THE CSTL-APP

(CYBER SCHEME TEAM LEADER - WEB APPLICATIONS).

SETTING THE STANDARD IN TECHNICAL EXAMINATIONS FOR SECURITY TESTERS.

ABOUT THE EXAM

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, and operating systems to demonstrate they can identify, assess and exploit common misconfigurations or vulnerabilities by identifying the key areas of weakness within the environment.

A pass in this highly regarded technical qualification is one of the mandatory requirements for the Principal and Chartered Level Professional Title with the UK Cyber Security Council (security testing).

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:
    - injection vulnerabilities e.g. SQL injection
    - cross-site scripting (XSS) vulnerabilities
    - privilege escalation vulnerabilities
    - information disclosure vulnerabilities.
- Core capability to produce an accurate site map.

ASSESSMENT COMPONENTS

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 assessment is split into 3 sections, with a 15 minute break.

1. Client Engagement/Scoping 15 minutes

All candidates will share a common scoping briefing to outline what is required. Candidates will have up to 10 minutes each to ask questions concerning the scope of the penetration test. During your scoping session, the Assessor will play the role of the commissioning client exploring your knowledge in a range of fields. Your performance during the individual scoping session will form part of the assessment.

All engagements are recorded for exams audit.

2. Technical analysis of the target Web Application (practical penetration test) 4 hours

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.

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.

3. Post assessment reporting/debrief (viva) 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 be able to highlight any additional steps you would undertake had there been more time allocated;

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.

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