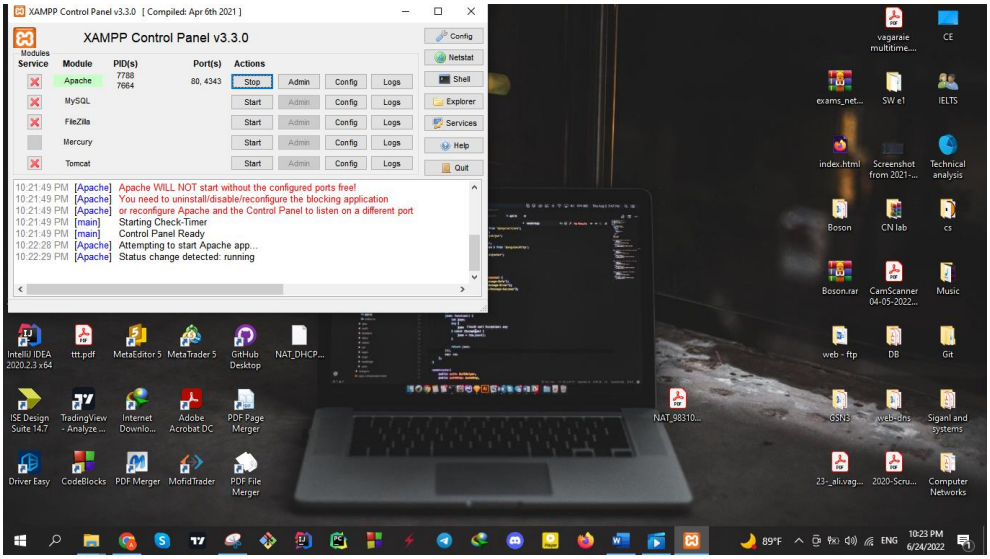
به نام خدا

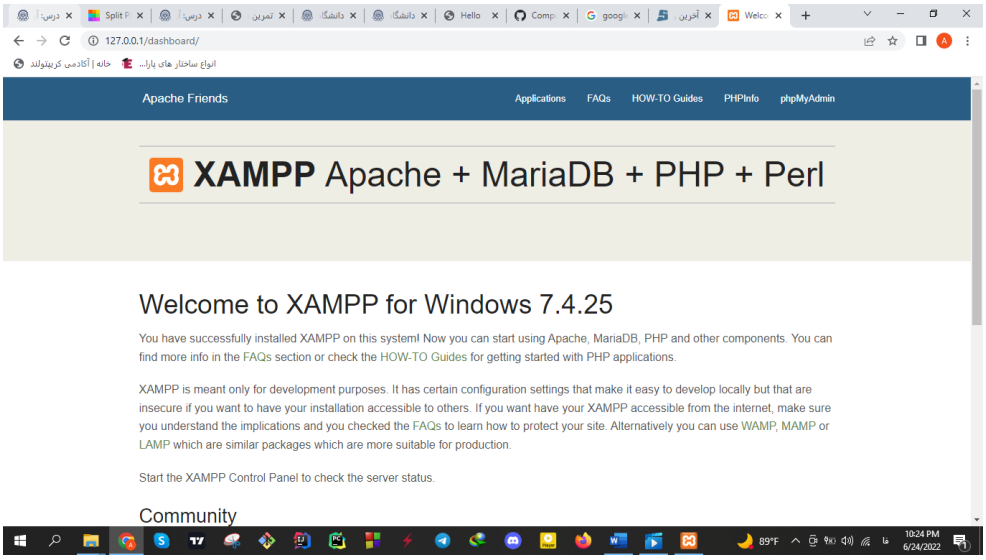
گزارش آزمایش web ftp

امیرحسین سرآهنگ 9831085

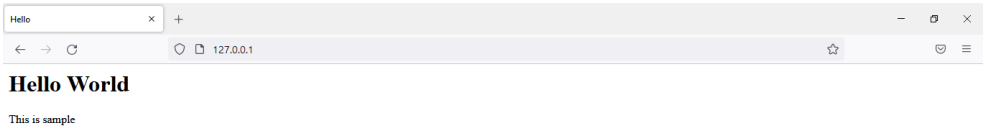
راه اندازی xampp با start کردن apache و رفع ایرادات



بالا آمدن 127.0.0.1 در مرورگر :



همون صفحه بعد از اضافه کردن فایل html :



بعد از تعریف کردن دامنه ها روی host میتوان نام دامنه را روس سایت دید

بعد از زدن آدرس صفحه ساخته شده و بررسی آن در wireshark ، بر روی یکی از بسته کلیک و follow http steam را انتخاب می کنیم :

```
GET / HTTP/1.1
Host: www.mahdirahmani.ir
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "83-5c23837adbc08"
If-Modified-Since: Thu, 13 May 2021 15:59:51 GMT

HTTP/1.1 304 Not Modified
Date: Thu, 13 May 2021 18:49:15 GMT
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/8.0.6
Last-Modified: Thu, 13 May 2021 15:59:51 GMT
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

سوال اول :

بدیهی هست که سیستم خودمون هم سرور و هم host است و دلیل برابر بودن آدرس source و destinarion به همین دلیل هست و آدرس برار با آدرس اولیمون : 127.0.0.1 است

پورت مبدا که 80 هست و طبیعیتا می دانیم که http روی چورت 80 گوش میدهد

میدانیم که http از tcp برای انتقال استفاده می کند پس در اولین گام کلاینت یک tcp connection برقرار می کند و پس از آن است که درخواست های http به سوکتش ارسال میشود و همان طور که در خود درس خواندیم این رابطه می تواند persistent یا non persistent باشد

اگر ارتباط persistent باشد برای ارسال تمامی اشیا درخواست شده تنها یک بار بین سرور و کلاینت ارتباط TCPبرقرار شده و در نهایت ارتباط بسته میشود . اما اگر non-persistent باشد ، برای ارسال هر ش به برقراری یک ارتباط جدید نیاز داریم چرا که د ر این نوع از ارتباط سرور بعد از هر بار ارسال ،

connection را میبندد و برای ش جدید به connection جدید نیاز است!

سوال دوم :

بخش کانکشن keep alive یا همان persistent است

همچنین درخواست از نوع http می باشد

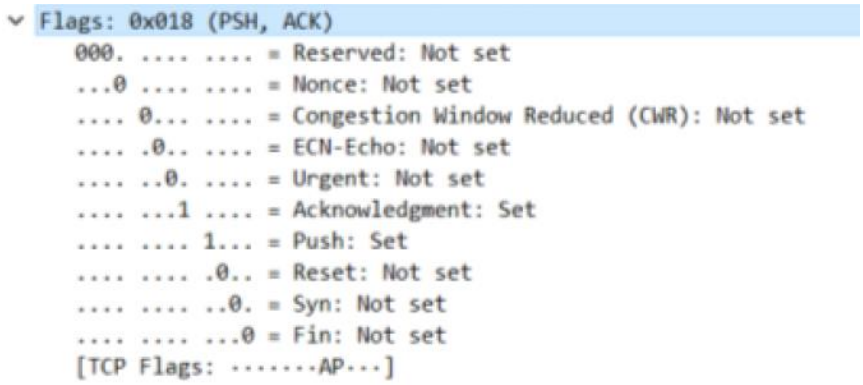
User agent : مرورگری که درخواست داده

هدر درخواست User-Agent یک رشته مشخصه است که به سرورها اجازه می دهد تا

application ، سیستم عامل و ورژن درخواست کننده را شناسایی کنند

سوال سوم :

در اولین بسته ack و psh در لایه transport درج شده



ACK همان تاییدیه بسته های موفقیت آمییز هست

PSH ، در صورت 1 بودن دیگه منتظر نمی شود به اندازه یک SEGMENT برسد و بلافاصله ارسال می کند

SYN : فقط برای بسته اول توسط فرستنده و گیرنده ست می شود و برای ترتیب توالی بسته ها که در درس هم بهش اشاره شد استفاده می شود !

سوال چهارم :

پس از انجام همه بخش ها برای سایت جدید ، مشاهده شد که پورت clinet پورتی متفاوت از قبلی است و با شنود بسته ها تفاوت در header line هارا متوجه شدیم

سوال پنجم :

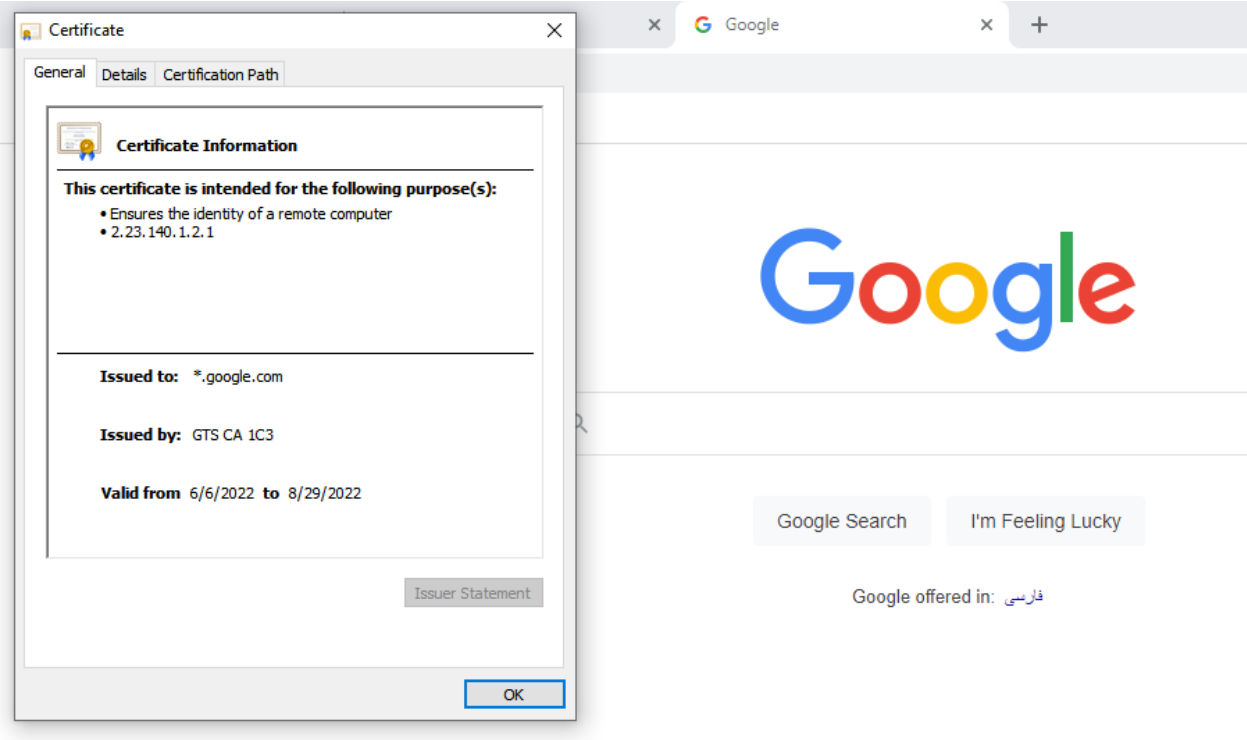
گواهی ر ا localhost برای localhost صادر کرده و زمان اعتبار نشان داده شده ، کلید عمومی الگوریتم RSA با key size = 1024 است .

امضای دیجیتال از الگوریتم SHA-1 with RSA Encryption استفاده میکندپ

سوال ششم :

متن ارتباط دیده نمیشود چرا که گواهی آن اعتبار ندارد و wireshark نتوانسته است اطالعات session را را decrypt کند

سوال هفتم :



این گواهی یک گواهی بسیار معتبر است و از GTS CA IC3 به Google اهدا شده است

تعداد فیلد بیشتر

Common name غیر یکسان بر خلاف گواهی ما

مدت زمان اعتبار کمتر و بروز تر

سوال هشتم :

نام کاربری با user درخواست میشه

از دستور list برای لیست کردن فایل های دایرکتوری استفاده شده

نام کاربری که تنظیم کردیم : test با رمز 123

پروتوکل لایه حمل که tcp است

پورت مقصد 21 و مبدا 8629

سوال نهم :

خیر زیرا در بخش نهم تنظیمات مربوط به ssl را فعال کردیم

سوال دهم :

پاسخ نه است چون user و pass قابل خواندن نیست

Html :

ارتباط keep alive است ، نوع درخواست get است همچنین user agent، bold شده

```
GET / HTTP/1.1
Host: aut.ac.ir
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36 Edg/90.0.818.62
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
Cookie: _ga=GA1.3.1799390975.1609054157

HTTP/1.1 301 Moved Permanently
Date: Mon, 17 May 2021 14:52:37 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
```

اطلاعاتی را درباره ی برنامه و همچنین نوع سیستم عاملی که درخواست را به سمت سرور ارسال کرده است و مسئولپ دریافت و نمایش محتوای http است را در اختیار ما قرار میدهد

```
▾ Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
```

FTP :

پورت مبدا 21

مقصد 51513

همچنین username، anonymous است وpass ، chrome.example.com می باشد