

# Программирование С

## Запуск скриптов с рутовыми правами без доступа к скриптам

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

void RemoveSlash(char* source)
{
    char* i = source;
    char* j = source;
    while(*j != 0)
    {
        *i = *j++;
        if(*i != '/')
            i++;
    }
    *i = 0;
}

int main(int argc, char** argv) {
    if (argc < 2) {
        printf("Usage: runme scriptname\n");
        exit(-1);
    }
    char myoutput_array[5000];

    strcat(myoutput_array, "bash /opt/scripts/");
    RemoveSlash(argv[1]);
    strcat(myoutput_array, argv[1]);
```

```
strcat(myoutput_array, "\n");  
/printf("%s", myoutput_array);/  
setuid(0);  
system(myoutput_array);  
return 0;  
}
```

```
gcc -o test test.c  
cp test /usr/bin/runme  
chmod 4775 /usr/bin/runme
```

---

Revision #1

Created 6 July 2023 02:34:15 by Admin

Updated 17 August 2023 07:54:00 by Admin