Redes: Protocolo HTTP

1. ¿Qué es una red?  La conexión entre múltiples dispositivos o computadoras utilizando dispositivos alámbricos o inalámbricos
2. ¿Qué es el modelo TCP/IP y escribe sus capas? Es un modelo que sirve para transferir información entre dispositivos físicos de manera segura. Tiene 4 capas pero las más importantes son IP, TCP y aplicación
3. ¿Qué es una IP?  Es la dirección que te identifica en la red
4. ¿Qué es el protocolo TCP? Un protocolo para transporte y control de datos entre distintos dispositivos a través de la red.
5. Dentro del protocolo TCP, ¿qué es el protocolo HTTP? Un protocolo de transferencia de datos que vuelve las comunicaciones más eficientes al utilizar un esquema de “petición-respuesta”.
6. Puerto del protocolo HTTP.  80
7. Puerto del protocolo HTTPS. 443
8. Diferencia entre HTTP y HTTPS. El protocolo HTTPS es más seguro al cifrar los datos, mientras que el HTTP sólo permite transferencias de texto plano
9. ¿Qué significa el modelo cliente - servidor? Significa que regula la comunicación entre cliente (quien pide recursos) y el servidor (quien proporciona esos recursos)
10. ¿Qué es una request? La solicitud de recursos por parte del cliente
11. ¿Qué es una response? La respuesta con el recursos por parte del servidor hacia la solicitud o request del cliente
12. Los siguientes códigos de respuesta a qué se refieren:

* 200: Ok, todo está correcto
* 301: El dominio se movió permanentemente
* 400: Solicitud incorrecta
* 401: No autorizado, el cliente no tiene las credenciales necesarias
* 403: Acceso denegado
* 404: El recurso no se ha encontrado
* 500: Error interno

1. Lenguajes de programación del lado del servidor (Back End). Php, asp.net, java, python
2. Lenguajes de programación del lado del cliente (Front End).  jQuery, Swift, SASS, React, JavaScript, CSS, HTML, Angular, Vue.
3. ¿Qué es Burp Suite? Un proxy que permite intervenir y modificar las comunicaciones entre un navegador y un servidor
4. Explica el modelo 3-Way Handshake. El cliente emite una solicitud de conexión a la capa TCP, luego el servidor envía al cliente un Syn y un ACK, y luego el cliente envía un ACK de regreso
5. Explica el modelo TLS Handshake. El cliente solicita al servidor una conexión segura. Luego, el servidor proporciona su certificado digital. Después, ambos establecen una clave de sesión usando la clave pública del servidor.
6. De la siguiente imagen obtén lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Método: GET
* Recurso: /advanced\_search?search-term=test’&organize\_by=DATE&writer=
* URL: http://acb01fc91f1ded42c005534500de0010.web-security-academi.net
* ¿Es una petición autenticada?: Si
* ¿Chrome o Firefox?: Chrome
* Versión del protocolo HTTP: 1.1
* ¿Cuántas cabeceras tiene?: 15

1. De la siguiente imagen obtén lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Tipo de documento: html
* Código de estado: 500, Error Interno
* Longitud: 2519

1. De la siguiente imagen obtén lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Método: Get
* Recurso: current\_user
* URL: https://hackerone.com
* ¿Es una petición autenticada?:  Si
* Versión del SO: 10.0
* ¿Cuál es la URL anterior?:  https://hackerone.com/reports/329837
* ¿Acepta código XML?: Si

1. De la siguiente imagen obtén lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Tipo de documento: json
* Código de estado: 200
* Longitud: No se muestra