File Upload Vulnerability and Webshells

A presentation on file upload vulnerabilities, PHP and ASP webshells, and defacing pages.

Table of Contents

1 File Upload Vulnerabilities

2 What is a PHP Webshell?

3 What is an ASP Webshell?

4 How Can We Upload a Webshell?

5 What is a Defaced Page?

1

File Upload Vulnerabilities

File upload vulnerabilities occur when an application improperly handles file uploads, allowing attackers to upload malicious files.
These vulnerabilities can lead to code execution, server compromise, or unauthorized access.

What is a PHP Webshell?

A PHP webshell is a malicious PHP script uploaded to a server that allows an attacker to control the server remotely. It provides an interface to execute commands on the server, often used to exploit a server after an initial breach.

What is an ASP Webshell?

Similar to PHP webshells, ASP webshells are malicious scripts written in ASP (Active Server Pages).
These webshells exploit file upload vulnerabilities to gain control over the server and perform unauthorized actions.

4

How Can We Upload a Webshell?

An attacker can upload a webshell by exploiting file upload vulnerabilities in web applications.
This can include bypassing file extension checks, uploading through weak security configurations, or exploiting weaknesses in file handling functions.

What is a Defaced Page?

A defaced page is a webpage whose content is altered by an attacker to display unauthorized information. Defacement is often a result of an attack leveraging webshells to modify page contents, demonstrating control over the server.

Thank You!