

# WIRESHARK TASK REPORT



@generalzodx28

# HTTP Form Capture

\*wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1336	17.692862168	192.168.0.144	44.228.249.3	HTTP	528	GET / HTTP/1.1
1343	17.992356344	44.228.249.3	192.168.0.144	HTTP	1691	HTTP/1.1 200 OK (text/html)
1345	18.036735301	192.168.0.144	44.228.249.3	HTTP	444	GET /acunetix-logo.png HTTP/1.1
1349	18.074978911	192.168.0.144	44.228.249.3	HTTP	390	GET /style.css HTTP/1.1
1401	18.332419873	44.228.249.3	192.168.0.144	HTTP	340	HTTP/1.1 200 OK (PNG)
1410	18.376878573	44.228.249.3	192.168.0.144	HTTP	1560	HTTP/1.1 200 OK (text/css)
1414	18.465199997	192.168.0.144	44.228.249.3	HTTP	438	GET /favicon.ico HTTP/1.1
1428	18.823189324	44.228.249.3	192.168.0.144	HTTP	440	HTTP/1.1 404 Not Found (text/html)
1771	67.765300525	192.168.0.144	44.228.249.3	HTTP	534	GET / HTTP/1.1
1779	68.068567265	44.228.249.3	192.168.0.144	HTTP	2750	HTTP/1.1 200 OK (text/html)
1784	68.170326168	192.168.0.144	44.228.249.3	HTTP	413	GET /static/css/style.css HTTP/1.1
1793	68.173645727	192.168.0.144	44.228.249.3	HTTP	459	GET /static/img/logo2.png HTTP/1.1
1829	68.479999673	44.228.249.3	192.168.0.144	HTTP	636	HTTP/1.1 200 OK (text/css)
1838	68.482687048	192.168.0.144	44.228.249.3	HTTP	395	GET /static/app/app.js HTTP/1.1
1839	68.483023337	192.168.0.144	44.228.249.3	HTTP	405	GET /static/app/libs/sessvars.js HTTP/1.1
1840	68.483102184	192.168.0.144	44.228.249.3	HTTP	396	GET /static/app/post.js HTTP/1.1
1841	68.483161070	192.168.0.144	44.228.249.3	HTTP	415	GET /static/app/controllers/controllers.js HTTP/1.1
1844	68.503297924	44.228.249.3	192.168.0.144	HTTP	2802	HTTP/1.1 200 OK (PNG)
1849	68.503904326	192.168.0.144	44.228.249.3	HTTP	413	GET /static/app/services/itemsService.js HTTP/1.1
1852	68.506090532	192.168.0.144	151.101.66.137	HTTP	391	GET /jquery-1.9.1.min.js HTTP/1.1
1951	68.777784535	151.101.66.137	192.168.0.144	HTTP	1308	HTTP/1.1 200 OK (application/javascript)
1955	68.815059451	44.228.249.3	192.168.0.144	HTTP	1950	HTTP/1.1 200 OK (application/javascript)
1967	68.816994556	44.228.249.3	192.168.0.144	HTTP	535	HTTP/1.1 200 OK (application/javascript)
1976	68.820317000	44.228.249.3	192.168.0.144	HTTP	1248	HTTP/1.1 200 OK (application/javascript)
1982	68.822033854	44.228.249.3	192.168.0.144	HTTP	585	HTTP/1.1 200 OK (application/javascript)

Frame 9020: 728 bytes on wire (5824 bits), 728 bytes captured (5824 bits) on interface wlan0, id 0

Ethernet II, Src: Intel\_22:e9:e4 (e2:2e:0b:22:e9:e4), Dst: DLinkInterna\_44:20:bc (48:ee:0c:44:20:bc)

Internet Protocol Version 4, Src: 192.168.0.144, Dst: 44.228.249.3

Transmission Control Protocol, Src Port: 51416, Dst Port: 80, Seq: 1244, Ack: 10784, Len: 662

Hypertext Transfer Protocol

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

Form item: "uname" = "GeneralZodX"

Key: uname

Value: GeneralZodX

Form item: "pass" = "MySecurePassword"

Key: pass

Value: MySecurePassword

0040 99 8e 50 4f 53 54 20 2f 75 73 65 72 69 6e 66 6f ..POST / userinfo

0050 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .php HTTP/1.1..H

0060 6f 73 74 3a 20 74 65 73 74 70 68 70 2e 76 75 6c ost: testphp.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: keep-alive

0090 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ..Content-Length

00a0 3a 20 33 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 : 39..Cache-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

00d0 65 73 74 70 68 70 2e 76 75 6e 6e 77 65 62 2e 63 estphp.vulnweb.c

00e0 6f 6d 0d 0a 44 4e 54 3a 20 31 0d 0a 55 70 67 72 om..DNT: 1..Upgr

00f0 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Insecure-Req

0100 75 65 73 74 73 3a 20 31 0d 0a 43 6f 6e 74 65 6e uests: 1 ..Conten

0110 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 t-Type: applicat

0120 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 ion/x-www-form-u

0130 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72 2d rlcencode d..User-

0140 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5

0150 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 .0 (X11; Linux x

0160 38 36 5f 36 34 29 20 41 70 70 6c 65 57 65 62 4b 86.64) AppleWebK

0170 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c it/537.3.6 (KHTML

0180 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 , like Gecko) Ch

0190 72 6f 6d 65 2f 31 32 37 2e 30 2e 30 2e 30 20 53 rome/127.0.0.0 S

01a0 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/537.3.6..Ac

01b0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: text/html,

01c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm

01d0 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml, applicatio