## 2.4. SQL Injection (demo)

Yêu cầu: Sử dụng extension hackbar V2 trên trình duyệ Mozilla Firefox

Website demo: <http://www.vietfarmsfsf.com>

Bước 1:

Nhập url: inurl: index.php? id=site vn để tìm các website bị lỗi

A screenshot of a computer

Description automatically generated with medium confidence

**Hình 2.24**

Bước 2:

Kiểm tra dấu nháy (‘) xem có lỗi hay không. Nguyên là do các file php không sử dụng PDO

Bước 3:

Dùng cậu lệnh “order by” để tìm số cột mà câu lệnh SQL truy vấn

Graphical user interface, text, application

Description automatically generated

**Hình 2.25**

Ta thấy nhập “19” sẽ có lỗi vì vậy sẽ có 18 cột của table

Bước 4:

Tìm cột bị lỗi bằng cách sử dụng cậu lệnh “union select”

Graphical user interface, application

Description automatically generated

**Hình 2.26**

Ta thấy cột 3 bị lỗi

Bước 5:

Kiểm tra một số thông tin như version, user, database của cột 3

Graphical user interface, application

Description automatically generated

**Hình 2.27**

**Graphical user interface, application

Description automatically generated**

**Hình 2.28**

**Graphical user interface, application

Description automatically generated**

**Hình 2.29**

Bước 6:

Truy vấn các bảng trong database

Graphical user interface, application

Description automatically generated

**Hình 2.30**

Bước 7:

Liệt kê các cột trong bảng tbl\_user

Graphical user interface, text, application

Description automatically generated

**Hình 2.31**

Bước 8:

Xem thông tin các cột của bảng tbl\_user

Graphical user interface, text, application

Description automatically generated

**Hình 2.32**

Ta có thể giải mã md5 của cột pwd trên trang: <https://crackstation.net/>