Protect your web app with ClamAV

...

Clam AntiVirus (ClamAV)

Free, open-source antivirus (GNU General Public License) software toolkit / engine able to detect many types of malicious software, including viruses. One of its main uses is on mail servers as a server-side email virus scanner.

Last stable release - 0.99.2.

Clam AntiVirus (ClamAV)

- Started 2002
- Project, trademark and copyrights bought on August 17th 2007 by Sourcefire
- Since October 7th 2013 Sourcefire has been owned by Cisco.

Clam AntiVirus (ClamAV)

Cross-platform:

- Unix, AIX, BSD, HP-UX, Linux
- macOS
- Microsoft Windows (from version 0.97.5 released June 1 2012)

Clam AntiVirus (ClamAV)

Main features:

- command-line scanner
- automatic database updater
- scalable multi-threaded daemon
- support for scanning inside compress files such as: Zip, RAR, Tar, Gzip, Bzip2, OLE2
- detects archive bombs / zip bombs / decompression bomb
- virus DB contained over 6,301,600 viruses
- support for MS Office and MacOffice files, HTML, Flash, RTF and PDF

Clam AntiVirus (ClamAV)

Components:

- clamscan
- freshclam
- clamd
- clamdscan
- clamconf
- scripts which start clamd i freshclam in daemon mode

Clam AntiVirus (ClamAV)

How to implement:

- clamdscan / cron
- pyClamd
- ProtectedFileField

Clam AntiVirus (ClamAV)

Clamdscan / cron

Clam AntiVirus (ClamAV)

pyClamd

- python interface to Clamd (ClamAV antivirus daemon)
- compatible with python 3 (tested with 3.4.3) and python 2 (tested 2.7.3).
- pip install pyclamd / python setup.py install
- usage...

Clam AntiVirus (ClamAV)

ProtectedFileField

- similar to django FileField
- pip install django-antivirus-field
- code & usage...

Clam AntiVirus (ClamAV)

ClamAV cons?

- Max 4GB files
- Scanning viruses results:
  - detected only 15.3% of Windows malware and ranked 16 out of 16
  - detected 66.1% of Linux malware and ranked 13 out of 16 for Linux

Clam AntiVirus (ClamAV)

Basic security tips for uploading files to your app:

- Avoid unnecessary file uploads
- Ensure that files uploaded by the user cannot be interpreted as script files by the web server,
- Ensure that the file extension matches the actual type of the file content
- If only images are to be uploaded, consider re-compressing them using a secure library to ensure they are valid
- Prevent users from uploading problematic file types like HTML, CSS, JavaScript, XML, SVG
- Prevent users from uploading special files (e.g. .htaccess, web.config, robots.txt, crossdomain.xml, clientaccesspolicy.xml)
- Consider delivering uploaded files with the “Content-disposition: attachment” header


THANKS!