

Auditoría

campus.isent.es

Son visibles los siguientes archivos de texto:

```
[+] CODE: 200 URL: http://campus.isent.es/INSTALL.txt
[+] CODE: 200 URL: http://campus.isent.es/install.txt
[+] CODE: 200 URL: http://campus.isent.es/INSTALL.TXT
[+] CODE: 200 URL: http://campus.isent.es/install.php
[+] CODE: 200 URL: http://campus.isent.es/LICENSE.txt
[+] CODE: 200 URL: http://campus.isent.es/license.txt
[+] CODE: 200 URL: http://campus.isent.es/LICENSE.TXT
[+] CODE: 200 URL: http://campus.isent.es/README.TXT
```

Las versiones de PHP y de JQuery son visibles, siendo esta última una versión desactualizada que presenta vulnerabilidades:

The screenshot shows the Burp Suite interface. The top panel displays the request details for a file named 'jquery-3.2.1.min.js'. The response status is 'HTTP/1.1 200 OK'. The server is identified as 'Apache' with 'X-Powered-By: PHP/7.2.32'. The 'Content-Disposition' header is 'inline; filename="jquery-3.2.1.min.js"'. The 'Expires' header is 'Wed, 15 Sep 2021 13:27:08 GMT'. The 'Pragma' header is 'Cache-Control: public, max-age=7776000, immutable'. The 'Accent-Ranges' header is 'none'. The response body contains the jQuery 3.2.1 source code.

The bottom panel shows the 'Alerts' tab with a list of detected vulnerabilities. The 'Vulnerable JS Library' alert is highlighted, indicating a vulnerability in the jQuery 3.2.1.min.js file. The alert details include the URL, risk level (Medium), confidence (Medium), attack type, evidence, CWE ID (829), WASC ID, origin (Passive), and a description stating that the identified library is vulnerable. Other alerts listed include 'X-Frame-Options Header Not Set', 'Absence of Anti-CSRF Tokens', 'Cookie No HttpOnly Flag', 'Cookie Without SameSite Attribute', 'Incomplete or No Cache-control and Pragma Headers', 'Server Leaks Information via "X-Powered-By" Header', 'Information Disclosure - Suspicious Comments', and 'Timestamp Disclosure - Unix'.

Al igual que ocurría con la web isent.es , es notable la ausencia del header X-Frame-Options.

webmail.isent.es

Falta el header X-Frame-Options y la versión de JQuery es una vulnerable desactualizada:

The screenshot shows the Burp Suite interface. The top pane displays the raw HTTP response from webmail.isent.es. The response headers include: HTTP/1.1 200 OK, Date: Thu, 17 Jun 2021 14:50:26 GMT, Server: Apache, Strict-Transport-Security: max-age=63072000, X-Content-Type-Options: nosniff, Last-Modified: Tue, 26 May 2020 02:23:47 GMT, ETag: "1582b-5a683c90492c0", Accept-Ranges: bytes, Content-Length: 88107. The response body contains a license notice for jQuery v3.2.1. The bottom pane shows a vulnerability alert titled 'Vulnerable JS Library' for the URL https://webmail.isent.es/program/js/jquery.min.js?s=1590459827. The alert indicates a Medium risk, with evidence from the jQuery v3.2.1 source code. The alert also lists CVE-2020-11023 and CVE-2020-11022 as related vulnerabilities.

newisent.isent.es

Los usuarios de WordPress son visibles

The screenshot shows a terminal window displaying the results of a WordPress user enumeration scan. The output is as follows:

```
[i] User(s) Identified:
[+] newisentadmin
    Found By: Author Posts - Author Pattern (Passive Detection)
    Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] admin
    Found By: Rss Generator (Passive Detection)
    Confirmed By: Rss Generator (Aggressive Detection)
```

Los siguientes plugins están desactualizados:

- wordpress-seo-premium
- woocommerce
- revslider
- elementor
- contact-form-7

La versión de JQuery es muy antigua y necesita actualizarse.