THỰC HÀNH SQL INJECTION

Mục đích

- Biết cách khai thác lỗ hổng SQL injection.
- Biết cách phòng chống SQL injection.

Bài tập

- Bài tập 1: Sử dụng các từ khóa để tìm kiếm những trang website bị lỗi SQL injection.
- Bài tập 2: Khai thác lỗ hổng SQL injection trên website cục bộ www.computershop.com
- Bài tập 3: Khai thác lỗ hổng SQL injection trên website bên ngoài, lấy kết quả từ Bài tập 1.

Yêu cầu

Để có thể thực tập chúng ta cần 1 máy:

- Sử dụng phần mềm tạo máy ảo VMWARE hoặc Virtual PC để tạo 1 máy ảo.
- Một máy Windows XP hoặc Windows 7 Professional.

Nội dung

Bài tập 1: Sử dụng các từ khóa để tìm kiếm những trang website bị dính lỗi SQL injection.

Hacker lần lượt gõ vào các từ khoá bên dưới để tìm kiếm các trang web bị dính lỗi SQL injection.

inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

inurl:article.php?id=

inurl:show.php?id=

inurl:staff_id=

inurl:newsitem.php?num=

inurl:readnews.php?id=

inurl:top10.php?cat=

inurl:historialeer.php?num=

inurl:reagir.php?num=

inurl:Stray-Questions-View.php?num=

inurl:forum_bds.php?num=

inurl:game.php?id=

inurl:view_product.php?id=

inurl:newsone.php?id=

inurl:sw_comment.php?id=

inurl:news.php?id=

inurl:avd_start.php?avd=

inurl:event.php?id=

inurl:product-item.php?id=

inurl:sql.php?id=

inurl:news_view.php?id=

inurl:select_biblio.php?id=

inurl:humor.php?id=

inurl:aboutbook.php?id=

inurl:ogl_inet.php?ogl_id=

inurl:fiche_spectacle.php?id=

inurl:communique_detail.php?id=

inurl:sem.php3?id=

inurl:kategorie.php4?id=

inurl:news.php?id=

inurl:index.php?id=

inurl:faq2.php?id=

inurl:show_an.php?id=

inurl:preview.php?id=

inurl:loadpsb.php?id=

inurl:opinions.php?id=

inurl:spr.php?id=

inurl:pages.php?id=

inurl:announce.php?id=

inurl:clanek.php4?id=

inurl:participant.php?id=

inurl:download.php?id=

inurl:main.php?id=

inurl:review.php?id=

inurl:chappies.php?id=

inurl:read.php?id=

inurl:prod_detail.php?id=

inurl:viewphoto.php?id=

inurl:article.php?id=

inurl:person.php?id=

inurl:productinfo.php?id=

inurl:showimg.php?id=

inurl:view.php?id=

inurl:website.php?id=

inurl:hosting_info.php?id=

inurl:gallery.php?id=

inurl:rub.php?idr=

inurl:view_faq.php?id=

inurl:artikelinfo.php?id=

inurl:detail.php?ID=

inurl:index.php?=

inurl:profile_view.php?id=

inurl:category.php?id=

inurl:publications.php?id=

inurl:fellows.php?id=

inurl:downloads_info.php?id=

inurl:prod_info.php?id=

inurl:shop.php?do=
part&id=

inurl:productinfo.php?id=

inurl:collectionitem.php?id=

inurl:band_info.php?id=

inurl:product.php?id=

inurl:releases.php?id=

inurl:ray.php?id=

inurl:produit.php?id=

inurl:pop.php?id=

inurl:shopping.php?id=

inurl:productdetail.php?id=

inurl:post.php?id=

inurl:viewshowdetail.php?id=

inurl:clubpage.php?id=

inurl:memberInfo.php?id=

inurl:section.php?id=

inurl:theme.php?id=

inurl:page.php?id=

inurl:shredder-categories.php?id=

inurl:tradeCategory.php?id=

inurl:product_ranges_view.php?ID=

inurl:shop_category.php?id=

inurl:transcript.php?id=

inurl:channel_id=

inurl:item_id=

inurl:newsid=

inurl:trainers.php?id=

inurl:news-full.php?id=

inurl:news_display.php?getid=

inurl:index2.php?option=

inurl:readnews.php?id=

inurl:top10.php?cat=

inurl:newsone.php?id=

inurl:event.php?id=

inurl:product-item.php?id=

inurl:sql.php?id=

inurl:aboutbook.php?id=

inurl:preview.php?id=

inurl:loadpsb.php?id=

inurl:pages.php?id=

inurl:material.php?id=

inurl:clanek.php4?id=

inurl:announce.php?id=

inurl:chappies.php?id=

inurl:read.php?id=

inurl:viewapp.php?id=

inurl:viewphoto.php?id=

inurl:rub.php?idr=

inurl:galeri_info.php?l=

inurl:review.php?id=

inurl:iniziativa.php?in=

inurl:curriculum.php?id=

inurl:labels.php?id=

inurl:story.php?id=

inurl:look.php?ID=

inurl:newsone.php?id=

inurl:aboutbook.php?id=

inurl:material.php?id=

inurl:opinions.php?id=

inurl:announce.php?id=

inurl:rub.php?idr=

inurl:galeri_info.php?l=

inurl:tekst.php?idt=

inurl:newscat.php?id=

inurl:newsticker_info.php?idn=

inurl:rubrika.php?idr=

inurl:rubp.php?idr=

inurl:offer.php?idf=

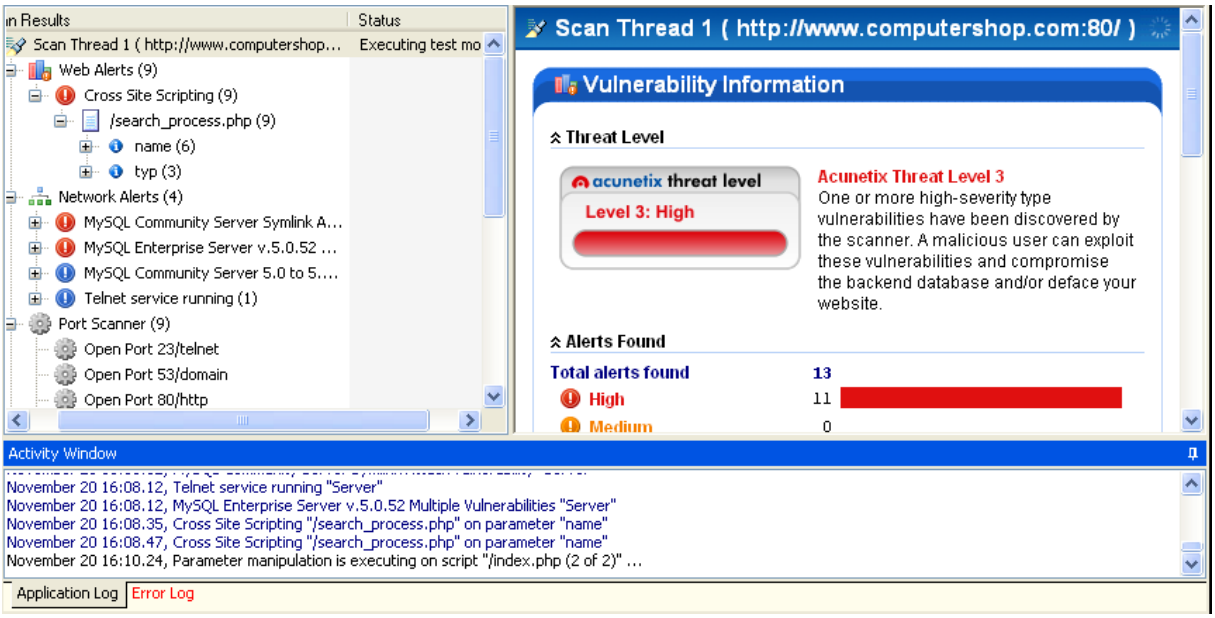
inurl:art.php?idm=

inurl:title.php?id=

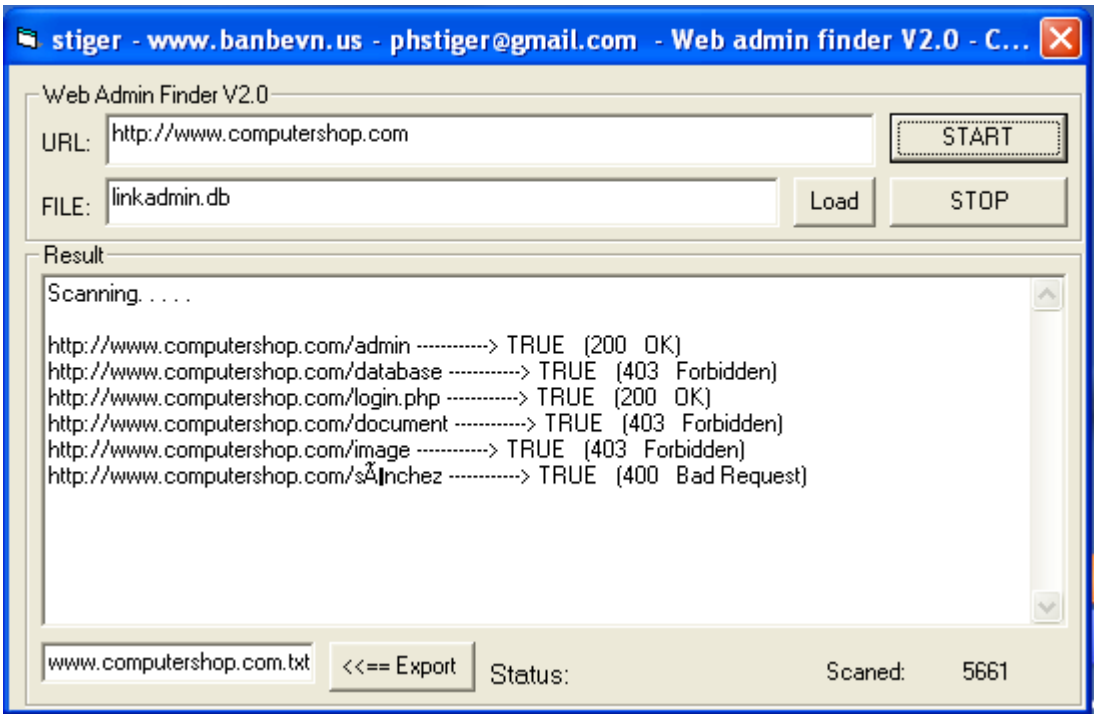
Bài tập 2: Khai thác lỗ hỏng SQL injection của website **www.computershop.com**

1. Cách tấn công

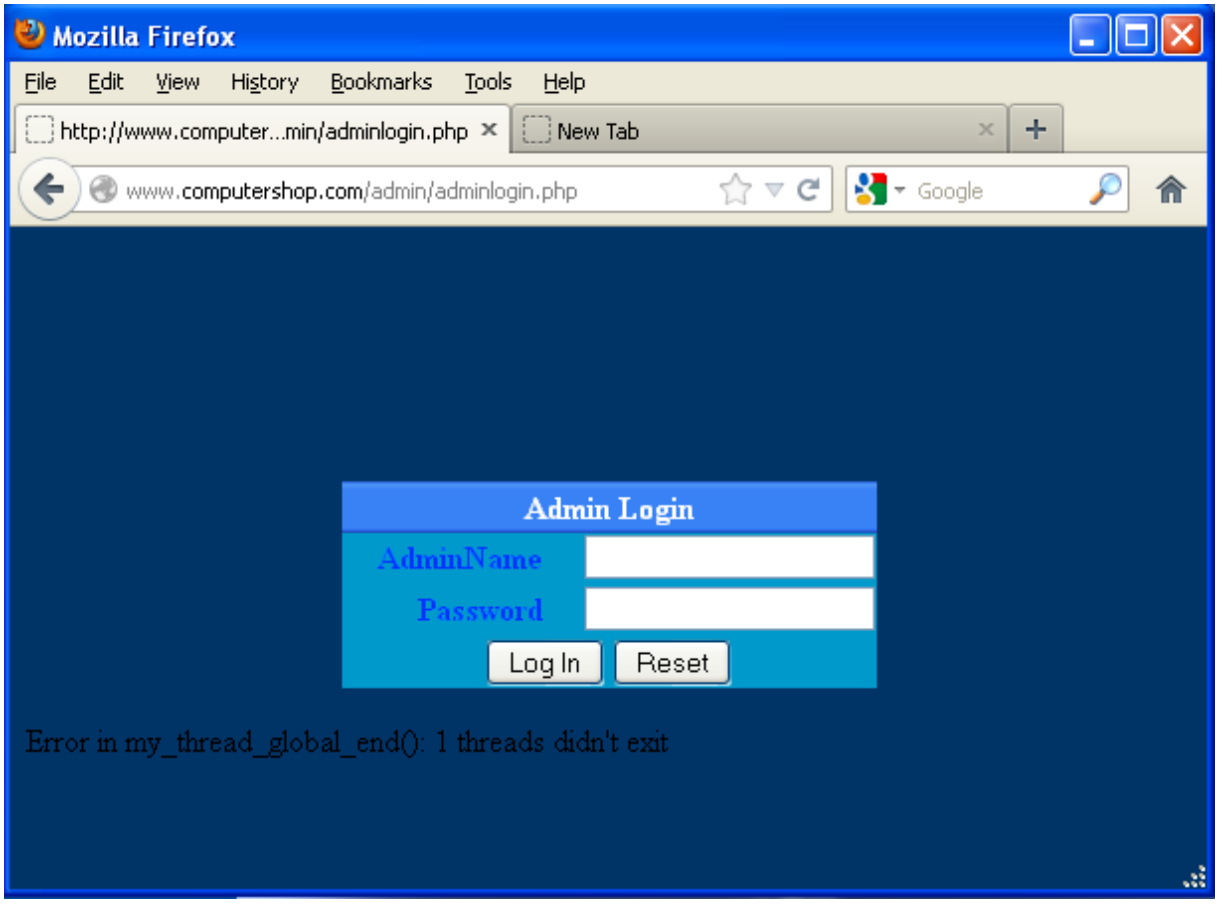
Bước 1: Sử dụng công cụ "Acunetix Web Vulnerability Scanner" để quét lỗi cho website.



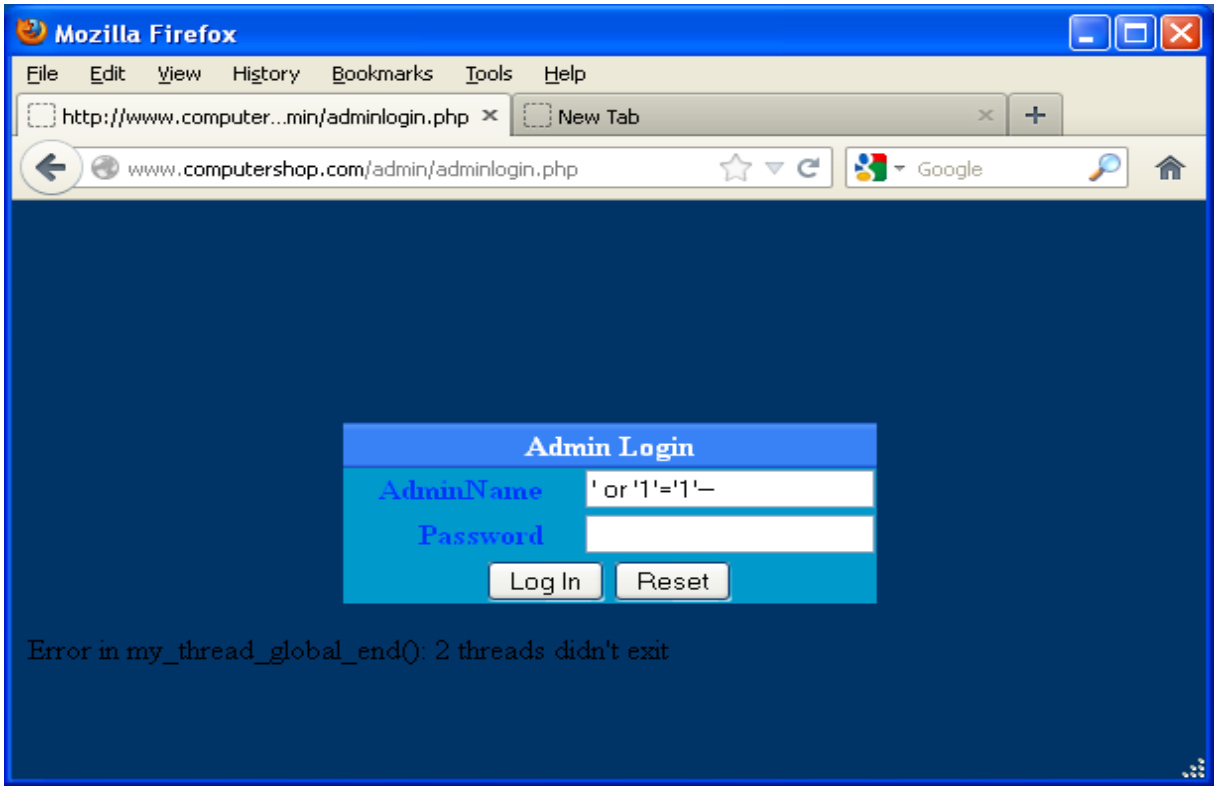
Bước 2: Tìm kiếm trang đăng nhập quản trị bằng công cụ Web Admin Finder V2.0.exe. Nhập địa chỉ website vào mục URL và click chọn Start.



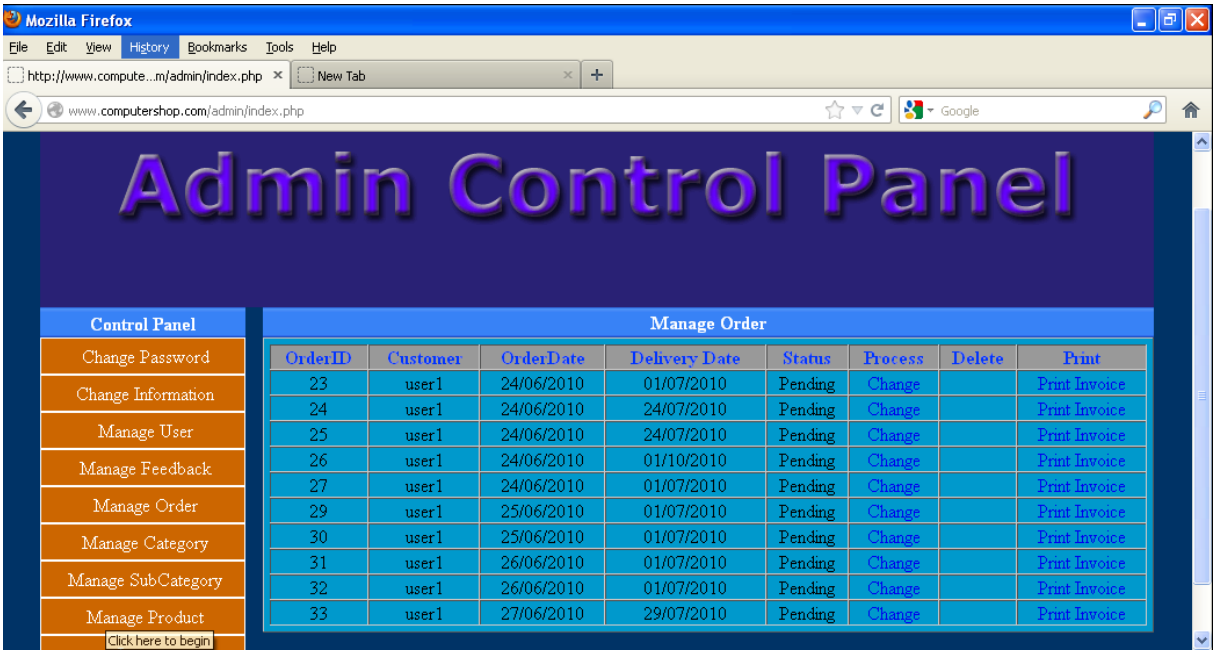
Bước 3: Sau khi đã phát hiện ra mục quản trị của website, tiến hành tấn công.



Bước 4: Nhập vào từ khóa ' or '1'='1' -- trong trường AdminName và chọn Log In.



Bước 5: Đăng nhập vào trang quản trị thành công.



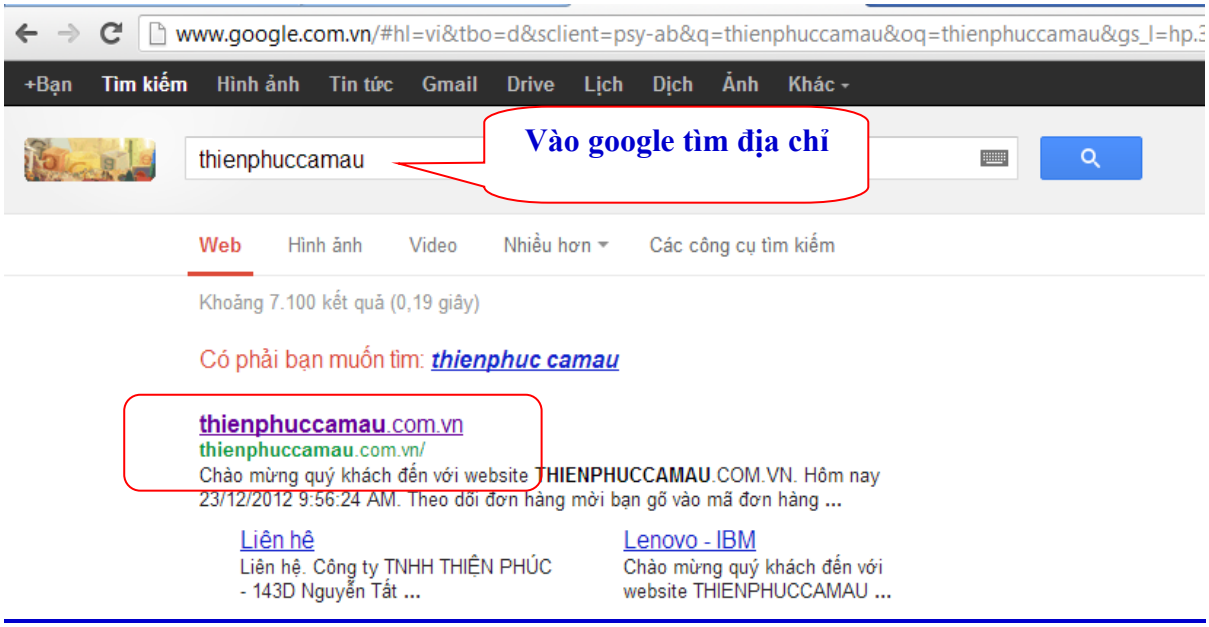
2. **Cách phòng chống:** viết hàm kiểm tra dữ liệu đầu vào cho form đăng nhập trên.

```
function checklogin()
    {
            var result= 0;
            //Check Username
            var name = /^[a-zA-Z]\w*$/;
            if(login.an.value=="")
            {
                    document.getElementById('man').innerHTML = wrong;
                    document.getElementById('can').innerHTML = blank;
            }
            else if(name.test(login.an.value)==true)
            {
                    document.getElementById('man').innerHTML = right;
                    document.getElementById('can').innerHTML = "";
                    result= result+1;
            }
            else
            {
                    document.getElementById('man').innerHTML = wrong;
                    document.getElementById('can').innerHTML = " <font
color='#FF0000'>Username is invalid</font>";
            }

            //Check Password
            if(login.pw.value=="")
            {
                    document.getElementById('mpw').innerHTML = wrong;
                    document.getElementById('cpw').innerHTML = blank;
            }
            else if(login.pw.value.length>=4 && login.pw.value.length<=20)
            {
                    document.getElementById('mpw').innerHTML = right;
                    document.getElementById('cpw').innerHTML = "";
                    result= result+1;
            }
            else
            {
                    document.getElementById('mpw').innerHTML = wrong;
                    document.getElementById('cpw').innerHTML = " <font
color='#FF0000'>Password must be from 4 to 20 letters</font>";
            }

            //Check Submit
            if(result== 2)
```

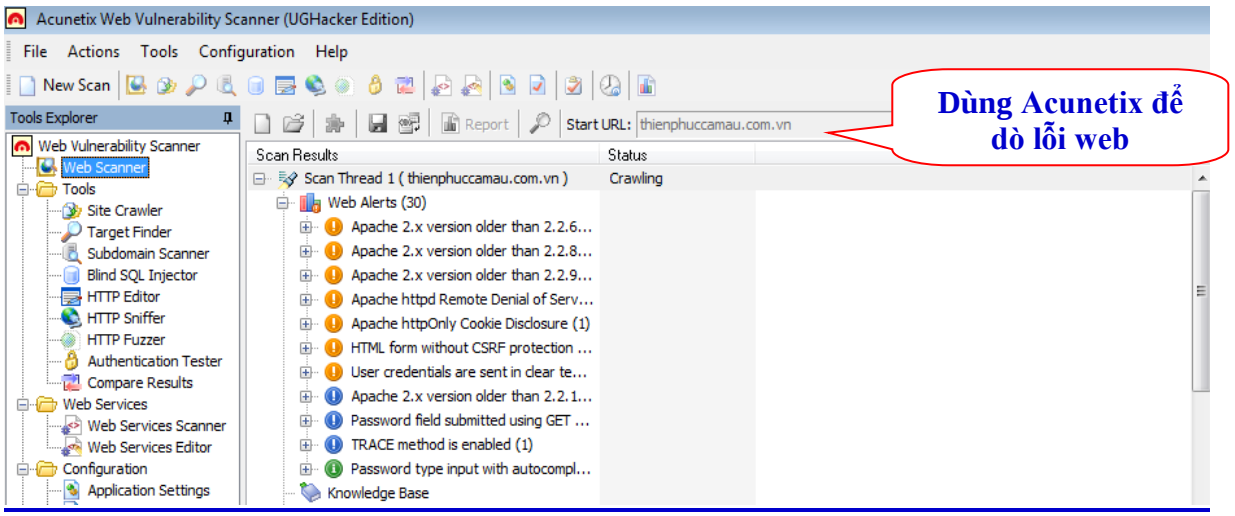
```
            {
                return true;
            }
            else
            {
                return false;
            }
    }
</script>
```

Bài tập 3: Khai thác lỗi SQL injection bên ngoài **http://thienphuccamau.com.vn**

Bước 1: vào google tìm địa chỉ **thienphuccamau.com.vn**

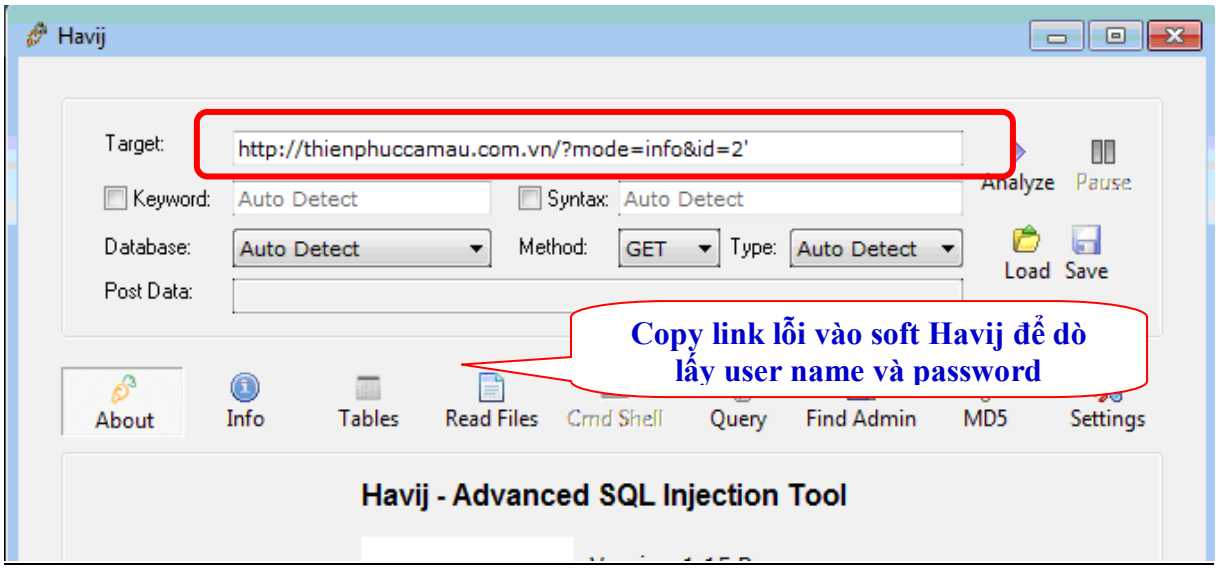


Bước 2: tìm kiếm lỗ hổng bảo mật trên website **thienphucamau.com.vn**

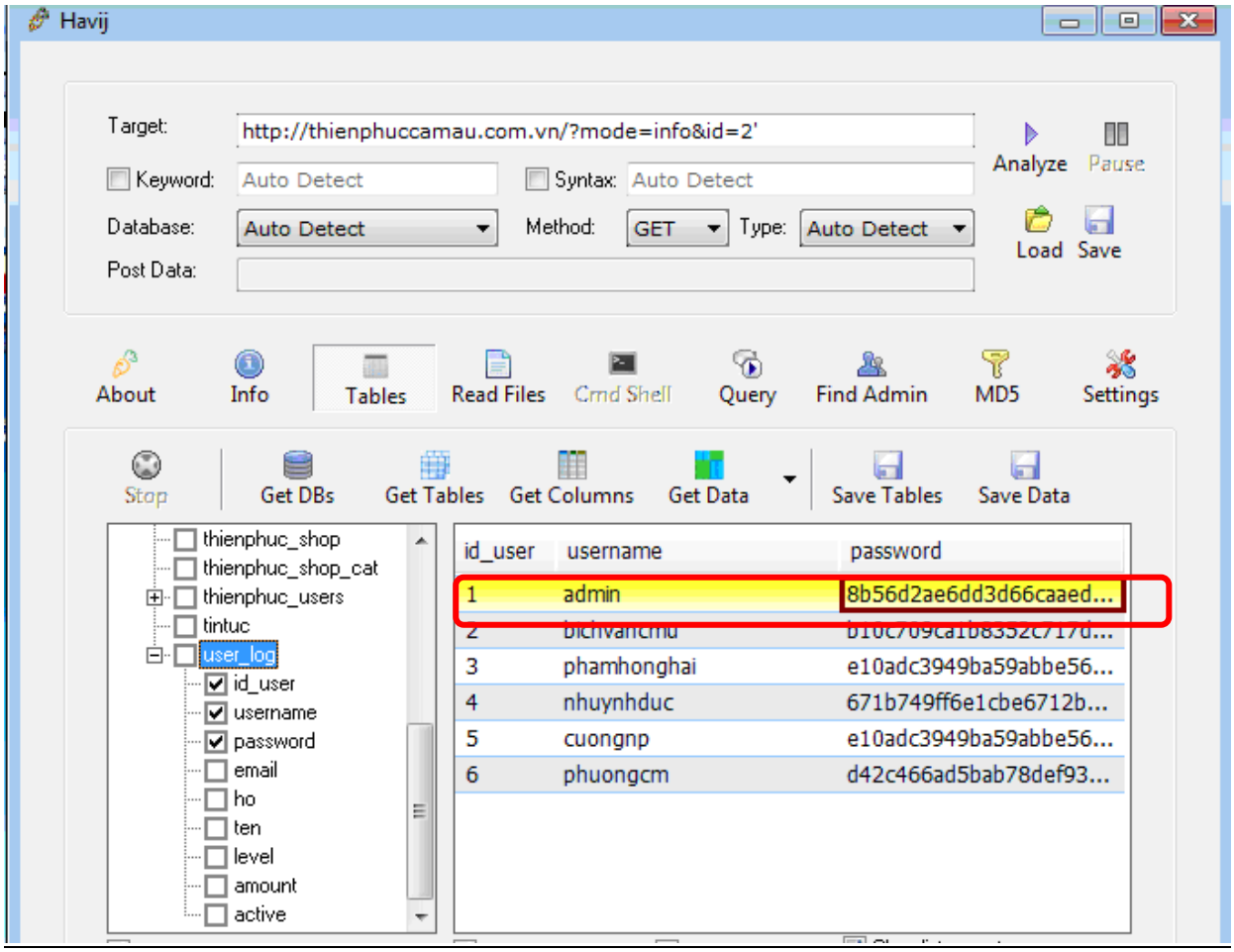


Bước 3: thêm dấu " ' " vào phần sau của bản tin.

Bước 4: copy địa chỉ bỏ vào phần Target của phần mềm **Havij.**

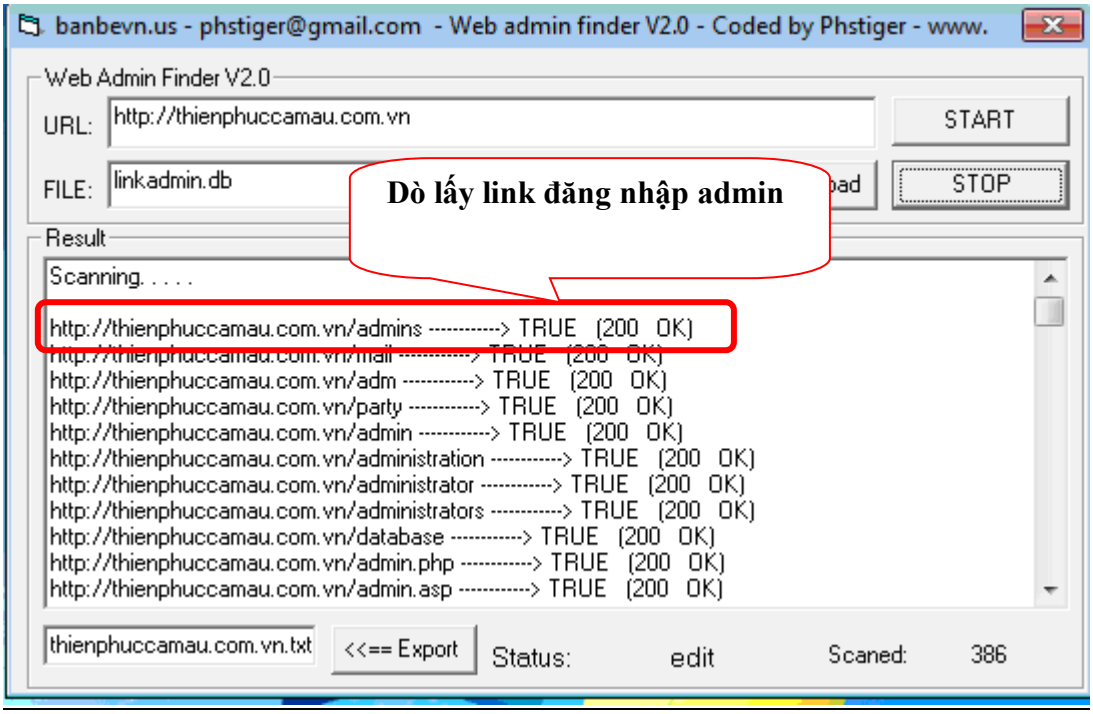


Bước 5: Chọn Get DBs -> Tables -> User_log

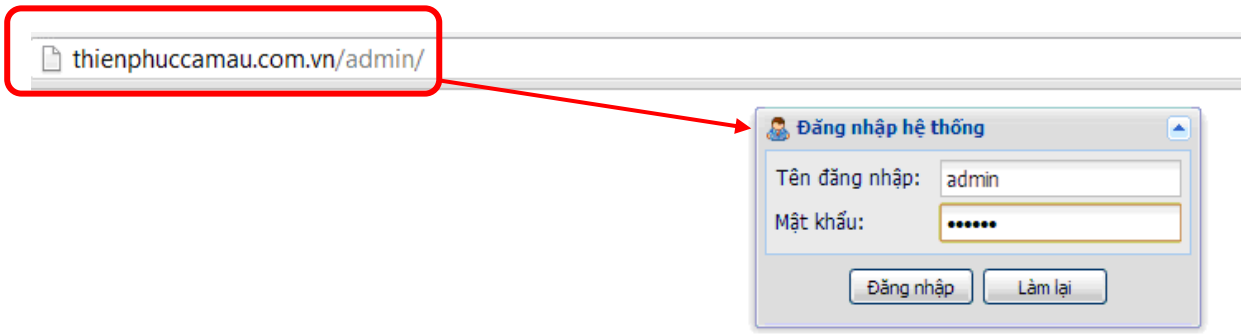


Bước 6: vào địa chỉ MD5Decrypter.co.uk để giải mã mật khẩu.

Bước 7: sử dụng phần mềm Web Admin Finder tìm trang quản trị của thienphuccamau.com.vn



Bước 8: đăng nhập vào trang quản trị.



Bước 9: Vào được trang quản trị.