BLUE GOAT
CYBER

Web Application Penetration Testing Services

Complete Web Application Penetration Testing services against your front-end, back-end (API), and mobile applications

Steps to Schedule Your Web Application Penetration Test:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

Are your web applications secure? We validate this for you with a **Web Application Penetration Test (includes both Black and Gray Box Testing).** Web applications are the most frequently attacked systems on the Internet and are often the most insecure.

We emulate an attacker by utilizing similar techniques to perform reconnaissance, identify vulnerabilities, and break into your systems. Unlike an attacker, however, we stop our test before exposing sensitive data or doing harm to your environment. We start our web application penetration testing with a Black Box (Unauthenticated) Penetration Test – this means we have unauthenticated access and little prior knowledge, except the URLs, about the systems in scope.

We then move to a Gray Box (Authenticated) Penetration Test of each system in scope. With a Gray Box Penetration Test, we have "user" level knowledge and access to a system. A Gray Box Penetration Test is used to test an application that supports multiple users by testing authenticated user access to ensure one user cannot access another user's data or escalate privileges. We test your application using a sample of authenticated users with various roles. We log on to the application as that user and perform testing to see if we can perform any of the following:

Horizontal Privilege Escalation – where an authenticated user can access another user's data. An example of horizontal privilege escalation is a bank application, where an authenticated user's account number appears in a URL. If I can change the account number in the URL to another account number and access another user's banking information, I've just performed a horizontal privilege escalation.

Vertical Privilege Escalation – where an authenticated user can escalate privileges to an administrator-level account. An example of this is a web application with a value representing the username in a hidden field that is returned after successful authentication. What would happen if we changed the value from 'username' to 'root' or administrator' and passed this back to the web application server?

We ensure our testing covers the latest Open Web Application Security Project (OWASP) Top 10, along with the following common web application vulnerabilities:

- SQL injection (Blind, Inference, Classic, Compounded)
- OS command injection (Informed, Blind)
- Server-side code injection
- Server-side template injection
- Reflected XSS
- Stored XSS
- Reflected DOM issues
- Stored DOM issues
- File path traversal/manipulation
- External/out-of-band interaction
- HTTP header injection
- XML / SOAP injection
- LDAP injection
- CSRF
- Open redirection
- Header manipulation
- Server-level issues

METHODOLOGY

We follow a seven-phase methodology designed to maximize our efficiency, minimize risk, and provide complete and accurate results. The overarching seven phases of the methodology are:

- Planning and Preparation
- Reconnaissance / Discovery
- Vulnerability Enumeration / Analysis
- Initial Exploitation
- Expanding Foothold / Deeper Penetration
- Cleanup
- Report Generation

BENEFITS / RETURN ON INVESTMENT

It is better to have an ethical hacker find the holes in your enterprise than an adversary. Our Web Application Penetration Testing Services provide details on exploitable web vulnerabilities in a prioritized, tangible manner. Our report allows you to understand better what your web application looks like from an attacker's perspective; what the "attack surface" looks like. This helps you prioritize efforts to mitigate risk to reduce data breach likelihood.

Not only do our Web Application Penetration Testing Services show you what your attack surface looks like to an adversary, but they can also be used as a safe way to test your organization's incident response capabilities. Our Penetration Testing services can also be used to tune and test your security controls, such as your IDS, Firewall, Web Application Firewall (WAF), Router Access Control Lists (ACLs), etc.

Our Web Application Penetration Testing services also help you meet compliance audit requirements such as HIPAA, PCI DSS, SOC 2 Type 2, and NIST.

DELIVERABLE

The **Web Application Penetration Test Report** includes URLs tested, vulnerabilities discovered, steps taken during the assessment, exploitable areas discovered, and prioritized recommendations. For any systems we exploit, an "Attack Narrative" section is used to discuss step-by-step the process we used to gain access, escalate privileges, etc.

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

☎ (307) 317-8884

✉ info@bluegoatcyber.com