enchant97 / **note-mark** Public

Code | Issues 9 | Pull requests | Discussions | Actions | Projects | Se

Commit `cf4c6f6`

enchant97 committed 5 days ago Verified

```
(backend) prevent CWE-208 for internal login

fixes GHSA-w6m9-39cv-2fwp.
```

main · v0.19.2

1 parent 6593898 commit cf4c6f6

2 files changed +9 -2 lines changed

Top

Filter files…

- backend
  - db
    - models.go
  - services
    - auth.go

2 files changed +9 -2 lines changed

Search within code

backend/db/models.go

```
@@ -33,6 +33,8 @@ type User struct {
33 33       OidcRegistrations []OidcUser `gorm:"foreignKey:UserID"
            json:"oidcRegistrations,omitempty"`
34 34   }
35 35
      36 + var nullPasswordHash, _ = bcrypt.GenerateFromPassword([]byte("null"),
           bcrypt.DefaultCost)
      37 +
36 38   func (u *User) SetPassword(newPlainPassword string) {
```

```
37  39          hashedPw, err := bcrypt.GenerateFromPassword([]byte(newPlainPassword),
                bcrypt.DefaultCost)
38  40          if err != nil {
        @@ -42,10 +44,14 @@ func (u *User) SetPassword(newPlainPassword string) {
42  44      }
43  45
44  46      func (u *User) IsPasswordMatch(plainPassword string) bool {
    47  +       var current []byte
45  48          if len(u.Password) == 0 {
46      -           return false
    49  +           // prevent CWE-208
    50  +           current = nullPasswordHash
    51  +       } else {
    52  +           current = u.Password
47  53          }
48      -       if err := bcrypt.CompareHashAndPassword(u.Password, []byte(plainPassword));
                err == nil {
    54  +       if err := bcrypt.CompareHashAndPassword(current, []byte(plainPassword)); err
                == nil {
49  55              return true
50  56          }
51  57          return false
```

backend/services/auth.go

```
        @@ -29,6 +29,7 @@ func (s AuthService) GetAccessToken(
29  29          if err := db.DB.
30  30              First(&user, "username = ?", username).
31  31              Select("id", "password").Error; err != nil {
    32  +           user.IsPasswordMatch(password) // prevent CWE-208
32  33              return core.AccessToken{}, InvalidCredentialsError
33  34          }
34  35
```

Comments 0

Please sign in to comment.