# What are file upload vulnerabilities?

File upload vulnerabilities occur when an application accepts a file without properly validating its type, content, or storage location, letting an attacker upload a web shell or malicious file that the server then executes or serves. The worst case is uploading a script (such as a `.php` file) into a web-accessible, executable directory, giving remote code execution. The fix combines server-side type validation, storing uploads outside the web root, and never executing uploaded content.

## HOW IT WORKS

### 01 How it works and example

The attacker tries to get an executable file into an executable location:

- Upload `shell.php` containing `<?php system($_GET[0]); ?>` and browse to it to run commands.
- Bypass weak filters: double extensions (`shell.php.jpg`), null bytes, case (`.pHp`), or trusting the client `Content-Type`.
- Bypass magic-byte checks by prepending valid image headers to a polyglot file.
- Path traversal in the filename (`../../shell.php`) to escape the upload directory.
- Upload an SVG with embedded script (stored XSS) or external entities (XXE).

Examples shown for defensive context.

> **STORE OUTSIDE THE WEB ROOT**
>
> *Even a successfully uploaded shell is harmless if it cannot be executed. Store uploads outside the web root (or in a bucket) and serve them through a handler that never executes them.*

## HOW TO DEFEND

- Validate type server-side by content, not the client-supplied extension or Content-Type, and allow-list permitted types.
- Store uploads outside the web root and serve via a controlled handler, so they are never executed.
- Rename files to server-generated names and strip path components from the original filename.
- Disable script execution in the upload directory (web-server config).
- Scan and size-limit uploads, and treat SVG/Office files as active content.
- Test the upload flow for filter bypasses.

## SOURCES

[1] OWASP: File Upload

[2] MITRE CWE-434: Unrestricted Upload of File with Dangerous Type

[3] OWASP Top 10

**Test your application for insecure file upload and 30+ other classes.**

securelayer7.net/learn/application-security/file-upload-vulnerabilities

Open online