huntr

# Reliance on Cookies without Validation and Integrity Checking in getgrav/grav

0

✓ Valid Reported on Sep 10th 2021

## ✍️ Description

Developers often set cookies to be accessible from the root context path ("/"). Doing so exposes the cookie to all web applications on the domain. Since cookies often carry sensitive information such as session identifiers, sharing cookies across applications can lead a vulnerability in one application to cause a compromise in another.

## 🕵️ Proof of Concept

```
 public function setFlashCookieObject($name, $object, $time = 60)
   {
       setcookie($name, json_encode($object), time() + $time, '/');

       return $this;
   }


{
       if (isset($_COOKIE[$name])) {
           $object = json_decode($_COOKIE[$name], false);
           setcookie($name, '', time() - 3600, '/');
           return $object;
       }
```

## 💥 Impact

A cookie with an overly broad path can be accessed through other applications on the same domain.

## Occurrences

Session.php L154 Session.php L169

CVE
CVE-2021-3818
(Published)

Vulnerability Type
CWE-565: Reliance on Cookies without Validation and Integrity Checking

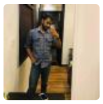
Severity
Medium (6.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by



Timmy
@lesveel
unranked

This report was seen 457 times.

We have contacted a member of the getgrav/grav team and are waiting to hear back a year ago

A getgrav/grav maintainer marked this as fixed with commit c51fb1 a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Session.php#L169 has been validated ✓

Session.php#L154 has been validated ✓

Chat with us

Jamie Slome a year ago Admin

CVE published! 🎉🎉

Timmy a year ago Researcher

Great @Jamie. Thanks :)

Sign in to join this conversation