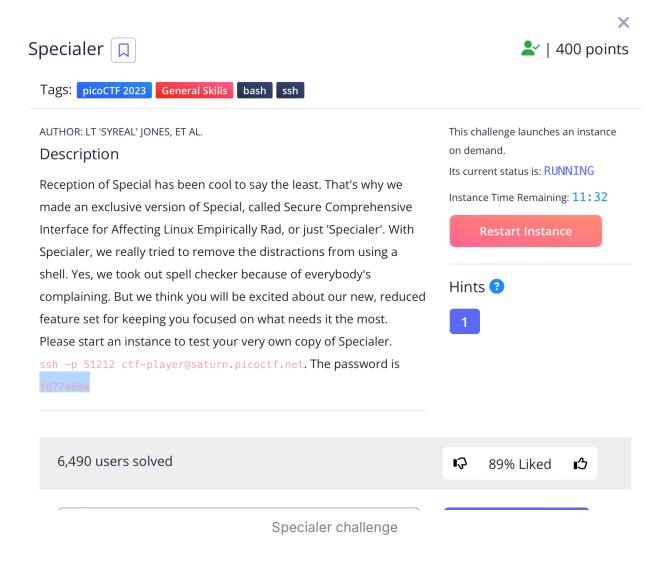
Specialer



Here we got a shell that uses only certain commands

Specialer 1

```
Specialer$ ls
-bash: ls: command not found
Specialer$
                                   fc
           caller
                       do
                                              kill
                                                          return
                                                                      true
           case
                       done
                                   fg
                                              let
                                                          select
                                                                      type
           cd
                       echo
                                   fi
                                              local
                                                          set
                                                                      typeset
                                   for
                                                          shift
                                                                      ulimit
           command
                       elif
                                              logout
                                              mapfile
           compgen
                       else
                                   function
                                                          shopt
                                                                      umask
                                                                      unalias
           complete
                       enable
                                   getopts
                                              popd
                                                          source
                                              printf
alias
           compopt
                                   hash
                                                          suspend
                                                                      unset
                       esac
bash
           continue
                       eval
                                   help
                                              pushd
                                                          test
                                                                      until
                                   history
                                              pwd
                                                          then
                                                                      wait
bg
           coproc
                       exec
bind
           declare
                                   if
                                                          time
                                                                      while
                       exit
                                              read
break
                                   in
                                                          times
           dirs
                       export
                                              readarray
builtin
                                                                      }
           disown
                       false
                                   jobs
                                              readonly
                                                          trap
Specialer$
```

Another thing we can see here is that to get a flag inside this shell we can rely on a few things:

- echo there is a format to print the contents of a file
- cd move to each directory
- (tabs) by pressing tabs to complete commands like cd we can see all the existing list of directories

Specialer 2

```
nutan — ssh -p 51212 ctf-player@saturn.picoctf.net — 80×24
                  ~/Downloads/nutan — ssh -p 51212 ctf-player@saturn.picoctf.net
Specialer$ echo "$(<cadabra.txt)"
Nothing up my sleeve!
Specialer$ echo cada
cadabra.txt cadaniel.txt
Specialer$ echo cada
cadabra.txt cadaniel.txt
Specialer$ echo "$(<cadaniel.txt)"
Yes, I did it! I really did it! I'm a true wizard!
Specialer$ cd ..
Specialer$ cd
.hushlogin .profile abra/ ala/
                                                 sim/
Specialer$ cd ala
Specialer$ ls
bash: ls: command not found
Specialer$ echo
kazam.txt mode.txt
Specialer$ echo
kazam.txt mode.txt
Specialer$ echo "$(<kazim.txt)"
bash: kazim.txt: No such file or directory
Specialer$ echo "$(<kazam.txt)"
return 0 picoCTF{y0u_d0n7_4ppr3c1473_wh47_w3r3_d01ng_h3r3_38f5cc78}
Specialer$
```

Specialer 3