# Risk Assessment:

Vulnerability: File Upload and Remote Code Execution (RCE)

Overall Risk Level: **Critical**

Assessment:

This assessment considers the combined risk of the identified file upload and RCE vulnerabilities. The potential consequences of exploiting these vulnerabilities are severe and immediate, justifying the Critical risk rating. The upload vulnerability gives an easy opportunity to run and exploit the RCE vulnerability. It is almost trivial how easy it is to get root privileges once a dangerous actor is in the same network.

Likelihood of Exploitation: **High**

- The exploit is very simple in nature as anyone with minimal knowledge can execute this attack. The know-how is very easy to find.
- The methodologies used to hack into this vulnerability is very well-known.
- Since this is an exploit that could be accessed through networks, it makes it even more possible to be exploited.

Impact of Exploitation: **Critical**

- This vulnerability seriously affects confidentiality as it becomes possible to access any file on this system. It is also possible to delete and upload any file.
- Due to the ability to get to root privileges through the RCE exploit, stored password hashes can be potentially broken through password crackers.
- This directly affects the trust an individual would have towards an organization that has this vulnerability in place. This would mean that all their data would be vulnerable if it were present in a system with this vulnerability.

**CVSS**:

- Base CVSS Score: **9.6**
- Base CVSS String: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- Attack Vector (AV:N): Remote attacks through the network can be done, it's a web server, any anyone in that network can attack this system.
- Attack Complexity (AC:L): Requires very low complexity, a simple file upload and a few lines of shell script available would suffice.
- Privileges Required (PR:N): Doesn't require any privilege, anyone on the website can do this.
- User Interaction (UI:N): Doesn't require user interaction. All interaction is done directly to the server.
- Scope (S:U): Doesn't go beyond the scope of the security authority involved. It is all their data.
- Confidentiality (C:H): Complete loss of confidentiality, RCE can get root privileges and through that password hashes and potential cracking of it.
- Integrity (I:H): Complete loss of integrity. With the use of password cracking, the hacker can pretend to be any of the current users.
- Availability (A:H): It  is possible to delete files and even the whole server.

- Relevant CWE Values:
    - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - This is the most common and well-known CWE associated with RCE. It occurs when an attacker can inject malicious code into an application's input, which is then processed as a command and executed by the operating system. This can allow the attacker to execute arbitrary code on the server.
    - CWE-434: Unrestricted Upload of File with Dangerous Type - This CWE occurs when an application allows users to upload files without any restrictions on the file type. This can be dangerous because it allows attackers to upload malicious files, such as executable files or scripts, that can be used to exploit other vulnerabilities on the system.

**ASVS Impact:**

Both RCE and file upload vulnerabilities severely compromise a web application's security posture. These vulnerabilities enable attackers to execute arbitrary code on the server, granting them complete control to access sensitive data, modify files, install malware, or even escalate their privileges. Additionally, attackers can exploit these vulnerabilities to upload malicious files that further compromise the application by exploiting other vulnerabilities like XSS or SQL injection, or even deface the website. Consequently, ensuring secure data storage and implementing robust authentication and authorization mechanisms are crucial to protecting against these critical vulnerabilities.

Exploiting this vulnerability would violate several ASVS requirements:

- ASVS Requirement V5.3: Output Encoding and Injection Prevention: This requirement states that applications must properly encode all output to prevent attackers from injecting malicious code into the application. The RCE vulnerability breaks this requirement because it allows attackers to inject malicious code into the application through a variety of methods, such as through user input or through file upload.

- ASVS Requirement V14.2: File and Resources Verification - This requirement states that applications must properly verify all file and resource access to prevent unauthorized access to sensitive data. The file upload vulnerability breaks this requirement because it allows attackers to upload files to the server without any restrictions. These files can then be used to exploit other vulnerabilities on the system or to access sensitive data.

- ASVS Requirement V7.1: Error Handling and Logging Verification - This requirement states that applications must properly handle and log errors to prevent attackers from exploiting them. The RCE vulnerability can break this requirement if the application does not properly log errors or if the attacker can gain access to the application's logs. This could allow them to troubleshoot exploits and bypass security controls.

- V12.1: Sensitive Data Storage Verification - This requirement verifies that the application stores sensitive data using secure methods to protect against unauthorized access, data breaches, and manipulation.