Matei Vlad Cristian
321 CC

Laborator

1.
Algoritmul folosit pentru semnarea certificatului :

sha256WithRSAEncryption

Entitatea care a eliberat certificatul :

Issuer: C = US, O = Google Trust Services, CN = GTS CA 1O1

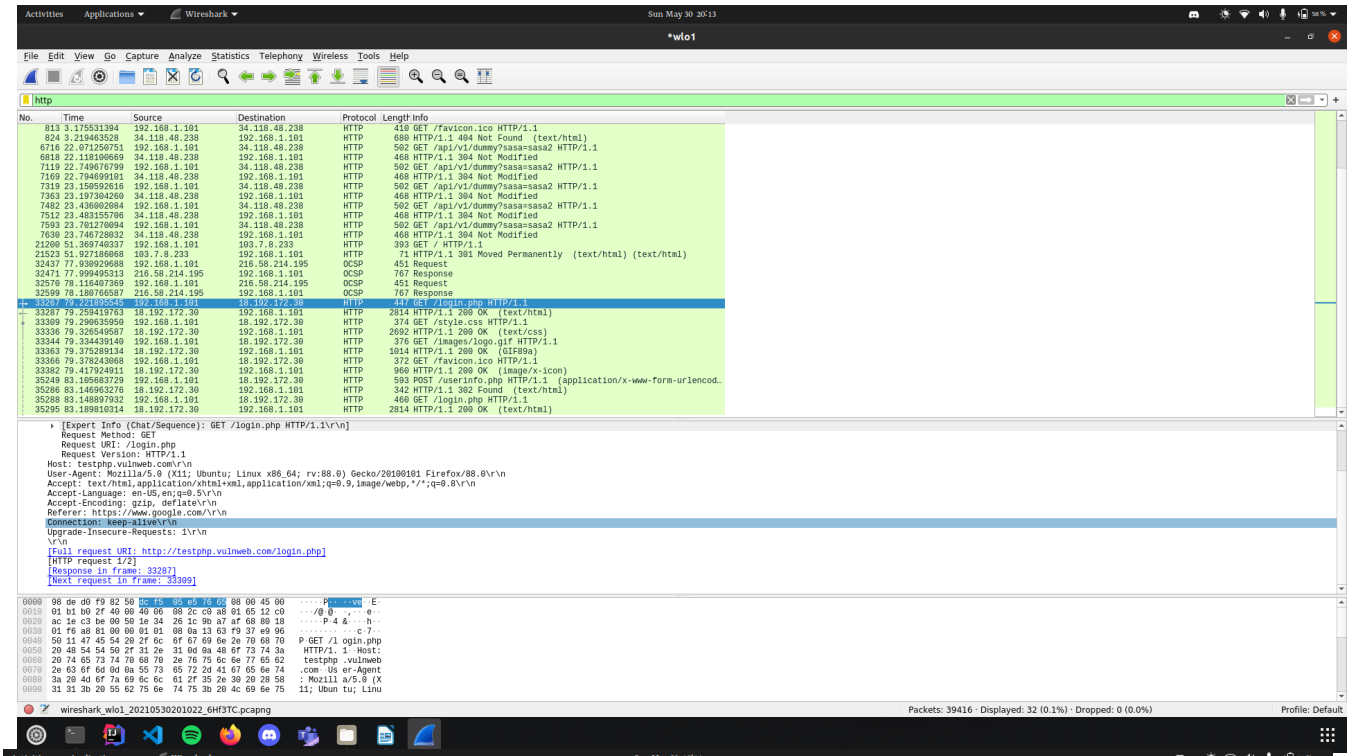
Intervalul de timp in care certificatul e valid :

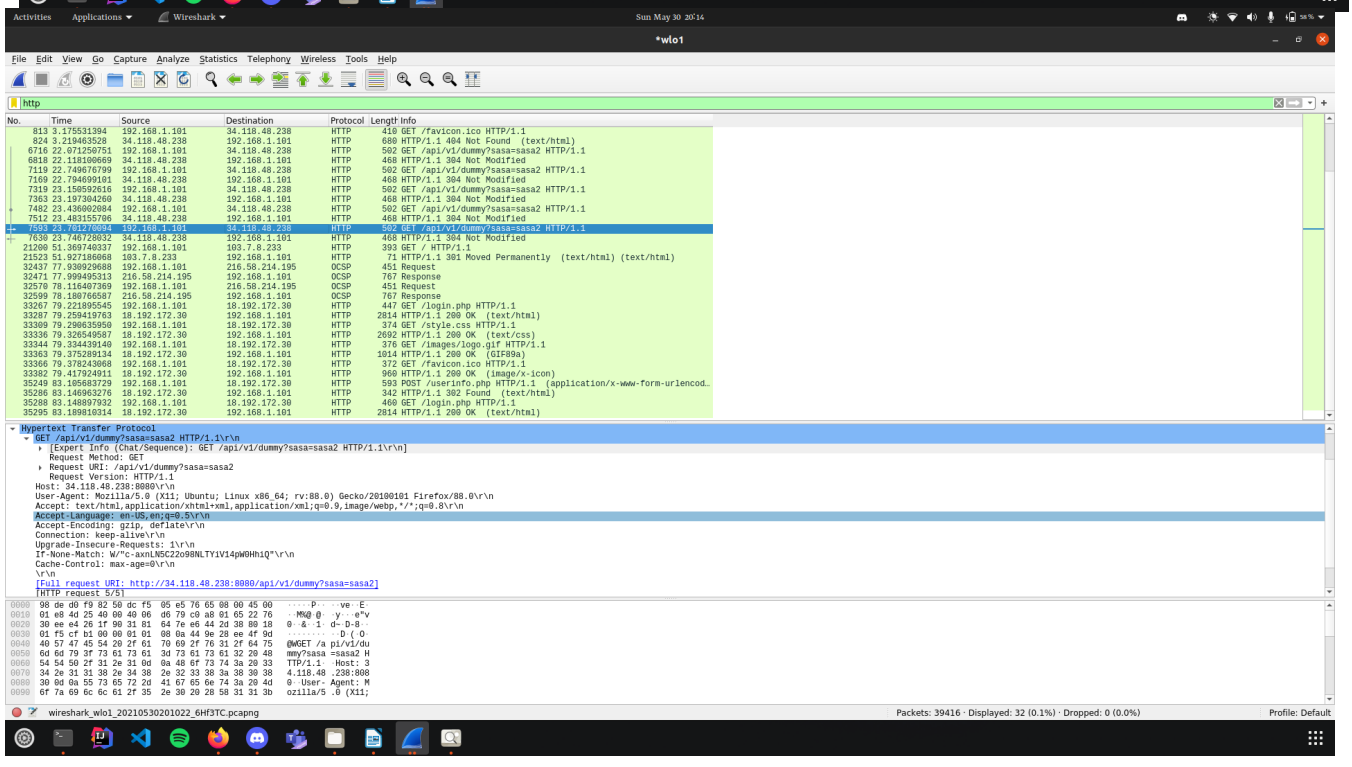
Validity
Not Before: May 3 09:02:30 2021 GMT
Not After : Jul 26 09:02:29 2021 GMT

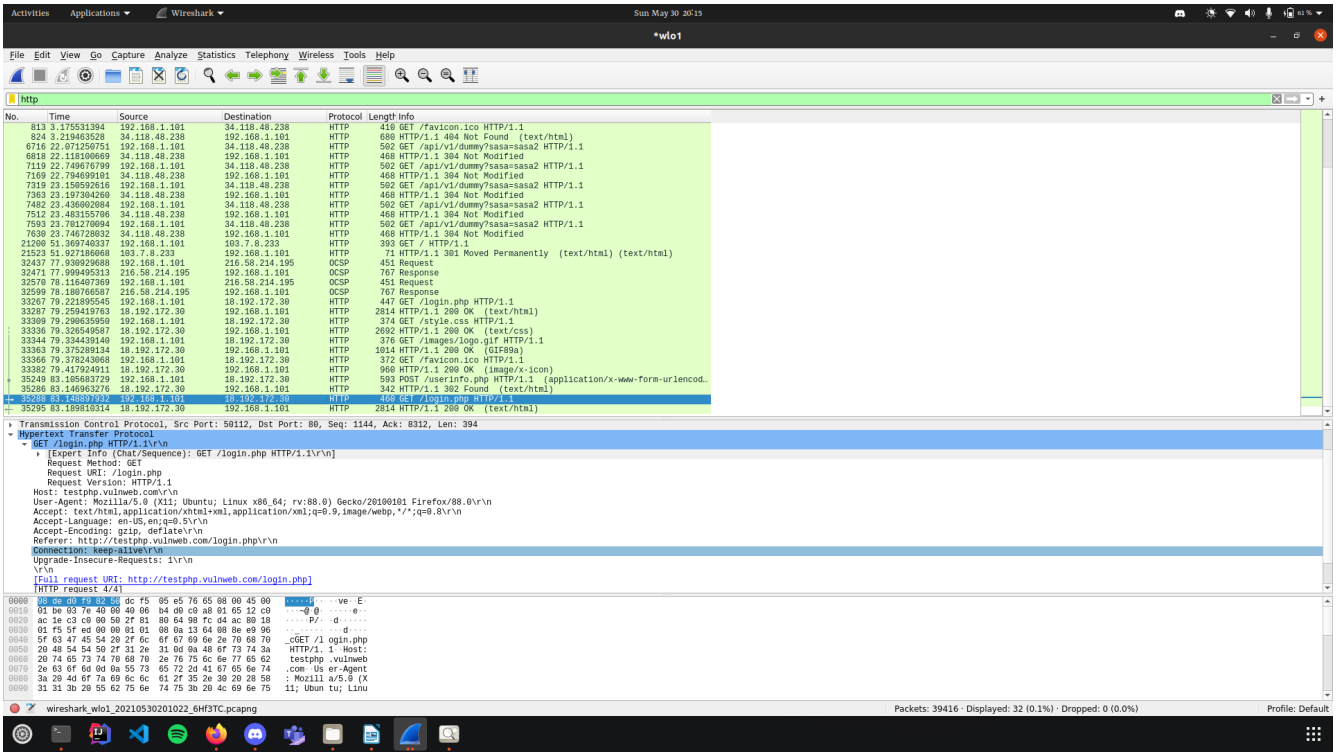
Cheia publica :

Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:f7:f7:de:4d:af:d6:b4:ca:b5:49:1f:df:90:71:
cd:f6:cb:b7:fd:7a:d9:db:39:e4:93:68:2c:9d:55:
fb:1f:30:4e:75:e0:ef:58:29:4c:ac:66:3e:02:63:
f5:e2:3f:bc:2c:e1:55:3d:ae:d8:54:95:84:03:7c:
3f:7b:d5:2f:25
ASN1 OID: prime256v1
NIST CURVE: P-256

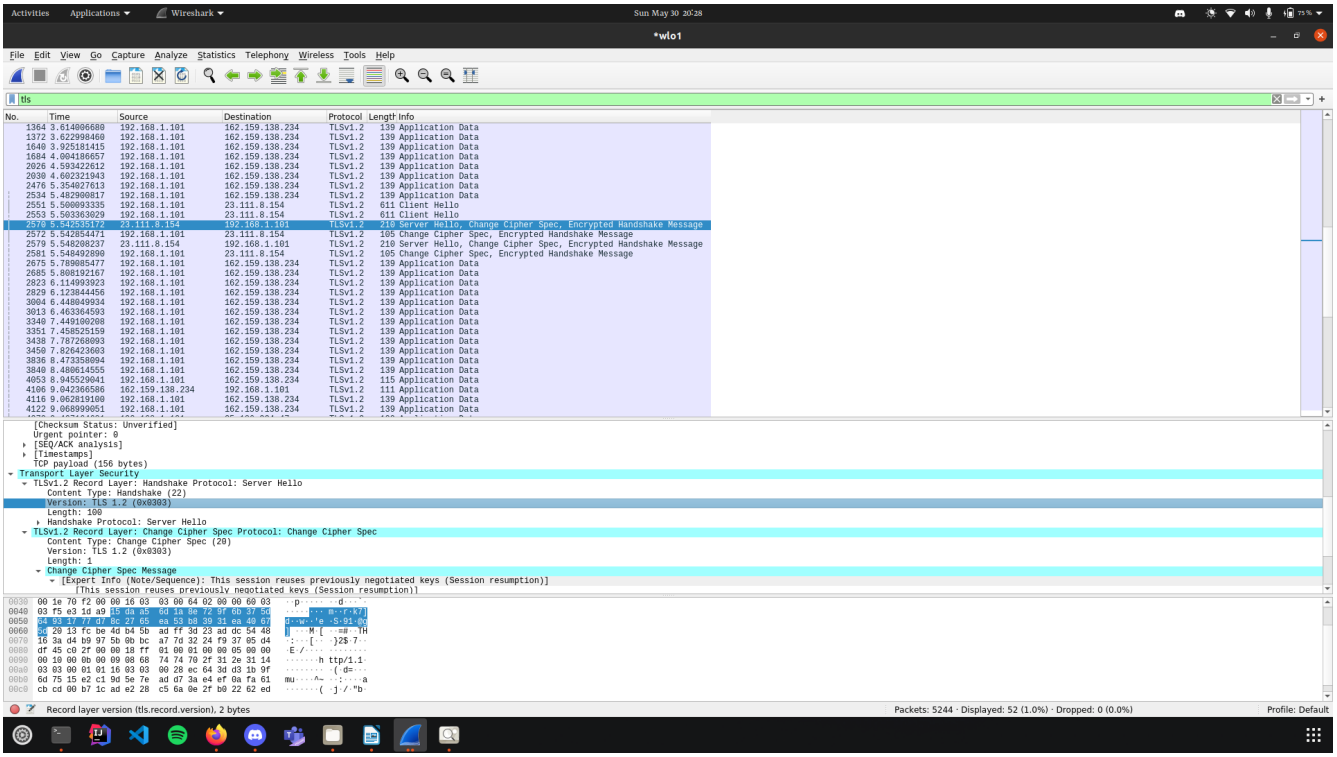
2.

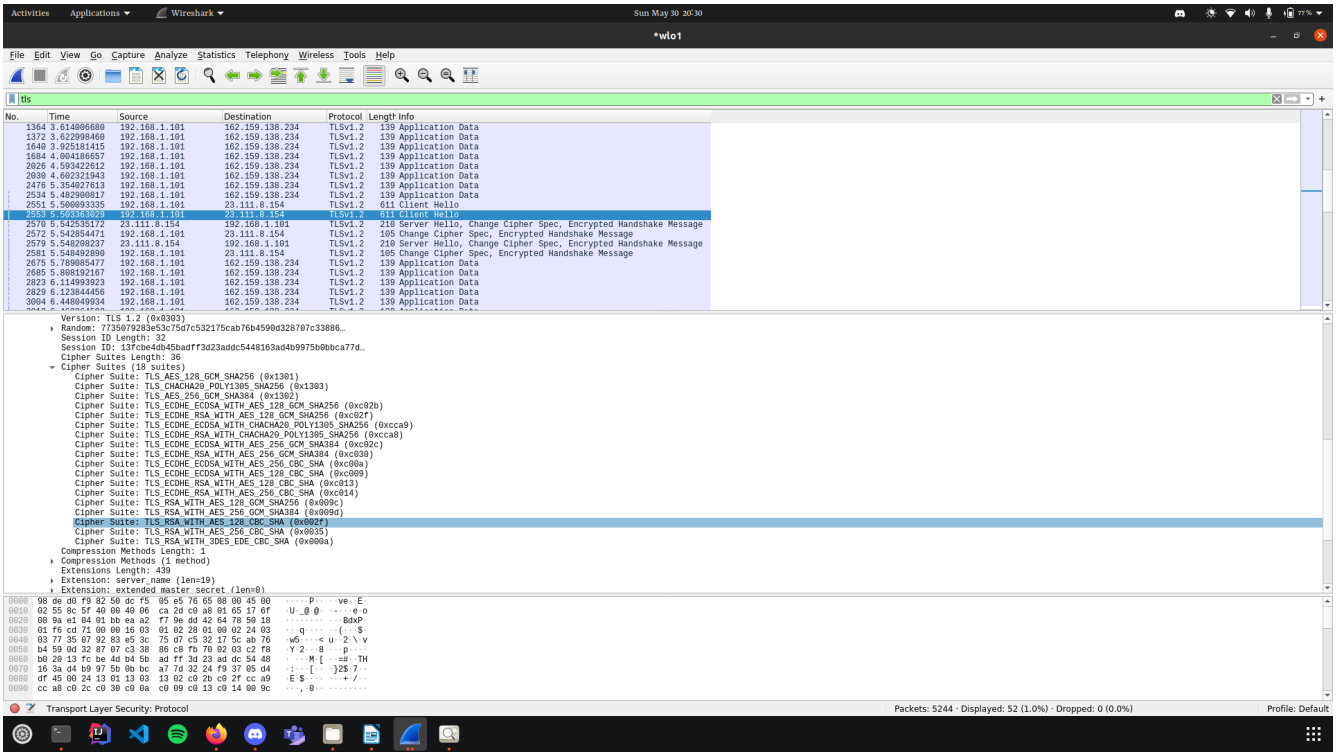

Activities
Applications
Wireshark
Sun May 30 20:13
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
813 3.175531394 192.168.1.101 34.118.48.238 HTTP 410 GET /favicon.ico HTTP/1.1
824 3.219463528 34.118.48.238 192.168.1.101 HTTP 680 HTTP/1.1 404 Not Found (text/html)
6716 22.071250751 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
6818 22.118100669 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7119 22.749676799 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7160 22.794609101 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7319 23.150592616 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7363 23.197304260 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7482 23.436002084 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7512 23.483155706 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7593 23.701270094 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7630 23.746728032 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
21200 51.369740337 192.168.1.101 103.7.8.233 HTTP 393 GET / HTTP/1.1
21523 51.927186068 103.7.8.233 192.168.1.101 HTTP 71 HTTP/1.1 301 Moved Permanently (text/html) (text/html)
32437 77.930929688 192.168.1.101 216.58.214.195 OCSP 451 Request
32471 77.999495313 216.58.214.195 192.168.1.101 OCSP 767 Response
32570 78.116407369 192.168.1.101 216.58.214.195 OCSP 451 Request
32599 78.180766587 216.58.214.195 192.168.1.101 OCSP 767 Response
33267 79.221895545 192.168.1.101 18.192.172.30 HTTP 447 GET /login.php HTTP/1.1
33287 79.259419763 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
33309 79.290635950 192.168.1.101 18.192.172.30 HTTP 374 GET /style.css HTTP/1.1
33336 79.326549587 18.192.172.30 192.168.1.101 HTTP 2692 HTTP/1.1 200 OK (text/css)
33344 79.334439140 192.168.1.101 18.192.172.30 HTTP 376 GET /images/logo.gif HTTP/1.1
33363 79.375289134 18.192.172.30 192.168.1.101 HTTP 1014 HTTP/1.1 200 OK (GIF89a)
33366 79.378243068 192.168.1.101 18.192.172.30 HTTP 372 GET /favicon.ico HTTP/1.1
33382 79.417924911 18.192.172.30 192.168.1.101 HTTP 960 HTTP/1.1 200 OK (image/x-icon)
35249 83.105683729 192.168.1.101 18.192.172.30 HTTP 593 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencod…
35286 83.146963276 18.192.172.30 192.168.1.101 HTTP 342 HTTP/1.1 302 Found (text/html)
35288 83.148097932 192.168.1.101 18.192.172.30 HTTP 460 GET /login.php HTTP/1.1
35295 83.189810314 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
[Expert Info (Chat/Sequence): GET /login.php HTTP/1.1\r\n]
Request Method: GET
Request URI: /login.php
Request Version: HTTP/1.1
Host: testphp.vulnweb.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: https://www.google.com/\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/login.php]
[HTTP request 1/2]
[Response in frame: 33287]
[Next request in frame: 33309]
0000 98 de d0 f9 82 50 dc f5 05 e5 76 65 08 00 45 00
0010 01 b1 b0 2f 40 00 40 06 d6 79 c0 a8 01 65 12 c0
0020 ac 1e c3 be 00 50 1e 34 26 1c 9b a7 af 68 80 18
0030 01 f6 a8 81 00 00 01 01 08 0a 13 63 f9 37 e9 96
0040 50 11 47 45 54 20 2f 6c 6f 67 69 6e 2e 70 68 70
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a
0060 20 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62
0070 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74
0080 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58
0090 31 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75
wireshark_wlo1_20210530201022_6Hf3TC.pcapng
Packets: 39416 · Displayed: 32 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Applications
Wireshark
Sun May 30 20:14
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
813 3.175531394 192.168.1.101 34.118.48.238 HTTP 410 GET /favicon.ico HTTP/1.1
824 3.219463528 34.118.48.238 192.168.1.101 HTTP 680 HTTP/1.1 404 Not Found (text/html)
6716 22.071250751 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
6818 22.118100669 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7119 22.749676799 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7160 22.794609101 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7319 23.150592616 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7363 23.197304260 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7482 23.436002084 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7512 23.483155706 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7593 23.701270094 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7630 23.746728032 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
21200 51.369740337 192.168.1.101 103.7.8.233 HTTP 393 GET / HTTP/1.1
21523 51.927186068 103.7.8.233 192.168.1.101 HTTP 71 HTTP/1.1 301 Moved Permanently (text/html) (text/html)
32437 77.930929688 192.168.1.101 216.58.214.195 OCSP 451 Request
32471 77.999495313 216.58.214.195 192.168.1.101 OCSP 767 Response
32570 78.116407369 192.168.1.101 216.58.214.195 OCSP 451 Request
32599 78.180766587 216.58.214.195 192.168.1.101 OCSP 767 Response
33267 79.221895545 192.168.1.101 18.192.172.30 HTTP 447 GET /login.php HTTP/1.1
33287 79.259419763 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
33309 79.290635950 192.168.1.101 18.192.172.30 HTTP 374 GET /style.css HTTP/1.1
33336 79.326549587 18.192.172.30 192.168.1.101 HTTP 2692 HTTP/1.1 200 OK (text/css)
33344 79.334439140 192.168.1.101 18.192.172.30 HTTP 376 GET /images/logo.gif HTTP/1.1
33363 79.375289134 18.192.172.30 192.168.1.101 HTTP 1014 HTTP/1.1 200 OK (GIF89a)
33366 79.378243068 192.168.1.101 18.192.172.30 HTTP 372 GET /favicon.ico HTTP/1.1
33382 79.417924911 18.192.172.30 192.168.1.101 HTTP 960 HTTP/1.1 200 OK (image/x-icon)
35249 83.105683729 192.168.1.101 18.192.172.30 HTTP 593 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencod…
35286 83.146963276 18.192.172.30 192.168.1.101 HTTP 342 HTTP/1.1 302 Found (text/html)
35288 83.148097932 192.168.1.101 18.192.172.30 HTTP 460 GET /login.php HTTP/1.1
35295 83.189810314 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
Hypertext Transfer Protocol
GET /api/v1/dummy?sasa=sasa2 HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /api/v1/dummy?sasa=sasa2 HTTP/1.1\r\n]
Request Method: GET
Request URI: /api/v1/dummy?sasa=sasa2
Request Version: HTTP/1.1
Host: 34.118.48.238:8080\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-None-Match: W/"c-axnLN6C2Zo9BNLTYiV14pW0HhiQ"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://34.118.48.238:8080/api/v1/dummy?sasa=sasa2]
[HTTP request 5/5]
0000 98 de d0 f9 82 50 dc f5 05 e5 76 65 08 00 45 00
0010 01 e8 4d 25 40 00 40 06 d6 79 c0 a8 01 65 22 76
0020 30 ee e4 26 1f 90 31 81 64 7e e6 44 2d 38 80 18
0030 01 f5 cf b1 00 00 01 01 08 0a 44 9e 28 ee 4f 9d
0040 40 57 47 45 54 20 2f 61 70 69 2f 76 31 2f 64 75
0050 6d 6d 79 3f 73 61 73 61 3d 73 61 73 61 32 20 48
0060 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 33
0070 34 2e 31 31 38 2e 34 38 2e 32 33 38 3a 38 30 38
0080 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
0090 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b
wireshark_wlo1_20210530201022_6Hf3TC.pcapng
Packets: 39416 · Displayed: 32 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Applications
Wireshark
Sun May 30 20:15
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
813 3.175531394 192.168.1.101 34.118.48.238 HTTP 410 GET /favicon.ico HTTP/1.1
824 3.219463528 34.118.48.238 192.168.1.101 HTTP 680 HTTP/1.1 404 Not Found (text/html)
6716 22.071250751 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
6818 22.118190669 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7119 22.749676799 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7169 22.794099101 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7319 23.150592616 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7363 23.197304260 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7482 23.436002084 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7512 23.483155706 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
7593 23.701270094 192.168.1.101 34.118.48.238 HTTP 502 GET /api/v1/dummy?sasa=sasa2 HTTP/1.1
7630 23.746728032 34.118.48.238 192.168.1.101 HTTP 468 HTTP/1.1 304 Not Modified
21200 51.369740337 192.168.1.101 103.7.8.233 HTTP 393 GET / HTTP/1.1
21523 51.927186068 103.7.8.233 192.168.1.101 HTTP 71 HTTP/1.1 301 Moved Permanently (text/html) (text/html)
32437 77.930929688 192.168.1.101 216.58.214.195 OCSP 451 Request
32471 77.999495313 216.58.214.195 192.168.1.101 OCSP 767 Response
32570 78.116407369 192.168.1.101 216.58.214.195 OCSP 451 Request
32599 78.180766587 216.58.214.195 192.168.1.101 OCSP 767 Response
33267 79.221895545 192.168.1.101 18.192.172.30 HTTP 447 GET /login.php HTTP/1.1
33287 79.259419763 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
33309 79.290635950 192.168.1.101 18.192.172.30 HTTP 374 GET /style.css HTTP/1.1
33336 79.326549587 18.192.172.30 192.168.1.101 HTTP 2692 HTTP/1.1 200 OK (text/css)
33344 79.334439140 192.168.1.101 18.192.172.30 HTTP 376 GET /images/logo.gif HTTP/1.1
33363 79.375289134 18.192.172.30 192.168.1.101 HTTP 1014 HTTP/1.1 200 OK (GIF89a)
33366 79.378243068 192.168.1.101 18.192.172.30 HTTP 372 GET /favicon.ico HTTP/1.1
33382 79.417924911 18.192.172.30 192.168.1.101 HTTP 960 HTTP/1.1 200 OK (image/x-icon)
35249 83.105683729 192.168.1.101 18.192.172.30 HTTP 593 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencod…
35286 83.146963276 18.192.172.30 192.168.1.101 HTTP 342 HTTP/1.1 302 Found (text/html)
35289 83.147039292 192.168.1.101 18.192.172.30 TCP 66 [TCP Dup ACK 35249#1] 46858 → 80 [ACK] Seq=1144 Ack=8312 Win=62848 Len=0 TSval=2814…
35295 83.180810314 18.192.172.30 192.168.1.101 HTTP 2814 HTTP/1.1 200 OK (text/html)
Transmission Control Protocol, Src Port: 50112, Dst Port: 80, Seq: 1144, Ack: 8312, Len: 394
Hypertext Transfer Protocol
GET /login.php HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /login.php HTTP/1.1\r\n]
Request Method: GET
Request URI: /login.php
Request Version: HTTP/1.1
Host: testphp.vulnweb.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
\r\n
[Full request URI: http://testphp.vulnweb.com/login.php]
[HTTP request 4/4]
wireshark_wlo1_20210530201022_6Hf3TC.pcapng
Packets: 39416 · Displayed: 32 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

3.


Activities
Applications
Wireshark
Sun May 30 20:28
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
No. Time Source Destination Protocol Length Info
1364 3.614006680 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
1372 3.622998460 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
1640 3.925181415 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
1684 4.004186657 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2026 4.593422612 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2030 4.602321943 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2476 5.354027613 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2534 5.482900817 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2551 5.500093335 192.168.1.101 23.111.8.154 TLSv1.2 611 Client Hello
2553 5.503363029 192.168.1.101 23.111.8.154 TLSv1.2 611 Client Hello
2570 5.541258172 23.111.8.154 192.168.1.101 TLSv1.2 210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
2572 5.542854471 192.168.1.101 23.111.8.154 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
2579 5.548208237 23.111.8.154 192.168.1.101 TLSv1.2 210 Server Hello, Change Cipher Spec, Encrypted Handshake Message
2581 5.548492090 192.168.1.101 23.111.8.154 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
2675 5.789085477 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2685 5.808192167 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2823 6.114993923 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
2829 6.123844456 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3004 6.448049934 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3013 6.463364593 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3340 7.449100208 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3351 7.458525159 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3438 7.787268093 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3450 7.826423603 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3836 8.473358094 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
3840 8.480614555 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
4053 8.945529041 192.168.1.101 162.159.138.234 TLSv1.2 115 Application Data
4106 9.042366586 162.159.138.234 192.168.1.101 TLSv1.2 111 Application Data
4116 9.062819100 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
4122 9.068999051 192.168.1.101 162.159.138.234 TLSv1.2 139 Application Data
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (156 bytes)
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 100
Handshake Protocol: Server Hello
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
[Expert Info (Note/Sequence): This session reuses previously negotiated keys (Session resumption)]
[This session reuses previously negotiated keys (Session resumption)]
Record layer version (tls.record.version), 2 bytes
Packets: 5244 · Displayed: 52 (1.0%) · Dropped: 0 (0.0%)
Profile: Default



Cea aleasa de server: