WWW.DETASECURE.COM

DeTaSECURE

Vulnerability Assessment & Penetration Testing Management 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

WWW.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

blackhat®

NULLCON

OWASP Open Web Application Security Project

contact@detasecure.com

VAPT Management Program

DeTaSECURE Vulnerability Assessment & Penetration Testing Program is a testing process used to find and categorise as many security issues as is practical in a given amount of time. With varied levels of rigour and a focus on comprehensive coverage, this approach could comprise both automatic and manual steps. With a risk-based methodology, vulnerability assessments can focus on a variety of technological layers, with host, network, and application-layer evaluations being the most common. Penetration testing usually mimics a variety of risks that can endanger your business. During a pen test, it may be examined whether a system can withstand attacks from users who are authenticated and those who are not, as well as from a number of other system roles. With the right scope, a pen test can probe into any area of a system that you require information about.

Security Assessment

- Utilizes industry leading practices, best in class tools and proven methodology to produce actionable recommendations for improvement.
- Assess current security technology and processes, against Cyber security maturity framework.

Vulnerability Assessments

- Help improve ongoing vulnerability management programs by charting policies and procedures against a set of leading practices.
- Independent perspective to measure the maturity of the program, identify gaps, focus on risk mitigation efforts, and help to prioritize spend.

Web Applications Black/Grey Box Testing

1. 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

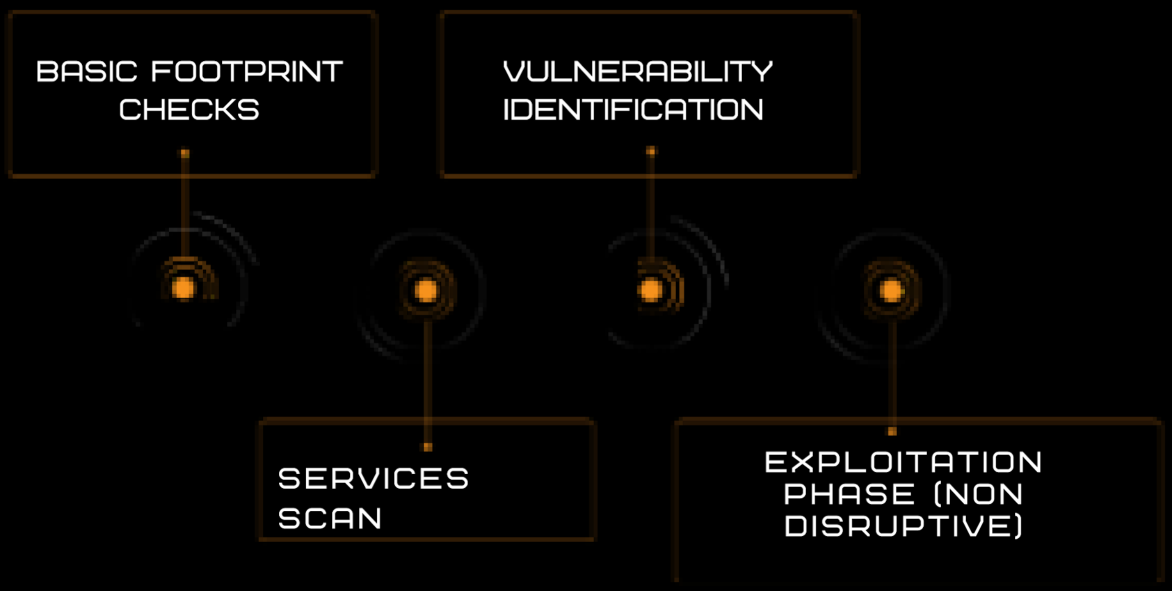
Mobile Application Testing

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.

OUR PROCESS

VULNERABILITY ASSESSMENT & PENETRATION TESTING

Understand application's architecture, infrastructure and security configuration.
Preform automated service scan to discover the active services and enumerate to gather more details Perform automated vulnerability scan targeting the services using tools against OWASP top 10 vulnerabilities Perform manual probes, where necessary, to identify or validate issues that require manual verification Confirm vulnerabilities, document it in reports and provide recommendations



BASIC FOOTPRINT CHECKS

SERVICES SCAN

VULNERABILITY IDENTIFICATION

EXPLOITATION PHASE (NON DISRUPTIVE)

APPLICATION

HOST/ OS LAYER

NETWORK LAYER

NETWORK

- Gather information of network via scanners
- Identify and exploit critical OS, service and application vulnerabilities

NETWORK DEVICES

Scan IP ranges of network devices

- Exploitation configuration vulnerabilities

WEB SERVERS

- Identify weakness in web servers and databases
- Exploit the application

TOOLS USED FOR VAPT

TRIPWIRE IP360

KALI LINUX

WIRESHARK

metasploit

Nessus vulnerability scanner

contact@detasecure.com

OUR PROCESS

APPLICATION SECURITY METHODLOGY

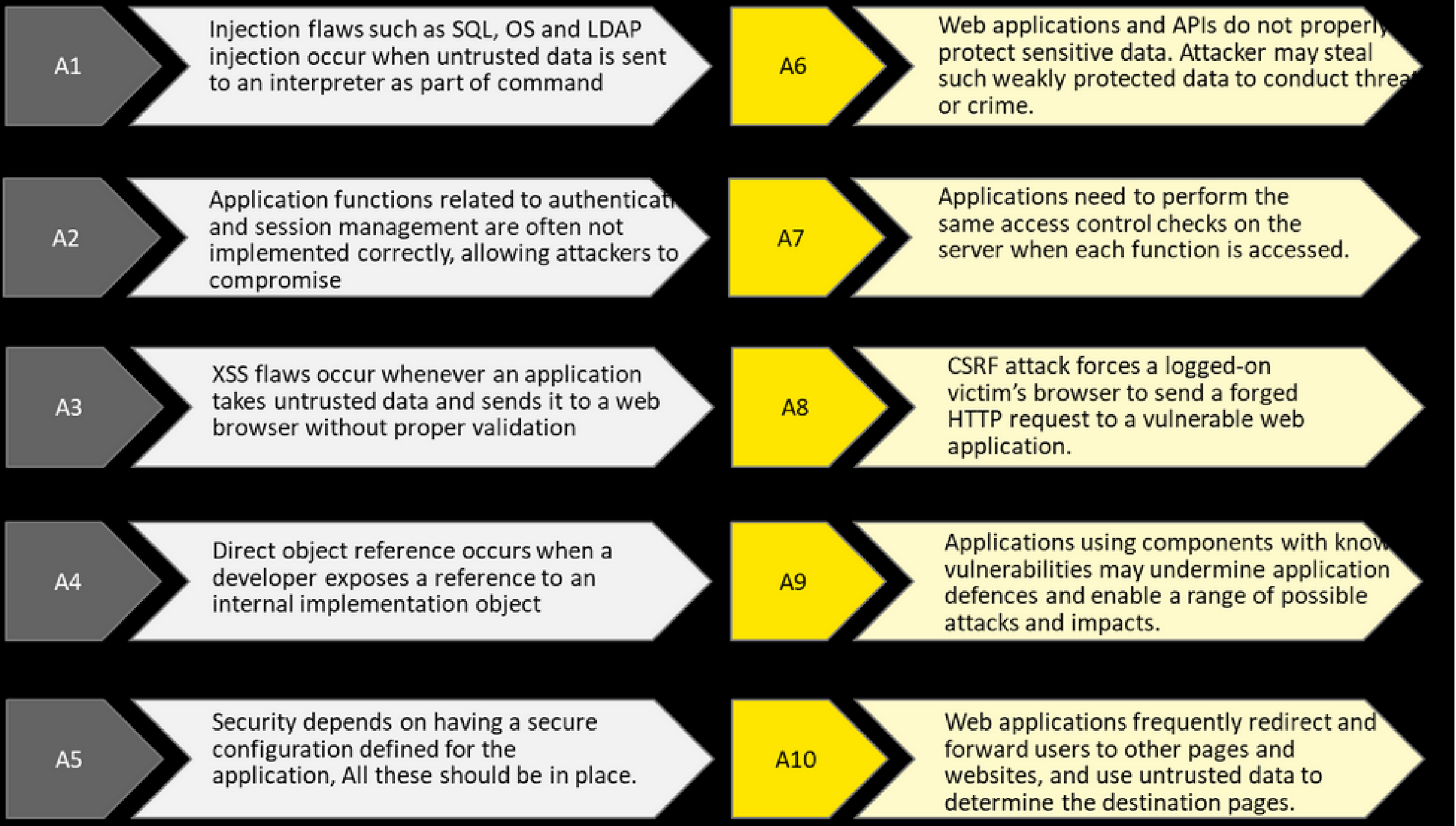
Phase 1: Target mapping:

- 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

A2 Application functions related to authenticati and session management are often not implemented correctly, allowing attackers to compromise

A3 XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation

A4 Direct object reference occurs when a developer exposes a reference to an internal implementation object

A5 Security depends on having a secure configuration defined for the application, All these should be in place.

A6 Web applications and APIs do not properl protect sensitive data. Attacker may steal such weakly protected data to conduct threa or crime.

A7 Applications need to perform the same access control checks on the server when each function is accessed.

A8 CSRF attack forces a logged-on victim's browser to send a forged HTTP request to a vulnerable web application.

A9 Applications using components with know vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.

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

CONTACT US!
GET SECURED!

DeTaSECURE

✉ SEND US AN EMAIL
contact@detasecure.com

🌐 VISIT OUR WEBSITE
www.detasecure.com