http://127.0.0.1存在文件上传测试漏洞

# 漏洞地址

http://127.0.0.1

# 漏洞详情

一共1组payload

## 第1组payload共发送2次请求

### **发送第1次请求:**

**请求数据包**

**POST /vulnerabilities/upload/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Host: 127.0.0.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarynuE9llij1hTVvCxk
Content-Length: 307
Cookie: PHPSESSID=unovse4qudsgfmtqvmkpggvppd; security=low
------WebKitFormBoundarynuE9llij1hTVvCxk
Content-Disposition: form-data; name="uploaded"; filename="t.PNG"
Content-Type: image/png
�PNG
12312312312312312312312312312
------WebKitFormBoundarynuE9llij1hTVvCxk
Content-Disposition: form-data; name="Upload"
Upload
------WebKitFormBoundarynuE9llij1hTVvCxk--**

**请求响应包**

**HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Fri, 10 Mar 2023 14:53:51 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 4141
Connection: keep-alive
X-Powered-By: PHP/7.3.4
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
<!DOCTYPE html>
<html lang="en-GB">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Vulnerability: File Upload :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</title>
<link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
<link rel="icon" type="\image/ico" href="../../favicon.ico" />
<script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>
</head>
<body class="home">
<div id="container">
<div id="header">
<img src="../../dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />
</div>
<div id="main\_menu">
<div id="main\_menu\_padded">
<ul class="menuBlocks"><li class=""><a href="../../.">Home</a></li>
<li class=""><a href="../../instructions.php">Instructions</a></li>
<li class=""><a href="../../setup.php">Setup / Reset DB</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../vulnerabilities/brute/">Brute Force</a></li>
<li class=""><a href="../../vulnerabilities/exec/">Command Injection</a></li>
<li class=""><a href="../../vulnerabilities/csrf/">CSRF</a></li>
<li class=""><a href="../../vulnerabilities/fi/.?page=include.php">File Inclusion</a></li>
<li class="selected"><a href="../../vulnerabilities/upload/">File Upload</a></li>
<li class=""><a href="../../vulnerabilities/captcha/">Insecure CAPTCHA</a></li>
<li class=""><a href="../../vulnerabilities/sqli/">SQL Injection</a></li>
<li class=""><a href="../../vulnerabilities/sqli\_blind/">SQL Injection (Blind)</a></li>
<li class=""><a href="../../vulnerabilities/weak\_id/">Weak Session IDs</a></li>
<li class=""><a href="../../vulnerabilities/xss\_d/">XSS (DOM)</a></li>
<li class=""><a href="../../vulnerabilities/xss\_r/">XSS (Reflected)</a></li>
<li class=""><a href="../../vulnerabilities/xss\_s/">XSS (Stored)</a></li>
<li class=""><a href="../../vulnerabilities/csp/">CSP Bypass</a></li>
<li class=""><a href="../../vulnerabilities/javascript/">JavaScript</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../security.php">DVWA Security</a></li>
<li class=""><a href="../../phpinfo.php">PHP Info</a></li>
<li class=""><a href="../../about.php">About</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="../../logout.php">Logout</a></li>
</ul>
</div>
</div>
<div id="main\_body">
<div class="body\_padded">
<h1>Vulnerability: File Upload</h1>
<div class="vulnerable\_code\_area">
<form enctype="multipart/form-data" action="#" method="POST">
<input type="hidden" name="MAX\_FILE\_SIZE" value="100000" />
Choose an image to upload:<br /><br />
<input name="uploaded" type="file" /><br />
<br />
<input type="submit" name="Upload" value="Upload" />
</form>
<pre>../../hackable/uploads/t.PNG succesfully uploaded!</pre>
</div>
<h2>More Information</h2>
<ul>
<li><a href="https://www.owasp.org/index.php/Unrestricted\_File\_Upload" target="\_blank">https://www.owasp.org/index.php/Unrestricted\_File\_Upload</a></li>
<li><a href="https://blogs.securiteam.com/index.php/archives/1268" target="\_blank">https://blogs.securiteam.com/index.php/archives/1268</a></li>
<li><a href="https://www.acunetix.com/websitesecurity/upload-forms-threat/" target="\_blank">https://www.acunetix.com/websitesecurity/upload-forms-threat/</a></li>
</ul>
</div>
<br /><br />
</div>
<div class="clear">
</div>
<div id="system\_info">
<input type="button" value="View Help" class="popup\_button" id='help\_button' data-help-url='../../vulnerabilities/view\_help.php?id=upload&security=low' )"> <input type="button" value="View Source" class="popup\_button" id='source\_button' data-source-url='../../vulnerabilities/view\_source.php?id=upload&security=low' )"> <div align="left"><em>Username:</em> admin<br /><em>Security Level:</em> low<br /><em>PHPIDS:</em> disabled</div>
</div>
<div id="footer">
<p>Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</p>
<script src='../..//dvwa/js/add\_event\_listeners.js'></script>
</div>
</div>
</body>
</html>**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**

### **发送第2次请求:**

**请求数据包**

**GET /hackable/uploads/t.PNG HTTP/1.1
User-Agent: fasthttp
Host: 127.0.0.1**

**请求响应包**

**HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Fri, 10 Mar 2023 14:53:51 GMT
Content-Type: image/png
Content-Length: 36
Last-Modified: Fri, 10 Mar 2023 14:53:51 GMT
Connection: keep-alive
Etag: "640b447f-24"
Accept-Ranges: bytes
�PNG
12312312312312312312312312312**

**漏洞存在判断条件**

**response.status == 200**

**结果：**

**存在漏洞**