<https://www.ehacking.net/2011/09>

use the Google docks search for the sites which as the index of/root folder by

allintitle: ”index of/root” passwd

allintitle: ”index of/root”

can also search for

inurl: admin

inurl: cgi

filetype: pdf

“auth\_user\_file.txt”

Index of ftp + .mdb allinurl:/cgi-bin/+mailto

Consider a url

<https://mis-security.com/file.jsp?file=report>.txt

the attacker can modify the parameters as

[https://mis-security.com/file,jsp?file=\*\*../../../etc/shadow\*\*](https://mis-security.com/file,jsp?file=**../../../etc/shadow**)

example:

<https://tic.com/customers/view/2145882>

tic.com/customers/viewdetails.aspx?ID=2145555445

Change to

Tic.com/customers/update/2145882

tic.com/customers/modify.aspx?ID=2145555445

tic.com/customers/admin

prevention?

validate user input

check the access rights

use the reference map rather than real values