

Matta Assessment Services



Application Security Assessment Service Overview and Information

Introduction

As an independent Information Risk Management company, **Matta** represents the new breed of Security Consultants. Through combining best practice application security assessment tools with hands-on vulnerability qualification and reporting, **Matta** provides its clients with a comprehensive application security assessment service.

Traditionally, application security assessment involves emulation of highly determined attackers with access to public applications that require a level of security assurance (such as e-commerce or online banking sites with custom written ASP or other server side scripts).

Matta has proven experience in the assessment of primarily ASP and Java-based web systems and server side processes. Our consultants have commercial experience in financial environments writing such scripts, along with querying of back-end servers such as SQL.

Risk Identification & Classification

An important first step in improving the security of any web site or application is to correctly identify areas of risk and set clear priorities in-line with business drivers. **Matta** understands real world network risk and business impact, focusing primarily on three key areas during an application security assessment:

- Resilience of applications from overflow and input validation attack
- Session resilience, attempting to compromise other user sessions
- Assessment of operating platform components and permissions

The **Matta** assessment methodology comprehensively covers each layer of the 7 layer OSI model. **Matta** is the first security consultancy to tackle technical network security in this manner, and offers world-class assessment of both application, network & physical layer devices to ensure complete end-to-end security.

Bespoke Assessment Application

A **Matta Application Security Assessment** is not simply a vulnerability assessment. **Matta** assessment services are offered to clients with a specific business goal or driver in-mind. Examples of bespoke **Matta** assessment services being used by our clients over the last year include:

- Emulation of a determined attack to test an online banking system
- Low-level code review of ASP script for an e-commerce site
- Secure application design consulting regarding Java development

Matta assessment services are geared completely around the client network type and requirement. A plethora of different offensive technologies are used depending on the goal and deliverable, ensuring that true value is realised and overall network security is effectively improved.

Matta Assessment Services



Application Security Assessment Service Overview and Information

Methodology

A standard **Matta Application Security Assessment** methodology used to assess a given ASP-based web site using back-end SQL database servers would involve the following being undertaken:

- A complete dump of the publicly accessible components being downloaded, allowing for insight into potential configuration files and arguments passed to scripts directly through POST and other HTTP methods.
- Comprehensive assessment of each and every script argument to test for overflow bugs (heap, stack, et al) and input validation problems such as format string input and SQL injection techniques.
- Use of publicly known web service vulnerabilities to attempt to circumvent environment security through reading fragments of protected system files (such as global.asa or other configuration files containing DSN connection strings)
- Full assessment of the web service and its enabled options (checking for responses to commands such as HTTP PUT)

The tools and systems selected are best of breed for a comprehensive application security assessment to be carried out. Due to the complex nature of assuring the security of custom built environments, many components are undertaken by hand in-line with a clear assessment methodology.

Client deliverables include a hand written report, clearly documenting the current state of application network security, and recommendations for improvement of server configuration, permissions, and bounds checking within accessible scripts. Due to the fact that **Matta** reports are hand written, the findings and recommendations are tailored with both the client business drivers, and technical network configuration in mind.