**Ethical Hacking Day #5**

**HTTP Methods:**

GET – POST – PUT – OPTIONS – HEAD – DELETE

HTTP Request

Method + URL + Headers

POST request → + Body

**GET**

parameter in URL

limited length

**POST**

parameters in body

Unlimited Length

**HTTP Request**

Method /endpoint

Request Headers

Host

User-Agent

Origin

Referer

Sessions → Token , key , dummy value, encrypted value, encoded value → relate to ur account

Session related Vulnerabilities

**- Session Misconfiguration**

**Vulnerability**: Concurrent Sessions

User can have many active sessions in the same time

**Vulnerability**: Session take a long time to expire

**Vulnerability**: Session Fixation

**Vulnerability**: Session Token Revealed in URL

JWT → JSON Web Token

APIs →

- JSON →

- XML →

Cryptography

Plain → Cyber Security is important

key = ITI

- Encryption

- Symmetric:

Plain → encrypt using Key → Encrypted

Encrypted → decrypt Key → Plain

- Asymmetric:

Plain → encrypt using Private Key → Encrypted

Encrypted → decrypt using public key → Plain

- Hashing → One way encryption

Data cannot be decrypted

- MD5 algorithm

- SHA1 algorithm

Rainbow Table

[1](mailto:p@ssw0rd)23456789

Salting

ITI+passwords →

[1](mailto:p@ssw0rd)23456789 -> ITI123456789

- Get password from the user in the login page

- Add the salt value to the password

- MD5 hash for the (salt+password)

- compare the generated hash value with the hash value in the DB

- Encoding

URL Encoding

HTML Encoding

Base64 Encoding

Phishing