



به نام خدا
دانشگاه تهران
پردیس دانشکدگان فنی
دانشکده مهندسی برق و کامپیوتر



تمرین کامپیوتری شماره 1 درس مبانی امنیت شبکه‌های کامپیوتری

نام استاد : دکتر صیادحقیقی

نام دانشجو : علی مهرانی

شماره دانشجویی : 810198542

1. راه اندازی سرور HTTP با احراز هویت کاربری

مطابق شکل زیر ابتدا اقدام به نصب وب سرور apache و همچنین apache-utils می کنیم.

```
mehrani@mehrani:~/Desktop$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
  libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 438 not upgraded.
Need to get 1,721 kB of archives.
After this operation, 7,532 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ir.archive.ubuntu.com/ubuntu focal/main amd64 libapr1 amd64 1.6.5-1ubu
```

شکل شماره 1- نصب apache

Apache-utils نیز همراه با آن نصب می شود

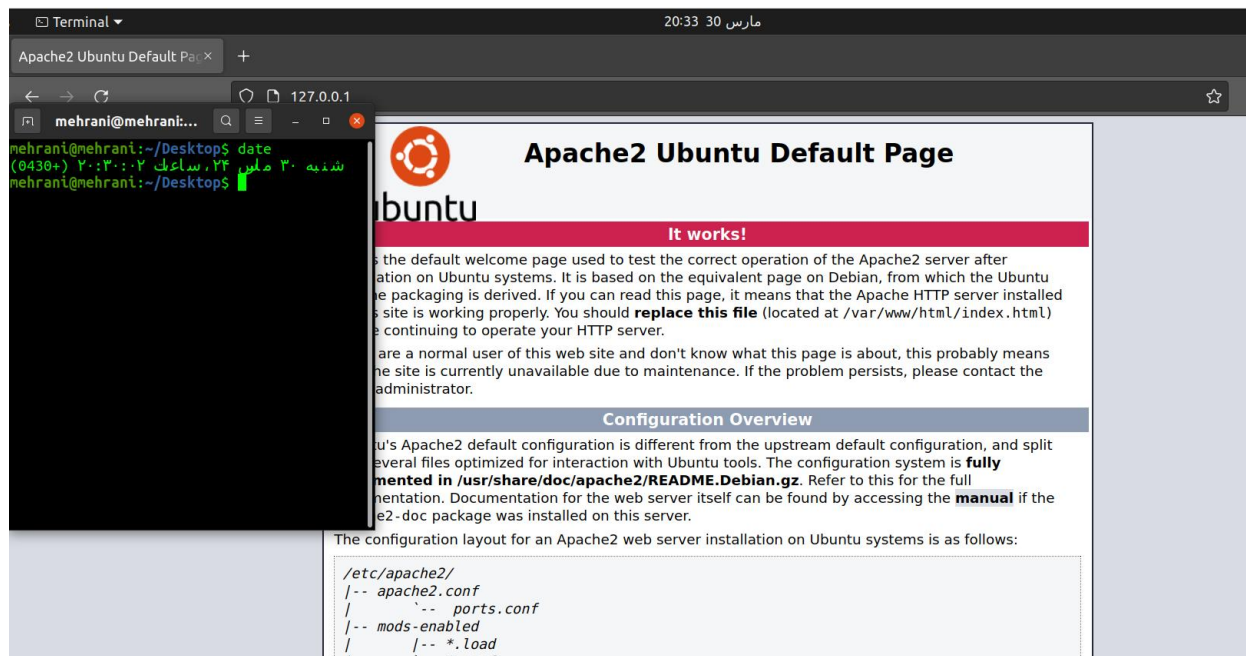
```
Terminal 20:43 30 مارس
mehrani@mehrani: ~/Desktop

mehrani@mehrani:~/Desktop$ sudo apt install apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2-utils is already the newest version (2.4.41-4ubuntu3.16).
apache2-utils set to manually installed.
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0 libva-wayland2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 438 not upgraded.
mehrani@mehrani:~/Desktop$

mehrani@mehrani:~$ date
شنبه ۳۰ مارس ۱۴۰۲، ساعت ۲۰:۴۳:۴۲ (+0430)
mehrani@mehrani:~$
```

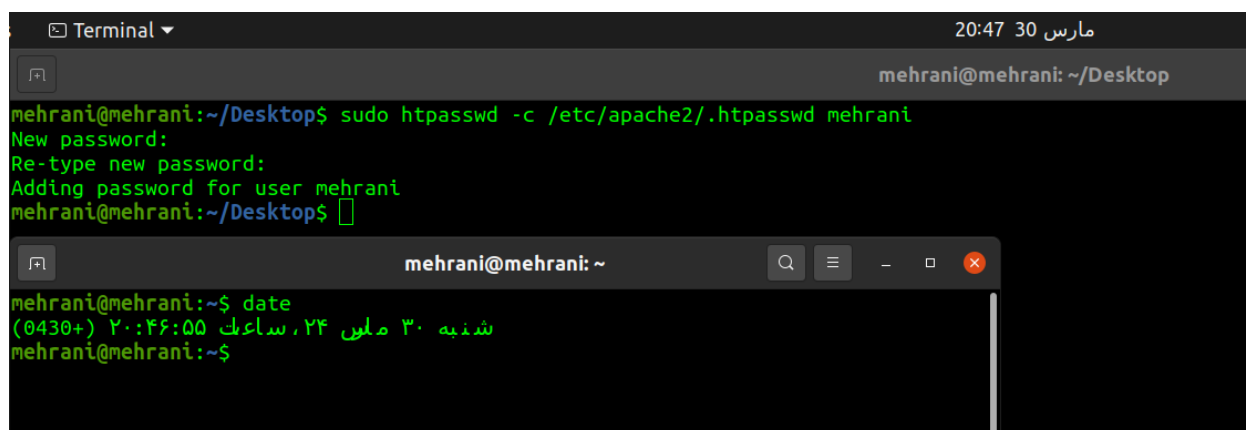
شکل 2- نصب apache-utils

پس از نصب apache آن را بر روی مرورگر مشاهده می‌کنیم.



شکل 3- صفحه اصلی apache در localhost

در ادامه مطابق موارد ذکر شده فرایند احراز هویت کاربری برای صفحه موجود در آدرس 127.0.0.1 را اجرا می‌کنیم. ابتدا احراز هویت htpasswd را انجام می‌دهیم.



شکل 5- ایجاد رمز در htpasswd

همانگونه که در شکل زیر نیز مشخص است، در این فایل اطلاعات user ها به همراه hash رمزشان قرار گرفته است.

```
Terminal 20:51 30 مارس
mehrani@mehrani: ~/Desktop
mehrani@mehrani:~/Desktop$ cat /etc/apache2/.htpasswd
mehrani:$apr1$IbD5v/Os$WDBwK2fPXC09cqYZ.LdU1
mehrani@mehrani:~/Desktop$
```

شکل 6- محتوای htpasswd

حال در تنظیمات apache برای آن مشخص می‌کنیم که دسترسی به محتواهای درون آدرس /var/www/html نیاز به احراز هویت کاربر دارد. شکل زیر این تنظیمات را نمایش می‌دهد.

```
GNU nano 4.8 000-default.conf
VirtualHost *:80
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

<Directory "/var/www/html">
    AuthType Basic
    AuthName "Restricted Content"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
</Directory>

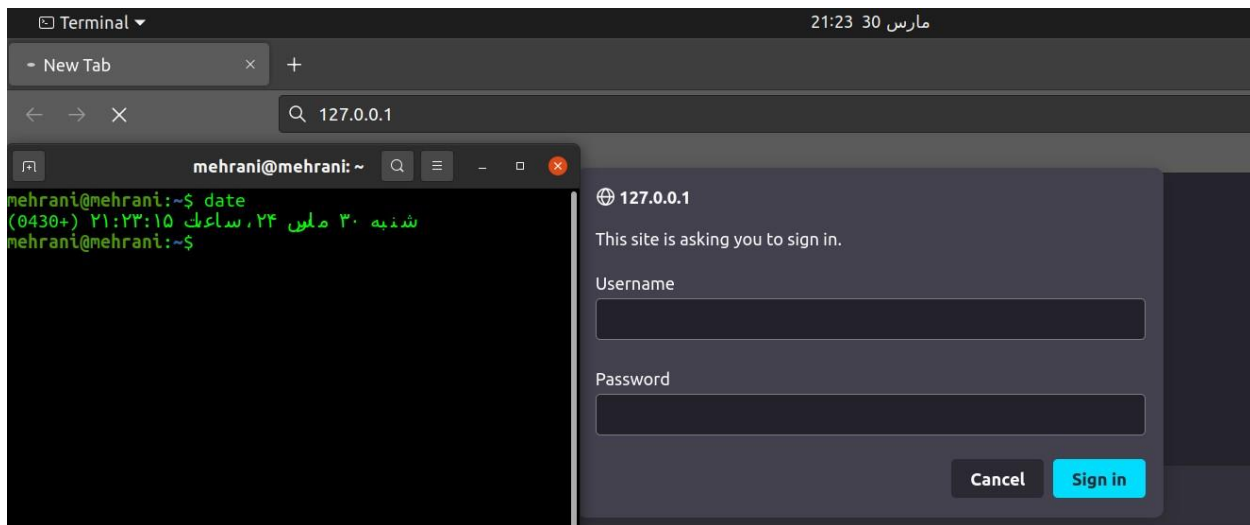
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

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
</VirtualHost>
```

شکل 7- تنظیمات apache

پس از انجام این کار و reload کردن apache مطابق شکل زیر مشاهده میکنیم که دسترسی به صفحه 127.0.0.1 یا همان localhost نیاز به احراز هویت کاربر دارد.



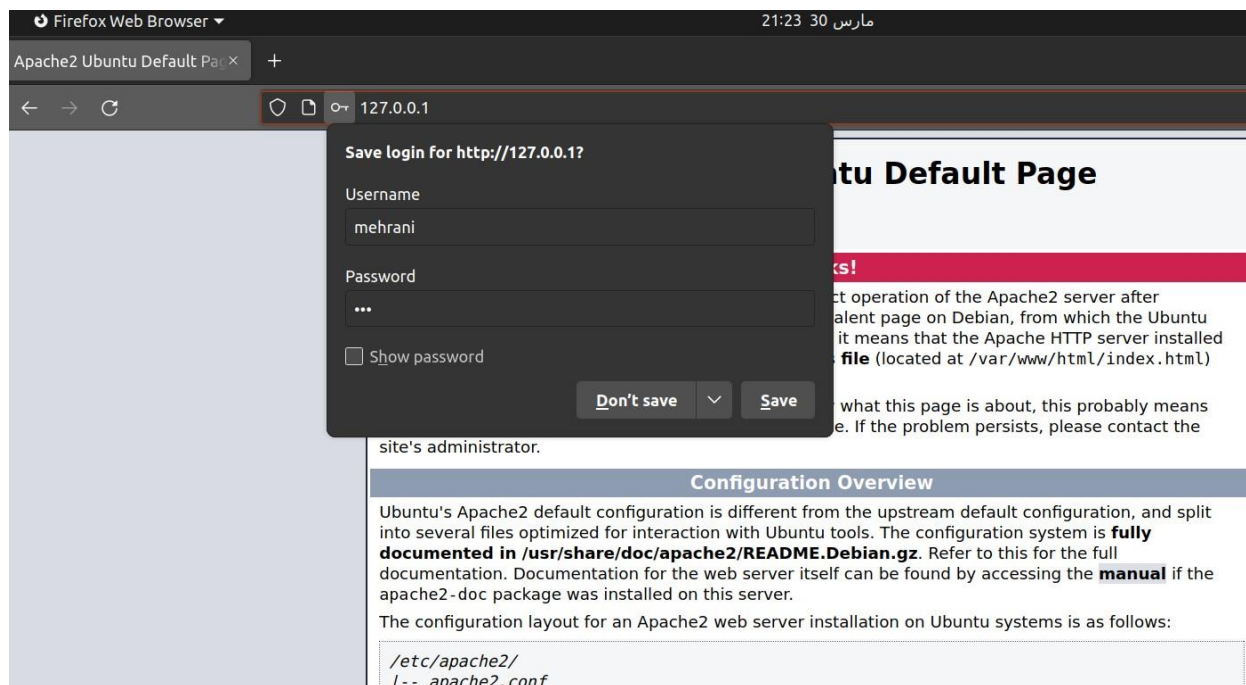
شکل 8- احراز هویت کاربری در صفحه localhost

در صورت اشتباه وارد کردن یا وارد نکردن اطلاعات، خطای unauthorized نمایش داده می‌شود.



شکل 9- نمایش خطای unauthorized

در صورت درست وارد شدن اطلاعات و احراز هویت موفق، صفحه پیش فرض به کاربر نمایش داده می‌شود.



شکل 10- نمایش صفحه پیش فرض پس از احراز هویت موفق

در ادامه به استفاده از ابزار Wireshark به جهت ضبط بسته‌های رد و بدل شده در حین دسترسی و تأمین اطلاعات احراز هویت کاربری روی آدرس 127.0.01 می‌پردازیم.

ابتدا آن را بر روی سیستم نصب می‌کنیم.


```

mehrani@mehrani:~/Desktop$ sudo add-apt-repository ppa:wireshark-dev/stable
Latest stable Wireshark releases back-ported from Debian package versions.

Back-porting script is available at https://github.com/rbalint/pkg-wireshark-ubuntu-ppa

From Ubuntu 16.04 you also need to enable "universe" repository, see:
http://askubuntu.com/questions/148638/how-do-i-enable-the-universe-repository

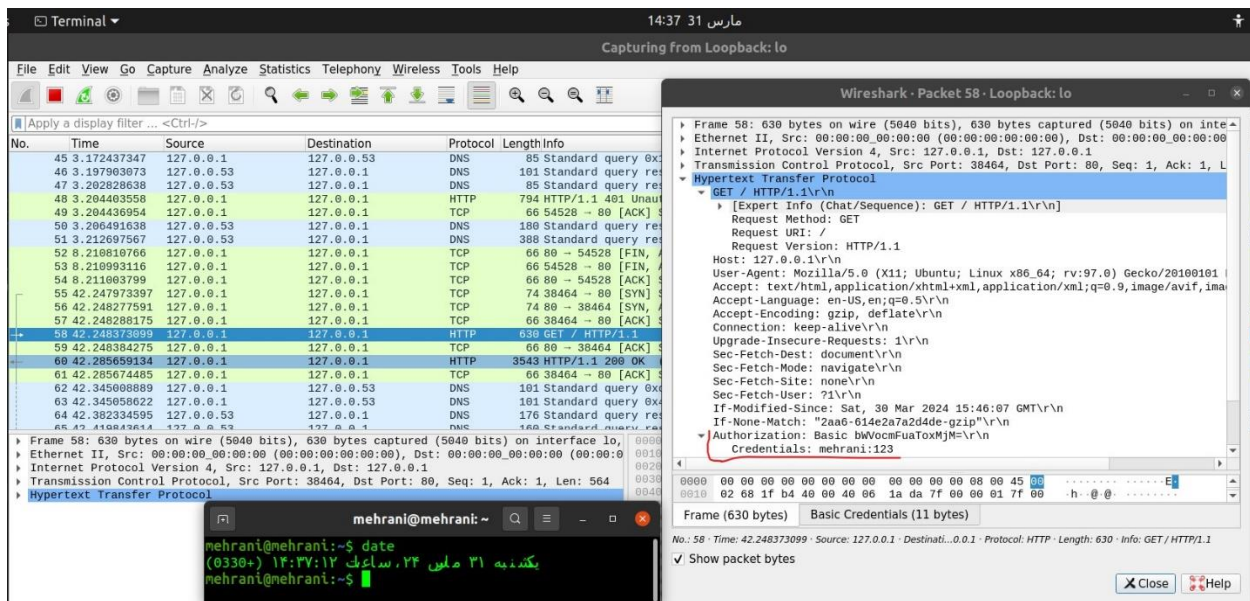
The packaging repository for Debian and Ubuntu is at: https://salsa.debian.org/debian/wireshark
More info: https://launchpad.net/~wireshark-dev/+archive/ubuntu/stable
Press [ENTER] to continue or Ctrl-c to cancel adding it.

Hit:1 http://ir.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://ir.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://ir.archive.ubuntu.com/ubuntu focal-backports InRelease
Get:4 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease [24.4 kB]
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:6 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main i386 Packages [1,596 B]
Get:7 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main amd64 Packages [5,484 B]
Get:8 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main Translation-en [2,200 B]
Fetched 33.6 kB in 1s (31.3 kB/s)
Reading package lists... Done
mehrani@mehrani:~/Desktop$ sudo apt update
Hit:1 http://ir.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://ir.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://ir.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
438 packages can be upgraded. Run 'apt list --upgradable' to see them.
mehrani@mehrani:~/Desktop$ sudo apt-get update
Hit:1 http://ir.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://ir.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://ir.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
mehrani@mehrani:~/Desktop$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:

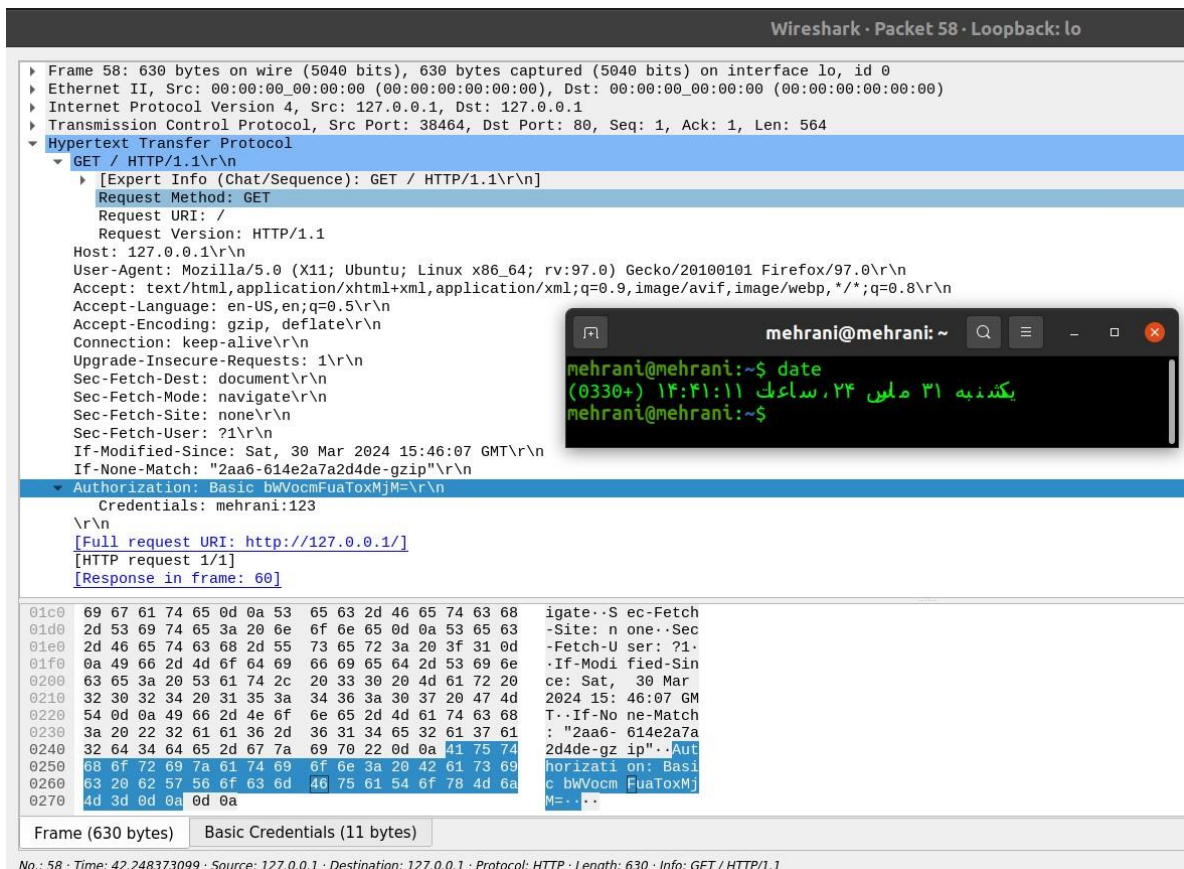
```

شکل 11- نصب wireshark

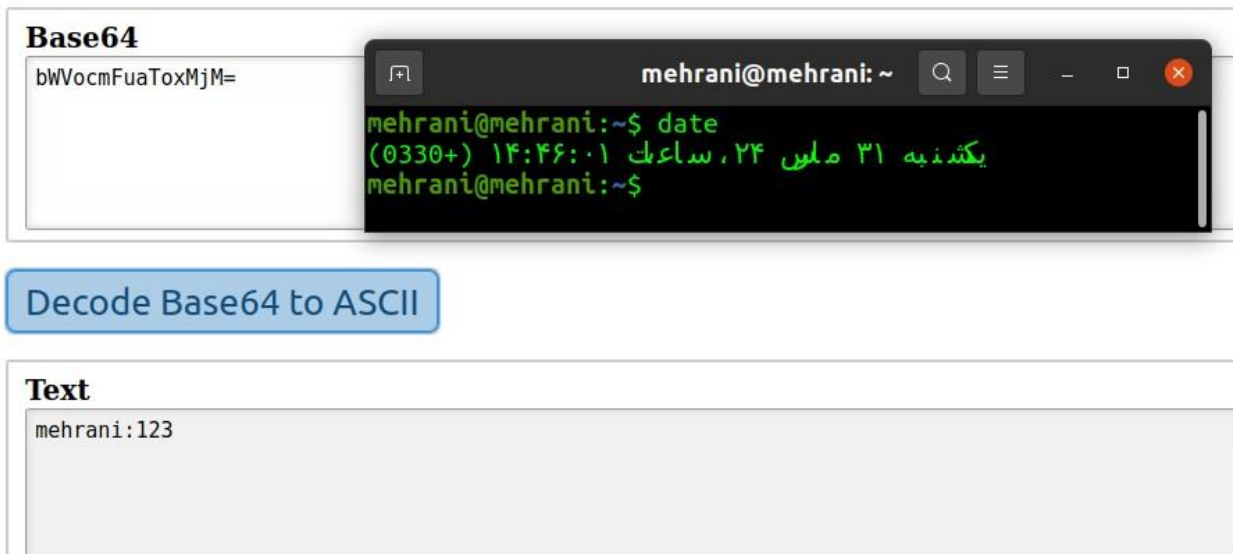
پس از نصب wireshark و انجام فرآیند احراز هویت، اقدام به capture کردن بسته‌های رد و بدل شده می‌کنیم. شکل زیر packet مربوط به فرآیند احراز هویت را نمایش می‌دهد و همانطور که در شکل نیز مشاهده می‌شود، نام کاربری و رمز عبور به صورت radix64 قابل مشاهده هستند که البته خود wireshark آن‌ها را به فرم ASCII نیز نمایش می‌دهد.



شکل ۱۲- دریافت اطلاعات packet در wireshark



شکل ۱۳- جزئیات packet فرآیند Authorization در wireshark



شکل ۱۴- تبدیل radix64 به ASCII

مطابق با تصاویر بالا، مشاهده می‌شود که نام کاربری برابر با mehrani و رمز عبور نیز برابر با 123 می‌باشد.

قابلیت decode کردن packet های ارسال شده به دلیل عدم رمزنگاری به راحتی امکان پذیر خواهد بود و برای شنود کفایت تنها فردی در میانه راه ارسال شدن اطلاعات، packet مربوط به (ارسال اطلاعات) احراز هویت یا همان Authorization را پیدا و decode کند.

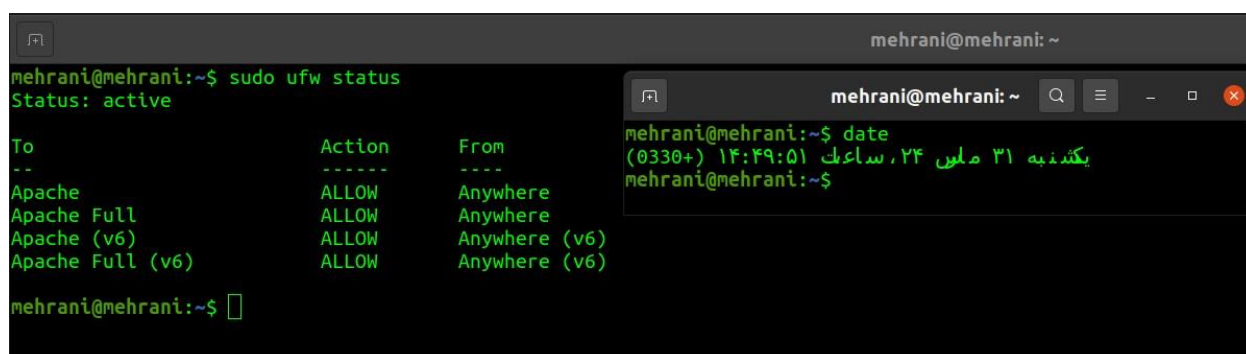
در یک http request ارسال اطلاعات در قالب plain text و رمز نشده صورت می‌گیرد و فرد با monitor کردن شبکه و بررسی آن می‌تواند اطلاعات احراز هویت را در بخش header آن HTTP Request مشاهده کند و ما نیز در این بخش این اطلاعات را در همین قسمت header در request مربوطه مشاهده کردیم.

در ادامه سرور HTTPS را راه اندازی می‌کنیم.

2. راه اندازی سرور HTTPS با احراز هویت کاربری

در ادامه برای ساخت سرور HTTPS تنظیمات apache را تغییر می دهیم.

تصاویر زیر فرآیند تنظیم کردن apache را نمایش می دهند.

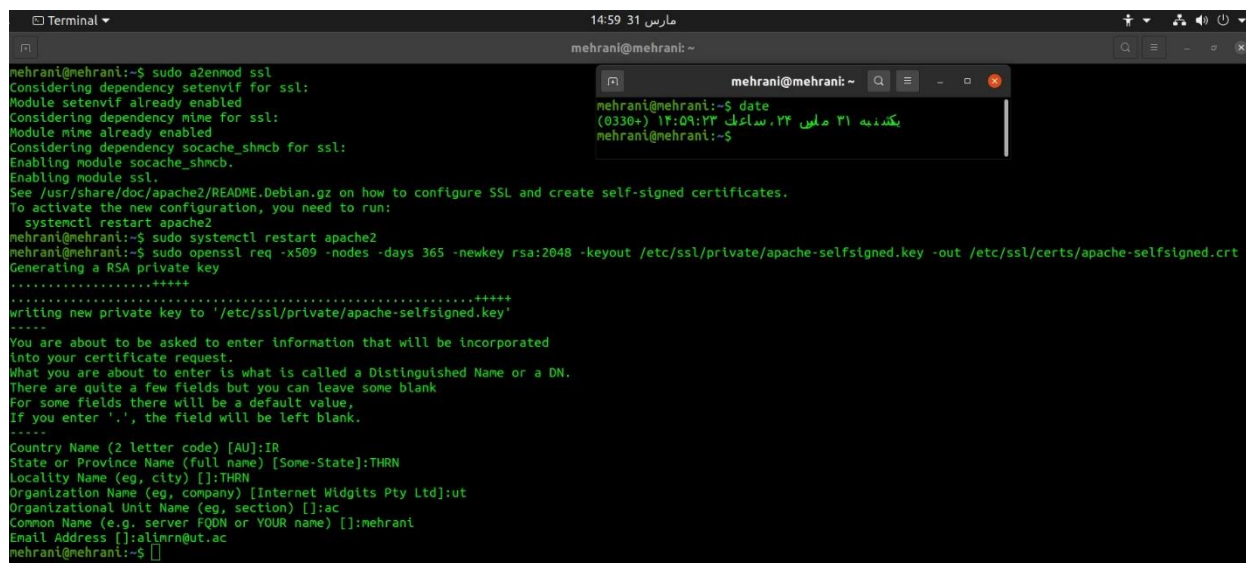


```
mehrani@mehrani:~$ sudo ufw status
Status: active

To Action From
--
Apache ALLOW Anywhere
Apache Full ALLOW Anywhere
Apache (v6) ALLOW Anywhere (v6)
Apache Full (v6) ALLOW Anywhere (v6)

mehrani@mehrani:~$
```

شکل 15- تنظیم apache



```
mehrani@mehrani:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
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
mehrani@mehrani:~$ sudo systemctl restart apache2
mehrani@mehrani:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
Generating a RSA private key
.....+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
+++++
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]:IR
State or Province Name (full name) [Some-State]:THRN
Locality Name (eg, city) []:THRN
Organization Name (eg, company) [Internet Wldgits Pty Ltd]:ut
Organizational Unit Name (eg, section) []:ac
Common Name (e.g. server FQDN or YOUR name) []:mehrani
Email Address []:alimn@ut.ac
mehrani@mehrani:~$
```

شکل 16- تنظیم apache

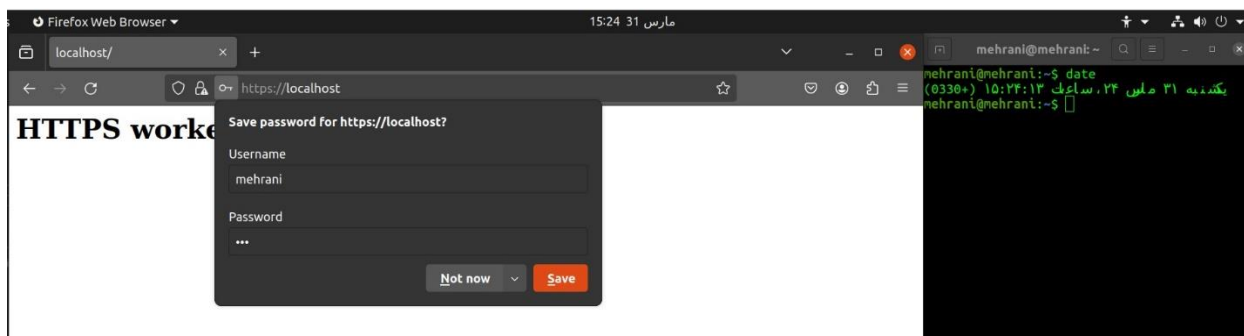
```
Terminal 15:13 31 مارس mehrani@mehrani: ~  
GNU nano 4.2.8 /etc/apache2/sites-available/mehrani.conf Modified  
<VirtualHost *:443>  
    ServerName mehrani  
    DocumentRoot /var/www/mehrani  
  
    SSLEngine on  
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  
  
    <Directory "/var/www/mehrani">  
        AuthType Basic  
        AuthName "Restricted Content"  
        AuthUserFile /etc/apache2/.htpasswd  
        Require valid-user  
    </Directory>  
</VirtualHost>
```

شکل 17- تنظیم apache

```
Terminal 15:21 31 مارس mehrani@mehrani: ~  
mehrani@mehrani:~$ sudo nano /var/www/mehrani/index.html  
mehrani@mehrani:~$ sudo a2ensite mehrani.conf  
Enabling site mehrani.  
To activate the new configuration, you need to run:  
    systemctl reload apache2  
mehrani@mehrani:~$ 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 message  
Syntax OK  
mehrani@mehrani:~$ sudo systemctl reload apache2  
mehrani@mehrani:~$
```

شکل 18- تنظیم apache

پس از انجام تنظیمات ذکر شده، مشاهده می‌شود که سرور apache بر روی https پس از احراز هویت موفق، فعال می‌شود.



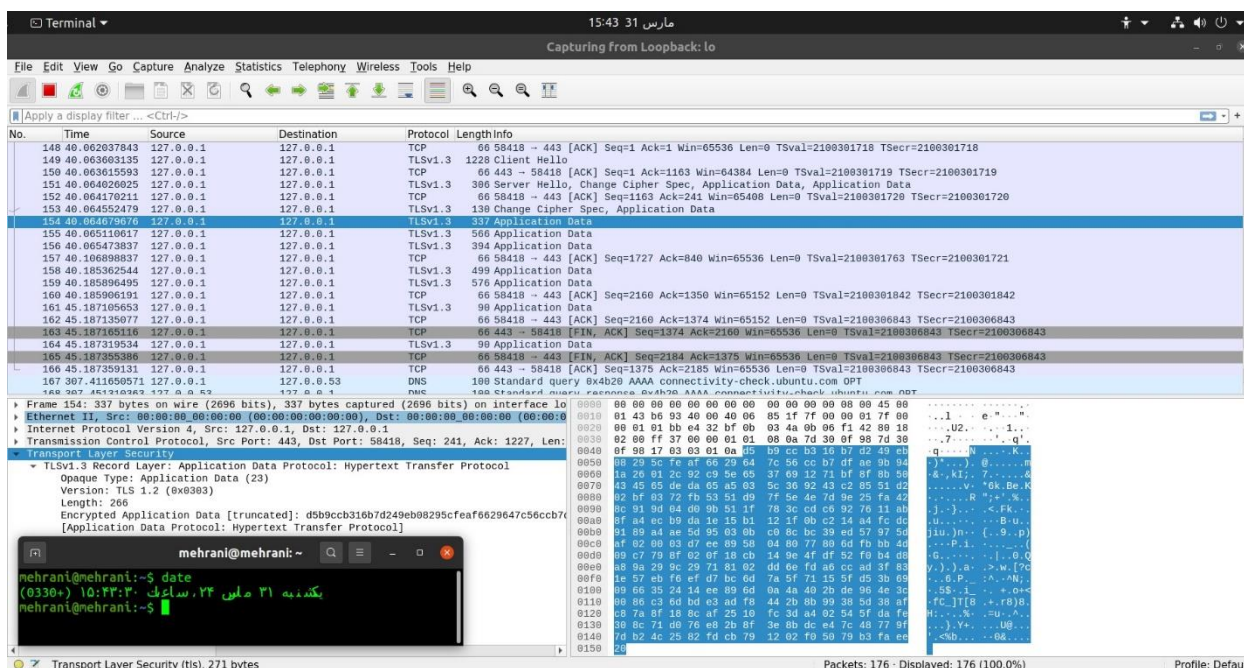
شکل 19- فعالسازی سرور https

در ادامه پس از احراز هویت موفق، اقدام به بررسی packet ها در wireshark می‌کنیم.

همانگونه که در شکل زیر نیز مشاهده می‌شود، اطلاعات packet قابل خواندن نیست و رمزگذاری شده است و فقط اطلاعات encrypt شده در دسترس می‌باشد.

اطلاعات قسمت header در http نیز قابل مشاهده نیست که این عمل به دلیل رمزنگاری با کلیدهای ساخته شده، صورت گرفته و packet ها encrypt شده اند.

امکان شنود اطلاعات احراز هویت وجود ندارد زیرا packet های ارسال شده تماماً توسط یک الگوریتم رمزنگاری با یک key مشخص، encode شده اند و فقط در صورتی که کلید را داشته باشیم می‌توانیم آن اطلاعات را رمزگشایی و decode کنیم.

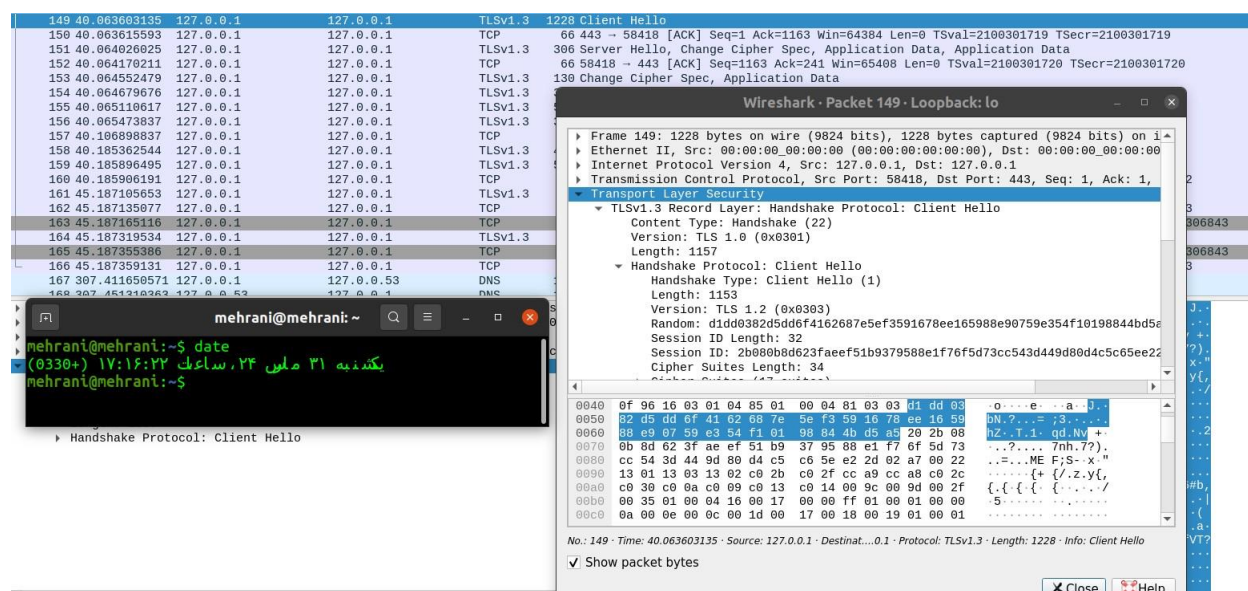


شکل 20- TLS و پکت encrypt شده

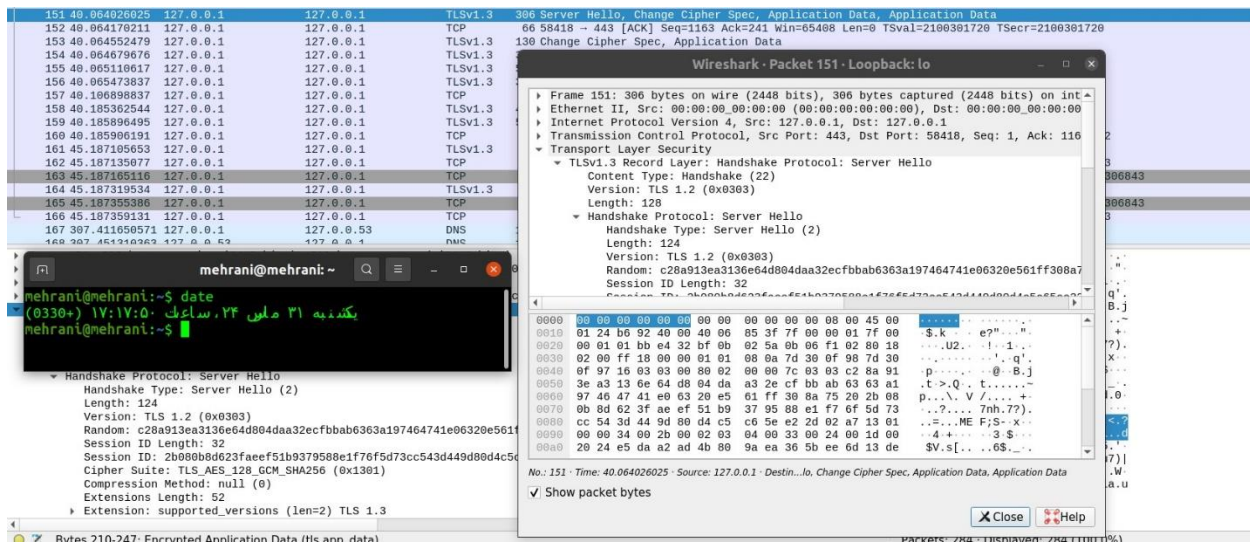
در ادامه به قسمت handshaking می‌پردازیم

مطابق با تصاویر زیر، ابتدا client hello در handshake انجام شده است (تصویر 21) و پس از آن در ادامه server_hello و همچنین change cipher spec به جهت تبادل کلید توسط سرور صورت گرفته است (تصویر 22). پس از آن نیز change cipher spec توسط client صورت گرفته (تصویر 23) و در ادامه تبادل اطلاعات صورت می‌گیرد.

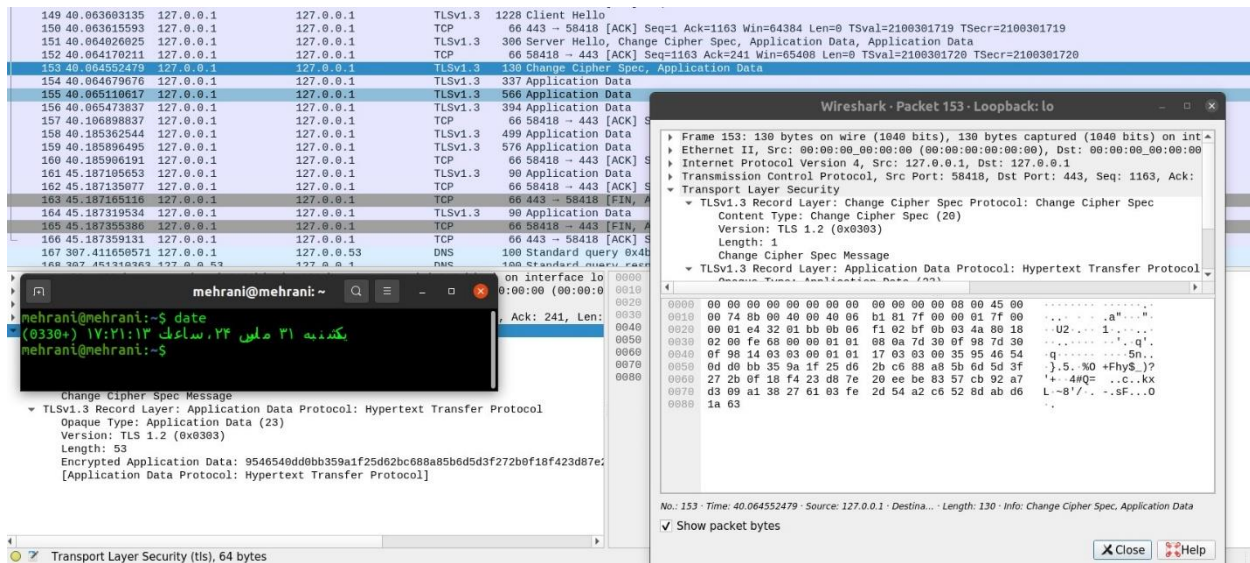
مطابق با موارد ذکر شده، تمامی مراحل اجباری در handshaking صورت گرفته است. البته مراحل اختیاری صورت نگرفته اند.



شکل 21- client hello



server hello -22 شکل



change cipher spec -23 شکل