DuckCorp Infrastructure - Enhancement #602

Deploy Content Security Policy (CSP) and check other security headers

2017-09-30 09:02 - Marc Dequènes

Status:	In Progress	**Start date:**	2017-09-30
Priority:	Normal	**Due date:**	
Assignee:	Marc Dequènes	**% Done:**	30%
Category:	Service :: Web	**Estimated time:**	0:00 hour
Target version:			
Patch Available:		**Entity:**	DuckCorp
Confirmed:	No	**Security:**	Yes
Branch:		**Help Needed:**	

Description

We should have a look at this: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Full specification: https://www.w3.org/TR/CSP/

Related issues:

Related to DuckCorp Infrastructure - Enhancement #571: Secure HTTP settings	**Resolved**	**2017-06-25**

History

#1 - 2017-09-30 09:03 - Marc Dequènes

This FF plugin could be handy: https://addons.mozilla.org/en-US/firefox/addon/laboratory-by-mozilla/

#2 - 2017-09-30 09:03 - Marc Dequènes

- Related to Enhancement #571: Secure HTTP settings added

#3 - 2017-09-30 12:02 - Marc Dequènes

- % Done changed from 0 to 10

Tested on test.duckcorp.org and fixed a few things. Now applied on www.duckcorp.org.

The FF plugin had a false positive on script-src 'unsafe-inline'. I found the error reporting clearer on Chromium.

#4 - 2018-01-08 14:41 - Marc Dequènes

```
Content Security Policy: The page’s settings blocked the loading of a resource at https://irconweb.milkypond.o
rg/#chan-1 (“form-action 'none'”).
```

#5 - 2018-12-06 12:15 - Marc Dequènes

- Subject changed from Experiment with Content Security Policy (CSP) to Deploy Content Security Policy (CSP) and check other security headers

- % Done changed from 10 to 30

It works, even if finding the right setting may need some trial and error.

I've already setup certain vhosts and certain applications may provide one (Nexcloud), so let's list the vhost needing one and fix them one by one.

I should also check the result of: https://securityheaders.com/

I updated the *httpd* role for more secure headers. I need to have a look at duplicate headers.

#6 - 2019-09-09 08:53 - Marc Dequènes

The Mozilla checker is interesting, especially for the CSP analysis. I'll make some fixes for our website soon and then try to add support for more vhosts.

#7 - 2019-09-10 08:25 - Marc Dequènes

Let's protect core services first:

- ca.duckcorp.org
- db.duckcorp.org
- ddns.duckcorp.org
- dico.duckcorp.org
- doc.duckcorp.org
- gossip.duckcorp.org
- lists.duckcorp.org
- myip.duckcorp.org
- ntp.duckcorp.org
- projects.duckcorp.org
- radio.duckcorp.org
- repository.duckcorp.org
- shizuka-STAR.duckcorp.org
- smokeping.duckcorp.org
- sources.duckcorp.org
- static.perso.duckcorp.org
- ~~stuff.milkypond.org~~ (handled by NextCloud)
- sup.duckcorp.org
- users.duckcorp.org
- vcs.duckcorp.org
- vcs-git.duckcorp.org
- vcs-git-viewer.duckcorp.org
- ~~webmail.duckcorp.org~~
- wiki.duckcorp.org
- www.duckcorp.org
- www.milkypond.org (redirection)

Excluded vhosts:

- perso.duckcorp.org: each user needs to adapt to its own need
- photos-ng.duckcorp.org: experimental at the moment

#8 - 2019-09-28 18:34 - Marc Dequènes

updated currently deployed CSP to use *upgrade-insecure-requests*