

Auditoría

campusyformacion.es

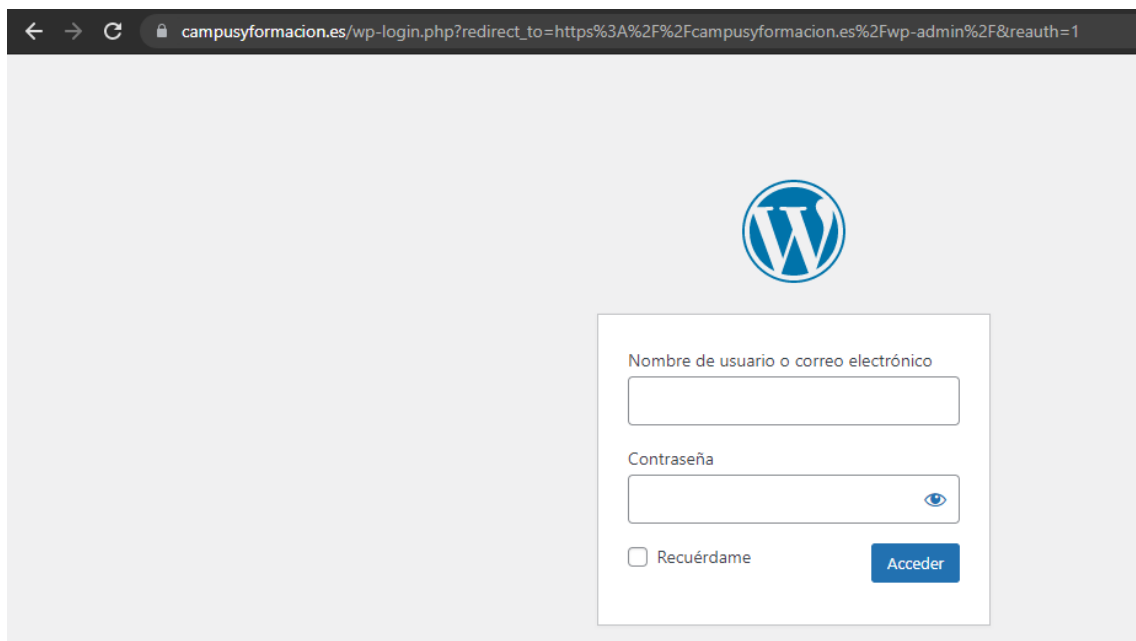
El plugin *wordpress-seo* está desactualizado.

```
[+] wordpress-seo
  Location: http://campusyformacion.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 The version is out of date, the latest version is 16.5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: 16.3 (60% confidence)
  Found By: Comment (Passive Detection)
  - https://campusyformacion.es/, Match: 'optimized with the Yoast SEO plugin v16.3 -'
```

La página de acceso a Wordpress es fácilmente accesible desde /wp-admin



The screenshot shows a web browser window with the address bar displaying the URL: `campusyformacion.es/wp-login.php?redirect_to=https%3A%2F%2Fcampusyformacion.es%2Fwp-admin%2F&reauth=1`. The page content features the WordPress logo at the top center. Below the logo is a white login box containing the following elements: a text input field labeled "Nombre de usuario o correo electrónico", a text input field labeled "Contraseña" with an eye icon for toggling visibility, a checkbox labeled "Recuérdame", and a blue button labeled "Acceder".

Se han identificado los siguientes usuarios de Wordpress:

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

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

[+] admin
| Found By: Wp Json Api (Aggressive Detection)
| - https://campusyformacion.es/wp-json/wp/v2/users/?per_page=100&page=1

[+] becarios_mkd
| Found By: Wp Json Api (Aggressive Detection)
| - https://campusyformacion.es/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] irene-barroso
| Found By: Wp Json Api (Aggressive Detection)
| - https://campusyformacion.es/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] soporte_n66x1595
| Found By: Wp Json Api (Aggressive Detection)
| - https://campusyformacion.es/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

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

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

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

No se ha configurado el header X-Frame-Options y las cookies no han sido aseguradas.

<div><div>Alertas (11)</div><div><div>X-Frame-Options Header Not Set (4)</div><div>Absence of Anti-CSRF Tokens (4)</div><div>Cookie No HttpOnly Flag</div><div>Cookie Without Secure Flag</div><div>Cookie without SameSite Attribute</div><div>Cross-Domain JavaScript Source File Inclusion (4)</div><div>Incomplete or No Cache-control Header Set (3)</div><div>Server Leaks Information via "X-Powered-By" H</div><div>X-Content-Type-Options Header Missing (5)</div><div>Information Disclosure - Suspicious Comments</div><div>Timestamp Disclosure - Unix (4)</div></div></div>	<div>Descripción:</div> <div>A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.</div> <div>Otra info:</div> <div>Solución:</div> <div>Ensure that the HttpOnly flag is set for all cookies.</div> <div>Referencia:</div> <div>https://owasp.org/www-community/HttpOnly</div>
<div><div>Alertas (11)</div><div><div>X-Frame-Options Header Not Set (4)</div><div>Absence of Anti-CSRF Tokens (4)</div><div>Cookie No HttpOnly Flag</div><div>Cookie Without Secure Flag</div><div>Cookie without SameSite Attribute</div><div>Cross-Domain JavaScript Source File Inclusion (4)</div><div>Incomplete or No Cache-control Header Set (3)</div><div>Server Leaks Information via "X-Powered-By" H</div><div>X-Content-Type-Options Header Missing (5)</div><div>Information Disclosure - Suspicious Comments</div><div>Timestamp Disclosure - Unix (4)</div></div></div>	<div>Descripción:</div> <div>A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.</div> <div>Otra info:</div> <div>Solución:</div> <div>Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.</div> <div>Referencia:</div> <div>https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html</div>