Alden Harcourt and Nathan Parker

- 1.
    - a) After accessing the webshell by using /uploadedimages/harcourta_webshell1.php, adding the “?command=whoami” command executes the linux command whoami. This returns www-data which is the name of the user account we are using. www-data only has low level permissions so the damage attacks under this account can do is limited.
    - b) The <pre> tag formats any output. When we use a webshell without <pre> tags, commands such as ls don’t have indentations or spacing which is necessary for reading the output.
- 2.
    - a) Danger’s website is located in /var/www
    - b) Currently all the names are akyianun, anyaegbunamu, harcourta, jondich, jwin, kleinhansc, lkeane, reyesm, winhallk, yuc3. We know this because using ls in the uploadedimages directory shows all the uploaded files which contain the user account names.
    - c) We think that we don’t have access to /etc/passwrd. Using command=cat /etc/passwrd gives a blank screen so it is likely that the www-data user does not have permission to access /etc/passwd. Any other commands such as ls-l or file don’t work either, corroborating the theory that we just don’t have access to the file. Google says that this file should contain a list of all user accounts and information about each user account.
    - d) cat /etc/shadow returns nothing, suggesting we don’t have permission to access the file. file /etc/shadow shows that it is a regular file with no read permission. Using stat /etc/shadow shows that it is 1242 bytes. Google says that /etc/shadow contains user account information along with hashed passwords so it makes sense that this file is blocked from www-data access.
    - e) Using ls .. shows the secret and youwontfindthiswithgobuster directories, both of which contain files for some cool ASCII art.
- 4.
    - a) 192.168.64.2. We ran the ip a command.
    - b) We tried 192.168.64.1 and 10.133.26.151 and one of them worked. Its hard for us to know which one worked, as we kept refreshing the page and changing the url trying to troubleshoot things, and nothing ever seemed to change until it just suddenly worked. Both IPs were outputted after using the ifconfig | grep inet command, and are local IP addresses.
    - e) We know we are executing commands on kali because it says kali in www-data@kali… line (shown in screenshot below).

```
(base) nathan@Nathans-MacBook-Air ~ % nc -l 5001
bash: cannot set terminal process group (2289): Inappropriate ioctl for device
bash: no job control in this shell
www-data@kali:/var/www/html$ whoami
whoami
www-data
www-data@kali:/var/www/html$
```

- f) The % codes are hexadecimal encodings of special characters that urls don't recognize.
- g)