MD5 hashing

A02:2021-Cryptographic Failures

Cryptographic Failures meaning

Sensitive data is poorly protected or not protected at all

Routes and files

Files

- frontend.js

Routes

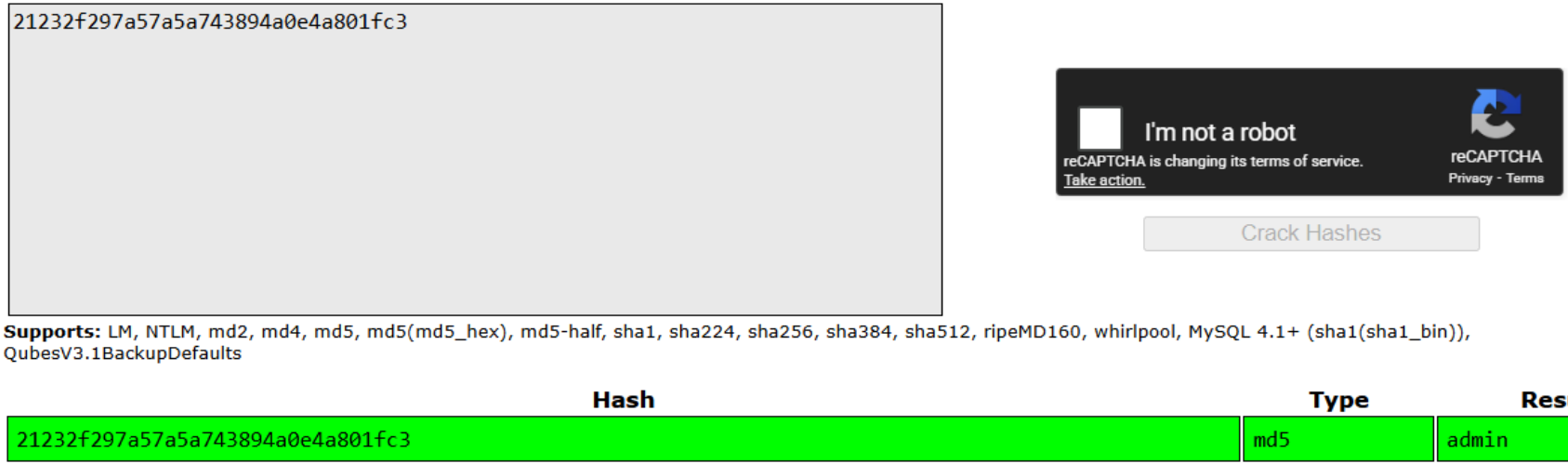
- /login
- /registerform

vulnerable code

```
    if (user[0].password === md5(userPassword)) {
      req.session.logged = true
      res.redirect('/profile?id='+user[0].id);
      return;
  }
```

exploitation

if the database was leaked an attacker could use a common wordlist or rainbow table to crack passwords
Ex:
21232f297a57a5a743894a0e4a801fc3 you could use (https://crackstation.net/) to crack hash



explanation

The application suffers from a Cryptographic Failure due to the use of MD5 for password hashing. MD5 is a broken and fast cryptographic hash function unsuitable for password storage. The implementation lacks salting and allows insecure password verification logic, making stored credentials vulnerable to offline attacks. The issue was mitigated by replacing MD5 with bcrypt, which provides adaptive hashing and built-in salting.

Semgrep rule

```yaml
rules:
  - id: md5-password
    patterns:
      - pattern: md5($X)
    message: "Insecure cryptographic algorithm detected (MD5)"
    severity: ERROR
    languages: [javascript]


```

fixes

```
const md5 = require('md5')
const new_user = db.user.create(
    {
        name:userName,
        email:userEmail,
        role:userRole,
        address:userAddress,
        password:md5(userPassword)
```

```
        const bcrypt = require('bcrypt');
        const hashedPassword = bcrypt.hashSync(userPassword, 10);
    const new_user = db.user.create(
        {
            name:userName,
            email:userEmail,
            role:userRole,
            address:userAddress,
            password: hashedPassword
```

```
const md5 = require('md5')
  if (user[0].password === md5(userPassword)) {
    req.session.logged = true
    res.redirect('/profile?id='+user[0].id);
    return;
}
```

```
const bcrypt = require('bcrypt');
if (bcrypt.compareSync(userPassword, user[0].password)) {
    req.session.logged = true
    res.redirect('/profile?id='+user[0].id);
    return;
}
```

example of "admin" with md5 and bcrypt:

Detailed demonstrations are shown in video

- md5: 21232f297a57a5a743894a0e4a801fc3
- becrypt: $2b$10$O47OeQHJ1SwKhWzsBo46HuLqwDd0F5rImIclEc.PxJxeW6efFdeoO