WhiteHat SECURITY

Business Logic Assessments

Uncovering flaws in application business logic

Business logic is the intended behavior and functionality that governs the core of what the application does. Hackers exploit business logic vulnerabilities in many ways to gain unauthorized access to websites. Session handling, credit card transactions, and password recovery are just a few examples of web-enabled business logic processes that malicious hackers have abused to compromise major websites.

Automated scanners cannot detect business logic flaws in applications, as they cannot be programmed to understand the context. These flaws can only be detected via manual testing, thus it is imperative to compliment the automated testing process with manual assessments by security experts. To understand the functionality of an application and to find unconventional ways in which a vulnerability can be exploited by a hacker, we need to approach security through the eyes of the hacker to find weaknesses.

Accurate detection of business logic vulnerabilities

WhiteHat Sentinel Dynamic Premium Edition (PE) service offers special testing to find business logic vulnerabilities through Business Logic Assessments (BLAs). Experienced security engineers from WhiteHat Security's Threat Research Center (TRC) perform manual business logic assessments, focused on:

- Mapping the entire application
- Examining sensitive areas of production applications
- Finding issues unlikely to be found via automated scanning
- Testing applications not accessible by automated scanners
- Assessing applications that cannot be tested in production-safe ways via automation
- Checking for authentication and authorization issues
- Identifying hard-to-find technical vulnerabilities such as blind XSS and blind SQLi
- Reviewing a detailed vulnerability checklist to ensure complete testing
- Maintaining a proprietary log to ensure all testing is documented

The BLAs include an evaluation of user-application interactions such as:

- Account Profile/Account Settings
- Account Transactions/Account History
- Checkout
- Contact Us
- File Upload
- Forgotten Username or Password
- Authentication/Authorization
- Session Management
- Registration
- Search
- Shopping Cart Processes (adding/removing items, updating the cart)
- Site Administration

Business logic vulnerabilities evaluated by TRC include:

- Clickjacking
- Cross-Site Scripting
- Cross-Site Request Forgery
- Embedded Flash and Silverlight modules
- Information Leakage
- SQL Injection
- Insufficient Authentication
- Insufficient Authorization
- Insufficient Transport Layer Protection

WhiteHat SECURITY

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com