ASSIGMENT FOR MODULE 3

STUDENT NAME: AKOGUN ABIODUN

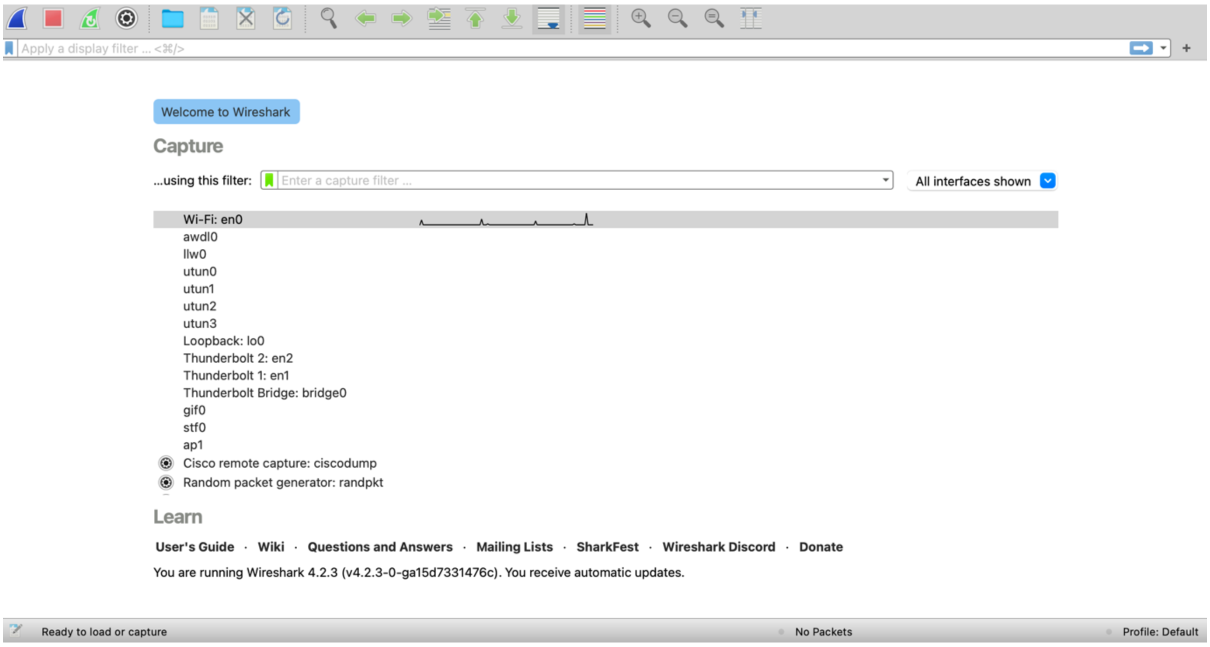
ASSIGNMENT TITLE:

UNDERSTANDING HTTP PACKET ANALYSIS USING WIRESHARK

Question 1

CAPTURE NETWORK TRAFFIC:

1. **I open a Wireshark and start a new capture session.**



Apply a display filter ... <⌘/>
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

...using this filter: Enter a capture filter ...

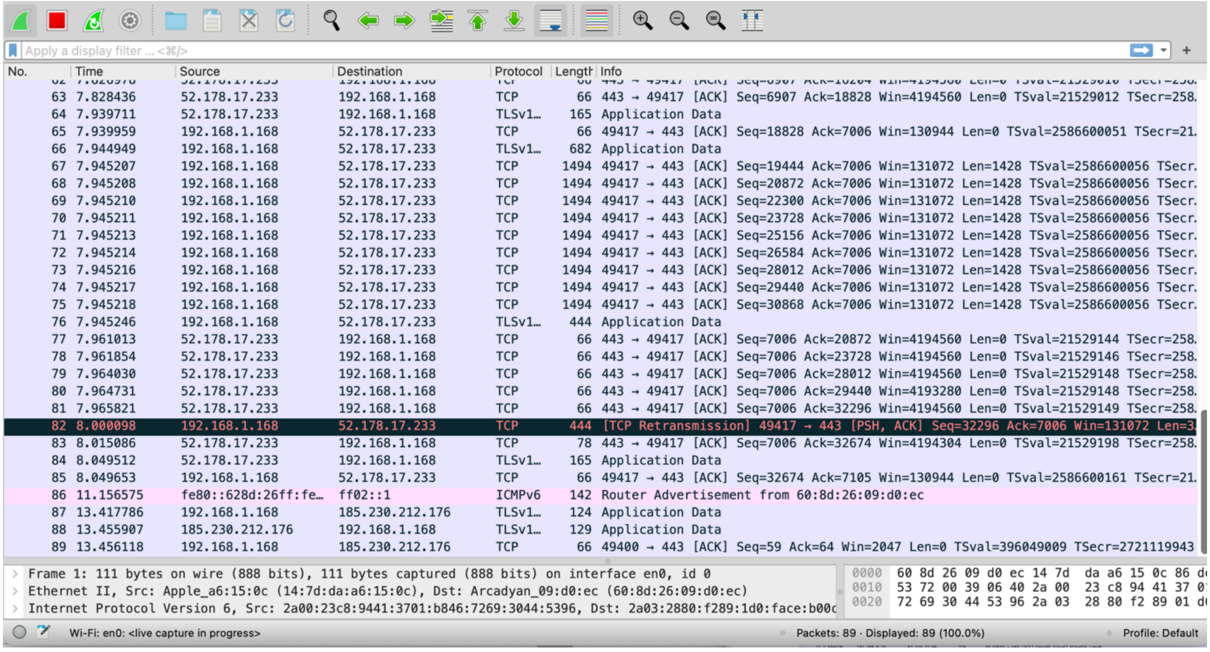
All interfaces shown

Wi-Fi: en0
awdl0
llw0
utun0
utun1
utun2
utun3
Loopback: lo0
Thunderbolt 2: en2
Thunderbolt 1: en1
Thunderbolt Bridge: bridge0
gif0
stf0
ap1
Cisco remote capture: ciscodump
Random packet generator: randpkt

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

Ready to load or capture · No Packets · Profile: Default

2. **Choose the appropriate network interface for capturing, begin capturing traffic by clicking the 'start' button on the WI-FI**



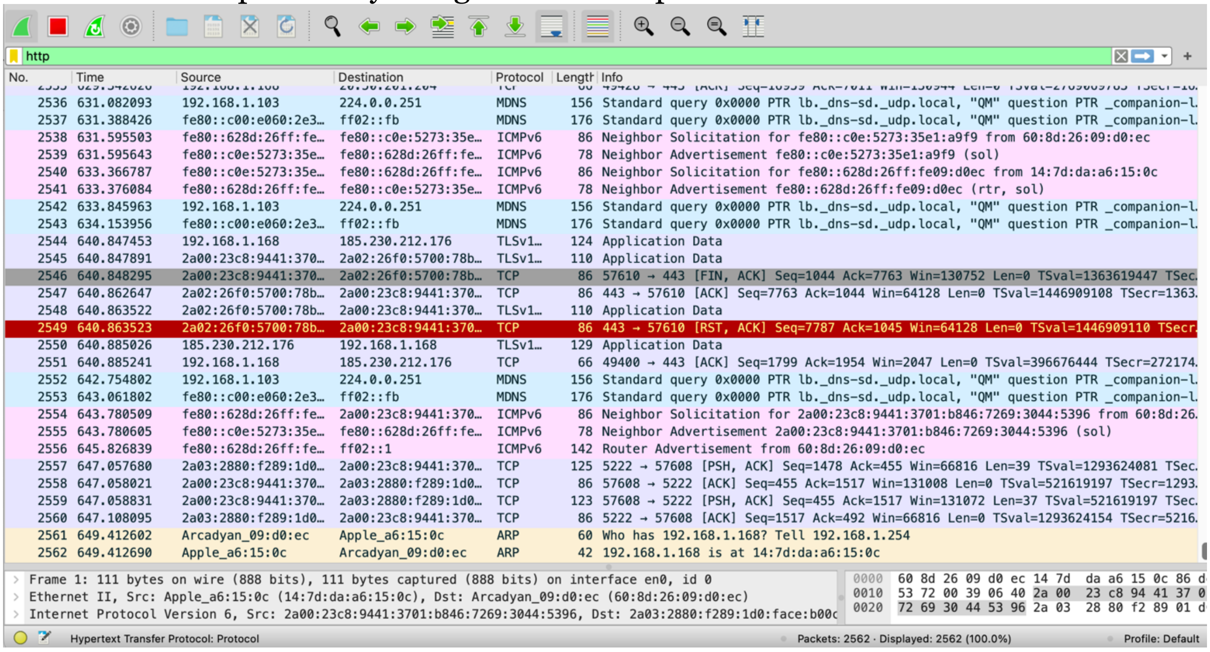
```
Apply a display filter ... <⌘/>
No.    Time       Source              Destination         Protocol  Length Info
    63 7.828436   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=6907 Ack=18828 Win=4194560 Len=0 TSval=21529012 TSecr=258.
    64 7.939711   52.178.17.233       192.168.1.168       TLSv1…    165 Application Data
    65 7.939959   192.168.1.168       52.178.17.233       TCP        66 49417 → 443 [ACK] Seq=18828 Ack=7006 Win=130944 Len=0 TSval=2586600051 TSecr=21.
    66 7.944949   192.168.1.168       52.178.17.233       TLSv1…    682 Application Data
    67 7.945207   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=19444 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    68 7.945208   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=20872 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    69 7.945210   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=22300 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    70 7.945211   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=23728 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    71 7.945213   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=25156 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    72 7.945214   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=26584 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    73 7.945216   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=28012 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    74 7.945217   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=29440 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    75 7.945218   192.168.1.168       52.178.17.233       TCP      1494 49417 → 443 [ACK] Seq=30868 Ack=7006 Win=131072 Len=1428 TSval=2586600056 TSecr.
    76 7.945246   192.168.1.168       52.178.17.233       TLSv1…    444 Application Data
    77 7.961013   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=7006 Ack=20872 Win=4194560 Len=0 TSval=21529144 TSecr=258.
    78 7.961854   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=7006 Ack=23728 Win=4194560 Len=0 TSval=21529146 TSecr=258.
    79 7.964030   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=7006 Ack=28012 Win=4194560 Len=0 TSval=21529148 TSecr=258.
    80 7.964731   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=7006 Ack=29440 Win=4193280 Len=0 TSval=21529148 TSecr=258.
    81 7.965821   52.178.17.233       192.168.1.168       TCP        66 443 → 49417 [ACK] Seq=7006 Ack=32296 Win=4194560 Len=0 TSval=21529149 TSecr=258.
    82 8.000098   192.168.1.168       52.178.17.233       TCP       444 [TCP Retransmission] 49417 → 443 [PSH, ACK] Seq=32296 Ack=7006 Win=131072 Len=3.
    83 8.015086   52.178.17.233       192.168.1.168       TCP        78 443 → 49417 [ACK] Seq=7006 Ack=32674 Win=4194304 Len=0 TSval=21529198 TSecr=258.
    84 8.049512   52.178.17.233       192.168.1.168       TLSv1…    165 Application Data
    85 8.049653   192.168.1.168       52.178.17.233       TCP        66 49417 → 443 [ACK] Seq=32674 Ack=7105 Win=130944 Len=0 TSval=2586600161 TSecr=21.
    86 11.156575  fe80::628d:26ff:fe… ff02::1             ICMPv6    142 Router Advertisement from 60:8d:26:09:d0:ec
    87 13.417786  192.168.1.168       185.230.212.176     TLSv1…    124 Application Data
    88 13.455907  185.230.212.176     192.168.1.168       TLSv1…    129 Application Data
    89 13.456118  192.168.1.168       185.230.212.176     TCP        66 49400 → 443 [ACK] Seq=59 Ack=64 Win=2047 Len=0 TSval=396049009 TSecr=2721119943

> Frame 1: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface en0, id 0      0000  60 8d 26 09 d0 ec 14 7d  da a6 15 0c 86 d
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09:d0:ec)  0010  53 72 00 39 06 40 2a 00  23 c8 94 41 37 0
> Internet Protocol Version 6, Src: 2a00:23c8:9441:3701:b846:7269:3044:5396, Dst: 2a03:2880:f289:1d0:face:b00c  0020  72 69 30 44 53 96 2a 03  28 80 f2 89 01 d

Wi-Fi: en0: <live capture in progress>          Packets: 89 · Displayed: 89 (100.0%)          Profile: Default
```

Question 2: **ANALYZE HTTP PACKETS**

1. Locate the HTTP packets by using the filter ‘http’ in the Wireshark filter bar.

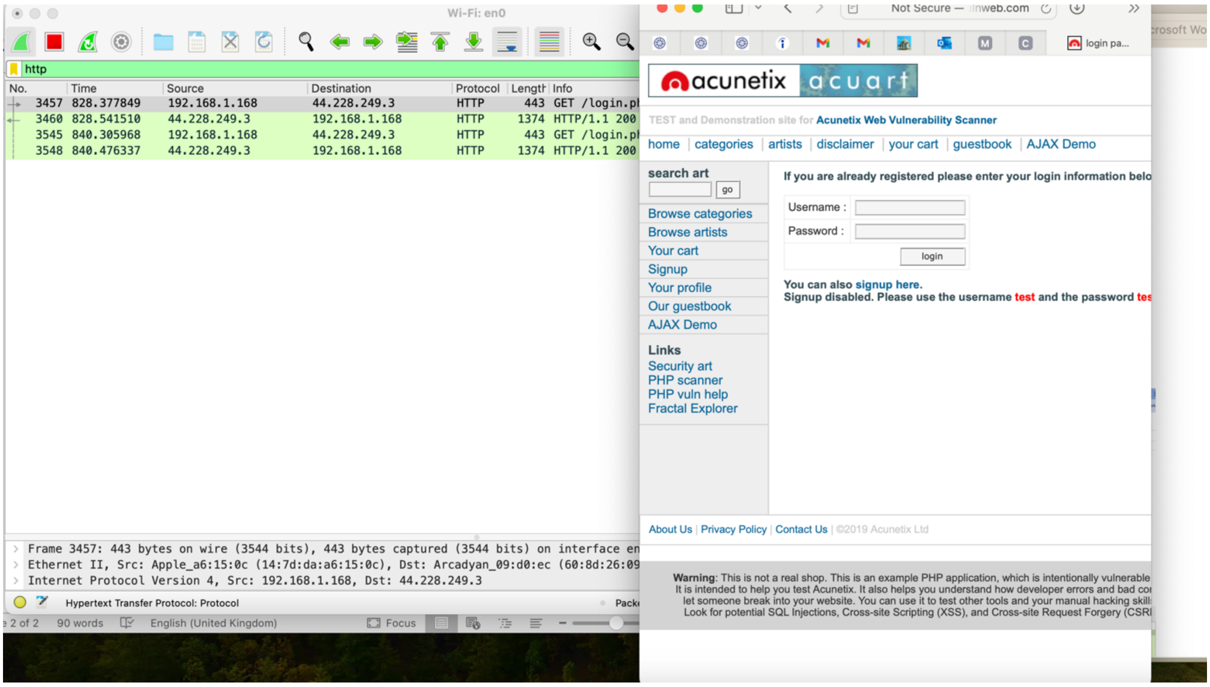


```
http
No.    Time        Source              Destination         Protocol  Length Info
  2536 631.082093  192.168.1.103       224.0.0.251         MDNS      156 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2537 631.388426  fe80::c00:e060:2e3… ff02::fb            MDNS      176 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2538 631.595503  fe80::628d:26ff:fe… fe80::c0e:5273:35e… ICMPv6     86 Neighbor Solicitation for fe80::c0e:5273:35e1:a9f9 from 60:8d:26:09:d0:ec
  2539 631.595643  fe80::c0e:5273:35e… fe80::628d:26ff:fe… ICMPv6     78 Neighbor Advertisement fe80::c0e:5273:35e1:a9f9 (sol)
  2540 633.366787  fe80::c0e:5273:35e… fe80::628d:26ff:fe… ICMPv6     86 Neighbor Solicitation for fe80::628d:26ff:fe09:d0ec from 14:7d:da:a6:15:0c
  2541 633.376084  fe80::628d:26ff:fe… fe80::c0e:5273:35e… ICMPv6     78 Neighbor Advertisement fe80::628d:26ff:fe09:d0ec (rtr, sol)
  2542 633.845963  192.168.1.103       224.0.0.251         MDNS      156 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2543 634.153956  fe80::c00:e060:2e3… ff02::fb            MDNS      176 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2544 640.847453  192.168.1.168       185.230.212.176     TLSv1…    124 Application Data
  2545 640.847891  2a00:23c8:9441:370… 2a02:26f0:5700:78b… TLSv1…    110 Application Data
  2546 640.848295  2a00:23c8:9441:370… 2a02:26f0:5700:78b… TCP        86 57610 → 443 [FIN, ACK] Seq=1044 Ack=7763 Win=130752 Len=0 TSval=1363619447 TSec.
  2547 640.862647  2a02:26f0:5700:78b… 2a00:23c8:9441:370… TCP        86 443 → 57610 [ACK] Seq=7763 Ack=1044 Win=64128 Len=0 TSval=1446909108 TSecr=1363.
  2548 640.863522  2a02:26f0:5700:78b… 2a00:23c8:9441:370… TLSv1…    110 Application Data
  2549 640.863523  2a02:26f0:5700:78b… 2a00:23c8:9441:370… TCP        86 443 → 57610 [RST, ACK] Seq=7787 Ack=1045 Win=64128 Len=0 TSval=1446909110 TSecr
  2550 640.885026  185.230.212.176     192.168.1.168       TLSv1…    129 Application Data
  2551 640.885241  192.168.1.168       185.230.212.176     TCP        66 49400 → 443 [ACK] Seq=1799 Ack=1954 Win=2047 Len=0 TSval=396676444 TSecr=272174.
  2552 642.754802  192.168.1.103       224.0.0.251         MDNS      156 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2553 643.061802  fe80::c00:e060:2e3… ff02::fb            MDNS      176 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _companion-l.
  2554 643.780509  fe80::628d:26ff:fe… 2a00:23c8:9441:370… ICMPv6     86 Neighbor Solicitation for 2a00:23c8:9441:3701:b846:7269:3044:5396 from 60:8d:26.
  2555 643.780605  fe80::c0e:5273:35e… fe80::628d:26ff:fe… ICMPv6     78 Neighbor Advertisement 2a00:23c8:9441:3701:b846:7269:3044:5396 (sol)
  2556 645.826839  fe80::628d:26ff:fe… ff02::1             ICMPv6    142 Router Advertisement from 60:8d:26:09:d0:ec
  2557 647.057680  2a03:2880:f289:1d0… 2a00:23c8:9441:370… TCP       125 5222 → 57608 [PSH, ACK] Seq=1478 Ack=455 Win=66816 Len=39 TSval=1293624081 TSec.
  2558 647.058021  2a00:23c8:9441:370… 2a03:2880:f289:1d0… TCP        86 57608 → 5222 [ACK] Seq=455 Ack=1517 Win=131008 Len=0 TSval=521619197 TSecr=1293.
  2559 647.058831  2a00:23c8:9441:370… 2a03:2880:f289:1d0… TCP       123 57608 → 5222 [PSH, ACK] Seq=455 Ack=1517 Win=131072 Len=37 TSval=521619197 TSec.
  2560 647.108095  2a03:2880:f289:1d0… 2a00:23c8:9441:370… TCP        86 5222 → 57608 [ACK] Seq=1517 Ack=492 Win=66816 Len=0 TSval=1293624154 TSecr=5216.
  2561 649.412602  Arcadyan_09:d0:ec   Apple_a6:15:0c      ARP        60 Who has 192.168.1.168? Tell 192.168.1.254
  2562 649.412690  Apple_a6:15:0c      Arcadyan_09:d0:ec   ARP        42 192.168.1.168 is at 14:7d:da:a6:15:0c

> Frame 1: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface en0, id 0      0000  60 8d 26 09 d0 ec 14 7d  da a6 15 0c 86 d
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09:d0:ec)  0010  53 72 00 39 06 40 2a 00  23 c8 94 41 37 0
> Internet Protocol Version 6, Src: 2a00:23c8:9441:3701:b846:7269:3044:5396, Dst: 2a03:2880:f289:1d0:face:b00c  0020  72 69 30 44 53 96 2a 03  28 80 f2 89 01 d

Hypertext Transfer Protocol: Protocol          Packets: 2562 · Displayed: 2562 (100.0%)          Profile: Default
```

2: Identify the packets related to the login process. Look for the POST request to the login endpoint. (http://testphp.vulnweb.com/login.php)



```
No.   Time        Source          Destination     Protocol Length Info
3457  828.377849  192.168.1.168   44.228.249.3    HTTP      443  GET /login.pl
3460  828.541510  44.228.249.3    192.168.1.168   HTTP     1374  HTTP/1.1 200
3545  840.305968  192.168.1.168   44.228.249.3    HTTP      443  GET /login.pl
3548  840.476337  44.228.249.3    192.168.1.168   HTTP     1374  HTTP/1.1 200
```

```
> Frame 3457: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface en
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 44.228.249.3
```

Hypertext Transfer Protocol: Protocol
2 of 2 90 words English (United Kingdom) Focus

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

If you are already registered please enter your login information belo

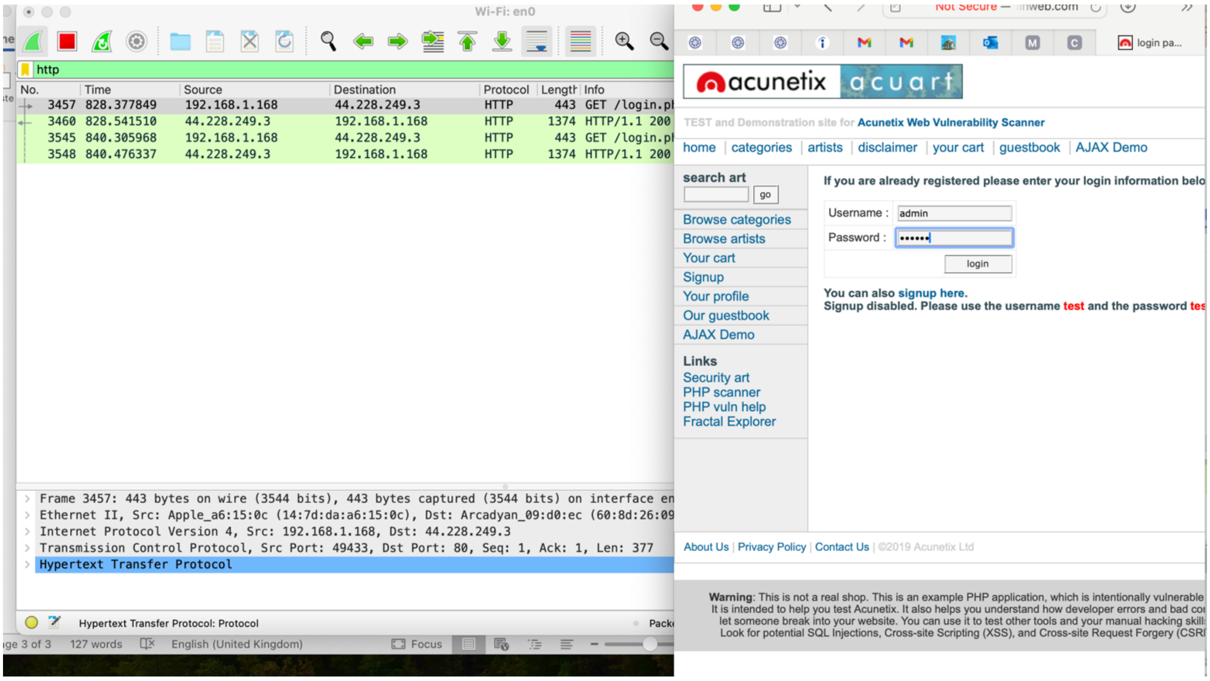
Username :
Password :
login

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

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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

Question 3: EXTRACT INFORMATION (USERNAME & PASSWORD)Enter the username and password and go to the Wireshark and you will find the list of information. Select userinfo. php and it will show all the detailed information with credentials.



```
No.   Time        Source          Destination     Protocol Length Info
3457  828.377849  192.168.1.168   44.228.249.3    HTTP      443  GET /login.pl
3460  828.541510  44.228.249.3    192.168.1.168   HTTP     1374  HTTP/1.1 200
3545  840.305968  192.168.1.168   44.228.249.3    HTTP      443  GET /login.pl
3548  840.476337  44.228.249.3    192.168.1.168   HTTP     1374  HTTP/1.1 200
```

```
> Frame 3457: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface en
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 49433, Dst Port: 80, Seq: 1, Ack: 1, Len: 377
> Hypertext Transfer Protocol
```

Hypertext Transfer Protocol: Protocol
ge 3 of 3 127 words English (United Kingdom) Focus

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

If you are already registered please enter your login information belo

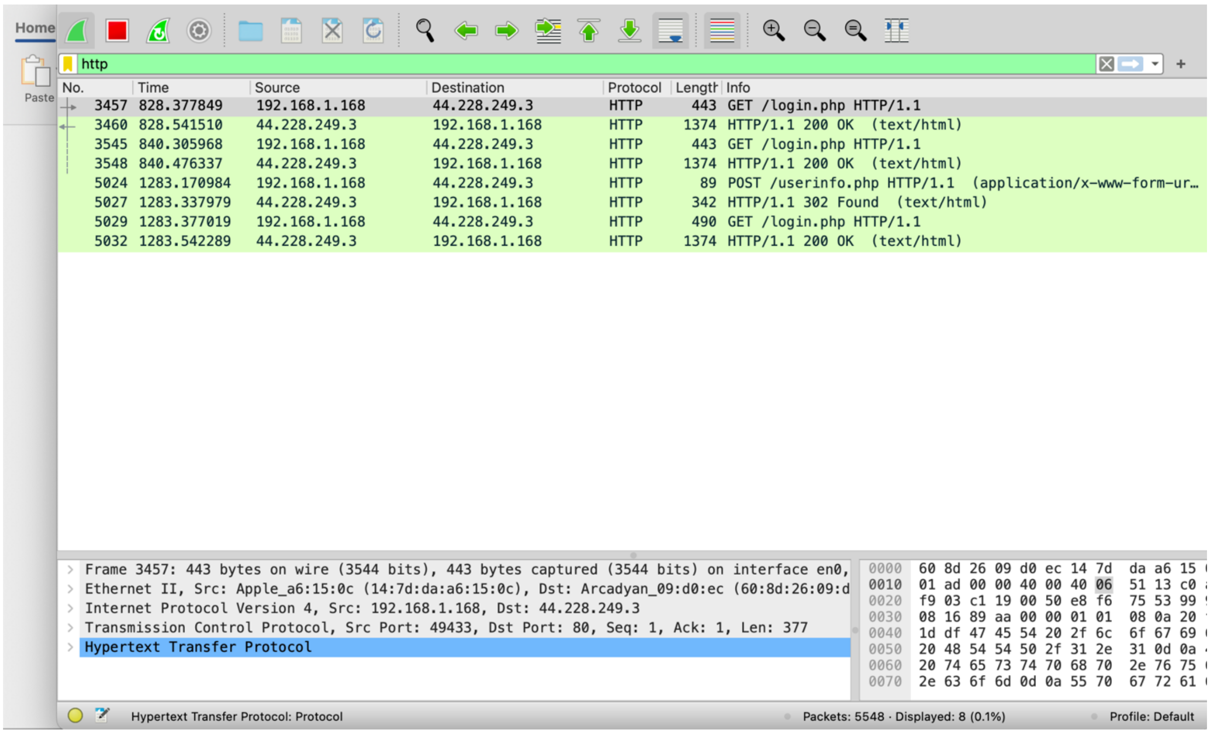
Username : admin
Password : ••••••
login

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

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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

After entering user name and password



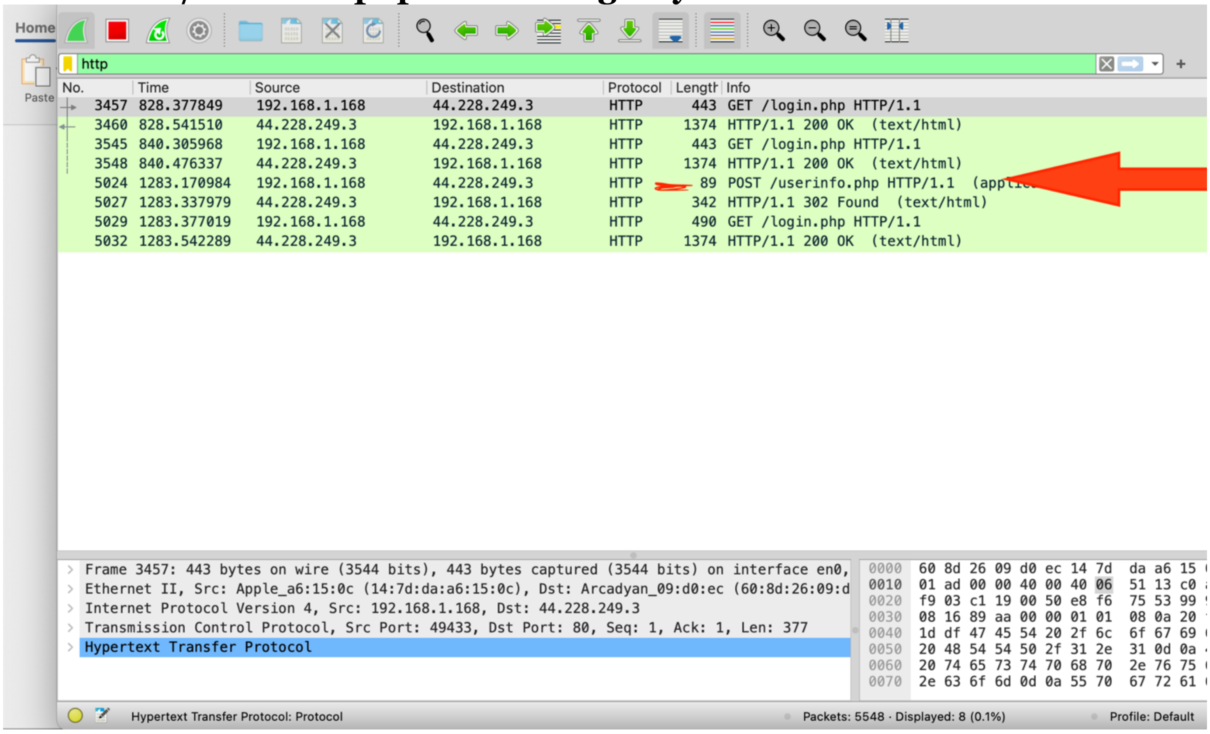
```
http
No.   Time         Source          Destination     Protocol Length Info
 3457 828.377849   192.168.1.168   44.228.249.3    HTTP       443 GET /login.php HTTP/1.1
 3460 828.541510   44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
 3545 840.305968   192.168.1.168   44.228.249.3    HTTP       443 GET /login.php HTTP/1.1
 3548 840.476337   44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
 5024 1283.170984  192.168.1.168   44.228.249.3    HTTP        89 POST /userinfo.php HTTP/1.1  (application/x-www-form-ur…
 5027 1283.337979  44.228.249.3    192.168.1.168   HTTP       342 HTTP/1.1 302 Found  (text/html)
 5029 1283.377019  192.168.1.168   44.228.249.3    HTTP       490 GET /login.php HTTP/1.1
 5032 1283.542289  44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 3457: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface en0,
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09:d
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 49433, Dst Port: 80, Seq: 1, Ack: 1, Len: 377
> Hypertext Transfer Protocol
```

```
0000  60 8d 26 09 d0 ec 14 7d  da a6 15
0010  01 ad 00 00 40 00 40 06  51 13 c0
0020  f9 03 c1 19 00 50 e8 f6  75 53 99
0030  08 16 89 aa 00 00 01 01  08 0a 20
0040  1d df 47 45 54 20 2f 6c  6f 67 69
0050  20 48 54 54 50 2f 31 2e  31 0d 0a
0060  20 74 65 73 74 70 68 70  2e 76 75
0070  2e 63 6f 6d 0d 0a 55 70  67 72 61
```

```
Hypertext Transfer Protocol: Protocol        Packets: 5548 · Displayed: 8 (0.1%)        Profile: Default
```

Select Post/userinfo. php and it will give you detailed information.



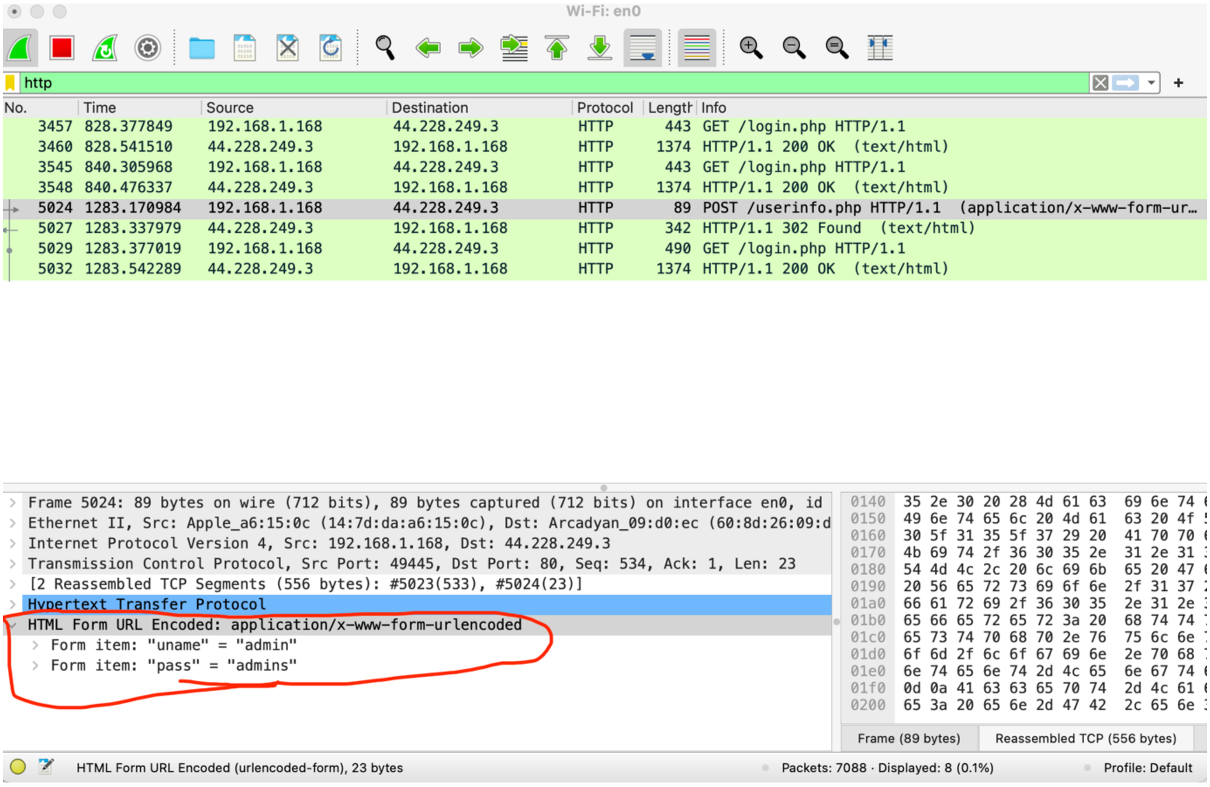
```
http
No.   Time         Source          Destination     Protocol Length Info
 3457 828.377849   192.168.1.168   44.228.249.3    HTTP       443 GET /login.php HTTP/1.1
 3460 828.541510   44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
 3545 840.305968   192.168.1.168   44.228.249.3    HTTP       443 GET /login.php HTTP/1.1
 3548 840.476337   44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
 5024 1283.170984  192.168.1.168   44.228.249.3    HTTP        89 POST /userinfo.php HTTP/1.1  (appli
 5027 1283.337979  44.228.249.3    192.168.1.168   HTTP       342 HTTP/1.1 302 Found  (text/html)
 5029 1283.377019  192.168.1.168   44.228.249.3    HTTP       490 GET /login.php HTTP/1.1
 5032 1283.542289  44.228.249.3    192.168.1.168   HTTP      1374 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 3457: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface en0,
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09:d
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 49433, Dst Port: 80, Seq: 1, Ack: 1, Len: 377
> Hypertext Transfer Protocol
```

```
0000  60 8d 26 09 d0 ec 14 7d  da a6 15
0010  01 ad 00 00 40 00 40 06  51 13 c0
0020  f9 03 c1 19 00 50 e8 f6  75 53 99
0030  08 16 89 aa 00 00 01 01  08 0a 20
0040  1d df 47 45 54 20 2f 6c  6f 67 69
0050  20 48 54 54 50 2f 31 2e  31 0d 0a
0060  20 74 65 73 74 70 68 70  2e 76 75
0070  2e 63 6f 6d 0d 0a 55 70  67 72 61
```

```
Hypertext Transfer Protocol: Protocol        Packets: 5548 · Displayed: 8 (0.1%)        Profile: Default
```

Examine the HTTP POST request payload for any parameters containing logininformation. The username and password may be encoded or encrypted.



```
No.    Time         Source          Destination     Protocol  Length  Info
  3457 828.377849   192.168.1.168   44.228.249.3    HTTP        443  GET /login.php HTTP/1.1
  3460 828.541510   44.228.249.3    192.168.1.168   HTTP       1374  HTTP/1.1 200 OK  (text/html)
  3545 840.305968   192.168.1.168   44.228.249.3    HTTP        443  GET /login.php HTTP/1.1
  3548 840.476337   44.228.249.3    192.168.1.168   HTTP       1374  HTTP/1.1 200 OK  (text/html)
  5024 1283.170984  192.168.1.168   44.228.249.3    HTTP         89  POST /userinfo.php HTTP/1.1  (application/x-www-form-ur…
  5027 1283.337979  44.228.249.3    192.168.1.168   HTTP        342  HTTP/1.1 302 Found  (text/html)
  5029 1283.377019  192.168.1.168   44.228.249.3    HTTP        490  GET /login.php HTTP/1.1
  5032 1283.542289  44.228.249.3    192.168.1.168   HTTP       1374  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 5024: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface en0, id
> Ethernet II, Src: Apple_a6:15:0c (14:7d:da:a6:15:0c), Dst: Arcadyan_09:d0:ec (60:8d:26:09:d
> Internet Protocol Version 4, Src: 192.168.1.168, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 49445, Dst Port: 80, Seq: 534, Ack: 1, Len: 23
> [2 Reassembled TCP Segments (556 bytes): #5023(533), #5024(23)]
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "admin"
  > Form item: "pass" = "admins"
```

```
0140  35 2e 30 20 28 4d 61 63  69 6e 74
0150  49 6e 74 65 6c 20 4d 61  63 20 4f
0160  30 5f 31 35 5f 37 29 20  41 70 70
0170  4b 69 74 2f 36 30 35 2e  31 2e 31
0180  54 4d 4c 2c 20 6c 69 6b  65 20 47
0190  20 56 65 72 73 69 6f 6e  2f 31 37
01a0  66 61 72 69 2f 36 30 35  2e 31 2e
01b0  65 66 65 72 65 72 3a 20  68 74 74
01c0  65 73 74 70 68 70 2e 76  75 6c 6e
01d0  6f 6d 2f 6c 6f 67 69 6e  2e 70 68
01e0  6e 74 65 6e 74 2d 4c 65  6e 67 74
01f0  0d 0a 41 63 63 65 70 74  2d 4c 61
0200  65 3a 20 65 6e 2d 47 42  2c 65 6e
```

HTML Form URL Encoded (urlencoded-form), 23 bytes

Packets: 7088 · Displayed: 8 (0.1%)

Profile: Default