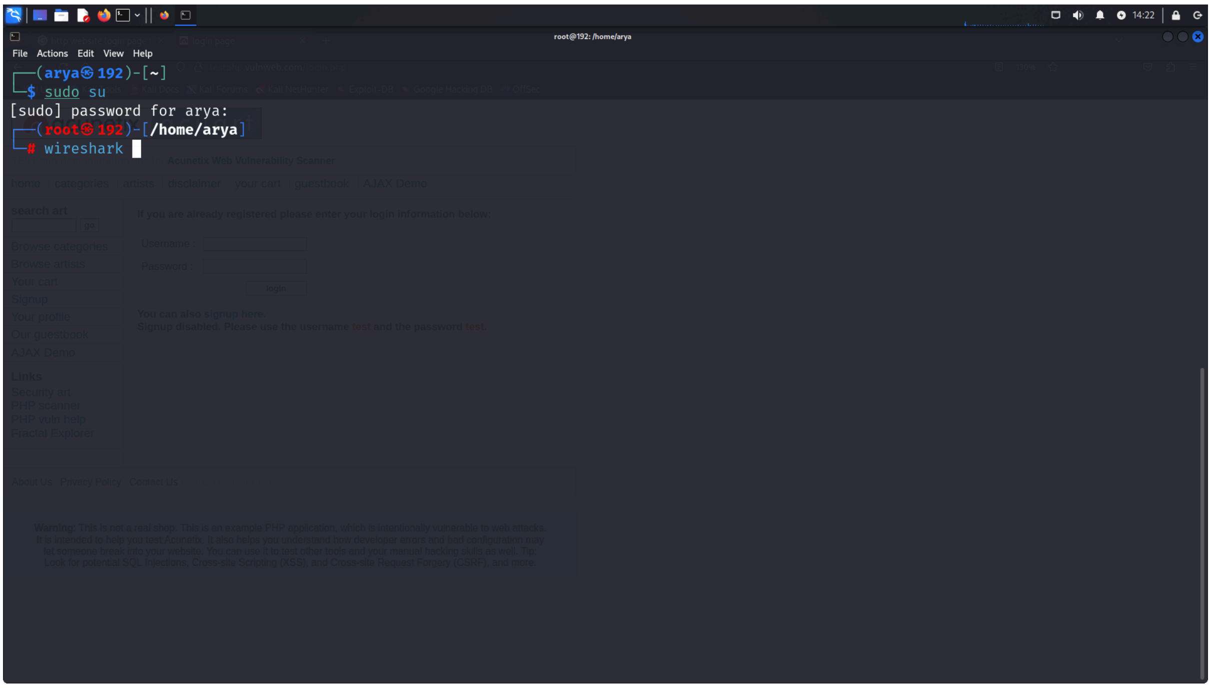
Wireshark-Packet Capturing and Analyzing

Performing a packet capture and analyzing login credentials using Wireshark on an HTTP website

Wireshark-Wireshark is an open-source network packet analyzer too that runs on both Windows and UNIX platforms. Wireshark captures the network packets and then display the packet data in detail. Wireshark is widely used to analyze the network traffic, to find the loopholes in the network architecture, to detect some of the attacks on the network.

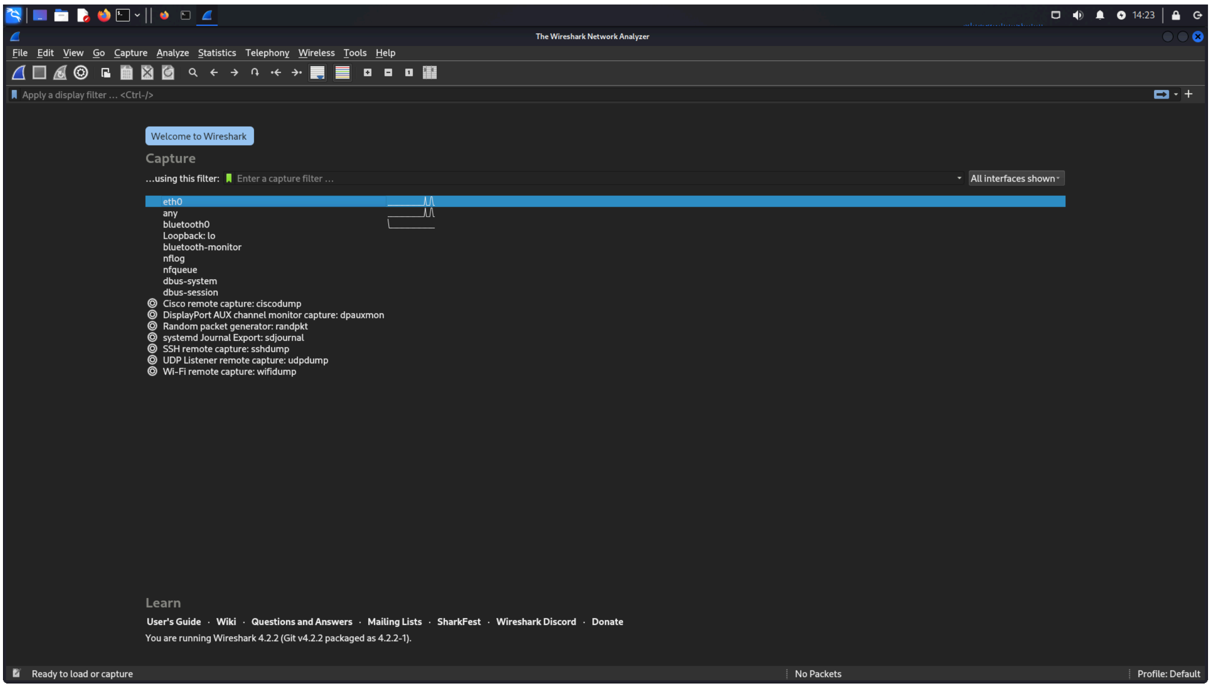
Step 1: Setting up Wireshark

1. Open the terminal on Kali Linux machine and type “Wireshark”.



```
┌──(arya㉿192)-[~]
└─$ sudo su
[sudo] password for arya:
┌──(root㉿192)-[/home/arya]
└─# wireshark
```

2. Open Wireshark and choose the appropriate network interface to capture packets (e.g., Ethernet, Wi-Fi).


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
bluetooth0
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

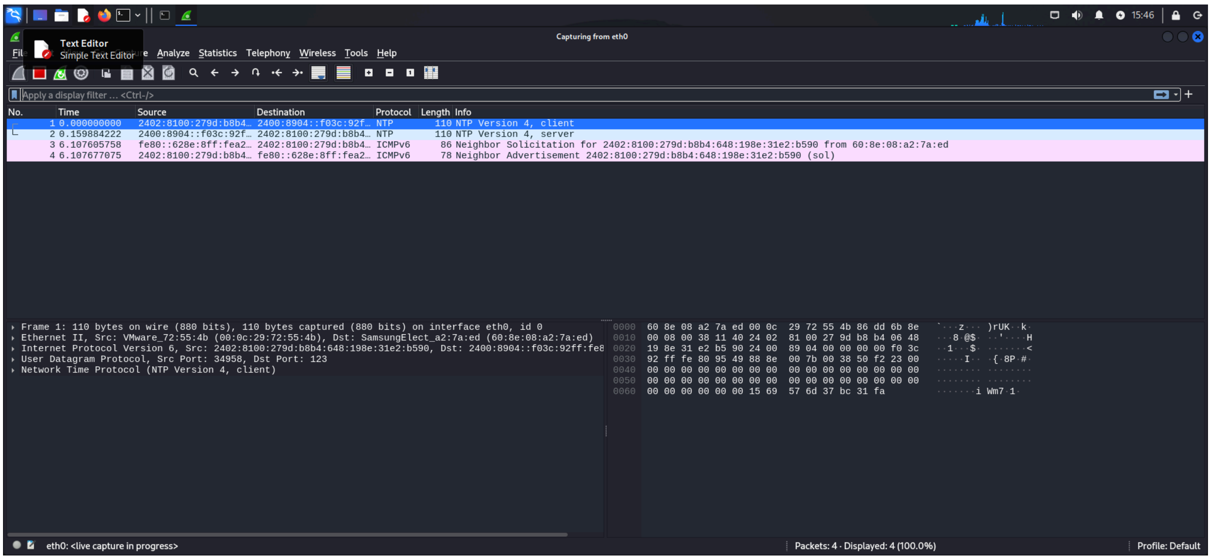
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

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

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

Step 2: Start Packet Capture

1. Start capturing packets by clicking on the 'Start' button in Wireshark.


15:46
Capturing from eth0
Text Editor
Simple Text Editor
Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

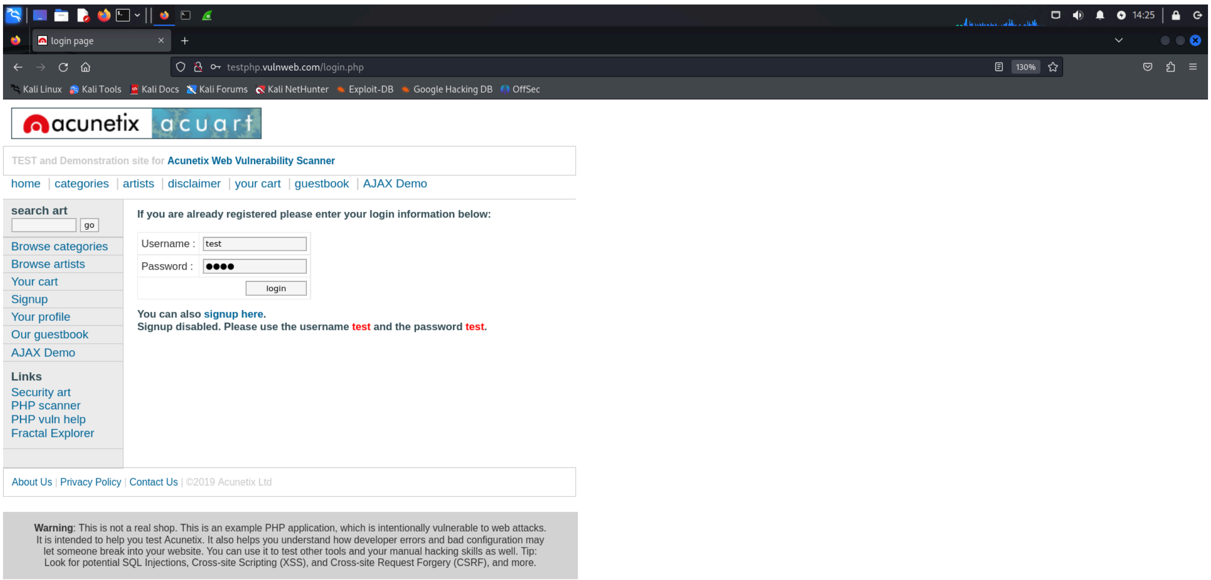
```
No.  Time          Source              Destination         Protocol Length Info
   1 0.000000000   2402:8100:279d:b8b4… 2400:8904::f03c:92f… NTP        110 NTP Version 4, client
   2 0.159884222   2400:8904::f03c:92f… 2402:8100:279d:b8b4… NTP        110 NTP Version 4, server
   3 6.107605758   fe80::628e:8ff:fea2… 2402:8100:279d:b8b4… ICMPv6      86 Neighbor Solicitation for 2402:8100:279d:b8b4:648:198e:31e2:b590 from 60:8e:08:a2:7a:ed
   4 6.107677075   2402:8100:279d:b8b4… fe80::628e:8ff:fea2… ICMPv6      78 Neighbor Advertisement 2402:8100:279d:b8b4:648:198e:31e2:b590 (sol)
```

```
› Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_72:55:4b (00:0c:29:72:55:4b), Dst: SamsungElect_a2:7a:ed (60:8e:08:a2:7a:ed)
› Internet Protocol Version 6, Src: 2402:8100:279d:b8b4:648:198e:31e2:b590, Dst: 2400:8904::f03c:92ff:fe8
› User Datagram Protocol, Src Port: 34958, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  60 8e 08 a2 7a ed 00 0c  29 72 55 4b 86 dd 6b 8e   `···z···)rUK··k·
0010  00 08 00 38 11 40 24 02  81 00 27 9d b8 b4 06 48   ···8·@$···'····H
0020  19 8e 31 e2 b5 90 24 00  89 04 00 00 00 00 f0 3c   ··1···$·········<
0030  92 ff fe 80 95 49 88 8e  00 7b 00 38 50 f2 23 00   ·····I···{·8P·#·
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0060  00 00 00 00 00 00 15 69  57 6d 37 bc 31 fa         ·······iWm7·1·
```

eth0: <live capture in progress> | Packets: 4 · Displayed: 4 (100.0%) | Profile: Default

2. Perform the login process on the HTTP website whose traffic you want to analyze.



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 : test
Password : ●●●●
login

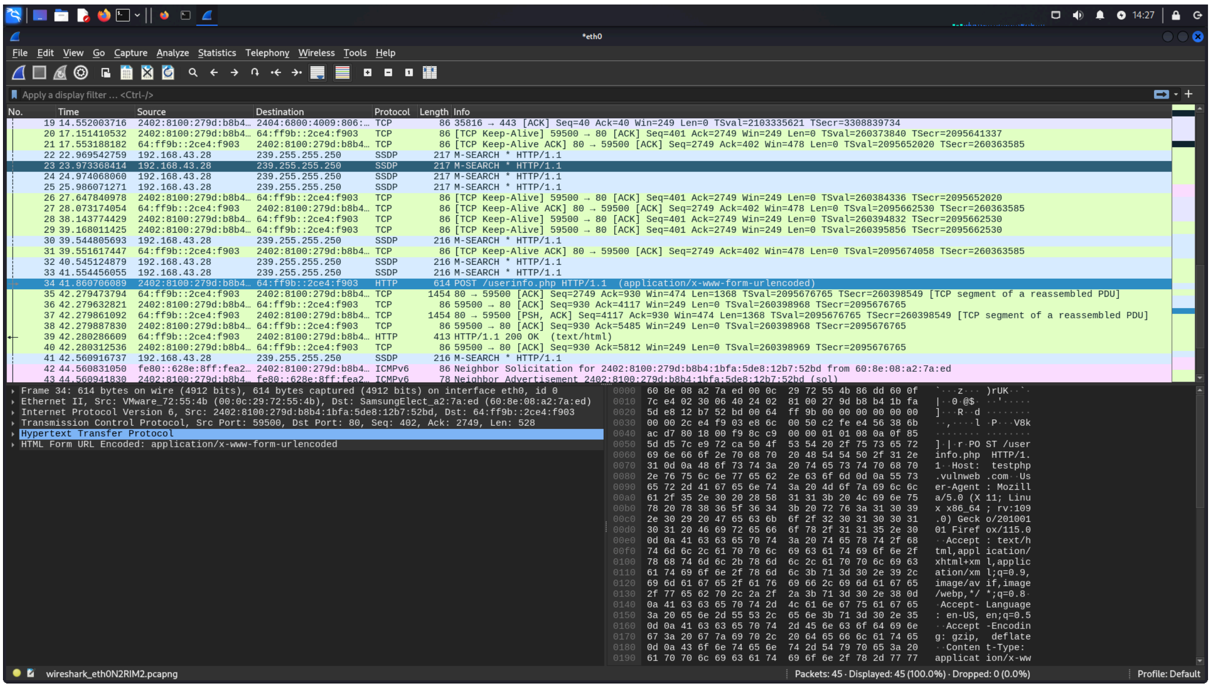
You can also signup here.
Signup disabled. Please use the username test and the password test.

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.

Step 3: Stop Packet Capture

1. After logging in or capturing sufficient data, stop the packet capture by clicking the 'Stop' button in Wireshark.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
14:27

```
No.  Time          Source                 Destination            Protocol Length Info
  19 14.552003716  2402:8100:279d:b8b4…   2404:6800:4009:806:…   TCP        86 35816 → 443 [ACK] Seq=40 Ack=40 Win=249 Len=0 TSval=2103335621 TSecr=3308839734
  20 17.151410532  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 [TCP Keep-Alive] 59500 → 80 [ACK] Seq=401 Ack=2749 Win=249 Len=0 TSval=260373840 TSecr=2095641337
  21 17.553188182  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   TCP        86 [TCP Keep-Alive ACK] 80 → 59500 [ACK] Seq=2749 Ack=402 Win=478 Len=0 TSval=2095652020 TSecr=260363585
  22 22.969542759  192.168.43.28          239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
  23 23.973368414  192.168.43.28          239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
  24 24.974068060  192.168.43.28          239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
  25 25.986071271  192.168.43.28          239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
  26 27.647840978  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 [TCP Keep-Alive] 59500 → 80 [ACK] Seq=401 Ack=2749 Win=249 Len=0 TSval=260384336 TSecr=2095652020
  27 28.073174054  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   TCP        86 [TCP Keep-Alive ACK] 80 → 59500 [ACK] Seq=2749 Ack=402 Win=478 Len=0 TSval=2095662530 TSecr=260363585
  28 38.143774429  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 [TCP Keep-Alive] 59500 → 80 [ACK] Seq=401 Ack=2749 Win=249 Len=0 TSval=260394832 TSecr=2095662530
  29 39.168011425  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 [TCP Keep-Alive] 59500 → 80 [ACK] Seq=401 Ack=2749 Win=249 Len=0 TSval=260395856 TSecr=2095662530
  30 39.544805693  192.168.43.28          239.255.255.250        SSDP      216 M-SEARCH * HTTP/1.1
  31 39.551617447  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   TCP        86 [TCP Keep-Alive ACK] 80 → 59500 [ACK] Seq=2749 Ack=402 Win=478 Len=0 TSval=2095674058 TSecr=260363585
  32 40.545124879  192.168.43.28          239.255.255.250        SSDP      216 M-SEARCH * HTTP/1.1
  33 41.554456055  192.168.43.28          239.255.255.250        SSDP      216 M-SEARCH * HTTP/1.1
  34 41.860706089  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     HTTP      614 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  35 42.279473794  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   TCP      1454 80 → 59500 [ACK] Seq=2749 Ack=930 Win=474 Len=1368 TSval=2095676765 TSecr=260398549 [TCP segment of a reassembled PDU]
  36 42.279632821  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 59500 → 80 [ACK] Seq=930 Ack=4117 Win=249 Len=0 TSval=260398968 TSecr=2095676765
  37 42.279861092  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   TCP      1454 80 → 59500 [PSH, ACK] Seq=4117 Ack=930 Win=474 Len=1368 TSval=2095676765 TSecr=260398549 [TCP segment of a reassembled PDU]
  38 42.279887830  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 59500 → 80 [ACK] Seq=930 Ack=5485 Win=249 Len=0 TSval=260398968 TSecr=2095676765
  39 42.280286609  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   HTTP      413 HTTP/1.1 200 OK  (text/html)
  40 42.280312536  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     TCP        86 59500 → 80 [ACK] Seq=930 Ack=5812 Win=249 Len=0 TSval=260398969 TSecr=2095676765
  41 42.560916737  192.168.43.28          239.255.255.250        SSDP      216 M-SEARCH * HTTP/1.1
  42 44.560831050  fe80::628e:8ff:fea2…   2402:8100:279d:b8b4…   ICMPv6     86 Neighbor Solicitation for 2402:8100:279d:b8b4:1bfa:5de8:12b7:52bd from 60:8e:08:a2:7a:ed
  43 44.560941830  2402:8100:279d:b8b4…   fe80::628e:8ff:fea2…   ICMPv6     78 Neighbor Advertisement 2402:8100:279d:b8b4:1bfa:5de8:12b7:52bd (sol)
```

```
› Frame 34: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_72:55:4b (00:0c:29:72:55:4b), Dst: SamsungElect_a2:7a:ed (60:8e:08:a2:7a:ed)
› Internet Protocol Version 6, Src: 2402:8100:279d:b8b4:1bfa:5de8:12b7:52bd, Dst: 64:ff9b::2ce4:f903
› Transmission Control Protocol, Src Port: 59500, Dst Port: 80, Seq: 402, Ack: 2749, Len: 528
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

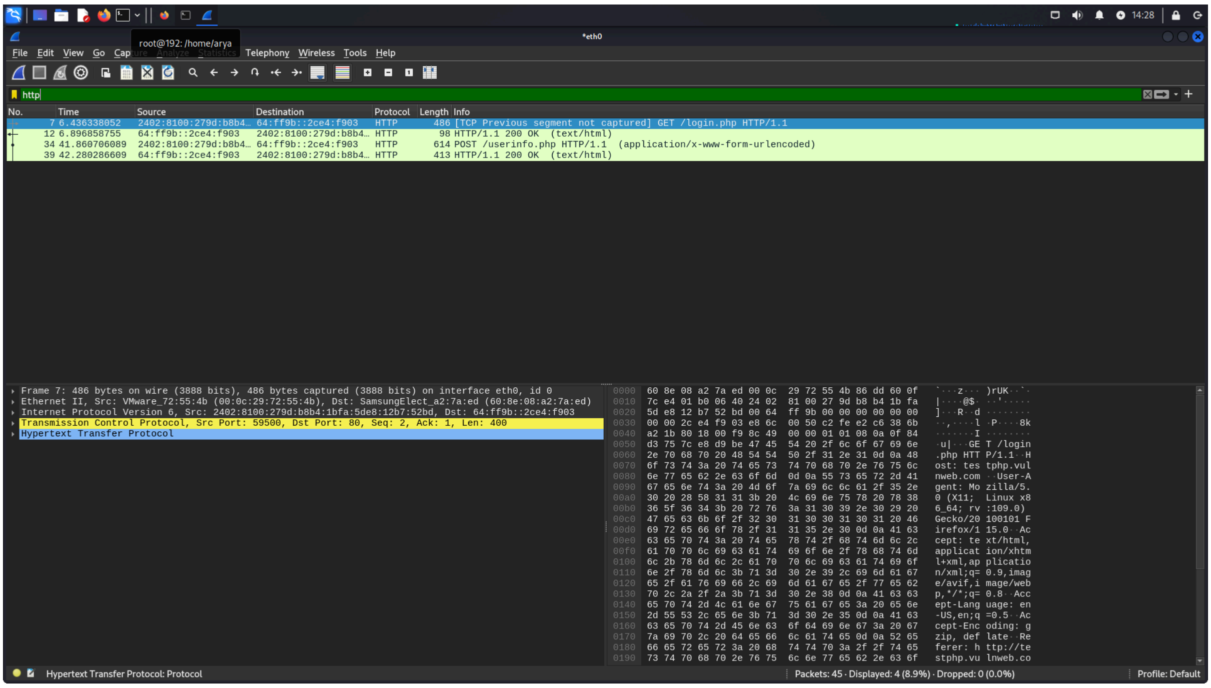
```
0000  60 8e 08 a2 7a ed 00 0c  29 72 55 4b 86 dd 60 0f   `···z··· )rUK··`·
0010  7c e4 02 30 06 40 24 02  81 00 27 9d b8 b4 1b fa   |··0·@$· ··'·····
0020  5d e8 12 b7 52 bd 00 64  ff 9b 00 00 00 00 00 00   ]···R··d ········
0030  00 00 2c e4 f9 03 e8 6c  00 50 c2 fe e4 56 38 6b   ··,····l ·P···V8k
0040  ac d7 80 18 00 f9 8c c9  00 00 01 01 08 0a 0f 85   ········ ········
0050  5d d5 7c e9 72 ca 50 4f  53 54 20 2f 75 73 65 72   ]·|·r·PO ST /user
0060  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0070  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0080  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0090  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00a0  61 2f 35 2e 30 20 28 58  31 31 3b 20 4c 69 6e 75   a/5.0 (X 11; Linu
00b0  78 20 78 38 36 5f 36 34  3b 20 72 76 3a 31 30 39   x x86_64 ; rv:109
00c0  2e 30 29 20 47 65 63 6b  6f 2f 32 30 31 30 30 31   .0) Geck o/201001
00d0  30 31 20 46 69 72 65 66  6f 78 2f 31 31 35 2e 30   01 Firef ox/115.0
00e0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 68   ··Accept : text/h
00f0  74 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   tml,appl ication/
0100  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
0110  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0120  69 6d 61 67 65 2f 61 76  69 66 2c 69 6d 61 67 65   image/av if,image
0130  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8·
0140  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0150  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0160  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0170  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0190  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
```

wireshark_eth0N2RIM2.pcapng   Packets: 45 · Displayed: 45 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

Step 4: Analyze Captured Packets

1. Filter captured packets to focus on HTTP traffic by typing 'HTTP' in the filter field.

2. Look for POST requests which typically contain login credentials.



http

```
No.    Time          Source                 Destination            Protocol  Length Info
     7 6.436338052   2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     HTTP         486 [TCP Previous segment not captured] GET /login.php HTTP/1.1
    12 6.896858755   64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   HTTP          98 HTTP/1.1 200 OK  (text/html)
    34 41.860706089  2402:8100:279d:b8b4…   64:ff9b::2ce4:f903     HTTP         614 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
    39 42.280286609  64:ff9b::2ce4:f903     2402:8100:279d:b8b4…   HTTP         413 HTTP/1.1 200 OK  (text/html)
```

```
Frame 7: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface eth0, id 0
Ethernet II, Src: VMware_72:55:4b (00:0c:29:72:55:4b), Dst: SamsungElect_a2:7a:ed (60:8e:08:a2:7a:ed)
Internet Protocol Version 6, Src: 2402:8100:279d:b8b4:1bfa:5de8:12b7:52bd, Dst: 64:ff9b::2ce4:f903
Transmission Control Protocol, Src Port: 59500, Dst Port: 80, Seq: 2, Ack: 1, Len: 400
Hypertext Transfer Protocol
```

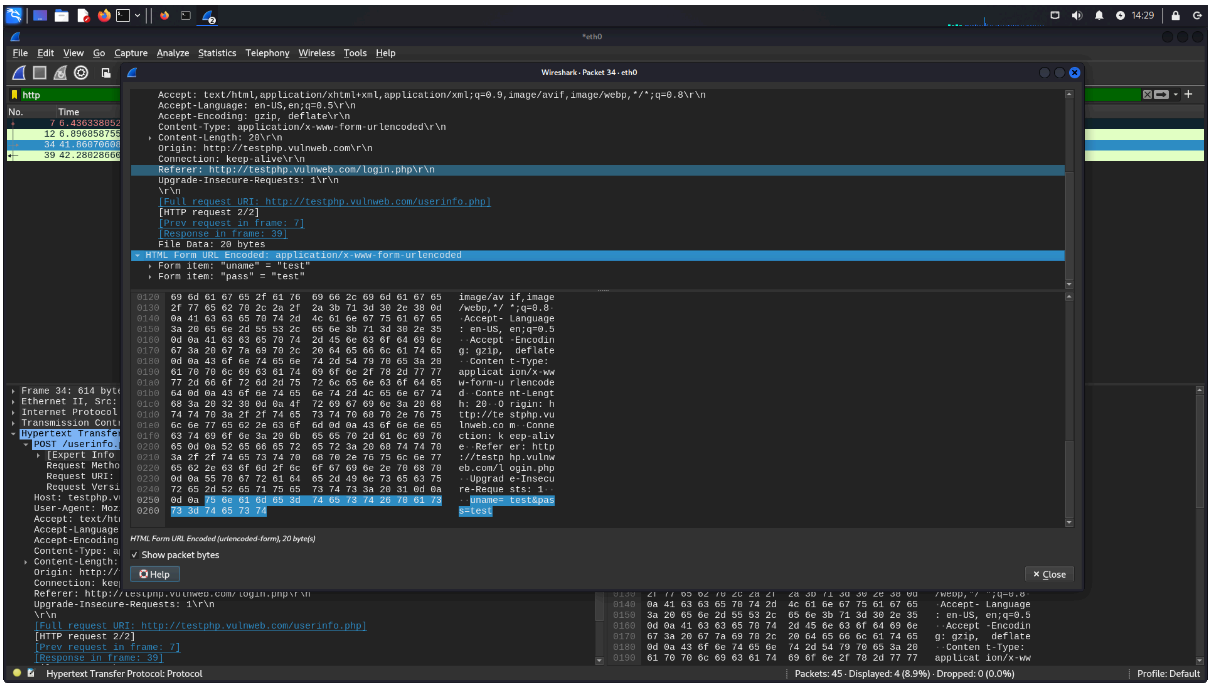
```
0000  60 8e 08 a2 7a ed 00 0c  29 72 55 4b 86 dd 60 0f   `···z··· )rUK··`·
0010  7c e4 01 b0 06 40 24 02  81 00 27 9d b8 b4 1b fa   |····@$· ··'·····
0020  5d e8 12 b7 52 bd 00 64  ff 9b 00 00 00 00 00 00   ]···R··d ········
0030  00 00 2c e4 f9 03 e8 6c  00 50 c2 fe e2 c6 38 6b   ··,····l ·P····8k
0040  a2 1b 80 18 00 f9 8c 49  00 00 01 01 08 0a 0f 84   ·······I ········
0050  d3 75 7c e8 d9 be 47 45  54 20 2f 6c 6f 67 69 6e   ·u|···GE T /login
0060  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0070  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0080  6e 77 65 62 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   nweb.com ··User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00a0  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
00b0  36 5f 36 34 3b 20 72 76  3a 31 30 39 2e 30 29 20   6_64; rv :109.0)
00c0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00d0  69 72 65 66 6f 78 2f 31  31 35 2e 30 0d 0a 41 63   irefox/1 15.0··Ac
00e0  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
00f0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0100  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0110  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0120  65 2f 61 76 69 66 2c 69  6d 61 67 65 2f 77 65 62   e/avif,i mage/web
0130  70 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   p,*/*;q= 0.8··Acc
0140  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
0150  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
0160  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0170  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 52 65   zip, def late··Re
0180  66 65 72 65 72 3a 20 68  74 74 70 3a 2f 2f 74 65   ferer: h ttp://te
0190  73 74 70 68 70 2e 76 75  6c 6e 77 65 62 2e 63 6f   stphp.vu lnweb.co
```

Hypertext Transfer Protocol: Protocol

Packets: 45 · Displayed: 4 (8.9%) · Dropped: 0 (0.0%)

Profile: Default

3. Analyze the packets to identify any login credentials transmitted over HTTP.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
*eth0
Wireshark · Packet 34 · eth0
http
No. Time
14:29

```
  7 6.436338052
 12 6.896858755
 34 41.86070608
 39 42.28028660
```

```
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 20\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
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/2]
    [Prev request in frame: 7]
    [Response in frame: 39]
    File Data: 20 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "test"
  › Form item: "pass" = "test"
```

```
0120  69 6d 61 67 65 2f 61 76  69 66 2c 69 6d 61 67 65   image/av if,image
0130  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8·
0140  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0150  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0160  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0170  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0190  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
01a0  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
01b0  64 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   d··Conte nt-Lengt
01c0  68 3a 20 32 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   h: 20··O rigin: h
01d0  74 74 70 3a 2f 2f 74 65  73 74 70 68 70 2e 76 75   ttp://te stphp.vu
01e0  6c 6e 77 65 62 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   lnweb.co m··Conne
01f0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
0200  65 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   e··Refer er: http
0210  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
0220  65 62 2e 63 6f 6d 2f 6c  6f 67 69 6e 2e 70 68 70   eb.com/l ogin.php
0230  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0240  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0250  0d 0a 75 6e 61 6d 65 3d  74 65 73 74 26 70 61 73   ··uname= test&pas
0260  73 3d 74 65 73 74                                  s=test
```

HTML Form URL Encoded (urlencoded-form), 20 byte(s)

✓ Show packet bytes

Help

× Close

```
› Frame 34: 614 byte
› Ethernet II, Src:
› Internet Protocol
› Transmission Contr
⌄ Hypertext Transfer
  ⌄ POST /userinfo.
    › [Expert Info
      Request Metho
      Request URI:
      Request Versi
    Host: testphp.v
    User-Agent: Moz
    Accept: text/ht
    Accept-Language
    Accept-Encoding
    Content-Type: a
  › Content-Length:
    Origin: http://
    Connection: kee
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/2]
    [Prev request in frame: 7]
    [Response in frame: 39]
```

```
0130  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8·
0140  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0150  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0160  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0170  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0190  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
```

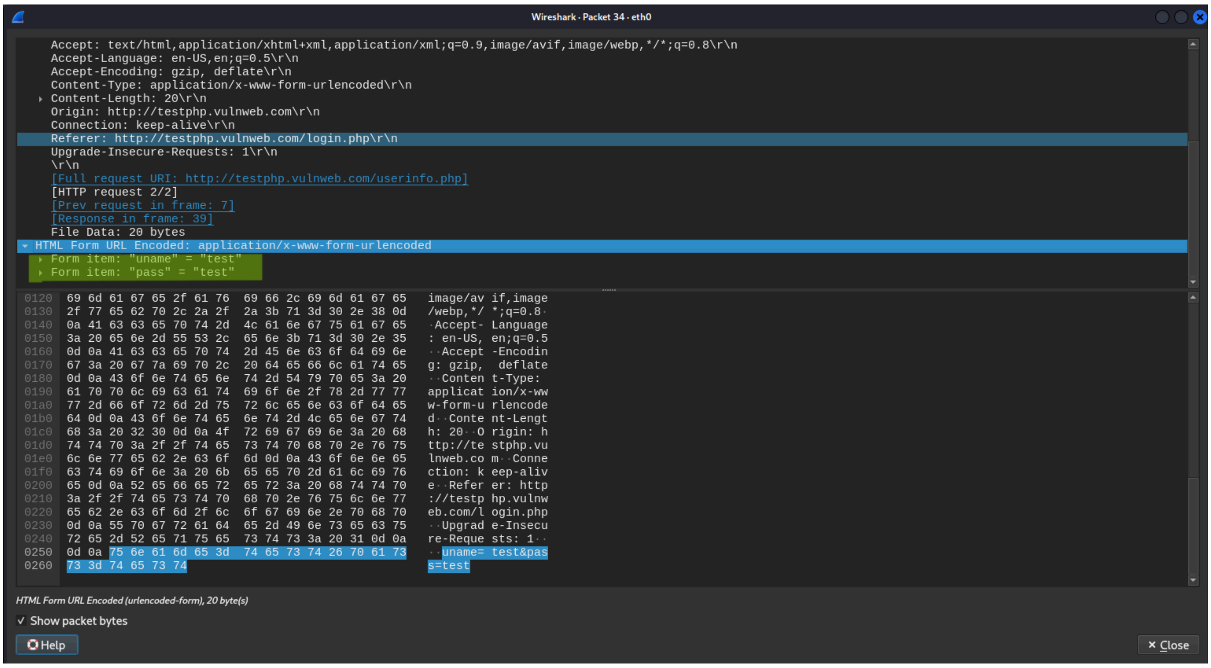
Hypertext Transfer Protocol: Protocol

Packets: 45 · Displayed: 4 (8.9%) · Dropped: 0 (0.0%)

Profile: Default

4. Login Credentials Analysis: login credentials found in the captured packets, including usernames and passwords.

Username: test
Password: test



```
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 20\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
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/2]
    [Prev request in frame: 7]
    [Response in frame: 39]
    File Data: 20 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uname" = "test"
  › Form item: "pass" = "test"
```

```
0120  69 6d 61 67 65 2f 61 76  69 66 2c 69 6d 61 67 65   image/av if,image
0130  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8·
0140  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
0150  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0160  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0170  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0190  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
01a0  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
01b0  64 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   d··Conte nt-Lengt
01c0  68 3a 20 32 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   h: 20··O rigin: h
01d0  74 74 70 3a 2f 2f 74 65  73 74 70 68 70 2e 76 75   ttp://te stphp.vu
01e0  6c 6e 77 65 62 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   lnweb.co m··Conne
01f0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
0200  65 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   e··Refer er: http
0210  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
0220  65 62 2e 63 6f 6d 2f 6c  6f 67 69 6e 2e 70 68 70   eb.com/l ogin.php
0230  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0240  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0250  0d 0a 75 6e 61 6d 65 3d  74 65 73 74 26 70 61 73   ··uname= test&pas
0260  73 3d 74 65 73 74                                  s=test
```

HTML Form URL Encoded (urlencoded-form), 20 byte(s)

✓ Show packet bytes

Help

× Close

Author: Abhishek Kori