

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

ZOOCHA

Alex Johnston Senior DevOps Alexj12 David Pratt Technical Director davepratt



Introducing Mozilla Observatory

observatory.mozilla.org

Observatory moz://a

The Mozilla Observatory has helped over 240,000 websites by teaching developers, system administrators, and security professionals how to configure their sites safely and securely.

Scan your site

enter domain name here

Scan Me

- □ Don't include my site in the public results
- □ Force a rescan instead of returning cached results
- □ Don't scan with third-party scanners





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

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



Basic Configuration Applied

drupalsecurity.co.uk



Super easy vegetarian pasta bake

A wholesome pasta bake is the ultimate comfort food. This delicious bake is super quick to prepare and an ideal midweek meal for all the family.

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

users

View recipe



Example Umami Drupal 9 Site Launched on AWS

Current Status: Not great...

X-XSS-Protection

×

-10

Scan Summary

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

6/11

Tests Passed:

Test Scores			
Test	Pass	Score	Reason
Content Security Policy	×	-25	Content Security Policy (CSP) header not implemented
Cookies	×	- <mark>4</mark> 0	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 HT
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 origi
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 header not implemented

Info

i

(i)

(i) (i)

i

(1)

(i)

(i)

i
 i

Let's get tweaking...

•





Current Status: Not great, not terrible...

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	í
Cookies	~	0	All cookies use the $\tt Secure$ flag and all session cookies use the $\tt HttpOnly$ flag	(i)
Cross-origin Resource Sharing	~	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	i
HTTP Public Key Pinning	-	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	i
HTTP Strict Transport Security	×	-20	HTTP Strict Transport Security (HSTS) header not implemented	i
Redirection	×	-20	Does not redirect to an HTTPS site	i
Referrer Policy	-	0	Referrer-Policy header set to "no-referrer-when-downgrade"	i
Subresource Integrity	-	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	(i)
X-Content-Type-Options	1	0	X-Content-Type-Options header set to "nosniff"	i
X-Frame-Options	~	0	X-Frame-Options (XFO) header set to SAMEORIGIN or DENY	i
X-XSS-Protection	×	-10	X-XSS-Protection header set to "0" (disabled)	i



Forced SSL

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

	Host:	www.drupalsecurity.co.uk
\cap	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	i
Cookies	1	0	All cookies use the Secure flag and all session cookies use the ${\tt HttpOnly}$ flag	i
Cross-origin Resource Sharing	~	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	i
HTTP Public Key Pinning	2 2	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	i
HTTP Strict Transport Security	×	-20	HTTP Strict Transport Security (HSTS) header not implemented	i
Redirection	1	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	i
Referrer Policy	-	0	Referrer-Policy header not implemented (optional)	í
Subresource Integrity	-	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	(j)
X-Content-Type-Options	~	0	X-Content-Type-Options header set to "nosniff"	i
X-Frame-Options	1	0	X-Frame-Options (XFO) header set to SAMEORIGIN OF DENY	i
X-XSS-Protection	×	-10	X-XSS-Protection header not implemented	í

Improving Drupal... Security Kit Module



Introducing Security Kit (seckit) module

drupal.org/project/seckit



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

		classify it solves betty
T. Dasiele krying		
Collars has an article termine of problem too one on printing states		
 Schot Scott May 		
· Kittle Printerson		
1 Utered Autors 1015 with		
1 Lines in the		
1 Down and Tempory		
1 Incentra		
1 10.01		

★ 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

		-	
	\prec		

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



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

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

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



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

Refused to apply inline style because it violates the following Content Security Policy <u>modernizr.min.js?v=3.8.0:3</u> directive: "style-src 'self' fonts.googleapis.com". Either the 'unsafe-inline' keyword, a hash ('sha256-7xqMqDOfWqvgvujBp1NXgw9yq9uWja1UZbZbBoSphjU='), or a nonce ('nonce-...') is required to enable inline execution.

- Refused to apply inline style because it violates the following Content Security Policy <u>modernizr.min.js?v=3.8.0:3</u> directive: "style-src 'self' fonts.googleapis.com". Either the 'unsafe-inline' keyword, a hash ('sha256-5uIP+HBVRu0WW8ep6d6+YVfhgkl0AcIabZrBS5JJAzs='), or a nonce ('nonce-...') is required to enable inline execution.
- Refused to apply inline style because it violates the following Content Security Policy <u>ckeditor.js?v=4.15.1:98</u> directive: "style-src 'self' fonts.googleapis.com". Either the 'unsafe-inline' keyword, a hash ('sha256-ZVjd2zfSTfAVhly7eCcNk0SPGUQ0P/H8vzrFJIVgg90='), or a nonce ('nonce-...') is required to enable inline execution.
- 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.

CONTENT SECURITY POLICY

Content Security Policy is a policy framework that allows to specify trustworthy sources of content and to restrict its capabilities. You may read more about it at Mozilla Wiki.

Send HTTP response header

Send Content-Security-Policy HTTP response header with the list of Content Security Policy directives.

VENDOR PREFIXED CSP HEADERS

Enable Upgrade Insecure Requests

Upgrade Insecure Requests (upgrade-insecure-requests) instructs user agents to rewrite URL schemes, changing HTTP to HTTPS. This directive is used to protect your visitors from insecure content or for websites with large numbers of old URL's that need to be rewritten.

default-src

'none'

Specify security policy for all types of content, which are not specified further (frame-ancestors excepted). Default is 'self'.

script-src

'self' *.google-analytics.com *.googletagmanager.com

Specify trustworthy sources for <script> elements.

object-src

Specify trustworthy sources for <object>, <embed> and <applet> elements.

style-src

'self' fonts.googleapis.com

Specify trustworthy sources for stylesheets. Note, that inline stylesheets and style attributes of HTML elements are allowed.

img-src

'self' *.google-analytics.com

Specify trustworthy sources for elements.

media-src

Specify trustworthy sources for <audio> and <video> elements.



Enabling CSP Header

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

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.

report-uri

/report-csp-violation

Specify a URL (can be relative to the Drupal root, or absolute) to which user-agents will report CSP violations. Use the default value, unless you have set up an alternative handler for these reports. Note that if you specify a custom relative path, it should typically be accessible by all users (including anonymous). Defaults to /report-csp-violation which logs the report data.

report-uri

https://o105440.ingest.sentry.io/api/5714703/security/?sentry_ke

Specify a URL (can be relative to the Drupal root, or absolute) to which user-agents will report CSP violations. Use the default value, unless you have set up an alternative handler for these reports. Note that if you specify a custom relative path, it should typically be accessible by all users (including anonymous). Defaults to /report-csp-violation which logs the report data.







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





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

https://github.com/mozilla/http-observatory

Thank you

