

WIRESHARK PROJECT : Sniffing Unencrypted Network Traffic

Group members:

1.Shivya Bali (2023d2r041)

2.Jasleen Kour (2023d2r027)

3.Anshika Mehra (2023D2R054)



MIET

Model Institute of Engineering & Technology

Introduction

- **Objective:**
- To showcase how **Wireshark** can be used to analyze **unencrypted network traffic** for educational and ethical hacking purposes.
- **What is Sniffing?**

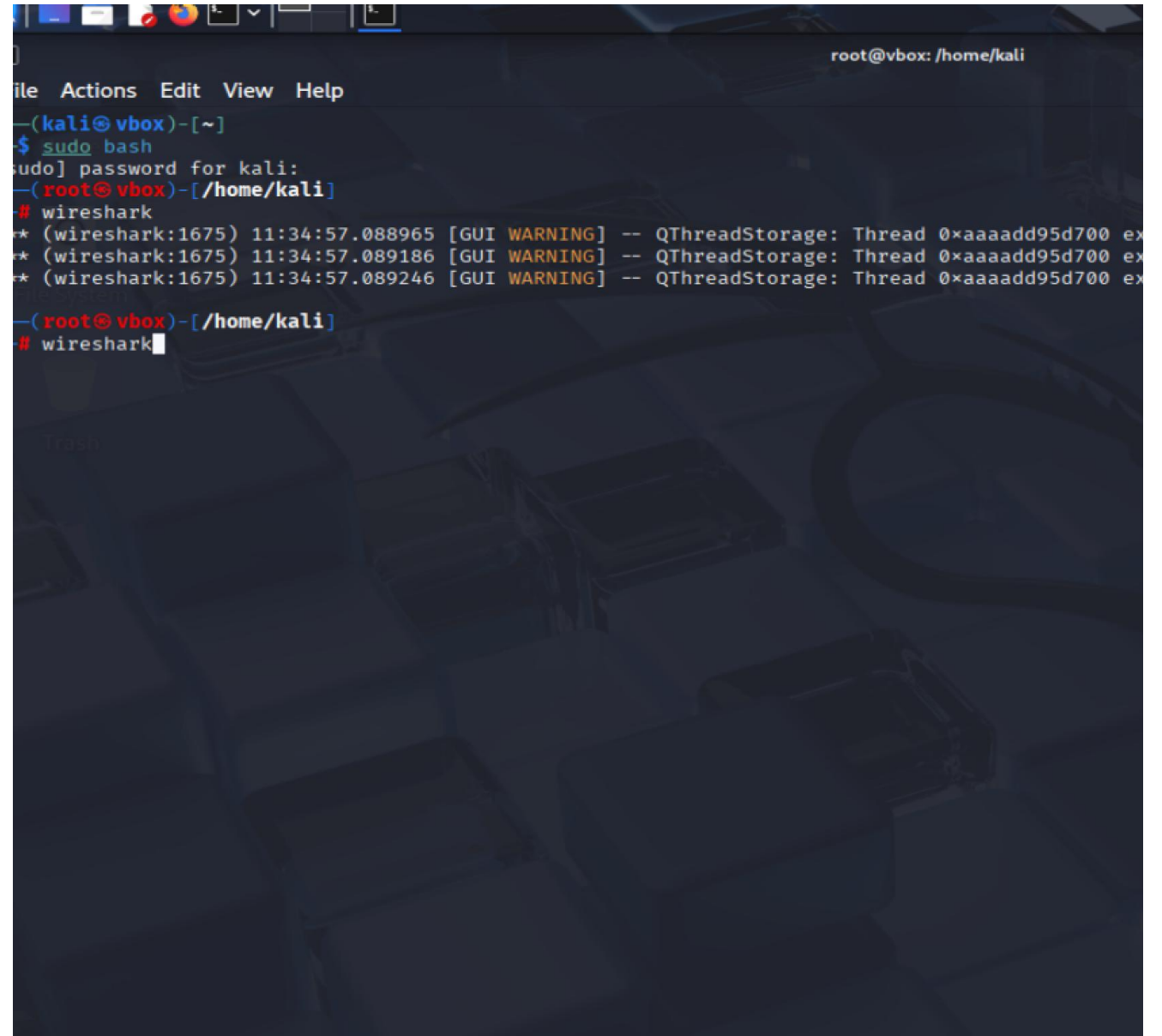
Sniffing refers to the **interception and monitoring of network data packets**.

- **Tool Used:**

Kali Linux + Wireshark

Step1:

Open Terminal and run:
wireshark

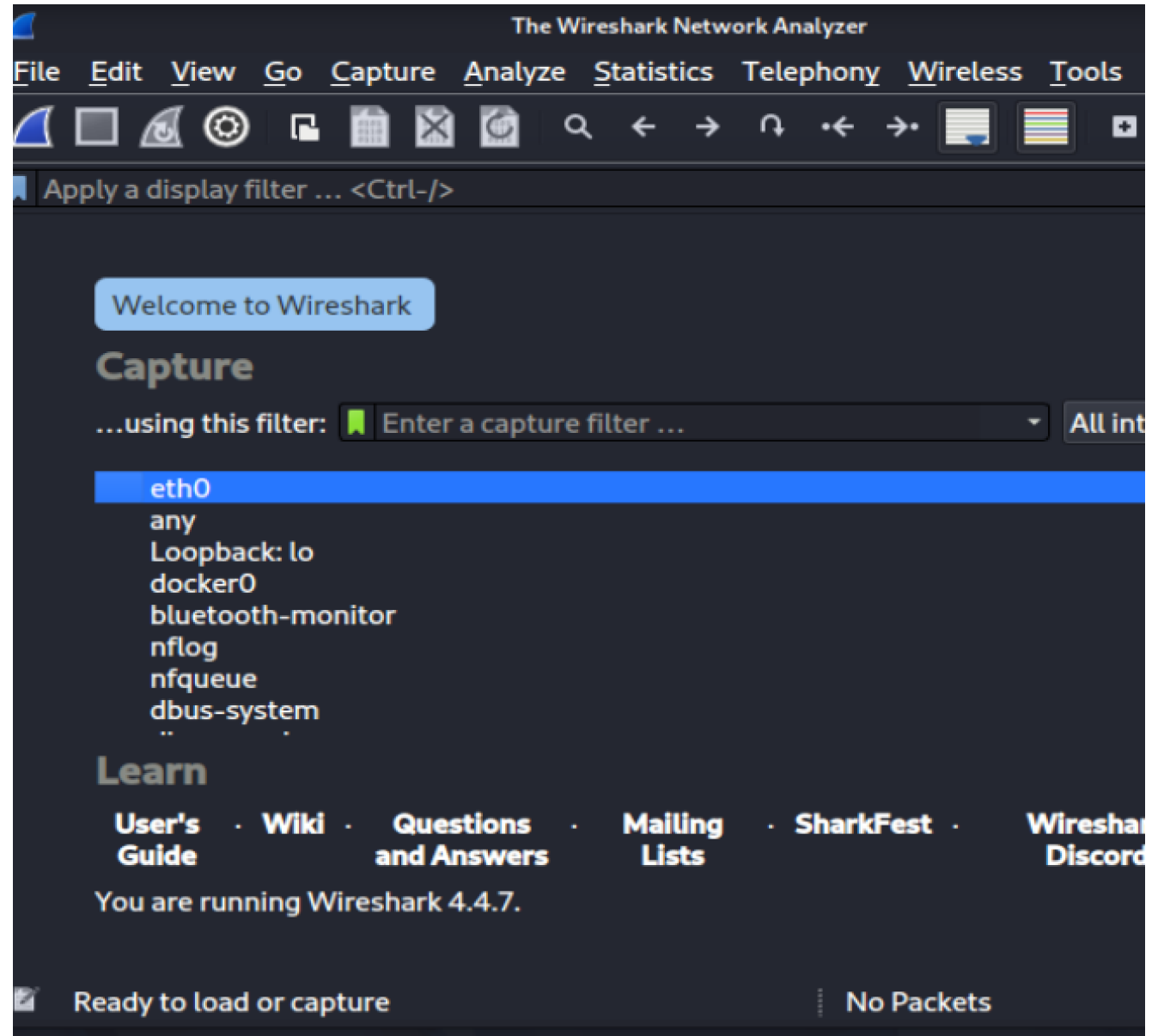


```
root@vbox: /home/kali
File Actions Edit View Help
--(kali@vbox)-[~]
$ sudo bash
[sudo] password for kali:
--(root@vbox)-[/home/kali]
# wireshark
* (wireshark:1675) 11:34:57.088965 [GUI WARNING] -- QThreadStorage: Thread 0xaaaadd95d700 ex
* (wireshark:1675) 11:34:57.089186 [GUI WARNING] -- QThreadStorage: Thread 0xaaaadd95d700 ex
* (wireshark:1675) 11:34:57.089246 [GUI WARNING] -- QThreadStorage: Thread 0xaaaadd95d700 ex
--(root@vbox)-[/home/kali]
# wireshark
```

Step 2:

Choose eth0 network interface.

It will Begin capturing packets from the network.

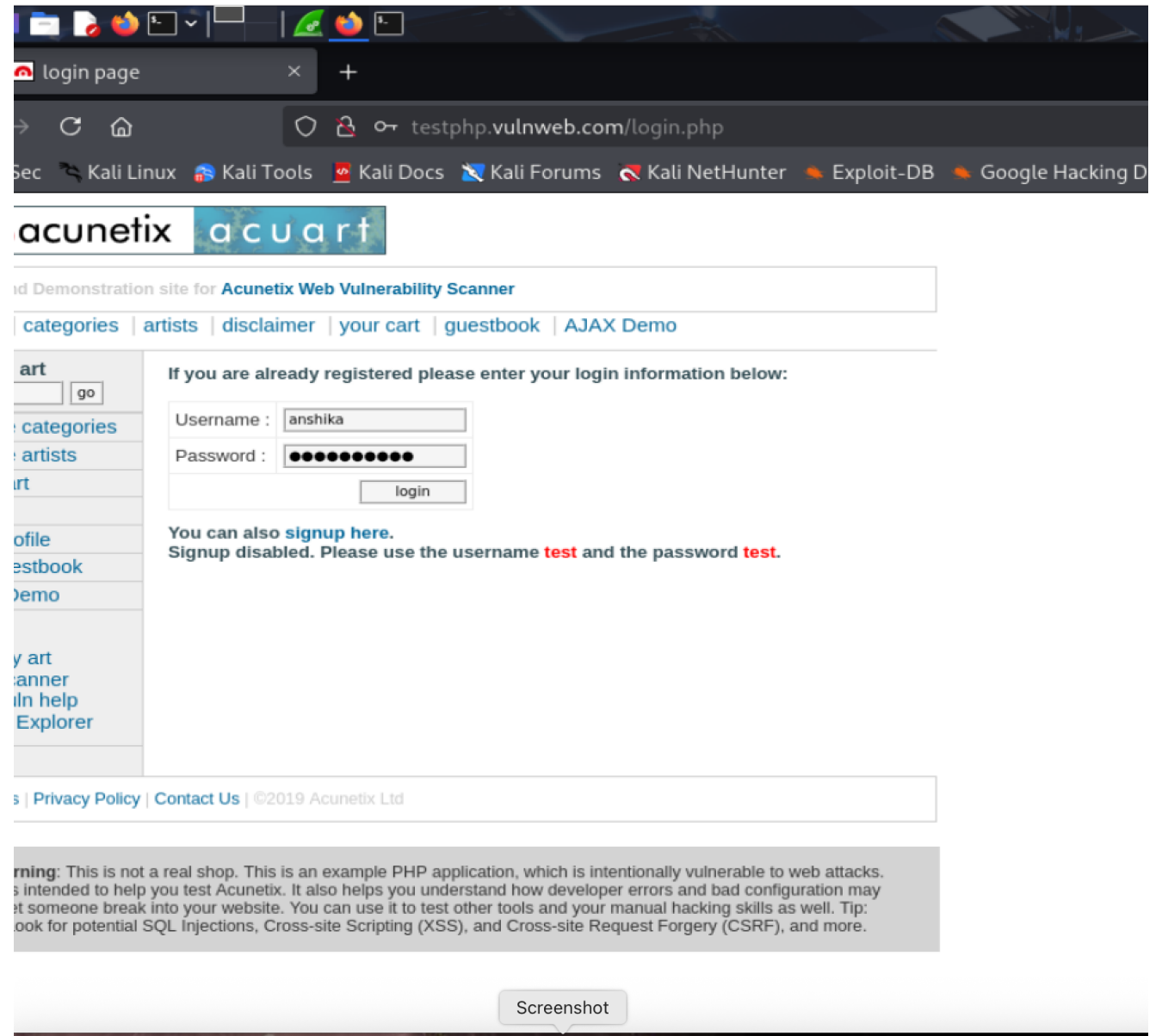


Step 3:

Open browser and go to <http://testphp.vulnweb.com>.

Go to the login page.

Enter any dummy username and password.

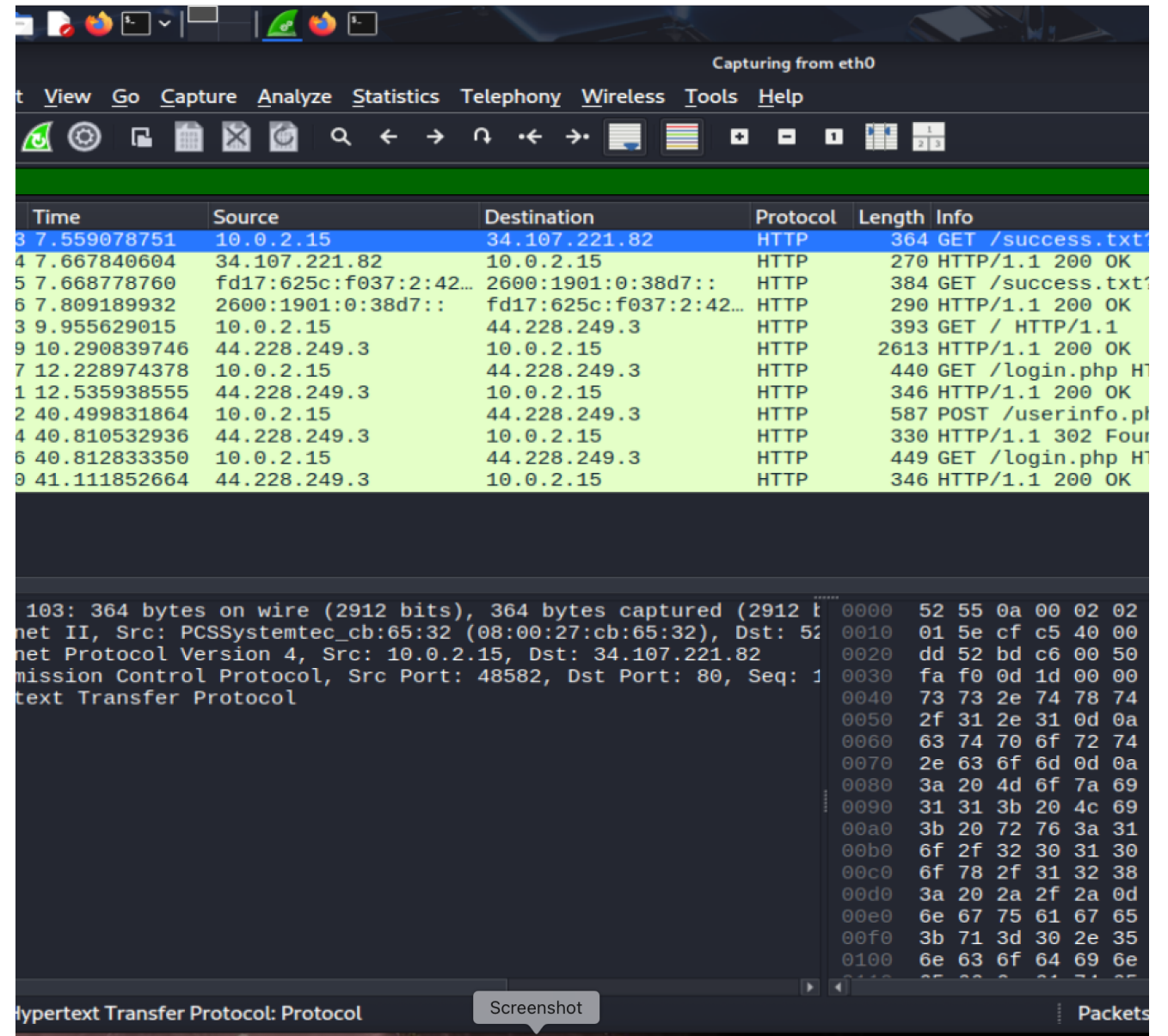


Step 4:

Go Back in Wireshark

Apply filter: http

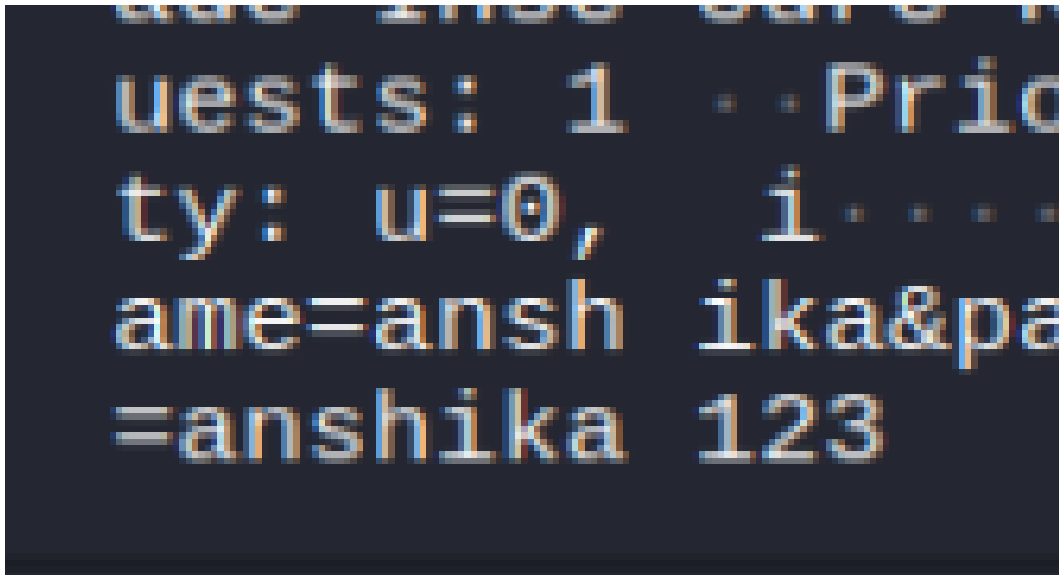
select http.request.method == "POST"



Step 5:

Right-click on the POST packet →
Follow → HTTP Stream.

We will get the username and
password in the plain text



HTML Form URL Encoded: application/x-www-form-urlencoded

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 39 0d	tent-Len gth: 29·
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 6e 73 68 69 6b 61 26 70 61 73 73	ame=ansh ika&pass
0240	3d 61 6e 73 68 69 6b 61 31 32 33	=anshika 123

No.: 252 · Time: 40.499831864 · Source: 10.0.2.15 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 587 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

✓ Show packet bytes Layout: Vertical (Stacked) Help Screenshot