THE SPYDER SECURITY

Bug Bounty

Beginners to Advance Course.

Course Content.

- Burp suite installation
- Kali Linux installation
- Click jacking Broken authentication
- HSTS
- CORS
- Relocation data not stripped from upload
- Email , password or delete account validation
- Basic testing on login , account and registration page Information disclosure
- Long password DOS attack
- Web Cache deception attack
- Session hijacking
- URL redirection
- Host Header attack
- LFI or RFI
- IDOR
- SSRF
- Word press CMS Vulnerability Hunting
- Command Injection
- Advance SQL injection
- XSS (Blind , Stored , Reflected)
- HTML injection
- NMAP

- SHODAN
- 2FA Bypass
- xmlprc.php exploit
- CRLF
- CVE
- Session does not expire after password reset and update
- DMARC and SPF
- Authentication bypass
- Rate limit bypass
- Catechu bypass
- CSRF -(basic to advance)
- Password token leak via third party
- File uploading
- Account lockout
- Parameter tempering
- Sub domain Takeover
- AWS Pen testing
- JWT Token Attack
- Apache Strict Race
- Dependency Confusion
- Recon
- Business Logic Bugs

- Cryptography Vulnerability
- Sensitive Data Exposure
- Broken Link Hijacking
- Session Fixation
- Failure to Invalidate Session
- Remote Code Execution
- Way back Archive