# Q2 JavaScript Injection

Cross-Site Scripting (XSS) is one of the most common JavaScript vulnerabilities. It occurs when attackers inject malicious scripts into JavaScript.

**Backdoor position: [Git Link](https://github.com/Shahzeb892/websokect_chat_app/blob/main/JsServer/client/clientService.js)** **line71**

**Vulnerable function position:** [**Git link**](https://github.com/Shahzeb892/websokect_chat_app/blob/main/JsServer/util/security.js) **line 50**

1. Analysis vulnerable function

A screenshot of a computer code

Description automatically generated

Figure 1 vulnerable function

The function recursively copies properties from json object to another data, without checking the names of keys. However, the copy function can modify the properties of a class. While a prototype had been modified, the changes affect all instances that are created from that prototype.

1. Verify the vulnerability of copy  
   A screen shot of a computer program

   Description automatically generated

Figure 2 test script

We try to use the copy to change the ‘\_\_proto\_\_’, and then state a new class.  
 A screenshot of a computer program

Description automatically generated

Figure 3 js prototype pollution

1. Understanding of the backdoor  
   A screen shot of a computer program

   Description automatically generated

Figure 4 backdoor

The attacker should build a json to apply {debug: Ture} and {debugCommend:any javascript} prototype for every { } by polluting prototypes. Subsequently, the server will execute debugCommend while a new user connect to server.

1. Start attack  
   [Attack script](https://github.com/FrogGuaGua/SQRPRGRM/blob/main/CTFanswer%26design/Q2/poc.js)  
   A screen shot of a computer program

   Description automatically generated

Figure 5 Attack script

We receive 