What you'll learn

- 90+ Videos to take you from a beginner to advanced in website hacking.
- Create a hacking lab & needed software (on Windows, OS X and Linux).
- Become a bug bounty hunters & discover bug bounty bugs!
- Discover, exploit and mitigate a number of dangerous web vulnerabilities.
- Exploit these vulnerabilities to hack into web servers.
- Bypass security & advanced exploitation of these vulnerabilities.
- Advanced post exploitation - hack other websites on the same server, dump the database, privilege escalation....etc
- Bypass security & filters.
- Intercept requests using a proxy.
- Adopt SQL queries to discover and exploit SQL injections in secure pages.
- Gain full control over target server using SQL injections.
- Discover & exploit blind SQL injections.
- Install Kali Linux - a penetration testing operating system.
- Learn linux commands and how to interact with the terminal.
- Learn linux basics.
- Understand how websites & web applications work.
- Understand how browsers communicate with websites.
- Gather sensitive information about websites.
- Discover servers, technologies & services used on target website.
- Discover emails & sensitive data associated with a specific website.
- Find all subdomains associated with a website.
- Discover unpublished directories & files associated with a target website.
- Find all websites hosted on the same server as the target website.
- Discover, exploit and fix file upload vulnerabilities.
- Exploit advanced file upload vulnerabilities & gain full control over the target website.
- Discover, exploit and fix code execution vulnerabilities.
- Exploit advanced code execution vulnerabilities & gain full control over the target website.
- Discover, exploit & fix local file inclusion vulnerabilities.
- Exploit local file inclusion vulnerabilities to to get a shell.
- Exploit advanced local file inclusion vulnerabilities & gain full control over the target website.
- Exploit advanced remote file inclusion vulnerabilities & gain full control over the target website.
- Discover, fix, and exploit SQL injection vulnerabilities.
- Bypass login forms and login as admin using SQL injections.

- Writing SQL queries to find databases, tables and sensitive data such as usernames ad passwords using SQL injections
- Bypass filtering, and login as admin without password using SQL injections.
- Bypass filtering and security measurements.
- Read / Write files to the server using SQL injections.
- Patch SQL injections quickly.
- Learn the right way to write SQL queries to prevent SQL injections.
- Discover basic & advanced reflected XSS vulnerabilities.
- Discover basic & advanced stored XSS vulnerabilities.
- How to use BeEF framwork.
- Hook users to BeEF using reflected & XSS vulnerabilities.
- Steal credentials from hooked targets.
- Run javascript code on hooked targets.
- Create undetectable backdoors.
- Hack computers using XSS vulnerabilities.
- Fix XSS vulnerabilities & protect yourself from them as a user.
- What do we mean by brute force & wordlist attacks.
- Create a wordlist or a dictionary.
- Launch a wordlist attack and guess admin's password.
- Discover all of the above vulnerabilities automatically using a web proxy.
- Run system commands on the target webserver.
- Access the file system (navigate between directories, read/write files).
- Download, upload files.
- Bypass security measurements.
- Access all websites on the same webserver.
- Connect to the database and execute SQL queries or download the whole database to the local machine.
- Discover, exploit and mitigate CSRF vulnerabilities.