Wireshark Sniffing Task

Tool Used: Wireshark
Target: Website (http://testphp.vulnweb.com/login.php)

Steps Performed:

1. **Started Wireshark**
   Launched Wireshark to capture network traffic.

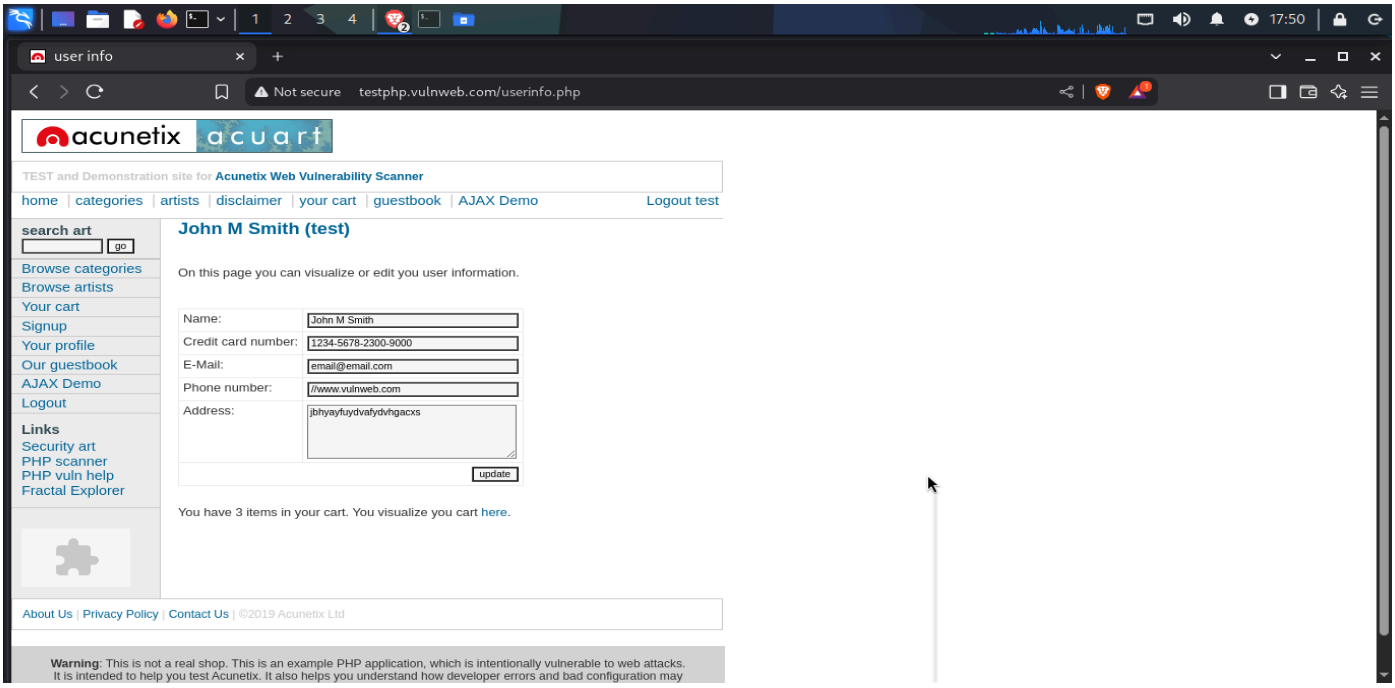
2. **Visited the Target Website**
   Accessed the website in a browser while Wireshark was running.

3. **Captured Packets**
   Let Wireshark collect all network packets during the visit.

4. **Analyzed Packets**
   Searched through captured packets, especially looking for HTTP traffic.

   (http.request.method == "POST")

5. **Found Sensitive Info**
   Discovered login credentials (like username and password) being sent in plain text.



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

John M Smith (test)

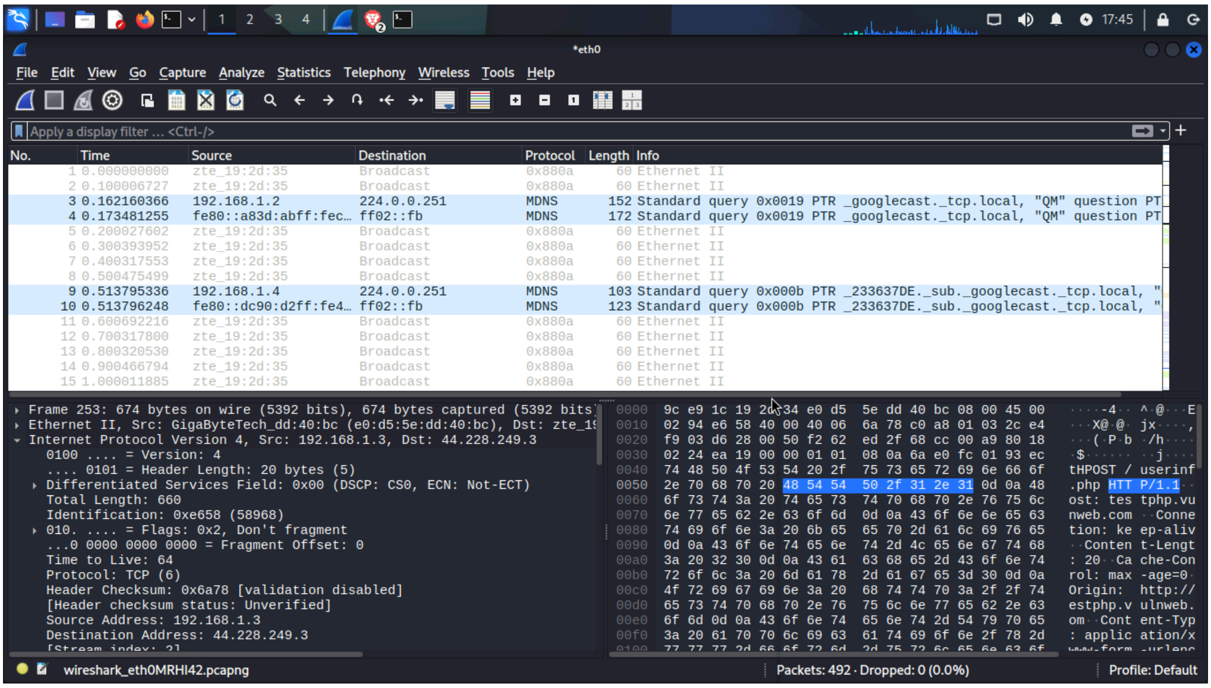
On this page you can visualize or edit you user information.

Name:	John M Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	//www.vulnweb.com
Address:	jbhyayfuydvafydvhgacxs

You have 3 items in your cart. You visualize you cart here.

©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



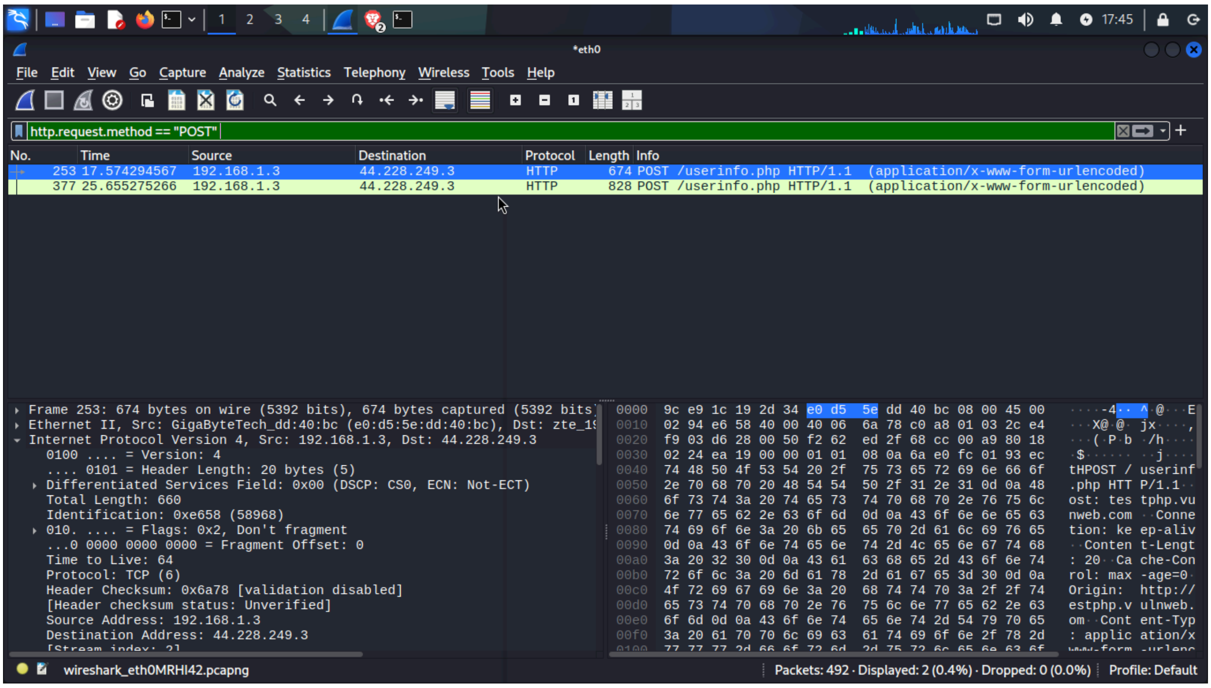
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
17:45

```
No.  Time          Source                    Destination   Protocol Length Info
   1 0.000000000   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   2 0.100006727   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   3 0.162160366   192.168.1.2               224.0.0.251   MDNS       152 Standard query 0x0019 PTR _googlecast._tcp.local, "QM" question PT
   4 0.173481255   fe80::a83d:abff:fec…      ff02::fb      MDNS       172 Standard query 0x0019 PTR _googlecast._tcp.local, "QM" question PT
   5 0.200027602   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   6 0.300393952   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   7 0.400317553   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   8 0.500475499   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
   9 0.513795336   192.168.1.4               224.0.0.251   MDNS       103 Standard query 0x000b PTR _233637DE._sub._googlecast._tcp.local, "
  10 0.513796248   fe80::dc90:d2ff:fe4…      ff02::fb      MDNS       123 Standard query 0x000b PTR _233637DE._sub._googlecast._tcp.local, "
  11 0.600692216   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
  12 0.700317800   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
  13 0.800320530   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
  14 0.900466794   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
  15 1.000011885   zte_19:2d:35              Broadcast     0x880a      60 Ethernet II
```

```
› Frame 253: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits
› Ethernet II, Src: GigaByteTech_dd:40:bc (e0:d5:5e:dd:40:bc), Dst: zte_19
⌄ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 44.228.249.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 660
    Identification: 0xe658 (58968)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x6a78 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 44.228.249.3
    [Stream index: 2]
```

```
0000  9c e9 1c 19 2d 34 e0 d5  5e dd 40 bc 08 00 45 00   ·····-4·· ^·@···E
0010  02 94 e6 58 40 00 40 06  6a 78 c0 a8 01 03 2c e4   ···X@·@· jx····,
0020  f9 03 d6 28 00 50 f2 62  ed 2f 68 cc 00 a9 80 18   ···(·P·b ·/h····
0030  02 24 ea 19 00 00 01 01  08 0a 6a e0 fc 01 93 ec   ·$······ ··j·····
0040  74 48 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   tHPOST / userinf
0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··
0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vu
0070  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Conne
0080  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-aliv
0090  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Lengt
00a0  3a 20 32 30 0d 0a 43 61  63 68 65 2d 43 6f 6e 74   : 20··Ca che-Con
00b0  72 6f 6c 3a 20 6d 61 78  2d 61 67 65 3d 30 0d 0a   rol: max -age=0·
00c0  4f 72 69 67 69 6e 3a 20  68 74 74 70 3a 2f 2f 74   Origin:  http://
00d0  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.
00e0  6f 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   om··Cont ent-Typ
00f0  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 2d   : applic ation/x
0100  77 77 77 2d 66 6f 72 6d  2d 75 72 6c 65 6e 63 6f   www-form -urlenc
```

wireshark_eth0MRHI42.pcapng   Packets: 492 · Dropped: 0 (0.0%)   Profile: Default



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
17:45

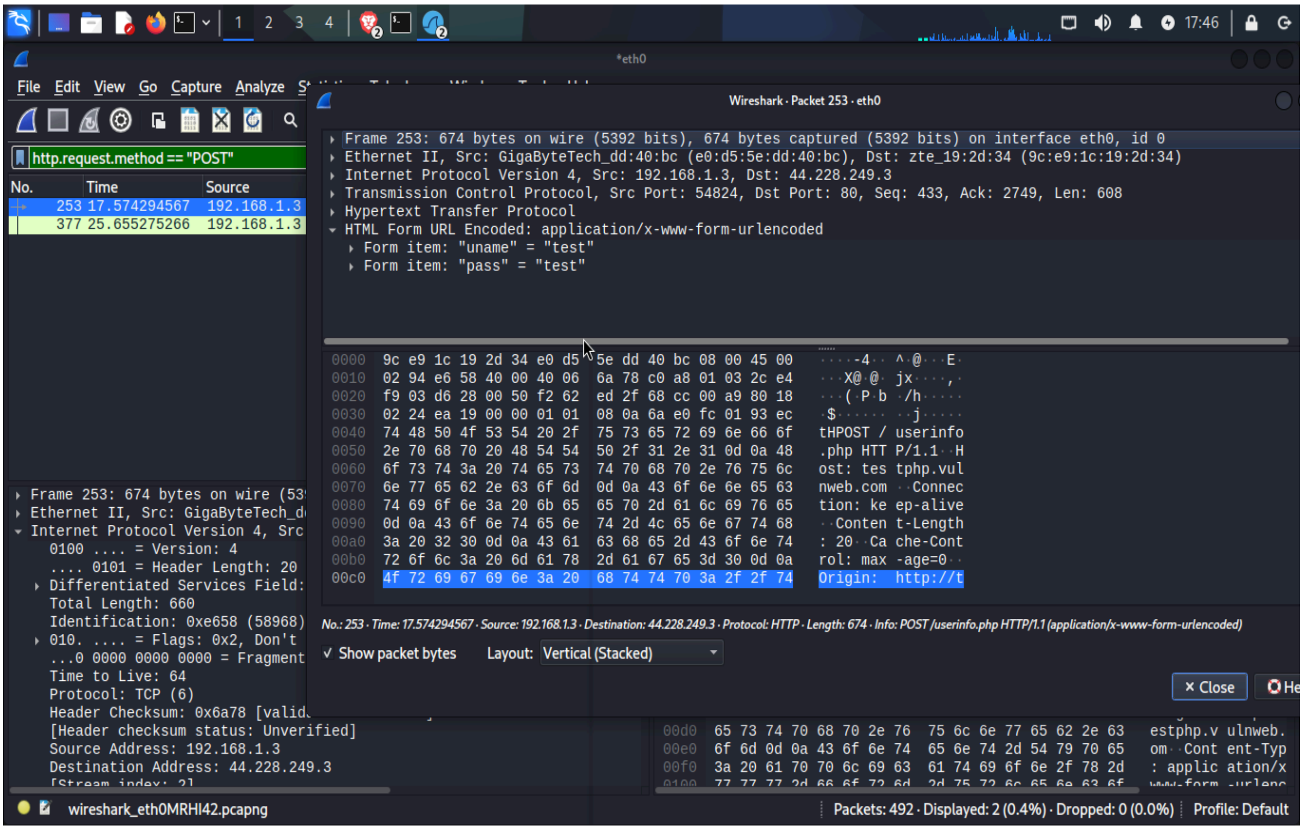
http.request.method == "POST"

```
No.  Time          Source        Destination    Protocol Length Info
 253 17.574294567  192.168.1.3   44.228.249.3   HTTP        674 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 377 25.655275266  192.168.1.3   44.228.249.3   HTTP        828 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

```
› Frame 253: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits
› Ethernet II, Src: GigaByteTech_dd:40:bc (e0:d5:5e:dd:40:bc), Dst: zte_19
⌄ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 44.228.249.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 660
    Identification: 0xe658 (58968)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x6a78 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.3
    Destination Address: 44.228.249.3
    [Stream index: 2]
```

```
0000  9c e9 1c 19 2d 34 e0 d5  5e dd 40 bc 08 00 45 00   ·····-4·· ^·@···E
0010  02 94 e6 58 40 00 40 06  6a 78 c0 a8 01 03 2c e4   ···X@·@· jx····,
0020  f9 03 d6 28 00 50 f2 62  ed 2f 68 cc 00 a9 80 18   ···(·P·b ·/h····
0030  02 24 ea 19 00 00 01 01  08 0a 6a e0 fc 01 93 ec   ·$······ ··j·····
0040  74 48 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   tHPOST / userinf
0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··
0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vu
0070  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Conne
0080  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-aliv
0090  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Lengt
00a0  3a 20 32 30 0d 0a 43 61  63 68 65 2d 43 6f 6e 74   : 20··Ca che-Con
00b0  72 6f 6c 3a 20 6d 61 78  2d 61 67 65 3d 30 0d 0a   rol: max -age=0·
00c0  4f 72 69 67 69 6e 3a 20  68 74 74 70 3a 2f 2f 74   Origin:  http://
00d0  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.
00e0  6f 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   om··Cont ent-Typ
00f0  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 2d   : applic ation/x
0100  77 77 77 2d 66 6f 72 6d  2d 75 72 6c 65 6e 63 6f   www-form -urlenc
```

wireshark_eth0MRHI42.pcapng   Packets: 492 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)   Profile: Default



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

```
No.   Time          Source
253 17.574294567  192.168.1.3
377 25.655275266  192.168.1.3
```

```
Frame 253: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface eth0, id 0
Ethernet II, Src: GigaByteTech_dd:40:bc (e0:d5:5e:dd:40:bc), Dst: zte_19:2d:34 (9c:e9:1c:19:2d:34)
Internet Protocol Version 4, Src: 192.168.1.3, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54824, Dst Port: 80, Seq: 433, Ack: 2749, Len: 608
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "test"
  Form item: "pass" = "test"
```

```
0000  9c e9 1c 19 2d 34 e0 d5  5e dd 40 bc 08 00 45 00   ····-4·· ^·@···E·
0010  02 94 e6 58 40 00 40 06  6a 78 c0 a8 01 03 2c e4   ···X@·@· jx····,·
0020  f9 03 d6 28 00 50 f2 62  ed 2f 68 cc 00 a9 80 18   ···(·P·b ·/h·····
0030  02 24 ea 19 00 00 01 01  08 0a 6a e0 fc 01 93 ec   ·$······ ··j·····
0040  74 48 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   tHPOST / userinfo
0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0070  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Connec
0080  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0090  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
00a0  3a 20 32 30 0d 0a 43 61  63 68 65 2d 43 6f 6e 74   : 20··Ca che-Cont
00b0  72 6f 6c 3a 20 6d 61 78  2d 61 67 65 3d 30 0d 0a   rol: max -age=0··
00c0  4f 72 69 67 69 6e 3a 20  68 74 74 70 3a 2f 2f 74   Origin:  http://t
```

No.: 253 · Time: 17.574294567 · Source: 192.168.1.3 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 674 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

✓ Show packet bytes   Layout: Vertical (Stacked)

```
Frame 253: 674 bytes on wire (53
Ethernet II, Src: GigaByteTech_d
Internet Protocol Version 4, Src
  0100 .... = Version: 4
  .... 0101 = Header Length: 20
  Differentiated Services Field:
  Total Length: 660
  Identification: 0xe658 (58968)
  010. .... = Flags: 0x2, Don't
  ...0 0000 0000 0000 = Fragment
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x6a78 [valid
  [Header checksum status: Unverified]
  Source Address: 192.168.1.3
  Destination Address: 44.228.249.3
  [Stream index: 2]
```

```
00d0  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.
00e0  6f 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   om··Cont ent-Typ
00f0  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 2d   : applic ation/x
0100  77 77 77 2d 66 6f 72 6d  2d 75 72 6c 65 6e 63 6f   www-form -urlenc
```

wireshark_eth0MRHI42.pcapng   Packets: 492 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)   Profile: Default

Conclusion:

The target website is vulnerable because it sends sensitive data without encryption. This allows attackers to intercept and steal information using tools like Wireshark.

This only works because **HTTP is plaintext**.

This will **not** work on HTTPS — that’s encrypted.