



Dash - bash_hacker

bash_hacker

Summary: this document is the subject for the dash @ 42Tokyo.

Contents

I	Foreword	2
II	Objective	3
III	Instructions	4
IV	Exercice 00 : bash_hacker	5

Chapter I

Foreword

Learn the vulnerabilites of unquoted variables in shell scripts...
And how to exploit them!

Chapter II

Objective

Bypass a script's security to recover the validation password.


Chapter III

Instructions

- This dash is a solo project.
- Turn in your file inside the turn-in repository.

Chapter IV

Exercise 00 : bash_hacker

	Exercise 00
	bash_hacker
	Turn-in directory : <i>ex00/</i>
	Files to turn in : bash_hacker.txt
	Allowed functions : None

- Navigate to the `/usr/bin/dash17/` directory.
- Find a way around the script's security and output the password in the `.passwd` file.
- Submit the password in your repository in `bash_hacker.txt`.
- Here's what the script looks like:

```
$>cat dash17.sh
#!/bin/bash

PATH=$(/usr/bin/getconf PATH || /bin/kill $$)

PASS=$(cat .passwd)

if test -z "${1}"; then
    echo "USAGE : $0 [password]"
    exit 1
fi

if test $PASS -eq ${1} 2>/dev/null; then
    echo "Well done you can validate the challenge with : $PASS"
else
    echo "Try again ,-)"
fi

exit 0
```



Always quote your variables ;)