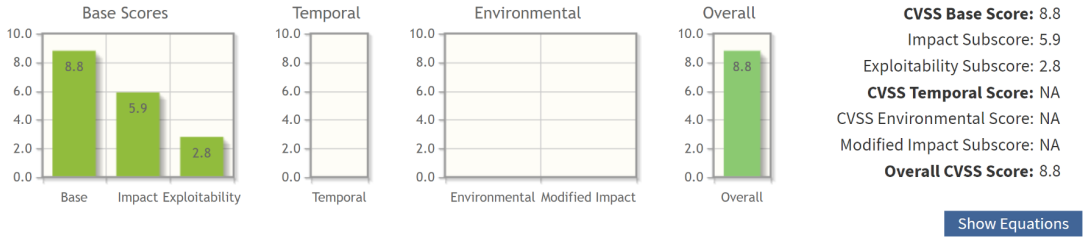
Vulnerability Risk Assessment

CVSS Risk Assessment



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

CVSS Base Score: 8.8

Exploitability Subscore: 2.8

Although the attack complexity is quite low and privileges are not required, the vulnerability requires user interaction (scripting), which greatly lowers the exploitability subscore.

Impact Subscore: 5.9

The impact subscore for this vulnerability is given the highest possible score due to high impact probabilities on confidentiality, integrity, and availability. This vulnerability gives control of the underlying operating system to the attacker, where the attacker can fully compromise the application and all its data.

CVSS Base Score Metrics

Attack Vector (AV): Network (AV:N) The vulnerability is exploitable with network access, meaning the vulnerability can be remotely executed.	**Scope (S):** Unchanged (U) The vulnerability can only affect resources managed by the same authority. The vulnerable component and impacted component are the same.
Attack Complexity (AC): Low (AC:L) The attack complexity is relatively low and can be repeated against the vulnerable web application server.	**Confidentiality Impact (C):** High (C:H) There is a complete loss of confidentiality, resulting in resources within the impacted component being divulged to the attacker.
Privileges Required (PR): None (PR:N) The attacker does not require access to privileged settings or files in order to carry out the attack.	**Integrity Impact (I):** High (I:H) There is a complete loss of integrity where an attacker is able to modify files within the web application server.
User Interaction (UI): Required (UI:R) The attack requires command injection, which requires user interaction with the web application server.	**Availability Impact (A):** High (A:H) There is a complete loss of availability, resulting in the attacker being able to fully deny any component of the web server.

CWE Risk Assessment

Relevant CWE Values:

- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CWE Assessment:

Command injection (shell injection) allows an attacker to execute arbitrary operating system commands on the server that is running the application where the attacker can fully compromise the application and all of its data.

Within the OWASP Application Security Verification Standard, several requirements within Validation, Sanitization and Encoding (V5) section have not been met including: verifying that the application has defenses against HTTP parameter pollution attacks (5.1.1), verifying that unstructured data is sanitized to enforce safety measures (5.2.2), and verifying that the operating system calls use parameterized OS queries or use contextual command line output encoding (5.3.8).