Web Application Assurance

Meeting the challenges of securing your Web Applications requires a commitment to a process of a continuous security program. New web attacks, updated code and content, and the supporting infrastructure mean that protecting your applications is a full-time job.

Ongoing consultant-based Web Application testing is too expensive to be practical, and should be reserved to annual tests, major new code releases, or new webapp launches.

However, leaving your Web Application untested for 12 months may leave your critical data at risk for an unacceptable length of time.

WebCheck™ is a revolutionary new service that bridges the gap between consultant tests, and acts as a critical component in 'Defense in Depth' best practice approach.

The Path to Web Application Security

WEB CHECK

Meeting the challenges of securing your Web Applications requires a commitment to a process of a continuous security program. New web attacks, updated code and content, and supporting web application infrastructure mean that protecting your applications is a full-time job.

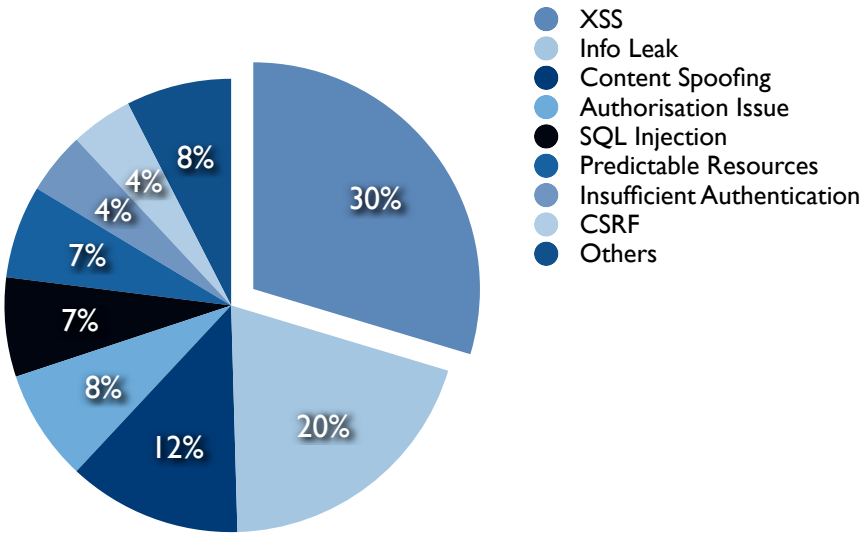
Modern Web Applications are now more dynamic and complex than ever. This flexibility is good for your business, but raises unprecedented challenges in security.

WebCheck™ helps you secure your Web Applications.

Webcheck™ is a unique service which combines the deep testing of a consultant with Integrity Auditor™, an intelligent auditing program which looks for suspicious changes between scans.

Over 60% of tested Web Applications contain Critical or High Risk vulnerabilities, over 80% would fail a PCI audit.

Run automatically as a service either daily or weekly, WebCheck™ is the most comprehensive fully automated Web Application and Integrity Checking service in the market today.



Vulnerabilities found on web applications during 2008

WEB CHECK

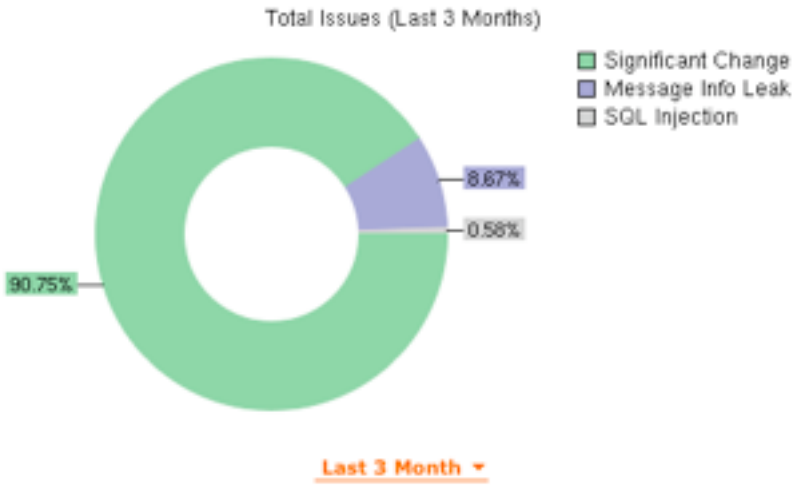
Reporting is on demand, and can be configured to send alerts triggered by events and broken thresholds.

The crystal-clear reports quickly let you see where the issues and suspicious changes reside.

The WebCheck™ portal allows reports to be downloaded. Clean and professional 2D charts show important metrics over user-customisable time frames.

Multiple Web Applications can be monitored simultaneously, giving you a single security portal for all your Web Applications.

Compliance requirements such as PCI require a pro-active approach to testing web applications, and these stipulations are likely to become more prominent as the threat of security breaches via applications continue to grow.



WEB CHECK

1. Security Report

1.1 Application Details

URL	[redacted]
Web pages scanned	78
Scan start time	24 March 2009 - 13:38:03
Scan time	1:12:24
Scan end time	24 March 2009 - 14:50:27

1.2 Summary

Number of Changes	[Baseline Scan]
Number of Vulnerabilities	2

1.3 Changes Detected

1.3.1 No changes were detected during the scan.

1.4 Vulnerabilities Detected

1.4.1 Comprehensive vulnerability scans were conducted and the following potential issues were identified.

SQL Injection	HIGH

Vulnerability

1.4.2 SQL Injection Vulnerabilities were discovered in the following scripts:

- [redacted]
- [redacted]
- [redacted]

1.4.3 When injecting SQL statements into a query being executed it is possible to either provide invalid SQL which throws an error, or in certain cases to supply SQL which evaluates as 'false'. The result of this is that either incomplete page data is retrieved from the database or a PHP (or other website scripting language) error is displayed on the resulting page.

1.4.4 By alternately supplying valid and invalid SQL data, or data that causes alternations between false and true evaluations it is possible to determine if unusual behaviour triggered in scripts is indeed being caused by the interpretation of supplied SQL.

Recommendations

1.4.5 Matta consultants recommend taking the following actions:

- It is important to ensure that all unquoted values, such as numbers are in fact numeric. Type checks should be used wherever possible in order to do this.
- It is also highly important to strip or escape all single-quote (') characters from any user-supplied input to any script before that data is used in a query to an SQL database.

Functionality Overview

Vulnerabilities

Crawler	HTML, Java Script, AJAX
Injection Attacks	Non-Blind SQL, Blind SQL
Cross Site Scripting	Reflected XSS
Cookie Evaluation	Session cookies evaluated, cookie secure flag check
Malicious Files	Searches for malicious content
Message Information Leak	Verbose error messages are tracked
Information Passed in Clear Text	Identify information that may be at risk in cleartext communication
Session Management	Session fixation and other session management issues

Integrity Audit

Defacement	Unique signature verification, Lexicon Scanning
Static Content Change	Small changes, significant changes, suspicious changes
Page Decomposition	WebCheck can understand the difference between dynamic and static content
Content Hashing	no data ever copied from your webapp for analysis

WEB CHECK

Matta
Falstaff House
34 Bardolph Road
Richmond Upon Thames
Surrey
TW9 2LH

Tel. +44 (0)203 051 3420
webcheck.trustmatta.com