High Level Web Application Risk Review

Overview

The High Level Web Application Risk service is designed to determine if an application's security is reasonable to protect associated sensitive data. This review enables companies to quickly determine if applications are vulnerable to basic level exploits without going through an in-depth penetration test. The High Level Web Application Risk Review is accomplished by performing scheduled and selective probes of the application or companies provide prior test results. Additionally, Emagined Security consultants assess the sensitivity of the web application's data. At the end of the review, risk is analyzed to determine if urgent comprehensive penetration test is required. Using this approach you can make educated decisions on where to apply your security funds and don't need to spend a fortune on testing every application.

Benefits

Do you know which of your own or your business partner's web applications should be reviewed further for security vulnerabilities? Which applications out of the hundreds you work with should be reviewed with our security budgets? Do clients want you to prove that your low risk application has undergone a basic security reviews?

Emagined Security's High Level Web Application Risk Review is designed for you to determine if your programmers applied the basic level protection to web applications and if it is acceptable based upon the sensitivity of associated data. In particular, the High Level Web Application Risk Review will:

- Provides a basic "battle-test" for a web application
- Assess a web application to determine if sensitive information is present
- Provides a mini risk assessment is performed so it can be determined if urgent comprehensive penetration testing is warranted
- Finally, a letter is created with Emagined Security's recommendation

Description of Service

Emagined Security's High Level Web Application Risk Review focuses on performing only automated portions a web application scan or reviewing prior tests. Additionally, Emagined Security consultants will assess the sensitivity of the web application to determine a risk level and if an additional penetration test should be required. At the end of the engagement, a basic level risk

level report will be provided along with raw test results so the company can determine the best approach moving forward.

Phase1) Reconnaissance:
During this phase the application's security controls are tested to determine if an attack may result in inappropriately viewing, altering, copying or deleting information. During passive website mapping, testing is performed mimicking up to two types of users:

- Unauthorized User attempting to gain access
- Authorized User trying to acquire and utilize enhanced or inappropriate privileges

Phase 2) Verification:
Automated checks are performed at this level to review control effectiveness such as automatable areas of the OWASP top 10:

- Encryption / SSL Testing
- HTML Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Cookie Poisoning
- Executable code testing such as buffer overflows and IIS weaknesses
- Etc.

Manual testing is not performed at this level. Manual testing can be performed during a subsequent penetration test if needed or desired.

Phase 3) Data Sensitivity Review
Emagined Security then will work to determine what sensitive data is being protected / processed. Emagined Security will use authenticated (if credentials are provided) or unauthenticated access to assess the data types and data sensitivity levels.

Phase 4) Urgent Penetration Test Warranted Decision

At the end of the review, Emagined Security will perform a mini risk assessment to determine if urgent comprehensive penetration test was warranted. This assessment will be based upon the following type of data:

- Potential Vulnerably Level
- Data Sensitivity Level Identified
- Brand Damage Potential