

FAST National University of  
Computer and Emerging Sciences

FYP Proposal

HealthBridge

* Name: Muhammad Abdullah, Muneel Haider, Abdullah Zahoor
* Roll No: 21I-0643 , 21I-0640 , 21I-2481

Contents

[**Problem 1**: 3](#_gjdgxs)

[**Task 1**: 3](#_17dp8vu)

[Pseudocode: 3](#_3rdcrjn)

[Time Complexity: 5](#_26in1rg)

[**Task 2**: 5](#_lnxbz9)

[Pseudocode: 5](#_35nkun2)

[Time Complexity: 6](#_1ksv4uv)

[Memoization: 6](#_44sinio)

[**Task 3**: 6](#_2jxsxqh)

[Pseudocode: 6](#_z337ya)

[Time Complexity: 7](#_3j2qqm3)

[**Task 4**: 7](#_1y810tw)

[Pseudocode: 7](#_4i7ojhp)

[Time Complexity: 8](#_2xcytpi)

[**Problem 2**: 8](#_30j0zll)

[Pseudocode: 8](#_1ci93xb)

[Time Complexity: 11](#_3whwml4)

[**Problem 3**: 11](#_3znysh7)

[**Part a)** 11](#_2et92p0)

[Pseudocode: 11](#_tyjcwt)

[Time Complexity: 12](#_3dy6vkm)

[**Part b)** 12](#_1t3h5sf)

[Pseudocode: 13](#_4d34og8)

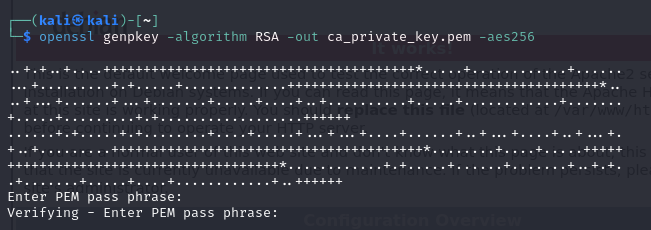
[Time Complexity: 15](#_2s8eyo1)

# **Setup VMWare Kali Linux:**

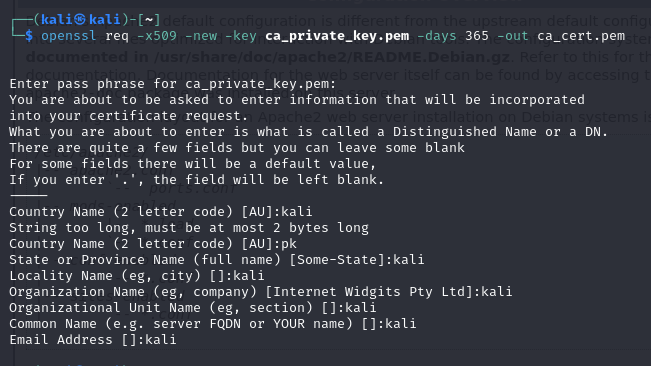
# **Installed openssl and apache2:**

# 

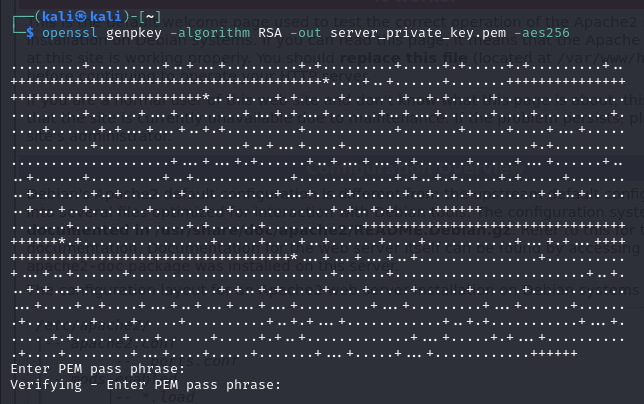
# **CA Private Key:**



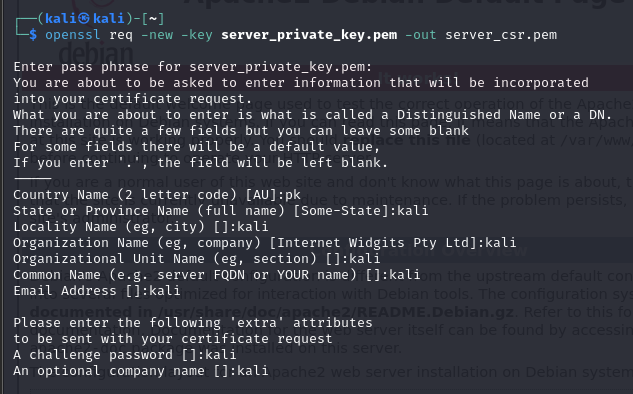
# **Using CA Private Key to Generate Self-Signed Root Certificate:**



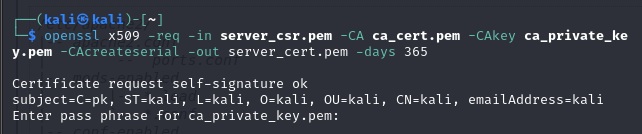
# **Server’s Private Key:**



# **Certificate Signing Request (CSR) for the Server:**



# **Sign the Server’s CSR with the CA Certificate:**



# **Local DNS (127.0.0.1) (muneel.com)**

# 

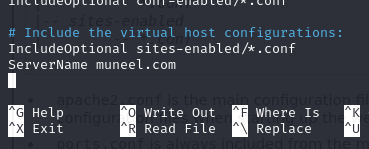
# **Enable SSL Module and Default SSL Site:**

# 

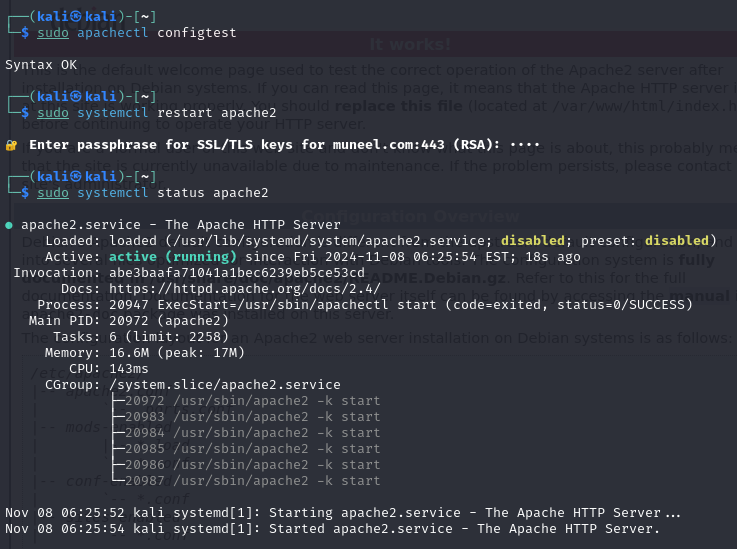
# **SSL site configuration file:**

# 

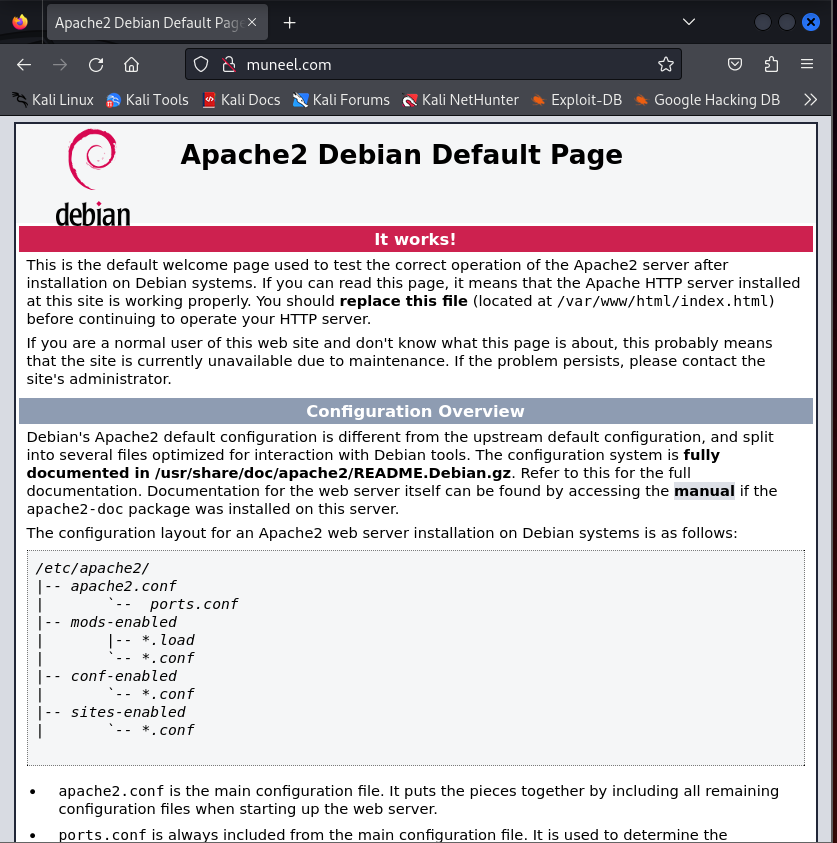
# **Adding ServerName (muneel.com):**



# **Start Apache2:**

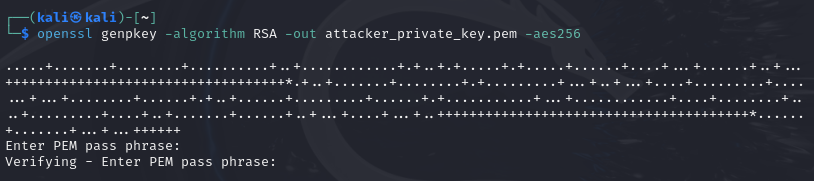


# **Visited muneel.com with Server Key and Certificate Configuration:**

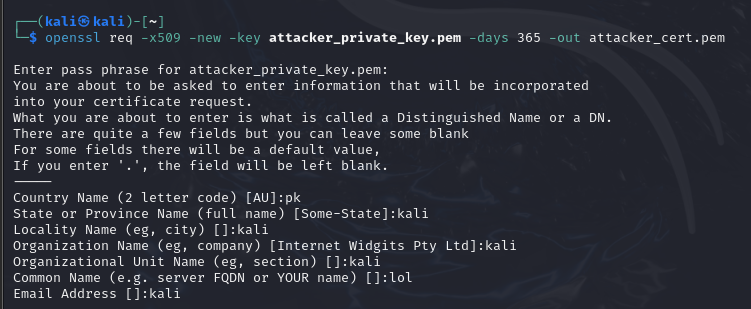


# **Man-in-the-Middle (MITM) Attack:**

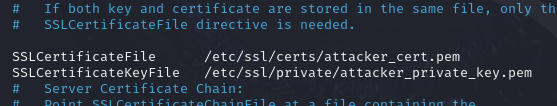
# **Private Key of the Attacker:**



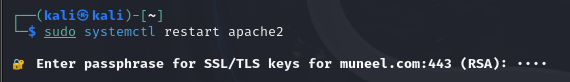
# **Self-Signed Certificate of the Attacker:**



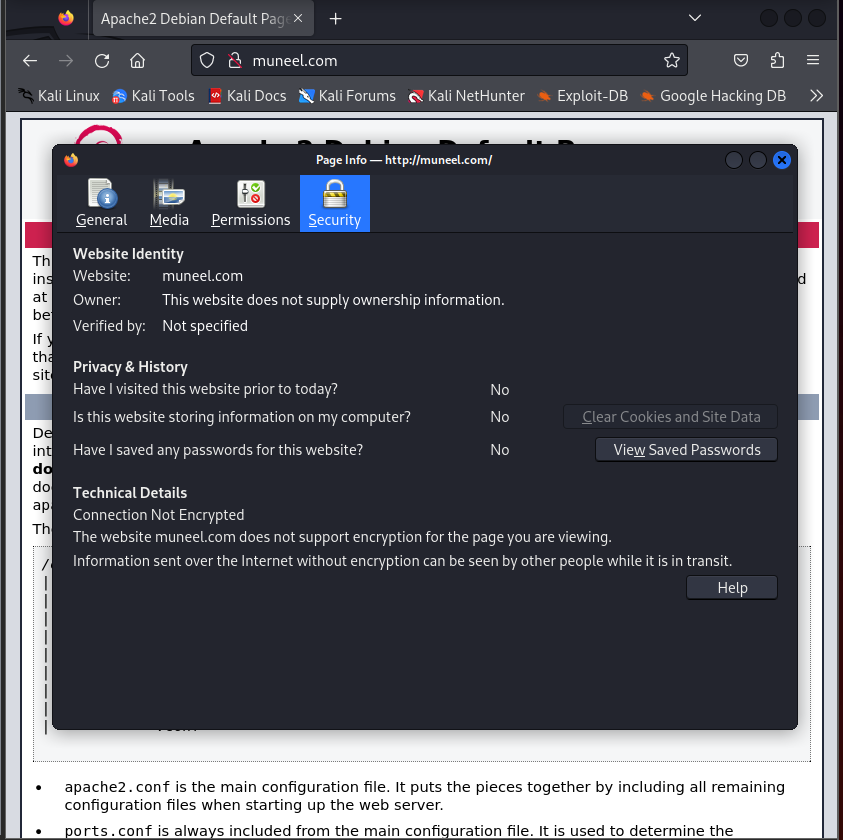
# **SSL configuration file editing to add attacker keys and certificate:**



# **Restart Apache2:**



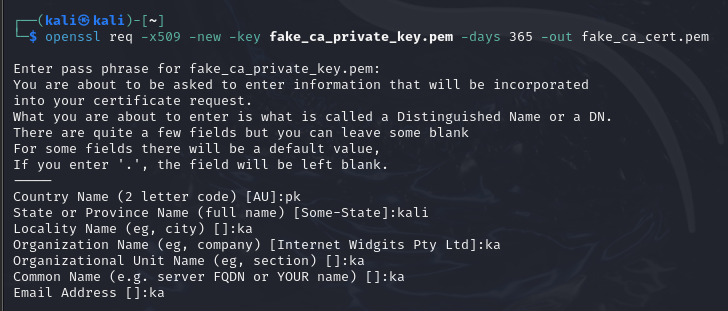
# **Revisited muneel.com as attacker:**



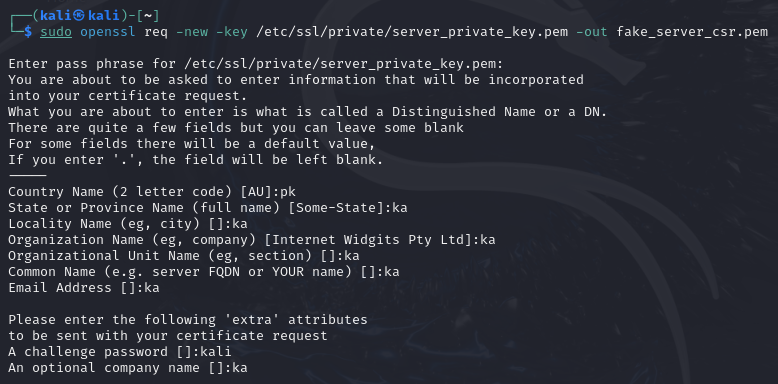
# **Man-in-the-Middle (MITM) Attack with Compromised Certificate Authority (CA):**

# **Private Key for the Fake CA:**

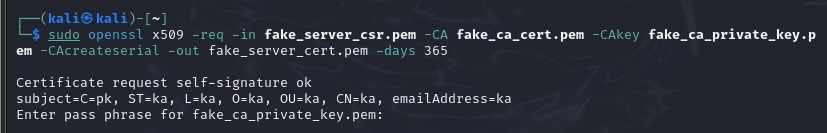
# **Self-Signed Certificate for the Fake CA:**



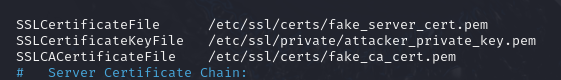
# **New Certificate for the Server Using the Fake CA:**



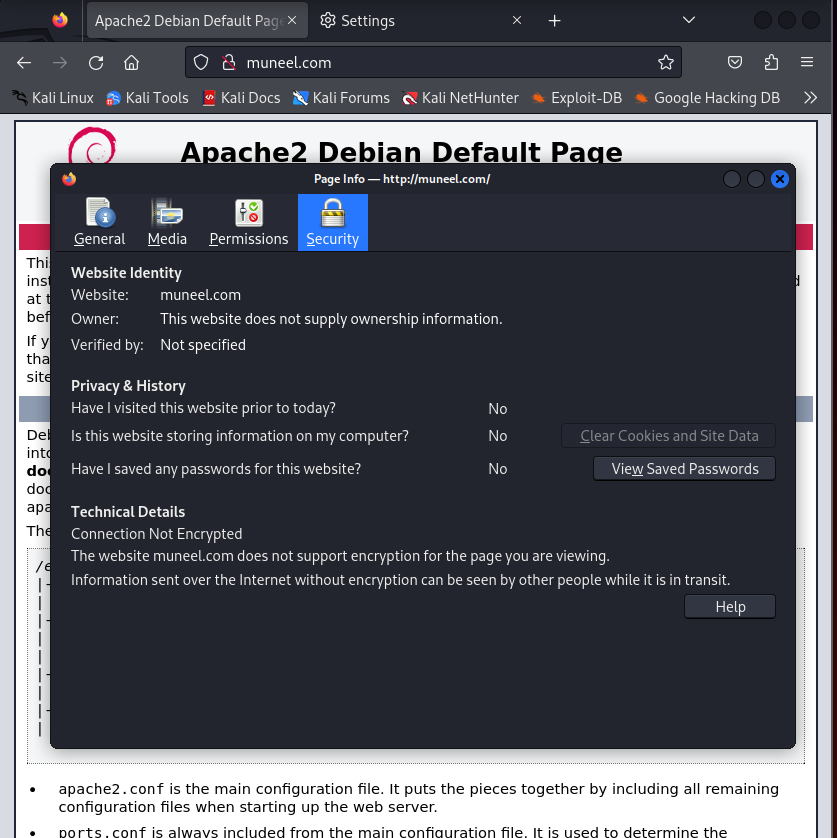
# **Sign the Server CSR with the Fake CA:**



# **SSL Configuration File to use the fake server certificate:**



# **Revisited muneel.com with Compromised CA:**



# **Attacker Keys:**

Access to timely and accurate medical diagnostics remains a significant challenge, especially in regions with limited healthcare resources. Traditional methods require patients to visit healthcare facilities, wait for appointments, and rely on overburdened healthcare professionals. This process can delay diagnosis and treatment, particularly in areas where healthcare infrastructure is weak or where there is a shortage of medical professionals. **HealthBridge** aims to bridge this gap by providing a platform that allows users to contact and book appointments with doctors nationwide, upload medical scans, receive automated diagnoses, and generate reports instantly, all while maintaining high standards of data security and accuracy.