

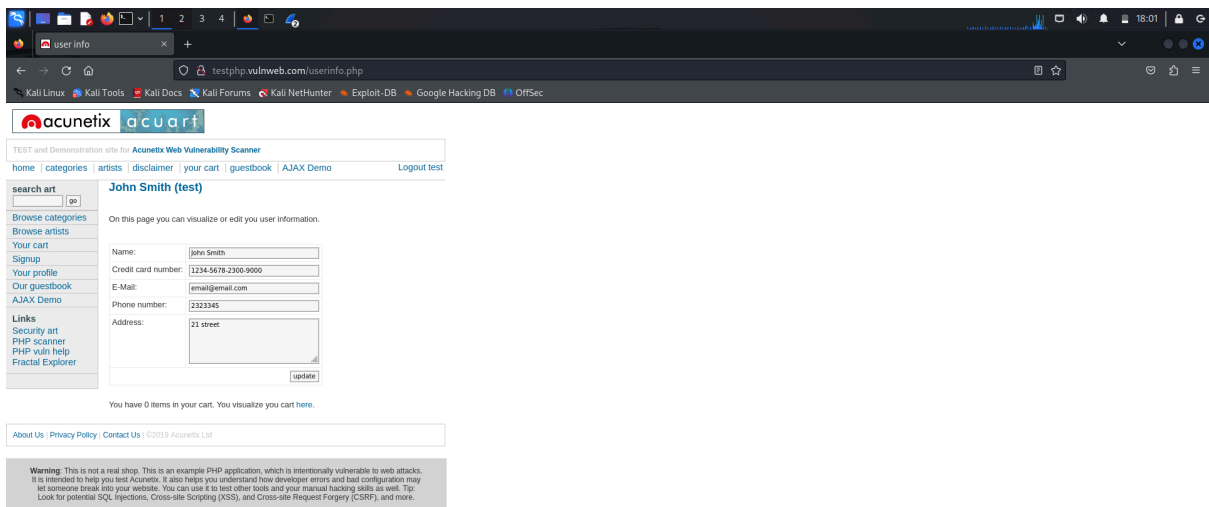
Session Persistence with Cookies in HTTP

1. Start Capturing in Wireshark:

- Begin by capturing traffic using Wireshark.

2. Perform a Login to a Website:

- Visit a website that requires a login (e.g., any forum or email service).
- Login with a test account and observe the packets in Wireshark.



Identify HTTP Cookies:

- Filter the traffic using `http`.
- Locate the HTTP requests and responses involving cookies.
- Take a screenshot of these packets

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
1 21.1.459961637 192.168.100.5 44.228.249.3 HTTP 448 GET /login.php HTTP/1.1
2 24.1.589802488 44.228.249.3 192.168.100.5 HTTP 1342 HTTP/1.1 200 OK (text/html)
3 30.9.362913835 192.168.100.5 44.228.249.3 HTTP 2974 HTTP/1.1 200 OK (text/html)

+ Frame 30: 502 bytes on wire (4056 bits), 502 bytes captured (4056 bits) on interface eth0, id 0
+ Ethernet II, Src: PCSysintec-ba-e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
+ Internet Protocol Version 4, Src: 192.168.100.5, Dst: 44.228.249.3
+ Transmission Control Protocol, Src Port: 80, Seq: 387, Ack: 2749, Len: 528
+ Hypertext Transfer Protocol
+ HTML Form URL Encoded: application/x-www-form-urlencoded
+ Form item: "uname" = "test"
+ Form item: "pass" = "test"

Hypertext Transfer Protocol (http), 508 byte(s) | Packets: 114 - Displayed: 4 (3.5%) | Profile: Default
```

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
1 21.1.459961637 192.168.100.5 44.228.249.3 HTTP 448 GET /login.php HTTP/1.1
2 24.1.589802488 44.228.249.3 192.168.100.5 HTTP 1342 HTTP/1.1 200 OK (text/html)
3 30.9.362913835 192.168.100.5 44.228.249.3 HTTP 2974 HTTP/1.1 200 OK (text/html)

+ Transmission Control Protocol, Src Port: 80, Seq: 37612, Seq: 2749, Ack: 915, Len: 2920
+ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
+ HTTP/1.1 200 OK\r\n
+ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
+ [HTTP/1.1 200 OK\r\n]
+ [Severity level: Chat]
+ [Group: Sequence]
+ Response Version: HTTP/1.1
+ Status Code: 200
+ [Status Code Description: OK]
+ Response Phrase: OK
+ Server: nginx/1.19.0\r\n
+ Date: Sun, 08 Sep 2024 21:54:03 GMT\r\n
+ Content-Type: text/html; charset=utf-8\r\n
+ Transfer-Encoding: chunked\r\n
+ Connection: keep-alive\r\n
+ X-Powered-By: PHP/5.6.40-38ubuntu20.04.1+deb.sury.org+1\r\n
+ Set-Cookie: login=test2;test=V\r\n
+ Content-Encoding: gzip\r\n
+ \r\n
+ [HTTP response 2/2]
+ [Time since request: 0.07715572 seconds]
+ [Prev request in frame: 24]
+ [Request in frame: 29]
+ [Request URI: http://testphp.vulnweb.com/userinfo.php]
+ HTTP chunked response
+ Content-encoded entity body (gzip): 2625 bytes -> 5963 bytes
+ File Data: 5963 bytes
+ Line-based text data: text/html (119 lines)

Hypertext Transfer Protocol (http.set_cookie), 31 byte(s) | Packets: 207 - Displayed: 4 (1.9%) | Profile: Default
```

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info
41 21.724415978 192.168.100.5 44.228.249.3 HTTP 748 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
42 27.338982789 192.168.100.5 44.228.249.3 HTTP 748 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
73 34.688988897 192.168.100.5 44.228.249.3 HTTP 424 GET / HTTP/1.1
75 34.814326423 44.228.249.3 192.168.100.5 HTTP 1188 HTTP/1.1 200 OK (text/html)
77 40.638982684 192.168.100.5 44.228.249.3 HTTP 471 GET /login.php HTTP/1.1
81 49.798850546 44.228.249.3 192.168.100.5 HTTP 1367 HTTP/1.1 200 OK (text/html)
88 51.080024193 192.168.100.5 44.228.249.3 HTTP 609 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
94 51.111622805 44.228.249.3 192.168.100.5 HTTP 228 HTTP/1.1 200 OK (text/html)

+ Frame 88: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits) on interface eth0, id 0
+ Ethernet II, Src: PCSysintec-ba-e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
+ Internet Protocol Version 4, Src: 192.168.100.5, Dst: 44.228.249.3
+ Transmission Control Protocol, Src Port: 40734, Dst Port: 80, Seq: 788, Ack: 5360, Len: 555
+ Hypertext Transfer Protocol
+ POST /userinfo.php HTTP/1.1\r\n
+ [Expert Info (Chat/Sequence): POST /userinfo.php HTTP/1.1\r\n]
+ [POST /userinfo.php HTTP/1.1\r\n]
+ [Severity level: Chat]
+ [Group: Sequence]
+ Request Method: POST
+ Request URI: /userinfo.php
+ Request Version: HTTP/1.1
+ Host: testphp.vulnweb.com\r\n
+ User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
+ 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=0.9
+ 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
+ Cookie: login=test2;test=V\r\n
+ Upgrade-Insecure-Requests: 1\r\n
+ \r\n
+ [Full request URI: http://testphp.vulnweb.com/userinfo.php]
+ [HTTP request 3/3]
+ [Prev request in frame: 77]

Hypertext Transfer Protocol (http.cookie), 27 byte(s) | Packets: 119 - Displayed: 11 (9.2%) | Profile: Default
```

GET request (loading the login page).

200 OK response (server's response to the GET request).

POST request (sending login credentials).

200 OK response (server's response after the login).

Analyze the Cookies:

- **Discuss how cookies are used to maintain session state.**

Cookie Set by the Server:

The server returned a response with a Set-Cookie header when you logged in:

Set-Cookie: test%2Ftest for login

The %2F is simply an encoded slash /. This instructs your browser to store a cookie called login with the value test/test.

The Cookie is stored by the browser:

This cookie (login=test/test) is saved by your browser and is linked to the page you visited.

The browser returns a cookie to the server.

This cookie is automatically included by your browser in the request header for all subsequent requests to the same website:

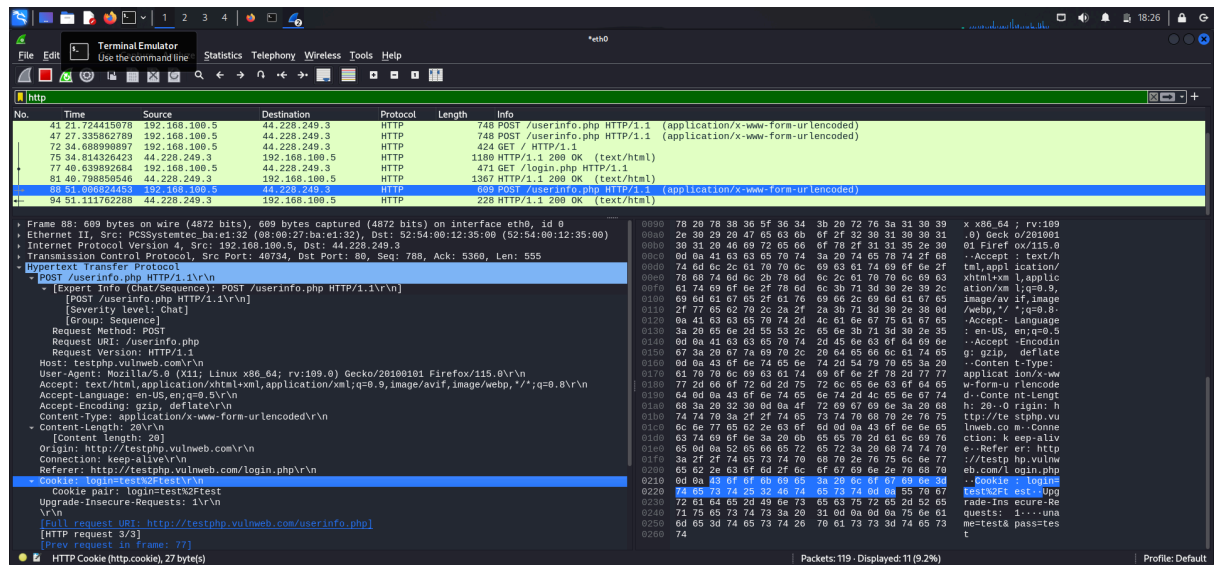
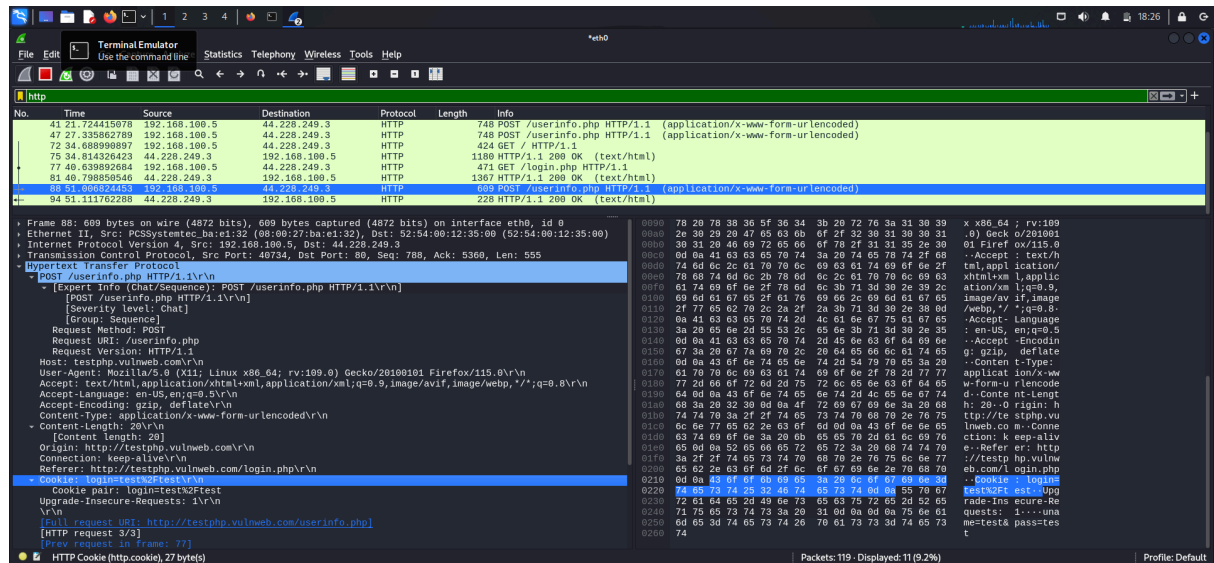
Cookie: test%2Ftest

In this manner, the server is aware that you are returning and can remember your choices or keep you logged in.

The cookie is used by the server to identify the session.

The login=test/test cookie is read by the server in order to identify your session and keep you logged in

Identify the Set-Cookie header in the server response and the Cookie header in subsequent client requests.



Document Findings:

- Write a report explaining how cookies help maintain sessions in HTTP.

Report: HTTP Session Maintenance via Cookies Overview

Cookies enable websites to keep track of you in between page views.

The server sends a cookie to your browser when you log in.

For instance: Cookie Set: login=test%2Ftest; Cookie Stored by the Browser:

This cookie is stored by your browser for that website.

Cookie is returned by the browser:

The browser transmits the cookie back to the server each time you interact with the website.

For instance: Cookie: login=test%2Ftest You Are Identified by the Server:

The cookie helps the server remember who you are, so it can maintain your login or store your preferences.

In summary

Cookies enable websites to retain your login information and continue your session when you visit different pages.