TP-Link TL-W841N has xss vulnerability

Vulnerability Description

Vulnerability: Router backend management page xss injection vulnerability

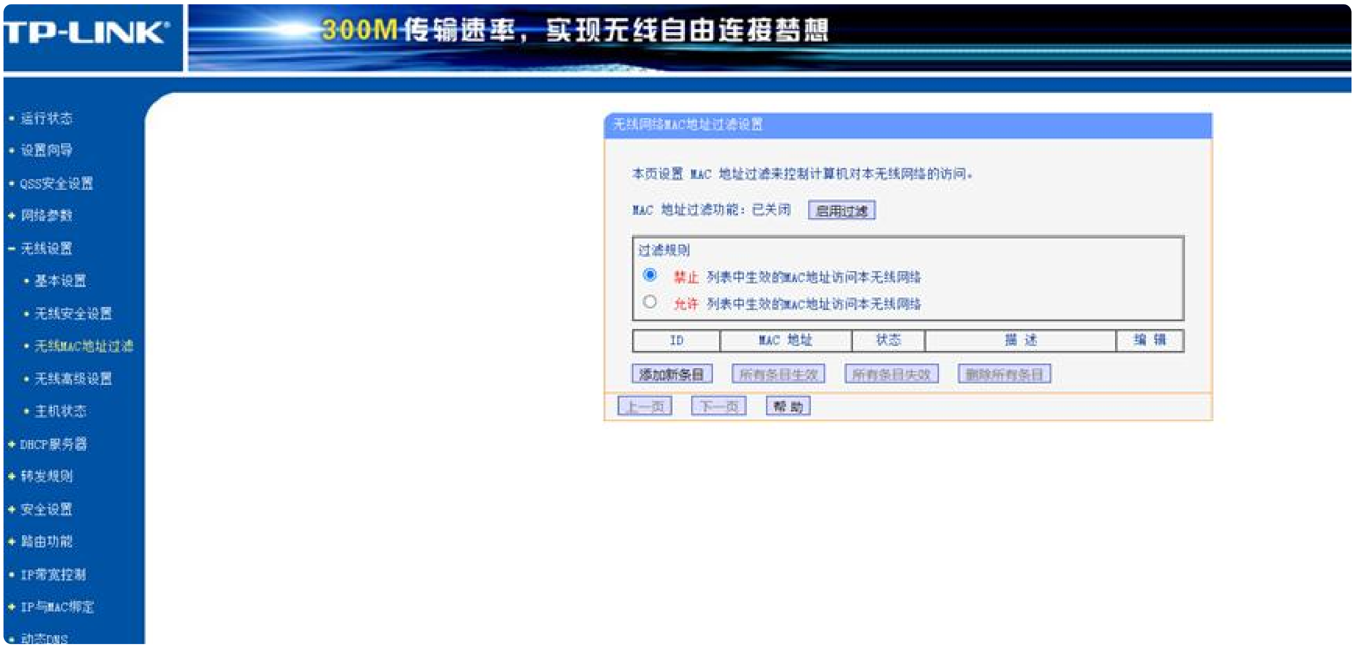
Affected hardware: TP-Link TL-WR841N 8.0

Affected version: 4.17.16 Build 120201 Rel.54750n

This vulnerability is due to the front-end not filtering special characters.

Vulnerability recurrence

After entering the backend (default password), add a new entry in Settings Wireless Settings - Wireless MAC Address Filtering.



本页设置 MAC 地址过滤来控制计算机对本无线网络的访问。

MAC 地址过滤功能：已关闭

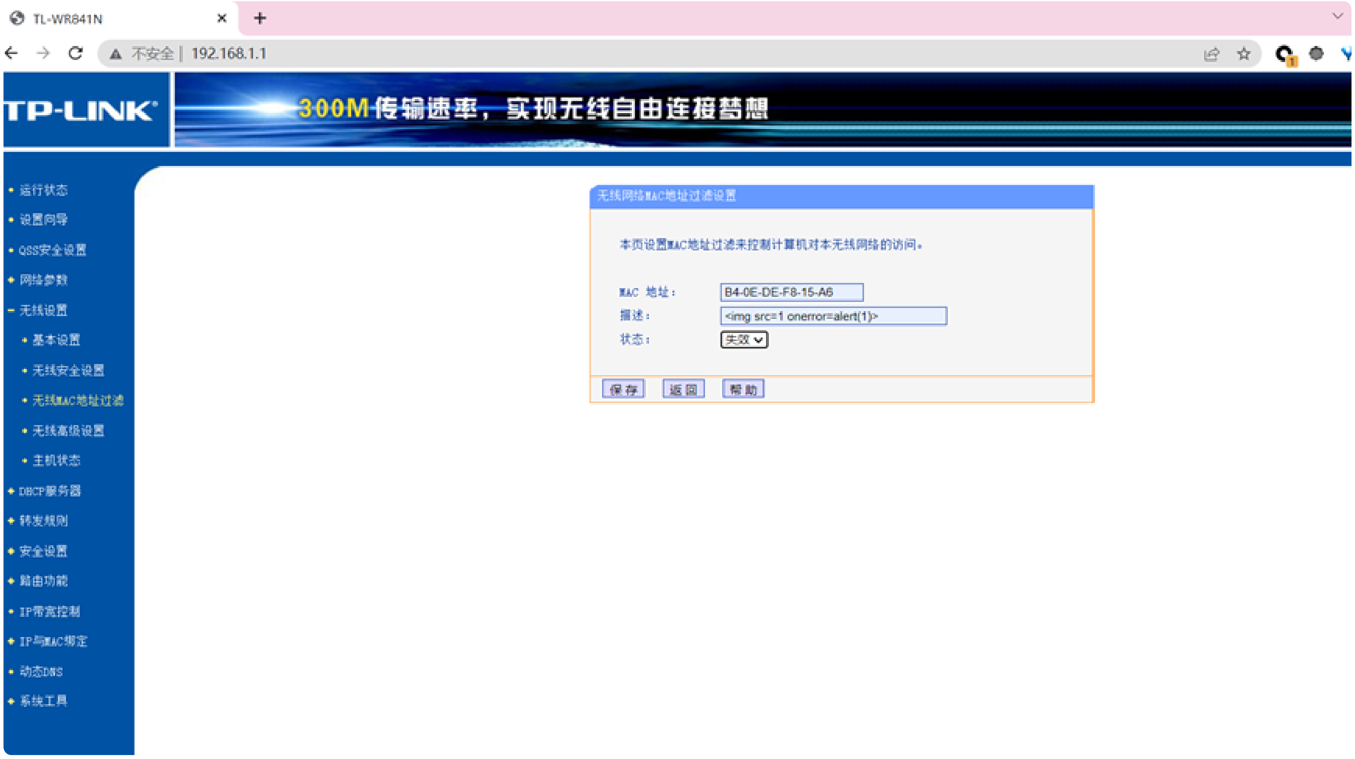
过滤规则

● 禁止 列表中生效的MAC地址访问本无线网络

○ 允许 列表中生效的MAC地址访问本无线网络

ID	MAC 地址	状态	描 述	编 辑

Then enter poc.



无线网络MAC地址过滤设置

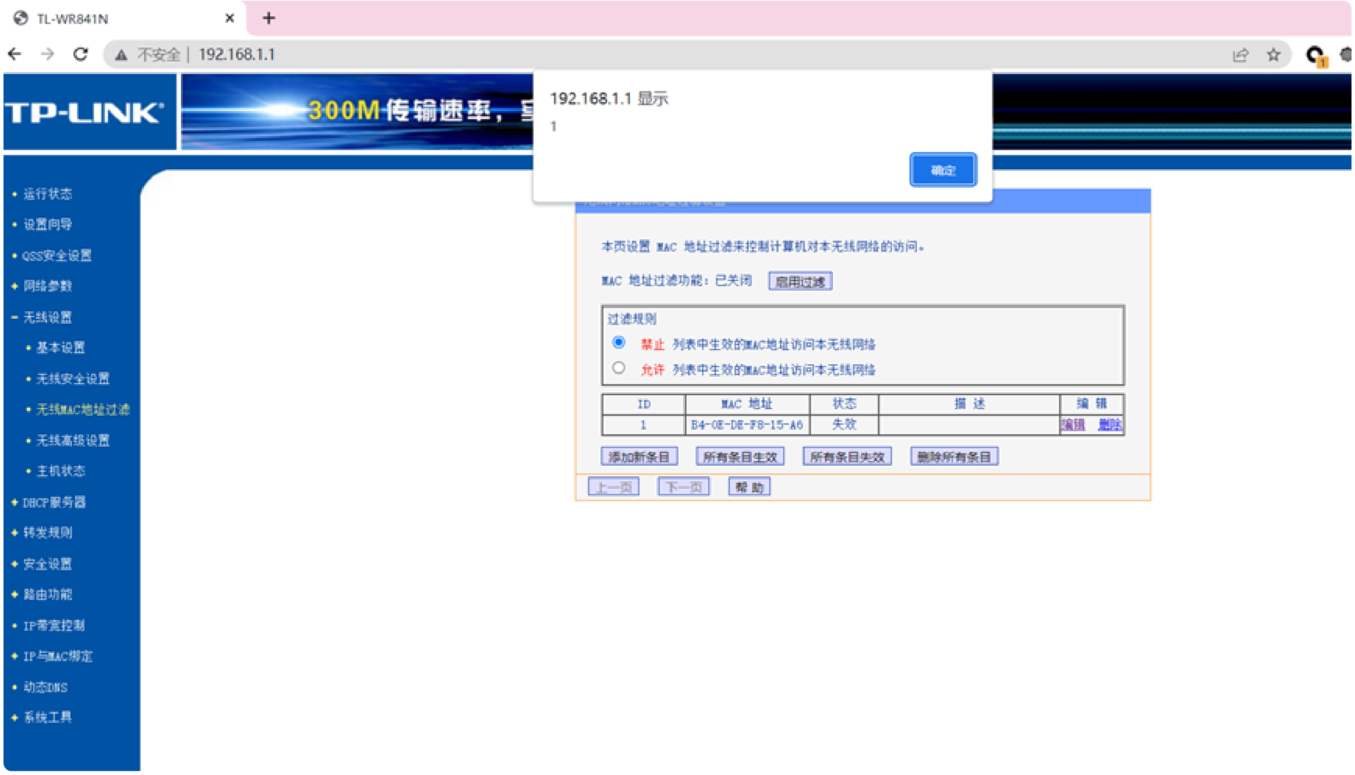
本页设置MAC地址过滤来控制计算机对本无线网络的访问。

MAC 地址： B4-0E-DE-F8-15-A6

描述： <img src=1 onerror=alert(1)>

状态： 失效

Save and rewind to the previous page, every user who enters that page in the backend will trigger the xss vulnerability.



192.168.1.1 显示

1

本页设置 MAC 地址过滤来控制计算机对本无线网络的访问。

MAC 地址过滤功能：已关闭

过滤规则

● 禁止 列表中生效的MAC地址访问本无线网络

○ 允许 列表中生效的MAC地址访问本无线网络

ID	MAC 地址	状态	描 述	编 辑
1	B4-0E-DE-F8-15-A6	失效		编辑 删除

Poc：

<img src=1 onerror=alert(1)>

Principle of the vulnerability

When typing '<script>alert(1);</script>' the source code can be found as

```
<script language="javascript" type="text/javascript">
var wlanFilterList = new Array(
"B4-0E-DE-F8-15-A6",1,1,"","<script>alert(1);</script>
</head>
<body>
",
0,0 );
```

The code directly transfers the input to js to process and print to the page resulting in xss.

Suggestions for fixing

Filter malicious characters