

# WEB saugumas

---

Marius Gžegoževskis



# Turinys

---

- Clickjacking.
  - Drag and Drop API.
  - Keyboard “Strokejacking”.
  - Ir kitos panašios atakų rūšys.
  - Apsaugos priemonės.
-

# Clickjacking

---

- Sekančios kartos clickjacking
- Clickjacking: Atakos ir apsisaugojimo būdai.

# Clickjacking esmė

---

- Jos esmė yra priversti vartotoją spragtelėti ant užmaskuotų tinklalapio elementų, pavyzdžiui, įdėtinio rėmelio (angl. iframe), kuriame yra užkrautas tarkime mokėjimų sistemos vartotojo paskyros nustatymų puslapis.
  - Vartotojas nė neįtaria, kad žaisdamas įdomų žaidimą tuo pat metu keičia paskyros nustatymus. Saugumo tyrinėtojai taip pat pateikė „Adobe Flash“ saugumo modelio trūkumus išnaudojantį demonstracinį kodą, kurį pasitelkę piktavaliai galėjo perimti aukos internetinės kameros ir mikrofono valdymą.
-

# Clickjacking (UI Redressing) vartotojo sąsajos uždengimas

---

- Kenkėjas užkloja keletą permatomų arba nepermatomų rėmelių taip siekdamas apgauti vartotoją paspausti mygtuką arba nuorodą esančią tame pačiame puslapyje, kuriame jis yra prisijungęs. Taigi paspaudęs nematomame rėmelį tam tikrą mygtuką ar nuorodą jis taip pat paspaudžia ir pagrindiniame puslapyje esantį mygtuką ar nuorodą.



- Mygtuko paspaudimai matomajame puslapyje yra perimami ir persiunčiami kitam, nematomam puslapiui.
-

# Clickjacking atakos

---

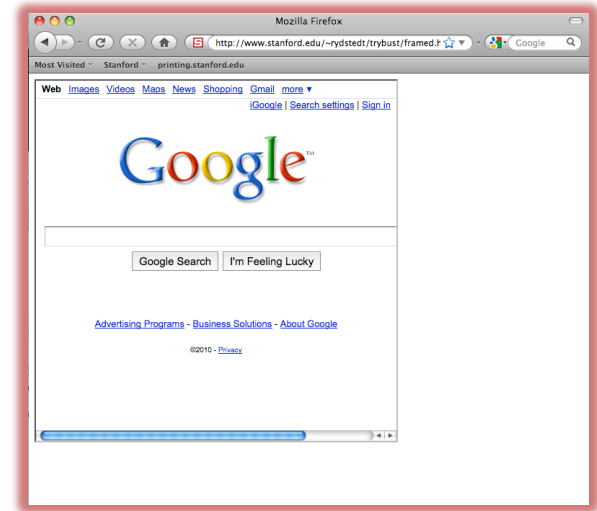
- Google paieškoje įvedūs „Clickjacking“ yra pateikiama apie 1 110 000 rezultatų, tai reiškia jog ši grėsmė yra gan plačiai paplitusi.
  - Daug clickjacing atakų buvo atlikta prieš žinomiausius socialinius tinklus: Facebook, Twitter.
  - Pavyzdžiui atakos prieš Twitter:
    - » Vartotojas siunčia savo žinutes priverstinai.
-

# Clickjacking pagrindas yra „IFrame“

- Bet kuri interneto svetainė gali turėti rėmelį, kuriame yra įterpta bet kuri kita svetainė.

```
<iframe  
  src="http://www.google.com/...">  
</iframe>
```

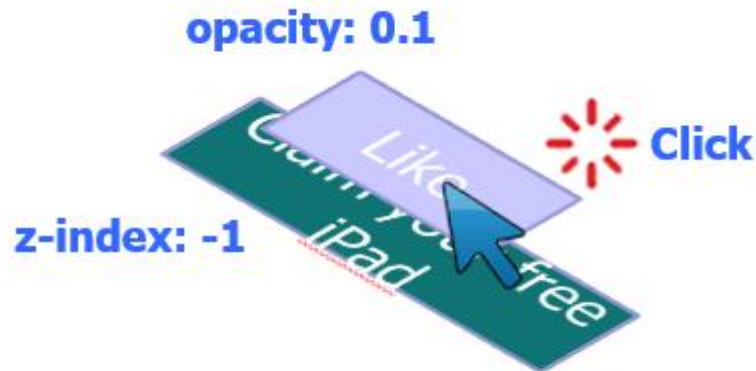
- HTML atributai:
- Style (Stilius)
- Opacity (permatomumas) apibrėžia procentinę iframe (rėmelio) permatomumą.
  - » 1.0: visiškai matomas.
  - » 1.1 visiškai nematomas.



# Paslėpti tikslo elementą

---

- Naudoti CSS opacity parametą ir z – index parametą skirta paslėpti pagrindiniui elementui, taip pakišti kenkėjišką elementą užklojant ant viršaus pagrindinį elementą. Paspaudūs mygtuką „LIKE“ bus įvykdomas ir apačioje pakištas mygtukas „Claim your free iPad“ arba nuoroda.





# Paslėpti tikslo elementą

---

- Naudoti CSS `pointer-events:none` parametą uždengti kenkėjišką mygtuką ar nuorodą virš tikslo elemento. Kenkėjiškas mygtukas „**Claim your free iPad**“ bus užklotas ant pagrindinio žemiau pavaizduotame pav. „**LIKE**“.

`pointer-event: none`



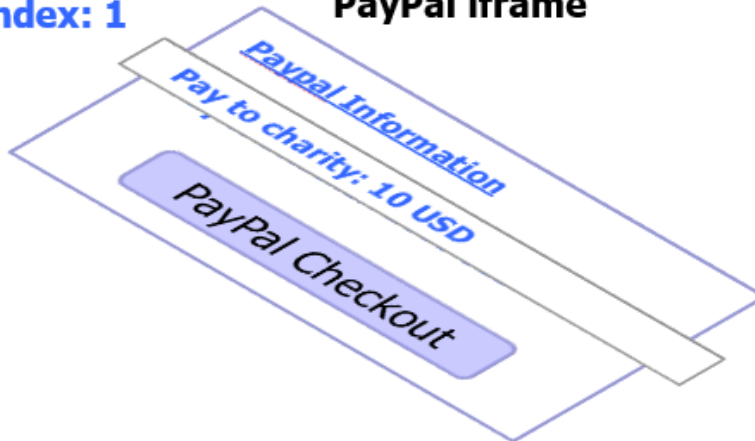
# Dalinės uždangos bei apkarpymas

---

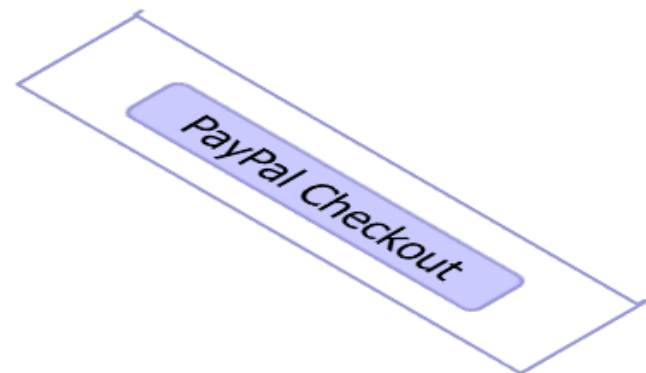
- Elementų dalinis uždengimas ant „IFRAME“ naudojant CSS z-index parametą arba Flash Window Mode wmode=direct parametą.
- Įsprausti tikslo elementą naujame rėmelyje (angl. Frame) ir pasirinkti CSS poziciją nurodant offset parametrus.

**z-index: 1**

**PayPal iframe**



**PayPal iframe**



# Drag-and-Drop API

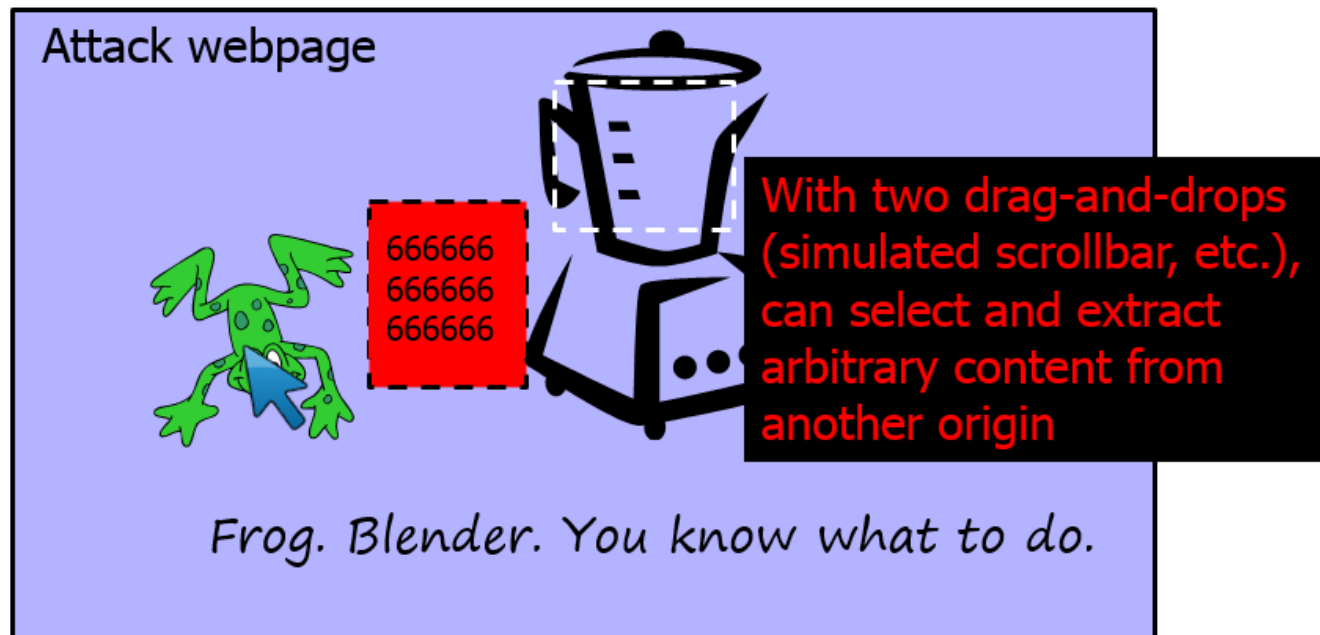
---

- Modernios naršyklės palaiko „Drag-and-Drop API“.
  - JavaScript gali pasinaudoti šiuo API ([Application programming interface](#)), kai elementas bus tempiamas į tam tikrą poziciją arba nuskaityti jo parametrus, kai jis bus išmetamas.
  - Nėra uždrausta tos pačios kilmės „politikos“:
  - Duomenis iš vieno šaltinio (angl. origin) gali būti tempiami į rėmą (angl. Frame) esantį kitame šaltinyje.
  - Priežastis: drag-and-drop gali būti inicijuojami vartotojo pelės paspaudimu ir tempimu, bet ne JavaScript aprašytu scenariju.
-

# Drag-and-Drop API piktnaudžiavimas

---

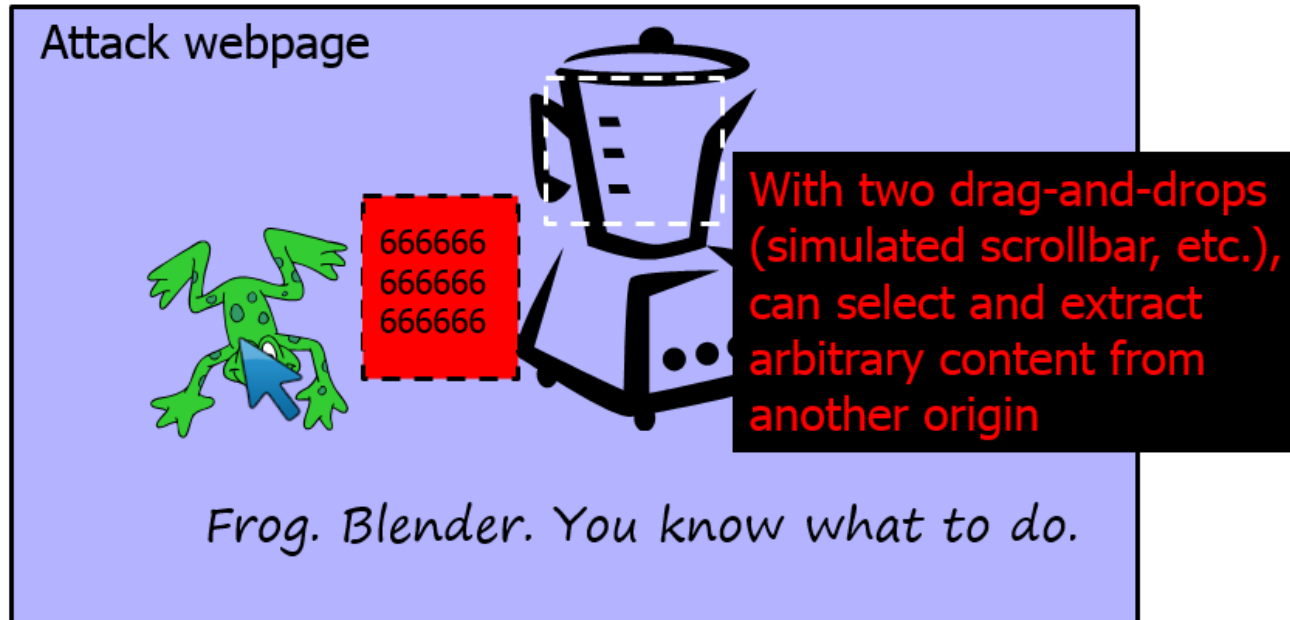
1. Sudominti vartotoją paspausti ant reklamos ar kito pobūdžio paveikslėlio ir pradėti tempti į kurią nors poziciją.



# Drag-and-Drop API piktnaudžiavimas

---

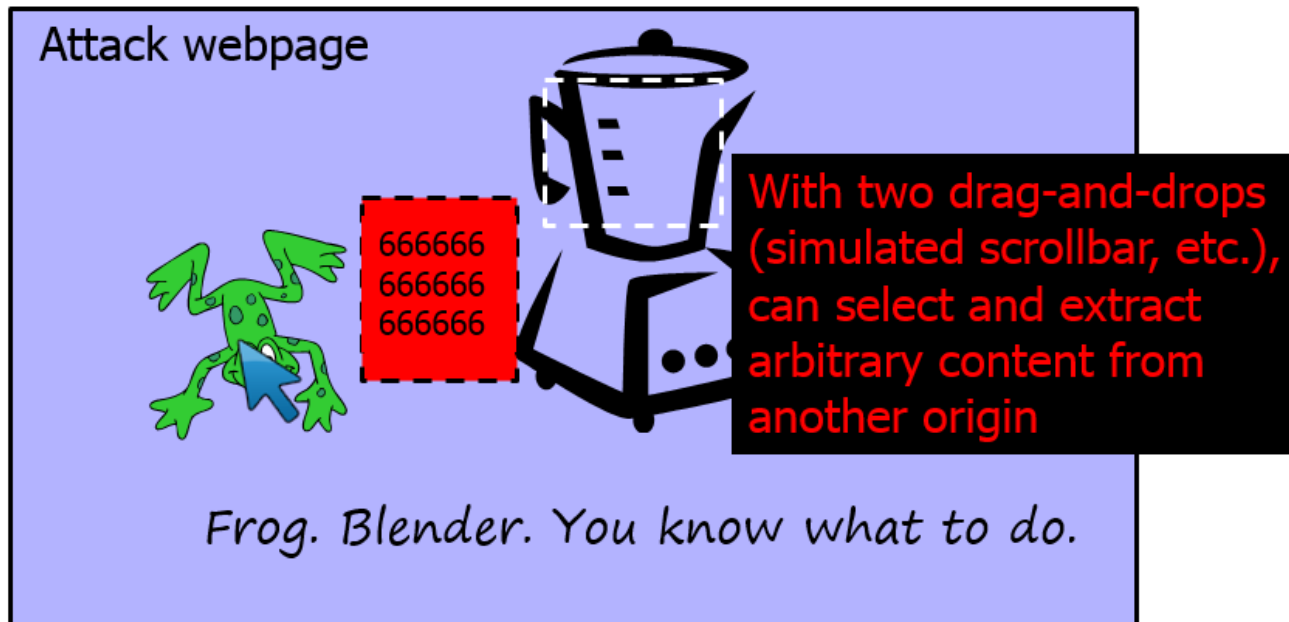
2. Nematomas piktavalių rėmelis su tekstiniu lauku yra po pelės žymekliu, naudojant API yra inicijuojamas pradėtas tempimas.



# Drag-and-Drop API piktnaudžiavimas

---

3. Nematomas IFrame iš kito šaltinio su formos lauku. Su dvejais drag-and-drops gali būti išrenkami duomenys ir įkeliamas turinys priklausantis kitam šaltiniui.



# Netikri kursoriai (angl. Fake Cursors)

---

- Panaudoti CSS cursor parametą ir panaudojant JavaScript pateikti netikro žymeklio įkoną ekrane.

**Real cursor icon**

**cursor: none**



**Fake cursor icon**





# Keyboard “Strokejacking”

- Netikras tekstinis laukelis skirtas informacijai įvesti, bet įvedamas tekstas vistiek turėtų būti įvedamas į tikslo laukelį be vartotojo žinios. Vartotojas nežinodamas jog įvesdamas informaciją į netikrą laukelį iš tiesų įveda ją į realų tekstinį laukelį, kuriame gali būti atliekami įvairiausi veiksmai skirti perduoda svarbią informaciją.

## Attacker's page

Typing Game  
Type whatever screen shows to you

Xfpog95403poigr06=2kfpX



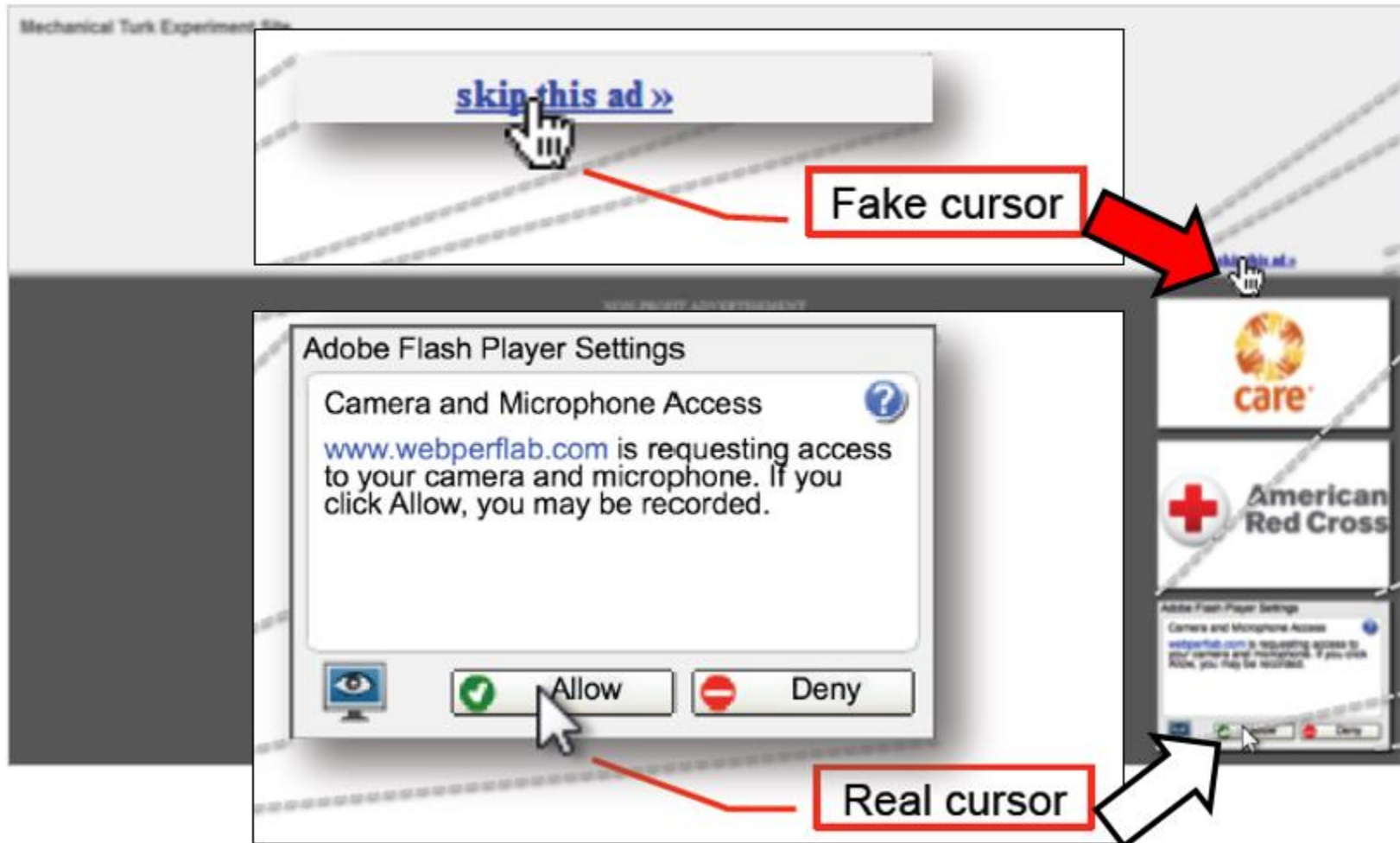
## Hidden iframe within attacker's page

Bank Transfer  
Bank Account: 9540  
Amount: 3062 USD

Transfer

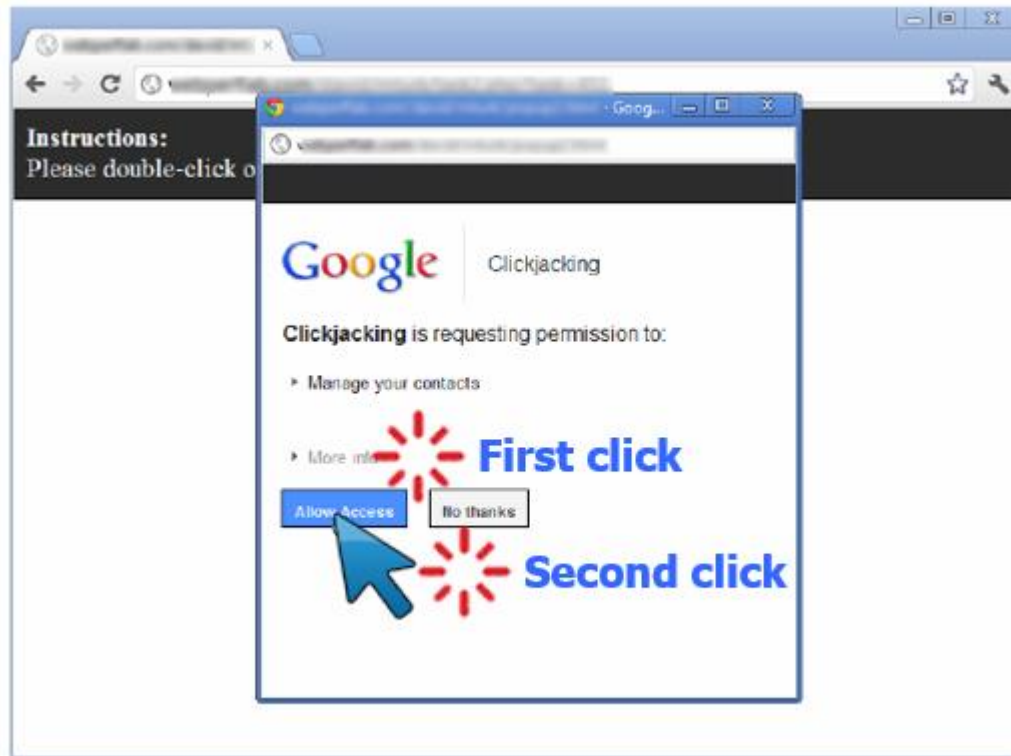


# Cursor Spoofing



# Double-Click Attack

- Sudominti vartotoją paspausti dvigubą pelės paspaudimą, sufokusuoti iššokusį langą tarp dviejų pelės paspaudimų.



# Whack-A-Mole Attack

- Nurodymas vartotojui paspausti kiek įmanoma daugiau ant nuorodos.

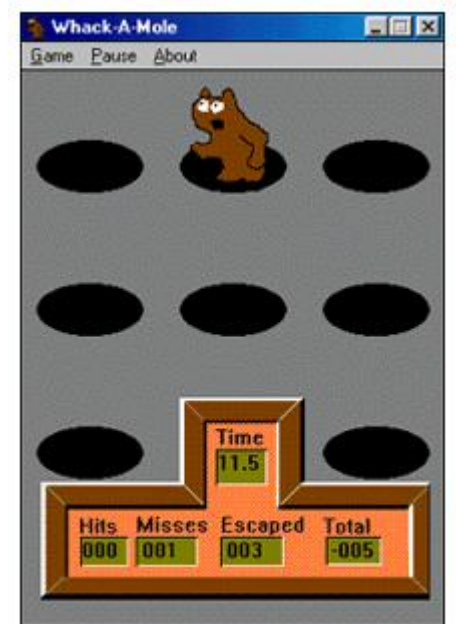
## Instructions:

Please click on blue buttons *as fast as possible*. The faster you complete this game, the greater your chances to win a \$100 prize! If you don't click on a button, the game will skip it in 10 seconds.

Buttons clicked: 17/20

Time elapsed: 27.6 sec

CLICK ME



# Apsauga nuo nepageidaujamųjų paslėptų rėmelių (angl. Frame busting)

- Reikia užtikrinti jog, kuriamos ar jau esamos svetainės puslapiai nebūtu įkraunami į uždengiančiuosius rėmelius.
- Įgyvendinus apsaugą nuo pradinių puslapių įkrovimo į rėmelį, uždengiančių kenkėjiškais rėmeliais, „Clickjacking“ problema yra išsprendžiama.
- Kodo fragmentas apsaugantis nuo nepageidaujamųjų rėmelių neaiškos kilmės.

```
if (top != self)
    top.location.href = location.href
```

---

# Jeigu esamosios svetainės rėmelis nėra viršuje.

---

## Conditional Statements

```
if (top != self)
```

```
if (top.location != self.location)
```

```
if (top.location != location)
```

```
if (parent.frames.length > 0)
```

```
if (window != top)
```

```
if (window.top !== window.self)
```

```
if (window.self !== window.top)
```

```
if (parent && parent !== window)
```

```
if (parent &&  
    parent.frames &&  
    parent.frames.length>0)
```

```
if((self.parent&&  
    !(self.parent===self))&&  
    (self.parent.frames.length!=
```

# Perkelti esamąjį (originalų) rėmelį perkelti į viršų

Counter-Action Statements
<code>top.location = self.location</code>
<code>top.location.href = document.location.href</code>
<code>top.location.href = self.location.href</code>
<code>top.location.replace(self.location)</code>
<code>top.location.href = window.location.href</code>
<code>top.location.replace(document.location)</code>
<code>top.location.href = window.location.href</code>
<code>top.location.href = "URL"</code>
<code>document.write('')</code>
<code>top.location = location</code>
<code>top.location.replace(document.location)</code>
<code>top.location.replace('URL')</code>
<code>top.location.href = document.location</code>
<code>top.location.replace(window.location.href)</code>
<code>top.location.href = location.href</code>
<code>self.parent.location = document.location</code>
<code>parent.location.href = self.document.location</code>
<code>top.location.href = self.location</code>
<code>top.location = window.location</code>
<code>top.location.replace(window.location.pathname)</code>

# O kaip gi dėl asmeninių Iframe užklojimo jeigu yra naudojamos pradinėje svetainėje ?

---

- Patikrinti ar uždengiantysis rėmelis yra asmeninis?
  - Kaip sunku gali būti įgyvendinti tokią apsaugą?
  - Atlikti tyrimai kelių šimtų tūkstančių žinomiausių interneto svetainių... Visi kenkėjiškų rėmelių (angl. frame busting) apsaugos metodai yra neveiksmingi bei lengvai pažeidžiami.
-

# Courtesy of Walmart

---

```
if (top.location != location) {  
    if(document.referrer &&  
        document.referrer.indexOf("walmart.com") == -1)  
    {  
  
        top.location.replace(document.location.href);  
    }  
}
```

---



# Error in Referrer Checking



IŠ: <http://www.attacker.com/walmart.com.html>  
<iframe src="http://www.walmart.com">

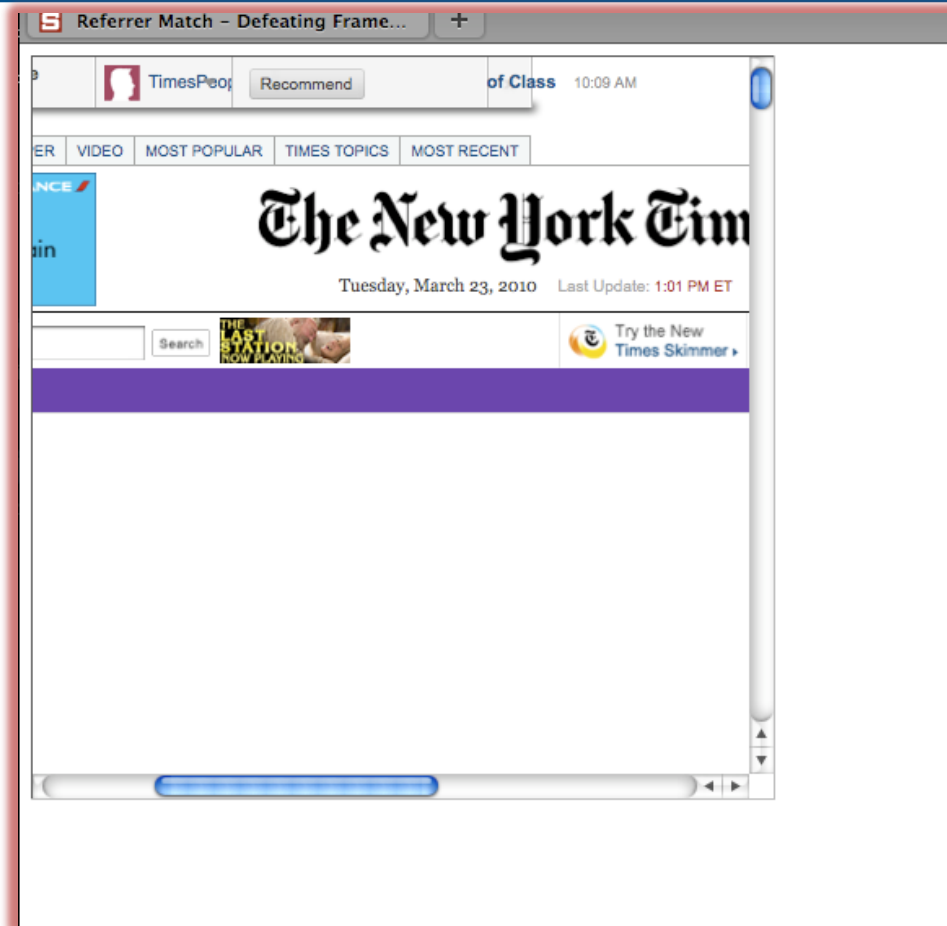
# The New York Times

---

```
if (window.self !== window.top &&  
    !document.referrer.match(  
        /https?:\W[^\W]+\.nytimes\.com\W/))  
{  
    self.location = top.location;  
}
```

---

# Error in Referrer Checking



Iš <http://www.attacker.com/a.html?b=https://www.nytimes.com/>  
<iframe src="http://www.nytimes.com">



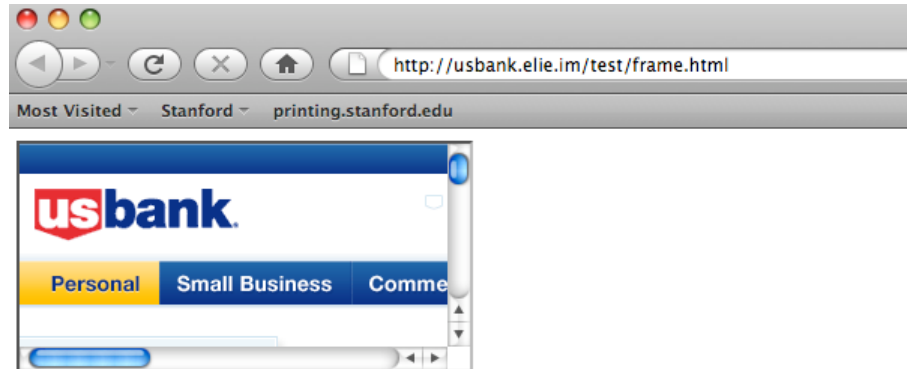
---

```
if (self != top) {  
    var domain = getDomain(document.referrer);  
    var okDomains = /usbank|localhost|usbnet/;  
    var matchDomain = domain.search(okDomains);  
  
    if (matchDomain == -1) {  
        // frame bust  
    }  
}
```

---

# Error in Referer Checking

---



From <http://usbank.attacker.com/>  
<iframe src="http://www.usbank.com">

---

---

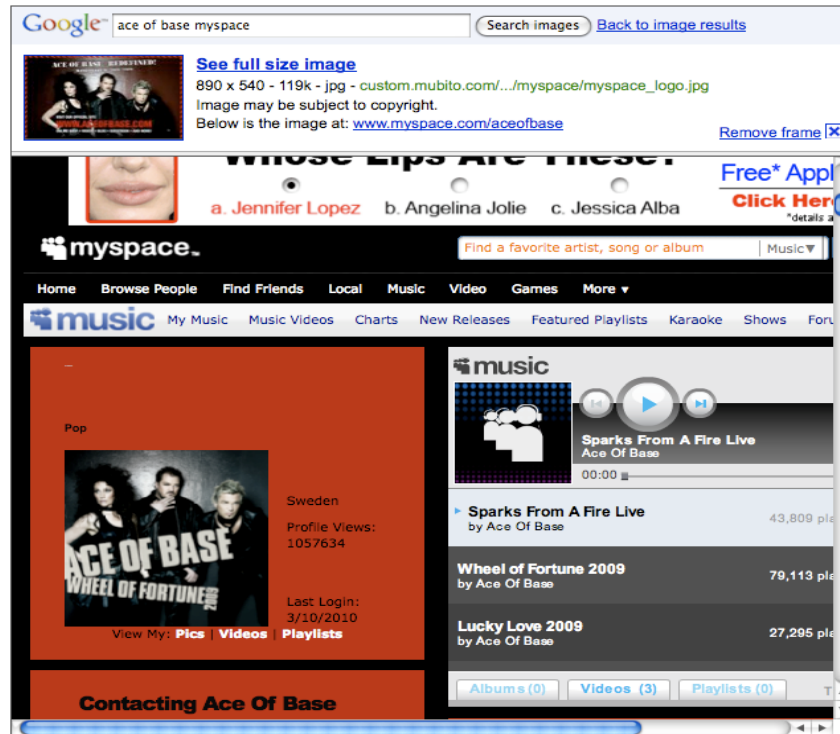
```
try{
  A=!top.location.href
} catch(B){}
A=A&&

!(document.referrer.match(/^https?:\W[-az09.]
*\.\google\.(co\.|com\.)? [a-z] +Vimgres/i))&&

!(document.referrer.match(/^https?:\W([^\V]*\.)?
(myspace\.com|
myspace\.cn|
simsidekick\.com|
levisawards\.com|
digg\.com)\V/i));
if(A){ // Frame bust }
```

---

# google ir kitos žinomos apsaugo nuo „clickjacking“?



- Google Images taip pat neturi „frame bust“ apsaugos.

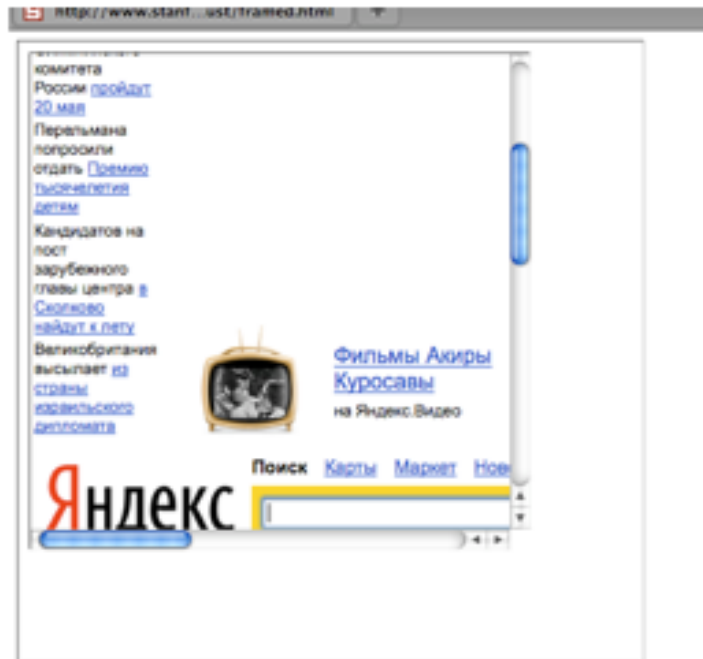
# Tipinis „Frame Busting“ scenarijaus kodas

---

```
if(top.location != self.location) {  
    parent.location = self.location;  
}
```



# Kuris yra pagrindinis rėmelis?



Double framing!!

```
framed1.html
<iframe
src="framed2.html">
```

```
framed2.html
<iframe
src="victim.com">
```

# Kuris rēmelis yra viršutinis?

---

```
if (top.location != self.location)  
    top.location = self.location
```

Jeigu **top.location** gali būti pakeistas arba atjungtas, šis kodas yra beprasmis.

---

# Location Clobbering

---

- IE 7

```
var location="clobbered";
```

- Safari

```
window.__defineSetter__("location", function(){});
```

» `top.location` yra neapibrėžtas (angl. undefined).

---

# Vartotojas gali sustabdyti „Frame busting“ patvirtindamas tai.

---

- Vartotojas gali atšaukti bet kokį bandymą „frame busting“ kodo nukreipti jį į pagrindinį puslapį.
- Kenkėjui tereikia paklausti vartotojo apie šį veiksmą. Ar jis tikrai nori atšaukti.

<script>

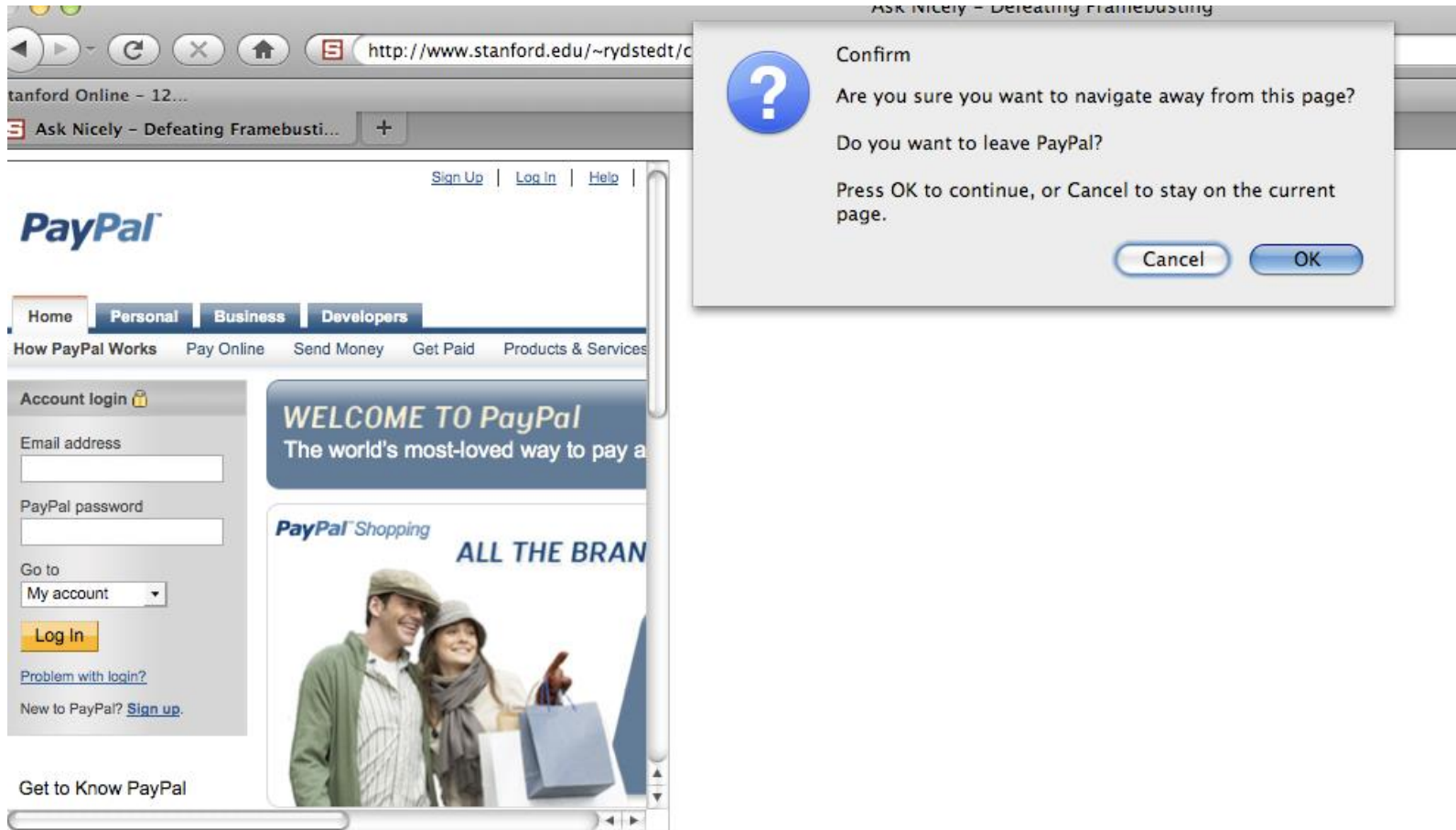
```
window.onbeforeunload = function() {  
    return "Do you want to leave PayPal?";  
}
```

</script>

<iframe src="http://www.paypal.com">

---

# Pavyzdys



# Neklausiant vartotojo apelinama „Frame bust“ apsauga

---

- Daugelis naršyklių leidžia kenkėjui atšaukti nukreipimą programiškai

```
var prevent_bust = 0
```

```
window.onbeforeunload = function() {kill_bust++ }
```

```
setInterval(function() {
```

```
    if (kill_bust > 0) {
```

```
        kill_bust -= 2;
```

```
        window.top.location = 'http://no-content-204.com'
```

```
    }
```

```
}, 1);
```

```
<iframe src="http://www.victim.com">
```

---

# X-Frame-Options

---

- HTTP antraštė siuntimui gali būti nurodomi 2 parametrai, kurie apsaugo nuo „clickjacking“ atakų.
  - Dvi galimybės: **DENY** arba **SAMEORIGIN**
  - **DENY**: puslapis nebus interpretuojamas jeigu bus panaudotas IFRAME taip atmesdamas visus rėmelius.
  - **SAMEORIGIN**: puslapis bus interpretuojamas jeigu „top frame“ bus tos pačios kilmės.
-

# Prisitaikymas X-Frame-Options naršyklėse

---

- Geras pritaikomumas šios opcijos X-Frame-Options naršyklėse.
  - Prastas prisitaikomumas pagal internetines svetaines struktūra bei realizaciją, kadangi kiekviena iš jų yra skirtingai suprojektuota.
  - Limitai
    - » Kiekvienam puslapiui atskirai nurodyti.
    - » Nėra „geriečių“ sąrašų priklausančių aiškos kilmės svetainei.
    - » Proxy serverių problemos.
-



# Content Security Policy (Firefox 4)

---

- Kita HTTP antraštė: **frame-ancestors** direktyva apibrėžianti, kaip ir patikimos kilmės svetainės, kurios gali naudoti framų's.
  - Leidžia priskirti kiekvienai svetainei leisti atlikti viena ar kitą funkciją.
-

# Clickjacking apsaugos metodai

---

- Egzistuoja keletas apsaugos mechanizmų nuo „clickjacking“ atakų. Pirmasis žinomas kaip „rėmelių žudikas“. Tai „JavaScript“ kodas, kuris neleidžia tinklalapio atvaizduoti rėmelyje. Šis kodas turi būti įterptas į kiekvieną norimą apsaugoti puslapį.
-

# Clickjacking apsaugos metodai (JavaScript)

---

- Paprasta realizacija, tačiau tai nėra universalus sprendimas, kadangi „Internet Explorer“ naršyklė supranta rėmelio atributą „security“, kurio reikšmė „restricted“ nurodo, kad rėmelyje esantis tinklalapis yra padidinto saugumo zonoje, kurioje JavaScript kodas paprasčiausiai neveiks. Taip pat šis apsaugos mechanizmas bus bejėgis prieš klientus su atjungtu „JavaScript“ palaikymu.
  - „Rėmelių žudikas“:
    - » `<script type="text/javascript">`
    - » `if (top!=self)`
    - » `top.location.href=self.location.href;`
    - » `</script>`
-

# Clickjacking apsaugos metodai (X-FRAME-OPTIONS)

---

- Norėdami apsaugoti IE8 naudotojus, web programuotojai gali gražinti specialią antraštę X-FRAME-OPTIONS, kuri nurodo kaip konkretus puslapis gali būti įrėmintas. X-FRAME-OPTIONS reikšmė DENY reiškia, kad puslapis negali būti įrėmintas, SAMEORIGIN – puslapis bus atvaizduotas rėmelyje, jeigu sutaps naršymo kontekstas.
-

# Clickjacking apsaugos metodai (X-FRAME-OPTIONS)

---

- Kuomet puslapis pažeidžia nustatytą X-FRAME-OPTIONS politiką, IE8 vietoj tinklalapio rodo įspėjantį pranešimą bei pateikia nuorodą, kuri atidaro rėmelio šaltinį naujame lange.

# Clickjacking apsaugos metodai ( „ClearClick“ modulis)

---

- Paskutinis apžvelgiamas apsaugos sprendimas yra „Mozilla“ šeimos interneto naršyklėms skirtas nemokamo papildinio „NoScript“ modulis „ClearClick“. Prieš tai du minėti apsaugos nuo „clickjacking“ atakos mechanizmai negali eiliniam vartotojui garantuoti, kad tam tikra interneto svetainė juos tinkamai įsidiegusi. „ClearClick“ modulis automatiškai aptinka ir nukenksmina bei praneša vartotojui apie vykdomą ataką. Naujausia modulio versija turi eksperimentinį X-FRAME-OPTIONS antraštės palaikymą taip pat moka atpažinti ne vien rėmeliais paremtas „clickjacking“ atakas , kas suteikia dar didesnį patikimumą.
-

# Kol kas geras būdas apsaugoti, bet nēra geriausias sprendimas

---

```
<style>html { visibility: hidden }</style>
```

```
<script>
```

```
if (self == top) {
```

```
    document.documentElement.style.visibility = 'visible';
```

```
} else {
```

```
    top.location = self.location;
```

```
}
```

```
</script>
```

---

# Frame Busting Mobilių įrenginių svetainėse

Site	URL	Framebusting
Facebook	<a href="http://m.facebook.com/">http://m.facebook.com/</a>	YES
MSN	<a href="http://home.mobile.msn.com/">http://home.mobile.msn.com/</a>	NO
<u>GMail</u>	<a href="http://m.gmail.com">http://m.gmail.com</a>	NO
<u>Baidu</u>	<a href="http://m.baidu.com">http://m.baidu.com</a>	NO
Twitter	<a href="http://mobile.twitter.com">http://mobile.twitter.com</a>	NO
MegaVideo	<a href="http://mobile.megavideo.com/">http://mobile.megavideo.com/</a>	NO
Tube8	<a href="http://m.tube8.com">http://m.tube8.com</a>	NO
PayPal	<a href="http://mobile.paypal.com">http://mobile.paypal.com</a>	NO
USBank	<a href="http://mobile.usbank.com">http://mobile.usbank.com</a>	NO
First Interstate Bank	<a href="http://firstinterstate.mobi">http://firstinterstate.mobi</a>	NO
NewEgg	<a href="http://m.newegg.com/">http://m.newegg.com/</a>	NO
MetaCafe	<a href="http://m.metacafe.com/">http://m.metacafe.com/</a>	NO
RenRen	<a href="http://m.renren.com/">http://m.renren.com/</a>	NO
MySpace	<a href="http://m.myspace.com">http://m.myspace.com</a>	NO
Vkontakte	<a href="http://pda.vkontakte.ru/">http://pda.vkontakte.ru/</a>	NO
WellsFargo	<a href="https://m.wf.com/">https://m.wf.com/</a>	NO
NyTimes	<a href="http://m.nytimes.com">http://m.nytimes.com</a>	Redirect
E-Zine Articles	<a href="http://m.ezinearticles.com">http://m.ezinearticles.com</a>	Redirect



# Tapjacking

---

- Priartina mygtukus į permatomą IFRAME taip užklodami visą ekrano zoną.
- Paslėpti arba suklastoti URL adresų juostą.
- Sukurti užmaskuotą puslapį, dar kitaip žinomą kaip programa skirta apgauti vartotoją paspausti mygtuką, nuorodą ar kokį kitą elementą.

Plačiau: <http://seclab.stanford.edu/websec/framebusting/>

---