TIGERSCHEME™

Providing excellence in penetration testing

# WEB APP

2 day assessment

Traditional firewalls provide a starting point for defence in depth for IT resources. However, that starting point often provides no defence against web application attacks, since it is designed and configured to allow web-based traffic. While it can offer some protection against e.g. denial of service attacks, it cannot effectively prevent attacks such as SQL injection and crosssite scripting. A 'defence in depth' approach for web applications must encompass critical aspects of design, operation and monitoring. Independent assurance is a key element, but one which requires specific and proven skills.

As part of their remit to improve levels of professionalization in this area, Tiger Scheme provides a Senior level certification relating to web application testing.

Please note that this assessment is a challenging exercise, demanding industry-leading abilities. Candidates should have a number of years of hands-on experience, with significant practical experience in this field. The Web Applications Security Tester assault course is more than simple assessment of technical skill and is designed to evaluate the candidate as a whole and their capabilities across the web security-testing spectrum.

## Areas of Assessment

The assessment covers various broad areas: legal, management, ethics, compliance; technical expertise; and effective delivery of results. The assessment itself consists of a one-hour multiple choice examination, a three hour written paper, a six hour practical assessment and an interview with an examiner. The practical element is based on a rig which as far as possible mimics the environment that an investigator would face in a real world assignment.

## Key Requirements

Candidates will also be expected to demonstrate an appropriate level of knowledge and expertise in the following key technical areas:

- An up-to-date knowledge of existing and emerging threats and vulnerabilities.
- The ability to gather Information from web requests relating to structure, content and web application/services
- The ability to identify and exploit weaknesses relating to the configuration of Web Content and Structure, and Web Applications and Services
- Demonstrate the ability to identify and exploit authentication methods such as account credentials, session tokens, compromise passwords, keys, session cookies, or other tokens.
- Demonstrate the ability to identify and exploit session management and the credentials and methods associated with the management of a users session.
- Demonstrate the ability to identify and exploit authorisation methods used by various web applications to confirm that a given user has the necessary rights and permissions.
- Demonstrate the ability to identify and exploit weakness in the various business logic methods used by innumerable web applications to check the validity of a business transaction.
- Demonstrate the ability to identify and exploit various data in which data is validated by web applications, such as cross-site scripting and inject flaws.
- Demonstrate the ability to identify and exploit various weaknesses that can result in a denial of service

**Course details continued on reverse >**

TIGERSCHEME

For more information visit **www.TigerScheme.org**

**Providing excellence in penetration testing**

TigerScheme™

Providing excellence in penetration testing

# WEB APP

## Course details continued:

- Demonstrate the ability to identify and exploit key weaknesses in association with the implementation and delivery of web services.
- Demonstrate the ability to identify and exploit insecure security weaknesses associated with various web server technologies.
- Demonstrate a reasonable level of proficiency in the suitable classification and analysis of technical risk posed by various technical security vulnerabilities and exposures. This will include understanding of impact and the identification of any mitigating factors or controls.
- Demonstrate knowledge of the strategies and technology that can be used to counter a security threat

These must be supported by a working knowledge, demonstrated through the application of best practice, in terms of an ability to produce a written and verbal summary of security testing results to a non-technical audience, and the ability to document and explain identified security issues, identifying the issue, impact, risk and suitable recommendations.

Tiger Scheme is a not-for profit organisation working in co-operation with The University of South Wales (formerly the University of Glamorgan) to provide an independent, University recognised assessment of the technical, legal and ethical capabilities of penetration testers within the UK. Buyers of penetration testing are vocal of the shortage of certified skill in the UK, and the negative impact this has on project timescales and costs. Tiger Scheme bridges this gap between buyers and suppliers of assessment services. Whilst many UK based certification concentrate purely on commercial service providers, Tiger Scheme offers certification to both professional penetration testers and IT professionals working within internal IT teams. This allows organisations to have leading edge expertise within their own teams, offering greater flexibility and cost effectiveness.