HEADERS SEGUROS HTTP

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

Daniel Torres Sandi

- Ingeniero de sistemas (USFX)
- Comptia security+
- Instructor cognos
- Entusiasta del software libre y de la seguridad informatica

OWASP
The Open Web Application Security Project

HTTP HEADERS

- Una manera de definir como **interactuan** cliente y servidor

TIPOS

- Headers de peticion (cliente):
  - Ej: Navegador (User-Agent)
- Headers de respuesta (servidor):
  - Ej: Codigo de respuesta (Response code)
- Headers generales (ambos):
  - Ej: Conexion (Connection)

OWASP
The Open Web Application Security Project

HTTP HEADERS SEGUROS

Headers de respuesta (servidor):

- X-FRAME-OPTIONS
- X-XSS-PROTECTION
- CONTENT-SECURITY-POLICY
- STRICT-TRANSPORT-SECURITY
- X-CONTENT-TYPE-OPTIONS

OWASP
The Open Web Application Security Project

AMENAZAS

1. Clickjacking
   - Engaña al usuario para que haga click en un boton oculto
2. Session hijacking
   - Secuestro de la sesion
3. XSS
   - Ejecucion de codigo malicioso en el navegador (Ej: javascript)

OWASP
The Open Web Application Security Project

Clickjacking DEMO

OWASP
The Open Web Application Security Project

X-FRAME-OPTIONS

- El servidor le indica al cliente que la pagina **no puede ser cargado** en un iframe
- Header usado para proteger sitios de ataques de c**lick jacking**

Opciones:

Define desde que dominios se puede cargar en un iframe

- Same Origin: Desde el mismo dominio
- Deny: De ningun dominio
- Allow from: De determinado dominio


3.7+

8+

4.1+

4+

OWASP
The Open Web Application Security Project

Session hijacking DEMO

OWASP
The Open Web Application Security Project

STRICT-TRANSPORT-SECURITY (HSTS)

- HSTS obliga a el navegador a "hablar" con el servidor solo mediante HTTPS
- Mitiga ataques de hombre en el medio (Man-in-the-middle)


OWASP
The Open Web Application Security Project

XSS DEMO

X-XSS-PROTECTION

- Los navegadores tienen un framework de proteccion XSS interno
- Este header habilita esta proteccion

Ejemplos:

- X-XSS-PROTECTION: 1
- X-XSS-PROTECTION: 1; report = http://xyz.com/add.php


OWASP
The Open Web Application Security Project

CONTENT-SECURITY-POLICY

Directivas:

- script-src: Definir desde donde **scripts** se pueden ejecutar
- img-src: Definir desde donde se puede cargar **imágenes**
- media-src: Definir desde donde se puede cargar **video/audio**
- frame-src: Definir desde donde se puede incrustar **frames**


23+


25+

7+

OWASP
The Open Web Application Security Project

CONTENT-SECURITY-POLICY

Directivas:

- object-src: Flash y otros objetos
- default-src: Definir la política de carga para todo tipo de recursos
- report-uri: Especifica la URL a la que se envíara el informes sobre violación de la política


OWASP
The Open Web Application Security Project

CONTENT-SECURITY-POLICY

Despues de implementar CSP los sitios web no podran usar:

Inline scripts

- no mas bloques <script>

- Eventos javascript
  - <a onclick="javascript:"

Modo: Content-Security-Policy-Report-Only

- Notificara de violaciones de la politica pero no las bloqueara

X-CONTENT-TYPE-OPTIONS

- Cuando permitimos que usuarios **suban contenido** para que otros usuarios los **descarguen**
- MIME sniffing: Inspeccionar el contenido para determinar el formato (text,video,etc)
- Imagenes PNG pueden ser interpretadas como HTML

X-CONTENT-TYPE-OPTIONS:nosniff


OWASP
The Open Web Application Security Project

¿Que header seguros usa mi sitio web?

http://cyh.herokuapp.com/cyh

OWASP
The Open Web Application Security Project

IMPLEMENTADO HEADERS SEGUROS

A nivel de servidor

- IISv7 : Administrador de IIS
  - ASP.NET 4.5 (shim.codeplex.com)
- Apache: Modulo mod_headers
- Nginx: Modulos ngx_http_headers_module

OWASP
The Open Web Application Security Project

IMPLEMENTADO HEADERS SEGUROS

A nivel de codigo

- JSP
  - response.addHeader("X-XSS-Protection","1")
- PHP
  - header("X-Frame-Options: DENY");

OWASP
The Open Web Application Security Project

GRACIAS!