Module 12 - Attacking Crypto

Padding Oracle Attack

- padding oracle attacks target CBC-mode decryption functions operating with PKCS7-mode padding.

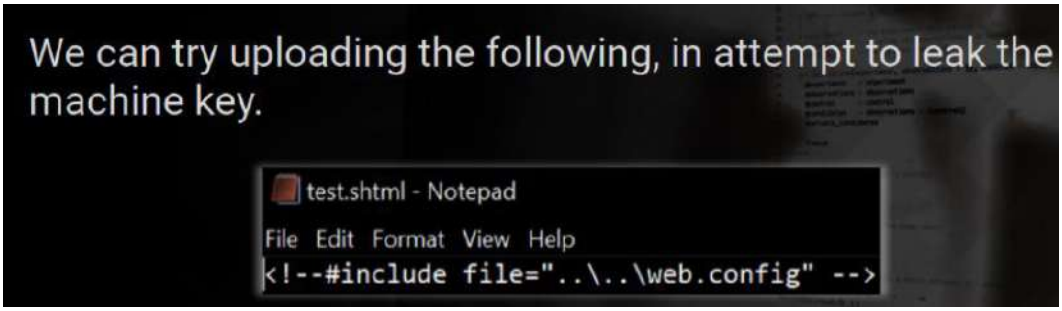
What is a padding oracle

- Google it

Hash Length Extension Attack

- algorithms like MD5, SHA-1 and most of SHA-2 that are based on the Merkle-Mamgard construction are susceptible to this kind of attack.
- Truncated versions of SHA-2, including SHA-384 and SHA-512/256 are not susceptible,[4] nor is the SHA-3 algorithm.[5] HMAC also uses a different construction and so is not vulnerable to length extension attacks.[6]
- Tool:
  - https://github.com/iagox86/hash_extender

Leveraging machineKey



- here we didn't attack crypto, but we stole the crypto key through SSII.