ATAQUES CSRF

HACKING

CONCEPTOS

HTTP: Estándar (protocolo) para acceder a páginas web.

Método HTTP: Forma de transmitir datos vía HTTP.

Parámetros: Valores pasados a un programa.

Query string: "Cadena de búsqueda" pasada a una página.

MÉTODOS HTTP

GET

Envía datos de forma **visible** a una página web. Se ve en forma de *URL*.

MÉTODOS HTTP

POST

Envía datos parcialmente **ocultos** a una página web. Es usado en formularios de registro, inicio de sesión, compras.

MÉTODOS HTTP

PUT

"Pone" o actualiza recursos en un servidor. Tiene usos especiales.

MÉTODOS HTTP

DELETE

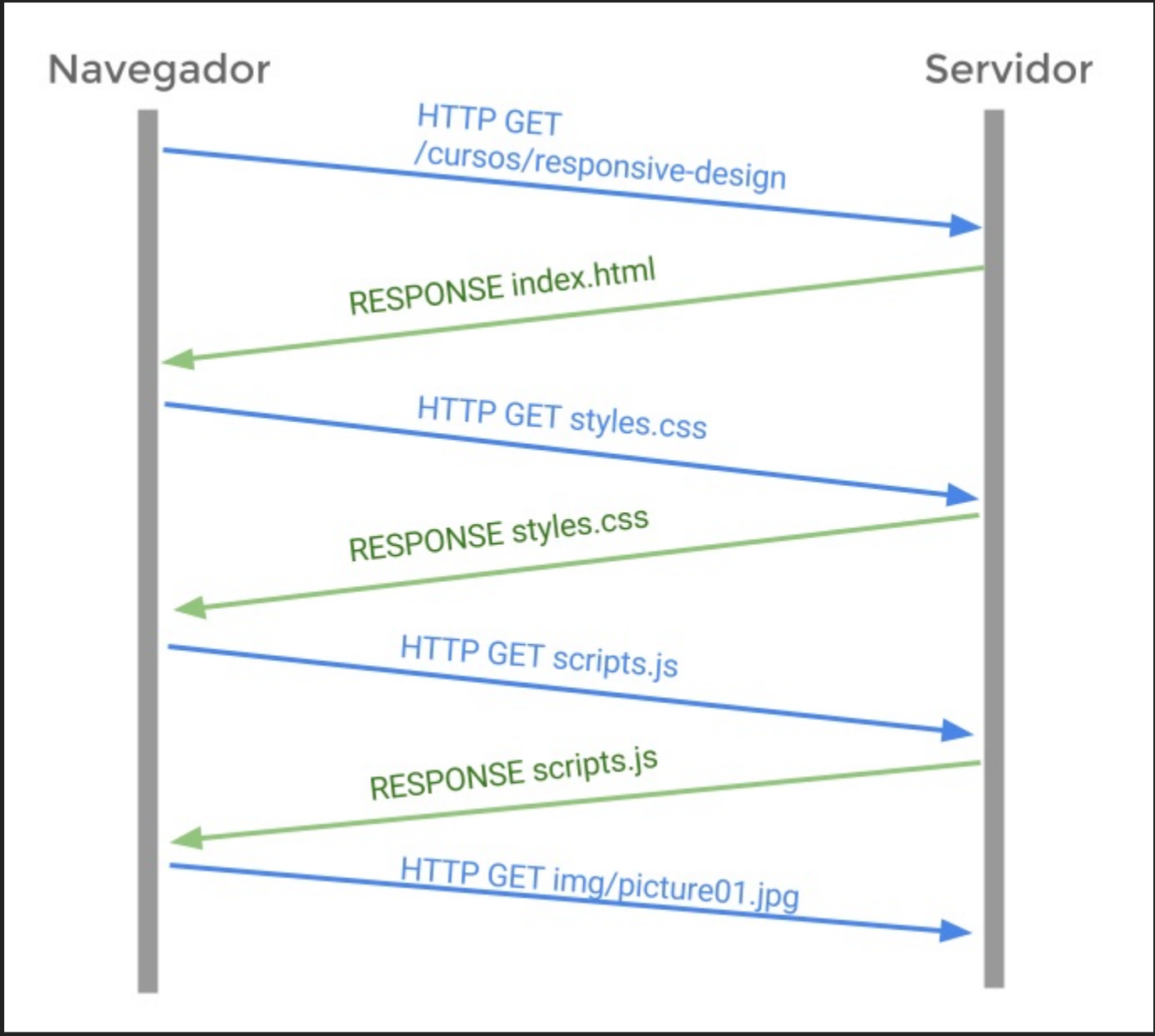
Elimina un recurso del servidor. También tiene usos especiales.

MÉTODOS HTTP

HEAD, OPTIONS, PATCH

Métodos adicionales, usados en aplicaciones grandes.

CARGA DE DATOS



¿QUÉ ES CSRF?

CSRF indica *Cross Site Request Forgery*.

¿QUÉ ES CSRF?

CROSS

"Cruz", o "cruce", hace referencia a un cruce de lugares, o sitios web.

¿QUÉ ES CSRF?

SITE

El sitio web siendo atacado, o que admite CSRF.

¿QUÉ ES CSRF?

REQUEST

La petición del usuario, al navegar, obtener imágenes, entre otros.

¿QUÉ ES CSRF?

FORGERY

Falsificación.

HTTP BASICS

OBTENCIÓN DE RECURSOS

Al cargar una página, el navegador:

1. Lee las etiquetas que piden recursos.
2. Pide el recurso al servidor web.
3. Si obtuvo el recurso, lo agrega localmente.
4. Si no lo obtuvo, notifica al navegador.

HTTP BASICS

OBTENCIÓN DE RECURSOS

¿Vieron algo de raro en la diapositiva anterior?

ESCENARIOS

SESIONES

Para que un CSRF sea "malo", se debe dar inicios de sesión.

ESCENARIOS

COMPRAS/PAGOS

En tu "carrito" pueden andar cosas sospechosas... Pero como tú vas a pagar por ellas, ¿qué importa?

ESCENARIOS

MUCHOS MÁS

¿Por qué los ataques CSRF pueden estar en todos lados?

IMPLICACIONES

SORPRESAS

Abriste un enlace y tienes US$ 5 dólares menos.

IMPLICACIONES

SORPRESAS ENORMES

Por cada F5 que haces, el navegador te cobra. :D

En otros términos: mantener presionada esa tecla por 5 segundos te cuesta *3 recargas por segundo * 5 segundos * US$ 5 = US$ 75*.

IMPLICACIONES

INSEGURIDAD

¿Y por qué no?

SOLUCIONES

Validación de "referer".

SOLUCIONES

CSRF Guard, o pedir y validar un campo oculto por cada transacción.

SOLUCIONES

Usar HTTPS (los sitios sólo HTTP no tienen permiso de cargar HTTPS).

FIN