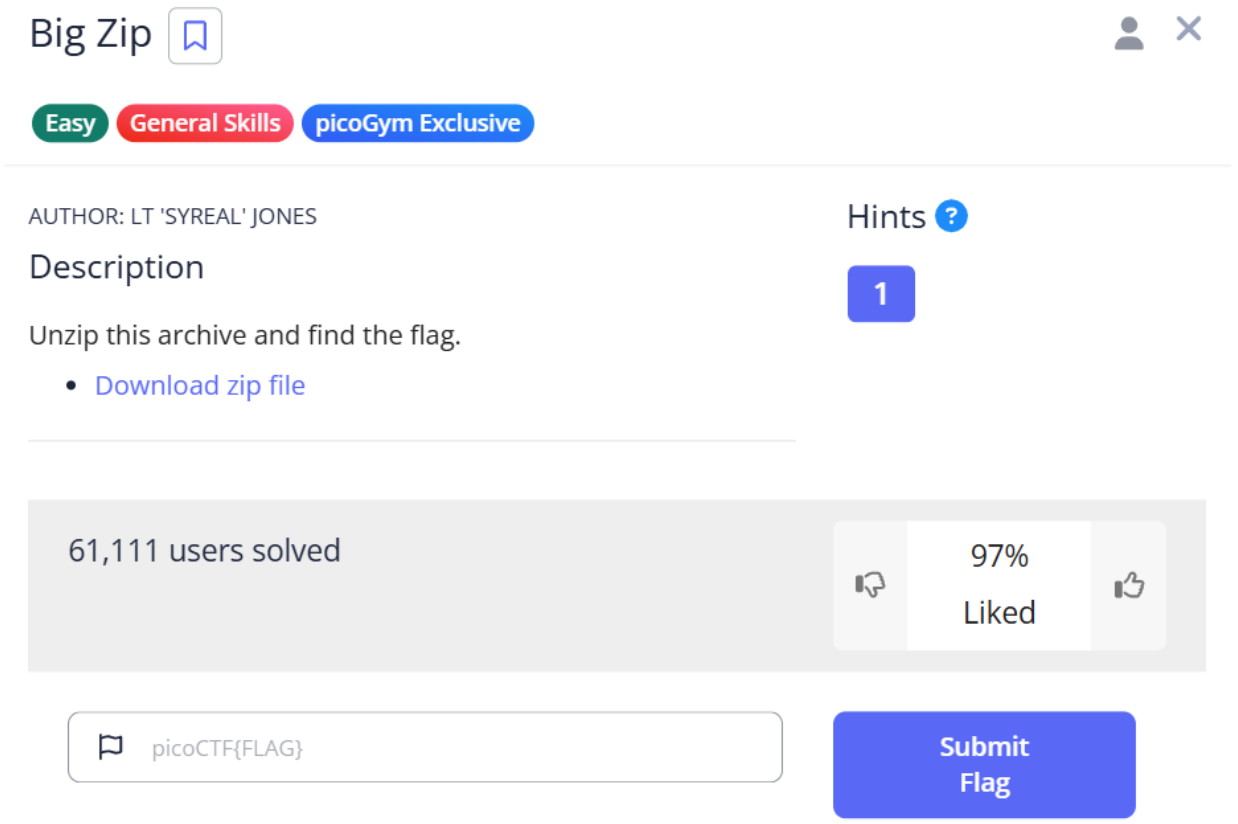
Big Zip



Author: The Analyst: Hyposelenia

Challenge: Big Zip

Category: General Skills

Date: 01/14/26

I. Objective

The objective of this task was to locate and extract a hidden picoCTF flag from a very large ZIP archive containing numerous directories and subdirectories.

II. Background

In Linux-based systems and Capture The Flag (CTF) challenges, flags are often hidden inside files within deeply nested directory structures. Manually opening each directory and file is inefficient and impractical, especially when dealing with large archives. Command-line text searching tools such as grep allow analysts to efficiently search for specific patterns across multiple files and directories.

III. Tool Used

- **Oracle VirtualBox (Kali Linux)** – Used as the Linux environment
- **Linux Terminal** – Used to execute decoding commands
- **unzip** – Used to extract the compressed archive
- **grep** – Used to search recursively for the flag pattern

IV. Methodology

1. Launched Kali Linux using Oracle VirtualBox
   (picoCTF WebShell can also be used as an alternative)
2. Extracted the provided ZIP file using: **unzip <Filename>**

```
┌──(kali㉿kali)-[/media/sf_Downloaded_Cybersecfiles]
└─$ unzip big-zip-files.zip
Archive:  big-zip-files.zip
   creating: big-zip-files/
 extracting: big-zip-files/jpvaawkrpno.txt
  inflating: big-zip-files/oxbcyjsy.txt
  inflating: big-zip-files/hllhxlvvdgiii.txt
  inflating: big-zip-files/bdvnqbuutefealgveyiqd.txt
  inflating: big-zip-files/fudfsewmaafsbniiyktzr.txt
   creating: big-zip-files/folder_fqmjtuthge/
  inflating: big-zip-files/folder_fqmjtuthge/file_eaigogtrdslbxenbnfisxepj.txt
  inflating: big-zip-files/folder_fqmjtuthge/file_ygocxgpzuxqjwfs.txt
  inflating: big-zip-files/folder_fqmjtuthge/file_lqqprxhjtarithwygepdnlf.txt
```

3. Since the archive contained many directories and subdirectories, a recursive search was required. The `grep` command was used to search for the picoCTF flag format: **grep -r picoCTF**

```
┌──(kali㉿kali)-[/media/sf_Downloaded_Cybersecfiles/big-zip-files]
└─$ grep -r picoCTF
folder_pmbymkjcya/folder_cawigcwvgv/folder_ltdayfmktr/folder_fnpfclfyee/whzxrpivpqld.txt:information on t
```

4. The command searched through all files recursively and displayed the line containing the flag along with its file location.

V. Result

picoCTF{gr3p_15_m4g1c_ef8790dc}

```
Genes and brains and books encode picoCTF{gr3p_15_m4g1c_ef8790dc}
```

VI. Explanation

"Why regular grep or strings was not sufficient?"

- Using "**grep picoCTF filename"** only searches **one file at a time**, which is impractical for large directory structures.
- Using **"strings file | grep picoCTF"** works only when you already know **which file** contains the data and is mainly used for binary analysis.
- In this challenge, the flag was buried across **many directories and files**, making manual file inspection inefficient.

Purpose of grep -r:

The -r (recursive) option tells grep to:

- Search **all files**
- Traverse **all subdirectories automatically**
- Locate matching text without manually specifying each file

grep -r picoCTF

This makes it ideal for large-scale searches in CTF challenges involving complex directory structures.

Other useful grep options for CTFs

Command	Purpose
grep -i	Case-insensitive search
grep -n	Shows line numbers
grep -o	Prints only the matching text
grep -h	Suppresses filenames
grep -R	Recursive search (same as -r)
grep -Roh "picoCTF{[^}]*}" .	Extracts only the full flag

Example (advanced flag extraction):

grep -Roh "picoCTF{[^}]*}" .

This outputs **only the flag**, ignoring directory paths and extra text.

VII. Conclusion

This challenge demonstrated the importance of recursive searching when working with large filesystems. By using grep -r, the flag was efficiently located without manually navigating directories. Mastery of tools like grep significantly improves speed and effectiveness in Linux-based CTF challenges.

— **The Analyst: Hyposelenia**