BLUE GOAT
CYBER

White Box Penetration Testing Services

As ethical (white hat) hackers, 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. With a White Box Penetration Test, we test a system with "administrator" or "root" level access and knowledge. This often includes access to architecture diagrams, design documents, specifications, and source code. A White Box Penetration Test is the most thorough and time-consuming.

A White Box Penetration Test is commonly used in the following scenarios:

- An organization is developing their own product
- An organization is developing their own software application
- An organization is integrating several products or applications

Steps to Schedule Your White Box 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

If you are developing your own product or application accessible over a computer network (wired or wireless), you should have it thoroughly tested to ensure it is not "hackable." White Box Penetration Testing is extremely important for devices that process, store, or transmit sensitive data and for devices involved with critical infrastructure, such as Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems. White Box Penetration Testing should also be a priority for devices used in healthcare or hospital environments where a compromised device could result in a violation of patient privacy, such as the release of Protected Health Information (PHI), or even become a threat to a patient, such as the compromise of a drug infusion pump.

If you are performing systems or product integration, White Box Penetration Testing is equally important, especially if you are responsible for the integration of components from multiple vendors. We have found numerous bugs and flaws in components designed and developed by a supplier for an integrated critical system.

There are three primary coverage areas used in white box penetration testing manual source code review:

- Path coverage
- Statement coverage
- Branch coverage

Path coverage looks at linearly independent paths throughout the code. This coverage is aimed at all paths. It determines if every path has been crossed.

Statement coverage tests all executable statements in the code at least once. It uncovers unused or missing statements and branches

Branch coverage tests all branch codes. It maps the code into branches of conditional logic and checks that all branches are covered.

Other coverage areas for white box source code review include:

- Decision coverage
- Condition coverage
- Multiple condition coverage
- Finite state machine coverage
- Control flow testing
- Data flow testing

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 (ROI)

We think it is better to have an ethical hacker find the holes into your enterprise than an adversary or insider. Our Penetration Testing provides details on exploitable vulnerabilities in a prioritized, tangible manner. Our report allows you to better understand what your device, application, or system looks like from an attacker perspective. This helps you prioritize efforts to mitigate risk to reduce breach likelihood or damage.

Our White Box Penetration Testing services also help you meet compliance audit requirements such as HIPAA, SOC 2, PCI DSS, and FISMA.

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

☎ (307) 317-8884
✉ info@bluegoatcyber.com