Information

[Task 1] Introduction

[OWASP Top 10 - A challenge everyday for 10 days]

Learn one of the OWASP vulnerabilities every day for 10 days in a row.
A new task will be revealed every day, where each task will be independent from the previous one.
These challenges will cover each OWASP topic:

- **Day 1) Injection**
- **Day 2) Broken Authentication**
- **Day 3) Sensitive Data Exposure**
- **Day 4) XML External Entity**
- **Day 5) Broken Access Control**
- **Day 6) Security Misconfiguration**
- **Day 7) Cross-site Scripting**
- **Day 8) Insecure Deserialization**
- **Day 9) Components with Known Vulnerabilities**
- **Day 10) Insufficent Logging & Monitoring**

The challenges are designed for beginners and assume no previous knowledge of security.

#1
Read the above.

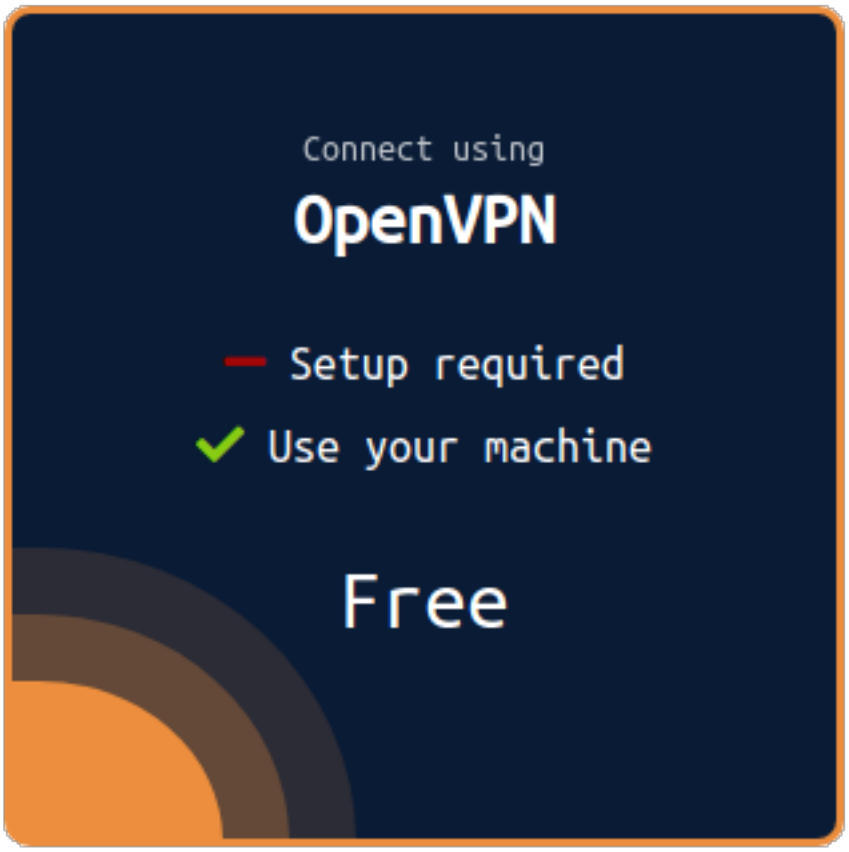
No answer needed

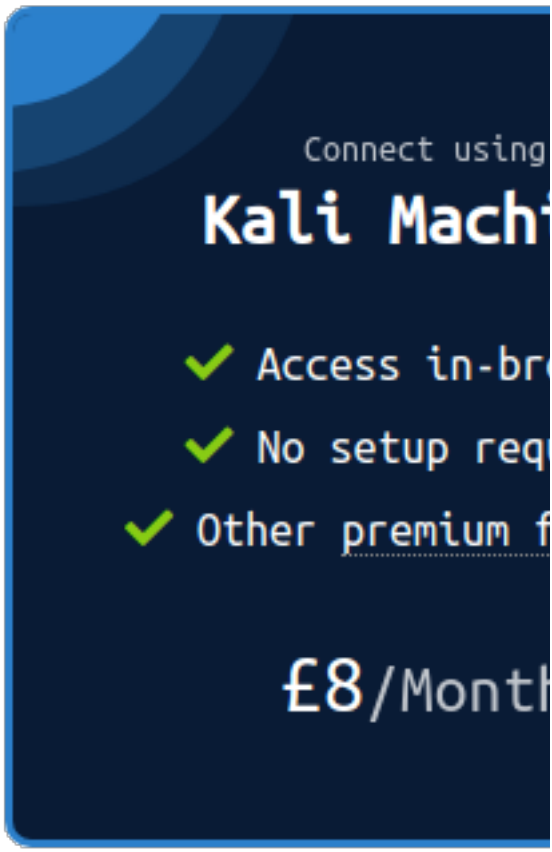
[Task 2] Accessing machines

Some tasks will have you learning by doing, often through hacking a virtual machine.

However, to access these machines you need to either:

OpenVPN	Kali Machine
Connect using OpenVPNFollow the guide here to connect using OpenVPN.	Use an in-browser Linux MachineIf you're subscrib machine!





#1
Practise connecting to our network.

No answer needed

[Task 3] Daily Prizes

Completing tasks gives you the opportunity to win prizes.
1 day after each challenge, we will randomly select a winner by picking a user who has completed the previous days challenge.

#1
Read the above.

No answer needed