Auditoría

starjobs.campusyformacion.com

El header X-Frame-Options no está configurado.

La versión de Jquery (1.2.3) está desactualizada y es vulnerable.

gadebs.campusyformacion.com

El header X-Frame-Options no está configurado.

La versión de Jquery (1.2.3) está desactualizada y es vulnerable.

masoneria.campusyformacion.com

El header X-Frame-Options no está configurado.

La versión de la librería de Bootstrap (3.3.6) está desactualizada y es vulnerable.

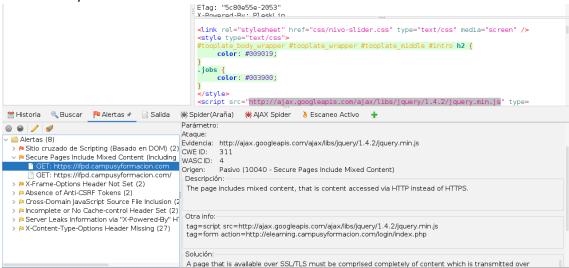
ifpd.campusyformacion.com

La web es vulnerable a ataques XSS basados en DOM.



El header X-Frame-Options no está configurado.

La web incluye contenido mixto HTTP.



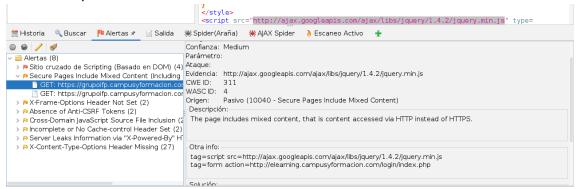
grupoifp.campusyformacion.com

La web es vulnerable a ataques XSS basados en DOM.



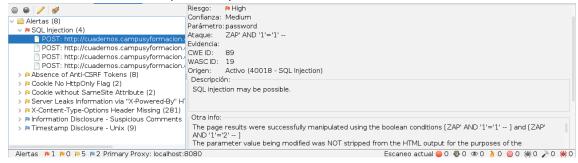
El header X-Frame-Options no está configurado.

La web incluye contenido mixto HTTP.



cuadernos.campusyformacion.com

La web es vulnerable a ataques de inyección de SQL.



beready.campusyformacion.com

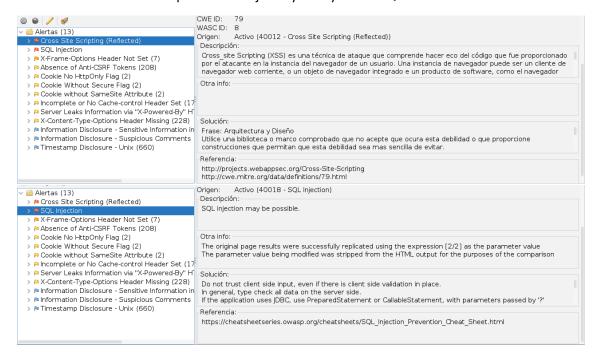
El header X-Frame-Options no está configurado.

aulavirtualtnc.campusyformacion.com

El header X-Frame-Options no está configurado.

cursos.campusyformacion.com

El sitio es vulnerable a ataques XSS reflejados y de inyección SQL.



El header X-Frame-Options no está configurado.

La versión de PHP/5.6.40 es visible.

```
https://cursos.campusyformacion.com/ [200 OK] Content-Language[es], Cookies[MoodleS
2], Moodle, PHP[5.6.40,], PasswordField[password], Plesk[Lin], Script[text/css,text
tent-style-type], X-Frame-Options[sameorigin], X-Powered-By[PHP/5.6.40, PleskLin],
```

tpv.campusyformacion.com

La web no cuenta con certificado SSL, por lo que cualquier dato introducido por el usuario es fácil de interceptar.

El sitio es extremadamente vulnerable a ataques de XSS.

El header X-Frame-Options no está configurado.

La versión de PHP/5.6.40 es visible.

archeformacion.campusyformacion.com

La versión de Jquery 1.11.1 está desactualizada y es vulnerable.



El header X-Frame-Options no está configurado.

elearning.campusyformacion.com

La web es vulnerable a ataques de invección de SQL.

```
Blind SQL Injection:
[+] Vul [Blind SQL-i]: https://elearning.campusyformacion.com/calendar/view.php?course=18time=16146396006view=day+AND+1=1
[+] Keyword: febrero
[+] Vul [Blind SQL-i]: https://elearning.campusyformacion.com/calendar/view.php?course=1&time=1614812400&view=day+AND+1=1
[+] Keyword: febrero
                                                                  Riesgo: 🏴 High
                                                                  Confianza: Medium
Alertas (11)
                                                                 Parámetro: password
Ataque: ZAP AND 1=1 --
 > P Cross Site Scripting (Reflected)
> P SQL Injection (4)
                                                                 Evidencia:
         POST: https://elearning.campusyformacion
POST: https://elearning.campusyformacion
                                                                  CWE ID: 89
WASC ID: 19
         POST: https://elearning.campusyformacion
                                                                  Origen: Activo (40018 - SQL Injection)
Descripción:
      POST: https://elearning.campusyformacion
Absence of Anti-CSRF Tokens (106)
                                                                   SQL injection may be possible.
 > Cookie No HttpOnly Flag (2)
 > Cookie Without Secure Flag (2)
> Cookie without SameSite Attribute (2)
                                                                  Otra info:
 > Polncomplete or No Cache-control Header Set (2
                                                                  The page results were successfully manipulated using the boolean conditions [ZAP AND 1=1-] and [ZAP AND 1=2-] The parameter value being modified was NOT stripped from the HTML output for the purposes of the
 > № Server Leaks Information via "X-Powered-By" |
> № X-Content-Type-Options Header Missing (238)
```

Es vulnerable a ataques de XSS reflejados.

```
v ៉ Alertas (11)
                                                                                                                                                                                                                                                                                          Parámetro: search
                                               GET: https://elearning.campusyformacion.co
                                                                                                                                                                                                                                                                                     Ataque: "onMouseOver="alert(1);
Evidencia: "onMouseOver="alert(1);
               > Absence of Anti-CSRF Tokens (106)
                                                                                                                                                                                                                                                                                       CWE ID:
                                                                                                                                                                                                                                                                                                                                                 79
                      <sup>№</sup> Cookie No HttpOnly Flag (2)

<sup>№</sup> Cookie Without Secure Flag (2)
                                                                                                                                                                                                                                                                                        WASC ID: 8
                                                                                                                                                                                                                                                                                     Origen:
                                                                                                                                                                                                                                                                                                                                                 Activo (40012 - Cross Site Scripting (Reflected))
            > P Cookie without SameSite Attribute (2)
            > Pincomplete or No Cache-control Header Set (2C)
> Pincomplete or No Cache-control Header Set (2C)
> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

> Pincomplete or No Cache-control Header Set (2C)

- Pincom
                                                                                                                                                                                                                                                                                           Cross_site Scripting (XSS) es una técnica de ataque que comprende hacer eco del código que fue proporcionado por el atacante en la instancia del navegador de un usuario. Una instancia de navegador puede ser un cliente de navegador web corriente, o un objeto de navegador integrado e un producto de software, como el navegador
            > № X-Content-Type-Options Header Missing (238)
> № Information Disclosure - Suspicious Comments
> № Timestamp Disclosure - Unix (422)
                                                                                                                                                                                                                                                                                           Otra info:
```