DrupalCon
NORTH AMERICA 2021
ONLINE APRIL 12-16

Achieving an A+ score on the Mozilla Observatory tool to help pass security testing

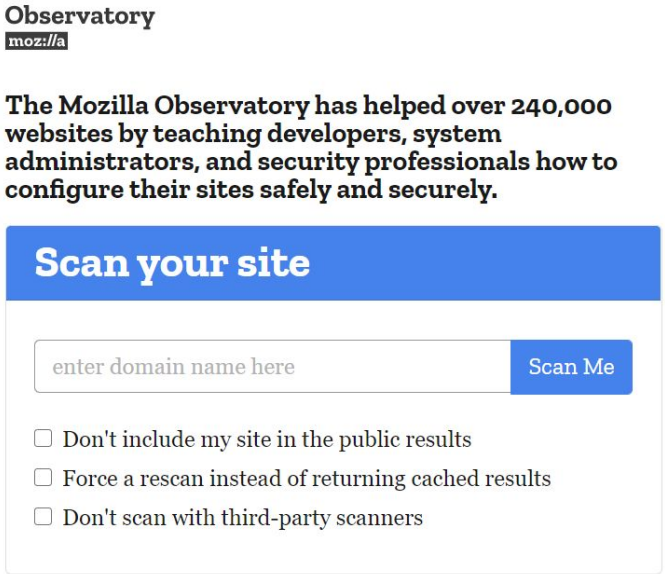
Alex Johnston
Senior DevOps
Alexj12

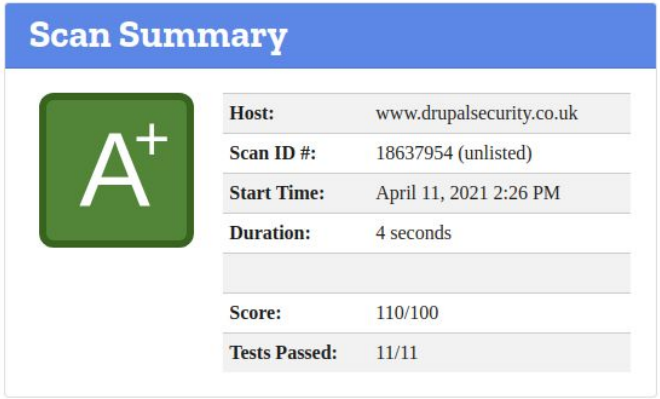
David Pratt
Technical Director
davepratt

ZOOCHA

Introducing Mozilla Observatory

observatory.mozilla.org

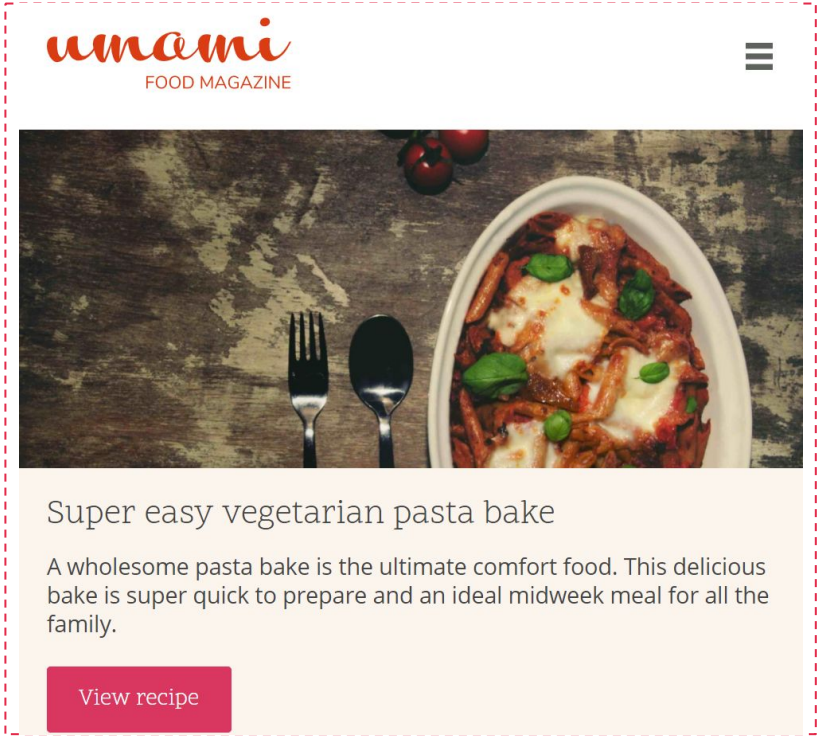




The beginning... new Drupal 9 site, new environment

Basic Configuration Applied

drupalsecurity.co.uk



- Added Google Analytics & Google Tag Manager
- Started a simulated session for all users

Example Umami Drupal 9 Site Launched on AWS

Current Status: Not great...

Scan Summary

F

Host:	www.drupalsecurity.co.uk
Scan ID #:	18577932 (unlisted)
Start Time:	April 7, 2021 11:27 PM
Duration:	2 seconds
Score:	0/100
Tests Passed:	6/11

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✗	-40	Session cookie set without using the `Secure` flag or set over HTTP	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header can't be implemented without HTTPS (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header cannot be set for sites not available over HTTPS	ⓘ
Redirection	✗	-20	Does not redirect to an HTTPS site	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Let’s get tweaking...

Adding SSL

Current Status: Not great, not terrible...

Scan Summary

D-

Host:	www.drupalsecurity.co.uk
Scan ID #:	18656881 (unlisted)
Start Time:	April 12, 2021 4:43 PM
Duration:	4 seconds
Score:	25/100
Tests Passed:	7/11

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✓	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	ⓘ
Redirection	✗	-20	Does not redirect to an HTTPS site	ⓘ
Referrer Policy	–	0	Referrer-Policy header set to `"no-referrer-when-downgrade"`	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header set to `"0"` (disabled)	ⓘ

Forced SSL

Forcing all users onto SSL means less risk and less confusion.

Scan Summary

C-

Host:	www.drupalsecurity.co.uk
Scan ID #:	18578037 (unlisted)
Start Time:	April 7, 2021 11:39 PM
Duration:	3 seconds
Score:	45/100
Tests Passed:	8/11

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✓	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Improving Drupal... Security Kit Module

Introducing Security Kit (seckit) module

drupal.org/project/seckit

Drupal™

Security Kit

View | Version control | View history | Automated testing

By p0deje on *26 March 2011*, updated *28 August 2020*

SecKit provides Drupal with various security-hardening options. This lets your mitigate the risks of exploitation of different web application vulnerabilities.

Cross-site Scripting

Content Security Policy implementation via Content-Security-Policy (official name), X-Content-Security-Policy (Firefox and IE) and X-WebKit-CSP (Chrome and Safari) HTTP response headers (configuration page and reporting CSP violations to

Star 106 | No mail

Maintainers for Security Kit

mcdruid - 24 commits
last: 10 months ago, first: 2 years ago

jweowu - 26 commits
last: 4 years ago, first: 7 years ago

badjava - 4 commits

Let's get configuring... Security Kit Module

Enabling HSTS

▼ **SSL/TLS**

Configure various techniques to improve security of SSL/TLS

☑ HTTP Strict Transport Security

Max-Age *

31536000

Specify Max-Age value in seconds. It sets period when user-agent should remember receipt of this header field from this server. Default is 1000.

☑ Include Subdomains

☑ Preload

Scan Summary

B-

Host:	www.drupalsecurity.co.uk
Scan ID #:	18637592 (unlisted)
Start Time:	April 11, 2021 1:56 PM
Duration:	3 seconds
Score:	65/100
Tests Passed:	9/11

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✓	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Enabling X-XSS-PROTECTION

X-XSS-PROTECTION HEADER

X-XSS-Protection HTTP response header controls Microsoft Internet Explorer, Google Chrome and Apple Safari internal XSS filters.

Configure

1; mode=block

- Disabled - XSS filter will work in default mode. Enabled by default
- 0 - XSS filter will be disabled for a website. It may be useful because of IE's XSS filter security flaws in past
- 1 - XSS filter will be left enabled, and will modify dangerous content
- 1; mode=block - XSS filter will be left enabled, but it will block entire page instead of modifying dangerous content

Scan Summary

B

Host:	www.drupalsecurity.co.uk
Scan ID #:	18637780 (unlisted)
Start Time:	April 11, 2021 2:09 PM
Duration:	3 seconds
Score:	75/100
Tests Passed:	10/11

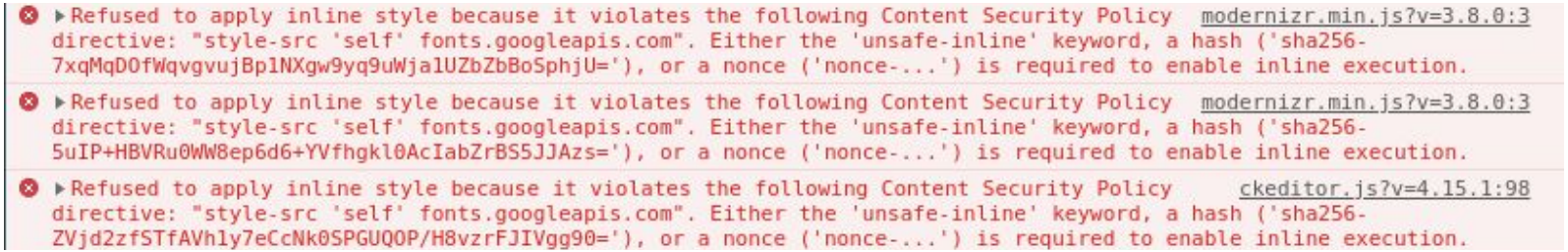
Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	✓	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✓	0	X-XSS-Protection header set to `"1; mode=block"`	ⓘ

Configuring CSP Header

Here be dragons...

- Trickiest to configure! By enabling CSP it places restrictions on potential content editing so may require maintenance.
- Drupal Core has elements that require '*unsafe-inline*' which impacts the score; CKEditor is breaks when enabled: https://www.drupal.org/project/drupal/issues/2789139



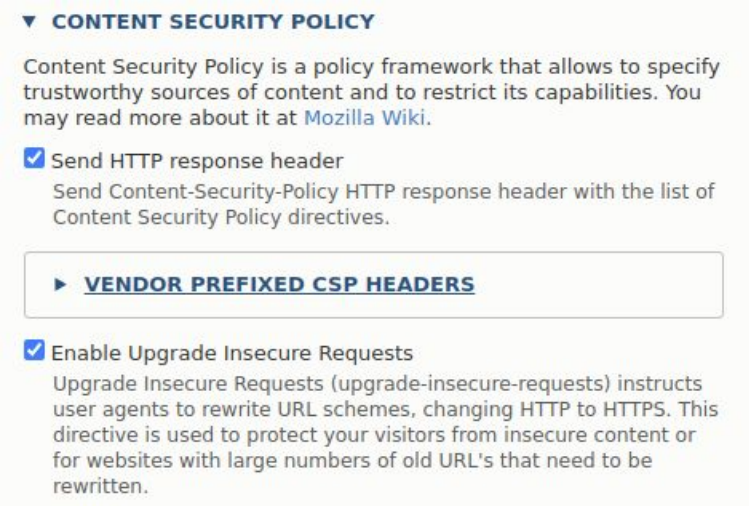
- This is about balance between optimum security and functionality

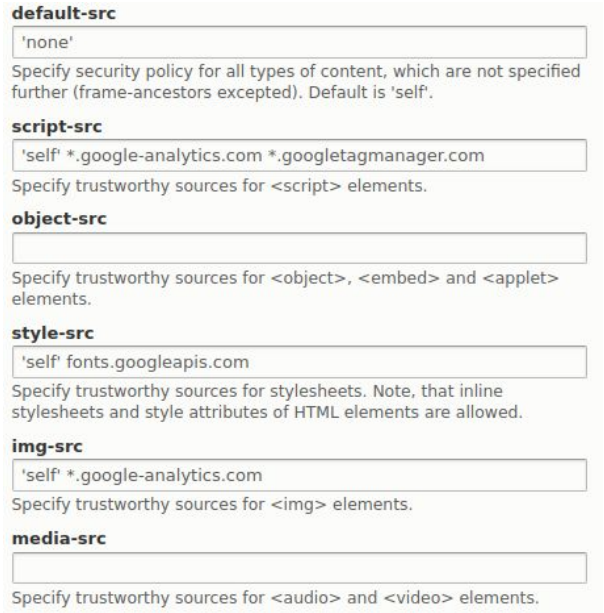
Configuring CSP Header

- Requires evaluation for what sources your application loads from.
- Define these expected sources in the header.

  https://addons.mozilla.org/en-US/firefox/addon/laboratory-by-mozilla/

  helps greatly in this area.





Enabling CSP Header

Scan Summary

A+

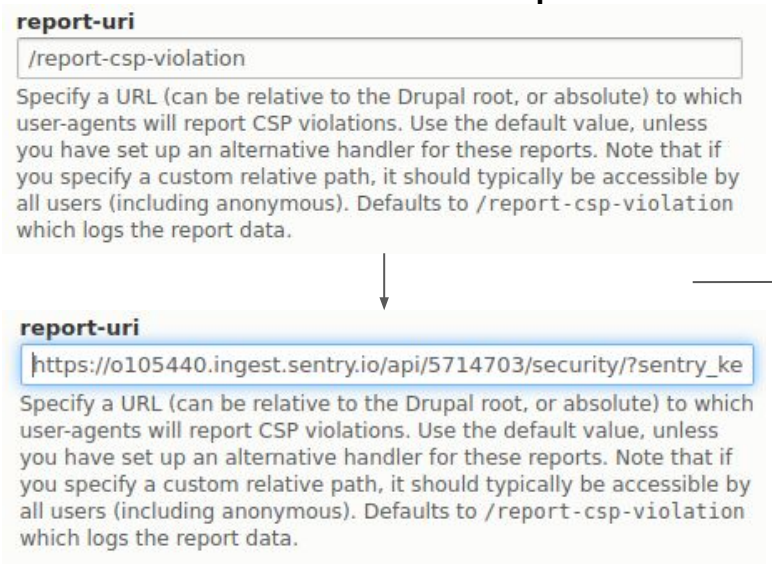
Host:	www.drupalsecurity.co.uk
Scan ID #:	18637954 (unlisted)
Start Time:	April 11, 2021 2:26 PM
Duration:	4 seconds
Score:	110/100
Tests Passed:	11/11

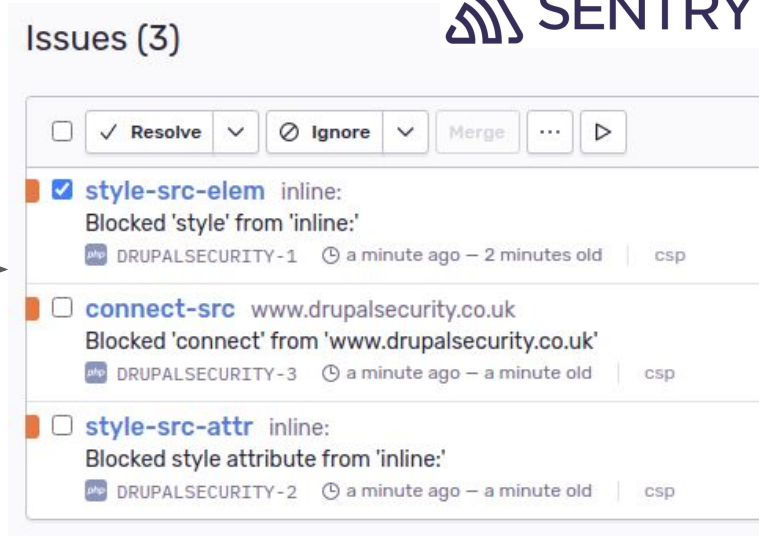
Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✓	+10	Content Security Policy (CSP) implemented with `default-src 'none'` and no `'unsafe'`	ⓘ
Cookies	✓	0	All cookies use the `Secure` flag and all session cookies use the `HttpOnly` flag	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	ⓘ
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to `SAMEORIGIN` or `DENY`	ⓘ
X-XSS-Protection	✓	0	X-XSS-Protection header set to `"1; mode=block"`	ⓘ

Security Kit module: Enable CSP - Reporting

- Browsers will send data to a URL to report breaches of the CSP, enabling breaches to be monitored.
- By default this is Drupal's error log. External services exist which can consume these reports.





Final Thoughts

Important Considerations

This is just one aspect of security testing!

- Don’t forget about outdated software versions, SQL injection vulnerabilities, weak password policies and such
- Implementing these recommendations is not a replacement for writing code with security in mind or running regular security based tests. Eg. OWASP ZAP/Nessus/Manual penetration testing
- The Security Kit module is not the only way to implement these recommendations, but it is generally the easiest
- Headers could be added at the CDN level, or Nginx/Apache level where less logic is required

Closing thoughts

- Some recommendations require training and awareness from content editors/business
- Balance is needed between functionality and scoring
- Lots of resources out there:
  https://developers.google.com/web/fundamentals/security
  https://infosec.mozilla.org/guidelines/web_security.html
  https://owasp.org/www-project-secure-headers/
- Mozilla Observatory is Open Source:
  https://github.com/mozilla/http-observatory

Thank you

ZOOCHA