CAPEC-563: Add Malicious File to Shared Webroot (Version 3.9)

Archived: 2026-04-05 15:46:47 UTC

Description

An adversaries may add malicious content to a website through the open file share and then browse to that content with a web browser to cause the server to execute the content. The malicious content will typically run under the context and permissions of the web server process, often resulting in local system or administrative privileges depending on how the web server is configured.

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type
ChildOf	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack. It

This table shows the views that this attack pattern belongs to and top level categories within that view.

Mitigations

Ensure proper permissions on directories that are accessible through a web server. Disallow remote access to the web root. Disable execution on directories within the web root. Ensure that permissions of the web server process are only what is required by not using built-in accounts and instead create specific accounts to limit unnecessary access or permissions overlap across multiple systems.

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (see parent)

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2015-11-09 (Version 2.7)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

More information is available — Please select a different filter.
