Certified AppSec Pentester (CAPen)

Home   Certified AppSec Pentester (CAPen)

Certified AppSec Pentester (CAPen)

Certified AppSec Pentester (CAPen) is an intermediate-level exam to test a candidate's knowledge on the core concepts involving application security. Candidates must be able to demonstrate practical knowledge to conduct an application pentest to pass this exam.

~~£400~~

£150

Buy Now

Who should take this exam?

CAPen is intended to be taken by pentesters, application security architects, SOC analysts, red and blue team members and any AppSec enthusiast, who wants to evaluate and advance their knowledge.

What is the format of the exam?

CAPen is an intense 4 hour long practical exam. It requires attendees to solve a number of challenges, identify and exploit various vulnerabilities and obtain flags. The exam can be taken online, anytime (on-demand) and from anywhere. Attendees will need to connect to the exam VPN server to access the vulnerable applications.

What is the pass criteria for the exam?

The pass criteria are as follows:

- Attendees scoring over 60% marks will be deemed to have successfully passed the exam.
- Attendees scoring over 75% marks will be deemed to have passed with a merit.

What is the experience needed to take the certification?

This is an intermediate-level exam. Attendees should have prior knowledge and experience of application pentesting. They should have an understanding of common application security related topics such as the OWASP Top 10, commonly identified security misconfigurations, and best security practices. They should be able to demonstrate their practical knowledge on AppSec topics by completing a series of tasks on identifying and exploiting vulnerabilities that have been created in the exam environment to mimic the real world scenarios.

Note: As this is an intermediate-level certification, a minimum of two years of professional pentesting/bug-bounty experience is recommended.

What will the attendees get?

On completing the exam, each attendee will receive:

- A certificate with their pass/fail and merit status.
- The certificate will contain a code/QR link, which can be used by anyone to validate the

certificate.

What is the exam retake policy?

Candidates who fail the exam, must purchase a new exam voucher to retake the exam.

What are the benefits of this certification?

The certificate will allow attendees to demonstrate their understanding of application security topics.

This will help them to advance in their career.

Certification syllabus

The exam will cover the following topics

- ✓ **Google Hacking, Dorking and OSINT techniques.**
    - Blacklisting
    - Whitelisting

- ✓ **Identification and exploitation of OWASP Top 10 Vulnerabilities**
- ✓ **XML External Entity attack**
- ✓ **SQL Injection**
- ✓ **Cross-Site Request Forgery**
- ✓ **Practical Cryptographic Attacks**
- ✓ **Authentication related Vulnerabilities**

    - Brute force Attacks
    - Password Storage and Password Policy

- ✓ **TLS Security**

    - Identification of TLS security Misconfigurations.

- ✓ **Server-Side Request Forgery**
- ✓ **Authorization and Session Management related flaws –**

    - Insecure Direct Object Reference (IDOR)
    - Parameter Manipulation attacks

- ✓ **Insecure File Uploads**
- ✓ **Code Injection Vulnerabilities**
- ✓ **Business Logic Flaws**
- ✓ **Directory Traversal Vulnerabilities**
- ✓ **Common Security Misconfigurations.**

✓ **Information Disclosure.**

Vulnerable and Outdated Components.

Common Supply Chain Attacks and Prevention Methods.

Common Security Weaknesses affecting Cloud Services such as a S3 Bucket.

Security Best Practices and Hardening Mechanisms.

- Security Headers.

Sample Question

Register an account on the target website. Identify a flaw within the reset password functionality and login as user admin@dummysite.com. After successful login, you will see a flag being displayed. Provide the flag below:

Certified AppSec Pentester (CAPen)

Buy Now

The SecOps Group   Quick Links

The SecOps Group is founded by industry veterans. We have over 15 years of experience in providing cyber security consultancy and have worked with some of the largest blue chip companies. Being an independent boutique company, we enable our customers to continuously identify and assess their security postures and provide advice in securing against the adversaries.

About Us

Services

Blockchain Security Services

Certifications

All Certifications

Certified Blockchain Practitioner (CBP)

Certified AppSec Practitioner (CAP)

Certified Network Security Practitioner (CNSP)

Certified AppSec Pentester (CAPen)

Contact Us

🇬🇧
The SecOps Group UK Limited.
Address: Stonecross, Trumpington High Street, Cambridge. CB2 9SU
Phone: +44-122-392-6819
🇺🇸
The SecOps Inc.
Address:16192 Coastal Highway, Lewes, Sussex,Delaware 19958U
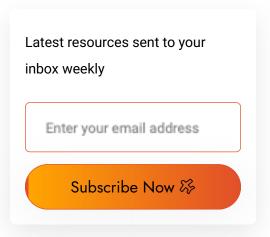**Phone:** +1-602-625-0641
🇮🇳
Security Ops India Pvt. Ltd.
Address:A/403, Shree Exotica, Opp. Aashtha Bunglows, Ahmedabad, Gujarat, India 382350.
Phone: +91-942-811-5003

Newsletter

Latest resources sent to your inbox weekly

Enter your email address

Subscribe Now ✈

Follow Us

Twitter

LinkedIn