Risk Assessment

Likelihood

High

The likelihood of this vulnerability being exploited is high. It has a very low attack complexity due to the simplicity of exploiting this vulnerability. A script kiddie or other low knowledge threat actor could very easily carry out a successful exploit of this vulnerability. The likelihood is not critical as some more advanced attackers may overlook this vulnerability due to its simplicity. They may assume it doesn't exist because it is very obvious.

Impact

Critical

This is a critical impact vulnerability because it allows the attacker to execute any commands they want on the system in the scope of the permissions of the account running the web server. The attacker can establish persistence by adding users or services, they can escalate privileges by looking at shadow files or other means, lateral movement is possible by using various networking tools. In essence the attacker has full access to the system and can do anything they want.

Overall Risk

Critical

Utilizing the risk matrix in Figure #1 and the Likelihood and Impact assessments above the overall risk is Critical.

Overall Risk Rating Matrix				
Risk Rating		Probability		
		1 (low)	2 (medium)	3 (high)
Impact	1 (low)	low	low	medium
	2 (medium	low	medium	high
	3 (high)	medium	high	critical
	4 (critical)	high	critical	critical

CVSS

Base Score: 9.8
Base String: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Attack Vector: Network

Network was selected as a user can exploit this vulnerability remotely given they have access to the web server. Web servers can often be interacted with from the internet.

Attack Complexity: Low

This attack is very easy to exploit and doesn't require technical knowledge. This attack could be automated making it possible for anyone to exploit it

Privileges Required: None

The web server doesn’t require any credentials to do any actions

User Interaction: None

This vulnerability can be exploited without any interaction from the user

Scope: Unchanged

All operations happen on the host running the web server

Confidentiality: High

This exploit allows the attacker to compromise the confidentiality of anything on the system as they are able to access it and exfiltrate it

Integrity: High

This exploit allows the attacker to manipulate files and logs meaning they can forge integrity

Availability: High

This exploit allows the attacker to destroy the machine through various means causing a high impact to availability

CWEs

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- CWE-88: Argument Injection or Modification
- CWE-73: External Control of File Name or Path
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory

ASVS

This vulnerability significantly impacts a web applications security posture. A server with this vulnerability would not meet the following ASVS requirements.

- **ASVS 3.1.1** Verify that user input is not directly included in any command or query without proper input validation, sanitization, and/or parameterization to prevent injection flaws. This requirement aims to prevent command injection vulnerabilities, which are exactly the kind of vulnerability that the server has.
- **ASVS 4.2.2** Verify that the application does not allow injection of operating system commands through any interface. This requirement is also related to preventing command injection vulnerabilities.
- **ASVS 4.3.4** Verify that the application properly encodes or sanitizes all user-controllable output to prevent cross-site scripting, cross-site request forgery, and other injection attacks. This requirement aims to prevent attackers from injecting malicious scripts or code into web pages served by the application.
- **ASVS 6.2.2** Verify that the application and all components are using the most current stable release or version. This requirement is important to ensure that all security patches and bug fixes are applied to the server software, including the web server, PHP, and any other relevant components.