Improper input

پیش از اینکه پیام ها بررسی شوند در توابع takeAction در متود checkSecurity بررسی می شود که موارد متعددی را چک میکند:

```
public void clientToServer(String command, Socket socket) {
    try {
        Security.securityCheck(command, socket);
    } catch (Exception e) {
        e.printStackTrace();
    }
    System.out.println("this is the answer: " + answer);
}
```

چند سناریو مختلف را بررسی می کنیم:

***پیام دارای طول بلند باشد و هدفش کند کردن سرور باشد: متود زیر طول بیشتر از 10000 بودن را چک می کند که باتوجه به نوع پیام ها ممکن نیست طول به این اندازه برسد. و حتی اگر پیام خیلی طولانی باشد هم در مدت زمان O(1) می تواند مسئله بررسی شود.

```java
public static boolean checkStringLength(String command) {
    try {
        command.charAt(10000);
        return true;
    } catch (Exception e) {
        return false;
    }
}
```

*** نکته دیگری که در بالا است معمولا کد های مخرب که همان کد های javascript یا به کد های script دار هستند را سعی میکنیم بررسی نکنیم که و این کار به وسیله بررسی نکردن پیام هایی که شامل بعضی کاراکتر های خاص هستند صورت می گیرد و ان پیام ها بررسی نمی شوند.

```java
public static boolean mayContainScript(String command) {
    return command.contains("<") || command.contains(">") ||
            command.contains("\\") || command.contains("/");
}
```

*** به طور کلی پیام ها به توجه به نوع اطلاعاتی که می خواهند دو نوع محرمانه و غیر محرمانه می تواند باشد که دو نوع pattern متفاوت خواهند داشت حال اولا اگر با هیچکدام از پترن ها و رمز ها تطابق نداشت که اصلا بررسی نمی شود

```java
public void takeAction(String command) throws ParseException {...}

public void takeActionNotSecure(String command) throws ParseException {...}
```

پس بنا بر آنچه که مبرم است اگر دسترسی به کد کلاینت نداشته باشیم چون پیام ها کد هست دو حالت وجود دارد یکی اینکه خود پیام را دوباره بفرستیم و یکی اینکه پیام را کمی تغییر و سپس فرستاده شود:

اگر پیام کاملا مشابه فرستاده شود که در بخش replay attack بررسی شده و مشکلی برایمان پیش نمی اورد و اگر هم پیام را تغییر دهد اولا که باتوجه به طول زیاد indentification احتمالا ان هم تغییر داده شود و پیام نامعتبر شود و اصلا بررسی نشود در غیر این صورت فرض کنید که پیام اصلی تغییر کند و توسط سرور بررسی شود چون که کد تابع takeAction که تابع اصلی بررسی پیام و واکنش است در try - catch قرار دارد بنا بر این اگر throw exception صورت بگیرد، catch exception صورت می گیرد و بر عملکر سرور تاثیری ندارد. توجه کنید چون که احتمالا علت exception ها نویز یا مزاحمت های خرجی است علت انها اصلا بررسی نمی شود.

حال اگر فرد به کد های کلاینت هم دسترسی داشته باشد اگر سعی کند پیام زیاد بفرستد، همان طور که گفته شد به IP Blakc List منتقل می شود و اجازه پیام دادن سلب می شود.

```
//making sure it doesn't send more than 10 requests in 100 milliseconds

if (IP.addIp(getIP(socket))) {
    blackListOfIPs.add(getIP(socket));
    return;
}
```

```java
public static boolean addIp(String Ip) {
    IP ip = getIp(Ip);
    if (ip == null) {
        new IP(Ip);
        return false;
    }
    if (ip.ip.equals(Ip)) {
        if (ip.tenRecentTimes.size() >= BOUND) {
            ip.tenRecentTimes.remove( index: 0);
            ip.tenRecentTimes.add(System.currentTimeMillis());
            return ip.tenRecentTimes.get(BOUND-1) - ip.tenRecentTimes.get(0) < 100;
        } else {
            ip.tenRecentTimes.add(System.currentTimeMillis());
        }
    }
    return false;
}
```

حال در صورت اگاهی به کد های کلاینت، به طور کامل در broken authentication کامل بررسی شده است که نمی تواند به اطلاعاتی بجز اطلاعات خودش، دسترسی داشته باشد.