SENSITIVE

AUSTRALIAN SPORTS COMMISSION

ATHLETE MANAGEMENT SYSTEM (AMS) SMARTBASE

SECURITY TEST PLAN

Final

Version 1.0

Cordelta

Management Technology People

Preconditions

This security testing plan is dependent on the following preconditions:

1. Sufficient information is provided to the Security Tester(s) by the System Owner in order to carry out the proposed security testing procedures. This includes, but is not limited to:
    a. Location (addresses, domains, URLs) of web resources and applications.
    b. Authentication credentials representing each user group to be tested (see Scope).
    c. Sufficient information about any Web Services (e.g. location of WSDL file, XML schema, sample test SOAP messages, valid encryption certificates) to communicate via SOAP Web Services messaging tools.
2. Approval for the proposed security testing is provided to the Security Tester(s) by the System Owner. Specifically, approval for the activities described in *Annex A: Rules of Engagement* is sought. The signing of this Security Testing Plan serves as the authorisation and entitlement for the Security Tester(s) to access the system (Paragraph 476.2, Cybercrime Act 2003).
3. Acknowledgement from the System Owner is provided to the Security Tester(s) that appropriate procedures have been put in place to recover from a system crash of the infrastructure being tested, and to recover from the corruption of any databases that might be affected from the security testing.

Test Conditions

Objective

The primary objective of the ASC is to independently test the effectiveness of the SMARTBASE system security controls by commissioning a Security Test.

The goal of this task is to ensure the SMARTBASE web application hosted by the ASC meets ISM compliance and technical security objectives, and achieves system certification and accreditation.

Scope

The scope of work for this engagement is primarily to conduct penetration testing and security assessment of the SMARTBASE web application.

The SMARTBASE web application is hosted at the following address:

- External: https://ams.ausport.gov.au (IP Address: 192.188.101.97)
- Internal: 172.20.24.10

The users/roles to be tested will include:

- Administrator;
- Coach; and
- Athlete.

Methodology

Cordelta's web security testing methodology is based on Open Web Application Security Project (OWASP), a globally recognised security testing methodology. The OWASP documentation is also recommended by DSD as detailed in the Australian Government ICT Security Manual (ISM):

> *Control 0971: It is recommended agencies follow the documentation provided in the Open Web Application Security Project guide to building secure web applications and web services.*

In order to tailor the assessment to the requirements, Cordelta will conduct a subset of the OWASP security test cases which will be negotiated with Dean Herpen, Business and System Owner. The test cases outside the scope of this engagement will be clearly identified, while those within the scope will provide succinct results for each test case.

The results of both positive and negative test cases and the tools and techniques to complete these test cases will be shared with ASC staff and stakeholders.

Cordelta's approach to the security testing of web infrastructure, applications and services for this engagement comprises the following tasks:

Phase 1 - Scoping

This phase develops the scope for the testing both in terms of identifying the assets to be tested, and in terms of the test cases to which these assets will be subjected. The identification of assets also identifies the system representatives who must authorise the security testing and to whom the results will be reported.

Phase 2 - Threat Modelling

This phase is concerned with developing an accurate threat model, which ensures the test results are relevant to the business process supported by the target system. The threat model for the application will be drawn from the existing security documentation.

Phase 3 - Execute Test Cases

This phase executes the test cases that have been negotiated with the system representatives. Test cases are selected based on those most appropriate to meet the stated testing objectives.

The Security Testing activities performed by Cordelta utilise a range of tools running on Unix and Microsoft platforms. These tools are used to identify ports and services that are open to the Internet, systems configurations, system and device settings and known vulnerabilities.

Based on the initial information gathered, the following open source and commercial tools listed below may be used in Cordelta's testing of web applications. Testing is conducted using virtual machines stored on partitions encrypted with AES using TrueCrypt.

Phase 4 - Analysis and Reporting

In this phase, all collected data and the results of the scans, probes and attempted exploits are analysed, and a report detailing the findings and recommendations is developed.

Tools

Cordelta utilises industry standard tools to undertake its security testing. As we base our testing methodologies and tools on open standards and common products we are willing to share the toolsets employed during security testing.

Documentation

- Open Security Testing Methodology Manual (OSSTMM), Version 3
- Open Web Application Security Project (OWASP) Testing Guide, Version 3
- The Penetration Testing Execution Standard (PTES), http://www.pentest-standard.org
- NIST SP800-44-rev2 Guidelines on Securing Public Web Severs
- NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- Protective Security Policy Framework (PSPF)
- Australian Government Information Security Manual (ISM) 2012 Release

Software

- VMware Workstation
- BackTrack 5 Linux
- MetaSploit 3 Framework
- Nessus
- GFI LANGuard

Testing will be conducted on Cordelta infrastructure that utilises Truecrypt disk encryption to protect data at rest. All deliverables will be transferred to ASC via write-once media and delivered by hand to the point of contact for this engagement.

Deliverables

The primary deliverable for this engagement is:

1. Security Test Report which will include the following:
    - Executive Summary
    - Explanation of scope of work and the approach taken
    - Summary of results with identified issues
    - Security Assessment of vulnerabilities and impacts
    - Recommendations for mitigation
    - Detailed technical report

Resources

The penetration testing and security assessment of the SMARTBASE web application will be conducted by Chris Marklew and Rebecca Buksh. Chris and Rebecca currently hold a Negative Vetting 1 (NV1) security clearance.

Schedule

Activity	Deliverable	Date (Inclusive)	Estimated Effort (Days)
Execute Test Cases	-	15/04/2013 – 18/04/2013	4
Vulnerability Assess iPhone	-	19/04/2013	1
Risk and Impact Assessment	-	20/04/2013	1
Draft Security Test Report	Security Test Report	21/04/2013 – 22/04/2013	2
			8 Days

**__Note__: Client debrief will be conducted on the morning of Friday 19th April 2013, if any critical/ high vulnerabilities are identified.*

Test Cases

The Security Test Plan comprises of test cases that comply with the OWASP Testing Guide v3.0 web application testing methodology.

Category	Test Reference	Test Case
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers
	OWASP-IG-002	Search Engine Discovery / Reconnaissance
	OWASP-IG-003	Identify application entry points
	OWASP-IG-004	Testing for Web Application Fingerprint
	OWASP-IG-005	Application Discovery
	OWASP-IG-006	Analysis of Error Codes / Information Leakage
Configuration Management	OWASP-CM-001	SSL / TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)
	OWASP-CM-002	DB Listener Testing
	OWASP-CM-003	Infrastructure Configuration Management Testing
	OWASP-CM-004	Application Configuration Management Testing (including Hidden Field analysis and Code Review)
	OWASP-CM-005	Testing for File Extensions Handling
	OWASP-CM-006	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST
Authentication	OWASP-AT-001	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account
	OWASP-AT-004	Brute Force Testing
	OWASP-AT-005	Testing for bypassing authentication schema
	OWASP-AT-006	Testing for vulnerable remember password and password reset
	OWASP-AT-007	Testing for Logout and Browser Cache Management
	OWASP-AT-008	Testing for CAPTCHA
	OWASP-AT-009	Testing Multiple Factors Authentication
	OWASP-AT-010	Testing for Race Conditions
Session Management	OWASP-SM-001	Testing for Session Management Schema
	OWASP-SM-002	Testing for Cookies attributes
	OWASP-SM-003	Testing for Session Fixation and Hijacking
	OWASP-SM-004	Testing for Exposed Session Variables
	OWASP-SM-005	Testing for Cross Site Request Forgery
Authorisation	OWASP-AZ-001	Testing for Path Traversal / Direct Object Reference / URL Manipulation
	OWASP-AZ-002	Testing for bypassing authorisation schema

Category	Test Reference	Test Case
	OWASP-AZ-003	Testing for Privilege Escalation
Business Logic	OWASP-BL-001	Business logic testing
Data (Input) Validation	OWASP-DV-001	Testing for Reflected Cross Site Scripting
	OWASP-DV-002	Testing for Stored Cross Site Scripting
	OWASP-DV-003	Testing for DOM based Cross Site Scripting
	OWASP-DV-004	Testing for Cross Site Flashing
	OWASP-DV-005	SQL Injection
	OWASP-DV-006	LDAP Injection
	OWASP-DV-007	ORM Injection
	OWASP-DV-008	XML Injection
	OWASP-DV-009	SSI Injection
	OWASP-DV-010	XPath Injection
	OWASP-DV-011	IMAP/SMTP Injection
	OWASP-DV-012	Code and Content Injection
	OWASP-DV-013	OS Commanding
	OWASP-DV-014	Buffer overflow (including Format String)
	OWASP-DV-015	Incubated vulnerability Testing
	OWASP-DV-016	Testing for HTTP Splitting/Smuggling
Denial of Service (Allowed with minimal impact. Required to generate noise and therefore trigger Alerts.)	OWASP-DS-001	Testing for SQL Wildcard Attacks
	OWASP-DS-002	Locking Customer Accounts
	OWASP-DS-003	Buffer Overflows
	OWASP-DS-004	User Specified Object Allocation
	OWASP-DS-005	User Input as a Loop Counter
	OWASP-DS-006	Writing User Provided Data to Disk
	OWASP-DS-007	Failure to Release Resources
	OWASP-DS-008	Storing too much Data in a Session
Web Services	OWASP-WS-001	WS Information Gathering
	OWASP-WS-002	Testing WSDL
	OWASP-WS-003	XML Structural Testing
	OWASP-WS-004	Content-level Testing
	OWASP-WS-005	HTTP GET parameters / REST Testing
	OWASP-WS-006	Naughty SOAP attachments
	OWASP-WS-007	Replay Testing
AJAX Testing	OWASP-AJ-001	AJAX vulnerabilities
	OWASP-AJ-002	AJAX testing

Annex A: Rules of Engagement

The Rules of Engagement (RoE) provide a summarised list of which activities may be performed and those that are expressly forbidden.

Activity	Execution Permission
Network Infrastructure Scanning and Vulnerability Identification	ALLOWED
Web Application and Services Scanning and Vulnerability Identification	ALLOWED
Network Infrastructure Vulnerability Probing and Proof of Concept (PoC)	ALLOWED
Web Application and Services Vulnerability Probing and Proof of Concept (PoC)	ALLOWED
Network Infrastructure Vulnerability Exploitation	ALLOWED
Web Application and Services Vulnerability Exploitation	ALLOWED
Denial of Service (DoS) Testing and Exploitation	ALLOWED
Modification of Data	ALLOWED
Brute Force Login Attempts	ALLOWED

The Project Manager and Primary Contact acknowledge:

- Testing of the web application will be conducted externally to the Commission.
- Testing of Network Infrastructure components will be excluded from testing.
- That the testing and/or exploitation of some vulnerabilities may cause disruptions to services on Servers, Devices and Services under review;
- It is the System Owner's responsibility to maintain backups and other means of recovering services and data that may be adversely affected;
- It is the System Owner's responsibility to inform the Primary Contact of any detected adverse effects caused by testing and early termination of testing if required due to these adverse effects;
- It is the System Owner's responsibility to obtain permission to carry out testing on third party owned systems and devices that are included in the scope for testing;
- It is the System Owner's responsibility to inform any third parties connecting to systems of the testing and potential disruptions to services;
- It is the System Owner's responsibility to verify the accuracy of the resource locators that are included in the Scope prior to commencement of security testing;
- Agreement to inform Primary Contact immediately of any changes to ownership of above application, or the inclusion of any third party servers, devices and services used by the application;
- Agreement to the Schedule of testing as listed in this document, and to inform Primary Contact immediately if a variation to the schedule is required; and

- The results of vulnerability identification and exploitation is neither conclusive or static. Vulnerabilities and exploits are continually discovered and developed resulting in the findings of the security test having a limited shelf life.