

ICS EXE 9

April 28, 2021

1 The TINY web server

Suppose a TINY web server (described in CSAPP:11.6) is going to be hosted on 10.0.0.32, at port 8000. However, someone modified line 26 of TINY `read_requesthdrs` to be `unsafe_readlineb(rp, buf, MAXLINE);`.

```
1 void doit(int fd)
2 {
3     /* Skipped... */
4
5     /* Read request line and headers */
6     Rio_readinitb(&rio, fd);
7     Rio_readlineb(&rio, buf, MAXLINE);
8     printf("Request headers:\n");
9     printf("%s", buf);
10    sscanf(buf, "%s %s %s", method, uri, version);
11    if (strcasecmp(method, "GET")) {
12        clienterror(fd, method, "501",
13                    "Not implemented",
14                    "Tiny does not implement this method");
15        return;
16    }
17    read_requesthdrs(&rio);
18
19    /* Skipped... */
20 }
21
22 void read_requesthdrs(rio_t *rp) {
23     char buf[MAXLINE];
24     Rio_readlineb(rp, buf, MAXLINE);
25     while(strcmp(buf, "\r\n")) {
26         Rio_readlineb(rp, buf, MAXLINE);
27         printf("%s", buf);
28     }
29     return;
30 }
```

The code of `unsafe_readlineb` is shown below.

```
1  ssize_t unsafe_readlineb(rio_t * rp,
2      void *usrbuf, size_t maxlen) {
3      int n, rc;
4      char c, *bufp = usrbuf;
5      n = 1;
6      while (1) {
7          if ((rc = rio_read(rp, &c, 1)) == 1) {
8              *bufp++ = c;
9              if (c == '\n') {
10                 n++;
11                 break;
12             }
13         } else if (rc == 0) {
14             if (n == 1)
15                 return 0;
16             else
17                 break;
18         } else
19             return -1;
20         n++;
21     }
22     *bufp = 0;
23     return n - 1;
24 }
```

Since `unsafe_readlineb` does not check `maxlen`, a buffer overflow (Section 3.10.3) may happen. Now suppose you are an attacker and want to kill the web server so that the others can no longer access the website. You somehow know 3 key info about the remote process (`./tiny 8000`):

1. the `exit` function is at `0x7ffff78a9dd0`.
2. when execute `read_requesthdrs`, the RBP is `0x7fffffec020`.
3. when execute `read_requesthdrs`, the variable `buf` is at `0x7fffffea020`.

How do you construct a HTTP request to do the attack?

2

Assume that a CGI program needs to send dynamic content to the client. This is typically done by making the CGI program send its content to the standard output. Explain how this content is sent to the client.