

Login

1) POST

Frame 125: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits) on interface vlp0s20f3, id 0	0000 70 4f 24 f7 44 f0 04 e7 0b f0 70 cc 00 00 00 00	xOS D... d...
Ethernet II, Src: Intel fe:70:cc (94:e7:0b:fe:70:cc), Dst: TaicangTAMEL f7:44:f0 (78:4f:24:f7:44:f0)	0010 02 71 b8 46 49 09 49 06 92 05 09 49 01 43 2c e4	gNg0g...e...c...
Internet Protocol Version 4, Src: 192.168.1.67, Dst: 44.228.249.3	0020 01 55 ea 36 00 00 01 01 08 0a 02 26 79 18 07 74	6...dy...t...
0100 = Version: 4	0030 da 8b 50 4f 53 54 20 2f 75 73 05 72 69 6e 66 6f	..POST / userinfo
... 0101 = Header Length: 20 bytes (5)	0040 2e 70 68 70 20 48 54 54 50 2f 31 26 31 0d 0a 48	.php HTTP/1.1
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	0050 6f 73 74 3a 20 74 65 73 74 70 68 70 2e 76 75 6c	ost: testphp.vul
Total Length: 625	0060 6e 77 65 62 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41	nweb.com - User-A
Identification: 0xb04e (48718)	0070 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e	gent: Mozilla/5.
010 = Flags: 0x2, Don't Fragment	0080 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38	0 (X11; Linux x8
... 0 0000 0000 0000 = Fragment Offset: 0	0090 36 5f 36 34 3b 20 72 76 3a 31 32 38 2e 30 29 29	6.64; rv:128.0)
Time to Live: 64	00a0 47 65 63 0b 6f 2f 32 30 31 30 30 31 30 31 30 46	Gecko/20100101 F
Protocol: TCP (6)	00b0 69 72 65 66 6f 78 2f 31 32 38 2e 30 0d 0a 41 63	irefox/128.0. Ac
Header Checksum: 0x9265 (validation disabled)	00c0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c	cept: text/html,
[Header checksum status: Unverified]	00d0 01 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d	applicat ion/xhta
Source Address: 192.168.1.67	00e0 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f	l+xml,ap plicatio
Destination Address: 44.228.249.3	00f0 6e 2f 78 6d 6c 30 71 3d 38 2e 39 2c 69 6d 61 67	n/xml;q= 0.9,imag
Transmission Control Protocol, Src Port: 51632, Dst Port: 80, Seq: 2, Ack: 1, Len: 573	0100 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62	e/avif,i mage/web
Source Port: 51632	0110 70 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67	p,image/ png,imag
Destination Port: 80	0120 65 2f 73 76 67 2b 78 6d 6c 2c 2a 2f 2a 3b 71 3d	e/svg+xml, */*;q=
[Stream index: 0]	0130 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67	0.8 - Acc ept-Lang
[Conversation completeness: Incomplete (12)]	0140 75 61 67 65 3a 20 65 6e 2d 65 53 2c 65 6e 30 71	uage: en-US,en;q
[TCP Segment Len: 573]	0150 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63	=0.5 - Ac cept-Enc
Sequence Number: 2 (relative sequence number)	0160 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66	oding: g zip, def
Sequence Number (raw): 2067839788	0170 6c 61 74 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79	late - Co ntent-Enc
[Next Sequence Number: 575 (relative sequence number)]	0180 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f	pe: applic ation/
Acknowledgment Number: 1 (relative sequence number)	0190 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e	x-www-fo rm-urle
Acknowledgment Number (raw): 1270574499	01a0 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c	coded -C ontent-L
1000 = Header Length: 32 bytes (8)	01b0 65 6e 67 74 68 3a 20 32 33 0d 0a 4f 72 69 67 69	ength: 2 3 - Origi
Flags: 0x010 (PSH, ACK)	01c0 6e 3a 20 68 74 74 70 3a 2f 2f 74 65 73 74 70 68	n: http: //testph
Window: 405	01d0 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43	p.vulnwe b.com - C
[Calculated window size: 405]	01e0 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0b 65 65 70 2d	onnectio n: keep-
[Window size scaling factor: -1 (unknown)]	01f0 61 6c 69 76 65 0d 0a 32 65 66 65 72 65 72 3a 29	alive - R eferer:
Checksum: 0xa036 (unverified)	0200 68 74 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 76	http://t estphp.v
[Checksum Status: Unverified]	0210	

Internet Protocol Version 4

Src: 192.168.1.67

Dst: 44.228.249.3

Transmission Control Protocol

Src Port: 51632

Dst Port: 80

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,image/avif,imag

e/webp,image/png,image/svg+xml,*/*;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: 23\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

[Full request URI: http://testphp.vulnweb.com/userinfo.php]

[HTTP request 1/2]

[Response in frame: 141]

[Next request in frame: 142]

File Data: 23 bytes

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

Form item: "uname" = "anish"

Form item: "pass" = "subedi"

Note: since no encryption method were used data send were plain text as we can see username and password clearly.

2) GET

Hypertext Transfer Protocol

```
GET /login.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,image/avif,image/webp,image/png,ima
ge/svg+xml,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://testphp.vulnweb.com/login.php\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Priority: u=0, i\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/login.php]
[HTTP request 2/2]
[Prev request in frame: 125]
[Response in frame: 146]
```

Security Analysis

1. **Transport Layer Security (TLS) / Secure Sockets Layer (SSL)**

- The communication uses HTTP on port 80, which is not encrypted. HTTPS, which operates over port 443, would be needed to secure the communication with TLS/SSL.

2. **Sensitive Data**

- The username and password (uname=anish&pass=subedi) are sent in plaintext. This can be easily intercepted by an attacker using a network sniffer.

3. **Connection**

- The Connection: keep-alive header indicates that the connection should be kept open for multiple requests, which is common for efficiency but does not impact security directly.

Security Measures to Consider

- **Use HTTPS:** Encrypt the communication using HTTPS to protect the data in transit.
- **Form Data Encryption:** Encrypt sensitive form data before sending it.

Summary

The analyzed packet uses plain HTTP, which does not provide any encryption, making it vulnerable to interception and eavesdropping. To secure the communication, switching to HTTPS and implementing additional security measures is essential.