

Forum:[Hack Forums](#)

Thread: [Help me please : shell injection & Session Cookie Without Secure Flag](#)

mchairi - August 13, 2017, 5:58 pm

Hi guys!

please help me

How to exploit this : Session Cookie Without Secure Flag

Code At a glance

Classification Information

Resource /

Risk High

Request

GET /

Resource Content

```
laravel_session=eyJpdil6IndxM2JuR3JuVnFhNkF6anA4WXRLcXc9PSIsInZhbHVlIjoistBERG14N3cxcXhsaEJwZDhObnA5dDh0ck5xWGtKWDFmTmRyakxOQlIDVWlvdKE4dUg0RW81SG1pcVUrMVFOc3A3dk43bGJLSEdhWkRNT3dQWEICcGc9PSIsIm1hYyI6ImU5MTdjN2QyODFmZmRiYzkyY2NhNmJjNzg4MmYzN2VhNTAzOWJiMTIxYmM1ZDZiMjYwNDhlOWRlNzAyMWQxYjMifQ%3D%3D; expires=Mon, 14-Aug-2017 00:02:28 GMT; Max-Age=7200; path=/; HttpOnly
```

Discussion

Vega has detected that a known session cookie may have been set without the secure flag.

Impact

Cookies can be exposed to network eavesdroppers.

Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

Remediation

When creating the cookie in the code, set the secure flag to true.

References

Some additional links with relevant information published by third-parties:

Secure Flag

HttpOnly OWASP Reference

and how i can exploit this : shell injection

Code At a glance

Classification Information

Resource /ar/https://www .xxxxx .com/ar/welcome

Parameter first_name

Method POST

Detection Type Linux/Unix Blind Timing Analysis Checks

Risk High

Request

POST /ar/https://www .xxxxx .com/ar/welcome

[_token=55MozeaGeYIC07DipYsUTGaxLhG0UNISoXnt4MBD first_name=; /bin/sleep 31 ; email=vega@example.com country=US code=000 number=1 g-recaptcha-response=1]

Resource Content

<!DOCTYPE html>

<html>

<head>

<meta charset="UTF-8" />

<meta name="robots" content="noindex,nofollow" />

<style> body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica, Arial, sans-serif; margin: 0; padding-bottom: 45px; }

a { cursor: pointer; text-decoration: none; }

a:hover { text-decoration: underline; }

...

Discussion

Command injection vulnerabilities often occur when inadequately sanitized externally supplied data is as part of a system command executed through a command interpreter, or shell. Vulnerabilities such as these can be exploited by using shell metacharacters to run additional commands that were not intended to be executed by the application developer. The system() function, and derivatives, are often responsible, as these functions are very simple to use. These vulnerabilities can grant remote access to attackers, if exploited successfully.

Impact

Vega has detected a possible command injection vulnerability.

Attackers may be able to run commands on the server.

Exploitation may lead to unauthorized remote access.

I have tried a lot to know a method and I could not

Please help me ? ? ?

LD_PRELOAD - August 14, 2017, 3:10 pm

Stop skidding. You'll learn more alone.