

## Redes: Protocolo HTTP

1. ¿Qué es una red? Es un conjunto de dispositivos interconectados como lo pueden ser computadoras, servidores, routers, etc.. y pueden comunicarse entre si
2. ¿Qué es el modelo TCP/IP y escribe sus capas? Es el modelo de Internet, y es un conjunto de protocolos que se usa para la comunicación en redes.
  - Capa de acceso: Es la comunicación física en la red, esta define los datos de transmisión a través de medios físicos.
  - Capa de Internet: Es la capa de enrutamiento de los datos, a través de la red y proporciona el direccionamiento IP de los dispositivos.
  - Capa de transporte: Esta capa se encarga de la comunicación de extremos a extremo y ahí están los protocolos TCP, UDP.
  - Capa de Aplicación: Esta capa se encarga de las aplicaciones y servicios de la red, se encuentran los protocolos HTTP, FTP, etc...
3. ¿Qué es una IP? Es una etiqueta numérica lógica que es asignada a un dispositivo conectado a una red, esta puede ser dinámica o estática y puede ser IPV4 o IPV6.
4. ¿Qué es el protocolo TCP? Transmission control protocol y es para poder tener una comunicación confiable entre los dispositivos de la red, garantiza la entrega ordenada de los paquetes.
5. Dentro del protocolo TCP, ¿qué es el protocolo HTTP? HTTP esta basado en la confiabilidad y la conexión que es establecida por el protocolo TCP, tiene el TLS Handshake
6. Puerto del protocolo HTTP. 80
7. Puerto del protocolo HTTPS. 443
8. Diferencia entre HTTP y HTTPS. La gran diferencia es que HTTP no es seguro y HTTPS agrega una capa de cifrado que nos ayuda a proteger la privacidad y la integración de los datos que transmitimos.
9. ¿Qué significa el modelo cliente - servidor? Es la forma de dividir al cliente y al servidor, ya que cada uno tiene un rol específico, por decir... el cliente es un dispositivo o aplicación que solicita recursos, envía peticiones y estos pueden ser computadoras, teléfonos, etc... y un servidor es una aplicación o dispositivo que proporciona los recursos a un cliente.
10. ¿Qué es una request? Es un mensaje enviado por un cliente a un servidor para solicitar un recurso específico.

11.¿Qué es una response? Es el mensaje enviado por un servidor en respuesta a la request de un cliente, esto puede ser a través de un navegador web.

12.Los siguientes códigos de respuesta a qué se refieren:

- 200: Es cuando la petición fue exitosa (OK)
- 301: Cuando existe un redireccionamiento
- 400: No se pudo interpretar la solicitud por una sintaxis invalida (Bad Request)
- 401: Es necesario autenticarse para obtener la respuesta indicada (Unauthorized)
- 403: El cliente no posee los permisos necesarios y el servidor rechaza la petición (Forbidden)
- 404: El servidor no logro encontrar el contenido (Not Found)
- 500: El servidor no sabe cómo manejar una situación específica por demasiadas peticiones (Internal Server Error)

13.Lenguajes de programación del lado del servidor (Back End). PHP, Python, Ruby, Java, C#

14.Lenguajes de programación del lado del cliente (Front End). HTML, CSS, JavaScript, Angular, jQuery

15.¿Qué es Burp Suite? Es una herramienta que nos ayuda a las pruebas de aplicaciones web, para identificar vulnerabilidades, cuenta con algunas características como lo son: Proxy, Intruder, Repeater,

16.Explica el modelo 3-Way Handshake. Es el proceso para poder establecer la conexión entre dos dispositivos en el protocolo TCP, y se hace de la siguiente manera: SYN – SYN ACK – ACK, esto es para garantizar que ambas partes estén sincronizadas.

17.Explica el modelo TLS Handshake. Es un proceso que se utiliza en la creación de conexiones seguras en internet. TLS es usado para garantizar la confidencialidad, la integridad y la autenticación de los datos y se hace de la siguiente manera. SYN – SYN ACK – ACK – Client Hello – Server Hello - Intercambio de llaves – Intercambio de llaves – HTTP

```

1 GET /advanced_search?search-term=test&organize_by=DATE&writer= HTTP/1.1
2 Host: acb01fc91f1ded42c005534500de0010.web-security-academy.net
3 Cookie: _lab=
4 47%7cMC0CFQvRgHmMdlwIIuFBGyv66dij71IAhUAK8SKLmvD8DahR562%2bxOI95kT6EnA%2f%2f8fv7Z15yS8f16wG1X2SzbC1I9RWbku
5 asTZApeydfTST9cn6NSEsQWhTFqVXtXCHk%2fOAc5j72NDwHN6vcvkY%2ff4c3zlVwLdsb3Jeqn5Ye4ZUCf0; session=
6 PHaOH0Zf1jIMEGPPahn7CVtP4QIKyuW
7
8 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"
9 Sec-Ch-Ua-Mobile: ?0
10 Sec-Ch-Ua-Platform: "Windows"
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Chrome/99.0.4844.84 Safari/537.36
14 Accept:
15 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/*;q=0.8,application/signed-exchange;v=b3;q=0.9
16
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: navigate
19 Sec-Fetch-User: ?1
20 Sec-Fetch-Dest: document
21 Referer: https://acb01fc91f1ded42c005534500de0010.web-security-academy.net/advanced_search
22 Accept-Encoding: gzip, deflate

```

- Método: GET
- Recurso: advanced\_search
- URL: acb01fc91fded42c005534500de0010.web-security-academy.net
- ¿Es una petición autenticada?: Si
- ¿Chrome o Firefox?: Chrome
- Versión del protocolo HTTP: 1.1
- ¿Cuántas cabeceras tiene?: 14

```

1 HTTP/1.1 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 2519
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
12      App 2 - 
13    </title>
14  </head>
15  <script src="/resources/labheader/js/labHeader.js">
16  </script>
17  <div id="academyLabHeader">
18    <section class='academyLabBanner'>
19      <div class=container>
20        <div class=logo>
21          </div>

```

- Tipo de documento: HTML
- Código de estado: 500
- Longitud: 2519

20. De la siguiente imagen obtén lo siguiente:

```

Pretty Raw Hex
1 GET /current_user HTTP/2
2 Host: hackerone.com
3 Cookie: h1_device_id=72d8469b-c716-421d-b2fe-0fdcf8f6bd96; __ga=GA1.2.1245302275.1648495179; amp_b7cba2=
v4nxCPX2qHxvGwq_om2PVJ...1fvp41gsk.1fvp41gu9.3.0.3; __gid=GA1.2.2129463882.1649036805; __Host-session=
MkEya0JN0WVreE9jTHA1bFNFTFc5bXpsb0M3eDj4eFk2K1J0cmkyVHZ4L0VEQ1l1ci9ZbndQRk10ZkZHd0hFbGgzTXpwcWxYa0hIOhNlaFRLeK
NKSnlIT0Z2NkpYaXVJV2I1ZXdbS84TEhPRUX1SDRQUHV3QktHMWRLS1hyN09qQ0dnQnMxbFBhby9KVXNYS0gyUS91VEFyZlNEWE1ZcnVuSTUx
cVdjS2lie1E3aFJKQ3JUQTJ0TH16cEFjQldCTGg5bFVJZ01LOV1lRXJ6cnRkUkcybVJld00vYzJud3d1eXpUa0JNaS9hdFpnaF1ENXVxZHJRWD
BvbVJaU3YrbnE3UEVTZ3EyYkVXbXNLTW1J0XlqUUhQOVNOU09KRGRZNzJ0MVZMTWtRY289LS1nZGh1d3pCRWhpbEx4VzR2MctSVjZnPT0%3D--
488e6fc026e509e113202b0ccf8bfebb40b376b
4 Sec-Ch-UA: " Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"
5 Accept: application/json, text/javascript, */*; q=0.01
6 X-Requested-With: XMLHttpRequest
7 Sec-Ch-UA-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.84 Safari/537.36
9 Sec-Ch-UA-Platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://hackerone.com/reports/329837

```

- Método: GET
- Recurso: /current\_user
- URL: [https://hackerone.com/current\\_user](https://hackerone.com/current_user)
- ¿Es una petición autenticada?: si
- Versión del SO: 10
- ¿Cuál es la URL anterior?: <https://hackerone.com/reports/329837>
- ¿Acepta código XML?: Si

21. De la siguiente imagen obtén lo siguiente:

```

Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Mon, 04 Apr 2022 01:47:02 GMT
3 Content-Type: application/json; charset=utf-8
4 Cache-Control: no-store
5 Content-Disposition: inline; filename="response.json"
6 Vary: Accept
7 X-Request-Id: 847b5f43-67d7-48af-82ea-937ca847437d
8 Etag: W/"5ebfb1ea5a116b061c5f99619845a2f0"
9 Set-Cookie: __Host-session=
NWpOY09WODUvYmFVUGdCUEQwVnh0SEURWnkY2tNSHV5bYtZYWoycHRqY2x6SmZ4TG15V1hBM1N0SnVOVnlzMmZXdDQ2MctGdTZMQ0QrUitOaD
lqWw51NVRyYjMxS01GwJf3U1NjdGRlUzFiNkc2WlhGcmZXSvBuc0RQV1VSL3hTSdhaTUZCwnltT0VaU3pFSgdlQn1PY0hWnXNlaEo0SURQY1RV
NE0yZkp3d2tKb0RjQ1FISVRPek1yV1N2RS9ISHRySHJrcWxGeVlCakh2bzVhaTVIbDFicmtJRTNiZmF1TTRvSVFRE1yWmdTMjb6WVdwWjc4ZF
BNUm1DTV1ldU5aNXMwOD13ZmtCaEoxdWRmaDAyVCTlUjcvUUVaL2phWFpimG55S1p4UTQ9LS1US1c2a1JjTjB1K3l0VmtaRUlmWGJ3PT0%3D--
8845b3315cc2b65e6ff56f8f331bacb4b6159824; path=/; expires=Mon, 18 Apr 2022 01:47:02 GMT; secure; HttpOnly;
SameSite=None
10 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
11 X-Frame-Options: DENY
12 X-Content-Type-Options: nosniff
13 X-Xss-Protection: 1; mode=block
14 X-Download-Options: noopen

```

- Tipo de documento: Json
- Código de estado: 200
- Longitud: N/A