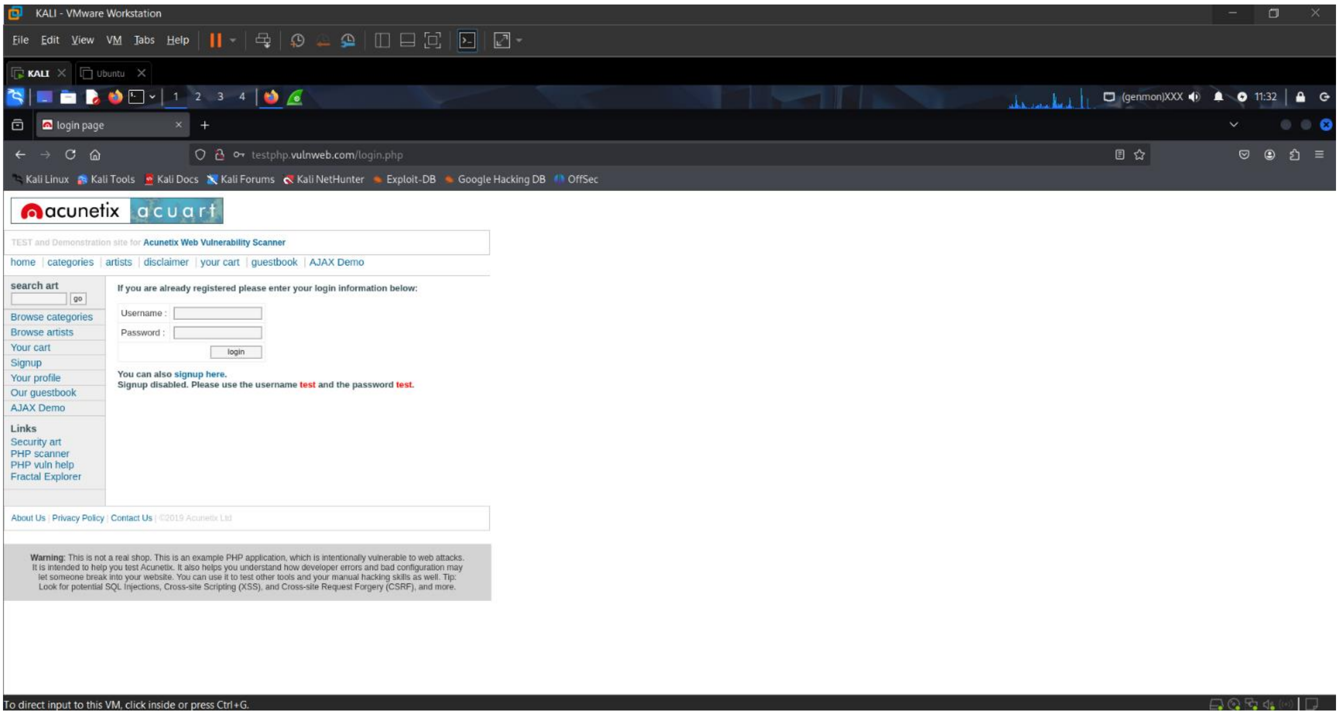
Network Packet Sniffing and Analysis

Capturing and analyse live network traffic to identify credentials or suspicious activity by Wireshark tool.

Target: vulbweb.com

Target IP: 44.228.249.3



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 below:

Username :
Password :
login

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

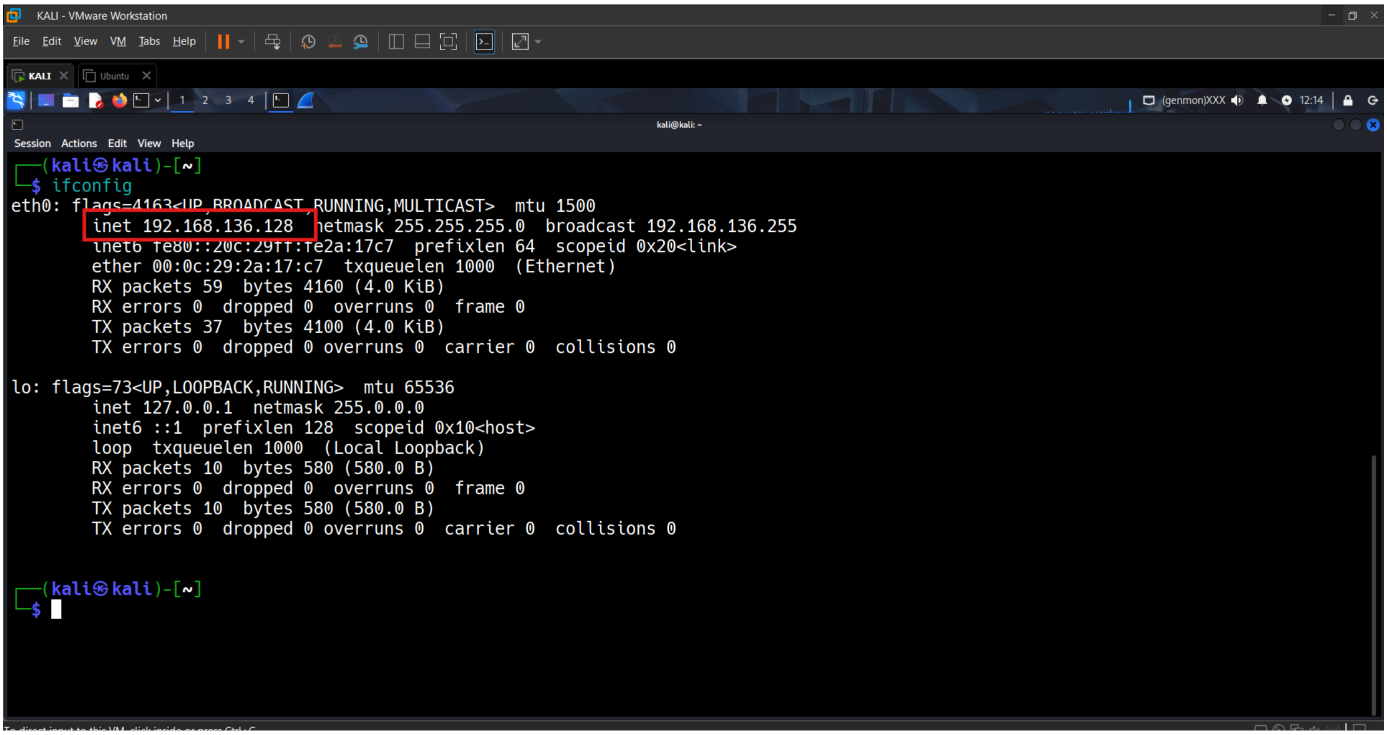
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable 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.

To direct input to this VM, click inside or press Ctrl+G.

Attacker: kali Linux

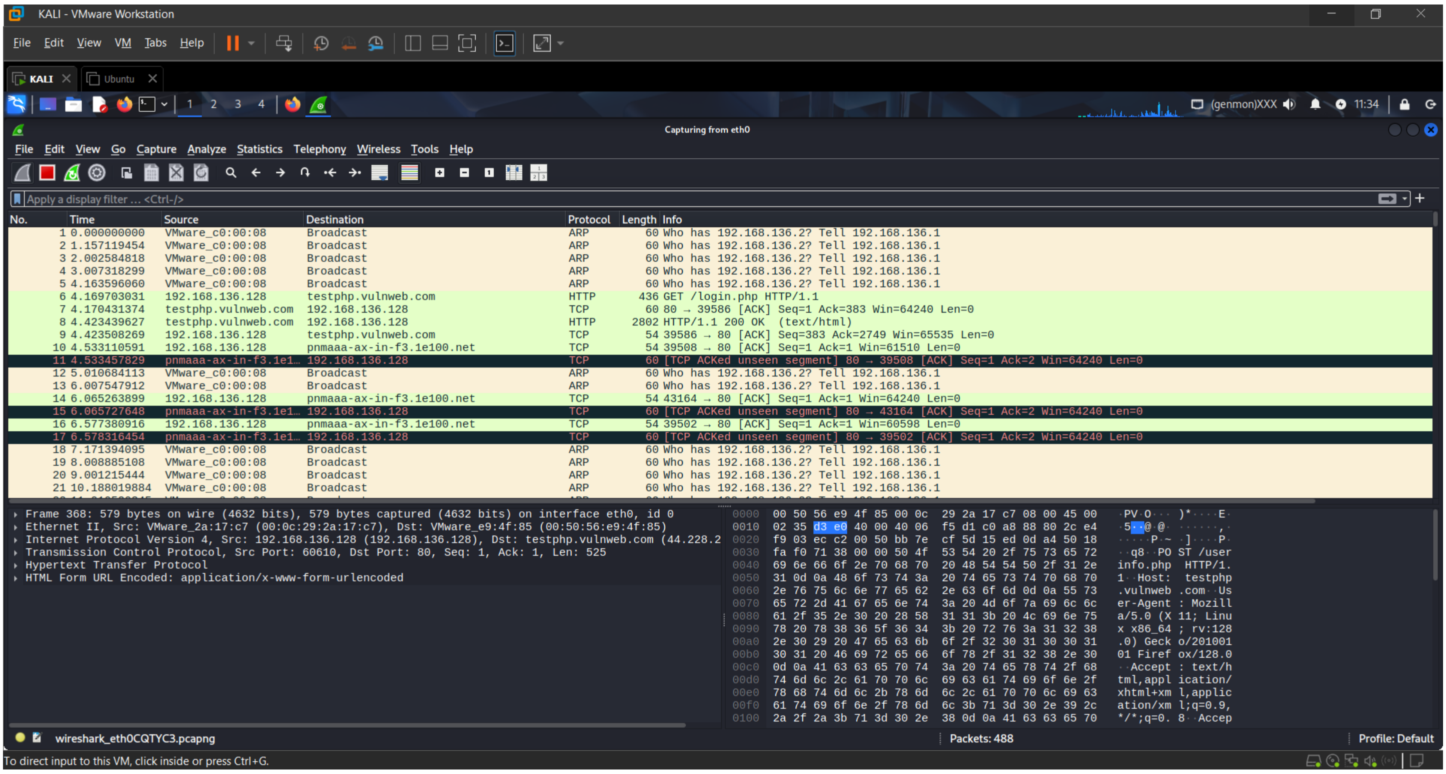
Attacker IP:192.168.136.128



KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
kali@kali: ~
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.136.128  netmask 255.255.255.0  broadcast 192.168.136.255
        inet6 fe80::20c:29ff:fe2a:17c7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2a:17:c7  txqueuelen 1000  (Ethernet)
        RX packets 59  bytes 4160 (4.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 4100 (4.0 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 10  bytes 580 (580.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 580 (580.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

The packets in below image are traffic generated by Wireshark tool

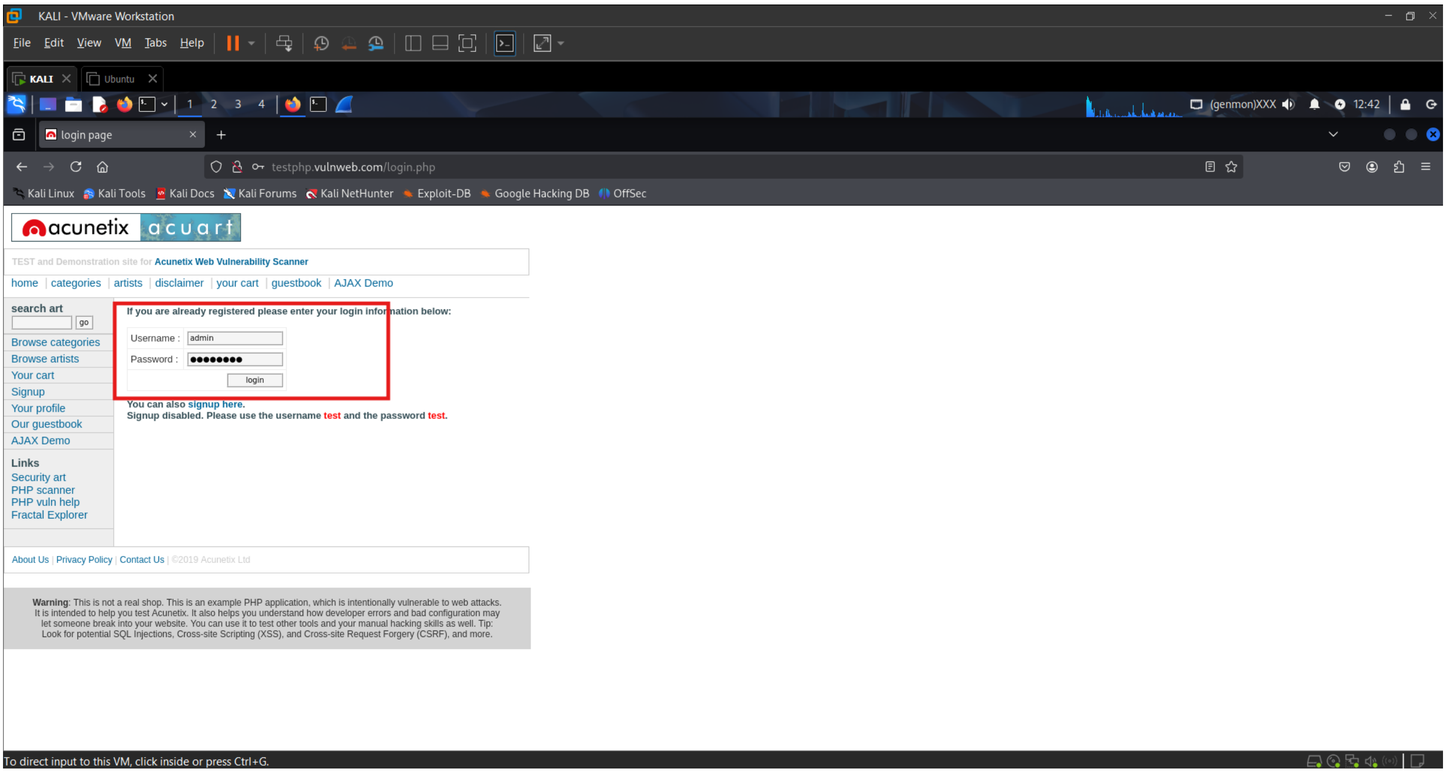

KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
(genmon)XXX
11:34
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
wireshark_eth0CQTYC3.pcapng
Packets: 488
Profile: Default
To direct input to this VM, click inside or press Ctrl+G.

```
No.  Time          Source                 Destination                  Protocol Length Info
   1 0.000000000   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   2 1.157119454   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   3 2.002584818   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   4 3.007318299   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   5 4.163596060   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   6 4.169703031   192.168.136.128        testphp.vulnweb.com          HTTP      436 GET /login.php HTTP/1.1
   7 4.170431374   testphp.vulnweb.com    192.168.136.128              TCP        60 80 → 39586 [ACK] Seq=1 Ack=383 Win=64240 Len=0
   8 4.423439627   testphp.vulnweb.com    192.168.136.128              HTTP     2802 HTTP/1.1 200 OK  (text/html)
   9 4.423508269   192.168.136.128        testphp.vulnweb.com          TCP        54 39586 → 80 [ACK] Seq=383 Ack=2749 Win=65535 Len=0
  10 4.533110591   192.168.136.128        pnmaaa-ax-in-f3.1e100.net    TCP        54 39508 → 80 [ACK] Seq=1 Ack=1 Win=61510 Len=0
  11 4.533457829   pnmaaa-ax-in-f3.1e1…   192.168.136.128              TCP        60 [TCP ACKed unseen segment] 80 → 39508 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  12 5.010684113   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  13 6.007547912   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  14 6.065263899   192.168.136.128        pnmaaa-ax-in-f3.1e100.net    TCP        54 43164 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  15 6.065727648   pnmaaa-ax-in-f3.1e1…   192.168.136.128              TCP        60 [TCP ACKed unseen segment] 80 → 43164 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  16 6.577380916   192.168.136.128        pnmaaa-ax-in-f3.1e100.net    TCP        54 39502 → 80 [ACK] Seq=1 Ack=1 Win=60598 Len=0
  17 6.578316454   pnmaaa-ax-in-f3.1e1…   192.168.136.128              TCP        60 [TCP ACKed unseen segment] 80 → 39502 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  18 7.171394095   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  19 8.008885108   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  20 9.001215444   VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  21 10.188019884  VMware_c0:00:08        Broadcast                    ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
```

```
› Frame 368: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128 (192.168.136.128), Dst: testphp.vulnweb.com (44.228.2
› Transmission Control Protocol, Src Port: 60610, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  00 50 56 e9 4f 85 00 0c  29 2a 17 c7 08 00 45 00   ·PV·O···  )*····E·
0010  02 35 d3 e0 40 00 40 06  f5 d1 c0 a8 88 80 2c e4   ·5··@·@·  ······,·
0020  f9 03 ec c2 00 50 bb 7e  cf 5d 15 ed 0d a4 50 18   ·····P·~  ·]····P·
0030  fa f0 71 38 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q8··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
```

Now try to login with random credentials in target website (vulnweb).



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

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 below:

Username :	admin
Password :	●●●●●●●●

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

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

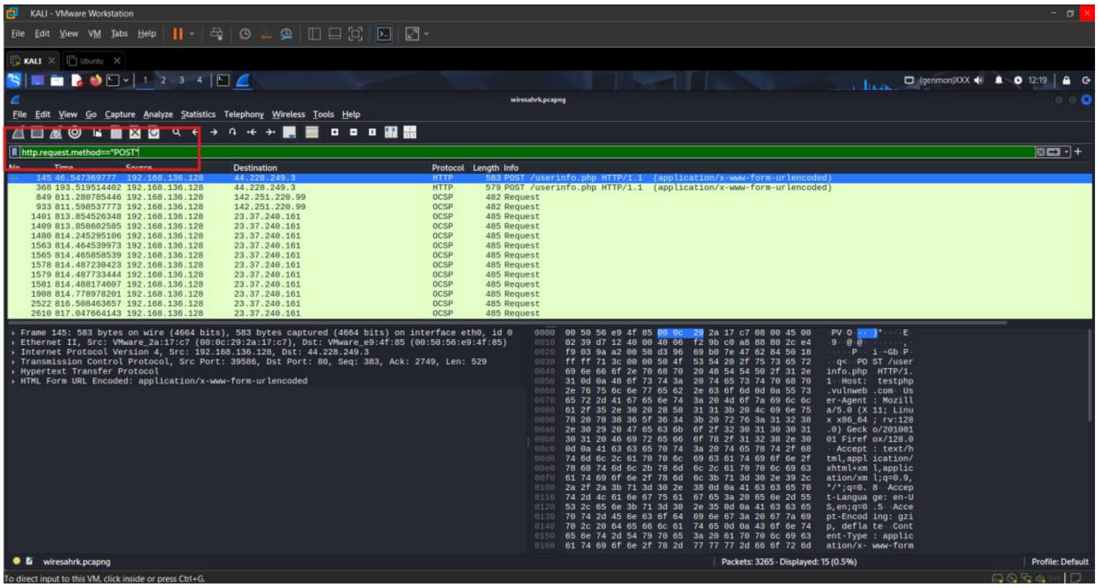
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other 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.

Now to inspect the packets we use filter to limit the packets to make the task easy.

Filter: http.request.method==”POST”

This filter will show packets which are http request and POST method.

POST method is where we send data to server, when we enter the credentials or user input then it is said to be POST method.



```
http.request.method=="POST"
No.  Time           Source           Destination      Protocol Length Info
 145 46.547369777   192.168.136.128  44.228.249.3     HTTP      583 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 368 193.519514402  192.168.136.128  44.228.249.3     HTTP      579 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 849 811.280785446  192.168.136.128  142.251.220.99   OCSP      482 Request
 933 811.598537773  192.168.136.128  142.251.220.99   OCSP      482 Request
1401 813.854526348  192.168.136.128  23.37.240.161    OCSP      485 Request
1409 813.858602585  192.168.136.128  23.37.240.161    OCSP      485 Request
1480 814.245295106  192.168.136.128  23.37.240.161    OCSP      485 Request
1563 814.464539973  192.168.136.128  23.37.240.161    OCSP      485 Request
1565 814.465858539  192.168.136.128  23.37.240.161    OCSP      485 Request
1578 814.487230423  192.168.136.128  23.37.240.161    OCSP      485 Request
1579 814.487733444  192.168.136.128  23.37.240.161    OCSP      485 Request
1581 814.488174607  192.168.136.128  23.37.240.161    OCSP      485 Request
1908 814.778978201  192.168.136.128  23.37.240.161    OCSP      485 Request
2522 816.508463657  192.168.136.128  23.37.240.161    OCSP      485 Request
2610 817.047664143  192.168.136.128  23.37.240.161    OCSP      485 Request
```

```
› Frame 145: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 39586, Dst Port: 80, Seq: 383, Ack: 2749, Len: 529
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  00 50 56 e9 4f 85 00 0c  29 2a 17 c7 08 00 45 00   ·PV·O···)*····E·
0010  02 39 d7 12 40 00 40 06  f2 9b c0 a8 88 80 2c e4   ·9··@·@·······,·
0020  f9 03 9a a2 00 50 d3 96  69 b0 7e 47 62 84 50 18   ·····P··i·~Gb·P·
0030  ff ff 71 3c 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q<··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
```

wiresahrk.pcapng | Packets: 3265 · Displayed: 15 (0.5%) | Profile: Default

KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
(genmon)XXX
12:19
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
To direct input to this VM, click inside or press Ctrl+G.

The 1st packet we had packet name “/userinfo.php” with HTTP (Hyper Text Transfer protocol) protocol.

In Transmission Control Protocol, we have

Source Port: 39586 (kali Linux),

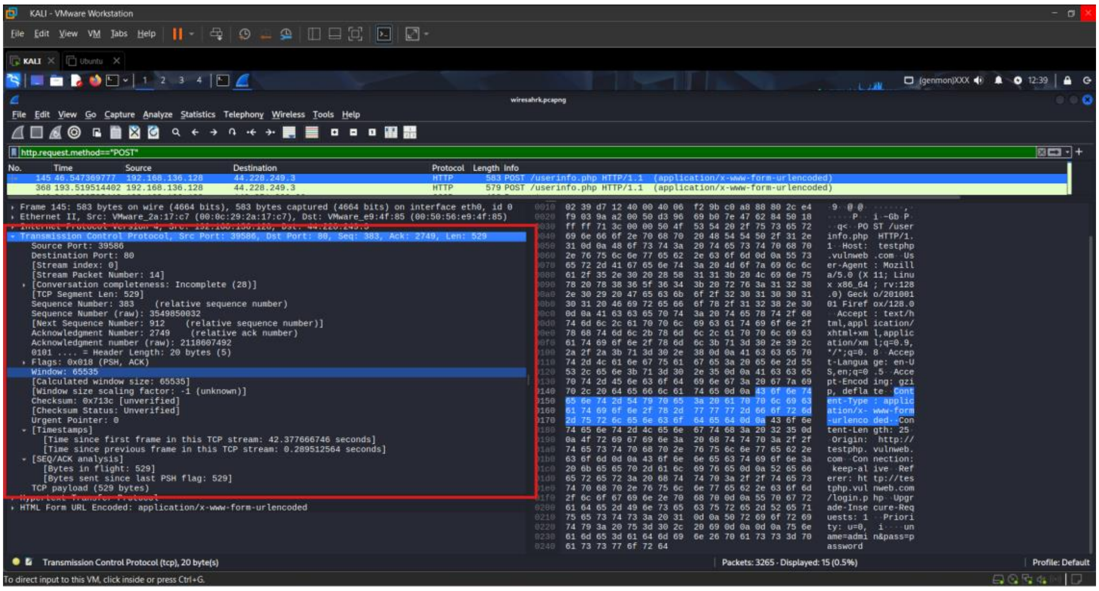
Destination Port: 80(target),

Seq: 383, Ack: 2749, Len: 529

IP version: IPV4

[SEQ/ACK analysis]

TCP payload and other details of packet as shown in below image.



```
http.request.method=="POST"
No.  Time           Source           Destination      Protocol Length Info
 145 46.547369777   192.168.136.128  44.228.249.3     HTTP      583 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 368 193.519514402  192.168.136.128  44.228.249.3     HTTP      579 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

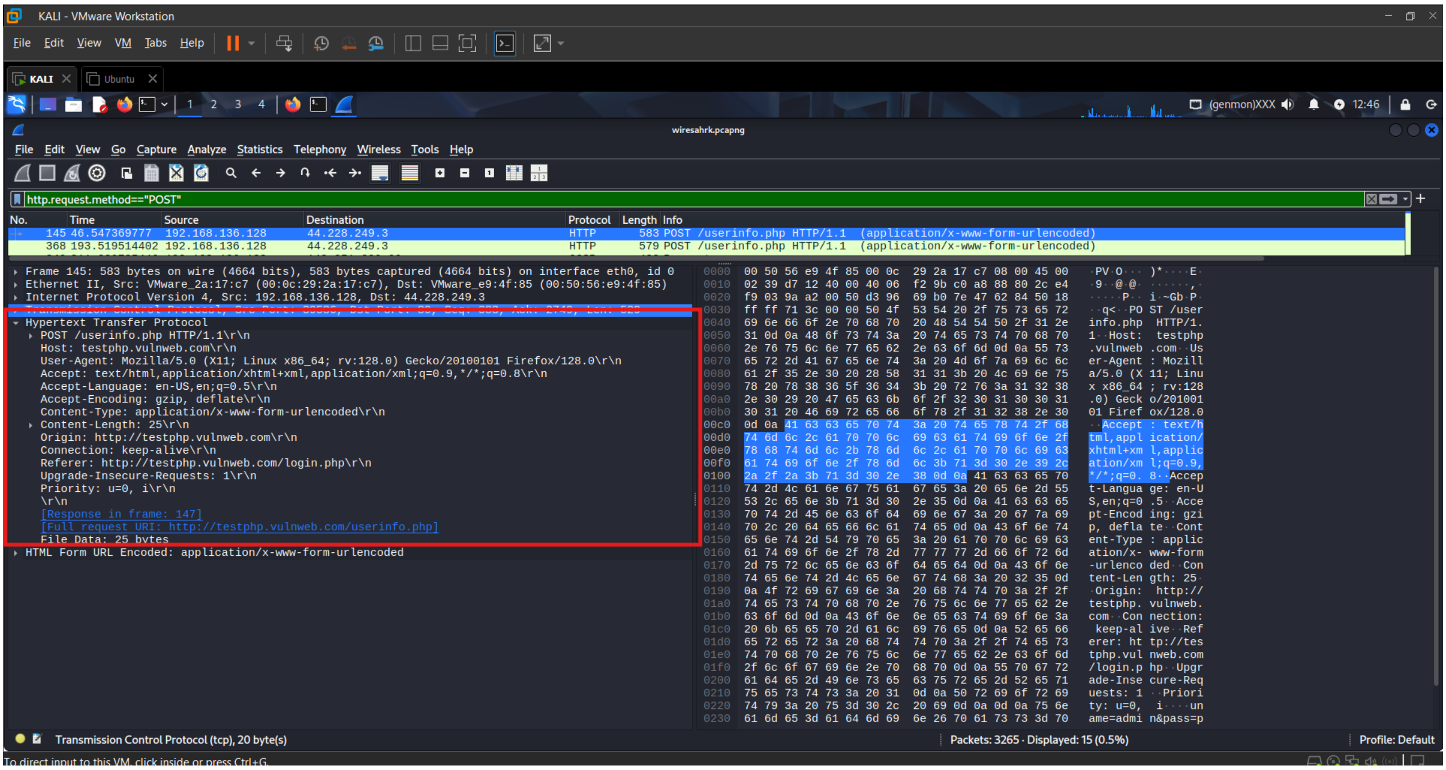
```
› Frame 145: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128, Dst: 44.228.249.3
⌄ Transmission Control Protocol, Src Port: 39586, Dst Port: 80, Seq: 383, Ack: 2749, Len: 529
    Source Port: 39586
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 14]
  › [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 529]
    Sequence Number: 383    (relative sequence number)
    Sequence Number (raw): 3549850032
    [Next Sequence Number: 912    (relative sequence number)]
    Acknowledgment Number: 2749    (relative ack number)
    Acknowledgment number (raw): 2118607492
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x713c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 42.377666746 seconds]
      [Time since previous frame in this TCP stream: 0.289512564 seconds]
  ⌄ [SEQ/ACK analysis]
      [Bytes in flight: 529]
      [Bytes sent since last PSH flag: 529]
    TCP payload (529 bytes)
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0010  02 39 d7 12 40 00 40 06  f2 9b c0 a8 88 80 2c e4   ·9··@·@·······,·
0020  f9 03 9a a2 00 50 d3 96  69 b0 7e 47 62 84 50 18   ·····P··i·~Gb·P·
0030  ff ff 71 3c 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q<··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
0170  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco ded··Con
0180  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 35 0d   tent-Len gth: 25·
0190  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
01a0  74 65 73 74 70 68 70 2e  76 75 6c 6e 77 65 62 2e   testphp. vulnweb.
01b0  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con nection:
01c0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 52 65 66    keep-al ive··Ref
01d0  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 74 65 73   erer: ht tp://tes
01e0  74 70 68 70 2e 76 75 6c  6e 77 65 62 2e 63 6f 6d   tphp.vul nweb.com
01f0  2f 6c 6f 67 69 6e 2e 70  68 70 0d 0a 55 70 67 72   /login.p hp··Upgr
0200  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
0210  75 65 73 74 73 3a 20 31  0d 0a 50 72 69 6f 72 69   uests: 1 ··Priori
0220  74 79 3a 20 75 3d 30 2c  20 69 0d 0a 0d 0a 75 6e   ty: u=0,  i····un
0230  61 6d 65 3d 61 64 6d 69  6e 26 70 61 73 73 3d 70   ame=admi n&pass=p
0240  61 73 73 77 6f 72 64                               assword
```

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 3265 · Displayed: 15 (0.5%) | Profile: Default

KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
(genmon)XXX
12:39
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
To direct input to this VM, click inside or press Ctrl+G.

If we inspect Hypertext Transfer Protocol we have version, URL and other details of target website as shown in below image.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
1 2 3 4
(genmon)XXX
12:46
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method=="POST"

No.  Time          Source           Destination    Protocol Length Info
145 46.547369777  192.168.136.128  44.228.249.3   HTTP     583 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
368 193.519514402 192.168.136.128  44.228.249.3   HTTP     579 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

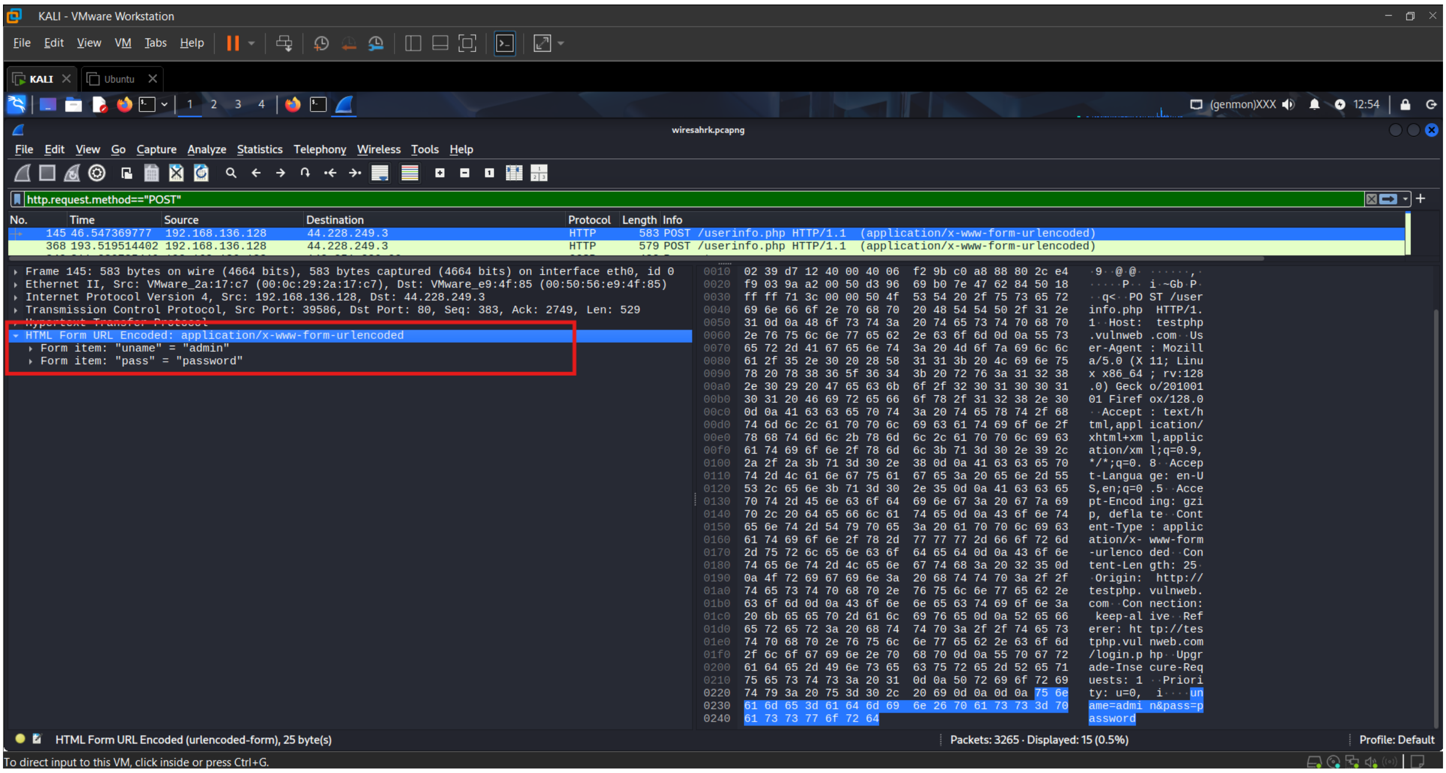
```
› Frame 145: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 39586, Dst Port: 80, Seq: 383, Ack: 2749, Len: 529
⌄ Hypertext Transfer Protocol
  › POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  › Content-Length: 25\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 147]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 25 bytes
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  00 50 56 e9 4f 85 00 0c  29 2a 17 c7 08 00 45 00   ·PV·O···  )*····E·
0010  02 39 d7 12 40 00 40 06  f2 9b c0 a8 88 80 2c e4   ·9··@·@·  ······,·
0020  f9 03 9a a2 00 50 d3 96  69 b0 7e 47 62 84 50 18   ·····P··  i·~Gb·P·
0030  ff ff 71 3c 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q<··PO  ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php   HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:   testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb  .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent  : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X  11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64  ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck  o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef  ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept  : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl  ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm  l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm  l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0.  8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua  ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0  .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod  ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla  te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type  : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x-  www-form
0170  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco  ded··Con
0180  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 35 0d   tent-Len  gth: 25·
0190  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:   http://
01a0  74 65 73 74 70 68 70 2e  76 75 6c 6e 77 65 62 2e   testphp.  vulnweb.
01b0  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con  nection:
01c0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 52 65 66    keep-al  ive··Ref
01d0  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 74 65 73   erer: ht  tp://tes
01e0  74 70 68 70 2e 76 75 6c  6e 77 65 62 2e 63 6f 6d   tphp.vul  nweb.com
01f0  2f 6c 6f 67 69 6e 2e 70  68 70 0d 0a 55 70 67 72   /login.p  hp··Upgr
0200  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse  cure-Req
0210  75 65 73 74 73 3a 20 31  0d 0a 50 72 69 6f 72 69   uests: 1  ··Priori
0220  74 79 3a 20 75 3d 30 2c  20 69 0d 0a 0d 0a 75 6e   ty: u=0,   i····un
0230  61 6d 65 3d 61 64 6d 69  6e 26 70 61 73 73 3d 70   ame=admi  n&pass=p
```

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 3265 · Displayed: 15 (0.5%) | Profile: Default

To direct input to this VM, click inside or press Ctrl+G.

If you see HTML form URL Encoded, inspect it there you see the plan text of credentials you gave in target website as shown in below image.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
1 2 3 4
(genmon)XXX
12:54
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

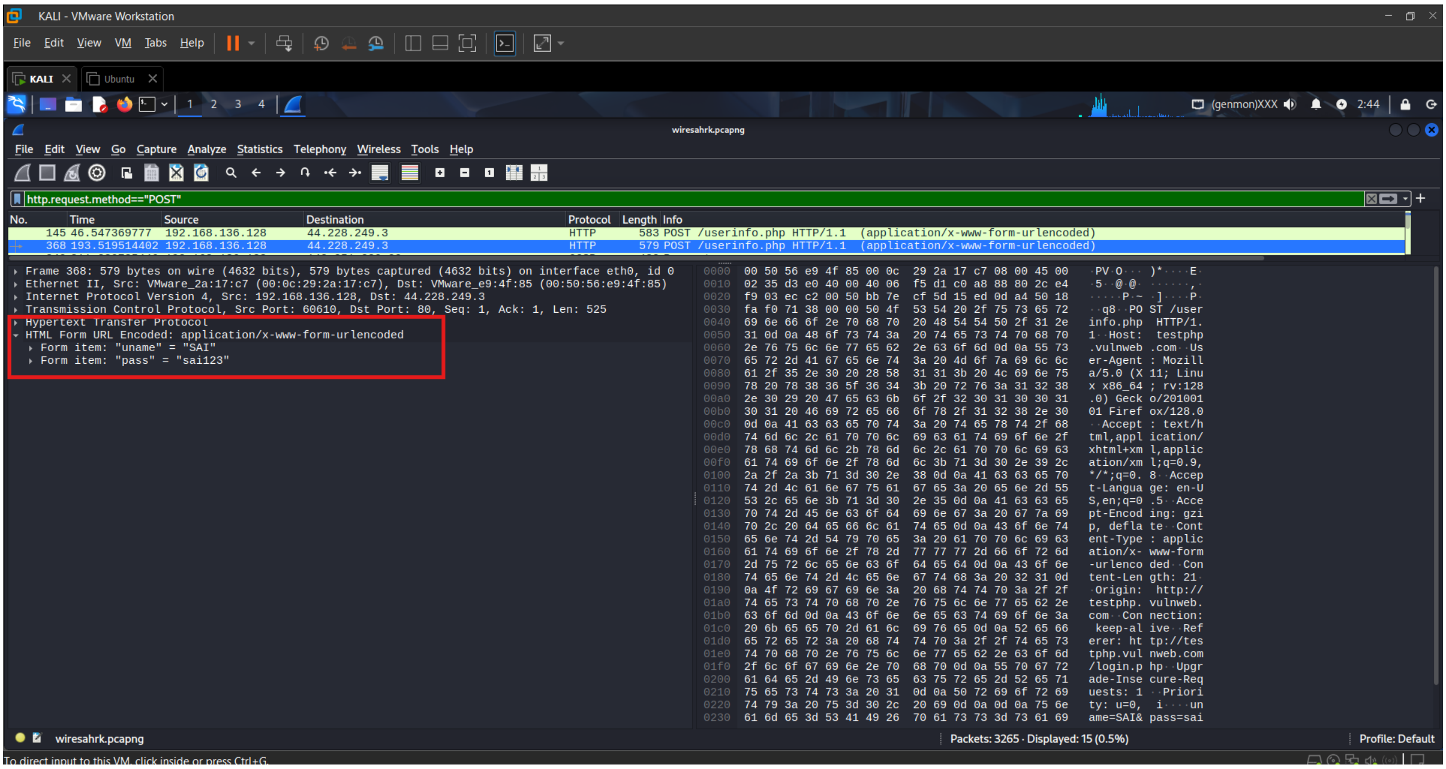
```
http.request.method=="POST"

No.  Time          Source           Destination    Protocol Length Info
145 46.547369777  192.168.136.128  44.228.249.3   HTTP     583 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
368 193.519514402 192.168.136.128  44.228.249.3   HTTP     579 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

```
› Frame 145: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 39586, Dst Port: 80, Seq: 383, Ack: 2749, Len: 529
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "admin"
  › Form item: "pass" = "password"
```

```
0010  02 39 d7 12 40 00 40 06  f2 9b c0 a8 88 80 2c e4   ·9··@·@·  ······,·
0020  f9 03 9a a2 00 50 d3 96  69 b0 7e 47 62 84 50 18   ·····P··  i·~Gb·P·
0030  ff ff 71 3c 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q<··PO  ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php   HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:   testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb  .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent  : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X  11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64  ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck  o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef  ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept  : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl  ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm  l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm  l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0.  8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua  ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0  .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod  ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla  te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type  : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x-  www-form
0170  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco  ded··Con
0180  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 35 0d   tent-Len  gth: 25·
0190  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:   http://
01a0  74 65 73 74 70 68 70 2e  76 75 6c 6e 77 65 62 2e   testphp.  vulnweb.
01b0  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con  nection:
01c0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 52 65 66    keep-al  ive··Ref
01d0  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 74 65 73   erer: ht  tp://tes
01e0  74 70 68 70 2e 76 75 6c  6e 77 65 62 2e 63 6f 6d   tphp.vul  nweb.com
01f0  2f 6c 6f 67 69 6e 2e 70  68 70 0d 0a 55 70 67 72   /login.p  hp··Upgr
0200  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse  cure-Req
0210  75 65 73 74 73 3a 20 31  0d 0a 50 72 69 6f 72 69   uests: 1  ··Priori
0220  74 79 3a 20 75 3d 30 2c  20 69 0d 0a 0d 0a 75 6e   ty: u=0,   i····un
0230  61 6d 65 3d 61 64 6d 69  6e 26 70 61 73 73 3d 70   ame=admi  n&pass=p
0240  61 73 73 77 6f 72 64                               assword
```

HTML Form URL Encoded (urlencoded-form), 25 byte(s) | Packets: 3265 · Displayed: 15 (0.5%) | Profile: Default

To direct input to this VM, click inside or press Ctrl+G.



```
http.request.method=="POST"

No.  Time           Source           Destination    Protocol Length Info
 145 46.547369777   192.168.136.128  44.228.249.3   HTTP      583 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 368 193.519514402  192.168.136.128  44.228.249.3   HTTP      579 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

```
› Frame 368: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
› Internet Protocol Version 4, Src: 192.168.136.128, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 60610, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "SAI"
  › Form item: "pass" = "sai123"
```

```
0000  00 50 56 e9 4f 85 00 0c  29 2a 17 c7 08 00 45 00   ·PV·O··· )*····E·
0010  02 35 d3 e0 40 00 40 06  f5 d1 c0 a8 88 80 2c e4   ·5··@·@· ······,·
0020  f9 03 ec c2 00 50 bb 7e  cf 5d 15 ed 0d a4 50 18   ·····P·~ ·]····P·
0030  fa f0 71 38 00 00 50 4f  53 54 20 2f 75 73 65 72   ··q8··PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
0090  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 32 38   x x86_64 ; rv:128
00a0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00b0  30 31 20 46 69 72 65 66  6f 78 2f 31 32 38 2e 30   01 Firef ox/128.0
00c0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00d0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
00e0  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
00f0  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0100  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 41 63 63 65 70   */*;q=0. 8··Accep
0110  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
0120  53 2c 65 6e 3b 71 3d 30  2e 35 0d 0a 41 63 63 65   S,en;q=0 .5··Acce
0130  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0140  70 2c 20 64 65 66 6c 61  74 65 0d 0a 43 6f 6e 74   p, defla te··Cont
0150  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0160  61 74 69 6f 6e 2f 78 2d  77 77 77 2d 66 6f 72 6d   ation/x- www-form
0170  2d 75 72 6c 65 6e 63 6f  64 65 64 0d 0a 43 6f 6e   -urlenco ded··Con
0180  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 32 31 0d   tent-Len gth: 21·
0190  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
01a0  74 65 73 74 70 68 70 2e  76 75 6c 6e 77 65 62 2e   testphp. vulnweb.
01b0  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con nection:
01c0  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 52 65 66    keep-al ive··Ref
01d0  65 72 65 72 3a 20 68 74  74 70 3a 2f 2f 74 65 73   erer: ht tp://tes
01e0  74 70 68 70 2e 76 75 6c  6e 77 65 62 2e 63 6f 6d   tphp.vul nweb.com
01f0  2f 6c 6f 67 69 6e 2e 70  68 70 0d 0a 55 70 67 72   /login.p hp··Upgr
0200  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
0210  75 65 73 74 73 3a 20 31  0d 0a 50 72 69 6f 72 69   uests: 1 ··Priori
0220  74 79 3a 20 75 3d 30 2c  20 69 0d 0a 0d 0a 75 6e   ty: u=0,  i····un
0230  61 6d 65 3d 53 41 49 26  70 61 73 73 3d 73 61 69   ame=SAI& pass=sai
```

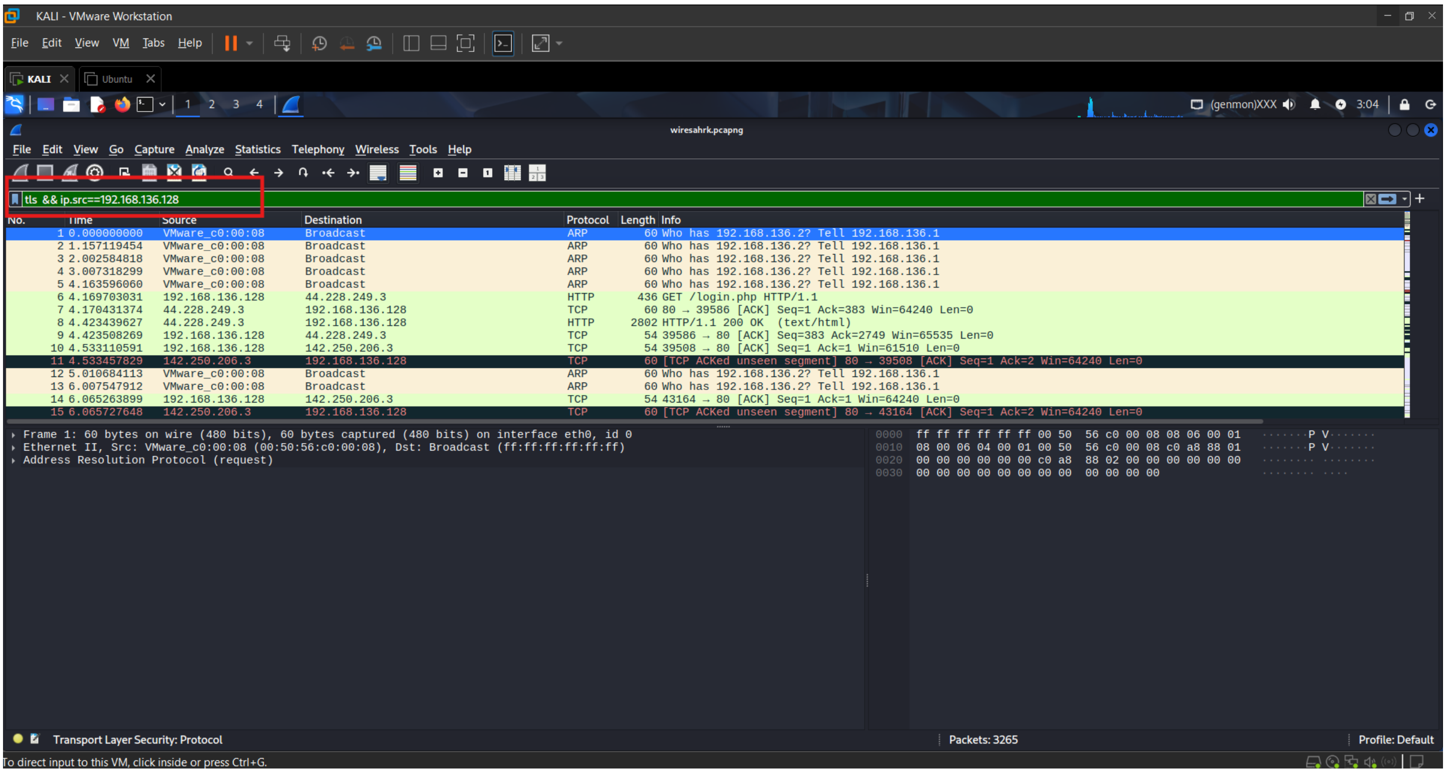
```
wiresahrk.pcapng          Packets: 3265 · Displayed: 15 (0.5%)          Profile: Default
```

KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
1 2 3 4
(genmon)XXX
2:44
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
To direct input to this VM, click inside or press Ctrl+G.

This says the website is vulnerable as the website discloses the credentials in a plain text.

Let’s check on another website (Instagram) how credentials are encrypted.

Use filter - tls && ip.src==192.168.136.128



```
tls && ip.src==192.168.136.128

No.  Time          Source           Destination      Protocol Length Info
   1 0.000000000   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   2 1.157119454   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   3 2.002584818   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   4 3.007318299   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   5 4.163596060   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
   6 4.169703031   192.168.136.128  44.228.249.3     HTTP      436 GET /login.php HTTP/1.1
   7 4.170431374   44.228.249.3     192.168.136.128  TCP        60 80 → 39586 [ACK] Seq=1 Ack=383 Win=64240 Len=0
   8 4.423439627   44.228.249.3     192.168.136.128  HTTP     2802 HTTP/1.1 200 OK  (text/html)
   9 4.423508269   192.168.136.128  44.228.249.3     TCP        54 39586 → 80 [ACK] Seq=383 Ack=2749 Win=65535 Len=0
  10 4.533110591   192.168.136.128  142.250.206.3    TCP        54 39508 → 80 [ACK] Seq=1 Ack=1 Win=61510 Len=0
  11 4.533457829   142.250.206.3    192.168.136.128  TCP        60 [TCP ACKed unseen segment] 80 → 39508 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  12 5.010684113   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  13 6.007547912   VMware_c0:00:08  Broadcast        ARP        60 Who has 192.168.136.2? Tell 192.168.136.1
  14 6.065263899   192.168.136.128  142.250.206.3    TCP        54 43164 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  15 6.065727648   142.250.206.3    192.168.136.128  TCP        60 [TCP ACKed unseen segment] 80 → 43164 [ACK] Seq=1 Ack=2 Win=64240 Len=0
```

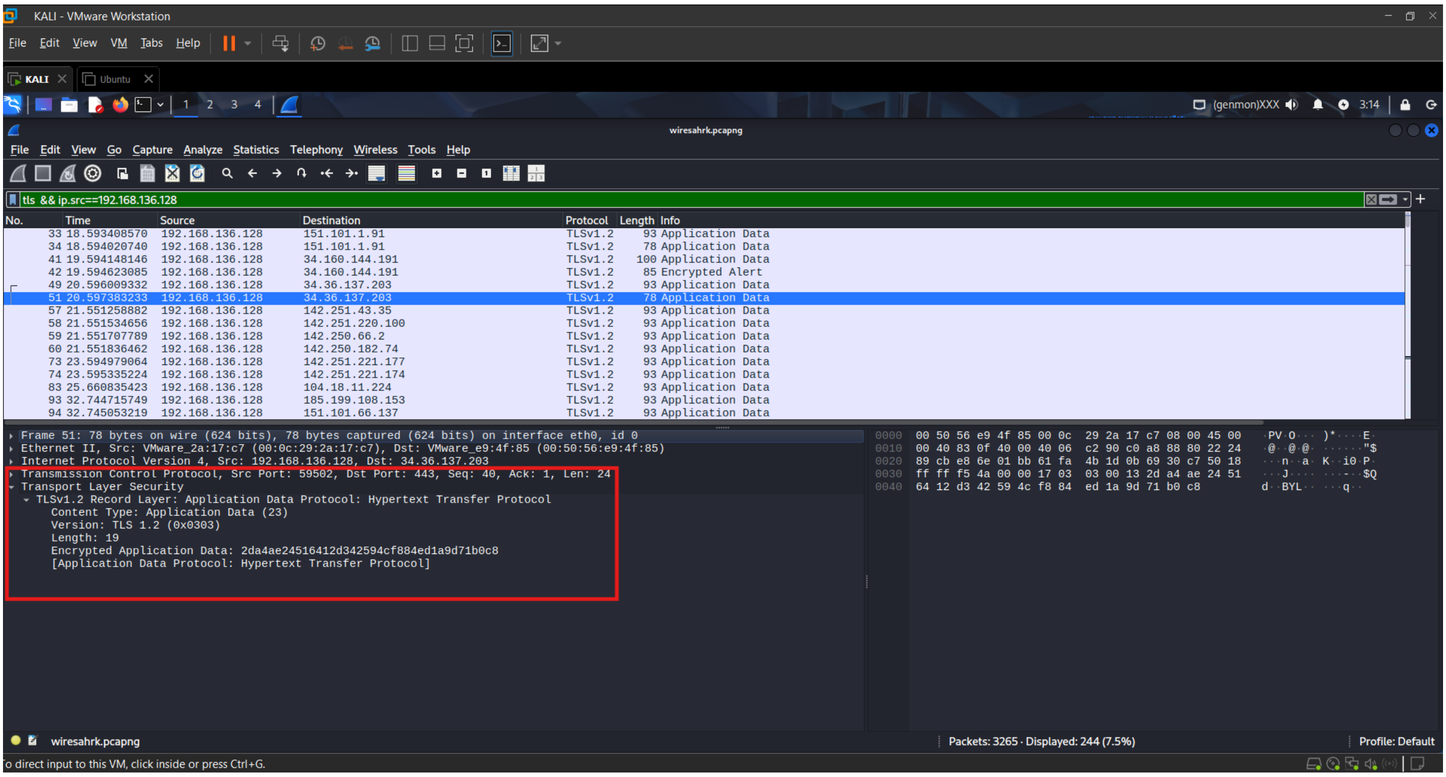
```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   ·······P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0 a8 88 01   ·······P V·······
0020  00 00 00 00 00 00 c0 a8  88 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

```
Transport Layer Security: Protocol          Packets: 3265          Profile: Default
```

KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
1 2 3 4
(genmon)XXX
3:04
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
To direct input to this VM, click inside or press Ctrl+G.

Now check any application data packet details there you see encrypted data in Transport Layer Security (TLS) as shown in below figure.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
Ubuntu
1 2 3 4
(genmon)XXX
3:14
wiresahrk.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls && ip.src==192.168.136.128
```

```
No.  Time          Source            Destination       Protocol  Length Info
  33 18.593408570  192.168.136.128   151.101.1.91      TLSv1.2      93 Application Data
  34 18.594020740  192.168.136.128   151.101.1.91      TLSv1.2      78 Application Data
  41 19.594148146  192.168.136.128   34.160.144.191    TLSv1.2     100 Application Data
  42 19.594623085  192.168.136.128   34.160.144.191    TLSv1.2      85 Encrypted Alert
  49 20.596009332  192.168.136.128   34.36.137.203     TLSv1.2      93 Application Data
  51 20.597383233  192.168.136.128   34.36.137.203     TLSv1.2      78 Application Data
  57 21.551258882  192.168.136.128   142.251.43.35     TLSv1.2      93 Application Data
  58 21.551534656  192.168.136.128   142.251.220.100   TLSv1.2      93 Application Data
  59 21.551707789  192.168.136.128   142.250.66.2      TLSv1.2      93 Application Data
  60 21.551836462  192.168.136.128   142.250.182.74    TLSv1.2      93 Application Data
  73 23.594979064  192.168.136.128   142.251.221.177   TLSv1.2      93 Application Data
  74 23.595335224  192.168.136.128   142.251.221.174   TLSv1.2      93 Application Data
  83 25.660835423  192.168.136.128   104.18.11.224     TLSv1.2      93 Application Data
  93 32.744715749  192.168.136.128   185.199.108.153   TLSv1.2      93 Application Data
  94 32.745053219  192.168.136.128   151.101.66.137    TLSv1.2      93 Application Data
```

```
▸ Frame 51: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_2a:17:c7 (00:0c:29:2a:17:c7), Dst: VMware_e9:4f:85 (00:50:56:e9:4f:85)
▸ Internet Protocol Version 4, Src: 192.168.136.128, Dst: 34.36.137.203
▸ Transmission Control Protocol, Src Port: 59502, Dst Port: 443, Seq: 40, Ack: 1, Len: 24
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 19
      Encrypted Application Data: 2da4ae24516412d342594cf884ed1a9d71b0c8
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  00 50 56 e9 4f 85 00 0c  29 2a 17 c7 08 00 45 00   ·PV·O···)*····E·
0010  00 40 83 0f 40 00 40 06  c2 90 c0 a8 88 80 22 24   ·@··@·@·······"$
0020  89 cb e8 6e 01 bb 61 fa  4b 1d 0b 69 30 c7 50 18   ···n··a·K··i0·P·
0030  ff ff f5 4a 00 00 17 03  03 00 13 2d a4 ae 24 51   ···J·······-··$Q
0040  64 12 d3 42 59 4c f8 84  ed 1a 9d 71 b0 c8         d··BYL·····q··
```

wiresahrk.pcapng | Packets: 3265 · Displayed: 244 (7.5%) | Profile: Default

o direct input to this VM, click inside or press Ctrl+G.

This how the data should be encrypted as shown in above image.