PrestaShop’s ‘EU Cookie Law GDPR (Banner + Blocker)’ SQLi

2022-11-06

Contents

Description

CVE-2022-44727

The PrestaShop e-commerce platform module EU Cookie Law GDPR (Banner + Blocker) contains a Blind SQL injection vulnerability up to version 2.1.2. This module is widely deployed and is a “Best seller” on the add-ons store.

This vulnerability permits reading the shop’s database, allowing access to PII, and installing malware such as credit card stealers.

The vulnerability lies in a cookie used by the module to store the user’s choices.

Exploitation

Version 2

For newer versions of the module, the cookie `lgcookieslaw` contains a Base64 encoded JSON object instead of CSV.

To exploit these versions, you'll need to modify the `lgcookieslaw_accepted_purposes` of the object and then reencode to Base64:

```
"lgcookieslaw_accepted_purposes":"[\"1\",\"2\",\"3\",\"4\",\"5 AND SLEEP(5)"]"
```

Version 1

For older versions set the `__lglaw` cookie to `1,2,3,4) AND SLEEP(5)--` .

Mitigation

Users should update to version 2.1.3 of the module.

Kudos to the vendor for their politeness and for promptly confirming and releasing a fix for the vulnerability.