Tiger Scheme
Senior Security Tester -
Web Applications
Notes to Candidates

Title	**Notes to Candidates on SST - Web Applications**
Version	1.4
Status	Public Release
Date	15th August 2019
Author	Mathew Evans

Version	Date	Author	Changes and Comments
1.0	-	Professor Andrew Blyth	-
1.1	13/03/13	Konstantinos Xynos	-
1.2	15/07/13	Konstantinos Xynos	-
1.3	8/10/13	Konstantinos Xynos	Minor amendments and corrections
1.4	15/08/19	Mathew Evans	Minor amendments and corrections

Table of Contents

1. Introduction

1.1 Setting the Scene

1.1.1 The Tiger Scheme Senior Security Tester - Web Applications Assessment is designed to assess candidates against a baseline of practical skills in testing Web Applications. The aim of the Assessment is to ensure candidates can perform a complete and thorough technical Web Application Security test within the criteria described in the OWASP Testing Guide v5.0.

1.1.2 The majority of this document is dedicated to describing the breadth and depth of knowledge required to complete the Tiger Scheme Senior Security Tester Assessment - Web Applications successfully and attain Senior Tester status. This document should be read in conjunction with the following:

- The Tiger Scheme Code of Conduct;
- The OWASP Testing Guide v5.0.

1.1.3 To indicate the depth of knowledge required, this document will use two terms:

- **Understand**: candidates must know about the existence, technical details and security implications of a subject, but are not required to demonstrate the knowledge practically
- **Demonstrate**: candidates must know about the existence, technical details and security implications of a subject, and will be required to demonstrate this knowledge practically.

1.2 Access to information

1.2.1 The Assault Course is an open book assessment; candidates may use any reference materials they feel are appropriate. They are allowed to use printed and digital sources of information.

1.3 Confidentiality

1.3.1 Candidates must not disclose the content or structure of the Tiger Scheme Senior Security Tester - Web Applications Assessment. Furthermore, candidates are reminded that these notes may not be reproduced without the permission of Tiger Scheme.

1.3.2 It should be noted that prior knowledge of the Assault Course network and setup will be of little use to the candidate, as it is constantly updated and revised (within the constraints set). Candidates will be required to demonstrate a thorough understanding of the theory behind the tools and techniques they use, and explain in detail to the assessors their analysis of the results obtained and any conclusions

drawn. Without this knowledge, a candidate will not pass the Assessment.

2. Scope, Schedule, Methodology and Equipment

2.1 The Scope of the Assessment

2.1.1 The Assessment schedule is divided into the following 5 Stages:

Key	Stage Description
S1	Submission of prior written report
S2	Multiple Choice Examination
S3	Written Examination
S4	Practical assessment
S5	Viva – Oral defence of practical assessment

2.1.2 The pass mark for each stage is 60%

2.1.3 The complete assessment schedule will span two days, and to pass the overall assessment the candidate is required to pass all 5 stages.

2.1.4 The overall marking/grading scheme is as follows:

Stage 1 (S1)	-	Marks: /040	-	Weight(%): 10%
Stage 2 (S2)	-	Marks: /060	-	Weight(%): 10%
Stage 3 (S3)	-	Marks: /050	-	Weight(%): 10%
Stage 4 (S4)	-	Marks: /300	-	Weight(%): 60%
Stage 5 (S5)	-	Marks: /050	-	Weight(%): 10%
TOTAL	**-**	**Marks: /500**	**-**	**Weight(%): 100%**

2.1.5 There are two Tiger Scheme Assessment Decisions: Pass or Fail.

2.1.6 **Pass:** The candidate has successfully completed the components assessed and is competent to fulfill the role of a Tiger Scheme Web Application Senior Security Tester. The Pass is valid for 3 years.

2.1.7 **Fail:** The candidate has not successfully completed the components and is required to improve the areas of weakness identified in the feedback information before rescheduling another Tiger Scheme Web Application Senior Security Tester Assessment.

2.1.8 If the candidate is unhappy with the assessment and/or the result, then they have the right to appeal against the decision of the Examination Body.

2.1.9 The current scope of the Tiger Scheme Web Application Senior Security Tester Assessment is restricted to popular UNIX/Linux like and Windows (2000,2003,2008,2012 and 2016) operating systems, web applications and common network components, including routers,

switches and firewalls. The network protocols assessed are restricted to the IP level.

2.2 The Assessment Schedule – Prior Written Report

2.2.1 The role of function of the assessment of the written report is to ascertain the candidates' ability to communicate with the customer in managerial and technical terms. In particular:

- Management presentation and results;
- Technical presentation of results.

2.2.2 This report must be written by the candidate and represent a Web Application Security test that has been undertaken by the candidate and a report submitted to a customer. This may be a recent report that has been anonymized,

2.3 The Assessment Schedule – The Examination

2.2.1 The multiple-choice examination is a 1-hour examination. The role of this examination is to assess the candidates' broad knowledge of all areas covered in the OWASP Testing Guide v5.0 and Senior Level technical standard. This is a closed book assessment and will consist of the following:

- A multiple-choice section with approx 120 questions. The candidate is required to answer all questions.

2.2.2 The written examination is a 3-hour written examination. The role of this examination is to assess the candidates broad knowledge of all areas covered in the OWASP Testing Guide v5.0 and Senior Level technical standard. This is a closed book assessment and will consist of the following:

- A long answer section consisting of 8 questions. The candidate is required to answer 6 questions.

2.2. The role and function of the written examination is to ascertain the candidates' ability in the areas of:

- Understanding Requirements
- Defining Scope
- Legal and Ethical Issues
- Planning and Management
- Management Risk
- Testing Methodology

- Testing Platform
- Technology and Vulnerabilities
- Assessing site layout
- Assessing application design

2.4 The Assessment Schedule – The Practical Assessment

2.4.1 The candidate is required to bring any computer equipment and software necessary to conduct a Web Application Security test against a 10/100Base-T Ethernet network. The candidate will not be provided with a connection to the Internet and are not allowed to make use of an Internet connection.

2.4.2 The Tiger Test Rigs contain the following:

i. Microsoft Windows 2000, 2008, 2012 or 2016.

ii. Ubuntu 14.10 or Ubuntu 16.04

iii. Cisco 2801 and Cisco PIX/ASA 515E.

2.4.3 The operating systems and tools used must be capable of conducting host discovery and demonstrating or identifying vulnerabilities against criteria detailed later in this document. Candidates may use any software tools they deem appropriate. However, they must ensure any tools used are appropriately licensed and function correctly. Ideally, a complete tool-set will contain complementary and alternative vulnerability discovery and/or system administration tools. Failure to demonstrate Web Application Security test capabilities due to hardware or software misconfiguration may result in failure.

2.4.4 When listing vulnerabilities candidates must use CVE numbers. Where CVE numbers are not available they are permitted to use BID numbers.

2.4.5 The practical assessment will last 6 hours.

2.4.6 The Candidates will be required to identify vulnerabilities in the Tiger Scheme Web Application Senior Security Tester Assessment. Exploitation of vulnerabilities is not a requirement *per se*, but candidates should use all techniques at their disposal to obtain the highest level of assurance regarding the presence or absence of vulnerabilities in the target systems. Candidates are expected to provide a value added service above that of an automated vulnerability scanner and should be able to eliminate false positives and negatives where possible. Techniques to accomplish this may include, but are not limited to, vulnerability exploitation.

2.4.7 The Tiger Scheme Senior Security Tester Assessment focuses on common vulnerabilities that are regularly identified when performing

Web Application Security tests of Web Applications. The candidate will be required to:

- Explain any vulnerabilities associated with the technology;
- Explain the limitations and default behavior of the vulnerabilities;
- Demonstrate the remote detection of vulnerabilities (the candidate will be required to eliminate possible false positives from scanning tools by, for example, manually demonstrating the exploitation of vulnerability) and describe how the detection mechanism works.
- Explain protection measures that could be implemented to secure the computer system

2.4.8 Candidates will be required to demonstrate a understanding of:

- Technology and Vulnerabilities
- Assessing network design
- Assessing application design
- Security testing – enumeration
- Security testing – identification and proof of issues
- Security testing – classifying risk
- Remediation

2.4.9 To pass the assessment the candidate is required to pass all of the MUST components of the technical standard. These are as follows:

Skill Set	Must Components/ID's
Understanding Requirements	A2
Defining Scope	B1, B2
Legal Issues	C1
Planning and Management	D1, D2, D3, D4, D5, D6
Managing Risk	E1, E2, E3, E4
Testing Methodology	F1
Testing Platform	G1
Technology and Vulnerability	H1, H2
Assessing Site Map	I1
Assessing Application Design	J1
Security Testing – Enumeration	K2, K3, K4, K5, K6
Security Testing – Identification and Proof of Issues	L1, L3, L4, L5, L6, L7, L9, L10
Security Testing – Classifying Risk	M1
Remediation	N1, N3
Management Presentation of Results	O1
Technical Presentation of Results	P1

2.4.10 The candidate will be required to perform/document a set of functions and activities on the Tiger Test Rigs. The activities will be defined in the practical assessment paper.

2.4.11 Appendix 17 demonstrates the mapping of the OWASP Testing Guide v3.0 controls against the components mentioned in section 2.4.8 and the relevant matrices found in the appendices.

2.5 The Assessment Schedule – The Viva

2.5.1 The role and function of the viva is to allow the examiners to explore the candidate's ability in certain key area. The viva will also give the candidate the ability to present their results.

2.5.2 The viva will be used to explore the candidate's strengths and weaknesses and will draw upon the results from the following assessment stages:

- S1 - Submission of prior written report,
- S2 - Written examination,
- S3 - Practical assessment.

3 Recommended Reading

[COM06] Douglas E. Commer, **Internetworking with TCP/IP: Principles, Protocols and Architectures**, 5th Edition, Prentice Hall, 2006.

[MCN08] Chris McNab, **Network Security Assessment**, 2nd Edition, O'Reilly, 2008.

[MCC03] Stuart McClure, Joel Scambray and George Kurtz, **Hacking Exposed: Network Security Secrets and Solutions**, 7th Edition, McGraw HIll, 2012.

[SCA10] Joel Scambray, **Hacking Exposed: Web Application**, 3RD Edition, McGraw HIll, 2010.

[STU12] Dafydd Stuttard and Marcus Pinto, **The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws**, Wiley Publishing, 2nd Edition, 2011.

Appendix 1 – Understanding Requirements

Skills ID	Details	State of Examination
A1	○ Knowledge of the type of tests that may be included in a Web Application test. ○ Understanding of the differences between white-box, block-box and grey-box testing. ○ Knowledge of the types of requirements associated with the various types of security tests related to Web Applications.	S2, S3, S5
A2	○ Knowledge of the requirements associated with the back-end of a web application. ○ Knowledge of the requirements associated with security testing of a web application.	S2, S3, S5
A3	○ Knowledge of the constraints that may be placed on the testing of various types of systems, such as: ○ White/Black listing for Safety Systems, Mission Critical Systems and Production Systems ○ Exclusion of Brute Forcing and DOS attacks ○ Exclusion of exploitation via vulnerabilities.	S2, S3, S5

Appendix 2 – Defining Scope

Skills ID	Details	State of Examination
B1	○ Ability to produce a project plan based on the client's/customer's requirements. In particular, accurate: ○ Timescale management ○ Resource planning ○ Ability to produce a requirements document that identifies the key stakeholders of the test along with their requirements/expectations. ○ Knowledge of, and ability to use a, project planning tools such as Microsoft Project. ○ Knowledge of risk management, and how to manage and mitigate risk in a Web Application test. ○ Ability to derive a test plan from a requirements specification with an accurate and realistic timescale plan.	S2, S3, S5
B2	○ Ability to communicate in a clear and precise manner with the various stakeholders. ○ An understanding of cost-benefit analysis and the various ways that trade-offs can be made. ○ Understanding of the structure of a Web Application test, including relevant process and procedures. ○ Understanding of the various reporting requirements. ○ The ability to manage stake holder's expectations and fulfil requirements.	S2, S3, S5

Appendix 3 – Legal Issues

Skills ID	Details	State of Examination
C1	○ Knowledge of the following pieces of legislation: ○ Computer Misuse Act 1990 and its amendments. ○ Data Protection Act 1998 ○ Human Rights Act 1998 ○ Police and Justice Act 2006 ○ Police and Criminal Evidence Act 1984 ○ Regulation of Investigatory Powers Act 2000 ○ Knowledge of the impact the UK legislation has on the Web Application Security test process. ○ Awareness of the ethical issues and codes of conduct associated with a Web Application Security testing. ○ Awareness of sector specific legislation and regulatory requirements. ○ An understanding of the role/function of a NDA in a security test	S2, S3, S5

Appendix 4 – Planning and Management

Skills ID	Details	State of Examination
D1	○ Understanding and awareness of the type of system (logical and physical) access associated with the various types of testing.	S2, S3, S5
D2	○ Awareness and understanding of the need for testing authority documents to be present during a test. ○ Awareness of the role that third parties can play in authorising security testing documents. ○ Understanding of the scope and limitation of testing authority documents. ○ Understand the needs for an authorised person to sign/approve testing authority documents.	S2, S3, S5
D3	○ Awareness of the need for physical security while on a customer's site. ○ Understanding and awareness of a client's policy and procedures associated with being escorted while on-site.	S2, S3, S5
D4	○ Ability to identify and interface with key technical customer staff for specific elements of the assessment.	S2, S3, S5
D5	○ An understanding of, and ability to perform, daily wash-up sessions associated with a test to the customer. ○ An understandings of, and ability to perform, project closure briefing sessions to the customer. ○ An understandings of, and ability to perform, immediate notification based on high risk issues.	S2, S3, S5
D6	○ Understanding and awareness of the security requirements associated with the delivery of the final report. ○ Understanding and awareness of report methods/standards and best practice.	S2, S3, S5

Appendix 5 – Managing Risk

Skills ID	Details	State of Examination
E1	○ Knowledge of the risks that a Web Application Security test can present to a customer's system, for example Denial of Service.	S2, S3, S5
E2	○ Knowledge of the risks that a Web Application Security test can present to customer systems and applications.	S2, S3, S5
E3	○ Knowledge of the risks that a Web Application Security test can present to a customer, such as lockout of user and application accounts	S2, S3, S5
E4	○ Knowledge of the risks that a Web Applications Security test can present to a customer ability to audit and monitor a system/infrastructure.	S2, S3, S5
E5	○ A detailed understanding of the role/function of customer emergency contacts can play in risk management and risk mitigation.	S2, S3, S5
E6	○ An understanding of the strategies that may be used in a Web Application Security test to mitigate various types of risks associated with data/system corruption. In particular: ○ Business continuity planning ○ Disaster recover ○ Back/up and restore procedures	S2, S3, S5
E7	○ A knowledge of the types of risks associated with excessive use of computer network and web application defence technology while a Web Application security test is on going.	S2, S3, S5
E8	○ The ability to suggest risk management strategies aimed at the reduction of risk to the critical applications/systems. ○ The ability to suggest alternative testing strategies for critical applications/systems.	S2, S3, S5

Appendix 6 – Testing Methodologies

Skills ID	Details	State of Examination
F1	○ An understanding of the role/function of the testing tools use by the candidate in assault course, and the ability to demonstrate this understanding.	S4

Appendix 7 – Testing Platform

Skills ID	Details	State of Examination
G1	○ The candidate must be in possession of a laptop system that is suitable for performing a Web Application security test. ○ The system should be configured with any choice of software and operating system(s) however the following conditions must be met: ○ All commercial software must be suitably licensed. ○ Anti-virus software should be installed and configured in such a way so as to not disrupt the security testing tools. ○ The candidate should be in possession networking capable to connect to an IP Cat5 network. [RJ45 connector]	S4

Appendix 8 – Technology and Vulnerabilities

Skills ID	Details	State of Examination
H1	○ Awareness of various IP protocols IPv4, IPv6, TCP, UDP, ICMP and other IP protocols. ○ In terms of network architectures the candidate should understand the following: ○ CAT 5 and Fibre ○ 10/100/1000baseT ○ Wireless (802.11) ○ Security implications of shared media and switched media ○ Data sniffing and session hi-jacking ○ VLAN ○ In terms of Authentication the candidate should understand the following: ○ Type of bio-metrics and how they can be applied ○ One time pads ○ Usernames and passwords ○ Digital certificates ○ In terms of Cryptography the candidate should understand the following: ○ The difference between encoding and encrypting. ○ The difference between symmetric and asymmetric encryption. ○ Encryption algorithms, such as DES, 3DES, AES, RSA, RC4. ○ Hashing algorithms, such as SHA1, MD4 and MD5. ○ Message integrity codes: HMAC ○ PKI, IKE Certificate Authorities, and trusted third parties. ○ In terms of applying cryptography the candidate should understand the following: ○ Secure Socket Layer/ TLS ○ PGP ○ Password hashing ○ In terms of unified threat management devices the candidate should	S2, S3, S5

	understand the following: ○ How a Web Application firewall functions ○ How a proxy/application-gateway firewall functions ○ How firewalls and routers can be used to implement access control lists ○ IDS and IPS devices ○ How to review a Web Application firewall rule base ○ Hardening Web applications, in particular: ○ Techniques to limit the exposure of information ○ Techniques to limit the exploitation of weaknesses in Web Applications. ○ Code review (Web Application) ○ ACL review of file permissions ○ ACL review of web application and database roles ○ Password security policy (on both web application and database backend) ○ Hardening Web application database back-end, in particular: ○ How to review weaknesses particular to the database implementation ○ How to review the exposure of the back-end database. ○ System auditing functions such as: ○ Identifying audit policies ○ Identifying and assessing patch levels ○ Identifying files with incorrect permissions set. ○ Listing network sockets mapped to processes	
H2	○ To demonstrate an awareness of: ○ Up-to-date vulnerability sources and information.	S2, S3, S4, S5
H3	○ The ability to locate vulnerability sources/information based on a CVE number.	S2, S3, S4, S5

Appendix 9 – Assessing Site Map

Skills ID	Details	State of Examination
I1	○ To demonstrate an understanding of how to map out a Web Application's design principle, in particular: ○ Site mapping via passive testing ○ Web application technology identification such as: ▪ Ruby (Ruby on Rails), Perl, PHP, ASP, ASP.NET(C#, VB.NET), JSP (Java), Python (Django), ○ Identification of potential weaknesses and security issues. ○ Determining web server types and network application versions from application banners. ○ Determine whether a database back-end is visible.	S2, S3, S4, S5
I2	○ Analysis of site map to identify: ○ Potential information leakage with suggestions for improvements ○ Intrusion Detection Systems and Intrusion Prevention Systems ○ Web Application Firewalls should be deployed ○ Where network and application based monitoring should be deployed ○ Network areas where additional access controls should be deployed ○ Strategies for network, application and database segregation and access control ○ Strategies for protecting against a variety of given 'internal threats.'	S2, S3, S5

Appendix 10 – Assessing Application Design

Skills ID	Details	State of Examination
J1	○ Ability to assess application architecture on paper and identify potential weaknesses and security issues. ○ Ability to suggest generic recommendations for addressing any issues	S2, S3, S5
J2	○ The candidate will be provided an architecture design chart for an application and should identify or discuss: ○ Effectiveness of application authentication ○ Effectiveness of application auditing ○ Effectiveness of segregation of user systems from application database(s) ○ Application communication security ○ Exposure of application infrastructure to 'external' attack ○ Types of vulnerability that may be present in various components of the application architecture. ○ Areas of application software that may be suitable for limited application security testing ○ OS and application patch-level requirements	S2, S3, S5

Appendix 11 – Security Testing - Enumeration

Skills ID	Details	State of Examination
K1	○ Analysis of misleading and incorrect information with a view to the identification of such instances of inaccurate or incorrect information.	S2, S3, S4, S5

K2	○ Analysis of WHOIS registration information for the identification of host and IP address details and DNS servers from WHOIS records;
	○ Analysis of data from DNS records showing Web servers
	○ Analysis of data from Spiders, robots and crawlers;
	○ Analysis of publicly available data from search engine discovery, including:
	  ○ Web Application structure
	  ○ Error pages
	  ○ Other sources that include OSINT (Open Source Intelligence)
	○ Understand of how the analysis of vendor manuals and documentation can be used to aid in a Web Application Security test.
	○ Analysis of the target's own web site
	○ Analysis of configuration information associated with target mail and name services;
	○ Analysing news group and e-mail headers to identify system information.
		S2, S3, S4, S5

K3	○ Analysis of passive web application testing; ○ Analysis of active web application testing;	S2, S3, S4, S5

K4	○ Analysis of active techniques for discovery of nodes on a network, such as:
	  ○ SYN and TCP-Connect scanning;
	  ○ FIN/NULL and XMAS scanning;
	  ○ UDP port scanning;
	  ○ TCP ping scanning;
	  ○ ICMP scanning.
	○ Analysis of passive techniques for discovery of nodes and web applications on a network, such as:
	  ○ Packet monitoring;
		S2, S3, S4, S5

	○ Passive OS fingerprinting.	
K5	○ An understanding of the methods associated with service identification, enumeration and validation, in particular: ○ Identification of key servers within the target domain ○ Identification of key web applications ○ Identification of where web servers exist, such as ▪ shared hosting ▪ dedicated servers ○ A practical knowledge of the tools and methods associated with ○ Service identification and validation; ○ Determine service versions and vendors; ○ Services such as: SSH, SMTP, IMAP, POP, SNMP, LDAP, DNS, SOAP, WSDL, UDDI, HTTP and HTTPS ○ Database service identification and enumeration (MSQL, MySQL, Oracle and PostgreSQL) ○ Identifying Secure HTTP communications, such as: ▪ SSL ▪ TLS ○ Identification, validation and exploitation of protocols commonly used for remote systems/device management, such as: ○ LDAP, SNMP ○ SSH and Telnet ○ WEB based protocols ○ TFTP ○ NTP ○ OS fingerprinting and banner grabbing ○ Web application fingerprinting ○ An understanding of the usage of error codes in the enumeration process	S2, S3, S4, S5
K6	○ An understanding of the methods associated with unknown service identification, enumeration and validation. ○ An understanding of advanced analysis techniques for unknown	S2, S3, S4, S5

	services and protocols.	
K7	○ Demonstrate the identification of other application entry points. ○ Demonstrate the identification of file extension handling ○ Demonstrate and explain the enumeration of old, backup and/or renamed files as part of information leakage	S2, S3, S4, S5
K8	○ Demonstrate and explain the enumeration of data from a variety of common service and web application weaknesses on various platforms, including: ○ User account information, such as: ▪ SMTP, SSH, Telnet, SNMP and RID cycling ▪ Log on pages ▪ Password reset pages ▪ Account management pages ○ Service or system configuration and management, such as: ▪ SNMP ▪ Database back-end system ▪ Database management system ▪ Account management pages ○ Infrastructure and/or application Admin interface exposure	S2, S3, S4, S5
K9	○ Demonstrate and explain: ○ Utilisation of man-in-middle proxy to capture site structure; ○ Hyperlink analysis ○ Brute force resource identification; ○ Analysis and inspection of available page source code for common coding mistakes in languages such as JSP, ASP, PHP, Perl, JavaScript, XML, AJAX and HTML; ○ Identification of the session control mechanism used within the application; ○ Identification of relevant	S2, S3, S4, S5

	scripts, applications and associated parameters.	
K10	○ Demonstrate understanding of the potential limitations of using automated software on some web applications. E.g.: ○ Sites that feature heavy use of dynamic client side scripting ○ Sites that use client side executable components; and ○ Sites that generate incorrect server responses.	S2, S3, S4, S5
K11	○ Demonstrate understanding of the dangers of allowing dangerous HTTP commands and Cross Site Tracing is not permitted. ○ Demonstrate understanding of HTTP splitting and/or smuggling	S2, S3, S4, S5

Appendix 12 – Security Testing – Identification and Proof of Issues

Skills ID	Details	State of Examination
L1	○ Demonstrate the ability to identify both false positives and false negatives and operate within the constraints of the scope of testing whilst keeping risk of disruption to an acceptable level. ○ An awareness of any risks involved; for example conducting an aggressive spider scan, to create a site map, that could bring down the system temporarily.	S2, S3, S4, S5
L2	○ Techniques for proving issues, which may fall outside of the constraints and scope in place during the assault course.	S2, S3, S4, S5
L3	• Demonstrate the ability to identify, explain and prove the existence of the following types of network infrastructure vulnerabilities and exposures: ○ Physical network weaknesses ○ Network protocol weaknesses and insecurities at all network layers, such as: ▪ ARP ▪ IP, TCP, UDP and ICMP ▪ Telnet and SSH ▪ Web based protocols ▪ SNMP ▪ FTP and TFTP ▪ DNS ▪ NTP ▪ IPSEC ▪ VOIP and SIP ○ Web application and server issues: ▪ Known software vulnerabilities ▪ Inadequate access control of server and services ▪ Trust relationship insecurities ▪ Management mechanism insecurities ▪ Bypassing the Authentication Schema ▪ Vulnerable remember password and resetting	S2, S3, S4, S5

	functions ▪ Logout and browsing cache management ▪ CAPTCHA ▪ Identification of multiple factors authentication ▪ Identification of race conditions ▪ Cookie Attributes ▪ Session fixation ▪ CSRF ▪ Path Traversal ▪ XSS (Cross Site Scripting) ▪ Incubated Vulnerability Testing ▪ Specified Object Allocation ▪ Input as a loop counter ▪ User provided data to disk ▪ Failure to release resources ▪ Too much data in session ▪ WSDL, SOAP, UDDI, AJAX ▪ Identification and analysis of HTTP GET parameters and REST ▪ Identification and analysis of replay vulnerabilities on web service o Business Logic o Network access control and segregation vulnerabilities	
L4	o Discuss current and existing vulnerabilities in a variety of common devices, such as: o Windows (NT, 2000, XP, 2003, 2008) o Unix. Solaris and Linux o Web servers o Web Applications (bespoke and 3rd party)	
L5	o Ability to exploit and understanding of risks/issues associated with the following in a Windows environment: o Identification of domains and workgroups; o Identification of servers within a domain; o Identification and analysis of browser list and SMB shares.	S2, S3, S4, S5

	○ Identification of configuration information via SNMP ○ Identification of user accounts using SNMP, LDAP and NetBIOS ○ SID enumeration and RID cycling ○ Identification and analysis of IIS ○ Identification and analysis of Exchange Servers ○ Identification and analysis of MSQL, MySQL, PostgreSQL and Oracle. ○ Ability to exploit and understanding of risks/issues associated with the following in a Unix environment: ○ FTP access control and anonymous FTP ○ Sendmail and SMTP (EXPN and VRFY commands) ○ Identification of configuration information via SNMP ○ Identification of user accounts using LDAP and SNMP ○ SSH and Telnet ○ Identification and analysis of Apache ○ Identification and analysis of MySQL, PostgreSQL and Oracle. ○ Brute forcing of accounts and password polices, such as: ○ Password cracking of Unix, Windows password file ○ Password cracking of Web Application-based and database back-end based passwords ○ Brute forcing of logins onto Windows, Unix, Databases and Web Applications ○ Offline password analysis via rainbow tables and hash brute forcing ○ Testing for the ability to conduct brute forcing ○ Microsoft patch management strategies such as: ○ SMS, SUS, WSUS and MBSA ○ The ability to identify, explain and prove the existence of the following types of Operating System vulnerabilities and exposures:	

	○ Known software vulnerabilities ○ Inadequate access control of network services ○ Privilege escalation ○ Management mechanism insecurities ○ Remote and Local user access control insecurities	
L6	○ Demonstrate the ability to perform a security build review of common Operating Systems.	S2, S3, S4, S5
L7	○ The ability to discuss current and existing vulnerabilities in a variety of common Operating Systems and Web Application technologies, ○ The ability to discuss common misconfigurations in a variety of common Operating Systems and Web Application technologies, ○ The ability to discuss current and existing vulnerabilities in a variety of common 3rd Party Software, ○ The ability to discuss the likelihood of exploitation and the likely impact of recently announced vulnerabilities.	S2, S3, S5
L8	○ Demonstrate knowledge of a number of more advanced operating system and web application vulnerabilities and identification methods including: ○ Remote and local buffer overflows ○ Use of tools and techniques to identify new OS software vulnerabilities ○ Use of tools and techniques to identify new Web Application vulnerabilities ○ Use of techniques to develop exploit code for existing and new vulnerabilities.	S2, S3, S4, S5
L9	○ Demonstrate the ability to identify, explain and prove the existence of the following types of web application vulnerabilities and exposures: ○ Information gathered from Web Mark-Up languages such as: ▪ Hidden Forms ▪ Database connection strings ▪ Credentials ▪ Developer comments ○ Input data validation vulnerabilities;	S2, S3, S4, S5

	○ Session control mechanism vulnerabilities; ○ Authentication mechanism vulnerabilities; ○ Functional logic and function access control; ○ Application server hardening flaws	
L10	○ Ability to exploit and understanding of risks/issues associated with web applications, such as: ○ Cross site scripting (reflected, stored, DOM based, object based (Adobe Flash, etc)) ○ Use of injection attacks such as: SQL, LDAP, ORM, XML, SSI, XPath, Code, IMAP and SMTP ○ Exploitation of SQL to enumerate a database and its structure ○ Exploitation of SQL to execute commands on the target server. ○ Identification of valid user accounts and account locking ○ Identification of configuration information via errors ○ Identification and analysis of SQL-based (MSQL, MySQL, PostgreSQL and Oracle) and NoSQL-based databases. ○ Identification of bypassing authentication schema ○ Vulnerable remember password and resetting functions ○ Logout and browsing cache management ○ Identification and analysis of multiple factors authentication ○ Identification and analysis of race conditions ○ Identification and analysis of cookie attributes ○ Availability and analysis of session fixation ○ Exposed session variables ○ CSRF ○ Demonstration of Privilege Escalation ○ Identification and analysis of OS Commanding ○ Identification and analysis of WSDL	S2, S3, S4, S5

	○ Identification and analysis of XML structure and content ○ Identification and analysis of HTTP GET parameters and REST ○ Identification and analysis of malicious SOAP attachments ○ Identification and analysis of replay vulnerabilities on web service ○ Identification and analysis of AJAX	

Appendix 13 – Security Testing – Classifying Risk

Skills ID	Details	State of Examination
M1	○ The candidate MUST be able to describe and understand the following aspects of a given security vulnerability/issue and how they relate to classifying an issue with regard to the risk that is posed: ○ The nature of the vulnerability ○ How the vulnerability might be exploited ○ The type of attacker capable of exploiting the vulnerability ○ Any pre-requisites that an attacker would need to exploit the vulnerability ○ The likelihood of a successful exploitation ○ The presence of mitigating factors that prevent the exploitation or reduce the likelihood of a successful exploitation ○ The technical impact to the target with regard to confidentiality, integrity and availability if the vulnerability is exploited ○ How to reference further information with respect to vulnerabilities (e.g. CVE/BID/CVSS)	S2, S3, S4, S5
M2	○ Ability to classify a number of given security issues with regard to risk posed and communicate this by attaching a quantity to the risk (e.g. High, Medium, Low or 5,4,3,2,1 etc.)	S2, S3, S4, S5

Appendix 14 – Remediation

Skills ID	Details	State of Examination
N1	○ Demonstrate a sound knowledge and understanding of suitable remediation strategies and steps suitable for addressing a variety of identified security risks and vulnerabilities. This will include design and architecture issues, technical configuration issues in a range of operating systems and application software security issues, although extensive knowledge of specific platforms and applications is not required.	S3, S4. S5
N2	○ Detailed recommendation sometimes require extensive product knowledge and if a candidate is not in possession of this knowledge then they should, in the least, suggest an overview recommendation.	S3, S4. S5
N3	○ The ability to provide a summary of how each issue identified or discussed during the assault course may ideally be solved.	S3, S4. S5

Appendix 15 – Management Presentation of Results

Skills ID	Details	State of Examination
O1	○ The candidate will be required to provide both a verbal and written summary of a security test to customers who are non-technical. Whilst it is appreciated that many security issues and vulnerabilities are by definition technical, it is always possible to relay concepts such as probability of exploitation and impact to information systems and associated data.	S3, S4. S5
O2	○ For each given issue, or group of issues if appropriate, the candidate will convey the following information: ○ The cause of the issue (e.g. misconfiguration, human error, software vulnerability) ○ Which type of attacker would most likely exploit the issue (e.g. authorised internal user, external Internet connected anonymous user, attacker with physical access etc.) ○ The difficulty and likelihood of a successful exploit ○ The potential impact to the customer's information systems and data preferably in terms of confidentiality, integrity and availability	S3, S4, S5

Appendix 16 – Technical Presentation of Results

Skills ID	Details	State of Examination
P1	○ The ability to provide detailed information on identified security issues to technical or technical security customers. Such information is likely to include a list of affected components, details of the issue, technical impact and recommended action(s) for remediation. In particular: ○ Rating of issues using numerical and /or colour scoring cards ○ Scoring of vulnerabilities using CVSS	S3, S4
P2	○ The ability to convey the following information: ○ A detailed description of the problem ○ A list of affected components (if relevant) ○ A description of the risk posed referencing the type of attack that can occur and what the impact of the attack would be with regard to the confidentiality, integrity and availability of the target system and other dependent systems. ○ A qualitative assessment of the risk posed (on a scale of High-Medium-Low, Red-Yellow-Green or 5-1 etc.) ○ Possible sources of further information. A recommendation or series of recommendations, which may extend beyond the technical arena, to mitigate the identified risk.	S3, S4

Appendix 17 – OWASP Testing Guide v3.0 Control to test mapped to skills

Category	Ref. Number	Test Name	Skills ID
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers -	K2
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	K2
	OWASP-IG-003	Identify application entry points	K7
	OWASP-IG-004	Testing for Web Application Fingerprint	K4, K5, K8
	OWASP-IG-005	Application Discovery	K5, K6
	OWASP-IG-006	Analysis of Error Codes	K2, K5
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	H1
	OWASP-CM-002	DB Listener Testing	H1, K4
	OWASP-CM-003	Infrastructure Configuration Management Testing	I1, I2
	OWASP-CM-004	Application Configuration Management Testing	I1, L7
	OWASP-CM-005	Testing for File Extensions Handling	K5, K7
	OWASP-CM-006	Old, backup and unreferenced files	K7
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	K8
	OWASP-CM-008	Testing for HTTP Methods and XST	K11, K5
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	H1
	OWASP-AT-002	Testing for user enumeration	K8, L5
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	L5
	OWASP-AT-004	Brute Force Testing	H1, K9, L5, L9
	OWASP-AT-005	Testing for bypassing authentication schema	L3, L10, L7, L9
	OWASP-AT-006	Testing for vulnerable remember password and pwd reset	L3, L10, L9
	OWASP-AT-007	Testing for Logout and Browser Cache Management	L3, L10, L9
	OWASP-AT-008	Testing for CAPTCHA	L3
	OWASP-AT-009	Testing Multiple Factors Authentication	H1, L3, L9, L10
	OWASP-AT-010	Testing for Race Conditions	L3, L10
Session Management	OWASP-SM-001	Testing for Session Management Schema	H1, K9, L9
	OWASP-SM-002	Testing for Cookies attributes	L3, L10
	OWASP-SM-003	Testing for Session Fixation	L3, L10
	OWASP-SM-004	Testing for Exposed Session Variables	L9, K9, L10

	OWASP-SM-005	Testing for CSRF	L3, L10
Authorization Testing	OWASP-AZ-001	Testing for Path Traversal	L3, L10
	OWASP-AZ-002	Testing for bypassing authorization schema	L3, L10, L7, L9
	OWASP-AZ-003	Testing for Privilege Escalation	L5, L10
Business logic testing	OWASP-BL-001	Testing for business logic	L3
Data Validation Testing	OWASP-DV-001	Testing for Reflected Cross Site Scripting	L3, L10
	OWASP-DV-002	Testing for Stored Cross Site Scripting	L3, L10
	OWASP-DV-003	Testing for DOM based Cross Site Scripting	L3, L10
	OWASP-DV-004	Testing for Cross Site Flashing	L3, L10
	OWASP-DV-005	SQL Injection	L10
	OWASP-DV-006	LDAP Injection	L10
	OWASP-DV-007	ORM Injection	L10
	OWASP-DV-008	XML Injection	L10
	OWASP-DV-009	SSI Injection	L10
	OWASP-DV-010	XPath Injection	L10
	OWASP-DV-011	IMAP/SMTP Injection	L10
	OWASP-DV-012	Code Injection	L10
	OWASP-DV-013	OS Commanding	L10
	OWASP-DV-014	Buffer overflow	L8
	OWASP-DV-015	Incubated vulnerability Testing	L3
	OWASP-DV-016	Testing for HTTP Splitting/Smuggling	K11, L10
Denial of Service Testing	OWASP-DS-001	Testing for SQL Wildcard Attacks	L10
	OWASP-DS-002	Locking Customer Accounts	L9, L10
	OWASP-DS-003	Testing for DoS Buffer Overflows	L8
	OWASP-DS-004	User Specified Object Allocation	L3, K9
	OWASP-DS-005	User Input as a Loop Counter	L3, K9
	OWASP-DS-006	Writing User Provided Data to Disk	L3, K9
	OWASP-DS-007	Failure to Release Resources	L3, K9
	OWASP-DS-008	Storing too Much Data in Session	L3, K9
Web Services Testing	OWASP-WS-001	WS Information Gathering	K5
	OWASP-WS-002	Testing WSDL	L10
	OWASP-WS-003	XML Structural Testing	L10
	OWASP-WS-004	XML content-level Testing	L10
	OWASP-WS-005	HTTP GET parameters/REST Testing	K11, K5, L3, L10
	OWASP-WS-006	Naughty SOAP attachments	L10
	OWASP-WS-007	Replay Testing	L3, L10
AJAX Testing	OWASP-AJ-001	AJAX Vulnerabilities	L3, K9
	OWASP-AJ-002	AJAX Testing	L10

This page is intentionally left blan