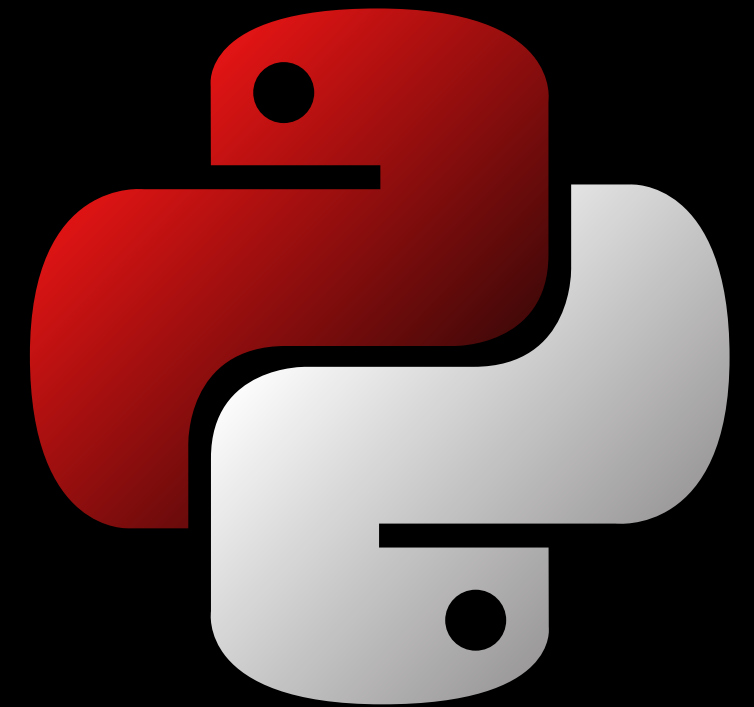


DEEPSEC ACADEMY

DeepSec **Pentesting Web** Python Course



Paginas Web

¿Que es Http?

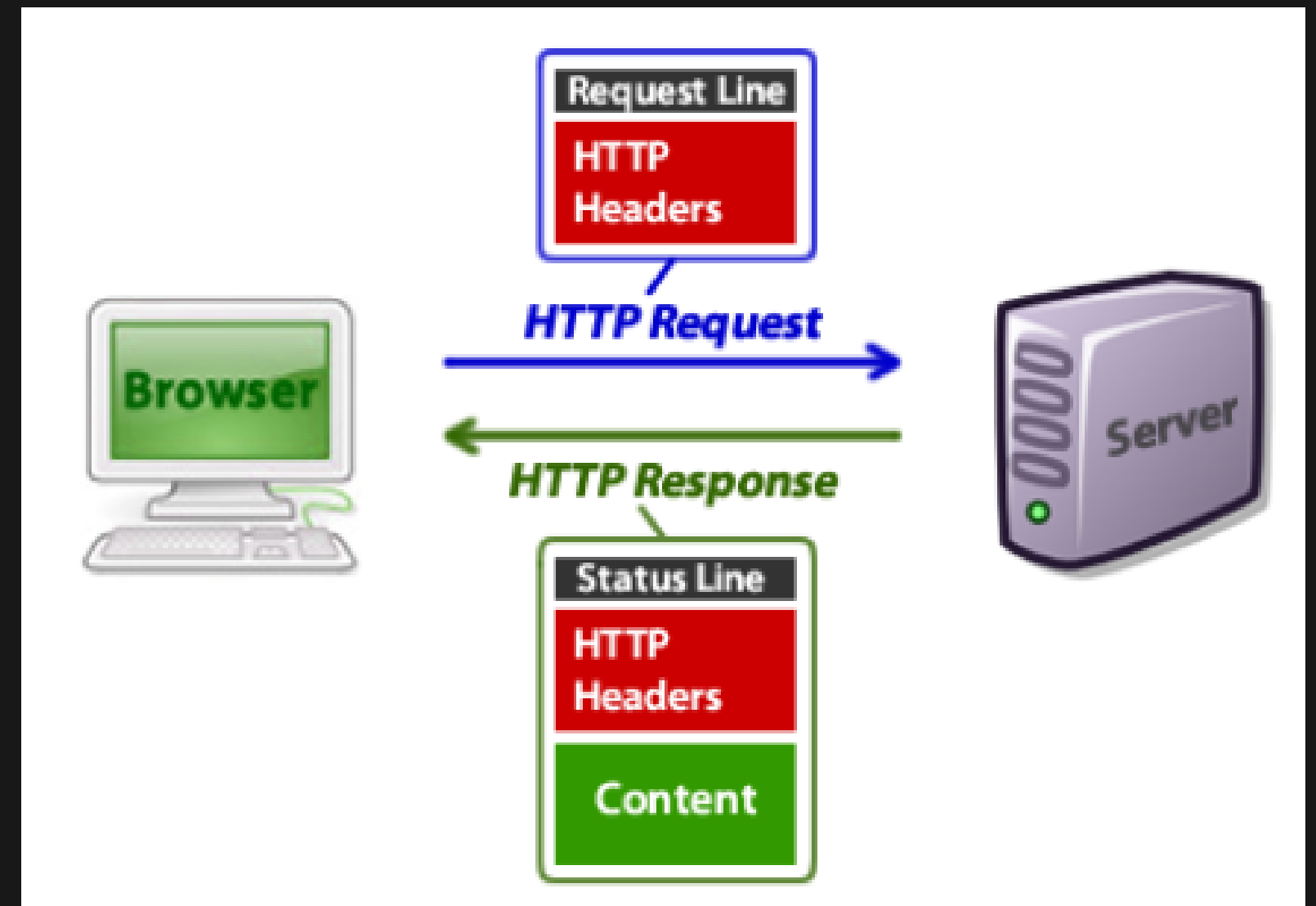
El protocolo de transferencia de hipertexto es el protocolo de comunicación que permite las transferencias de información a través de archivos en la World Wide Web.



Paginas Web

¿Que son las cabeceras HTTP?

Las cabeceras HTTP son la parte central de esas solicitudes y respuestas HTTP, y transportan informacion sobre el navegador cliente, la pagina solicitada, el servidor, etc.



Paginas Web

HTTP Request

Cuando envias una solicitud HTTP desde tu navegador por detras se vee:

GET / HTTP/1.1

Host: 192.168.86.33

User-Agent: curl/7.84.0

Accept: */*

Paginas Web

HTTP Request

Un HTTP Request se compone de:

Metodo: GET, POST, PUT, etc Indica que tipo de request es.

Path: /static/files/ La URL que se solicita, donde se encuentra el resource

Protocolo: HTTP/1.1 Contiene la version de HTTP, actualmente 1.1

Headers. Son esquemas de key:value que contienen informacion sobre el HTTP request y el navegador

Body. Si se envia informacion al servidor a traves de POST o PUT esta va en el body

Paginas Web

Headers comunes

Uno de los Headers mas comunes en los HTTP Requests son:

- **Host:** 192.168.86.33 (Host server)
- **User-Agent:** Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36 (nombre y version de navegador, sistema operativo y idioma por defecto)
- **Accept-Language:** en-us, en;q=0.5 (Lenguaje por defecto del usuario)
- **Accept-Encoding:** gzip, deflate, sdch (Codificacion del contenido, algortimo de compresion)

Paginas Web

Metodos HTTP

GET: Se emplea para leer una representacion de un resource. En caso de respuesta positiva (**200 OK**), GET devuelve la representacion en un formato concreto HTML, XML, JSON o imagenes, Javascript, CSS, etc. En caso de respuesta negativa se devuelve (**404 Not Found**) o (**400 Bad Request**).

Ejemplo carga de una pagina web, primero carga la URL solicitada:

GET files/docs HTTP/1.1


En este caso devuelve un HTML y despues se cargan los resources (js, css):

GET files/docs/logo.png HTTP/1.1

Paginas Web

Metodos HTTP

```
<form action="formget.php" method="get">  
  Nombre: <input type="text" name="nombre"><br>  
  Email: <input type="text" name="email"><br>  
  <input type="submit" value="Enviar">  
</form>
```



Nombre:

Email:

GET ejemplo.com/login.php?nombre=Gabriel&email=gabrielcock@gmail.com HTTP/1.1

Paginas Web

Metodos HTTP

POST: Aunque se puedan enviar datos a traves del metodo GET, en muchos casos se utiliza POST por la limitaciones de GET(La URL solo puede tener ASCII y no es posible enviar 2000 caracteres). En caso de respuesta positiva devuelve (201 Created). Los POST requests se envian normalmente con formularios

Paginas Web

Metodos HTTP

```
<form action="formget.php" method="get">
  Nombre: <input type="text" name="nombre"><br>
  Email: <input type="text" name="email"><br>
  <input type="submit" value="Enviar">
</form>
```



Nombre:

Email:

POST ejemplo.com/login.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Content-Length: 43

.....

nombre=Gabo&email=gabrielcock@gmail.com

Paginas Web

HTTP Response

Cuando el servidor recibe el HTTP Request recibiras una respuesta HTTP, y la cabecera que envia el HTTP Response es masomenos asi:

HTTP/1.1 200 OK

Date: Thu, 18 Aug 2022 13:01:24 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

Content-Type: text/html

Paginas Web

HTTP Response

Uno de los Headers mas comunes en los HTTP Response son:

- **Cache-Control:** `max-age=3600, public` (max-age: segundos en los cuales es valida, public: significa que cualquiera puede cachear esa Header)
- **Cache-Control:** `no-cache` (Se puede evitar el cacheo con no-cache)
- **Content-Type:** `text/html; charset=UTF-8` (decide como el navegador debera de interpretar el contenido) (mime-type)
- **Content-Type:** `application/pdf`
- **Content-Disposition:** `attachment; filename="descargar.zip"` (Indica al navegador que abra una caja de descarga de archivos, en lugar de analizar el contenido)

Paginas Web

HTTP Response

Uno de los Headers mas comunes en los HTTP Response son:

- **Content-Length:** 12345 (Longitud del contenido)
- **Etag:** "pub121212441;gz" (Util al momento de descargar archivos, asi el navegador puede calcular el progreso de la descarga)
- **Last-Modified:** Thu, 19 Aug 2022 11:50:11 GMT (Indica la ultima fecha de modificacion del documento en formato GMT)
- **Set-Cookie:** <cookie> (Envio de una cookie)
- **Content-Encoding:** gzip (Header enviado cuando el contenido esta comprimido)

DEEPSEC ACADEMY

¡Muchas gracias!