Preventing malicious file upload

1. The application should use a whitelist of allowed file types. This list determines the types of files that can be uploaded, and rejects all files that do not match approved types.
2. The application should use client- or server-side input validation to ensure evasion techniques have not been used to bypass the whitelist filter. These evasion techniques could include appending a second file type to the file name (e.g. image.jpg.php) or using trailing space or dots in the file name.
3. The application should set a maximum length for the file name, and a maximum size for the file itself.
4. The directory to which files are uploaded should be outside of the website root.
5. All uploaded files should be scanned by antivirus software before they are opened.
6. The application should not use the file name supplied by the user. Instead, the uploaded file should be renamed according to a predetermined convention.