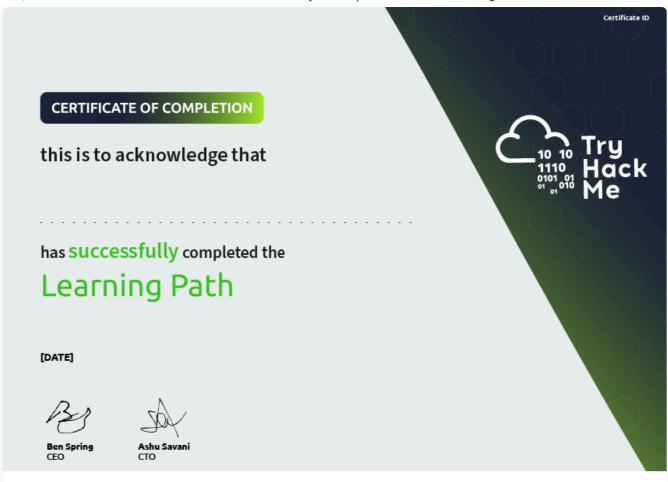




A pathway to web application security.

- Understand web fundamentals
- Major vulnerabilities explained
- Learn industry-used tools
- Web application assessments



Complete this learning path and earn a certificate of completion

Introduction

The aim of this path is to teach you how to attack web applications. To successfully attack and exploit web applications, you need to understand how they work. The first section (Web Fundamentals) will give you all the pre-requisite knowledge on this.

The second section (Security Tools) focuses on learning how to use Industry Standard tooling to interact with your targets.

The third section (Vulnerabilities) covers various vulnerabilities found in web applications today. This section will go over root causes of these vulnerabilities and give you hands on experience on exploiting them.

The final section (Practise Makes Perfect) will help you apply what you've learnt in previous sections.

After completing this path, you should be able to:

- understand how web applications work
- utilise industry standard tooling when attacking web applications
- explain and exploit common web vulnerabilities
- apply this knowledge to other targets (be it within an interview or a professional web applications security assessment)

SECTION 1

How The Web Works



DNS in detail



HTTP in Detail



How Websites Work



Putting it all together

SECTION 2

Introduction To Web Hacking



Walking An Application



Content Discovery



Subdomain Enumeration



Authentication Bypass



IDOR



File Inclusion



Intro to SSRF



Intro to Cross-site Scripting



Command Injection



SQL Injection

SECTION 3

Burp Suite



Burp Suite: The Basics



Burp Suite: Repeater



Burp Suite: Intruder



Burp Suite: Other Modules



Burp Suite: Extensions

SECTION 4

Web Hacking Fundamentals



How Websites Work



HTTP in Detail



Burp Suite: The Basics



OWASP Top 10 - 2021



OWASP Juice Shop



Upload Vulnerabilities



Pickle Rick

Copyright TryHackMe 2018-2025











