The Command Execution section covers attacks designed to execute remote commands on the web site. All web sites utilize user-supplied input to fulfill requests. Often these user-supplied data are used to create commands resulting in dynamic web page content. If this process is done insecurely, an attacker could alter command execution.

The Authentication section covers attacks designed to acquire system-specific information about a web site. System-specific information includes the software distribution, version numbers, and patch levels. On the information may contain the location of backup files and temporary files. In most cases, divulging this information is not required to fulfill the needs of the user. Most web sites will reveal a certain amount of data, but it's still to the attacker's advantage. The more information about the web site an attacker learns, the easier the system becomes to compromise.

The Authorization section covers attacks designed to target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action. For example, many web sites should only allow certain users to access specific content or functionality. Other times a user's access to other resources might be restricted. Using various techniques, an attacker can find a web site into increasing their privileges to protected areas.

The Information Disclosure section covers attacks designed to acquire system-specific information about a web site. System-specific information includes the software distribution, version numbers, and patch levels. On the information may contain the location of backup files and temporary files. In most cases, divulging this information is not required to fulfill the needs of the user. Most web sites will reveal a certain amount of data, but it's still to the attacker's advantage. The more information about the web site an attacker learns, the easier the system becomes to compromise.

Logical Attacks

Abuse of Functionality

Denial of Service

Insufficient Anti-automation

Insufficient Process Validation