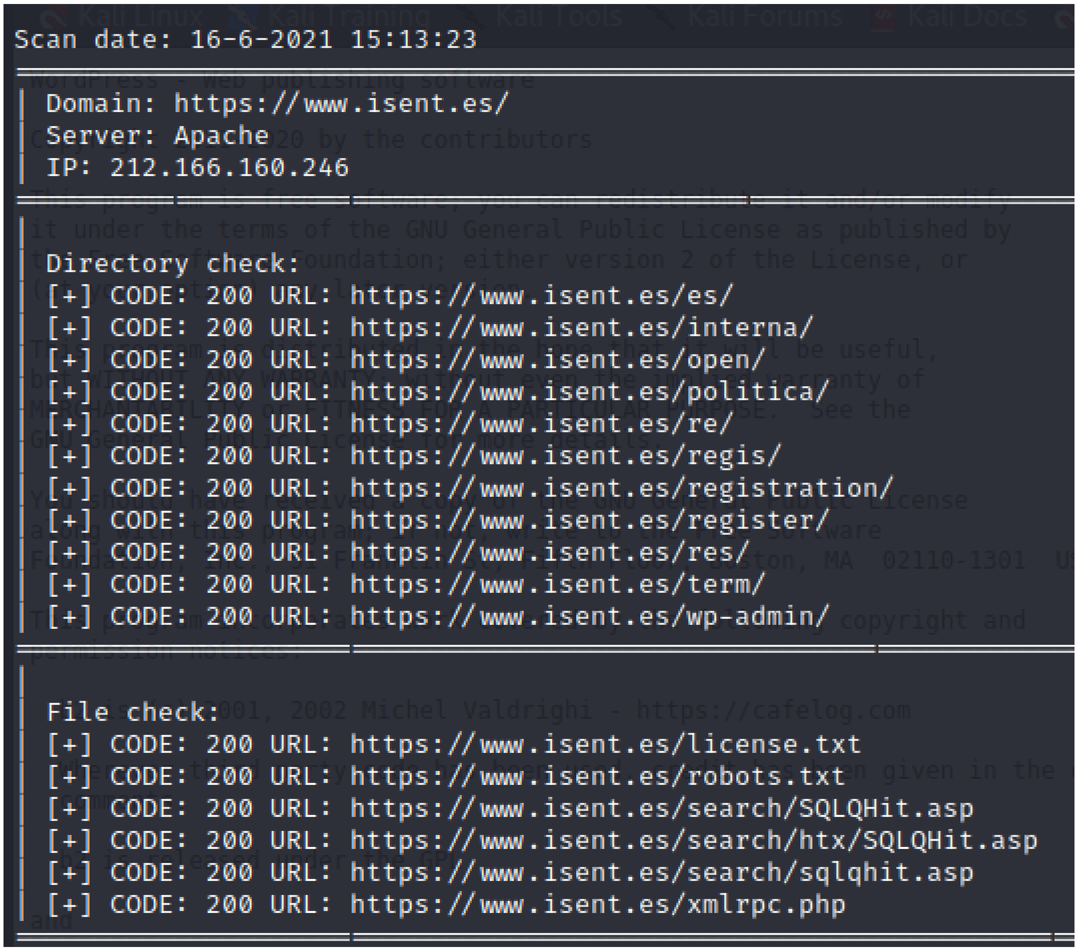
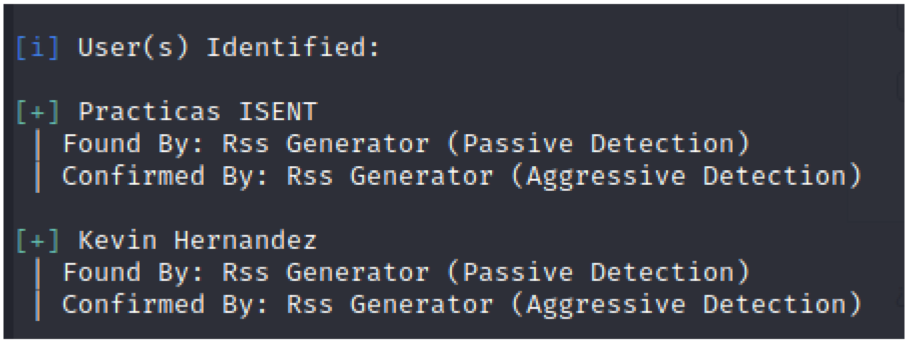
Durante los escaneos a la web ***isent.es*** que he realizado utilizando diversas herramientas (uniscan, wpscan, owasp) no he encontrado ninguna vulnerabilidad grave, pero sí algunas leves que sería adecuado solventar para garantizar la seguridad de los datos de la web y de los usuarios que accedan a ella.

He detectado que los siguientes directorios son públicos, siendo de especial relevancia el de *wp-admin/* , ya que al tener tan fácil acceso a este directorio se puede hacer un intento forzado de login. También son visibles los archivos *license.txt* y *robots.txt .*



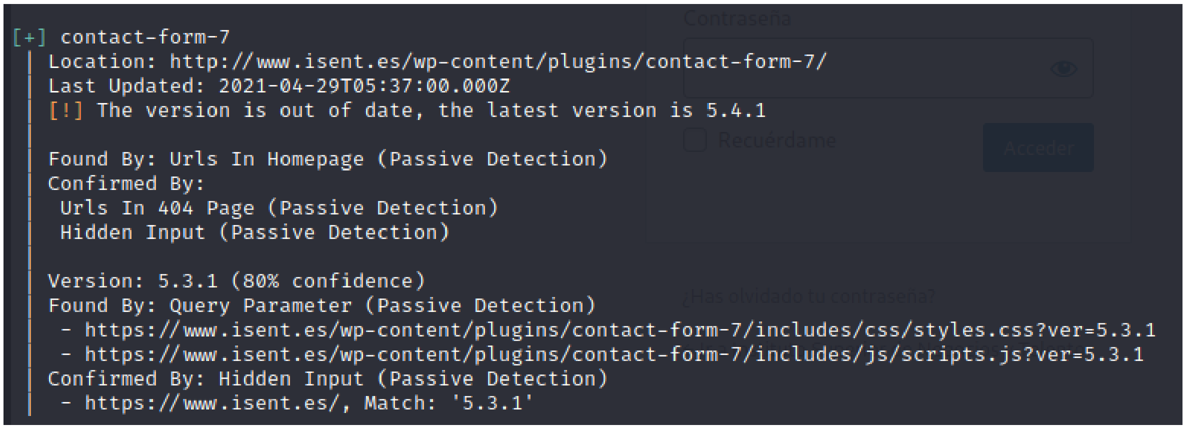
```
Scan date: 16-6-2021 15:13:23
═══════════════════════════════════════════════════════════════
| Domain: https://www.isent.es/
| Server: Apache
| IP: 212.166.160.246
═══════════════════════════════════════════════════════════════
|
| Directory check:
| [+] CODE: 200 URL: https://www.isent.es/es/
| [+] CODE: 200 URL: https://www.isent.es/interna/
| [+] CODE: 200 URL: https://www.isent.es/open/
| [+] CODE: 200 URL: https://www.isent.es/politica/
| [+] CODE: 200 URL: https://www.isent.es/re/
| [+] CODE: 200 URL: https://www.isent.es/regis/
| [+] CODE: 200 URL: https://www.isent.es/registration/
| [+] CODE: 200 URL: https://www.isent.es/register/
| [+] CODE: 200 URL: https://www.isent.es/res/
| [+] CODE: 200 URL: https://www.isent.es/term/
| [+] CODE: 200 URL: https://www.isent.es/wp-admin/
═══════════════════════════════════════════════════════════════
|
| File check:
| [+] CODE: 200 URL: https://www.isent.es/license.txt
| [+] CODE: 200 URL: https://www.isent.es/robots.txt
| [+] CODE: 200 URL: https://www.isent.es/search/SQLQHit.asp
| [+] CODE: 200 URL: https://www.isent.es/search/htx/SQLQHit.asp
| [+] CODE: 200 URL: https://www.isent.es/search/sqlqhit.asp
| [+] CODE: 200 URL: https://www.isent.es/xmlrpc.php
═══════════════════════════════════════════════════════════════
```

He detectado también el listado de usuarios de la web, facilitando así todavía más el acceso forzado.

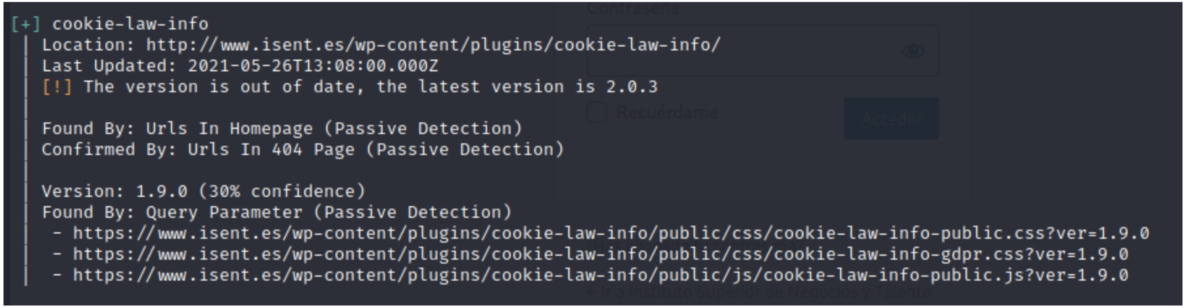


```
[i] User(s) Identified:

[+] Practicas ISENT
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[+] Kevin Hernandez
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)
```

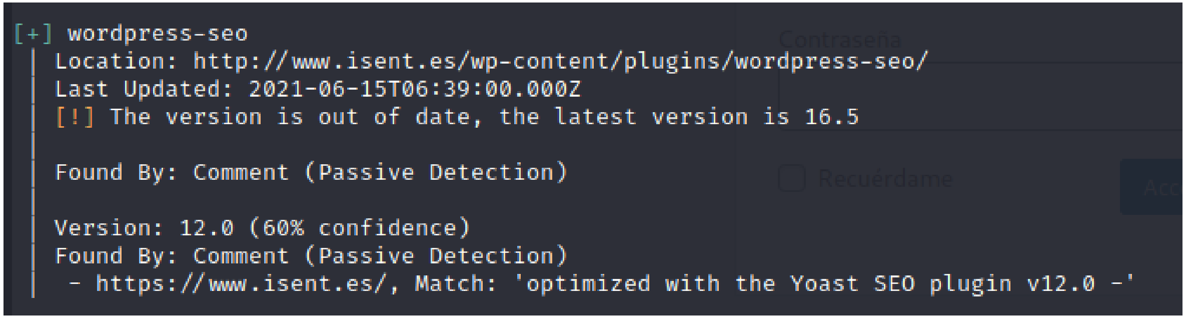
También he identificado algunos plugins que necesitan actualizarse:
- contact-form-7
- cookie-law-info
- elementor
-woocomerce-products-filter
-wordpress-seo



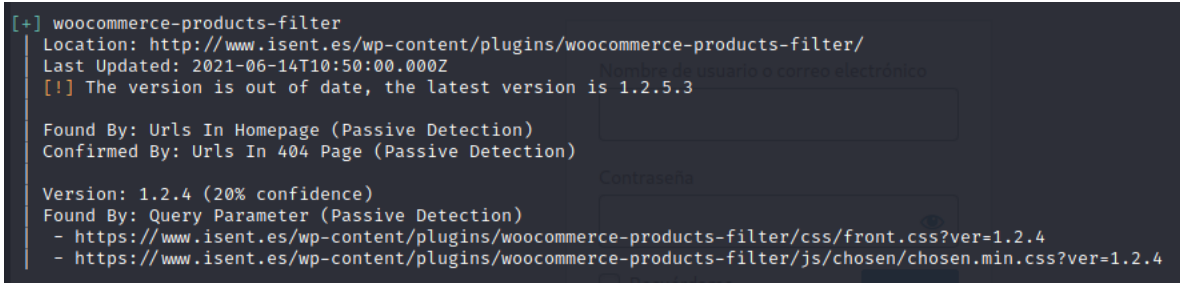
```
[+] contact-form-7
 | Location: http://www.isent.es/wp-content/plugins/contact-form-7/
 | Last Updated: 2021-04-29T05:37:00.000Z
 | [!] The version is out of date, the latest version is 5.4.1
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By:
 |  Urls In 404 Page (Passive Detection)
 |  Hidden Input (Passive Detection)
 |
 | Version: 5.3.1 (80% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://www.isent.es/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.3.1
 |  - https://www.isent.es/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.3.1
 | Confirmed By: Hidden Input (Passive Detection)
 |  - https://www.isent.es/, Match: '5.3.1'
```



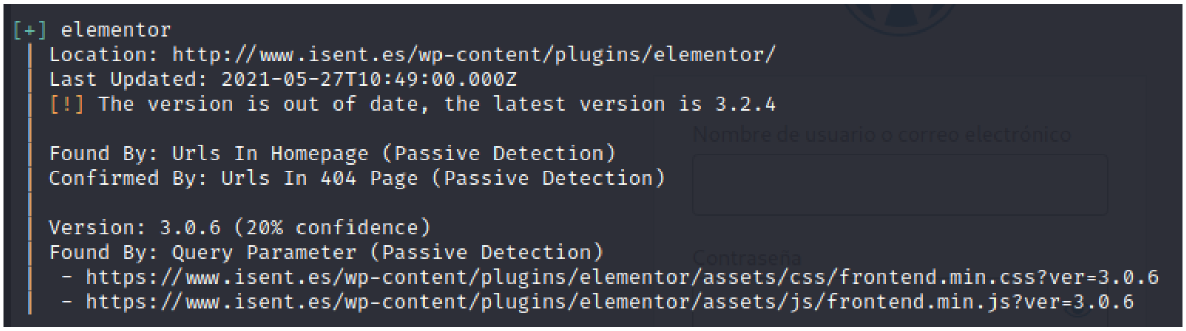
```
[+] cookie-law-info
 | Location: http://www.isent.es/wp-content/plugins/cookie-law-info/
 | Last Updated: 2021-05-26T13:08:00.000Z
 | [!] The version is out of date, the latest version is 2.0.3
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.9.0 (30% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://www.isent.es/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-public.css?ver=1.9.0
 |  - https://www.isent.es/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-gdpr.css?ver=1.9.0
 |  - https://www.isent.es/wp-content/plugins/cookie-law-info/public/js/cookie-law-info-public.js?ver=1.9.0
```



```
[+] wordpress-seo
 | Location: http://www.isent.es/wp-content/plugins/wordpress-seo/
 | Last Updated: 2021-06-15T06:39:00.000Z
 | [!] The version is out of date, the latest version is 16.5
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 12.0 (60% confidence)
 | Found By: Comment (Passive Detection)
 |  - https://www.isent.es/, Match: 'optimized with the Yoast SEO plugin v12.0 -'
```

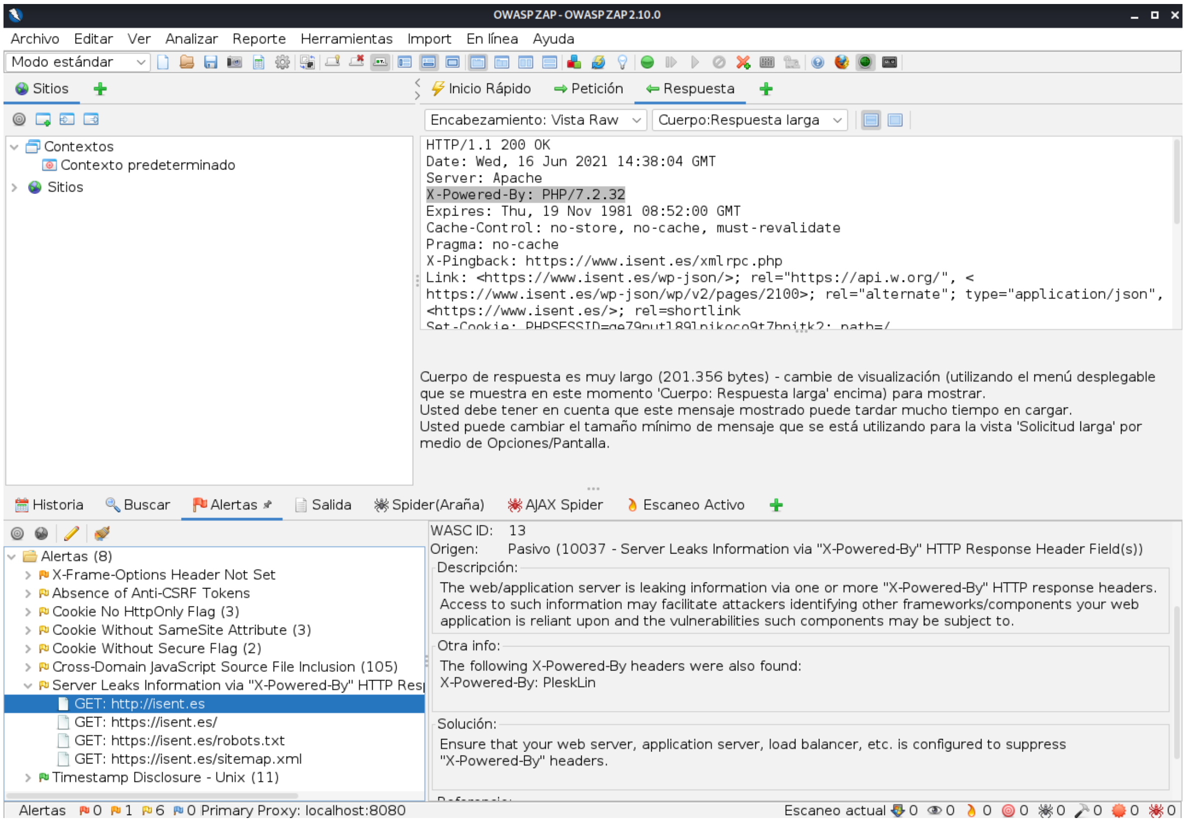


```
[+] woocommerce-products-filter
 | Location: http://www.isent.es/wp-content/plugins/woocommerce-products-filter/
 | Last Updated: 2021-06-14T10:50:00.000Z
 | [!] The version is out of date, the latest version is 1.2.5.3
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.2.4 (20% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://www.isent.es/wp-content/plugins/woocommerce-products-filter/css/front.css?ver=1.2.4
 |  - https://www.isent.es/wp-content/plugins/woocommerce-products-filter/js/chosen/chosen.min.css?ver=1.2.4
```



```
[+] elementor
 | Location: http://www.isent.es/wp-content/plugins/elementor/
 | Last Updated: 2021-05-27T10:49:00.000Z
 | [!] The version is out of date, the latest version is 3.2.4
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 3.0.6 (20% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://www.isent.es/wp-content/plugins/elementor/assets/css/frontend.min.css?ver=3.0.6
 |  - https://www.isent.es/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.0.6
```

He detectado que la versión utilizada de PHP es visible. Conocer esta información facilita el uso de frameworks específicos para atacar la web.



```
HTTP/1.1 200 OK
Date: Wed, 16 Jun 2021 14:38:04 GMT
Server: Apache
X-Powered-By: PHP/7.2.32
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Pingback: https://www.isent.es/xmlrpc.php
Link: <https://www.isent.es/wp-json/>; rel="https://api.w.org/", <
https://www.isent.es/wp-json/wp/v2/pages/2100>; rel="alternate"; type="application/json",
<https://www.isent.es/>; rel=shortlink
Set-Cookie: PHPSESSID=ge79nut1891nikoco9t7bnitk2; path=/
```

Cuerpo de respuesta es muy largo (201.356 bytes) - cambie de visualización (utilizando el menú desplegable que se muestra en este momento 'Cuerpo: Respuesta larga' encima) para mostrar.
Usted debe tener en cuenta que este mensaje mostrado puede tardar mucho tiempo en cargar.
Usted puede cambiar el tamaño mínimo de mensaje que se está utilizando para la vista 'Solicitud larga' por medio de Opciones/Pantalla.

Alertas (8)
- X-Frame-Options Header Not Set
- Absence of Anti-CSRF Tokens
- Cookie No HttpOnly Flag (3)
- Cookie Without SameSite Attribute (3)
- Cookie Without Secure Flag (2)
- Cross-Domain JavaScript Source File Inclusion (105)
- Server Leaks Information via "X-Powered-By" HTTP Res
  - GET: http://isent.es
  - GET: https://isent.es/
  - GET: https://isent.es/robots.txt
  - GET: https://isent.es/sitemap.xml
- Timestamp Disclosure - Unix (11)

WASC ID: 13
Origen: Pasivo (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

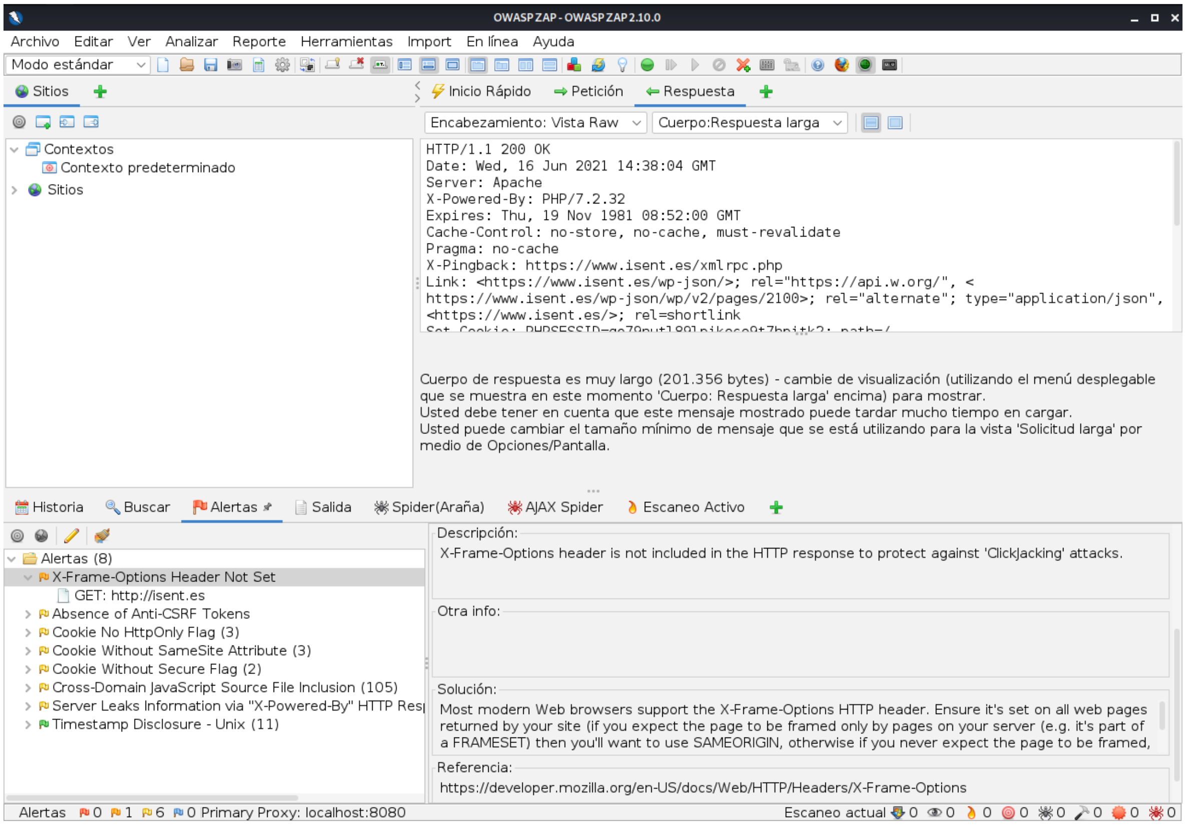
Descripción:
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Otra info:
The following X-Powered-By headers were also found:
X-Powered-By: PleskLin

Solución:
Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

Alertas 0 1 6 0 Primary Proxy: localhost:8080 Escaneo actual 0 0 0 0 0 0 0 0

También he notado la ausencia del header X-Frame-Options en el código, que evitarían posibles ataques de clickjacking dirigidos al usuario.


OWASP ZAP - OWASP ZAP 2.10.0
Archivo Editar Ver Analizar Reporte Herramientas Import En línea Ayuda
Modo estándar
Sitios
Inicio Rápido
Petición
Respuesta
Encabezamiento: Vista Raw
Cuerpo:Respuesta larga
Historia Buscar Alertas Salida Spider(Araña) AJAX Spider Escaneo Activo

Contextos
Contexto predeterminado
Sitios

```
HTTP/1.1 200 OK
Date: Wed, 16 Jun 2021 14:38:04 GMT
Server: Apache
X-Powered-By: PHP/7.2.32
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Pingback: https://www.isent.es/xmlrpc.php
Link: <https://www.isent.es/wp-json/>; rel="https://api.w.org/", <
https://www.isent.es/wp-json/wp/v2/pages/2100>; rel="alternate"; type="application/json",
<https://www.isent.es/>; rel=shortlink
```

Cuerpo de respuesta es muy largo (201.356 bytes) - cambie de visualización (utilizando el menú desplegable que se muestra en este momento 'Cuerpo: Respuesta larga' encima) para mostrar.
Usted debe tener en cuenta que este mensaje mostrado puede tardar mucho tiempo en cargar.
Usted puede cambiar el tamaño mínimo de mensaje que se está utilizando para la vista 'Solicitud larga' por medio de Opciones/Pantalla.

Alertas (8)
- X-Frame-Options Header Not Set
  - GET: http://isent.es
- Absence of Anti-CSRF Tokens
- Cookie No HttpOnly Flag (3)
- Cookie Without SameSite Attribute (3)
- Cookie Without Secure Flag (2)
- Cross-Domain JavaScript Source File Inclusion (105)
- Server Leaks Information via "X-Powered-By" HTTP Res
- Timestamp Disclosure - Unix (11)

Descripción:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

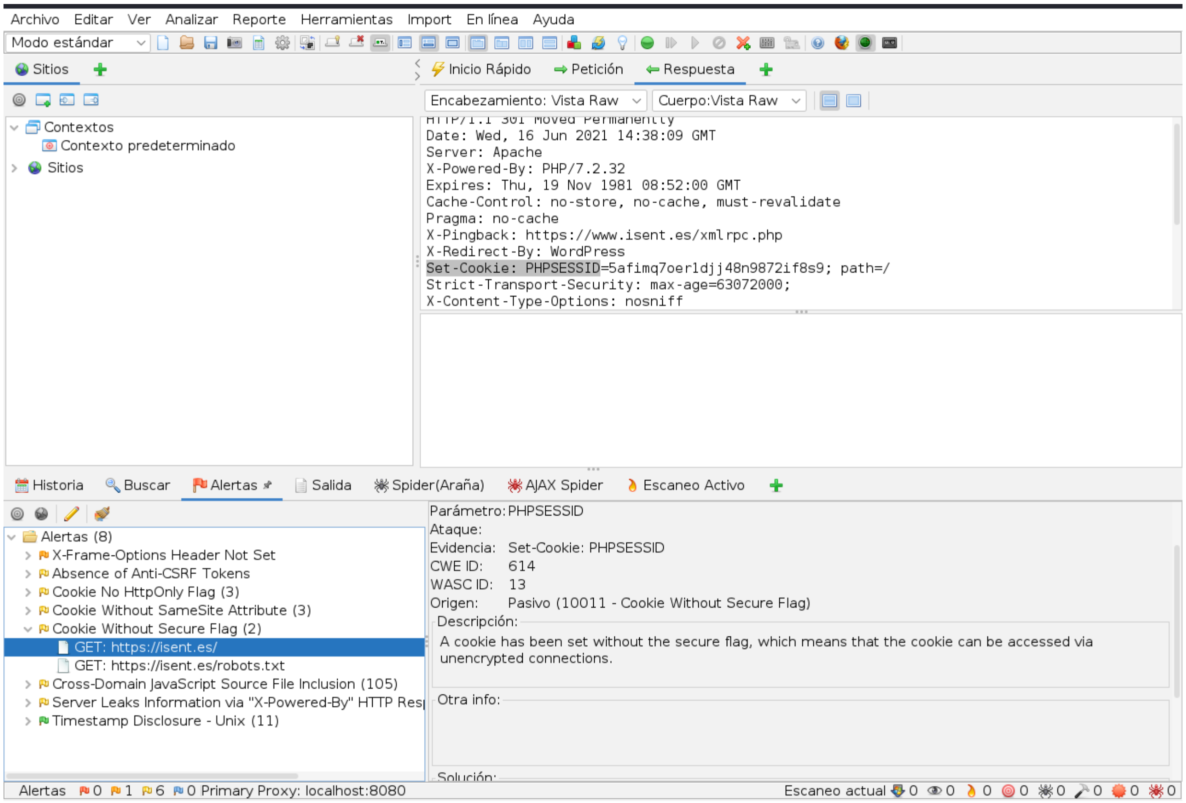
Otra info:

Solución:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed,

Referencia:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Alertas 0 1 6 0 Primary Proxy: localhost:8080 Escaneo actual 0 0 0 0 0 0 0 0

Por último, algunas cookies del sitio web no han sido del todo aseguradas.


Archivo Editar Ver Analizar Reporte Herramientas Import En línea Ayuda
Modo estándar
Sitios
Inicio Rápido
Petición
Respuesta
Encabezamiento: Vista Raw
Cuerpo:Vista Raw
Historia Buscar Alertas Salida Spider(Araña) AJAX Spider Escaneo Activo

Contextos
Contexto predeterminado
Sitios

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 16 Jun 2021 14:38:09 GMT
Server: Apache
X-Powered-By: PHP/7.2.32
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Pingback: https://www.isent.es/xmlrpc.php
X-Redirect-By: WordPress
Set-Cookie: PHPSESSID=5afimq7oer1djj48n9872if8s9; path=/
Strict-Transport-Security: max-age=63072000;
X-Content-Type-Options: nosniff
```

Alertas (8)
- X-Frame-Options Header Not Set
- Absence of Anti-CSRF Tokens
- Cookie No HttpOnly Flag (3)
- Cookie Without SameSite Attribute (3)
- Cookie Without Secure Flag (2)
  - GET: https://isent.es/
  - GET: https://isent.es/robots.txt
- Cross-Domain JavaScript Source File Inclusion (105)
- Server Leaks Information via "X-Powered-By" HTTP Res
- Timestamp Disclosure - Unix (11)

Parámetro: PHPSESSID
Ataque:
Evidencia: Set-Cookie: PHPSESSID
CWE ID: 614
WASC ID: 13
Origen: Pasivo (10011 - Cookie Without Secure Flag)

Descripción:
A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Otra info:

Solución:

Alertas 0 1 6 0 Primary Proxy: localhost:8080 Escaneo actual 0 0 0 0 0 0 0 0