DMS Vinamilk

1. Vulnerable javascript lib :

Detail: Sử dụng jquery bản 1.7.1 có chứa các lỗ hổng đã được report, fix ở ver mới

URL: http://203.190.162.25:8100/resources/scripts/plugins/ckfinder/plugins/gallery/colorbox/jquery.min.js

How to fix: update newest version jquery

1. Captcha bypass:

Chức năng đăng nhập (<http://203.190.162.25:8100/login>) sử dụng captcha để giới hạn các request tự động. Tuy nhiên, attacker vượt qua cơ chế này chỉ cần xóa cookies

1. Login page password- guessing attack
2. Hệ thống không cài HTTPS

DMS ABBott

1. Vulnerable javascript lib:

Sử dụng jquery 1.4.4 có cảnh báo CVE-2011-4969 . Cần update version mới cho jquery

1. HTTP Strict Transport Security on implemented
2. Captcha bypass:

Chức năng đăng nhập (<https://dms.3anutrition.com/login> ) sử dụng captcha để giới hạn các request tự động. Tuy nhiên, attacker vượt qua cơ chế này chỉ cần xóa cookies