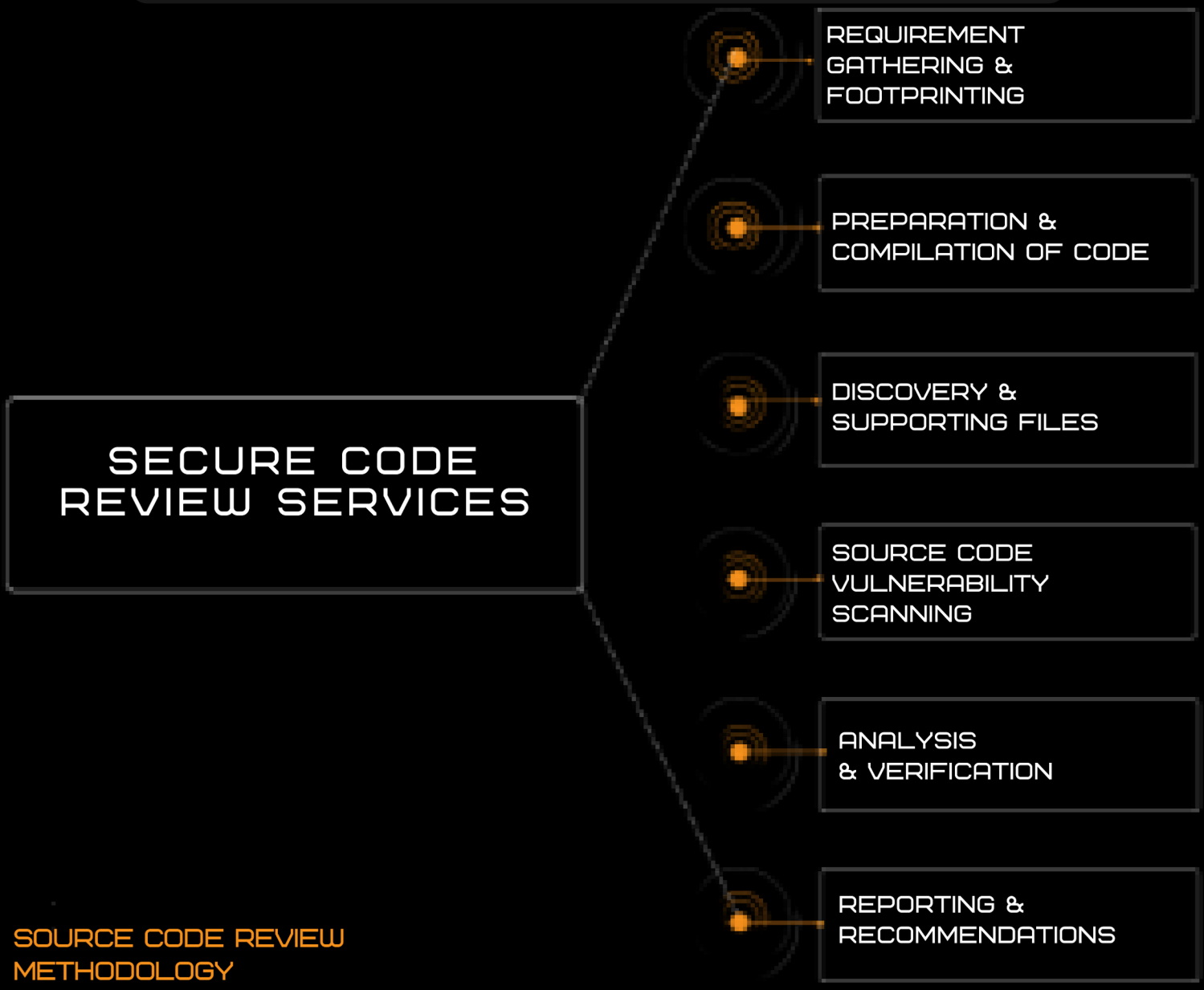
Applications will be assessed for the OWASP top 10 -2017 Most Critical Web Application Security Risks

A1	Injection flaws such as SQL, OS and LDAP injection occur when untrusted data is sent to an interpreter as part of command	A6	Web applications and APIs do not properly protect sensitive data. Attacker may steal such weakly protected data to conduct threat or crime.
A2	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise	A7	Applications need to perform the same access control checks on the server when each function is accessed.
A3	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation	A8	CSRF attack forces a logged-on victim's browser to send a forged HTTP request to a vulnerable web application.
A4	Direct object reference occurs when a developer exposes a reference to an internal implementation object	A9	Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.
A5	Security depends on having a secure configuration defined for the application, All these should be in place.	A10	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages.

contact@detasecure.com

OUR PROCESS

SECURE CODE REVIEW SERVICES



SOURCE CODE REVIEW METHODOLOGY

We will follow OWASP Secure Coding Practice Guidelines for Secure Code Review: A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting XSS
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

contact@detasecure.com

CONTACT US!
GET SECURED!

DeTaSECURE

SEND US AN EMAIL

contact@detasecure.com

VISIT OUR WEBSITE

www.detasecure.com