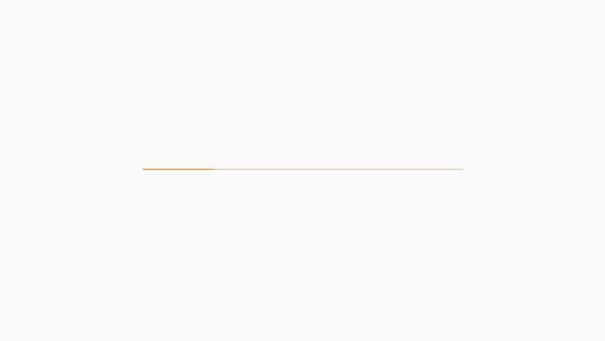
true

2025-05-16

output: revealjs: theme: beige transition: slide margin: 0.2 smaller: false logo: \_resources/image/logo\_rudn.png —



- •
- •
- Land
- 1132236050@rudn.ru
- https://yamadharma.github.io/ru/

:

• (1988)

•

.

■ C/C++

- ( , , )
- •
- •
- •

:----

```
int main(int argc, char *argv[]) {
  int valid = 0;
  char str1[8]; char str2[8];
  strcpy(str1, "START");
  gets(str2);
  if (strncmp(str1, str2, 8) == 0) valid = 1;
  printf("str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);
}
```

## (Exploit Development)

```
(payload),
Shellcode —
               ). Shellcode
ROP-
          (Return-Oriented Programming) —
            shellcode ( , DEP). ROP
```

## (buffer overflow)

- 1.
  - •
  - .
- 2.
  - strncpy strcpy,
    - snprintf sprintf,
    - memcpy\_s memcpy.