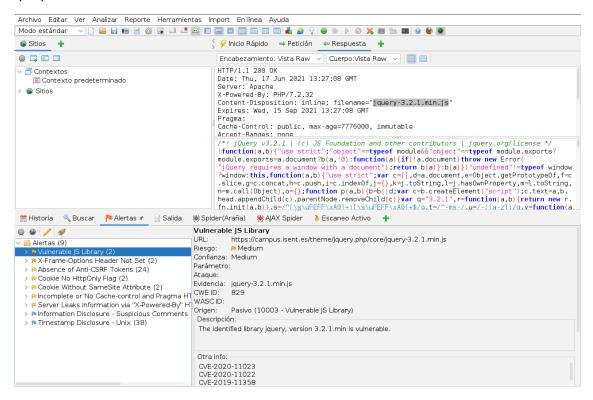
Auditoría

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
```

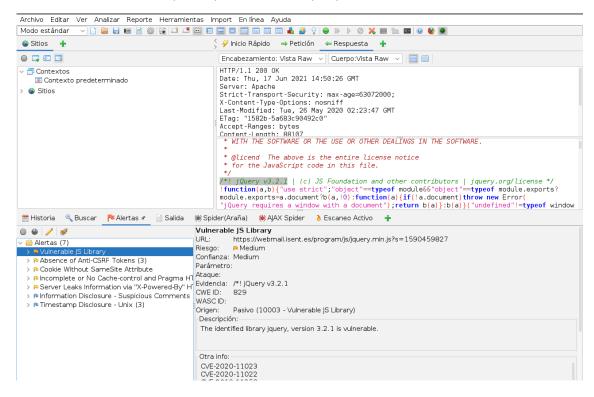
Las versiones de PHP y de Jquery son visibles, siendo esta última una versión desactualizada que presenta vulnerabilidades:



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:



newisent.isent.es

Los usuarios de WordPress son visibles

```
[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.