Задача: Bash - System 1  
Исходный код:

1. #include <stdlib.h>
2. #include <sys/types.h>
3. #include <unistd.h>
4. int main(void)
5. {
6. setreuid(geteuid(), geteuid());
7. [system](http://www.opengroup.org/onlinepubs/009695399/functions/system.html)("ls /challenge/app-script/ch11/.passwd");
8. return 0;
9. }

Здесь мы можем попробовать изменить работу команды ls:

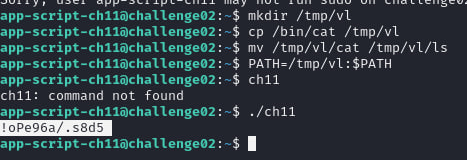
1. Создаем директорию в /tmp/vl

2. Копируем /bin/cat в /tmp/vl

3. Переименуем /tmp/vl/cat на /tmp/vl/ls для изменения работы команды ls

4. Заменяем путь PATH=/tmp/vl:$PATH. Теперь при выполнении команды ls будет выполняться команда cat

5. При выполнение ./ch11 выполнится команда cat вместо ls и мы получим флаг



Задача Bash - System 2

Исходный код:

1. #include <stdlib.h>
2. #include <stdio.h>
3. #include <unistd.h>
4. #include <sys/types.h>
5. int main(){
6. setreuid(geteuid(), geteuid());
7. [system](http://www.opengroup.org/onlinepubs/009695399/functions/system.html)("ls -lA /challenge/app-script/ch12/.passwd");
8. return 0;
9. }

Здесь можно изменить команду ls на другую команду, которая работает с флагом –lA. После нескольких попыток, такой командой будет nano

1. Создаем директорию /tmp/un
2. Копируем /bin/nano в /tmo/un
3. Переименовываем /tmp/un/nano в /tmp/un/ls
4. Изменяем переменное окружение PATH=/tmp/un:$PATH
5. Запускаем файл ./ch12 и у нас откроется окно с выводом /challenge/app-script/ch12/.passwd

