

Examine postMessage uses in Alexa top 10,000 sites.



- ### Defenses
1. Origin-based defense
 2. Frame-based defense
 3. CSP extension



- We collected postMessage receivers from Alexa top 10,000 sites
 - **RvScope**: our tool for collecting receivers
-

postMessage Vulnerabilities in the Wild

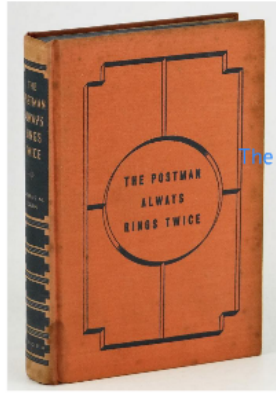
Among 14,112 frames from 10,111 host origins, 2,241 frames (24%) have a postMessage receiver. 1,480 frames have a receiver with an origin (14%) and 761 frames are receiver-less (7%).

14,112 frames from 10,111 host origins

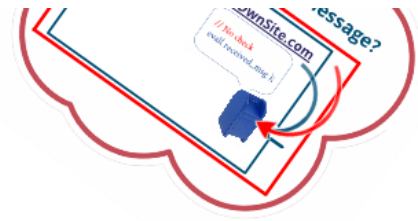
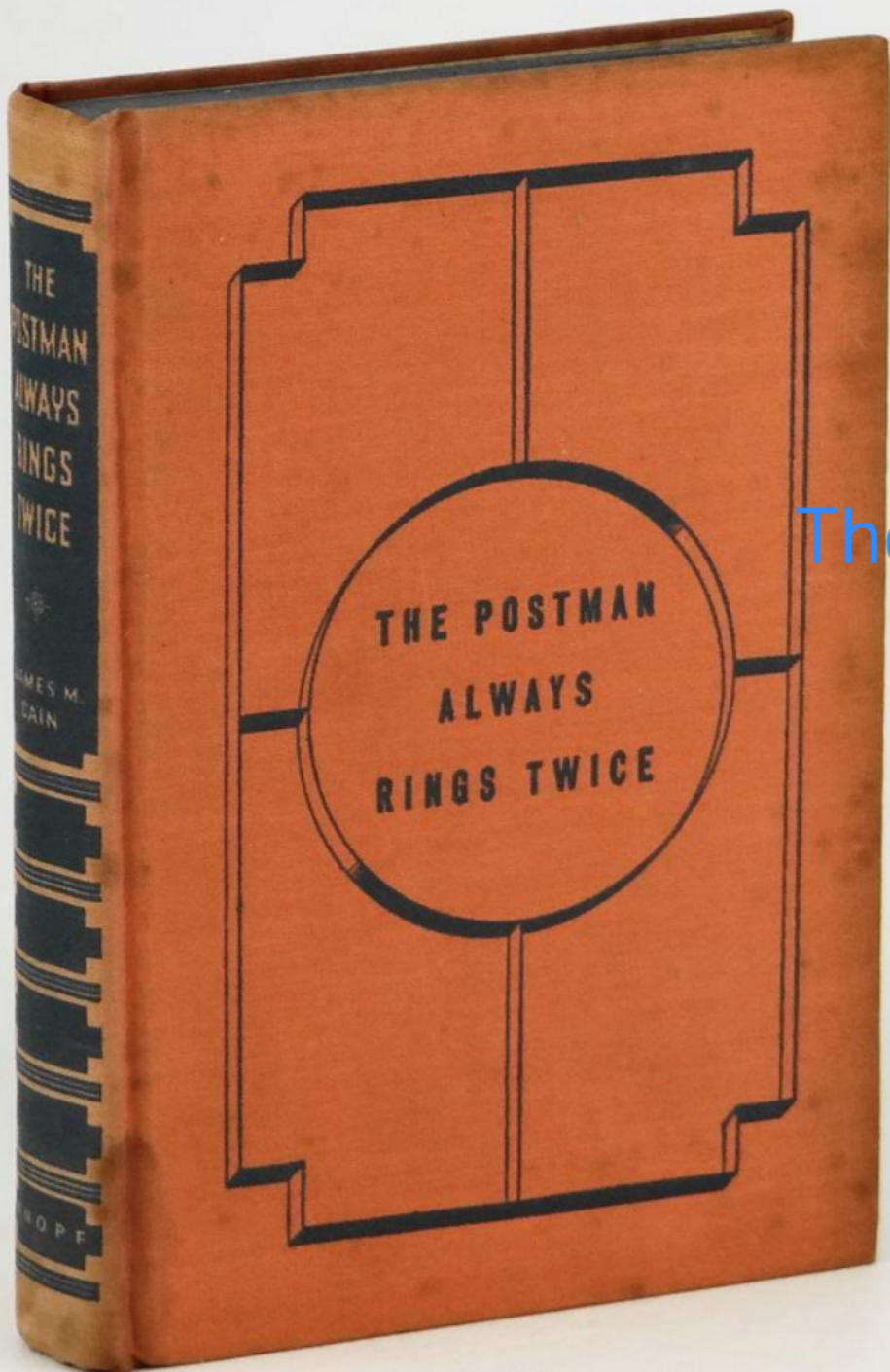
Lessons

Q&A

Introduce safe use patterns.



The Postman Always Rings Twice: Attacking & Defending postMessage in HTML5 Websites

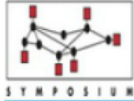


The Postman Always Rings Twice: Attacking & Defending postMessage in HTML5 Websites



NDSS 2013 call for papers

TOP STORY 09:45AM EST



THE LATEST

MOST SHARED

The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites

10:00AM EST

The camera-ready due for NDSS 2013 is coming up

TV WATCH ONLY ON PEOPLE.COM 09:10AM EST

Internet Society 20 years

09:05AM EST

19th Annual Network & Distributed System Security Symposium



WHAT YOU RIGHT NOW



READ IT

Like

12k

Tweet

+1

Sooel Son and Vitaly Shmatikov

The University of Texas at Austin



Examine postMessage uses in Alexa top 10,000 sites.

- Defenses**
1. Origin-based defense
 2. Frame-based defense
 3. CSP extension



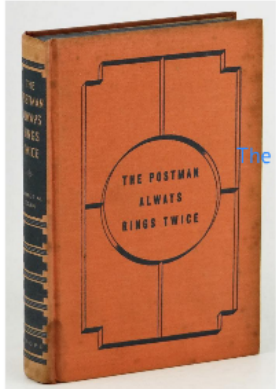
- We collected postMessage receivers from Alexa top 10,000 sites
 - **RvScope**: our tool for collecting receivers
-

postMessage Vulnerabilities in the Wild

Among 14,155 pages from 14,151 host names (2011-2012) 1241 have a postMessage receiver (8.8%) which have a receiver with an origin check (7.2%)

All links here: [http://www.wisecoders.com/postmessage/](#)

Introduce safe use patterns.



The Postman Always Rings Twice:
Attacking & Defending postMessage in HTML5 Websites

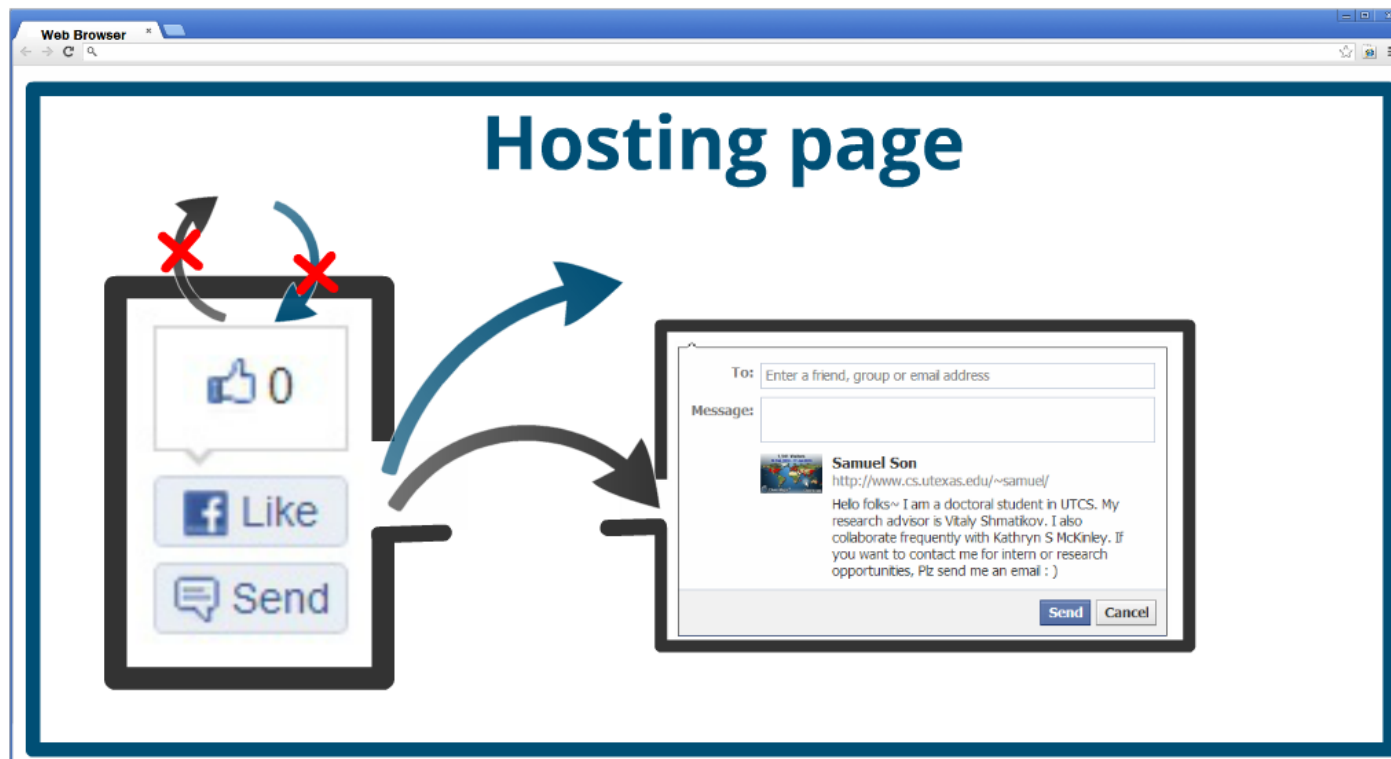
Lessons
A collection of lessons learned from the research.

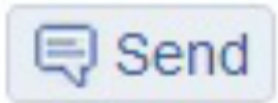
Q & A
A collection of frequently asked questions.



postMessage

Purpose: a "hole" in same origin policy





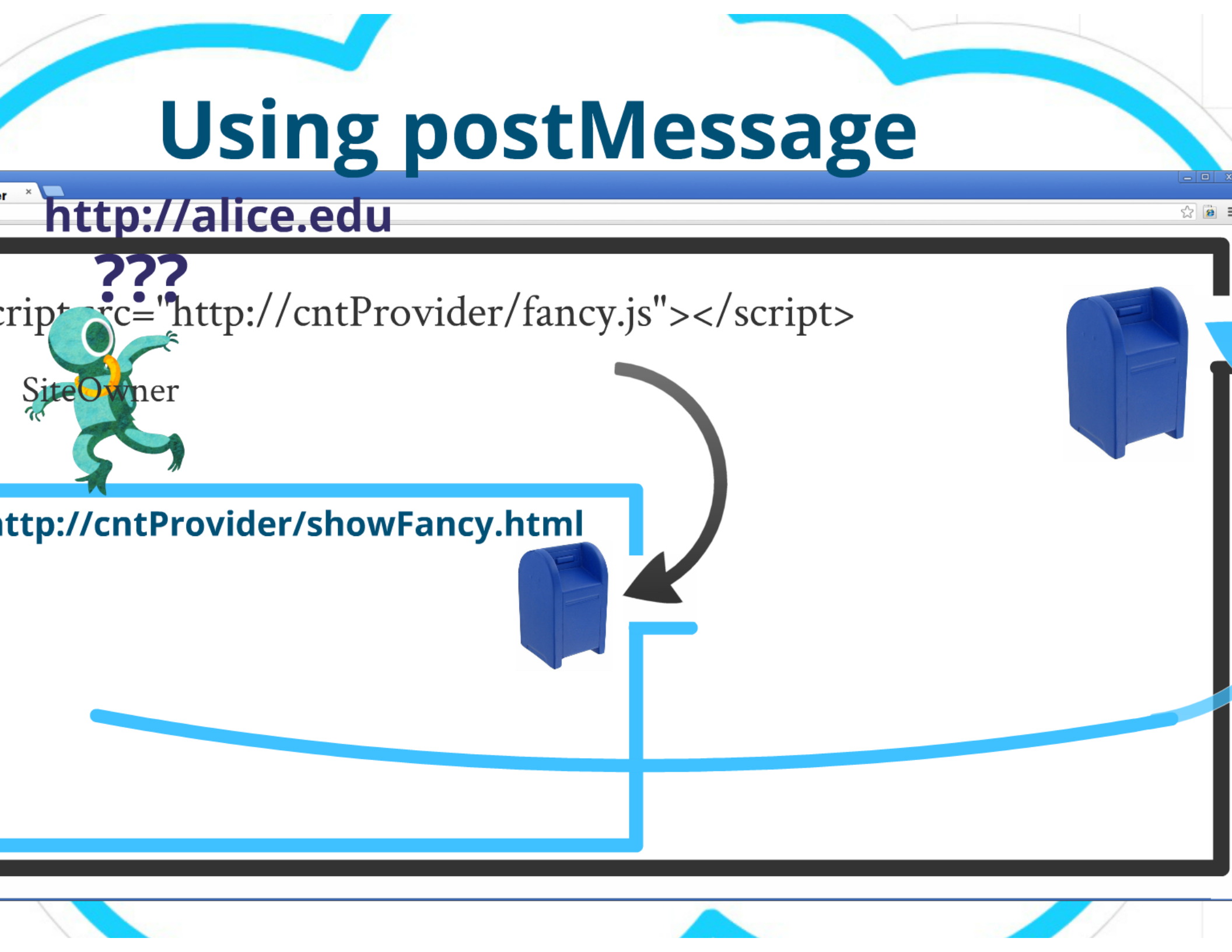
Using postMessage

http://alice.edu

???
`<script src="http://cntProvider/fancy.js"></script>`

SiteOwner

http://cntProvider/showFancy.html



Check the origin of received messages!



```
function msgReceiver(e) {  
  if(e.origin !== "http://hostA")
```

HTML Living Standard (whatwg.org)

Authors should check the origin attribute to ensure that messages are only accepted from domains that they expect to receive messages from

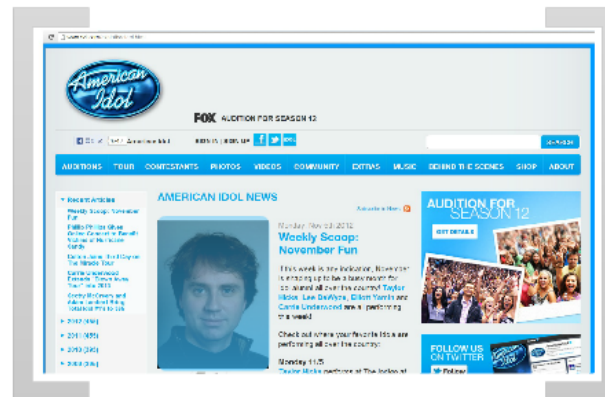
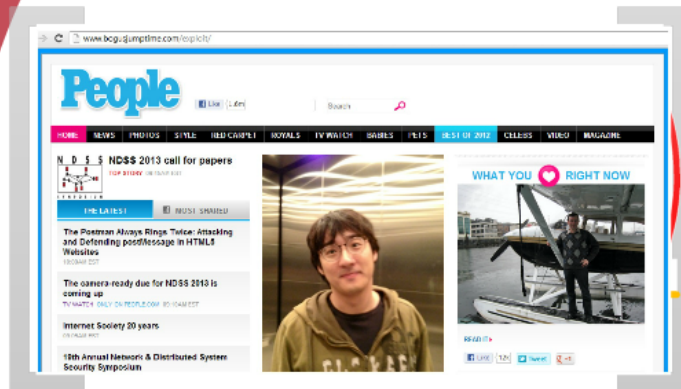
Why check the origin of received message?

<http://myOwnSite.com>

// No check
eval(received_msg);



And if the check is wrong?



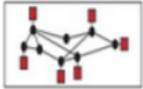
People

 Like 1.6m

Search 

HOME NEWS PHOTOS STYLE RED CARPET ROYALS TV WATCH BABIES PETS BEST OF 2012 CELEBS VIDEO MAGAZINE


NDSS NDSS 2013 call for papers



TOP STORY 09:45AM EST

SYMPOSIUM

THE LATEST

 MOST SHARED

The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites

10:00AM EST

The camera-ready due for NDSS 2013 is coming up

TV WATCH ONLY ON PEOPLE.COM 09:10AM EST

Internet Society 20 years

09:05AM EST

19th Annual Network & Distributed System Security Symposium



WHAT YOU RIGHT NOW



READ IT ▶

 Like 12k  Tweet  +1



FOX AUDITION FOR SEASON 12

좋아요 974만 American Idol

SIGN IN | SIGN UP



SEARCH

- AUDITIONS
- TOUR
- CONTESTANTS
- PHOTOS
- VIDEOS
- COMMUNITY
- EXTRAS
- MUSIC
- BEHIND THE SCENES
- SHOP
- ABOUT

Recent Articles

Weekly Scoop: November Fun

Phillip Phillips Gives Online Concert to Benefit Victims of Hurricane Sandy

Colton Joins Third Day on The Miracle Tour

Carrie Underwood Extends "Blown Away Tour" into 2013

Scotty McCreery and Adam Lambert Bring Total Idol #1's to 365

- ▶ 2012 (455)
- ▶ 2011 (455)
- ▶ 2010 (395)
- ▶ 2009 (395)

AMERICAN IDOL NEWS

Subscribe to News



Monday, Nov 5th 2012

Weekly Scoop: November Fun

If this week is any indication, November is shaping up to be a busy month for Idol alumni all over the country! Taylor Hicks, Lee DeWyze, Elliott Yamin and Carrie Underwood are all performing this week!

Check out where your favorite Idols are performing all over the country:

Monday 11/5 Taylor Hicks performs at The Indigo at

AUDITION FOR SEASON 12

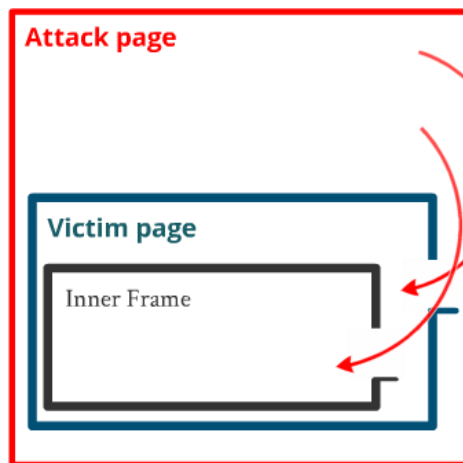
GET DETAILS

FOLLOW US ON TWITTER

Follow

- We collected postMessage receivers from Alexa top 10,000 sites
- **RvScope**: our tool for collecting receivers

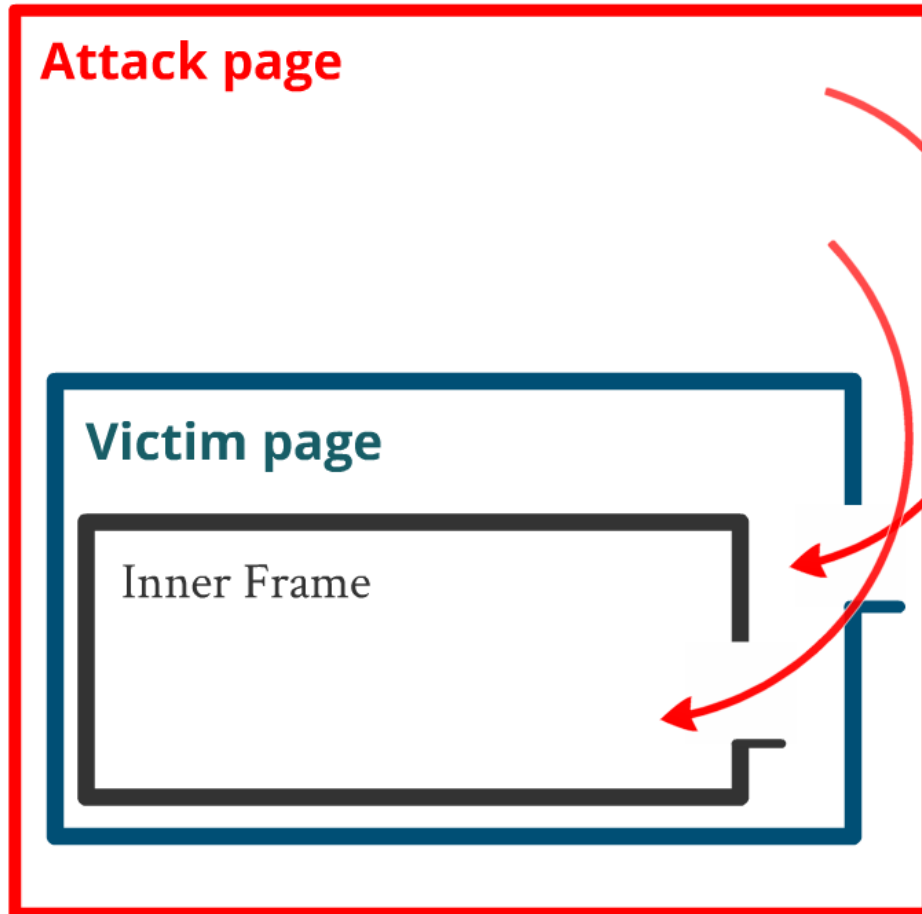
Attack page



X-Frame-Header could have prevented our attack...

... only 298 pages use X-Frame-Header among Alexa top 10,000

Attack page



X-Frame-Header could have prevented our attack...

... only 298 pages use X-Frame-Header among Alexa top 10,000



Incorrect origin checks

Origin check	Host name that passes the check	Existing domains
<code>if(/[\\ \\.]chartbeat.com\$/ .test(a.origin))</code>	evil.chartbeat-com	0
<code>if(m.origin.indexOf("sharethis.com") != -1)</code>	sharethis.comnet.com evilsharethis.com	2,291
<code>if(a.origin && a.origin.match(/\\.kissmetrics\\.com/))</code>	www.kissmetrics.comnet.com www.kissmetrics.com.evil.com	2,276
<code>var w = /jumptime\\.com(:[0-9]?\$/; if(!v.origin.match(w))</code>	bogusjumptime.com	2



<code>if(/[\\ \.]chartbeat.com\$/.test(a.origin))</code>	<code>evil.chartbeat-com</code>	0
<code>if(m.origin.indexOf("sharethis.com") != -1)</code>	<code>sharethis.comnet.com</code> <code>evilsharethis.com</code>	2,291
<code>if(a.origin && a.origin.match(/\.kissmetrics\.com/))</code>	<code>www.kissmetrics.comnet.com</code> <code>www.kissmetrics.com.evil.com</code>	2,276
<code>var w = /jumptime\.com(:[0-9]?\$/; if(!v.origin.match(w))</code>	<code>bogusjumptime.com</code>	2



Exploitable receivers				
No	Hosts	Number	Vulnerability	Cause
1	www.sfgate.com, www.instyle.com, www.timesunion.com, www.nbcnews.com, www.ew.com, www.nyrecipen.com, www.ctpost.com, www.7up.com, www.metro.co.uk, msn.foxsports.com, www.ladygaga.com, www.rosemix.com, www.wholefoodsmarket.com, www.sundrop.com, www.fox.com	20	Attacker can inject scripts (cross-site scripting)	Missing check
2	www.southparkstudios.com, www.teennick.com	1	leaking the types of	check
3	www.xsxy.net, www.readnovel.com, www.qidian.com, www.rongshuxia.com, www.juchang.com, club.ku6.com, g.aa.sdo.com	7	Attacker can inject scripts (cross-site scripting)	Missing check
4	www.cnn.com, www.roblox.com, www.turkmedya.tv, www.dailytech.com, www.kariyerhaber.com	5	Attacker can inject scripts (cross-site scripting)	Missing check
5	www.ieee.org, www.canalplus.fr, pass.canal-plus.com	3	Attacker can inject scripts (cross-site scripting)	Incorrect check
6	www.yourki.com, www.wvsi.com, www.geocities.com, www.overstock.com	2	Attacker can inject scripts (cross-site scripting)	Missing check
7	www.userreport.com, tag.userreport.com	2	Attacker can read and write any key/value into local storage	Missing check
8	www.wack.com	1	Attacker can inject scripts (cross-site scripting)	Missing check
9	www.sports.com, www.fox.com, www.fox.com, www.fox.com	1	Attacker can read the user's cookie address in the cookies	Missing check

Conditionally exploitable receivers				
No	Hosts	Number	Vulnerability	Cause
10	www.fanpop.com, www.webshots.com, www.theforce.com, www.self.com, www.wired.com, www.fox.com, www.fox.com, www.fox.com, www.stylc.com, www.glamour.com, www.wowwiki.com, www.vanityfair.com, www.gq.com, fls.doubleclick.net, www.sidereel.com, www.sodahead.com	16	Attacker can inject scripts (cross-site scripting) if the victim site has an element with "LOI(CC.status" id	Missing check

XSS
Reading cookies
Reading/writing arbitrary values into Web localStorage

Lessons

Perform correct checks on the origin of received messages

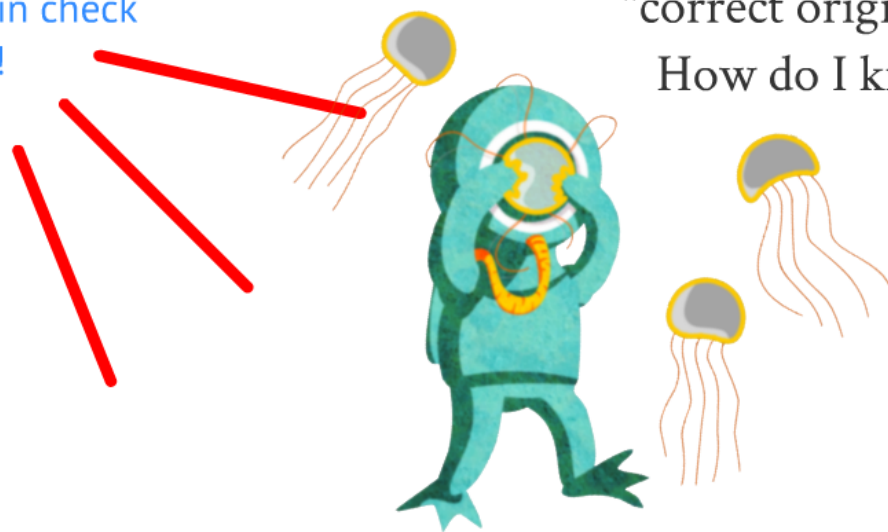


Put a correct origin
check in every receiver!



the origin of rece

Put a correct origin check
in every receiver!



"correct origin"?

How do I know what origin to check ?

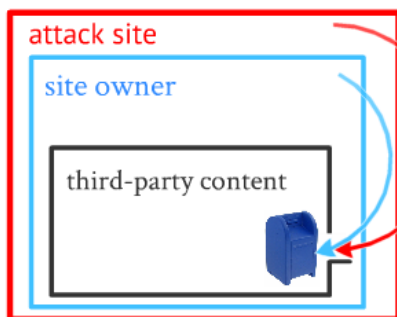
Content provider

Put a correct origin
check in every receiver!



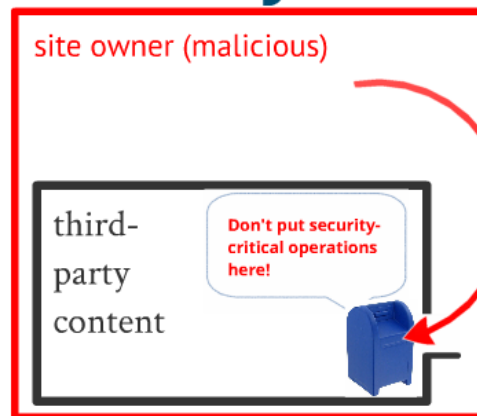
Threat models

Light threat model



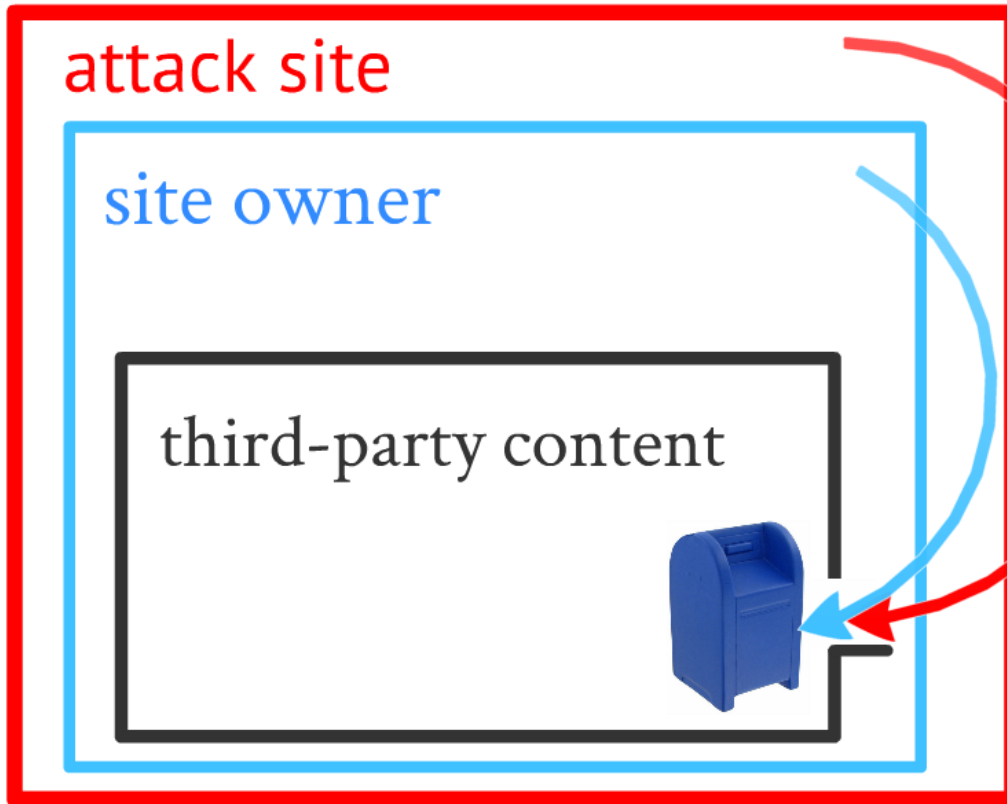
- Site owner is honest.
- The receiver in third-party content should accept messages only from site owner's origin.

Heavy threat model



- Site owner is **malicious**.
- Site owner abuses a receiver in third-party content

Light threat model



- Site owner is honest.
- The receiver in third-party content should accept messages only from site owner's origin.

Heavy threat model

site owner (malicious)



- Site owner is **malicious**.
- Site owner abuses a receiver in third-party content

Defenses

1. Origin-based defense



2. Frame-based defense



3. CSP extension



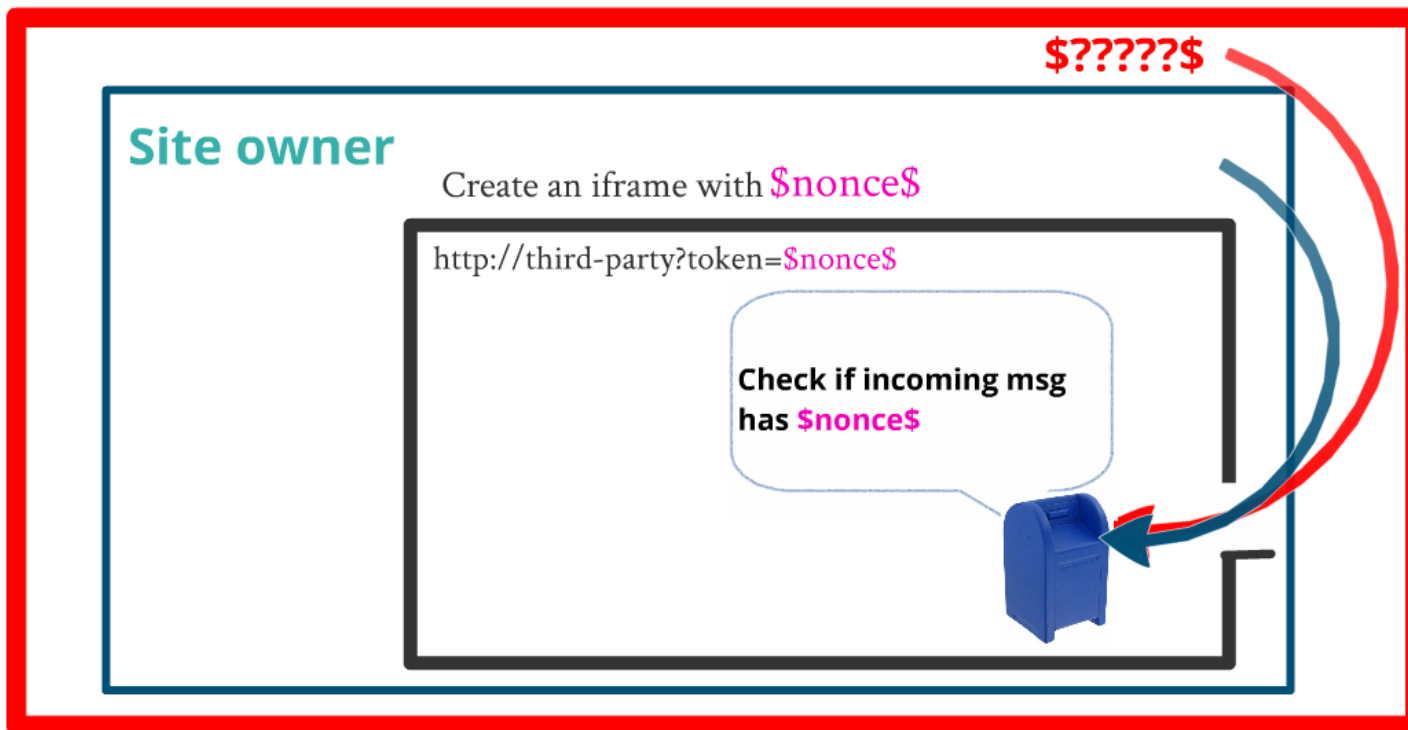
Lessons

Perform correct checks on the origin of received messages



Origin-based defense with a shared token

- Defense for third-party content
- Works against the "light" threat model



Defenses

1. Origin-based defense



2. Frame-based defense



3. CSP extension



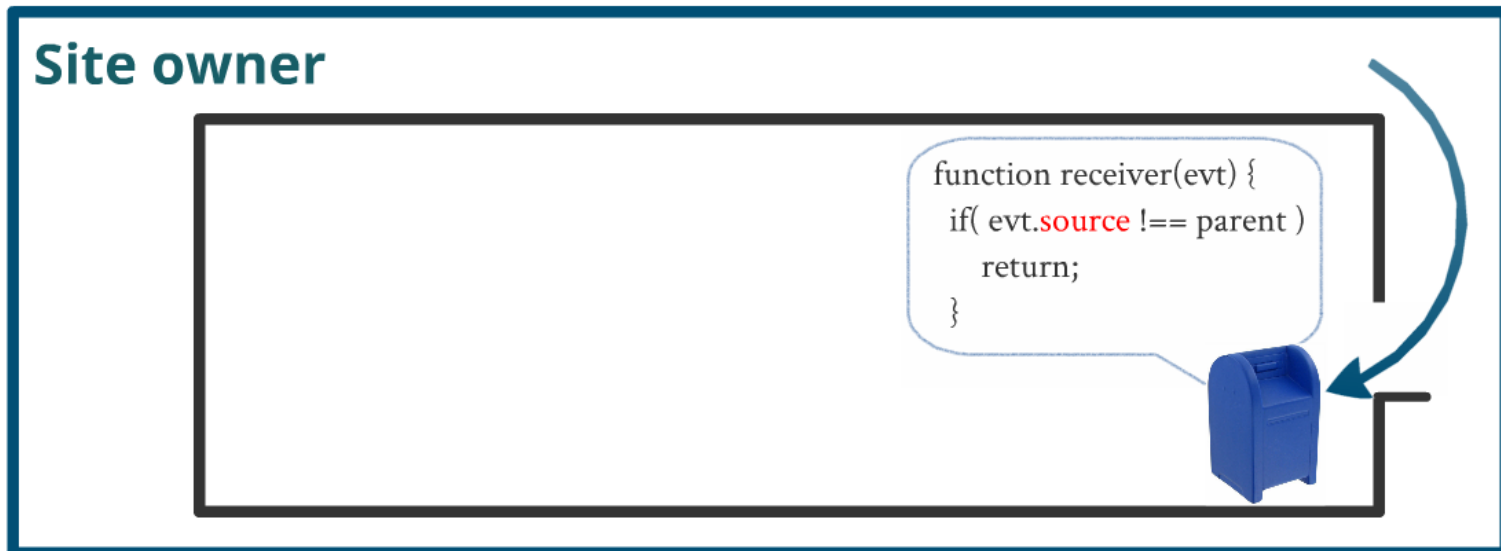
Lessons

Perform correct checks on the origin of received messages



Frame-based Defense

- Defense for third-party content
- Works against the "light" threat model



Works against the "light" threat model

Site owner

```
function receiver(evt) {  
  if( evt.source !== parent )  
    return;  
}
```



Defenses

1. Origin-based defense



2. Frame-based defense



3. CSP extension



Lessons

Perform correct checks on the origin of received messages



Extended Content Security Policy (CSP)

- Defense for site owners
- Explicitly restricts origins of received messages
- Requires browser support

X-Content-Security-Policy:

msg-src <http://www.valid.com> *.edu;

Accept postMessage only from
<http://www.valid.com> or *.edu

Defenses

1. Origin-based defense



2. Frame-based defense



3. CSP extension



Lessons

Perform correct checks on the origin of received messages



Q & A