ASCOTBARCLAY™

www.ascotbarclay.com
info@ascotbarclay.com

HACKER HARDENING™ SERVICE

KEEP HACKERS OUT AND SECURE YOUR FUTURE

Are you concerned that you have been hacked or are susceptible to cyber compromise?

Our affordable and comprehensive Professional Application Testing is here to help you protect your critical information, data and reputation.

APPLICATION PENETRATION TESTING

APPLICATION TESTING METHODOLOGY

Application testing is the practice of testing a computer system, network or web application to find vulnerabilities that an attacker could exploit. The main objective is to determine security weaknesses and to help you become **Hacker Hardened™**. The process includes gathering information for target applications before the test, identifying possible entry points and attempting, with your written permission of course, to break in.

A penetration test can be used to test your security policy compliance, your level of staff security awareness and your organisation's ability to identify and respond to security incidents.

Our standard testing procedure is divided into nine phases:

1. INFORMATION GATHERING

a. Reconnaissance for Information Leakage
b. Fingerprinting Web Server
c. Crawling the application
d. Scanning for open ports on the server
e. Review Webpage Comments and Metadata for Information Leakage
f. Identify application entry points
g. Map execution paths through application
h. Fingerprint Web Application Framework
i. Fingerprint Web Application
j. Map Application Architecture

2. IDENTITY MANAGEMENT TESTING

a. Test Role Definitions
b. Test User Registration Process
c. Test Account Provisioning Process
d. Testing for Account Enumeration and Guessable User Account
e. Testing for Weak or unenforced username policy

3. AUTHENTICATION TESTING

a. Testing for Credentials Transported over an Encrypted Channel
b. Testing for default credentials
c. Testing for Weak lock out mechanism
d. Testing for bypassing authentication schema
e. Test remember password functionality
f. Testing for Browser cache weakness
g. Testing for Weak password policy, Weak security question/answer
h. Testing for weak password change or reset functionalities
i. Testing for Weaker authentication in alternative channel
j. Testing for bypasses of 2-factor authentication

4. AUTHORISATION TESTING

a. Testing Directory traversal/file include
b. Testing for bypassing authorisation schema
c. Testing for Privilege Escalation
d. Testing for Insecure Direct Object References
e. Session Management Testing
f. Input Validation Testing
g. Error Handling
h. Cryptography
i. Business Logic Testing
j. Client Side Testing

5. SESSION MANAGEMENT TESTING

a. Testing for Bypassing Session Management Schema
b. Testing for Cookies attributes
c. Testing for Session Fixation
d. Testing for Exposed Session Variables
e. Testing for Cross Site Request Forgery (CSRF)
f. Testing for logout functionality
g. Test Session Timeout
h. Testing for Session puzzling

6. INPUT VALIDATION TESTING

a. Testing for Reflected Cross Site Scripting
b. Testing for Stored Cross Site Scripting
c. Testing for HTTP Verb Tampering, HTTP Parameter pollution
d. Testing for SQL Injection, LDAP Injection, ORM Injection, XML Injection
e. Testing for SSI Injection, XPath Injection, IMAP/SMTP Injection, Code Injection
f. Testing for Local File Inclusion, Remote File Inclusion, Command Injection
g. Testing for Buffer overflow, Heap overflow, Stack overflow
h. Testing for Format string, incubated vulnerabilities, HTTP Splitting/Smuggling

7. TESTING FOR ERROR HANDLING

a. Analysis of Error Codes, Stack Traces
b. Testing for weak Cryptography, weak SSL/TLS Ciphers, Insufficient TLP
c. Testing for Padding Oracle
d. Testing for Sensitive information sent via unencrypted channels

8. BUSINESS LOGIC TESTING

a. Test Business Logic Data Validation, Ability to Forge Requests
b. Test Integrity Checks, Test for Process Timing
c. Test Number of Times a Function Can be Used Limits
d. Testing for the Circumvention of Work Flows
e. Test Defences against Application misuse
f. Test Upload of Unexpected File Types
g. Test Upload of Malicious Files

9. CLIENT SIDE TESTING

a. Testing for DOM based Cross Site Scripting
b. Testing for JavaScript Execution
c. Testing for HTML Injection
d. Testing for Client Side URL Redirect
e. Testing for CSS Injection
f. Testing for Client Side Resource Manipulation
g. Test Cross Origin Resource Sharing
h. Testing for Cross Site Flashing
i. Testing for Clickjacking
j. Testing WebSockets
k. Test Web Messaging
l. Test Local Storage

On completion, we produce a report on the findings and define the best mitigation paths for minimising risk and plugging the vulnerabilities. Our standards ensure the use of the best security testing practises and provide insight into your organisations security risk levels and the minimisation of any risk identified.

RESILIENCE THROUGH REGULAR TESTING

We offer a fixed price managed service to meet your budget, risk appetite and the level of threat faced by your organisation at just £1000 per test based on our monthly platinum service. Regular testing accounts for changes in the dynamic nature of your business and the ever evolving threat landscape, providing our most robust service.

Note:

Our testing methodology is priced to be effective and efficient and delivers productive results at low cost. All our tests are carried out by certified professionals with deep knowledge supported by years of experience. Tailored or specialised testing can be conducted subject to agreement. All testing is conducted with written permission from the client and on agreed terms at the clients own risk and on the understanding that no testing company can guarantee 100% security.

SERVICES	STARTER	SILVER	GOLD	PLATINUM
Hours of Testing	10	25	60	90
OWASP Top10	10	25	●	●
WASC	●	●	●	●
Business Logic Testing	●	●	●	●
WAF Testing & Bypass	●	●	●	●
Automated Test	●	●	●	●
Manual Test	-	●	●	●
In-depth POC	●	●	●	●
Mitigation Support	-	-	●	●
Retest	-	-	-	●

Hacker Hardened™

Contact us today to book your slot on our testing schedule:

ASCOT BARCLAY

71-75 Shelton Street, Covent Garden
London, UK, WC2H 9JQ
+44 (0)20 3897 2249
info@ascotbarclay.com
www.ascotbarclay.com
ascotbarclay