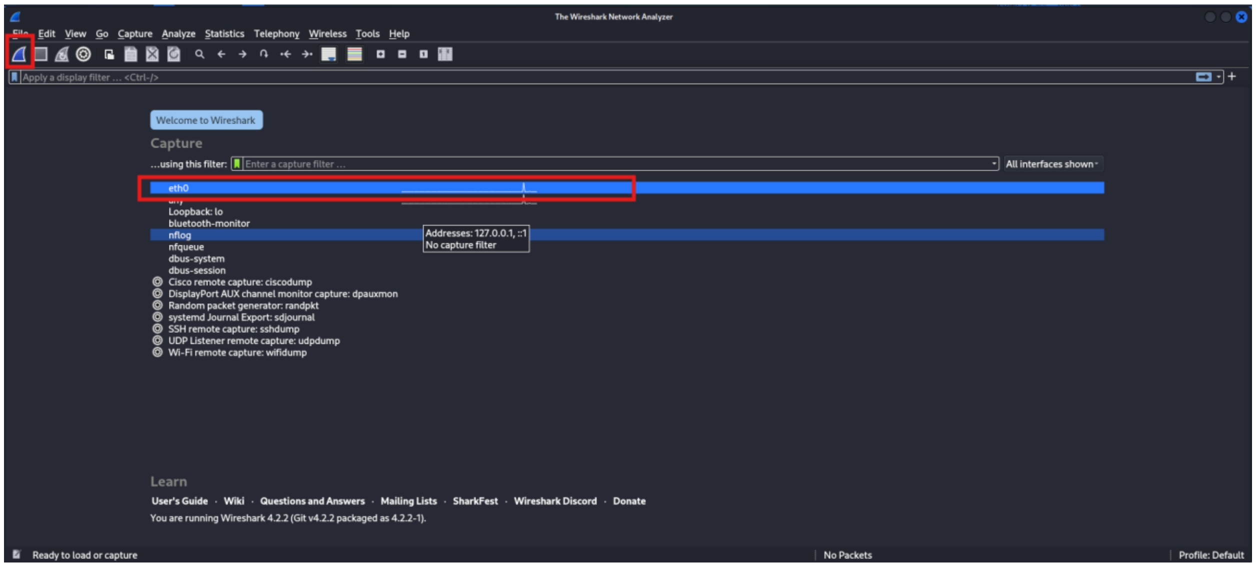
Wireshark- Sniffing the Login Credentials

Sniffing login credentials and passwords using Wireshark from a website that uses the HTTP protocol involves capturing and analyzing unencrypted HTTP traffic where sensitive information is transmitted in plain text. When a user logs into a website over HTTP, their credentials, including username and password, are sent from the client's browser to the server without encryption. By starting a packet capture in Wireshark and applying the HTTP filter (` http `), an attacker can intercept these packets and view the raw data. Within the captured packets, the attacker can look at the HTTP requests and responses to locate the login credentials in the clear text, typically within the POST request payload. This vulnerability highlights the importance of using HTTPS, which encrypts data in transit, to protect sensitive information from being intercepted by unauthorized parties.

Using HTTP instead of HTTPS has several critical disadvantages. The primary issue is the lack of encryption, meaning that any data transmitted, including passwords and personal information, is sent in plain text and can be easily intercepted by attackers using tools like Wireshark. This makes HTTP highly vulnerable to man-in-the-middle attacks, where attackers can intercept and alter the data without the user's knowledge. Additionally, HTTP does not ensure data integrity, allowing for potential data corruption or unauthorized modifications during transmission. Without proper authentication mechanisms, HTTP also leaves users susceptible to phishing attacks and impersonation. Furthermore, search engines like Google penalize HTTP websites, resulting in lower search rankings and visibility. Modern web browsers also warn users about the insecurity of HTTP sites, which can deter visitors and reduce trust. These drawbacks make HTTPS, which provides encryption, integrity, and authentication, the preferred choice for secure web communications.

Examples: -

1. Open wireshark and choice the interface to start capturing the packets.

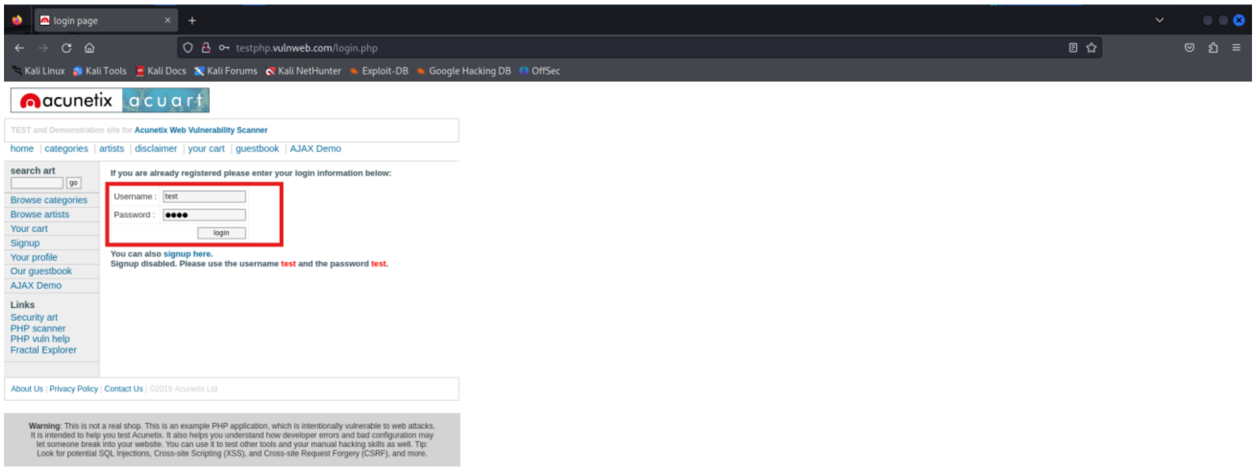

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
No Packets
Profile: Default

Addresses: 127.0.0.1, ::1
No capture filter

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1).

Ready to load or capture

2. Now went to the target website and filled up the login credentials.


login page
testphp.vulnweb.com/login.php
Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
login
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

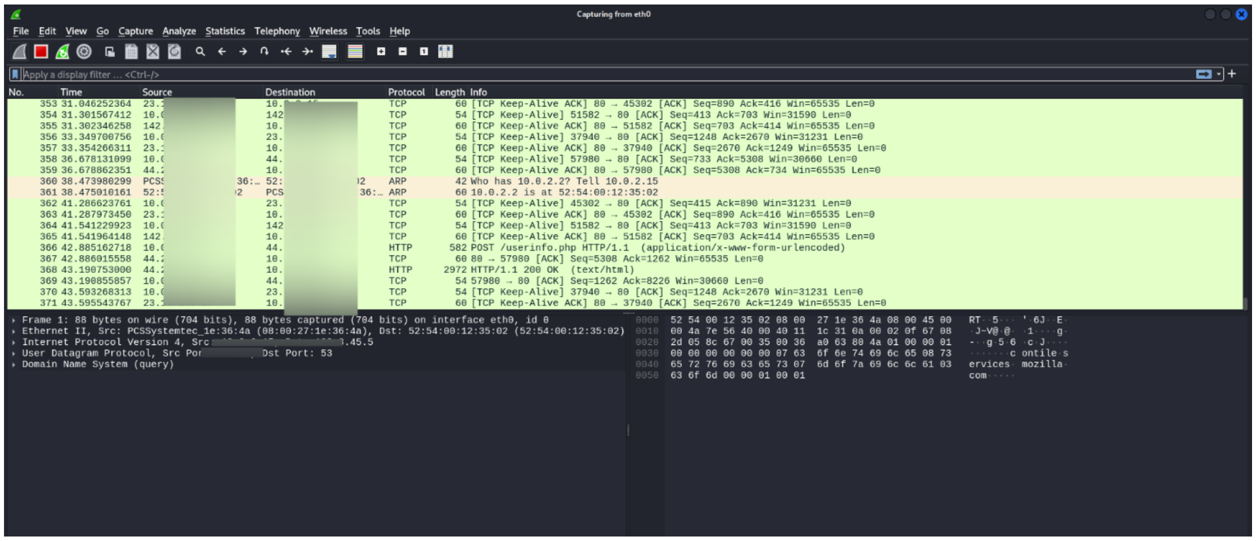
If you are already registered please enter your login information below:

Username : test
Password : ●●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.

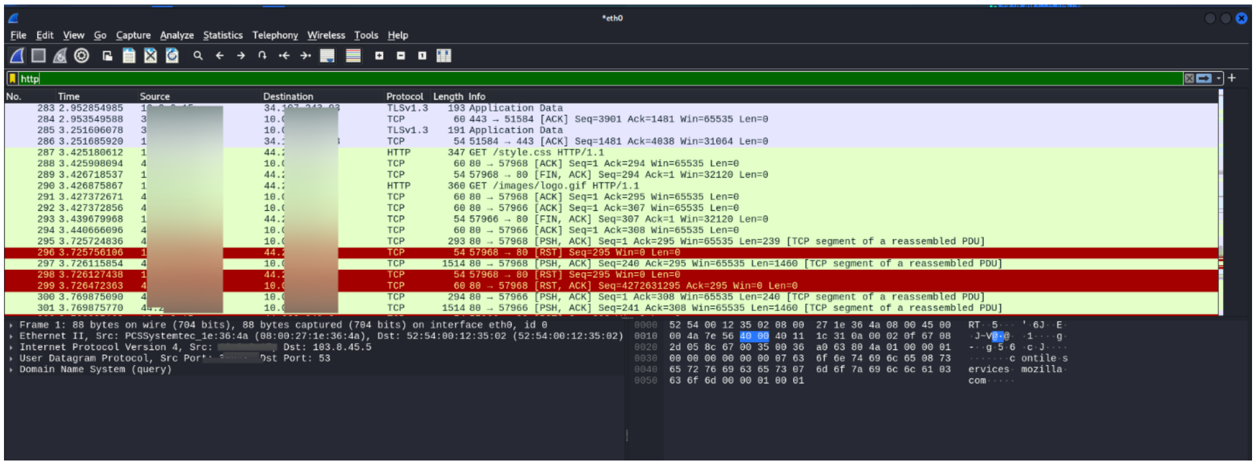
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

3. Now open wireshark to have insight of captured packets.



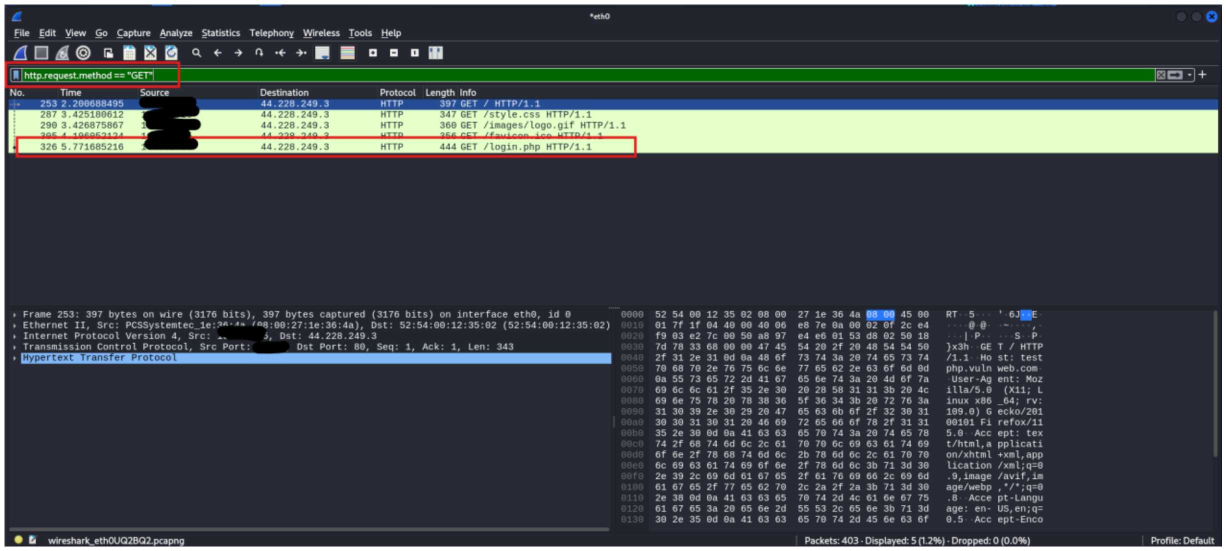
```
Capturing from eth0
Apply a display filter … <Ctrl-/>
No.   Time          Source          Destination     Protocol  Length  Info
  353 31.046252364  23.1[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 45302 [ACK] Seq=890 Ack=416 Win=65535 Len=0
  354 31.301567412  10.0[redacted]  142[redacted]   TCP         54 [TCP Keep-Alive] 51582 → 80 [ACK] Seq=413 Ack=703 Win=31590 Len=0
  355 31.302346258  142.[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 51582 [ACK] Seq=703 Ack=414 Win=65535 Len=0
  356 33.349700756  10.0[redacted]  23.[redacted]   TCP         54 [TCP Keep-Alive] 37940 → 80 [ACK] Seq=1248 Ack=2670 Win=31231 Len=0
  357 33.354266311  23.1[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 37940 [ACK] Seq=2670 Ack=1249 Win=65535 Len=0
  358 36.678131099  10.0[redacted]  44.[redacted]   TCP         54 [TCP Keep-Alive] 57980 → 80 [ACK] Seq=733 Ack=5308 Win=30660 Len=0
  359 36.678862351  44.2[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 57980 [ACK] Seq=5308 Ack=734 Win=65535 Len=0
  360 38.473980299  PCS[redacted]36:…  52:[redacted]2  ARP     42 Who has 10.0.2.2? Tell 10.0.2.15
  361 38.475010161  52:5[redacted]2  PCS[redacted]36:…  ARP     60 10.0.2.2 is at 52:54:00:12:35:02
  362 41.286623761  10.0[redacted]  23.[redacted]   TCP         54 [TCP Keep-Alive] 45302 → 80 [ACK] Seq=415 Ack=890 Win=31231 Len=0
  363 41.287973450  23.1[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 45302 [ACK] Seq=890 Ack=416 Win=65535 Len=0
  364 41.541229923  10.0[redacted]  142[redacted]   TCP         54 [TCP Keep-Alive] 51582 → 80 [ACK] Seq=413 Ack=703 Win=31590 Len=0
  365 41.541964148  142.[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 51582 [ACK] Seq=703 Ack=414 Win=65535 Len=0
  366 42.885162718  10.0[redacted]  44.[redacted]   HTTP       582 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  367 42.886015558  44.2[redacted]  10.[redacted]   TCP         60 80 → 57980 [ACK] Seq=5308 Ack=1262 Win=65535 Len=0
  368 43.190753000  44.2[redacted]  10.[redacted]   HTTP      2972 HTTP/1.1 200 OK  (text/html)
  369 43.190855857  10.0[redacted]  44.[redacted]   TCP         54 57980 → 80 [ACK] Seq=1262 Ack=8226 Win=30660 Len=0
  370 43.593268313  10.0[redacted]  23.[redacted]   TCP         54 [TCP Keep-Alive] 37940 → 80 [ACK] Seq=1248 Ack=2670 Win=31231 Len=0
  371 43.595543767  23.1[redacted]  10.[redacted]   TCP         60 [TCP Keep-Alive ACK] 80 → 37940 [ACK] Seq=2670 Ack=1249 Win=65535 Len=0

› Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src[redacted].45.5
› User Datagram Protocol, Src Por[redacted]Dst Port: 53
› Domain Name System (query)

0000  52 54 00 12 35 02 08 00  27 1e 36 4a 08 00 45 00   RT··5···'·6J··E·
0010  00 4a 7e 56 40 00 40 11  1c 31 0a 00 02 0f 67 08   ·J~V@·@··1····g·
0020  2d 05 8c 67 00 35 00 36  a0 63 80 4a 01 00 00 01   -··g·5·6·c·J····
0030  00 00 00 00 00 00 07 63  6f 6e 74 69 6c 65 08 73   ·······c ontile·s
0040  65 72 76 69 63 65 73 07  6d 6f 7a 69 6c 6c 61 03   ervices· mozilla·
0050  63 6f 6d 00 00 01 00 01                            com·····
```

4. We are looking for http packets so, we will use the http filter.



```
*eth0
http
No.   Time          Source          Destination     Protocol  Length  Info
  283 2.952854985   1[redacted]     34.[redacted]   TLSv1.3    193 Application Data
  284 2.953549588   3[redacted]     10.0[redacted]  TCP         60 443 → 51584 [ACK] Seq=3901 Ack=1481 Win=65535 Len=0
  285 3.251606078   3[redacted]     10.0[redacted]  TLSv1.3    191 Application Data
  286 3.251685920   1[redacted]     34.1[redacted]  TCP         54 51584 → 443 [ACK] Seq=1481 Ack=4038 Win=31064 Len=0
  287 3.425180612   1[redacted]     44.2[redacted]  HTTP       347 GET /style.css HTTP/1.1
  288 3.425908094   4[redacted]     10.0[redacted]  TCP         60 80 → 57968 [ACK] Seq=1 Ack=294 Win=65535 Len=0
  289 3.426718537   1[redacted]     44.2[redacted]  TCP         54 57968 → 80 [FIN, ACK] Seq=294 Ack=1 Win=32120 Len=0
  290 3.426875867   1[redacted]     44.2[redacted]  HTTP       360 GET /images/logo.gif HTTP/1.1
  291 3.427372671   4[redacted]     10.0[redacted]  TCP         60 80 → 57968 [ACK] Seq=1 Ack=295 Win=65535 Len=0
  292 3.427372856   4[redacted]     10.0[redacted]  TCP         60 80 → 57966 [ACK] Seq=1 Ack=307 Win=65535 Len=0
  293 3.439679968   1[redacted]     44.2[redacted]  TCP         54 57966 → 80 [FIN, ACK] Seq=307 Ack=1 Win=32120 Len=0
  294 3.440666096   4[redacted]     10.0[redacted]  TCP         60 80 → 57966 [ACK] Seq=1 Ack=308 Win=65535 Len=0
  295 3.725724836   4[redacted]     10.0[redacted]  TCP        293 80 → 57968 [PSH, ACK] Seq=1 Ack=295 Win=65535 Len=239 [TCP segment of a reassembled PDU]
  296 3.725756106   1[redacted]     44.2[redacted]  TCP         54 57968 → 80 [RST] Seq=295 Win=0 Len=0
  297 3.726115854   4[redacted]     10.0[redacted]  TCP       1514 80 → 57968 [PSH, ACK] Seq=240 Ack=295 Win=65535 Len=1460 [TCP segment of a reassembled PDU]
  298 3.726127438   1[redacted]     44.2[redacted]  TCP         54 57968 → 80 [RST] Seq=295 Win=0 Len=0
  299 3.726472363   4[redacted]     10.0[redacted]  TCP         60 80 → 57968 [RST, ACK] Seq=4272631295 Ack=295 Win=0 Len=0
  300 3.769875090   4[redacted]     10.0[redacted]  TCP        294 80 → 57966 [PSH, ACK] Seq=1 Ack=308 Win=65535 Len=240 [TCP segment of a reassembled PDU]
  301 3.769875770   44.2[redacted]  10.0[redacted]  TCP       1514 80 → 57966 [PSH, ACK] Seq=241 Ack=308 Win=65535 Len=1460 [TCP segment of a reassembled PDU]

› Frame 1: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: [redacted] Dst: 103.8.45.5
› User Datagram Protocol, Src Port[redacted]Dst Port: 53
› Domain Name System (query)

0000  52 54 00 12 35 02 08 00  27 1e 36 4a 08 00 45 00   RT··5···'·6J··E·
0010  00 4a 7e 56 40 00 40 11  1c 31 0a 00 02 0f 67 08   ·J~V@·@··1····g·
0020  2d 05 8c 67 00 35 00 36  a0 63 80 4a 01 00 00 01   -··g·5·6·c·J····
0030  00 00 00 00 00 00 07 63  6f 6e 74 69 6c 65 08 73   ·······c ontile·s
0040  65 72 76 69 63 65 73 07  6d 6f 7a 69 6c 6c 61 03   ervices· mozilla·
0050  63 6f 6d 00 00 01 00 01                            com·····
```

5. There are too many http packets out of most is not required by us. So, we will use http.request.method == “GET” filter in order to fetch out get requests.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wireshark_eth0UQ2BQ2.pcapng

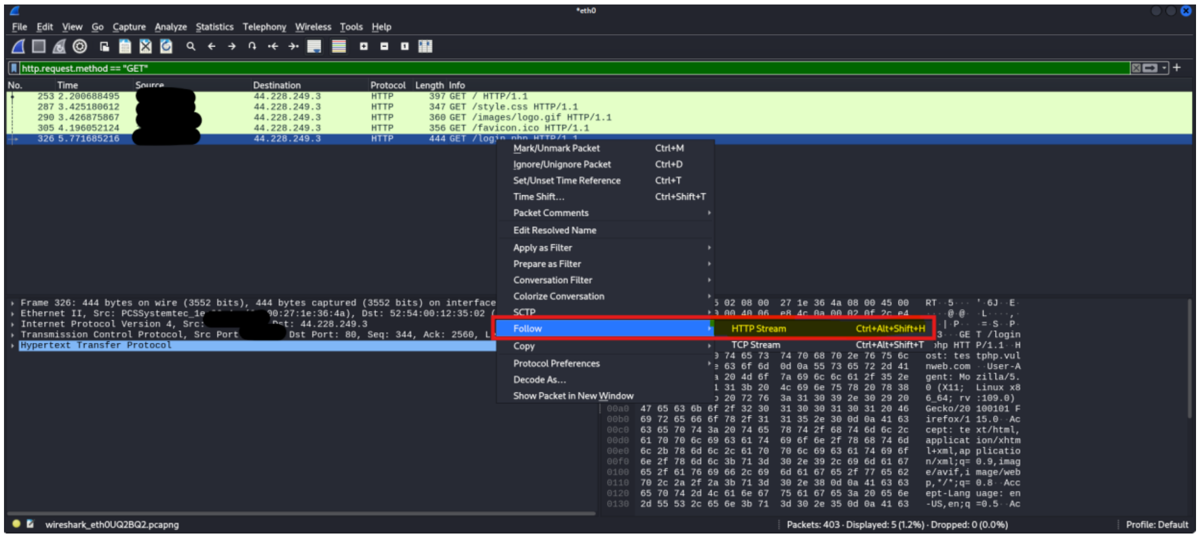
```
http.request.method == "GET"

No.  Time         Source      Destination    Protocol Length Info
253 2.200688495  [redacted]  44.228.249.3   HTTP     397 GET / HTTP/1.1
287 3.425180612              44.228.249.3   HTTP     347 GET /style.css HTTP/1.1
290 3.426875867              44.228.249.3   HTTP     360 GET /images/logo.gif HTTP/1.1
305 4.196052124              44.228.249.3   HTTP     356 GET /favicon.ico HTTP/1.1
326 5.771685216              44.228.249.3   HTTP     444 GET /login.php HTTP/1.1
```

```
Frame 253: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_1e:[redacted] (08:00:27:1e:36:4a), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: [redacted], Dst: 44.228.249.3
Transmission Control Protocol, Src Port: [redacted] Dst Port: 80, Seq: 1, Ack: 1, Len: 343
Hypertext Transfer Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 1e 36 4a 08 00 45 00   RT··5···  '·6J··E·
0010  01 7f 1f 04 40 00 40 06  e8 7e 0a 00 02 0f 2c e4   ····@·@·  ·~····,·
0020  f9 03 e2 7c 00 50 a8 97  e4 e6 01 53 d8 02 50 18   ···|·P··  ···S··P·
0030  7d 78 33 68 00 00 47 45  54 20 2f 20 48 54 54 50   }x3h··GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 74 65 73 74   /1.1··Ho st: test
0050  70 68 70 2e 76 75 6c 6e  77 65 62 2e 63 6f 6d 0d   php.vuln web.com·
0060  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0070  69 6c 6c 61 2f 35 2e 30  20 28 58 31 31 3b 20 4c   illa/5.0  (X11; L
0080  69 6e 75 78 20 78 38 36  5f 36 34 3b 20 72 76 3a   inux x86 _64; rv:
0090  31 30 39 2e 30 29 20 47  65 63 6b 6f 2f 32 30 31   109.0) G ecko/201
00a0  30 30 31 30 31 20 46 69  72 65 66 6f 78 2f 31 31   00101 Fi refox/11
00b0  35 2e 30 0d 0a 41 63 63  65 70 74 3a 20 74 65 78   5.0··Acc ept: tex
00c0  74 2f 68 74 6d 6c 2c 61  70 70 6c 69 63 61 74 69   t/html,a pplicati
00d0  6f 6e 2f 78 68 74 6d 6c  2b 78 6d 6c 2c 61 70 70   on/xhtml +xml,app
00e0  6c 69 63 61 74 69 6f 6e  2f 78 6d 6c 3b 71 3d 30   lication /xml;q=0
00f0  2e 39 2c 69 6d 61 67 65  2f 61 76 69 66 2c 69 6d   .9,image /avif,im
0100  61 67 65 2f 77 65 62 70  2c 2a 2f 2a 3b 71 3d 30   age/webp ,*/*;q=0
0110  2e 38 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   .8··Acce pt-Langu
0120  61 67 65 3a 20 65 6e 2d  55 53 2c 65 6e 3b 71 3d   age: en- US,en;q=
0130  30 2e 35 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.5··Acc ept-Enco
```

Packets: 403 · Displayed: 5 (1.2%) · Dropped: 0 (0.0%)   Profile: Default

6. As we can see here is a GET request of php login page that might consist login details. To do so right click on that packet and click on follow button than click on HTTP stream button to have summary of the particular http request.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
HTTP Stream Ctrl+Alt+Shift+H
TCP Stream Ctrl+Alt+Shift+T
wireshark_eth0UQ2BQ2.pcapng

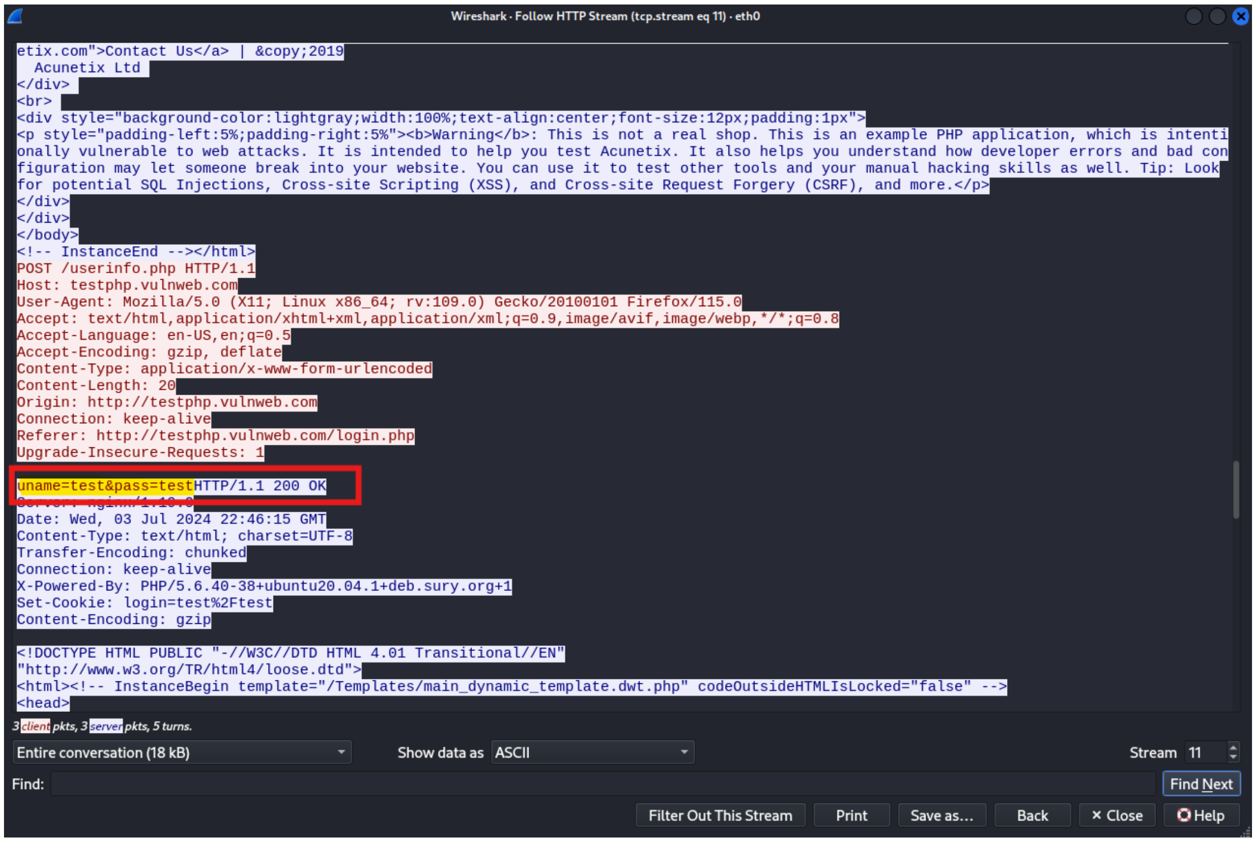
```
http.request.method == "GET"

No.  Time         Source      Destination    Protocol Length Info
253 2.200688495  [redacted]  44.228.249.3   HTTP     397 GET / HTTP/1.1
287 3.425180612              44.228.249.3   HTTP     347 GET /style.css HTTP/1.1
290 3.426875867              44.228.249.3   HTTP     360 GET /images/logo.gif HTTP/1.1
305 4.196052124              44.228.249.3   HTTP     356 GET /favicon.ico HTTP/1.1
326 5.771685216              44.228.249.3   HTTP     444 GET /logi
```

```
Frame 326: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface
Ethernet II, Src: PCSSystemtec_1e[redacted]00:27:1e:36:4a), Dst: 52:54:00:12:35:02 (
Internet Protocol Version 4, Src: [redacted] Dst: 44.228.249.3
Transmission Control Protocol, Src Port [redacted] Dst Port: 80, Seq: 344, Ack: 2560, L
Hypertext Transfer Protocol
```

```
      5 02 08 00  27 1e 36 4a 08 00 45 00   RT··5···  '·6J··E·
      3 00 40 06  e8 4c 0a 00 02 0f 2c e4   ····@·@·  ·L····,·
                                            ·|·P··  ·=·S··P·
                                            3··GE T /login
                                            php HTT P/1.1··H
      9 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
      e 63 6f 6d  0d 0a 55 73 65 72 2d 41   nweb.com ··User-A
      a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
      1 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
      ) 20 72 76  3a 31 30 39 2e 30 29 20   6_64; rv :109.0)
00a0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00b0  69 72 65 66 6f 78 2f 31  31 35 2e 30 0d 0a 41 63   irefox/1 15.0··Ac
00c0  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
00d0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00e0  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
00f0  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0100  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0110  70 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   p,*/*;q= 0.8··Acc
0120  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0130  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
```

Packets: 403 · Displayed: 5 (1.2%) · Dropped: 0 (0.0%)   Profile: Default

7. Here we can see, the client side request contains that password that we have filled up inside the sign up page of our target website.



Wireshark · Follow HTTP Stream (tcp.stream eq 11) · eth0

```
etix.com">Contact Us</a> | &copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real shop. This is an example PHP application, which is intenti
onally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad con
figuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look
for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.</p>
</div>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 03 Jul 2024 22:46:15 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (18 kB) — Show data as: ASCII — Stream: 11