
DEBUG
SECURITY

COMPANY OVERVIEW

DEBUG SECURITY

DEBUG SECURITY

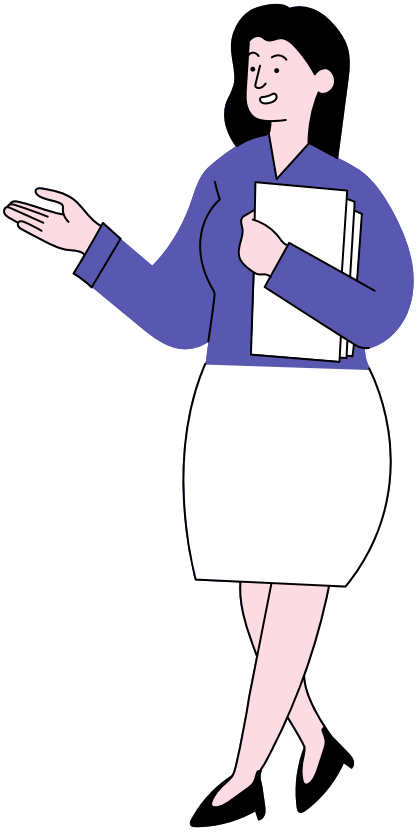
188/2/A Road# Kakoli Road, Ahmed Nagar,
Mirpur, Dhaka-1216.
Call Us: +88 01727 957 026 , Email: info@debugsec.com

TABLE OF CONTENT

INTRODUCTION

SECURITY

CONCLUSION



DEBUG SECURITY

BACKGROUND

Debug Security was established on December 20, 2017, with a mission to help organizations build and maintain secure digital systems. As cyber threats grew in frequency and complexity, we recognized the need for expert-driven security services tailored to modern business challenges.

What began as a small team offering manual vulnerability assessments soon evolved into a full-service cybersecurity company. In 2019, we launched our flagship product VWrap Scanner, a powerful web-based vulnerability scanner that helps clients identify weaknesses in their systems before attackers can exploit them.

Since our founding, we've worked with a wide range of clients from startups to government agencies delivering practical, efficient, and reliable security solutions. We've successfully contributed to over 15+ government and non-government projects, building a reputation for trust, innovation, and technical excellence.

Today, Debug Security is a recognized name in cybersecurity, offering services and support worldwide. Our focus remains the same: to protect, strengthen, and support businesses in an increasingly digital world.

About Us

Debug Security is a cybersecurity company focused on helping organizations secure their digital infrastructure. We provide expert services like vulnerability assessments, penetration testing, network security, mobile application security, red team assessments, source code review and security consultations to protect businesses from cyber threats.

Our in-house tool, VWrap Scanner, helps clients detect vulnerabilities early and stay ahead of attackers. Since 2017, we've supported both government and private sectors, delivering reliable, customized, and results-driven security solutions.

What We Do?

At Debug Security, we help organizations secure their digital systems by identifying and eliminating vulnerabilities before they can be exploited. Our services include vulnerability assessments, penetration testing, mobile app security, source code review, and network audits. We also conduct red team assessments, as well as load, performance, and stress testing. Using our in-house tool, VWrap Scanner, we deliver accurate, efficient, and customized security solutions for businesses of all sizes from startups to government agencies.

Our Mission

Our mission is to protect what matters most in the digital age. We aim to deliver high-impact cybersecurity services and tools like our VWrap Scanner that help organizations identify threats, close security gaps, and stay one step ahead of attackers. Through expert knowledge, ethical practices, and continuous innovation, we empower our clients to operate securely and confidently across the globe.

Our Vision

At Debug Security, our vision is to become a globally recognized leader in cybersecurity a company known for securing the digital future of businesses, governments, and individuals. We strive to create a safer internet by delivering innovative, reliable, and scalable security solutions that help organizations build trust, maintain resilience, and thrive in a connected world.

Security Services

Red Team Assessment

This advanced service mimics real attackers by combining social engineering, phishing, and stealth network intrusion tactics. The goal is to test your organization's detection, response, and defense capabilities. It’s ideal for evaluating overall cybersecurity maturity.

Vulnerability Assessment (VA)

Detects security weaknesses in systems, applications, and networks before attackers can exploit them. Helps prioritize risks and recommends effective remediation.

Penetration Testing (PT)

Simulates real-world attacks to test your system’s defenses and uncover critical vulnerabilities. Provides insights into potential impact and security gaps.

Mobile Application Security

Tests Android and iOS apps for issues like insecure storage, weak authentication, and data leaks. Ensures your mobile apps are safe and compliant.

Source Code Review

Analyzes code to find hidden bugs, insecure practices, and logic flaws. Helps secure your application from the inside out.

Network Security

Evaluates your network for misconfigurations, exposed services, and access control issues. Strengthens infrastructure against internal and external threats.

Performance & Reliability Testing

Load Testing

Measures how a system performs under expected user load. It helps identify performance bottlenecks and ensures the application can handle normal usage smoothly.

Performance Testing

Evaluates the overall speed, responsiveness, and stability of a system under varying conditions to ensure optimal user experience and system reliability.

Stress Testing

Pushes the system beyond its maximum capacity to see how it behaves under extreme conditions. It helps determine the system's breaking point and how well it recovers.

Our Product

VWRAP

vwrap.live

VWrap Scanner is our powerful, next-generation vulnerability scanning tool designed to give you complete visibility into your digital security. It scans Websites, Web apps, APIs, Networks and Mobile Applications to detect threats like RCE, SQL injection, XSS, misconfigurations, and outdated components.

With real-time detection, custom scan options, and easy-to-understand reports, VWrap helps teams quickly find vulnerabilities and provides recommendations to fix them before attackers can take advantage. Whether you're securing a single site or managing large systems, VWrap is built for speed, accuracy, and ease of use.

Security Consultation

At Debug Security, our Security Consultation service is tailored to help organizations understand and strengthen their overall cybersecurity posture. We go beyond tools we help you build a security-first culture through strategic guidance, risk identification, and system hardening.

Security Awareness Training

We help build a cyber-aware workforce by training employees on best practices, real-world threats, and their roles in protecting the organization. Human error is the weakest link we help you strengthen it.

Penetration Testing Advisory

Our team guides you through simulated attacks to uncover weaknesses in your systems, networks, and applications. We provide a clear action plan for defense and resilience, customized to your environment.

SOC Gap Assessment

We assess your organization's readiness to build or upgrade a Security Operations Center (SOC), evaluating people, processes, and technologies. Our consultation helps you align SOC capabilities with business goals.

Security Risk Assessment

We evaluate your environment from an attacker's perspective, helping you identify critical vulnerabilities and prioritize remediation efforts. This includes technical, organizational, and operational risk analysis.

Compliance & Policy Guidance

We provide expert recommendations to help you align with frameworks such as OWASP, ISO 27001, GDPR, and local regulatory standards. Our goal is to make compliance simpler and more achievable.

METHODOLOGY

At Debug Security, we follow a structured and industry-aligned methodology to ensure every security assessment is thorough, repeatable, and results-driven. Our process combines both automated tools and manual techniques based on globally accepted standards such as OWASP, PTES, NIST SP 800-115, and OSSTMM.

OWASP TOP 10 VULNERABILITIES

OWASP TOP 10 VULNERABILITIES

At Debug Security, we use the OWASP Top 10 (2021) as a core standard for web application security testing. It guides our manual and automated assessments to ensure all critical vulnerabilities such as broken access control, cryptographic failures, and injection flaws are thoroughly tested. Our team develops targeted test cases based on each OWASP category and integrates them into both manual reviews and our in-house tool, VWrap Scanner. During audits, we simulate real-world attacks and assess how each risk applies to the specific technologies in use. Finally, we map all findings to OWASP categories in our reports, helping clients understand each issue's impact and prioritize remediation effectively.

VULNERABILITY ASSESSMENT METHODOLOGY

AT DEBUG SECURITY, OUR TESTING APPROACH BEGINS WITH SCOPE DEFINITION, WHERE WE IDENTIFY THE ASSETS TO BE ASSESSED, SUCH AS WEB APPLICATIONS, APIS, MOBILE APPS, CLOUD INFRASTRUCTURE, AND IOT DEVICES. THE ENGAGEMENT IS GOVERNED BY A SIGNED NDA AND APPROVED TESTING WINDOWS TO ENSURE SECURITY AND TRANSPARENCY. THE TESTING PROCESS IS DIVIDED INTO THREE STRUCTURED PHASES.

SCOPE DEFINITION

TESTING PROCESS

PHASE 1 (DISCOVERY)

WE USE OUR IN-HOUSE TOOL, VWRAP, TO PERFORM PORT SCANNING, SERVICE ENUMERATION (E.G., IDENTIFYING VERSIONS OF SSH, FTP), AND CVE MAPPING BASED ON NVD AND CVSS SCORES.

ANALYSIS

PHASE 2 (ANALYSIS)

WE CONDUCT MANUAL VALIDATION TO ELIMINATE FALSE POSITIVES AND PRIORITIZE RISKS. SEVERITY LEVELS ARE DEFINED BY CVSS SCORES: CRITICAL (9.0–10) MUST BE REMEDIATED WITHIN 24 HOURS, WHILE HIGH (7.0–8.9) REQUIRES ACTION WITHIN 72 HOURS. FINALLY,

DISCOVERY

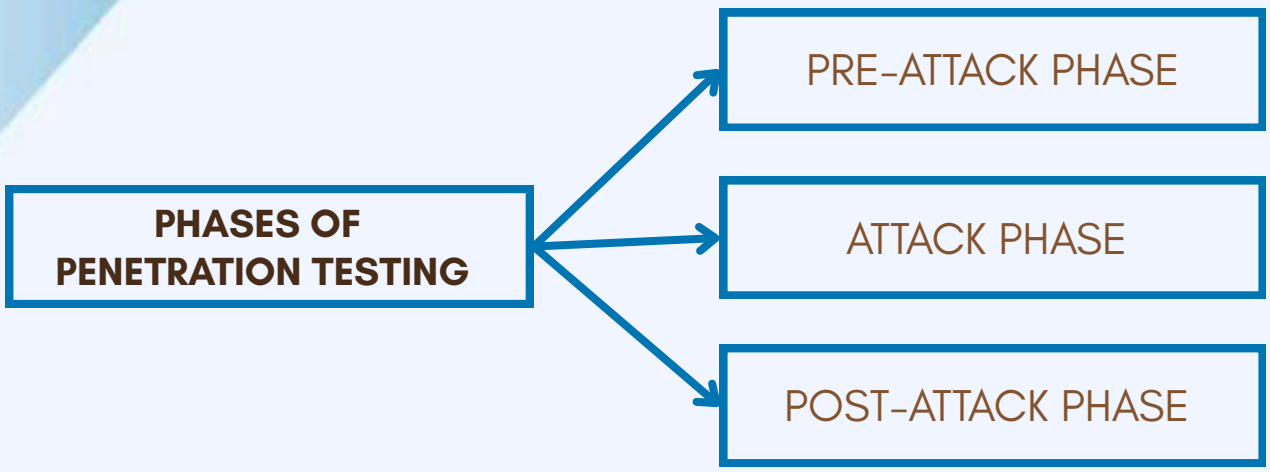
PHASE 3 (REPORTING)

DELIVERS TWO KEY OUTPUTS: AN EXECUTIVE SUMMARY FOCUSED ON BUSINESS IMPACT, AND A TECHNICAL REPORT CONTAINING DETAILED FINDINGS, INCLUDING POC SCREENSHOTS, CURL COMMANDS, AND REMEDIATION STEPS.

REPORTING

PENETRATION TESTING METHODOLOGY

AT DEBUG SECURITY, OUR PENETRATION TESTING METHODOLOGY IS DESIGNED TO SIMULATE REAL-WORLD CYBERATTACKS UNDER CONTROLLED CONDITIONS. THIS HELPS ORGANIZATIONS IDENTIFY EXPLOITABLE VULNERABILITIES, TEST THEIR DEFENSES, AND UNDERSTAND THE BUSINESS IMPACT OF SECURITY BREACHES. THE PROCESS IS DIVIDED INTO THREE MAIN PHASES:



PRE-ATTACK PHASE

OSINT (OPEN-SOURCE INTELLIGENCE) GATHERING

BEFORE LAUNCHING ANY ATTACK SIMULATIONS, WE COLLECT PUBLICLY AVAILABLE INFORMATION TO MAP THE TARGET ENVIRONMENT.

- WE USE TOOLS LIKE HUNTER.IO TO HARVEST EMPLOYEE EMAILS, WHICH COULD BE USED FOR PHISHING OR CREDENTIAL STUFFING ATTACKS.
- DNSDUMPSTER IS USED TO DISCOVER SUBDOMAINS AND DNS RECORDS THAT MAY EXPOSE HIDDEN SERVICES OR STAGING ENVIRONMENTS.
- SOCIAL MEDIA, GITHUB, AND COMPANY JOB POSTINGS ARE ALSO ANALYZED FOR LEAKED CREDENTIALS OR INFRASTRUCTURE CLUES.

THREAT MODELING

BASED ON THE OSINT FINDINGS, WE PERFORM THREAT MODELING TO UNDERSTAND POTENTIAL ATTACK SURFACES AND DEFINE REALISTIC SCENARIOS.

- WE IDENTIFY HIGH-RISK VECTORS SUCH AS PHISHING, API ABUSE, INSECURE FILE UPLOADS, OR PRIVILEGE ESCALATION PATHS.
- THE GOAL IS TO SIMULATE THE MINDSET OF AN ATTACKER WITH LIMITED INITIAL ACCESS, PLANNING A PATH TOWARD CRITICAL SYSTEMS.

ATTACK PHASE

THIS PHASE INVOLVES HANDS-ON EXPLOITATION OF THE DISCOVERED WEAKNESSES ACROSS BOTH EXTERNAL AND INTERNAL ATTACK SURFACES.

EXTERNAL TESTING

- WEB APPLICATIONS
  - WE TEST FOR VULNERABILITIES FROM THE OWASP TOP 10, SUCH AS SQL INJECTION (SQLI), CROSS-SITE SCRIPTING (XSS), SERVER-SIDE REQUEST FORGERY (SSRF), AND INSECURE DESERIALIZATION.
  - BEYOND TECHNICAL FLAWS, WE MANUALLY TEST FOR BUSINESS LOGIC VULNERABILITIES, SUCH AS UNAUTHORIZED ACCESS, PRICE MANIPULATION, OR WORKFLOW ABUSE.
- NETWORK INFRASTRUCTURE
  - ATTEMPT TO BYPASS FIREWALLS USING TECHNIQUES LIKE ICMP TUNNELING OR PROTOCOL SMUGGLING.
  - PERFORM PASSWORD SPRAYING ATTACKS ON EXPOSED SERVICES LIKE RDP, SMB, OR KERBEROS, IDENTIFYING WEAK CREDENTIALS OR MISCONFIGURED AUTHENTICATION.

INTERNAL TESTING (POST-COMPROMISE SIMULATION)

IF INTERNAL ACCESS IS GRANTED (OR ASSUMED THROUGH SUCCESSFUL PHISHING), WE SIMULATE ACTIONS THAT AN ATTACKER MIGHT TAKE AFTER BREACHING PERIMETER DEFENSES.

- LATERAL MOVEMENT: USE TOOLS AND TECHNIQUES LIKE PASS-THE-HASH, REMOTE WMI, OR PSEXEC TO MOVE ACROSS MACHINES.
- PRIVILEGE ESCALATION: ATTEMPT TO ELEVATE PRIVILEGES USING KNOWN EXPLOITS LIKE DIRTYPIPE, SUDO MISCONFIGURATIONS, OR KERNEL-LEVEL WEAKNESSES.
- DATA EXFILTRATION SIMULATION: IDENTIFY SENSITIVE DATA (E.G., PII, CREDENTIALS, BUSINESS SECRETS) AND DEMONSTRATE HOW IT COULD BE EXTRACTED.

PRE-ATTACK PHASE

EVIDENCE PRESERVATION

- ALL ACTIONS ARE LOGGED AND ARCHIVED USING TOOLS SUCH AS METASPLOIT LOGS, PCAP FILES, AND TERMINAL TRANSCRIPTS.
- THIS HELPS IN RECREATING THE TEST SCENARIO AND PROVIDES A DEFENSIBLE AUDIT TRAIL FOR COMPLIANCE PURPOSES.

SYSTEM RESTORATION

- ANY CHANGES MADE DURING TESTING ARE REVERTED TO MAINTAIN PRODUCTION STABILITY.
- WE ASSIST IN RESTORING SNAPSHOTS, REPAIRING ACCESS CONTROL LISTS (ACLS), AND REMOVING TEMPORARY TEST ACCOUNTS OR PAYLOADS.
- A RETESTING PHASE MAY BE SCHEDULED AFTER REMEDIATION TO VERIFY ALL VULNERABILITIES ARE PROPERLY ADDRESSED.

MOBILE APP SECURITY METHODOLOGY

AT DEBUG SECURITY, WE APPROACH MOBILE APP SECURITY WITH A LAYERED TESTING STRATEGY FOCUSED ON IDENTIFYING VULNERABILITIES IN BOTH THE CODE AND RUNTIME BEHAVIOR OF ANDROID AND IOS APPLICATIONS. OUR METHODOLOGY ALIGNS WITH INDUSTRY STANDARDS LIKE OWASP MASVS AND UTILIZES TOOLS SUCH AS VWRAP SCANNER, BURP SUITE, MOBSF, AND JADX-GUI ENSURING END-TO-END VISIBILITY AND PROTECTION.

Static Analysis (SAST)

We perform source code and binary analysis without executing the application to uncover insecure configurations and logic flaws early in development.

Tools Used: MobSF, QARK, VWrap Scanner

Key Checks Include:

- Hardcoded keys, tokens, or credentials in the APK.
- Insecure Broadcast Receivers, exported components, or misconfigured permissions.
- Weak or misused cryptographic functions and insecure storage mechanisms.

Dynamic Analysis (DAST)

This stage focuses on runtime testing to evaluate how the app behaves when it's running in a test environment.

Tools Used: Burp Suite, VWrap Scanner

Key Activities:

- Burp Suite is used to intercept and fuzz API calls to detect insecure endpoints, broken authentication, or data leaks.
- VWrap Scanner performs runtime testing of mobile APIs, insecure communication channels, misconfigured security headers, and more all without requiring rooted devices or complex instrumentation.

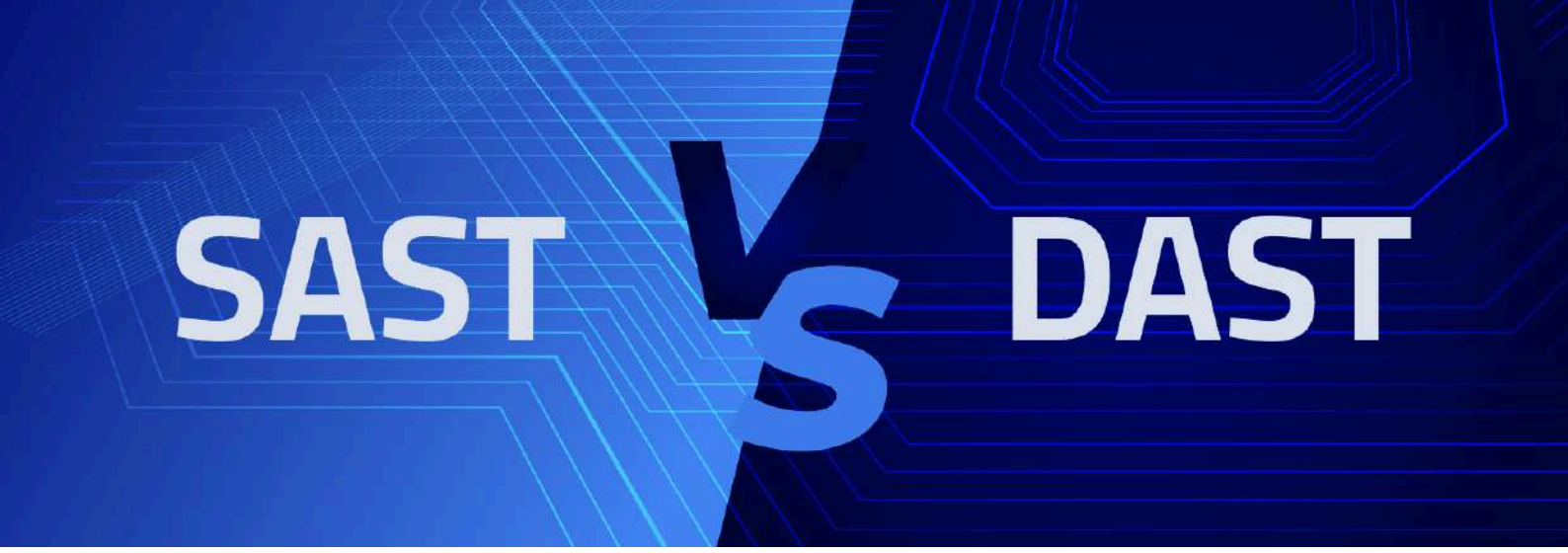
Reverse Engineering

Reverse engineering helps us understand internal logic, expose hidden functions, and simulate attacker behavior.

Tools Used: Jadx-GUI, apktool

Key Activities:

- APK decompilation to inspect code for sensitive logic, API keys, and unsafe practices.
- Tampering tests, such as modifying behavior to bypass root detection (e.g., with Magisk modules) or debug flags.



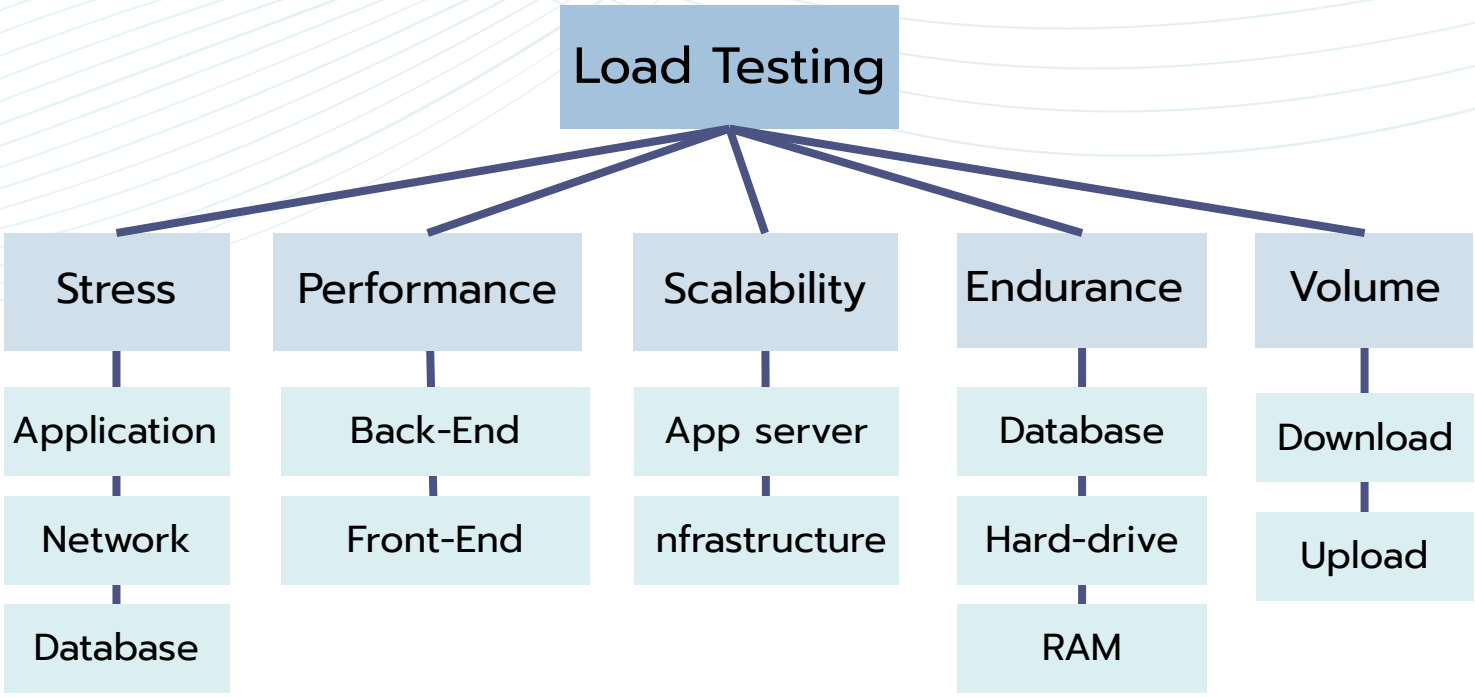
	SAST	DAST
1	SAST (Static Testing): This is a white-box testing approach, where the application's source code or compiled binaries are analyzed without executing the program. It helps uncover flaws within the code itself, including syntax errors, insecure functions, or improper input validation.	DAST (Dynamic Testing): A black-box testing method, DAST tests the application in its running state—mimicking the actions of a real attacker. It requires no knowledge of the source code and focuses on how the app behaves during execution, especially under attack conditions.
2	Performed early in the Software Development Life Cycle (SDLC)—typically during development or in CI/CD pipelines. This helps developers fix issues before deployment, reducing cost and risk.	Conducted on a deployed or staging version of the application. It's often used in QA or pre-production environments to find issues that appear only at runtime.
3	Generally faster and automated, it can be integrated into build systems for continuous analysis. Ideal tools include QARK, MobSF, SonarQube (VWrap supports parts of it).	Usually slower and more intensive, since it interacts with the app in real-time. Tools like Burp Suite and VWrap Scanner are used to fuzz inputs, inspect behavior, and log responses.
4	Detects code-level issues such as hardcoded secrets, buffer overflows, logic errors, and insecure function use. It's particularly good at finding vulnerabilities that can't be seen externally.	Detects runtime flaws like broken authentication, insecure session management, input validation issues (e.g., XSS, SQLi), and exposed APIs—things that manifest during user interaction.
5	Offers deep insights into the structure and security posture of the code but lacks context of how the app operates in production. May produce false positives without validation.	Offers real-world simulation of attacks and provides actionable results. However, it doesn't pinpoint the exact code location of issues—making remediation slower if not combined with SAST.

RED TEAM ASSESSMENT METHODOLOGY

Red Team Assessment is a simulated cyberattack that mimics real-world threat actors to test an organization’s detection, response, and defense capabilities. It evaluates not just technical security, but also human and procedural readiness against advanced threats.

At Debug Security, our Red Team assessments simulate advanced, persistent threats (APT) using real-world adversarial techniques. The objective is to test not just technical vulnerabilities, but also an organization's detection, response, and resilience. We blend manual tradecraft with automated capabilities using trusted tools like VWrap Scanner for surface mapping and vulnerability identification during early reconnaissance and lateral phases.

Load & Performance Testing Methodology



At Debug Security, our Load and Performance Testing services ensure your applications and infrastructure perform reliably under varying conditions. We simulate realistic workloads to assess responsiveness, stability, and scalabilityenabling you to deliver a seamless experience to users even during peak demand. We use industry-standard tools like JMeter, Locust, and our in-house analysis framework.

Our ISO 27001 services are designed to align your Information Security Management System (ISMS) with international best practices.

Our Services Include:

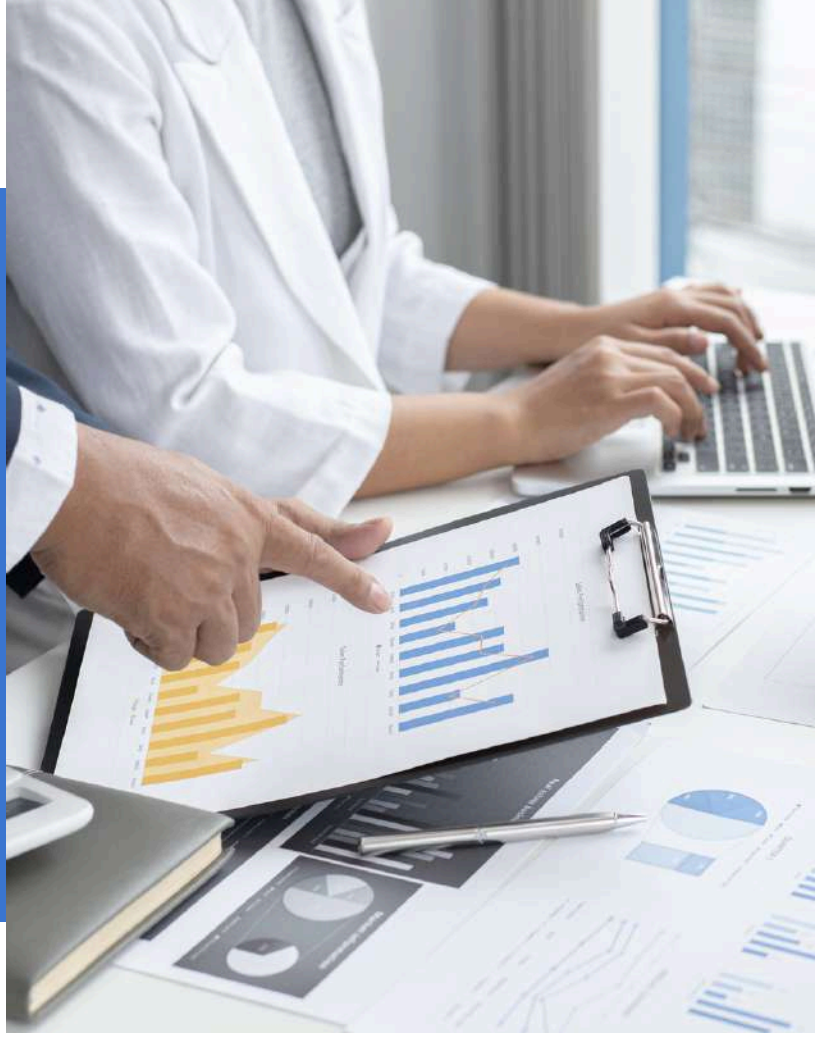
- **Gap assessment and risk analysis**
- **Documentation: IS policies, SoA, Risk Treatment Plan**
- **Implementation of Annex A controls**
- **Integration of security into development processes**
- **Audit preparation and ongoing support**

Benefits:

- **Enhances market trust and compliance posture**
- **Reduces reputational and legal risks**
- **Boosts internal process maturity and risk response**
- **Enables global business and partnerships**

PCI-DSS Compliance Services

At Debug Security, we help businesses that process, store, or transmit payment card data meet PCI-DSS standards.



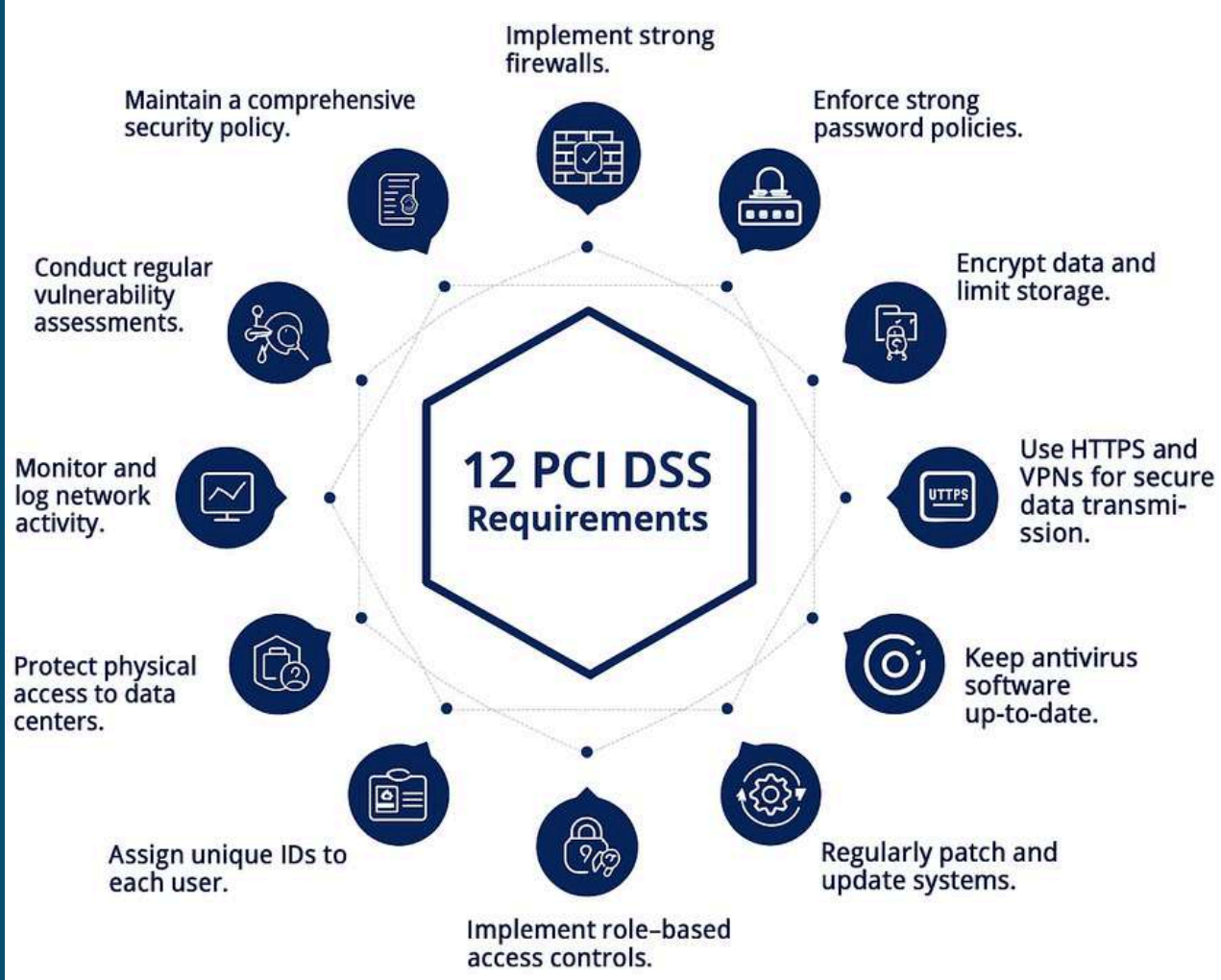
Our Approach:

- Perform a full risk profile and asset inventory.
- Develop a custom PCI compliance plan.
- Implement access controls, encryption, monitoring, and patch management.
- Use tools like VWrap Scanner for vulnerability scans and compliance validation.

Deliverables:

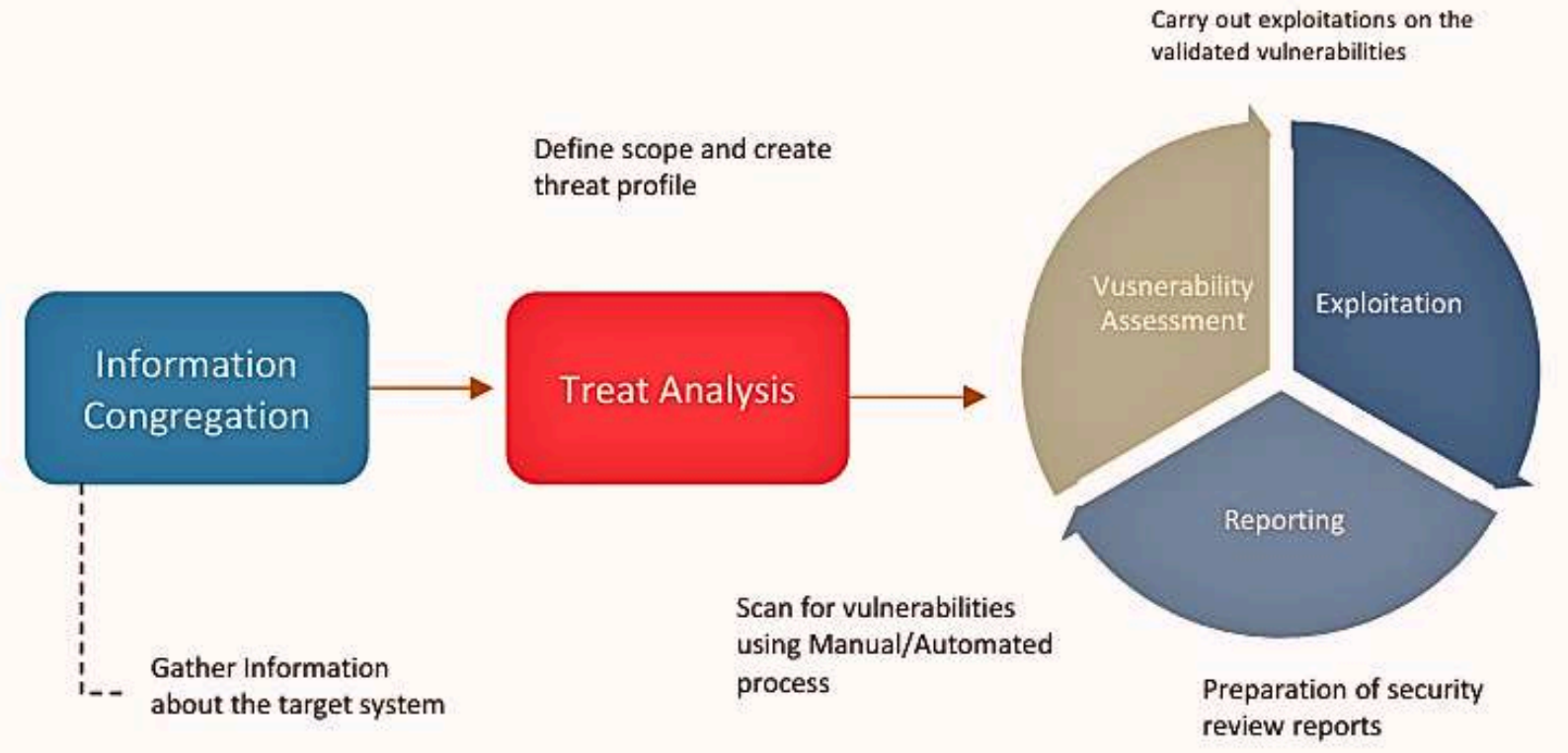
- PCI Compliance Roadmap
- Technical Configuration & Gap Reports
- Remediation Support
- Quarterly Audit Reports

PCI DSS Rqquirements



System Vulnerability Testing

Our system vulnerability testing will be follow the bellow methodology



API SECURITY TESTING

Our API assessments validate RESTful, SOAP, GraphQL, and custom APIs through:

- **Authentication/Authorization Checks (OAuth2, JWT).**
- **Injection & Data Exposure Tests using tools like Postman, Burp Suite, and VWrap Scanner.**
- **Rate Limiting, Replay, and Throttling Tests.**
- **Functional and Load Tests using jMeter and REST Assured.**

We simulate real-world abuse scenarios to ensure your APIs are not a backdoor to your business.

SOURCE CODE REVIEW

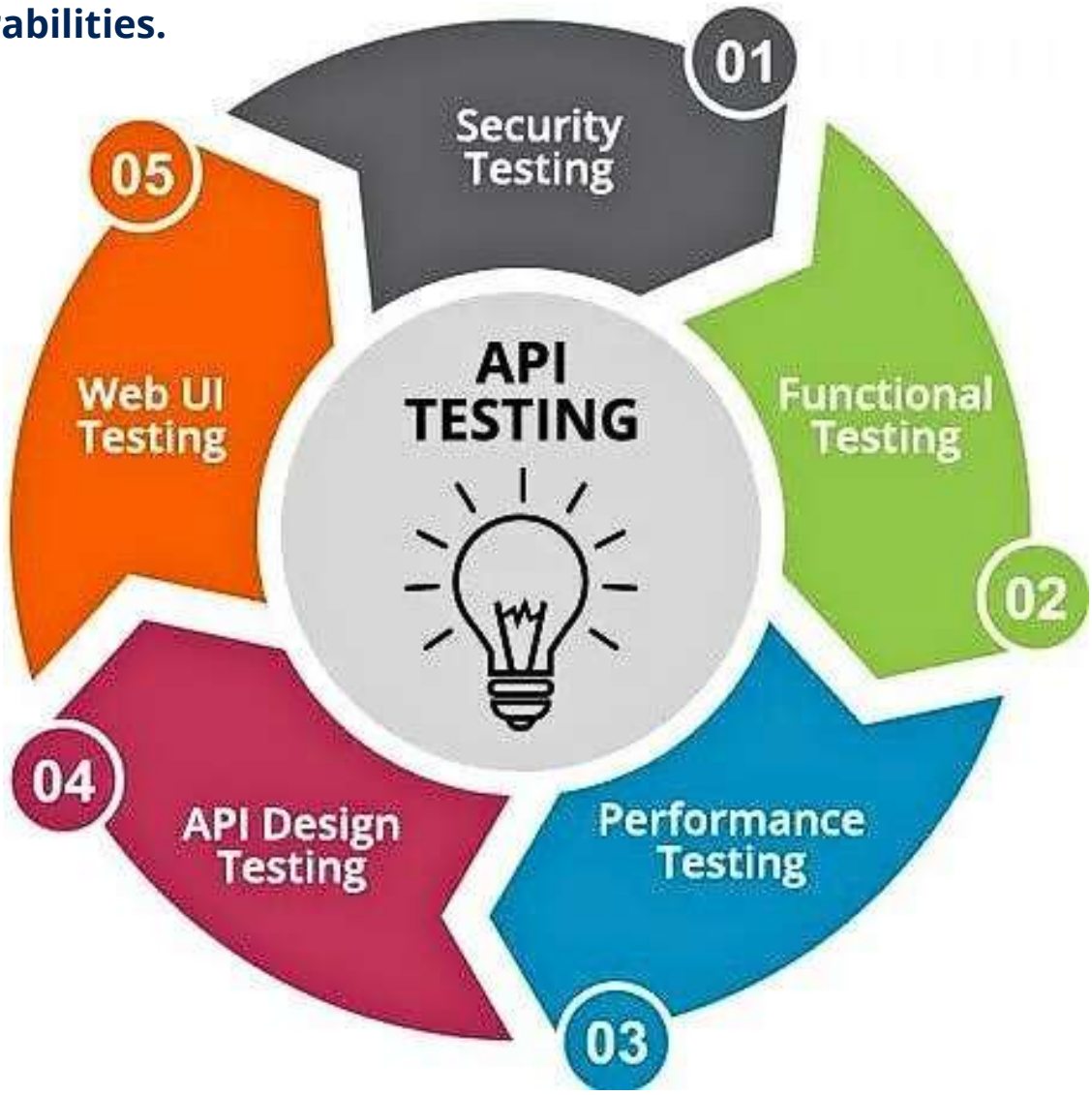
We perform in-depth source code reviews to identify insecure coding practices, logic flaws, and overlooked vulnerabilities. Our audits cover:

- **Manual & Automated Review using tools like SonarQube, Snyk and JetBrains Space.**
- **Static/Dynamic Analysis, tailored for languages like PHP, JavaScript, Python, C# .Net, etc.**
- **Secure Coding Practice Validation against OWASP, CERT, and language-specific standards.**
- **Code audits can be conducted as white-box or grey-box assessments, depending on the project scope.**

API SECURITY TESTING

API Security Testing ensures that APIs are protected from unauthorized access, data breaches, and malicious attacks. It involves testing authentication, authorization, input validation, rate limiting, and data encryption. The goal is to identify flaws like broken object-level access, improper authentication, or data exposure. Tools like Burp Suite and VWrap Scanner are used to detect and exploit API-specific vulnerabilities.

Types of API testing are given:



System Infrastructure & Database Testing

Our Infrastructure Testing covers network devices, virtual environments, cloud assets, and security appliances. It ensures your infrastructure is hardened and monitored against evolving threats.

Database Testing focuses on

- Authentication & Access Control: Ensuring proper user roles and permission sets.
- Data Integrity & Injection Protection: Safeguarding against SQL Injection and logic tampering.
- Stress & Load Testing: Evaluating database behavior under heavy queries and concurrent sessions.
- Whether your backend uses MySQL, PostgreSQL, MongoDB, or enterprise-grade systems, our tests ensure data confidentiality, integrity, and availability.

System Vulnerability Testing

At Debug Security, our system vulnerability testing begins with defining the testing scope and understanding the target environment. The goal is to uncover weaknesses in applications, servers, endpoints, and infrastructure before they can be exploited.

Key Milestones

- Use of Intrusion Detection and Prevention Systems (IDPS) to identify malicious activity.
- Authentication control checks on all internal and external communication endpoints.
- Validation of all form fields, headers, cookies, and payloads against global best practices.
- Enforcement of page-level access control and session integrity.
- Verification of strong encryption for data in transit and at rest.
- We follow a structured methodology to ensure every attack surface is examined using automated tools like VWrap Scanner combined with manual analysis.

BUSINESS LOGIC TESTING

Business logic vulnerabilities result not from technical flaws but from process misuse. We simulate logical misuse and abuse paths in:

- Presentation Layer: Input/output validation, workflow bypasses.
- Business Layer: Improper discount logic, order manipulation.
- Data Layer: Data leakage via object relationship flaws.

Our testers map the intended vs. actual behavior of your application to uncover issues that automated scanners typically miss.

REPORTING FORMAT

The overall report format that apply for technical summary is following:

Our reporting framework at Debug Security is structured to deliver clear, actionable, and technically sound insights. We provide comprehensive details about every vulnerability discovered, ranked by severity, and supplemented with remediation guidance, ensuring our clients can address each issue with clarity and confidence.

REPORTING FORMAT

INTERIM REPORTS & POST-EXECUTION ACTIVITIES

During and after assessment phases, we deliver interim reports for ongoing visibility. These documents highlight vulnerabilities that could impact your organization's security posture, even if no exploitation was achieved. Every finding technical, procedural, or environmental is validated as per the project scope and execution schedule.

All findings are rated using industry-standard scoring models (CVSS/NVD). Where applicable, we highlight the potential risk based on both exploitation probability and business impact. If required, reports are submitted for internal approval before project closure.

Severity Scoring

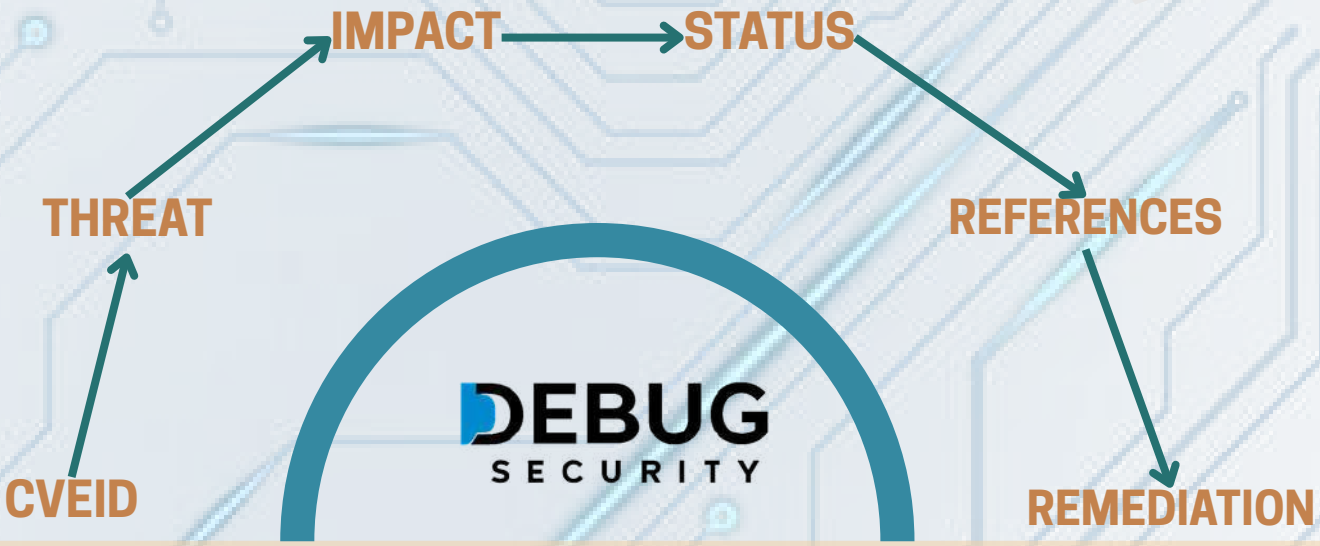
Not all vulnerabilities carry the same risk. We assign risk rankings to prioritize remediation efforts. Our severity classification references the following industry standards:

- CVSS (Common Vulnerability Scoring System)
- CVE (Common Vulnerabilities and Exposures)
- CWE (Common Weakness Enumeration)
- NVD (National Vulnerability Database)
- OSVDB (pen Source Vulnerability Database)
- Bugtraq ID (BID)

If a custom scoring mechanism is adopted (e.g., adjusted based on business impact or threat likelihood), a clear rationale is included to explain deviation from industry benchmarks.

Debug Security provide CVE assignment information to the CNA level above them using the following format. The use of this format facilitates the automation of CVE assignment.

REPORTING FORMAT



VULNERABILITY METRICS

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. The official CVSS documentation can be found at **https://www.first.org/cvss/**

Vulnerability Severity Ratings: We provide qualitative severity rankings of "Low", "Medium", "High", "Critical" for CVSS v3.1 base score ranges for this project

CVSS v3.1 Ratings	
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Sample Report

Vulnerability Summary & Report

The following tables illustrate the vulnerabilities found by impact and recommended remediation:

Vulnerability Findings

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
1	2	0	1	0

Finding	Risk	
	Risk Rating	Severity
SQL Injection	9.8	Critical
Stored XSS	8.2	HIGH
Server-Side Template Injection	8.0	High
Error Page Disclosure	3.0	Low

Technical Findings

1. **< Name of the Vulnerability >**

9.8 CRITICAL

Host:	:	example.com
Path	:	<where is the vulnerability found>
Confidence	:	Confident
Method	:	$_GET() / $_POST
Tools/Payload	:	<Method that are used to exploit>

WORKING PROCEDURE

At Debug Security, our working process is structured, transparent, and tailored to meet each client's unique security needs. We follow a step-by-step approach to ensure thorough assessment, clear communication, and actionable outcomes.

1. PLANNING & SCOPING

We begin by defining the scope of the assessment, identifying assets, targets, goals, and limitations. A Non-Disclosure Agreement (NDA) is signed, and timelines are finalized.

2. INFORMATION GATHERING

We collect data about the target environment using passive and active reconnaissance techniques. This includes domain info, open ports, exposed services, and technologies in use.

WORKING PROCEDURE

3. VULNERABILITY IDENTIFICATION

Using both automated scanners (like our VWrap Scanner) and manual testing, we identify security flaws in the target system, application, or network.

4. EXPLOITATION

We attempt to exploit critical vulnerabilities in a controlled manner to demonstrate the impact and prove the existence of the flaws without causing real damage.

5. POST-EXPLOITATION & PRIVILEGE ESCALATION

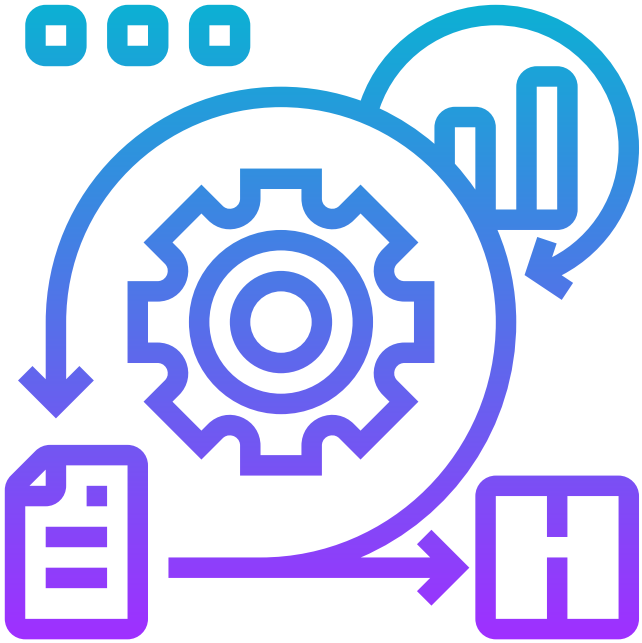
If access is gained, we test for lateral movement, privilege escalation, and data exposure showing how deep an attacker could go if the vulnerability were exploited.

6. REPORTING

A detailed report is prepared with vulnerability details, risk ratings, PoC (Proof of Concept), business impact, and actionable remediation steps. Reports are designed for both technical and non-technical audiences.

7. REMEDIATION SUPPORT & RETESTING

We begin by defining the scope of the assessment, identifying assets, targets, goals, and limitations. A Non-Disclosure Agreement (NDA) is signed, and timelines are finalized.



CERTIFICATE
& ACHIEVEMENT

OFFENSIVE SECURITY OSCP

CISA Certified Information Systems Auditor. An ISACA® Certification

ISC2 CC SM

FORTINET NSE

LEAD AUDITOR ISO 27001 Information Security Management System

EHE Ethical Hacking Essentials

CEH Certified Ethical Hacker

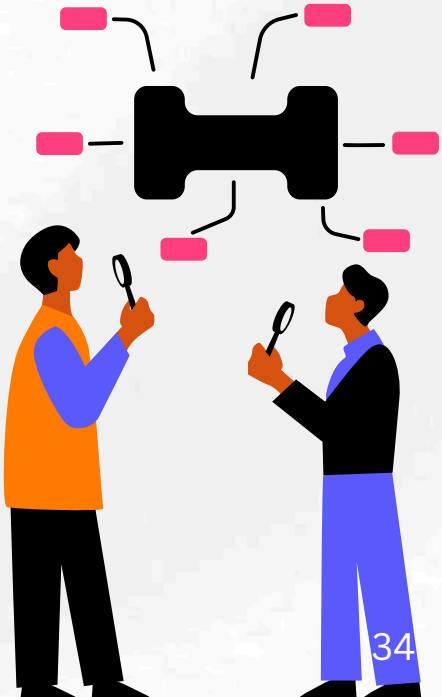
Project 30+

70+ CVE

7+ Years Experience

OUR STRENGTHS

1. Premium-Grade Services
2. Aligned with Global Standards
3. Time & Cost Effectiveness
4. Innovation-Driven Technology



DEBUG SECURITY

FUTURE PLAN

A COMPREHENSIVE STRATEGY FOR FUTURE SUCCESS.

- Launching a desktop version of VWrap Scanner for offline environments.
- Integrating AI and machine learning for faster, more intelligent threat detection.
- Establishing a SOC to provide 24/7 monitoring and incident response.
- Offering cybersecurity training and awareness programs for organizations.
- Investing in R&D to explore advanced technologies like IoT and cloud security.

Your security is our priority

Let's build a safer digital world.

DEBUG SECURITY

CONTACT US

+88 01727 957 026

info@debugsec.com

debugsec.com

188/2/A Road# Kakoli Road, Ahmed Nagar,
Mirpur, Dhaka-1216