SYLLABUS

TEAM LEADER WEB APPLICATION

CORE LEARNING OBJECTIVES AND ASSESSMENT METHODOLOGY

CONTENTS

1 Introduction

1.1 Course

1.2 Exam

1.3 Aims of the course

1.4 Learning Objectives

2 Course Outline

2.1 Section 1 – Web Application Penetration Testing

2.2 Section 2 –Web application misconfigurations and web

2.3 Section 3 – Web Application Enumeration

2.4 Section 4 – Common Web Application vulnerabilities (review of core knowledge)

2.5 Section 5 – Privilege Escalation techniques

2.6 Section 6 – Site Component Topology

3 Cyber Scheme Assessment structure – CSTL Web App Certification

3.1 The assessment

3.2 Phase 2 - Practical Penetration Test (4.0 hours)

3.3 Phase 3 – Interview (30 Minutes)

3.4 Assessment Outcome

3.5 Assessment requirements

Our Purpose

1 INTRODUCTION

1.1 Course

This Key learning objectives syllabus comprises the technical skills and risk knowledge that Cyber Scheme and the National Cyber Security Centre (the UK's National Technical Authority for Cyber Security) expects candidates to possess to apply for CHECK Team Leader membership. The necessary qualification to apply for that is through certification by exam. During an approved course, a technical lab guide and technical course notes will be provided. Together both documents will support your learning.

Please note: where this material has been sourced from publicly available/open source an appropriate citation and or acknowledgement of use has been included.

The Cyber Scheme Team Leader (CSTL) web app exam tests candidates' knowledge and expertise of common web vulnerabilities and weaknesses along with an understanding of web application components.

Candidates are expected to be able to demonstrate a high level of understanding of different web applications, their services, & Operating System's to demonstrate they can identify, assess and exploit common misconfigurations or vulnerabilities by identifying the key areas of weakness within the environment.

The syllabus and course are split into a series of modules taught throughout the course. Each module will begin with theory and demonstrations where applicable, followed by a series of practical exercises to reinforce the theory. Students are provided with a lab guide that walks the student through each exercise. The instructor will provide support where required.

1.2 Exam

The CSTL Web Application exam has been designed with the NCSC to replicate as closely as possible a real-world penetration testing engagement with a client. The engagement is split into 3 sections:

1. Client Engagement

a. A short brief by the client (assessor) to outline what is required;

b. Several questions from the client exploring your knowledge in a range of fields;

c. An opportunity for you to ask questions about the scope of the work you have been tasked with;

d. All engagements are recorded for exams audit.

2. Technical analysis of the target Web Application (Assault course)

a. You are required to use your chosen tools and manual techniques to identify any vulnerabilities;

b. You are required to document your findings and provide the client with a site map of the application;

c. All of your interactions with the target application are recorded in detail;

d. You are allowed 4 hours to complete the tasks.

3. Post assessment reporting/debrief (aka Viva)

a. You will make a presentation to the client on your findings including the methodology you selected and why;

b. You will be able to highlight any additional steps you would undertake had there been more time allocated;

c. The client (assessor) will ask several questions to identify the depth of your knowledge and understanding.

1.3 Aims of the course

The CSTL Web Application course aims to build on candidates' already well-rounded understanding of the cybersecurity landscape by introducing more advanced techniques of enumeration and exploitation. The course aims to ensure that candidates understand how environments that do not yield obvious flaws may have been implemented badly and how a security consultant can leverage those weaknesses during an engagement to move/spread through a network and highlight the key weaknesses.

Additionally:

- Provide an overview of the techniques and skills required from senior penetration testers
- Learn about the limitations of automated tools used by penetration testers and alternative methodologies of addressing those;
- Provide a detailed overview of the security principals used during scoping and wash-up meetings where an understanding of engagement legality, risk management and risk mitigation will be key knowledge areas;
- Apply critical thinking to solve problems encountered during a test.

The NCSC seeks to have validation that an individual seeking to become an Infrastructure CHECK Team Leader (CTL-WEB) has demonstrated an appropriate level of knowledge and understanding of:

- Common front-end web application coding languages
- Web application technologies
- Modern Databases and languages associated with them
- Security misconfigurations
- Logging/monitoring
- Advanced web application issues

The course, therefore, aims to provide candidates with a good understanding of the following topics as a minimum:

- Common protocols, misconfigurations and Operating system weaknesses
- Web Application enumeration
- Common Web Application vulnerabilities
- Privilege Escalation techniques
- Importance of report quality and presentation of findings

1.4 Learning Objectives

- Understand Information security governance and management;
- Understand how threat assessment and information risk management impact testing methodology and approach;
- Understand how testing supports the implementation of secure systems (both architecture and development);
- Understand the role of penetration testing within the assurance portfolio (audit, compliance and testing) – THIS IS THE MAIN FOCUS OF THE COURSE
- Understand the importance of report quality to a client's operational security management and cyber resilience processes;
- Understand the role penetration testing plays in influencing intrusion detection and analysis and incident management;
- Understand the requirements for senior penetration testers to engage and influence client management and leadership, which recognises business constraints and priorities.

2 COURSE OUTLINE

2.1 Section 1 – Web Application Penetration Testing

- LO1.1 - Understanding complex Risk Requirements
- LO1.2 - Defining the 'Scope' and any special requirements
- LO1.3 – What a plan of action contains
- LO1.4 – How to approach changing scope for the assessment
- LO1.5 – Reporting
- LO1.6 – Choosing solutions – Objectivity
- LO1.7 – Ethics
- LO1.8 – Client Debriefing – Providing information to the client

2.2 Section 2 –Web application misconfigurations and web

- **LO2.4 – Understand Web application software and components**

2.3 Section 3 – Web Application Enumeration

- LO3.1 – Understanding Enumeration
- LO3.2 – Understanding the high-level approach to Site Enumeration

2.4 Section 4 – Common Web Application vulnerabilities (review of core knowledge)

- LO4.1 - Web Application Reconnaissance
- LO4.2 - Threat Modelling and Attack Vectors
- LO4.3 - Information gathering
- LO4.4 - Authentication Mechanisms
- LO4.5 - Authorisation Mechanisms
- LO4.6 - Input Validation
- LO4.7 - Information Disclosure
- LO4.8 - Use of Cross-Site Scripting Attacks
- LO4.9 - Use of Injection attacks
- LO4.10 - Session Handling
- LO4.11 - Encryption and Encoding
- LO4.12 - Source Code Review
- LO4.13 - Parameter Manipulation
- LO4.14 – Logging and Monitoring review
- LO4.15 – Web API Attacks
- LO5.16 – Modern Database Technologies Attacks
- LO5.17 – Use of Third Party Libraries and Attacks
- LO5.18 - Web Application Race Conditions

2.5 Section 5 – Privilege Escalation techniques

- LO5.1 - Understanding what privilege escalation is
- LO5.2 – Understanding the process of increasing the level of access to a web application
- LO5.3 – Understanding core methods that can enable exploitation

2.6 Section 6 – Site Component Topology

- LO6.1 – Understanding Application Site Mapping and Enumeration

Note: This is a significant topic

3 CYBER SCHEME ASSESSMENT STRUCTURE – CSTL WEB APP CERTIFICATION

3.1 The assessment

The assessment, designed with NCSC, simulates a real-world penetration test. It comprises three phases

3.1.1 Phase 1 - Scoping (15 Minutes)

All candidates will share a common scoping briefing. Following the common scoping briefing, individually candidates will have up to 10 minutes to ask questions concerning the scope of the penetration test. During your scoping session, the Assessor will play the role of the commissioning client. Your performance during the individual scoping session will form part of the assessment.

3.2 Phase 2 - Practical Penetration Test (4.0 hours)

The candidate's laptop will be connected to the assessment infrastructure, from which you will perform the practical penetration test, as defined in the scoping session. Connectivity will end after 4 hours. During the final 30 minutes, candidates will be advised to prepare for the interviews which follow, specifically in producing a site map.

(Break – 15 minutes)

There will be a 15 minute lunch break during the practical penetration test. During this time candidates will not be permitted to use their computers. This 15 minute break will not contribute towards the 4 hours of the practical assessment. You may take additional breaks for refreshments within the practical test, but no additional time will be allowed for any additional breaks that are taken.

3.3 Phase 3 – Interview (30 Minutes)

During the interview, you will be required to produce a site map on a whiteboard or flip chart. The site map must detail the application's pages and API functionality, but it does not need to include static assets, such as media or script. The interview is an assessed component of the examination; care should be taken to ensure that the site map reflects your full understanding of the assessment application.

You will also be expected to inform the commissioning client (Assessor) of the significant aspects of your practical penetration test. The Assessor may ask you to explain any aspect of the process that you followed during the practical test.

3.4 Assessment Outcome

Under normal circumstances, you will be notified of success or failure within one working week by Cyber Scheme.

3.5 Assessment requirements

In order to pass the test, you must demonstrate all of the following:

• appropriate interaction with the commissioning client,

• knowledge of the process of conducting a penetration test including legal and ethical issues,

• core capability to identify and exploit OWASP top 10 vulnerabilities, especially with regard to:

o injection vulnerabilities e.g. SQL injection,

o cross-site scripting (XSS) vulnerabilities,

o privilege escalation vulnerabilities,

o information disclosure vulnerabilities,

• core capability to produce an accurate site map.

OUR PURPOSE

Cyber Scheme is a Not for Profit organisation that is focussed on providing assessments and training in support of the standards that the National Cyber Security Centre (NCSC) has defined for the CHECK scheme.

Cyber Scheme is one of two contracted examinations bodies to support the CHECK scheme.

Cyber Scheme undertakes technical assessments for Team Members and Team Leaders Infrastructure and Web Applications).

It is important to recognise that the NCSC is the only body that can award CHECK team member or CHECK team leader status within the scheme but individuals undertaking the exams with Cyber Scheme are issued with a certificate (subject to passing the exam) confirming they meet the required technical standards. This certificate forms part of the evidence requirements in order to achieve CHECK status. For individuals not intending to apply for CHECK status, an exam pass also demonstrates that the candidate has met the minimum technical standards set by the UK national authority on cyber security and as such is applicable to all companies seeking assurance over professional skill levels and competence in penetration testing.

Cyber Scheme Ltd 2022

Eagle Tower | Montpelier Drive | Cheltenham | Gloucestershire | GL50 1TA

admin@thecyberscheme.org | www.thecyberscheme.org

Cyber Scheme is a company registered in England with Company Number 08686981

The above address is the official registered address of The Cyber Scheme