



phpbash / README.md

 paralex spelling fix, no content changes003ce03 · 6 years ago 

28 lines (22 loc) · 1.27 KB

Preview Code Blame

Raw     

# phpbash

phpbash is a standalone, semi-interactive web shell. It's main purpose is to assist in penetration tests where traditional reverse shells are not possible. The design is based on the default Kali Linux terminal colors, so pentesters should feel right at home.

## Requirements

Javascript must be enabled on the client browser for phpbash to work properly. The target machine must also allow execution of the `shell_exec` PHP function, although it is very simple to modify the script to use an alternate function.

## Features

- Requires only a single PHP file
- POST-based requests
- Support for current working directory
- Command history with arrow keys
- Upload files directly to target directory

Have a feature idea? Open an [Issue](#).

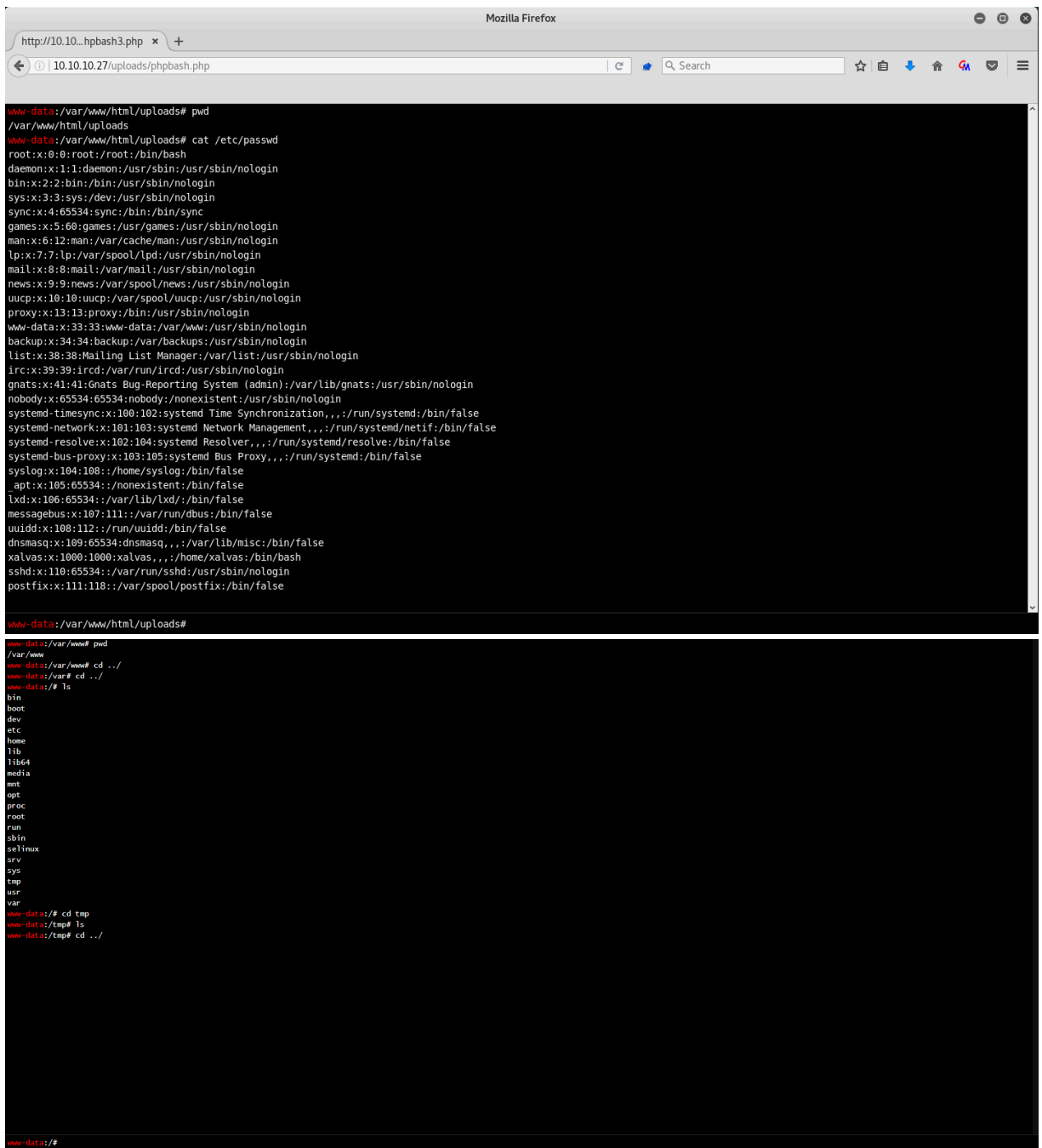
## Custom Commands

- `cd` Return to default shell directory
- `cd <path>` Change directory
- `cd -` Return to previous directory
- `clear` Clears all output
- `upload` Opens the file browser and uploads selected file

## Usage

Simply drop the `phpbash.php` or `phpbash.min.php` file on the target and access it with any Javascript-enabled web browser.

## Screenshots



The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://10.10.27/uploads/phpbash.php`. The main content area is a terminal window with a red prompt `www-data:/var/www/html/uploads#`. The terminal displays the output of the `pwd` command, followed by `cat /etc/passwd`, which lists system users and their home directories. Below this, the terminal shows the output of `ls` in the `/var/www` directory, listing subdirectories like `bin`, `boot`, `dev`, `etc`, `home`, `lib`, `lib64`, `media`, `mnt`, `opt`, `proc`, `root`, `run`, `sbin`, `selinux`, `srv`, `sys`, `tmp`, `usr`, and `var`. Finally, the terminal shows the output of `ls` in the `/var/www/tmp` directory, which is currently empty.

```
www-data:/var/www/html/uploads# pwd
/var/www/html/uploads
www-data:/var/www/html/uploads# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uidd:x:108:112::/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,:/var/lib/misc:/bin/false
xalvas:x:1000:1000:xalvas,,:/home/xalvas:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:111:118::/var/spool/postfix:/bin/false

www-data:/var/www/html/uploads#

www-data:/var/www# pwd
/var/www
www-data:/var/www# cd ../
www-data:/var# cd ../
www-data:/# ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
selinux
srv
sys
tmp
usr
var
www-data:/# cd tmp
www-data:/tmp# ls
www-data:/tmp# cd ../
www-data:/#
```