Completed   Congrats!

Avenger666
Gold Annual

⬡ 567   ▭ 2

LEARN
- 🖥 Dashboard
- 🎓 Exams
- 📒 Modules
- 📍 Paths
- 🕸 Academy x HTB Labs

MY ACHIEVEMENTS
- 🎓 My Certificates
- 🏆 My Badges   **1**

REFERRALS
- 🎁 Invite friends

GET HELP
- ❓ Help Center
- ❓ FAQ
- 💬 Discord
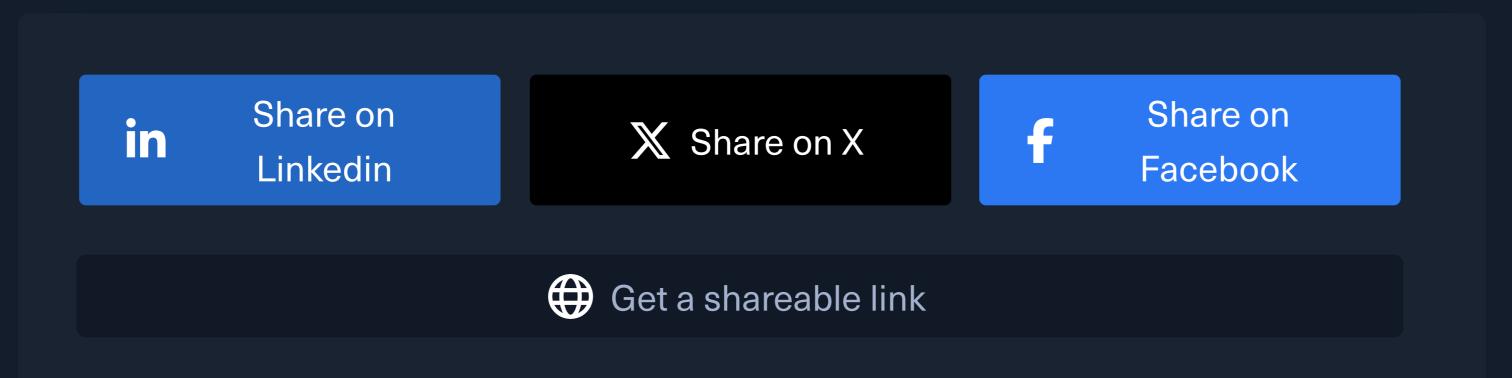
Hacking WordPress

Congratulations!

You have just completed the Hacking WordPress module
You earned +20 ⬡

★ ★ ★ ★ ☆

in   Share on Linkedin

𝕏   Share on X
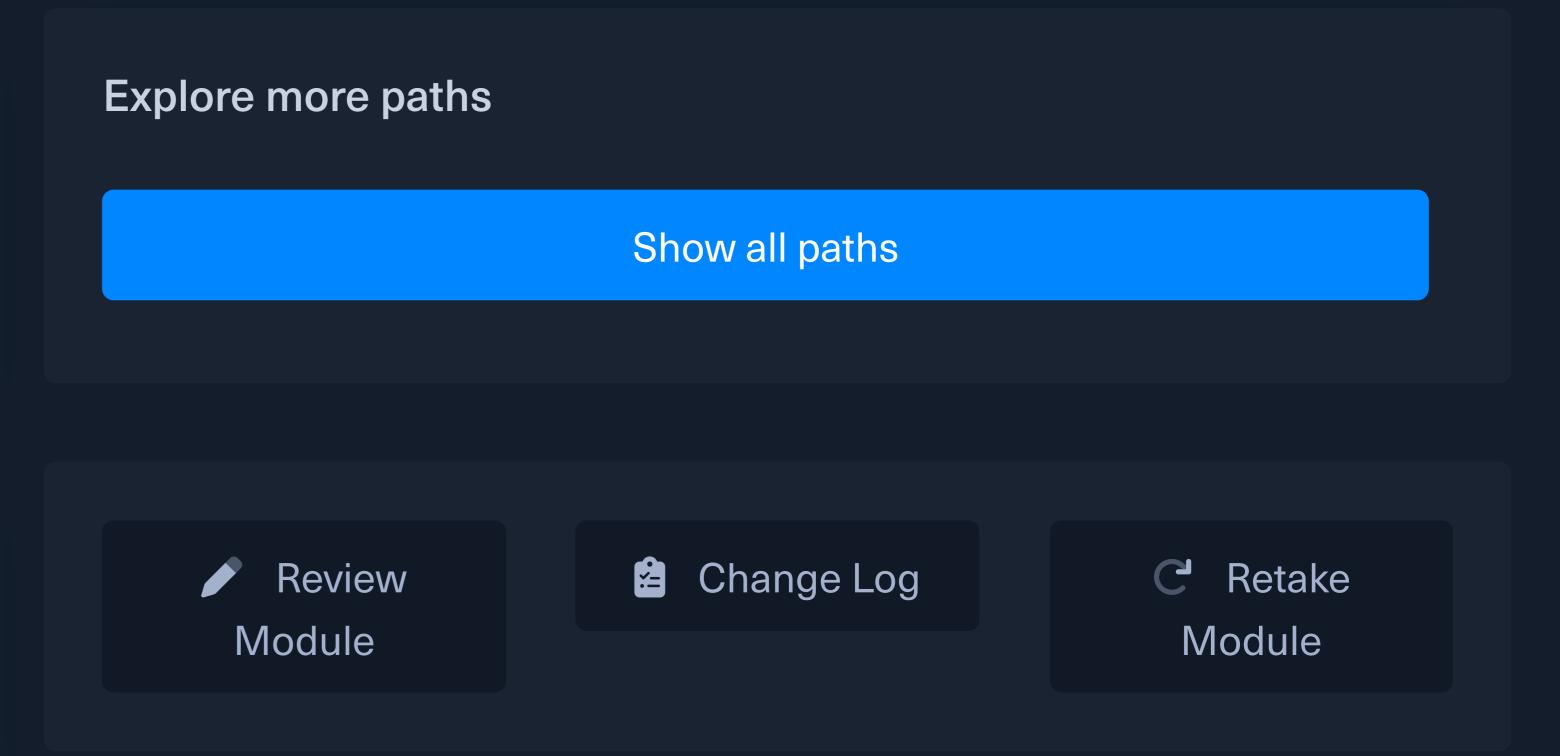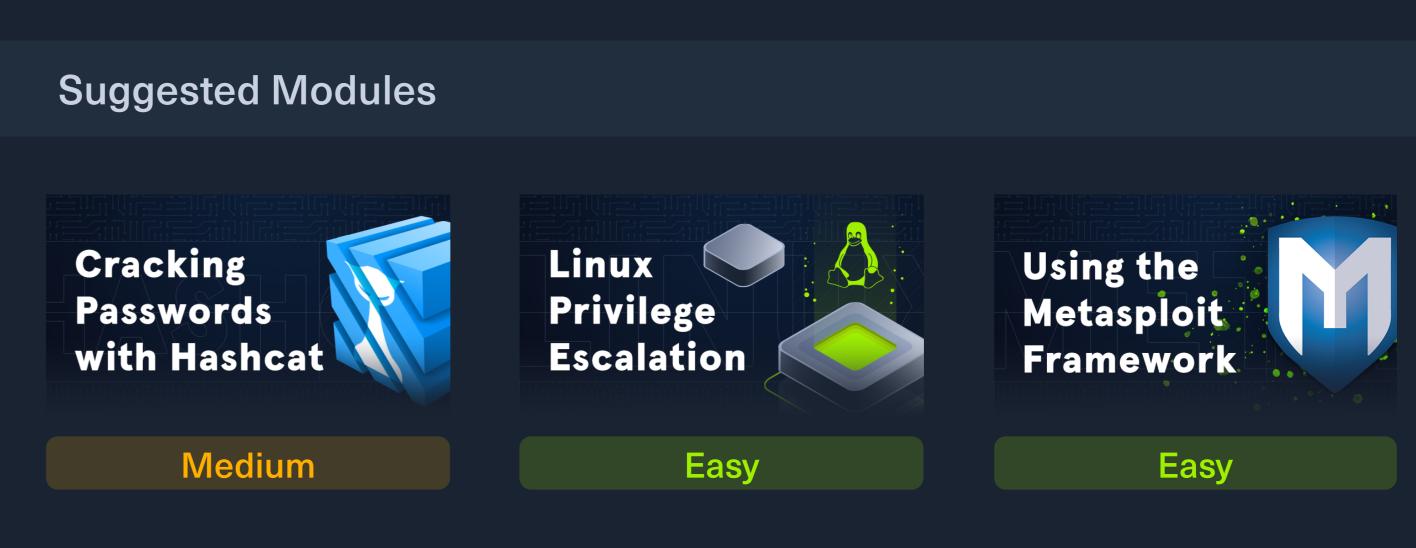
f   Share on Facebook

🌐   Get a shareable link

Conclusion

In this module, we covered the structure of a WordPress website to better understand manual and automated WordPress enumeration techniques and a variety of attacks against users, WordPress components, and the WordPress web server.
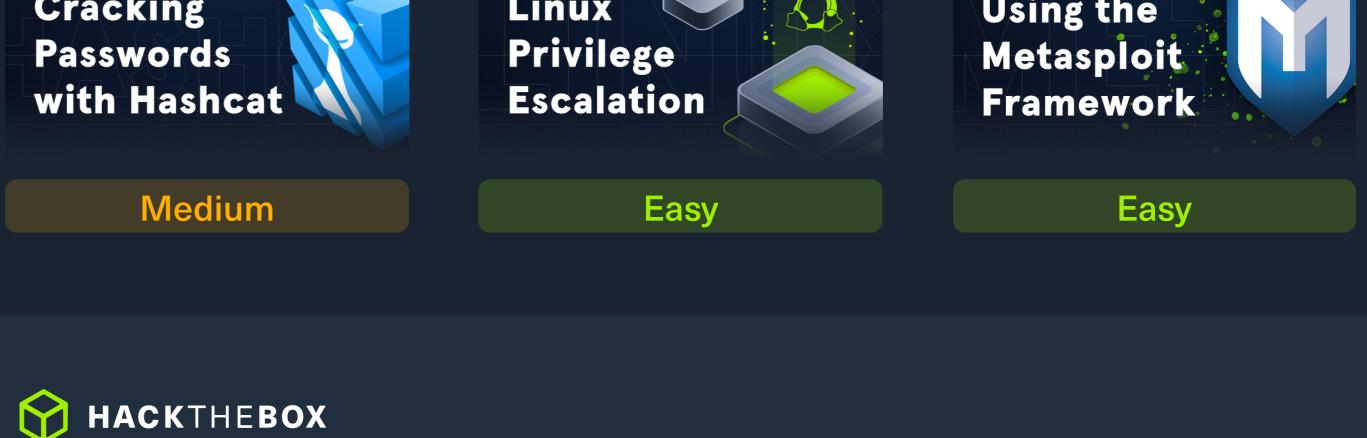
Module Key Takeaways

- The structure of a WordPress website
- Manual enumeration techniques
- Automated enumeration techniques using the `WPScan` tool
- Attacking WordPress users
- Manual attacks against WordPress features
- Automated attacks against WordPress core
- WordPress security hardening best practices

Explore more paths

Show all paths

✏ Review Module   📋 Change Log   ↻ Retake Module

What's Next?

Here are a few suggestions to try out based on the path you 've just completed!

Suggested Modules

Cracking Passwords with Hashcat	Linux Privilege Escalation	Using the Metasploit Framework
Medium	Easy	Easy

🔲 **HACK**THE**BOX**

In order to play the content below, you need an active subscription at Hack The Box

Machines

- 🔴 Tenten M
- 🔴 Brainfuck I
- 🔵 Blocky E
- 🔴 Apocalyst M
- 🟠 Enterprise M
- 🟠 Aragog M
- 🔴 TartarSauce M
- 🔵 Chaos M
- 🟠 Tenet M
- 🔵 Spectra E
- 🔴 Monitors H
- 🔵 Toby I
- 🟠 Backdoor E
- 🔴 Paper E
- 🔴 Pressed H
- 🔴 Moderators H
- 🔴 Phoenix H
- 🔵 MetaTwo E

Prolabs

- 🔴 Dante I