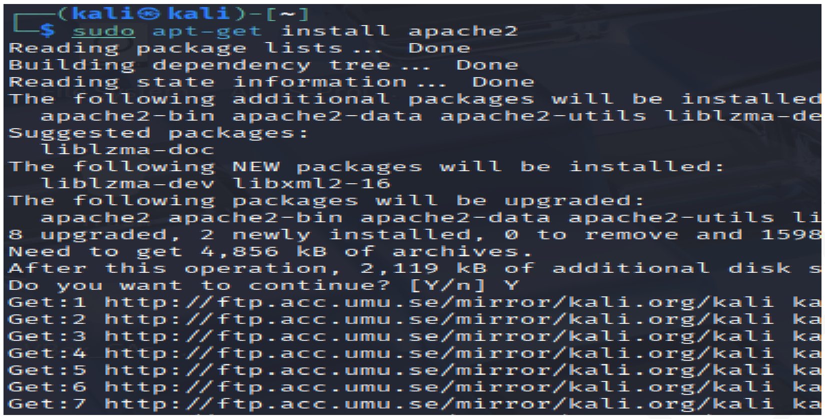
## Installation and Configuration of SSL/TLS Certificate on Apache Server

**Project Description:** This project details the installation and configuration of a TLS certificate on an Apache Server

### Installation of the Apache server

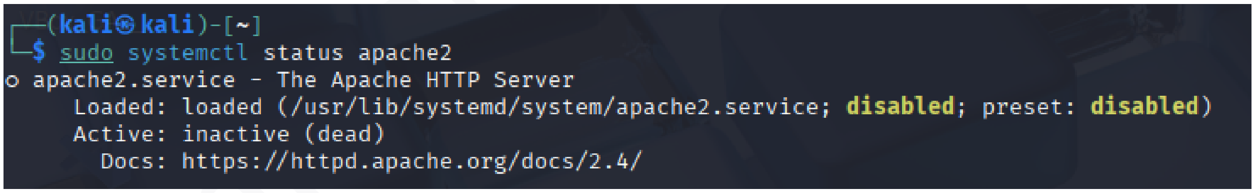
The snippet below shows the installation of the Apache 2 server through the command **“sudo apt-get install apache2.”**



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install apache2
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed
  apache2-bin apache2-data apache2-utils liblzma-de
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  liblzma-dev libxml2-16
The following packages will be upgraded:
  apache2 apache2-bin apache2-data apache2-utils li
8 upgraded, 2 newly installed, 0 to remove and 1598
Need to get 4,856 kB of archives.
After this operation, 2,119 kB of additional disk s
Do you want to continue? [Y/n] Y
Get:1 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:2 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:3 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:4 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:5 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:6 http://ftp.acc.umu.se/mirror/kali.org/kali ka
Get:7 http://ftp.acc.umu.se/mirror/kali.org/kali ka
```

### Status Verification of Apache 2 Server

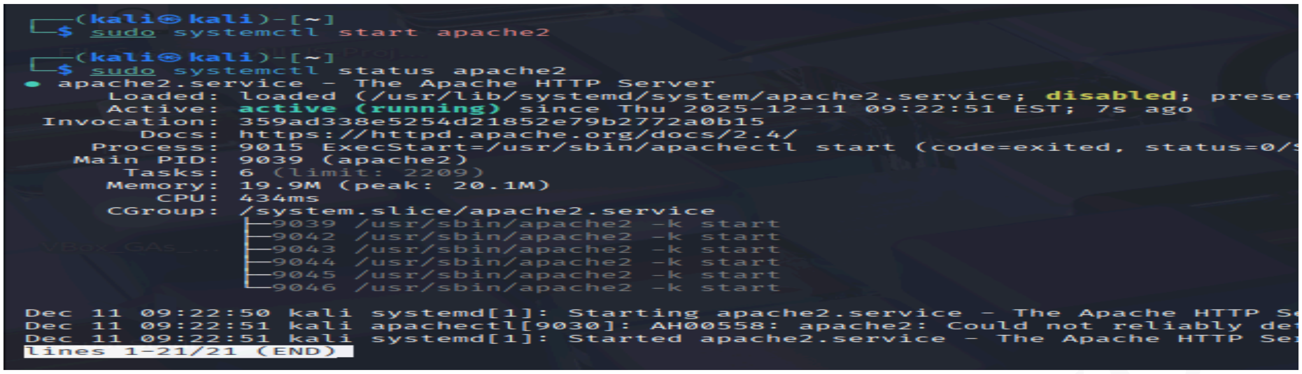
The snipnet checks the status of the Apache2 server through the command **“sudo systemctl status apache2”** and confirms that the status is inactive



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
○ apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/
```

### Starting the Apache 2 Server

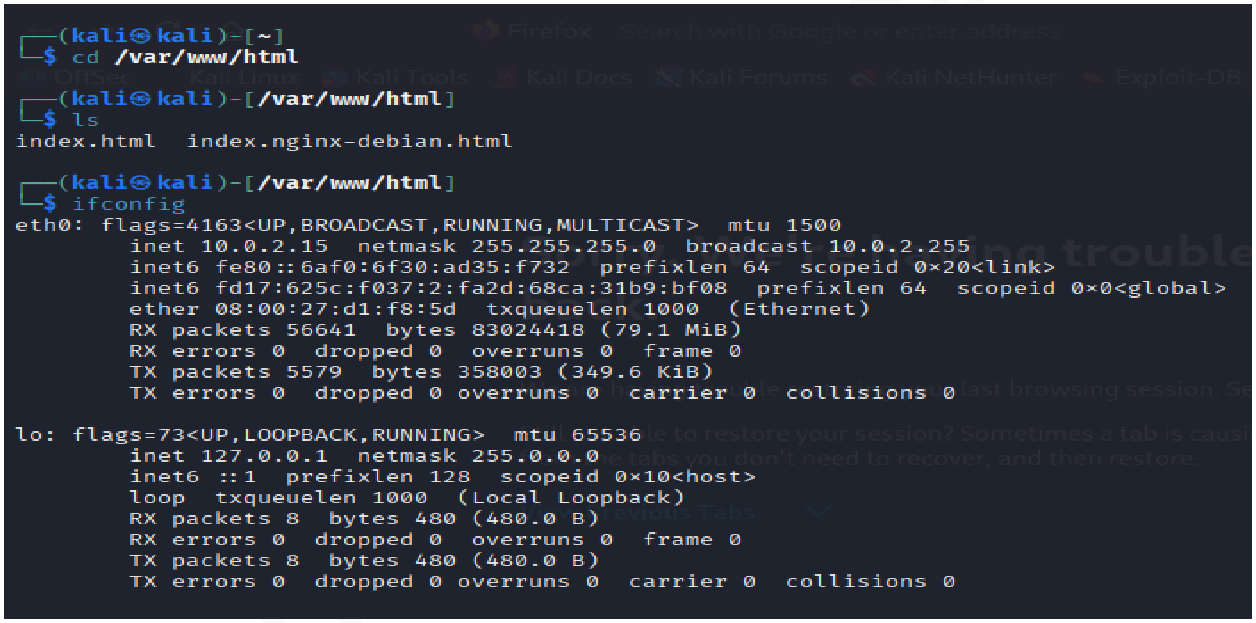
The command **“sudo systemctl start apache 2”** was used to start the Apache server, and the status turned to active (running)



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; prese
     Active: active (running) since Thu 2025-12-11 09:22:51 EST; 7s ago
 Invocation: 359ad338e5254d21852e79b2772a0b15
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 9015 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/
   Main PID: 9039 (apache2)
      Tasks: 6 (limit: 2209)
     Memory: 19.9M (peak: 20.1M)
        CPU: 434ms
     CGroup: /system.slice/apache2.service
             ├─9039 /usr/sbin/apache2 -k start
             ├─9042 /usr/sbin/apache2 -k start
             ├─9043 /usr/sbin/apache2 -k start
             ├─9044 /usr/sbin/apache2 -k start
             ├─9045 /usr/sbin/apache2 -k start
             └─9046 /usr/sbin/apache2 -k start

Dec 11 09:22:50 kali systemd[1]: Starting apache2.service - The Apache HTTP Se
Dec 11 09:22:51 kali apachectl[9030]: AH00558: apache2: Could not reliably de
Dec 11 09:22:51 kali systemd[1]: Started apache2.service - The Apache HTTP Se
lines 1-21/21 (END)
```

### Accessing Webpages on the Apache2 Server

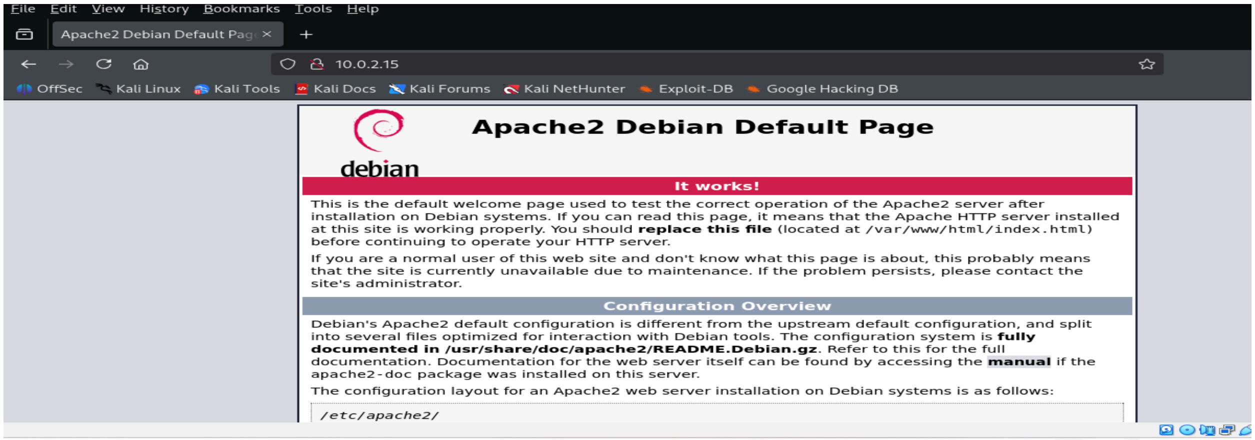
To access the default webpage on the Apache server, change to the html folder with the command **“cd /var/www/html”. You** can decide to change the files in this folder if you want to experiment with your websites. To access the website using the IP address of the system



```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html

┌──(kali㉿kali)-[/var/www/html]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::6af0:6f30:ad35:f732  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:fa2d:68ca:31b9:bf08  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
        RX packets 56641  bytes 83024418 (79.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5579  bytes 358003 (349.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

### Accessing the websites via the browser

We can access the webpages via the browser and confirm the connection to the webpage to see that it is not secure, and verification was also carried out via Wireshark, as the TCP stream is not encrypted.



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

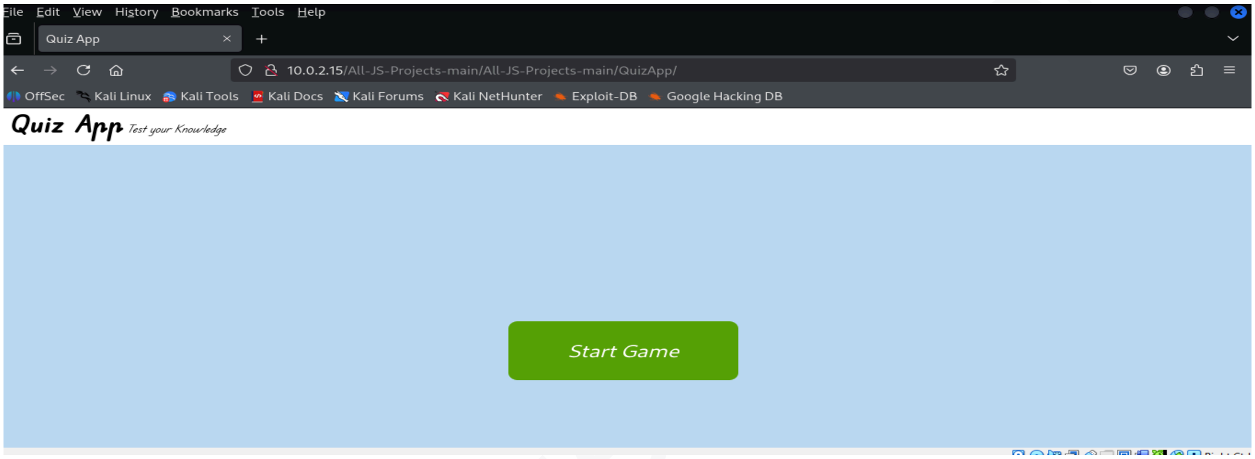
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

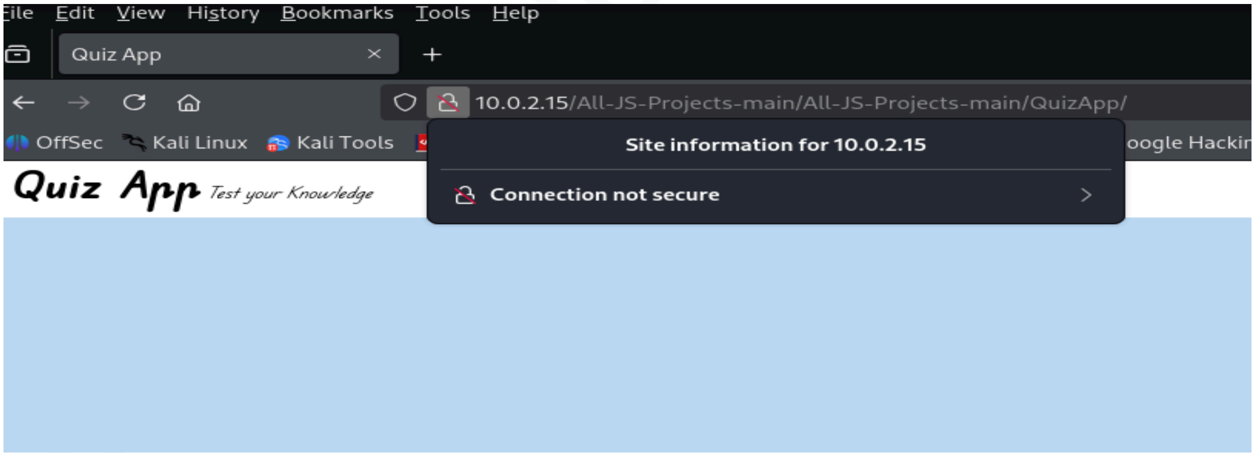
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

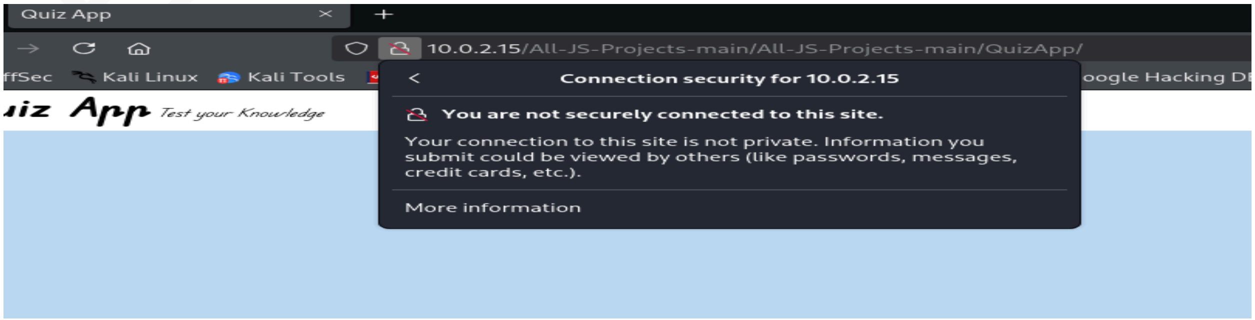
```
/etc/apache2/
```


File Edit View History Bookmarks Tools Help
Quiz App ×
10.0.2.15/All-JS-Projects-main/All-JS-Projects-main/QuizApp/
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Quiz App Test your Knowledge
Start Game


File Edit View History Bookmarks Tools Help
Quiz App ×
10.0.2.15/All-JS-Projects-main/All-JS-Projects-main/QuizApp/
OffSec
Kali Linux
Kali Tools
oogle Hackin
Quiz App Test your Knowledge

Site information for 10.0.2.15

Connection not secure

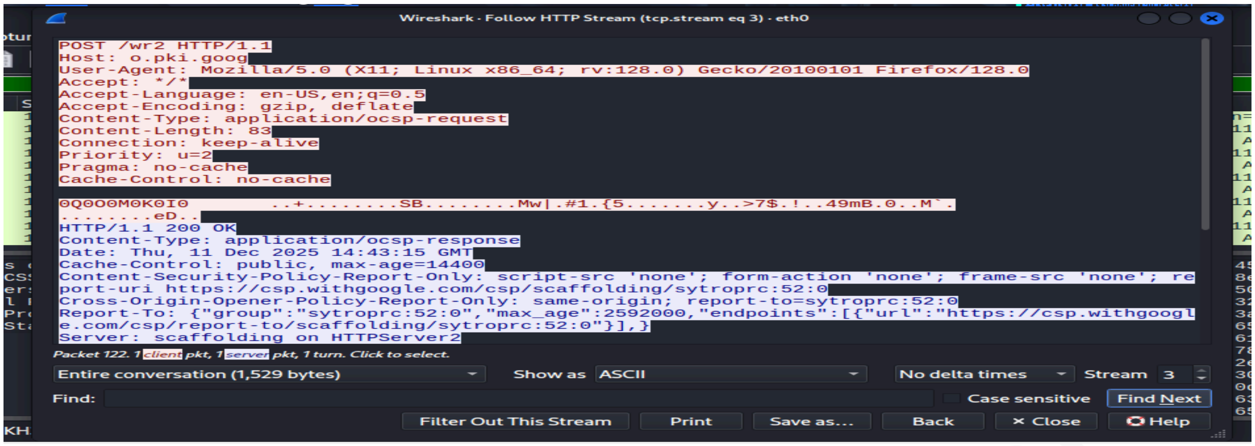

Quiz App ×
10.0.2.15/All-JS-Projects-main/All-JS-Projects-main/QuizApp/
ffSec
Kali Linux
Kali Tools
oogle Hacking D
iiz App Test your Knowledge

Connection security for 10.0.2.15

You are not securely connected to this site.

Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

More information



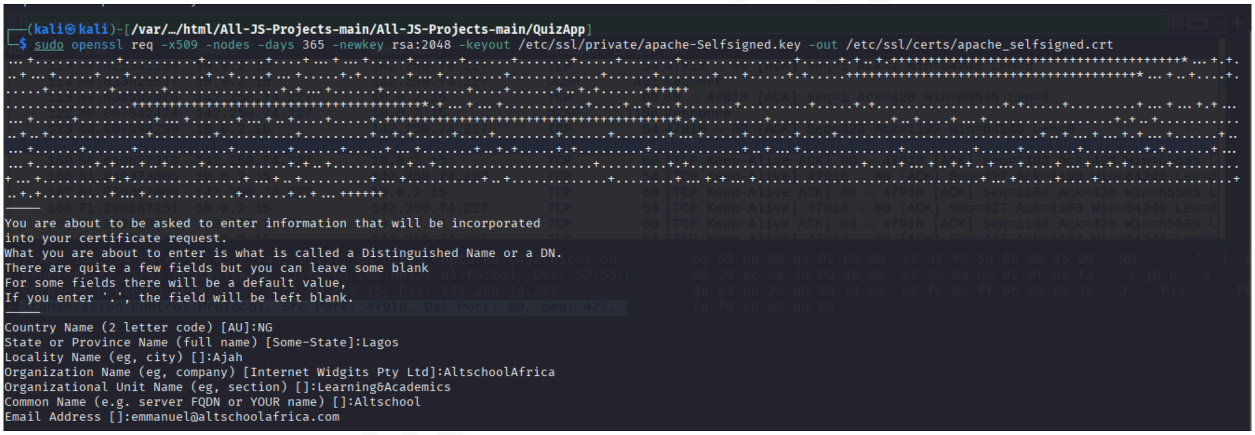
```
POST /wr2 HTTP/1.1
Host: o.pki.goog
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
Priority: u=2
Pragma: no-cache
Cache-Control: no-cache

0Q0O0M0K0I0       ..+........SB........Mw|.#1.{5.......y..>7$.!..49mB.0..M`.
........eD..
HTTP/1.1 200 OK
Content-Type: application/ocsp-response
Date: Thu, 11 Dec 2025 14:43:15 GMT
Cache-Control: public, max-age=14400
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; re
port-uri https://csp.withgoogle.com/csp/scaffolding/sytroprc:52:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=sytroprc:52:0
Report-To: {"group":"sytroprc:52:0","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogl
e.com/csp/report-to/scaffolding/sytroprc:52:0"}],}
Server: scaffolding on HTTPServer2
```

Packet 122. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,529 bytes) · Show as: ASCII · No delta times · Stream: 3

## Creation of the SSL/TLS Certificate using a self-signed Certificate

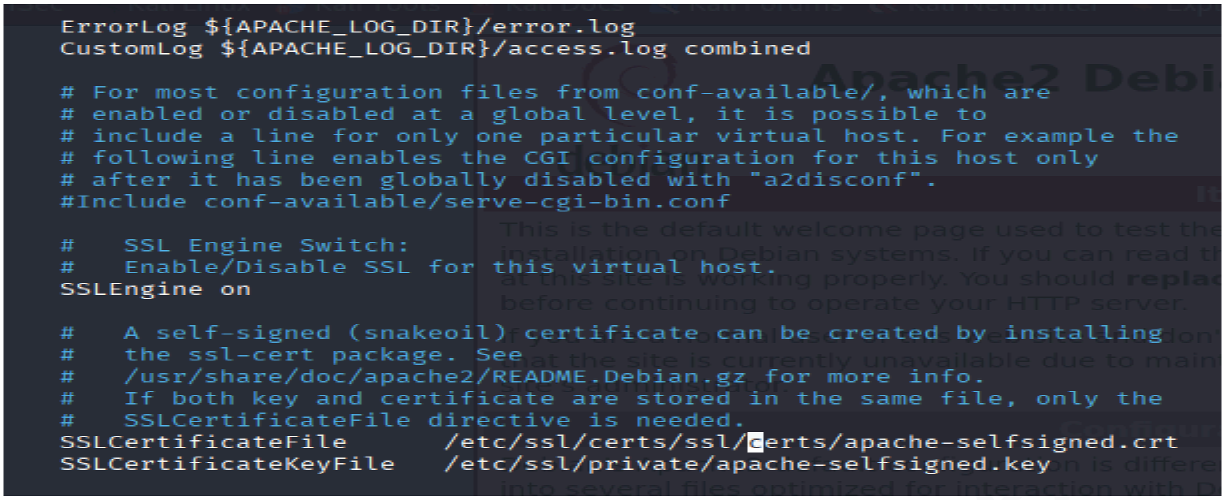
A Self-signed Certificate and a private key were created with the command **“sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache_Selfsigned.key -out /etc/ssl/certs/apache-Selfsigned.crt”**



```
┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-Selfsigned.key -out /etc/ssl/certs/apache_selfsigned.crt
...+..........+..........+.....+....+...+...+.....+......+......+.......+.....+.......+.......+..+.+++++++++++++++++++++++++++++++++++++++*...+.+.
..+...+.....+...+..........+..+.....+.+.........+.....+...+...........+.....+.+.....+++++++++++++++++++++++++++++++++++++++*...+..+...+.
.....+.........+.......+.......+..+...+.......+..........+...+......+..+.+......++++++
................+++++++++++++++++++++++++++++++++++++++*.+...+...+...........+.....+......+....+........+........+...+...+.+...
...+.....+.........+...+.....+..+....+.....+.+++++++++++++++++++++++++++++++++++++++*.+........+.....+...........+..+.......+.+.....
..+..+............+.......+..........+..........+..+.+......+.....+........+.......+........+.........+...+.+.........+...+..
...+......+......+...........+.......+......+.....+...+.......+..+.+.....+.+..........+..........+.+...
...+........+.+...+..+...+...........+.+..+...........+..+......................+............+.....+.+....
+...+.........+.+...........+...+..+.........+...+.........+..+.................+.........+.......+...+
..+.+........+...+..........+.......+..+...++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:NG
State or Province Name (full name) [Some-State]:Lagos
Locality Name (eg, city) []:Ajah
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AltschoolAfrica
Organizational Unit Name (eg, section) []:Learning&Academics
Common Name (e.g. server FQDN or YOUR name) []:Altschool
Email Address []:emmanuel@altschoolafrica.com
```

## Changing the SSL Apache Configuration File

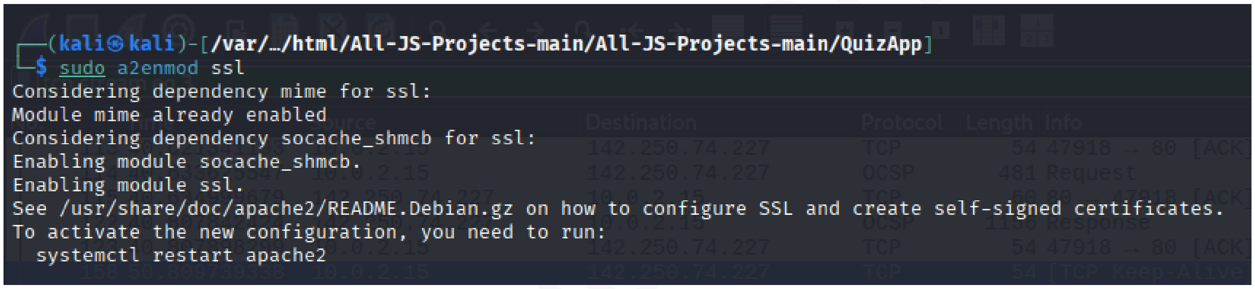
It is important to change the SSL Apache Configuration File by changing the directory of the SSL Certificate and the SSL Certificate key using the command **“sudo nano /etc/apache2/sites-available/default-ssl.conf”** and only change the part of **SSLCertificateFile and SSLCertificateKeyFile**



```
	ErrorLog ${APACHE_LOG_DIR}/error.log
	CustomLog ${APACHE_LOG_DIR}/access.log combined

	# For most configuration files from conf-available/, which are
	# enabled or disabled at a global level, it is possible to
	# include a line for only one particular virtual host. For example the
	# following line enables the CGI configuration for this host only
	# after it has been globally disabled with "a2disconf".
	#Include conf-available/serve-cgi-bin.conf

	#   SSL Engine Switch:
	#   Enable/Disable SSL for this virtual host.
	SSLEngine on

	#   A self-signed (snakeoil) certificate can be created by installing
	#   the ssl-cert package. See
	#   /usr/share/doc/apache2/README.Debian.gz for more info.
	#   If both key and certificate are stored in the same file, only the
	#   SSLCertificateFile directive is needed.
	SSLCertificateFile      /etc/ssl/certs/ssl/certs/apache-selfsigned.crt
	SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key
```

### Enabling the SSL Module

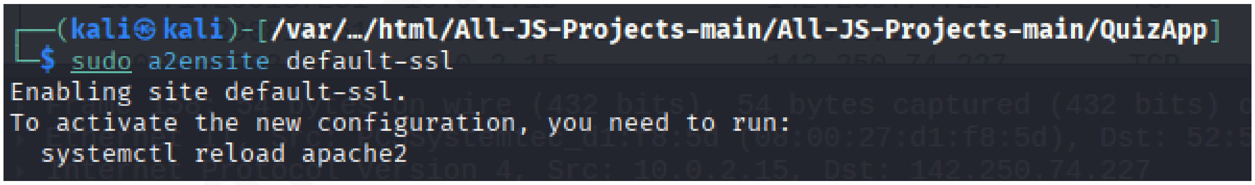
To enable the SSL module, we use the command **“sudo a2enmod ssl”**, this command activates the SSL module



```
┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

### Enabling the SSL Virtual Host

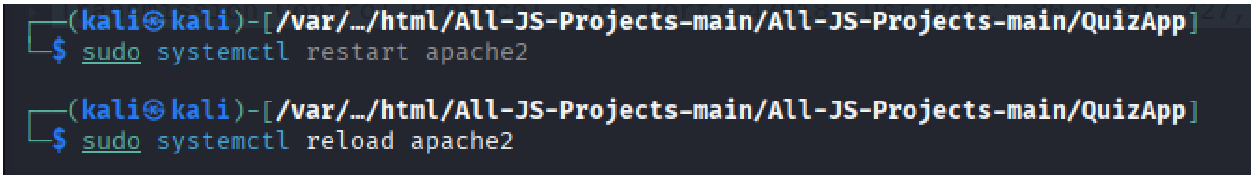
To enable the  SSL Virtual Host, we use the command **“sudo a2ensite default-ssl”,** which enables the website to take on the SSL Certificate



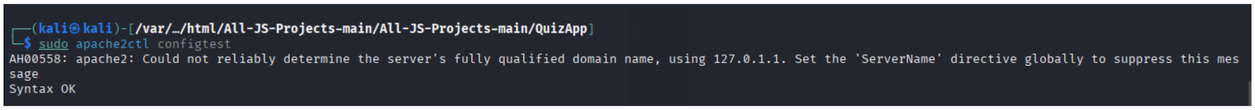
```
┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

### Restart and Reboot of the Apache Server

To restart and reboot the server with the commands **“sudo systemctl restart apache2”** and **“sudo systemctl reload apache2”,** this activates the Apache server to function effectively, and the command **“sudo apache2ctl configtest”** is used to confirm that the function works properly

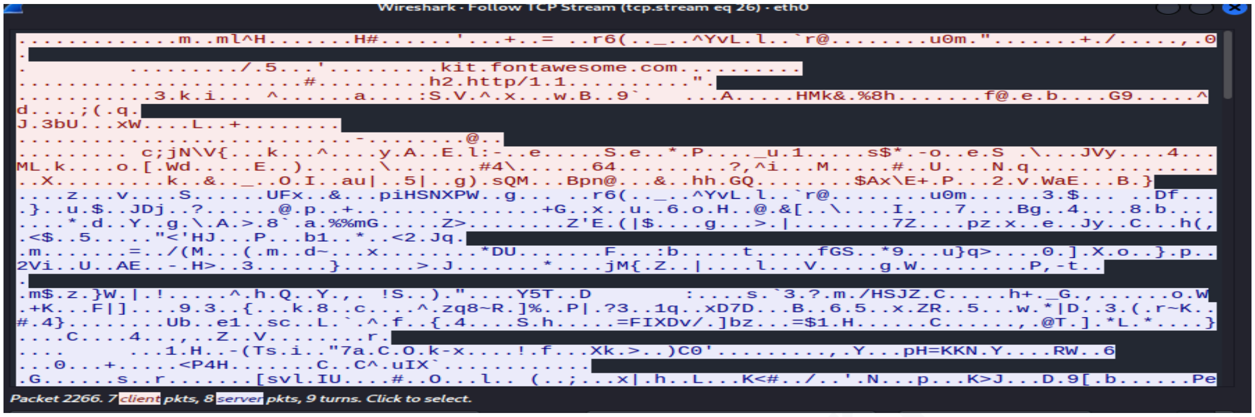


```
┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo systemctl reload apache2
```



```
┌──(kali㉿kali)-[/var/…/html/All-JS-Projects-main/All-JS-Projects-main/QuizApp]
└─$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this mes
sage
Syntax OK
```

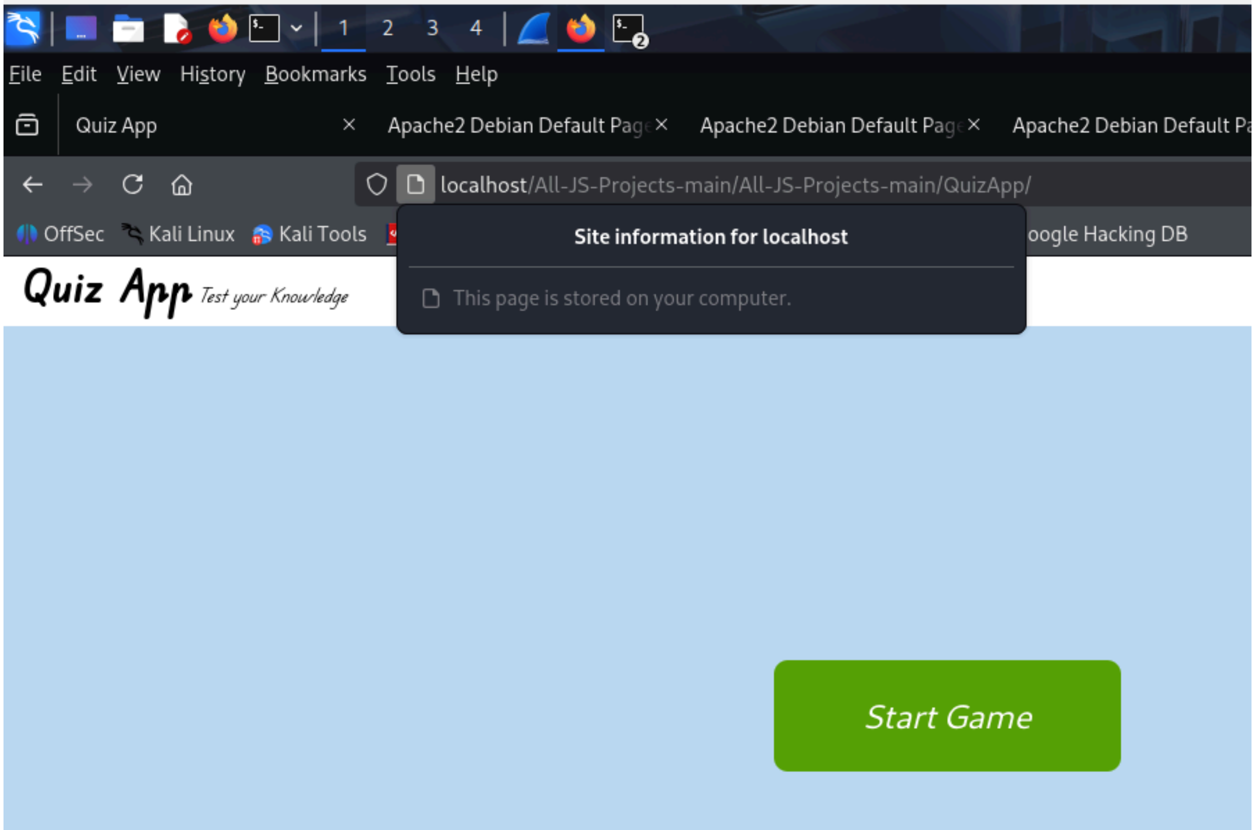
## Verfication of the Installation of the TLS Certicate and encrypted stream on wireshark



Wireshark · Follow TCP Stream (tcp.stream eq 26) · eth0

```
..............m..ml^H.......H#......'...+..= ..r6(..._...^YvL.l..`r@........u0m.".......+./.....,.0
.
.        ........./.5...'.........kit.fontawesome.com..........
.........................#.........h2.http/1.1.........".
...........3.k.i... ^......a....:S.V.^.x...w.B..9`.  ...A.....HMk&.%8h.......f@.e.b....G9.....^
d....;(.q.
J.3bU...xW....L..+........
.................................-.........@..
.........  c;jN\V{...k...^....y.A..E.l:-..e.....S.e..*.P...._u.1.....s$*.-o..e.S .\...JVy....4...
ML.k....o.[.Wd.....E..).....\.......#4\.....64.........?,^i...M.....#..U....N.q...............
..X..........k..&.._...O.I..au|..5|..g).sQM...Bpn@...&..hh.GQ........$Ax\E+.P...2.v.WaE...B.}
....z...v....S......UFx..&...piHSNXPW..g...  ..r6(..._...^YvL.l..`r@........u0m......3.$...  ..Df...
.}..u.$..JDj..?......@.p..+...................+G..x..u..6.o.H..@.&[..\....I....7....Bg..4....8.b....
....*.d..Y..g.\.A.>.8`.a.%%mG.....Z>.........Z'E.(|$....g...>.|.........7Z....pz.x..e..Jy..C...h(,
.<$..5....."<'HJ...P...b1..*..<2.Jq.
.m........=../(M...(.m..d~...x..........*DU.......F...:b.....t.....fGS..*9...u}q>....0.].X.o..}.p..
2Vi..U..AE..-.H>..3......}......>.J.......*....jM{.Z..|....l...V.....g.W.........P,-t..
.
.m$.z.}W.|.!.....^.h.Q..Y.,. !S..)."....Y5T..D          :....s.`3.?.m./HSJZ.C.....h+._G.,......o.W
.+K...F|]....9.3..{...k.8..c....^.zq8~R.]%..P|.?3..1q..xD7D...B..6.5..x.ZR..5...w.*|D..3.(.r~K..
#.4}.........Ub..e1..sc..L.`.^.f..{.4....S.h.....=FIXDv/.]bz...=$1.H......C......,.@T.].*L.*....}
....C....4...,..Z..V..........r.
....       ...1.H..-(Ts.i.."7a.C.O.k-x....!.f...Xk.>..)C0'.........,.Y...pH=KKN.Y....RW..6
...0...+.....<P4H.......C..C^.uIX`.............
.G......s..r........[svl.IU....#..O...l.. (..;...x|.h..L...K<#../..'.N...p...K>J...D.9[.b......Pe
```

Packet 2266. 7 client pkts, 8 server pkts, 9 turns. Click to select.


1
2
3
4
File
Edit
View
History
Bookmarks
Tools
Help
Quiz App
Apache2 Debian Default Pag
Apache2 Debian Default Pag
Apache2 Debian Default Pa
localhost/All-JS-Projects-main/All-JS-Projects-main/QuizApp/
OffSec
Kali Linux
Kali Tools
oogle Hacking DB
Site information for localhost
This page is stored on your computer.
Quiz App
Test your Knowledge
Start Game