Web Application Discovery & Risk Prioritization

Overview

Do you have thousands of Web Applications but not know where your greatest risk lies? Do you have no idea of what Web Applications are online in your IP range and don't know where to being on assessing their risk?

Web Application Discovery and Risk Prioritization enables Emagined Security to quickly scan our client's entire IP range and associated URLs for running applications on common web ports. Once the web applications are discovered each application is scanned to determine the complexity and associated security risk vectors. Once each web application is reviewed, the applications are prioritized so our clients can begin performing Web Application Penetration Testing in a strategic manner.

Benefits

Web Application Discovery and Risk Prioritization is a unique service only available at Emagined Security. Many companies do not have a method for getting a handle on risks associated with their web presence. Many of these companies have old abandoned applications sitting vulnerable to attack. Many of these companies are assessing the low risk applications while high value targets are left vulnerable. Through the use of our custom tool, Emagined Security can:

- Identify all of your web applications running on standard ports in your IP range
- Assess your running web applications to determine potential risk
- Identify key risk identifiers like authentication mechanism, presence of credit card transactions, etc.
- Prioritize your web presence so companies can begin assessing risk in a strategic manner

Description of Service

The following table presents Emagined Security's methodology:

Phase	Description
1	Data Gathering
2	Website & IP Scanning
3	Penetration Test Scoping & Prioritization Report

PHASE 1: Data Gathering

Emagined Security will work with our client to gather required data to perform the assessment. Data required will consist of associated IP addresses and known websites / web applications URLs.

PHASE 2: Website Scanning

Emagined Security will perform an Internet based scan of the associated websites / web applications using a Emagined Security proprietary tool. This effort will be performed using the following tasks:

- Scan for unidentified URLs on associated IPs
- Scan of identified URLs and discovered URLs for relevant statistics
  - Number of accessible pages
  - Login identification
  - Web Server versions
  - Operating systems
  - Programming language
  - Headers
- URL Data Report Creation

All websites must be accessible during the Emagined Security discovery.

Sample site: www.abc.com

Priority: High **HTTP:** Yes	**Effort:** High **HTTPS:** No	**Web Application:** Yes
Web Crawler Stats: Pages: 43	Links: 175	Avg. Page Size: 1.69 kb
Web Server: Server: Apache	SSL Cert Valid: n/a	Operating System: Linux

Figure 1- www.abc.com

PHASE 3: Penetration Test Scoping & Prioritization Report

Emagined Security will use information gathered in Phases 1 & 2 to develop a Web Application Risk Prioritization Document that will group applications into risk order and suggest a levels of effort required for each application.

- Prioritization of websites / web applications
  - Websites / web applications risk level score
  - Suggested level of effort / scope
  - Suggested test schedule