POODLE

Cryptographic Attack

by
Yonatan Goldenberg

Background

- The POODLE (Padded Oracle On Downgraded Legacy Encryption) is a type attack that's aimed to decrypt the encrypted traffic between a server and a user.

- It takes advantage of a vulnerability existing in the SSL 3.0 protocol that was used for HTTPS since 1996 to about 2015.

- This vulnerability was disclosed to the public by Google in 2014, and the SSL 3.0 protocol was declared deprecated shortly after.

Steps of the Attack

- The attack requiered to first establish a MITM connection where the attacker can sniff all the traffic between the user and the server.

- Additionally the attacker needs to inject a script to the user that would start sending requests through the user, taking advantage of his session cookies etc.

- The attacker would then start dropping the TLS handshake proccess with the server making it think the client can't support current versions of TLS. So then some servers would downgrade to SSL 3.0.

Steps of the Attack

- Now that the communication uses SSL 3.0 for encryption the attacker would send repeated requests through the user. He then can sniff them, modify and send them again, monitoring which requests the server accepted and after which the connection droped.

- That way the attacker could reveal on byte at a time and eventually decrypt enough of the request to get the session cookie and log in freely as the user.

- The actual cryptographic vulnerability in the protocol you will have to research and implement yourself in the challenge.

Challenge Instructions

- This challenge is made to run in a closed docker environment by running "docker compose up –d" in the main folder (named POODLE)

- It is possible to run directly on sour system but it will require to install all the dependencies from the requierments.txt and changing the server and victim URLs as described in the readme of the project

- Note that the server must be up first and then the victim since it has to get the cookie from the server for the challenge to begin

Challenge Instructions

- In this challenge you will only work in the client/attacker.py file as you are the attacker

- You cannot import any libraries and can't change any existing code in other files. You can only add code to the main funcion and add helper functions if needed.

- The only tool you have is 2 functions provided by the victim_api. get_request takes 2 string, one for path and one for data and gives you a series of bytes that are the encrypted request to the server with the path and data provided. The encryption is with the key sets the server provides the victim. The original request look like this: POST /{path} HTTP/1.1\r\n Cookies: session-cookie={secret_cookie}\r\nBody: {data}

Challenge Instructions

- The second function is send_request which takes your request bytes and sends them to the server through the victim along with his session cookie.

- You will have to use these 2 functions to find that session cookie. To be sure you are correct you can pass the cookie you found to the check_solution function that the victim also provides. You will get a victory response and complete the challenge if the cookie is right.

- There is more information in the readme.md of the repository including tips for different levels of skill to help you solve the challenge. Good luck!!!