CAPEC-650: Upload a Web Shell to a Web Server (Version 3.9)

Archived: 2026-04-05 16:37:38 UTC

Description

By exploiting insufficient permissions, it is possible to upload a web shell to a web server in such a way that it can be executed remotely. This shell can have various capabilities, thereby acting as a "gateway" to the underlying web server. The shell might execute at the higher permission level of the web server, providing the ability the execute malicious code at elevated levels.

Typical Severity

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.

Prerequisites

The web server is susceptible to one of the various web application exploits that allows for uploading a shell file.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Confidentiality	Read Data	
Confidentiality Access Control Authorization	Gain Privileges	
Confidentiality Integrity Availability	Execute Unauthorized Commands	

Mitigations

Make sure your web server is up-to-date with all patches to protect against known vulnerabilities.
Ensure that the file permissions in directories on the web server from which files can be execute is set to the "least privilege" settings, and that those directories contents is controlled by an allowlist.

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 (also see parent)

Entry ID	Entry Name
1505.003	Server Software Component:Web Shell

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2018-05-31 (Version 2.11)	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 Mitigations, Taxonomy_Mappings	
2020-12-17 (Version 3.4)	CAPEC Content Team	The MITRE Corporation
	Updated Mitigations	

More information is available — Please select a different filter.
