bluedog SECURITY MONITORING

bluedog VAPT

"Forewarned is Forearmed"

With bluedog ISO27001 certified VAPT Service, organizations of all sizes now have the power to protect themselves with either an affordable recurring automated VAPT or an intensive one-time manual VAPT service.

What is VAPT?

Vulnerability Assessment and Penetration Testing (VAPT) as the name suggests scans your public facing network interfaces and website to find any vulnerabilities that can be exploited by cyber criminals to gain entry to your network or the workings of your website.

Because VAPT is such an important weapon in your armory against cyber-attacks, at bluedog we offer a suite of VAPT services to suit all operational scenarios and budgets, all of which are backed by our 24/7 fully staffed SOC.

We offer both automated VAPT scanning and a manual Penetration Testing service.

Key Features of bluedog VAPT

- ✓ Over a million different checks are done each time.
- ✓ Performs active reconnaissance.
- ✓ Scans against direct exploitation.
- ✓ Performs partial authentication and authorization bypass.
- ✓ Updated for new issues daily from multiple trusted sources.
- ✓ Provides detail over time.
- ✓ See the full coverage of each scan through our dashboard and generate report anytime.
- ✓ Handles the false positives.
- ✓ Provides descriptions, insights, detection, summary, solutions, and other hosts with the same issue in one view.
- ✓ Reviewed and governed by the bluedog 24/7 Security Operation Center.

bluedog Automated VAPT

Automated VAPT is a low cost way to keep your eye on the state of your network and website either on a regular monthly basis or maybe a one-off snapshot.

The process is non-invasive and will not cause any downtime or harm to your network or website.

A regular VAPT scan will show you how your security is improving over time, the reports we generate highlight deficiencies and vulnerabilities to enable you to strengthen your defenses.

bluedog Manual Penetration Testing

While Automated VAPT is an amazing way to fill in your compliance gaps and provides detailed insight on an ongoing basis. We cannot change the fact that cybercriminals are people who know how to adapt, which is why bluedog also offers a Manual Penetration Testing Service.

The bluedog team has more than 20 years' experience in ethical hacking and have conducted manual pentests to almost all verticals in over 30 countries. Our team of experts is capable of identifying and exploiting different vulnerabilities of any verticals.

	Automated VAPT	Manual VAPT
Reconnaissance		
Passive		✓
Active	✓	✓
Issue Scope		
Exploitation Types	Direct exploitation	Combining issues
Existing Exploits	✓	✓
Create new exploits		✓
Business logic exploit		✓
Authentication bypasses	partial	✓
Authorization bypassed	partial	✓
Lateral Movement		✓
Reporting	Automated Report	Custom Report
Management Summary	✓	✓
Proof of concept	✓	✓
Retest capability	In full only	Custom testing possible

Test Checklist

Each scan tests over 1,000,000 vulnerabilities and grows every day; obviously too many to list here. However, the list of key features below gives a feel for the depth of our manual and automated scanning, which is based on recognised OWASP global standards.

Information Gathering

- Conduct Search Engine Discovery and Reconnaisance for Information Leakage (OTG-INFO-001)
- Fingerprint Web Server (OTG-INFO-002)
- Review Webserver Metafiles for Information Leakage (OTG-INFO-003)
- Enumerate Applications on Webserver (OTG-INFO-004)
- Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)
- Identify application entry points (OTG-INFO-006)
- Map execution paths through application (OTG-INFO-007)
- Fingerprint Web Application Framework (OTG-INFO-008)
- Fingerprint Web Application (OTG-INFO-009)
- Map Application Architecture (OTG-INFO-010)

Configuration and Deployment Management Testing

- Test Network/Infrastructure Configuration (OTG-CONFIG-001)
- Test Application Platform Configuration (OTG-CONFIG-002)
- Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)
- Review Old, Backup and Unreferenced Files for Sensitive Information (OTG-CONFIG-004)
- Enumerate Infrastructure and Application Admin Interfaces (OTG-CONFIG-005)
- Test HTTP Methods (OTG-CONFIG-006)
- Test HTTP Strict Transport Security (OTG-CONFIG-007)
- Test RIA cross domain policy (OTG-CONFIG-008)

Identity Management Testing

- Test Role Definitions (OTG-IDENT-001)
- Test User Registration Process (OTG-IDENT-002)
- Test Account Provisioning Process (OTG-IDENT-003)
- Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
- Testing for Weak or unenforced username policy (OTG-IDENT-005)

Authentication Testing

- Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)
- Testing for default credentials (OTG-AUTHN-002)
- Testing for Weak lock out mechanism (OTG-AUTHN-003)
- Testing for bypassing authentication schema (OTG-AUTHN-004)
- Test remember password functionality (OTG-AUTHN-005)
- Testing for Browser cache weakness (OTG-AUTHN-006)
- Testing for Weak password policy (OTG-AUTHN-007)
- Testing for Weak security question/answer (OTG-AUTHN-008)
- Testing for weak password change or reset functionalities (OTG-AUTHN-009)
- Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)

Authorisation Testing

- Testing Directory traversal/file include (OTG-AUTHZ-001)
- Testing for bypassing authorization schema (OTG-AUTHZ-002)
- Testing for Privilege Escalation (OTG-AUTHZ-003)
- Testing for Insecure Direct Object References (OTG-AUTHZ-004)

Session Management Testing

- Testing for Bypassing Session Management Schema (OTG-SESS-001)
- Testing for Cookies attributes (OTG-SESS-002)
- Testing for Session Fixation (OTG-SESS-003)
- Testing for Exposed Session Variables (OTG-SESS-004)
- Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)
- Testing for logout functionality (OTG-SESS-006)
- Test Session Timeout (OTG-SESS-007)
- Testing for Session puzzling (OTG-SESS-008)

Input Validation Testing

- Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)
- Testing for Stored Cross Site Scripting (OTG-INPVAL-002)
- Testing for HTTP Verb Tampering (OTG-INPVAL-003)
- Testing for HTTP Parameter pollution (OTG-INPVAL-004)
- Testing for SQL Injection (OTG-INPVAL-005)
- Oracle Testing
- MySQL Testing
- SQL Server Testing
- Testing PostgreSQL (from OWASP BSP)
- MS Access Testing
- Testing for NoSQL injection
- Testing for LDAP Injection (OTG-INPVAL-006)
- Testing for ORM Injection (OTG-INPVAL-007)
- Testing for XML Injection (OTG-INPVAL-008)
- Testing for SSI Injection (OTG-INPVAL-009)
- Testing for XPath Injection (OTG-INPVAL-010)
- IMAP/SMTP Injection (OTG-INPVAL-011)
- Testing for Code Injection (OTG-INPVAL-012)
- Testing for Local File Inclusion
- Testing for Remote File Inclusion
- Testing for Command Injection (OTG-INPVAL-013)
- Testing for Buffer overflow (OTG-INPVAL-014)
- Testing for Heap overflow
- Testing for Stack overflow
- Testing for Format string
- Testing for incubated vulnerabilities (OTG-INPVAL-015)
- Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)
- Testing for Error Handling
- Analysis of Error Codes (OTG-ERR-001)

- Analysis of Stack Traces (OTG-ERR-002)
- Testing for weak Cryptography
- Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)
- Testing for Padding Oracle (OTG-CRYPST-002)
- Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

Business Logic Testing

- Test Business Logic Data Validation (OTG-BUSLOGIC-001)
- Test Ability to Forge Requests (OTG-BUSLOGIC-002)
- Test Integrity Checks (OTG-BUSLOGIC-003)
- Test for Process Timing (OTG-BUSLOGIC-004)
- Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)
- Testing for the Circumvention of Workflows (OTG-BUSLOGIC-006)
- Test Defences Against Application Misuse (OTG-BUSLOGIC-007)
- Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)
- Test Upload of Malicious Files (OTG-BUSLOGIC-009)

Client-Side Testing

- Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
- Testing for JavaScript Execution (OTG-CLIENT-002)
- Testing for HTML Injection (OTG-CLIENT-003)
- Testing for Client-Side URL Redirect (OTG-CLIENT-004)
- Testing for CSS Injection (OTG-CLIENT-005)
- Testing for Client-Side Resource Manipulation (OTG-CLIENT-006)
- Test Cross Origin Resource Sharing (OTG-CLIENT-007)
- Testing for Cross Site Flashing (OTG-CLIENT-008)
- Testing for Clickjacking (OTG-CLIENT-009)
- Testing WebSockets (OTG-CLIENT-010)
- Test Web Messaging (OTG-CLIENT-011)
- Test Local Storage (OTG-CLIENT-012)

Subscription Plans

Name	*Essential VAPT*	*Pro VAPT*	*One-Off VAPT*	*Manual VAPT*
Type	Automated VAPT	Automated VAPT	Automated VAPT	Manual VAPT (with VPN Connection)
Frequency	Monthly Scan	Monthly Scan	One-off Scan	One-off Penetration Test
Features	Includes all key features	Includes all key features	Includes all key features	Includes all the key features, fully customisable
Scope	Scans up to 4 IPs and 1 website	Scans up to 16 IPs and 1 website	Scans up to 16 IPs and 1 website	Custom IP ranges
	Low monthly subscription	Low monthly subscription	One-off Fee	Daily Rate

To find out more about our VAPT Service and our other solutions, email us at **sales@bluedogsec.com** or visit **bluedog-security.com**.

CERTIFIED ISO 27001 CERTIFIED

bluedog SECURITY MONITORING