WEB PENTEST FUNDAMENTALS

1. Introduction
2. How the internet works?
3. Introduction
4. Network nodes
* server
* client
* host
1. What is the Internet?
2. OSI model
* Introduction and example
* TCP/UDP
1. Connection
	* IP and Port
	* Public and Private IP
	* 3-way TCP handshake
	* Netcat, make a connection
2. Content encoding
3. web server
	* What is Web Server?
	* How Web Server Works?
4. Domain name system (DNS)
	* Concept
	* How DNS works?
	* DNS server
	* DNS client
	* Name server
	* DNS lookup by DIG
	* Host file
5. HTTP protocol
* Versions and RFCs
* Webserver again
* URLs
	+ Syntax and parts
	+ Check a URL list
* HTTP
	+ Message
	+ Request line
	+ HTTP method
	+ Status line
	+ Headers
	+ Body
	+ Sending some HTTP requets
* [the list of all headers](https://developer.mozilla.org/en-US/docs/Web/API/Headers)
	+ Important headers
* Authentication
* Caching
* Conditional
* Cookie
* CORS
* Message Body
* Proxies
* Redirects
* Request Context
* Security
* http security headers (youtube playlist)
1. HTTPS
	* Reveiw, Problem
	* Symmetric Encryption
	* Asymmetric Encryption
	* Signature and authentication
	* SSL Protocol
	* Certificates and authorities
	* Trust chain
	* How does SSL work?
	* The handshake
	* Implementation
	* Security issues
2. Encoding Schemas
	* url encoding
	* Unicode encoding
	* Html Encoding
	* Base64 Encoding
	* Hex Encoding
3. Web Functionality
	* The Client & Server Model
	* Http requests and responses
	* Internet Security Controls
* Server Side Functionality
* Client Side Functionality
* Frameworks and Libraries
1. Security
* Vulnerability
	+ The root cause
	+ Technical vulnerabilities
	+ Logical vulnerabilities
	+ Severity
	+ Categories
	+ CVSS score
	+ Exploit
	+ Payload
	+ Attack vector
	+ CVE
	+ 0day, 1day
	+ OWASP
1. Pentest Mythologies and standards
2. Footprinting
	* Spider Application
	* Discover Server Information
	* Discover Hidden Content
	* Automate Scans
	* Analyze Resault
3. Introducing Most used tools in Web Pentesting
4. DataBases
	* Types of Data bases
	* Redis
5. Authentication
	* Authentication Tenchnologies
* Session Management and http cookie
* Json Web Tokens
	+ Design Flaws in Authentication
	+ Mechanisims
	+ Bad passwords
	+ Brute forcible Login
	+ Verbose Failure Messages
	+ Password Change Functionality
	+ Forget Password Functionality
1. OAuth 2.0 Security
	* Introducing the OAuth 2.0 model
	* Receiving grants
	* Exploiting OAuth for fun
2. Api
	* Introducing to Api
	* Understanding REST APIs
	* Learning the API
	* Basic methodology to test developer APIs