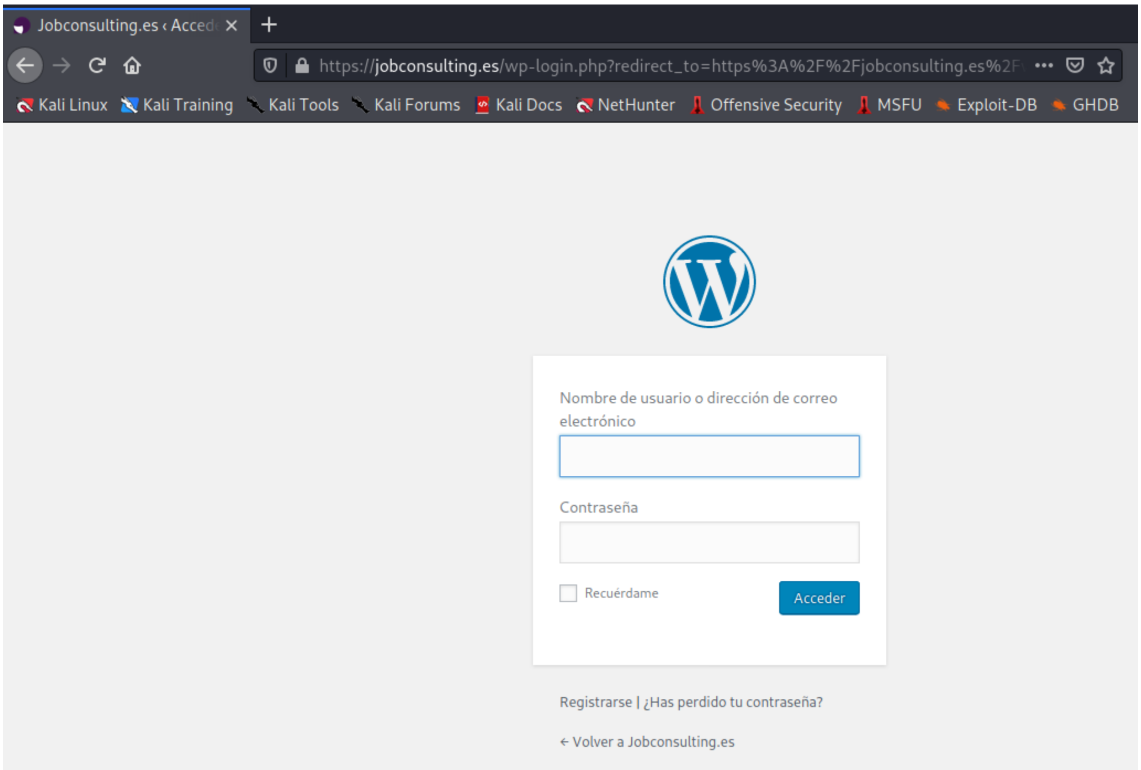
Auditoría

jobconsulting.es

La página de inicio de sesión de Wordpress es visible y fácilmente accesible desde jobconsulting.es/wp-login



Nombre de usuario o dirección de correo electrónico

Contraseña

□ Recuérdame

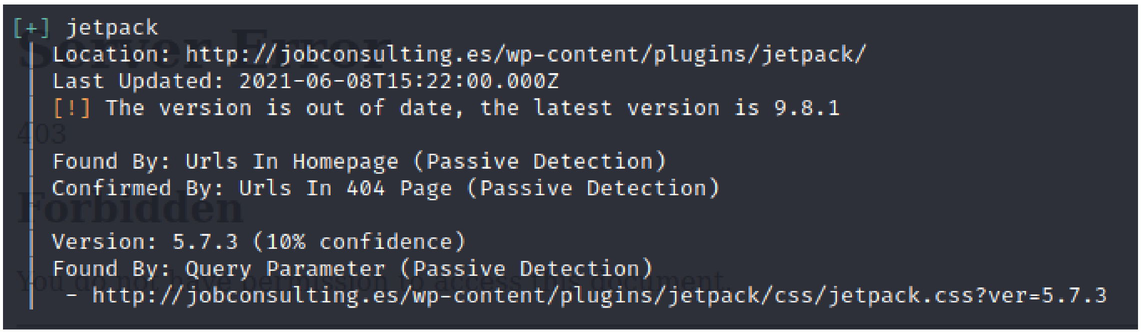
Acceder

Registrarse | ¿Has perdido tu contraseña?

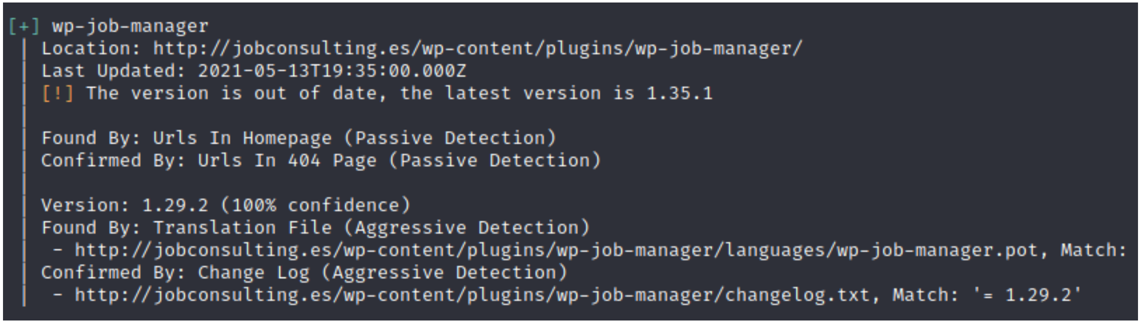
← Volver a Jobconsulting.es

Los siguientes plugins están desactualizados:

-jetpack
-wp-job-manager

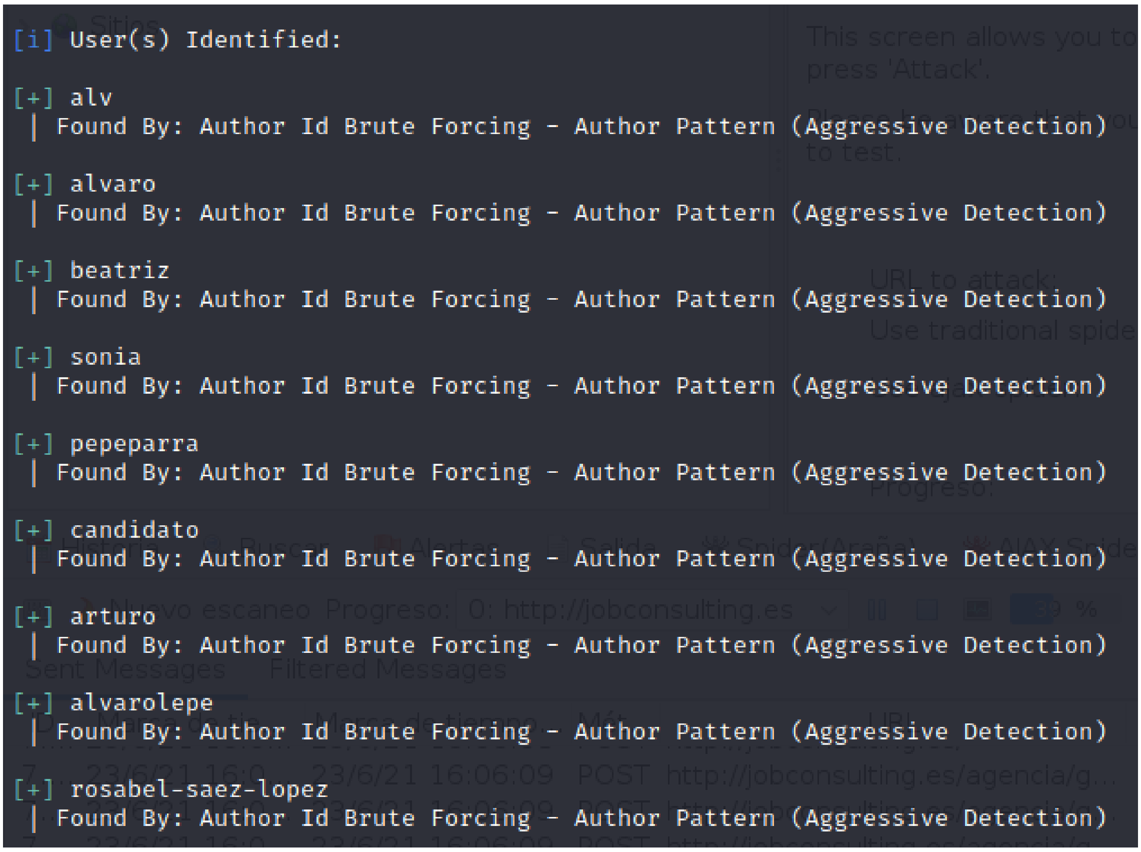


```
[+] jetpack
 | Location: http://jobconsulting.es/wp-content/plugins/jetpack/
 | Last Updated: 2021-06-08T15:22:00.000Z
 | [!] The version is out of date, the latest version is 9.8.1
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 5.7.3 (10% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - http://jobconsulting.es/wp-content/plugins/jetpack/css/jetpack.css?ver=5.7.3
```



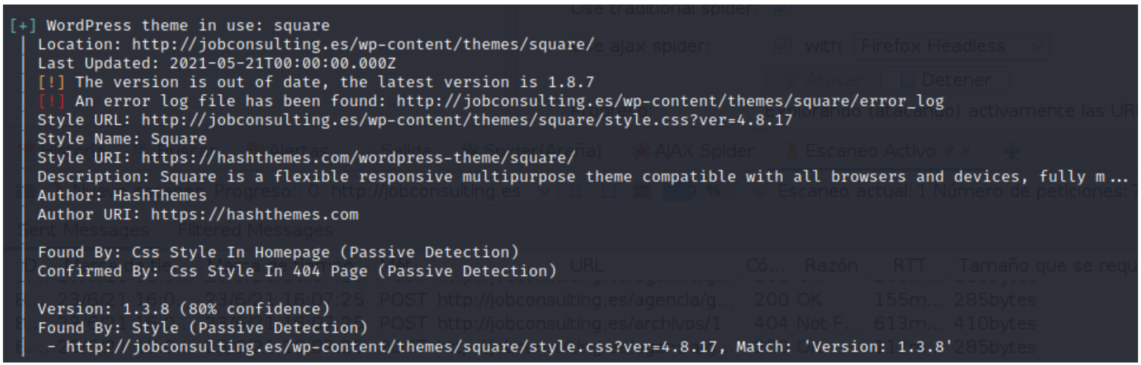
```
[+] wp-job-manager
 | Location: http://jobconsulting.es/wp-content/plugins/wp-job-manager/
 | Last Updated: 2021-05-13T19:35:00.000Z
 | [!] The version is out of date, the latest version is 1.35.1
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.29.2 (100% confidence)
 | Found By: Translation File (Aggressive Detection)
 |  - http://jobconsulting.es/wp-content/plugins/wp-job-manager/languages/wp-job-manager.pot, Match:
 | Confirmed By: Change Log (Aggressive Detection)
 |  - http://jobconsulting.es/wp-content/plugins/wp-job-manager/changelog.txt, Match: '= 1.29.2'
```

Se han identificado los siguientes usuarios de Wordpress:

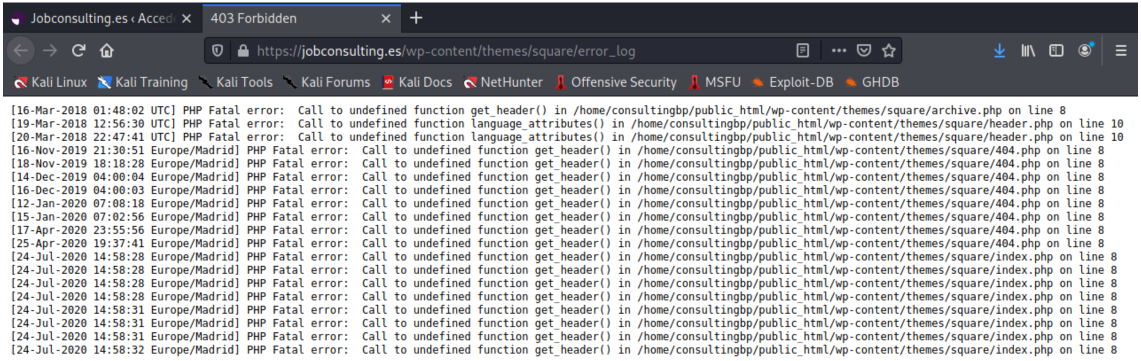


```
[i] User(s) Identified:

[+] alv
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] alvaro
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] beatriz
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] sonia
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] pepeparra
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] candidato
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] arturo
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] alvarolepe
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] rosabel-saez-lopez
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

El tema utilizado (square) está desactualizado y presenta errores.



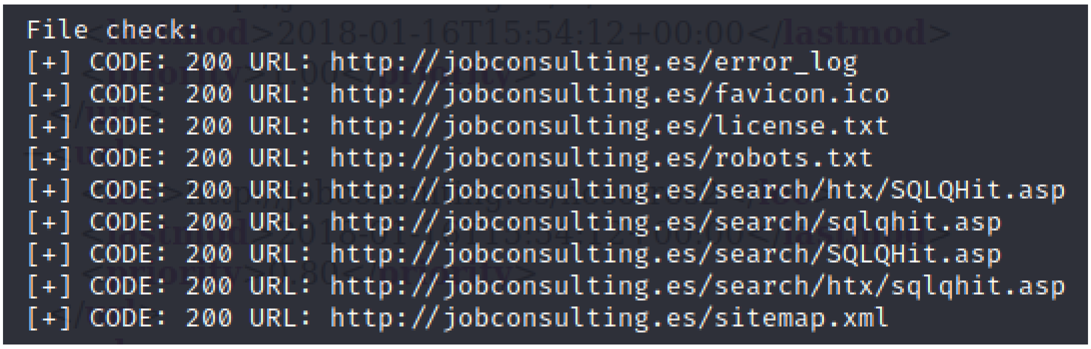
```
[+] WordPress theme in use: square
 | Location: http://jobconsulting.es/wp-content/themes/square/
 | Last Updated: 2021-05-21T00:00:00.000Z
 | [!] The version is out of date, the latest version is 1.8.7
 | [!] An error log file has been found: http://jobconsulting.es/wp-content/themes/square/error_log
 | Style URL: http://jobconsulting.es/wp-content/themes/square/style.css?ver=4.8.17
 | Style Name: Square
 | Style URI: https://hashthemes.com/wordpress-theme/square/
 | Description: Square is a flexible responsive multipurpose theme compatible with all browsers and devices, fully m...
 | Author: HashThemes
 | Author URI: https://hashthemes.com
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://jobconsulting.es/wp-content/themes/square/style.css?ver=4.8.17, Match: 'Version: 1.3.8'
```



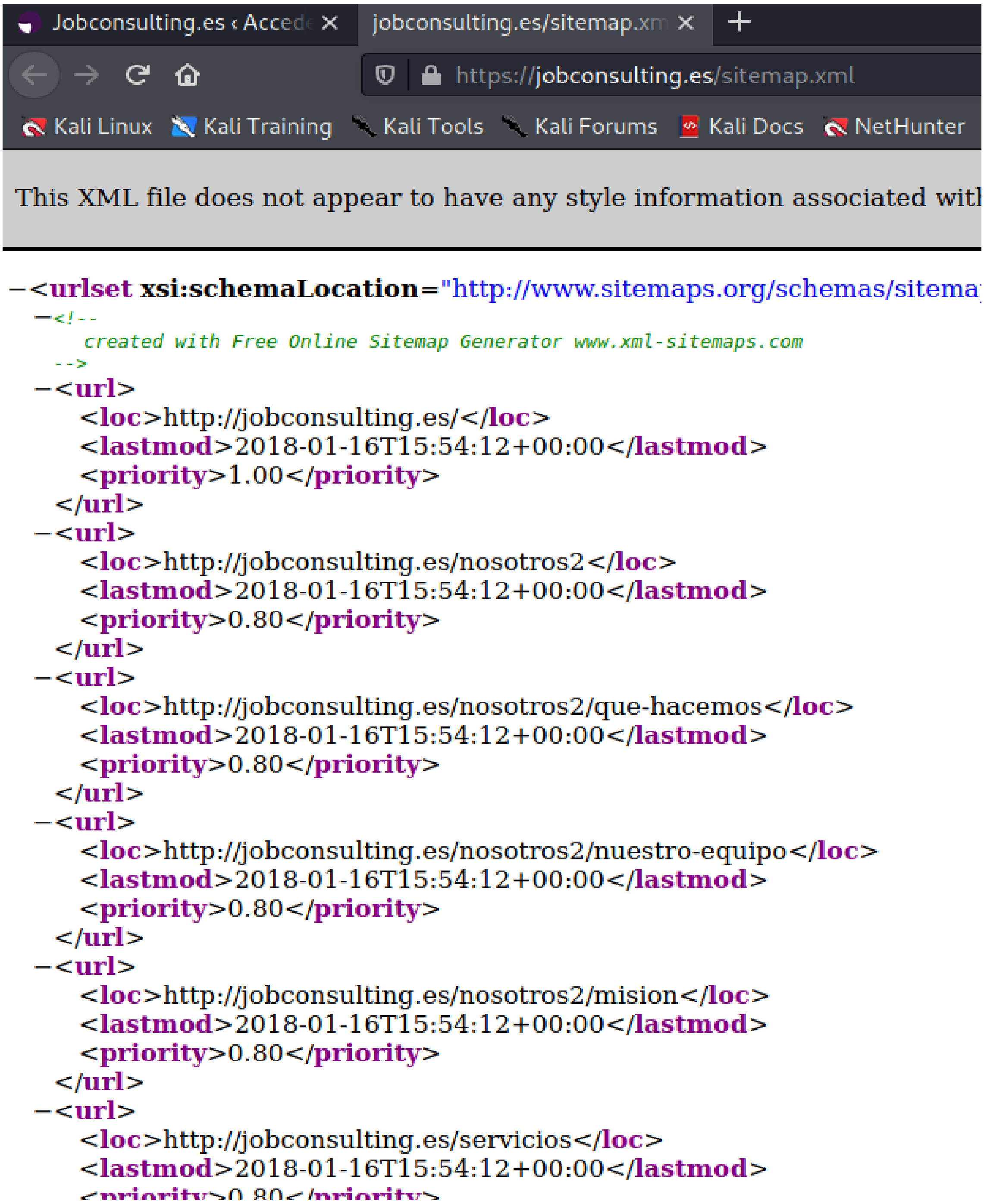
https://jobconsulting.es/wp-content/themes/square/error_log

```
[16-Mar-2018 01:48:02 UTC] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/archive.php on line 8
[19-Mar-2018 12:56:30 UTC] PHP Fatal error:  Call to undefined function language_attributes() in /home/consultingbp/public_html/wp-content/themes/square/header.php on line 10
[20-Mar-2018 22:47:41 UTC] PHP Fatal error:  Call to undefined function language_attributes() in /home/consultingbp/public_html/wp-content/themes/square/header.php on line 10
[16-Nov-2019 21:30:51 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[18-Nov-2019 18:18:28 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[14-Dec-2019 04:00:04 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[16-Dec-2019 04:00:03 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[12-Jan-2020 07:08:18 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[15-Jan-2020 07:02:56 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[17-Apr-2020 23:55:56 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[25-Apr-2020 19:37:41 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/404.php on line 8
[24-Jul-2020 14:58:28 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:28 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:28 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:28 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:31 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:31 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:31 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
[24-Jul-2020 14:58:32 Europe/Madrid] PHP Fatal error:  Call to undefined function get_header() in /home/consultingbp/public_html/wp-content/themes/square/index.php on line 8
```

El documento XML es visible, entre otros archivos



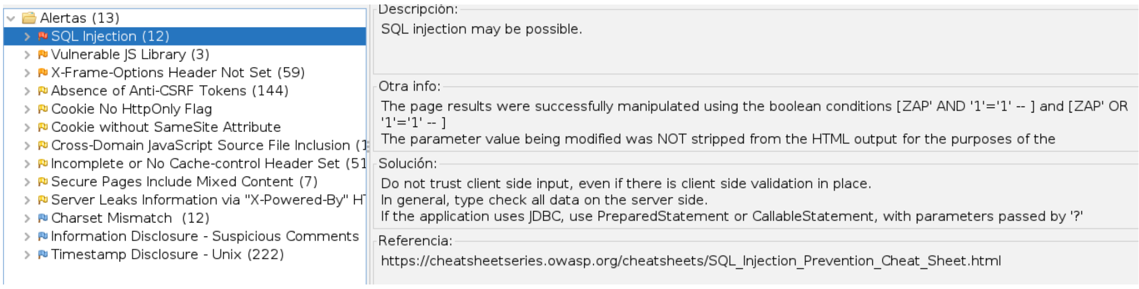
```
File check:
[+] CODE: 200 URL: http://jobconsulting.es/error_log
[+] CODE: 200 URL: http://jobconsulting.es/favicon.ico
[+] CODE: 200 URL: http://jobconsulting.es/license.txt
[+] CODE: 200 URL: http://jobconsulting.es/robots.txt
[+] CODE: 200 URL: http://jobconsulting.es/search/htx/SQLQHit.asp
[+] CODE: 200 URL: http://jobconsulting.es/search/sqlqhit.asp
[+] CODE: 200 URL: http://jobconsulting.es/search/SQLQHit.asp
[+] CODE: 200 URL: http://jobconsulting.es/search/htx/sqlqhit.asp
[+] CODE: 200 URL: http://jobconsulting.es/sitemap.xml
```


Jobconsulting.es ‹ Accede
jobconsulting.es/sitemap.xm
https://jobconsulting.es/sitemap.xml
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter

This XML file does not appear to have any style information associated wit

```
–<urlset xsi:schemaLocation="http://www.sitemaps.org/schemas/sitema
  –<!--
      created with Free Online Sitemap Generator www.xml-sitemaps.com
   -->
  –<url>
      <loc>http://jobconsulting.es/</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>1.00</priority>
   </url>
  –<url>
      <loc>http://jobconsulting.es/nosotros2</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>0.80</priority>
   </url>
  –<url>
      <loc>http://jobconsulting.es/nosotros2/que-hacemos</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>0.80</priority>
   </url>
  –<url>
      <loc>http://jobconsulting.es/nosotros2/nuestro-equipo</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>0.80</priority>
   </url>
  –<url>
      <loc>http://jobconsulting.es/nosotros2/mision</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>0.80</priority>
   </url>
  –<url>
      <loc>http://jobconsulting.es/servicios</loc>
      <lastmod>2018-01-16T15:54:12+00:00</lastmod>
      <priority>0.80</priority>
```

Existe el riesgo de que la página sufra ataques de inyección de SQL.



- Alertas (13)
  - SQL Injection (12)
  - Vulnerable JS Library (3)
  - X-Frame-Options Header Not Set (59)
  - Absence of Anti-CSRF Tokens (144)
  - Cookie No HttpOnly Flag
  - Cookie without SameSite Attribute
  - Cross-Domain JavaScript Source File Inclusion (1
  - Incomplete or No Cache-control Header Set (51
  - Secure Pages Include Mixed Content (7)
  - Server Leaks Information via "X-Powered-By" H
  - Charset Mismatch (12)
  - Information Disclosure - Suspicious Comments
  - Timestamp Disclosure - Unix (222)

Descripción:
SQL injection may be possible.

Otra info:
The page results were successfully manipulated using the boolean conditions [ZAP' AND '1'='1' --] and [ZAP' OR '1'='1' --]
The parameter value being modified was NOT stripped from the HTML output for the purposes of the

Solución:
Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

Referencia:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

La versión de Jquery (1.12.4) está desactualizada y es vulnerable.

No se ha configurado el header X-Frame-Options.

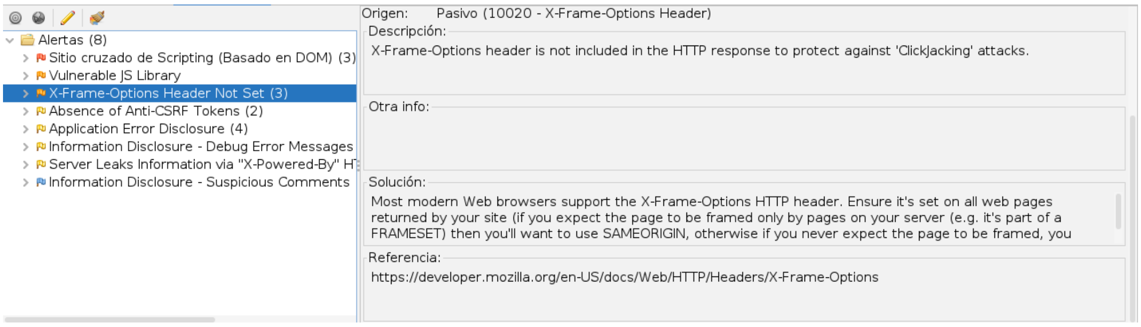
La web no está protegida contra ataques DDOS

contrato.jobconsulting.es

La web es vulnerable a ataques XSS basados en DOM.

La versión de Jquery (1.8.2) está desactualizada y es vulnerable.

El header X-Frame-Options no está configurado



- Alertas (8)
  - Sitio cruzado de Scripting (Basado en DOM) (3)
  - Vulnerable JS Library
  - X-Frame-Options Header Not Set (3)
  - Absence of Anti-CSRF Tokens (2)
  - Application Error Disclosure (4)
  - Information Disclosure - Debug Error Messages
  - Server Leaks Information via "X-Powered-By" H
  - Information Disclosure - Suspicious Comments

Origen: Pasivo (10020 - X-Frame-Options Header)

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, you

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