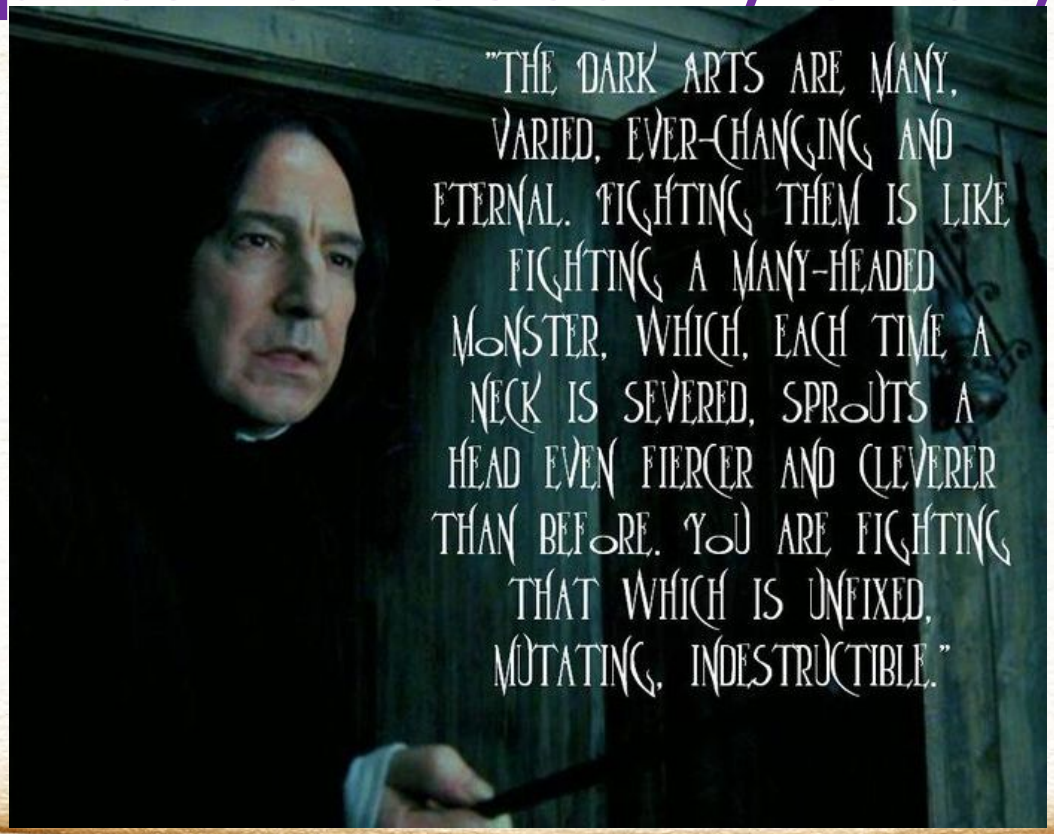
Defense Against The Dark Arts: Application security and you



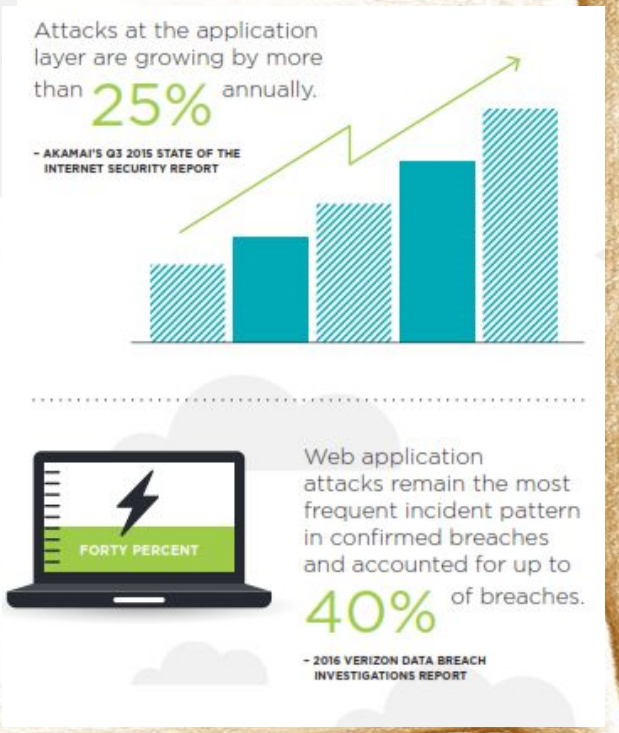
https://uk.pinterest.com/pin/335518240961936792/

Joe Kuemerle

- Application security engineer & developer in a broad range of technologies
- Specialize in application and data security, coding best practices and regulatory compliance
- Presenter at community, regional and national events.

@jkuemerle / www.kuemerle.com

https://proftalon.smugmug.com/Hogwarts/2914-summer/i-v4tSLNL/A



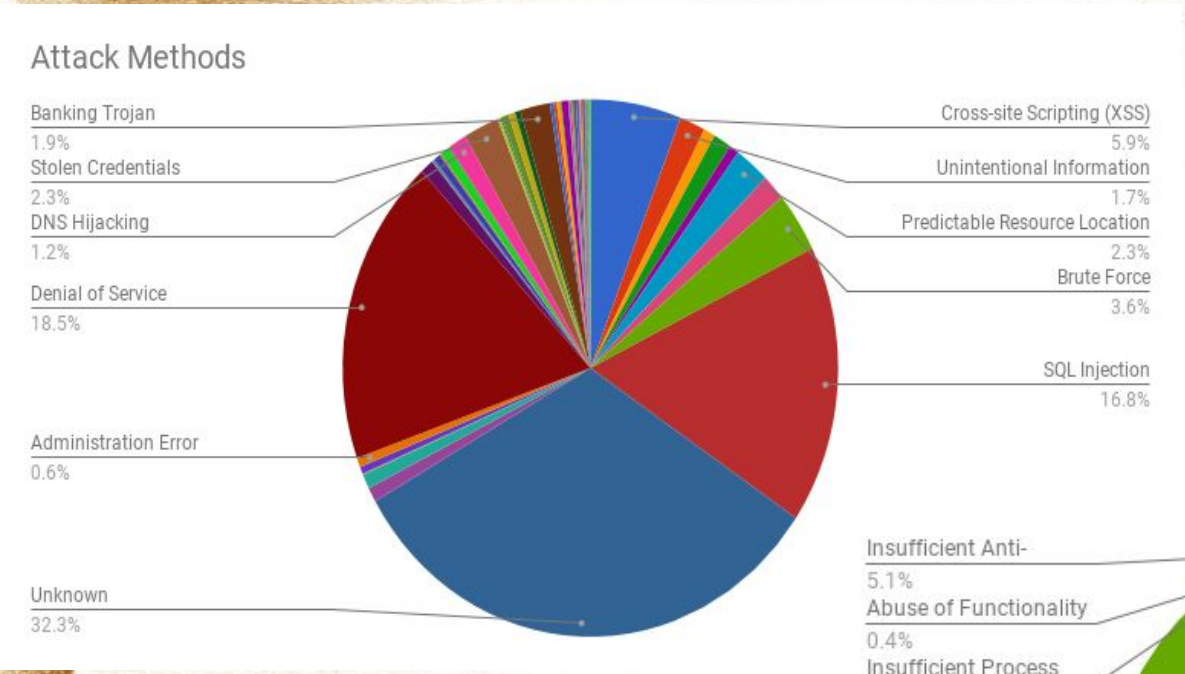
https://www.veracode.com/resources

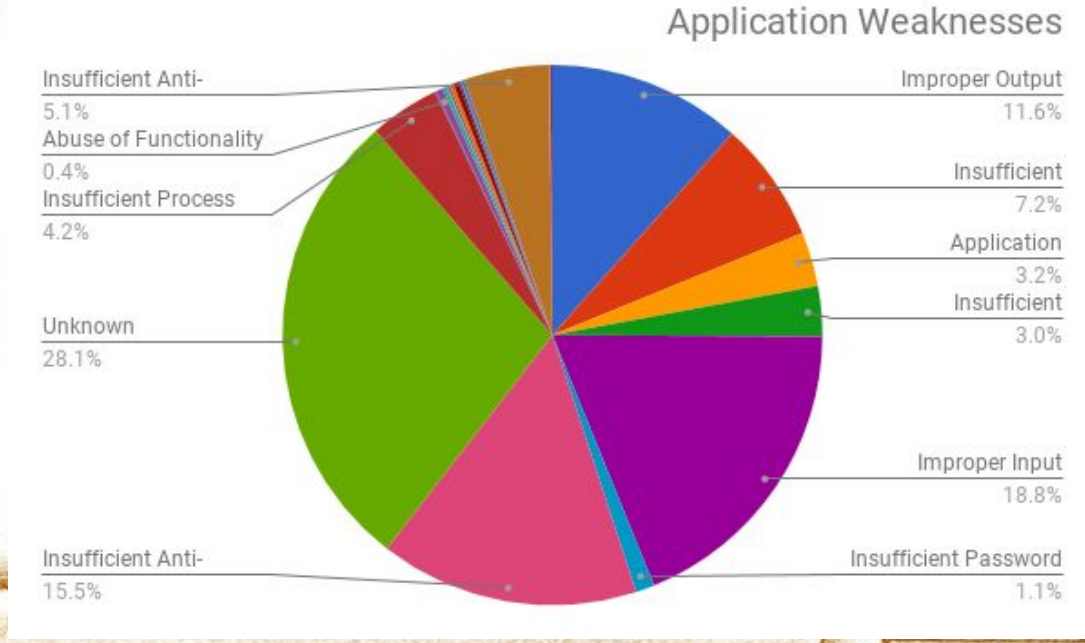
www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

http://cdn.quotesgram.com/small/79/88/1743520670-top-10.jpg

https://www.owasp.org/index.php/Top_10-2017_Top_10

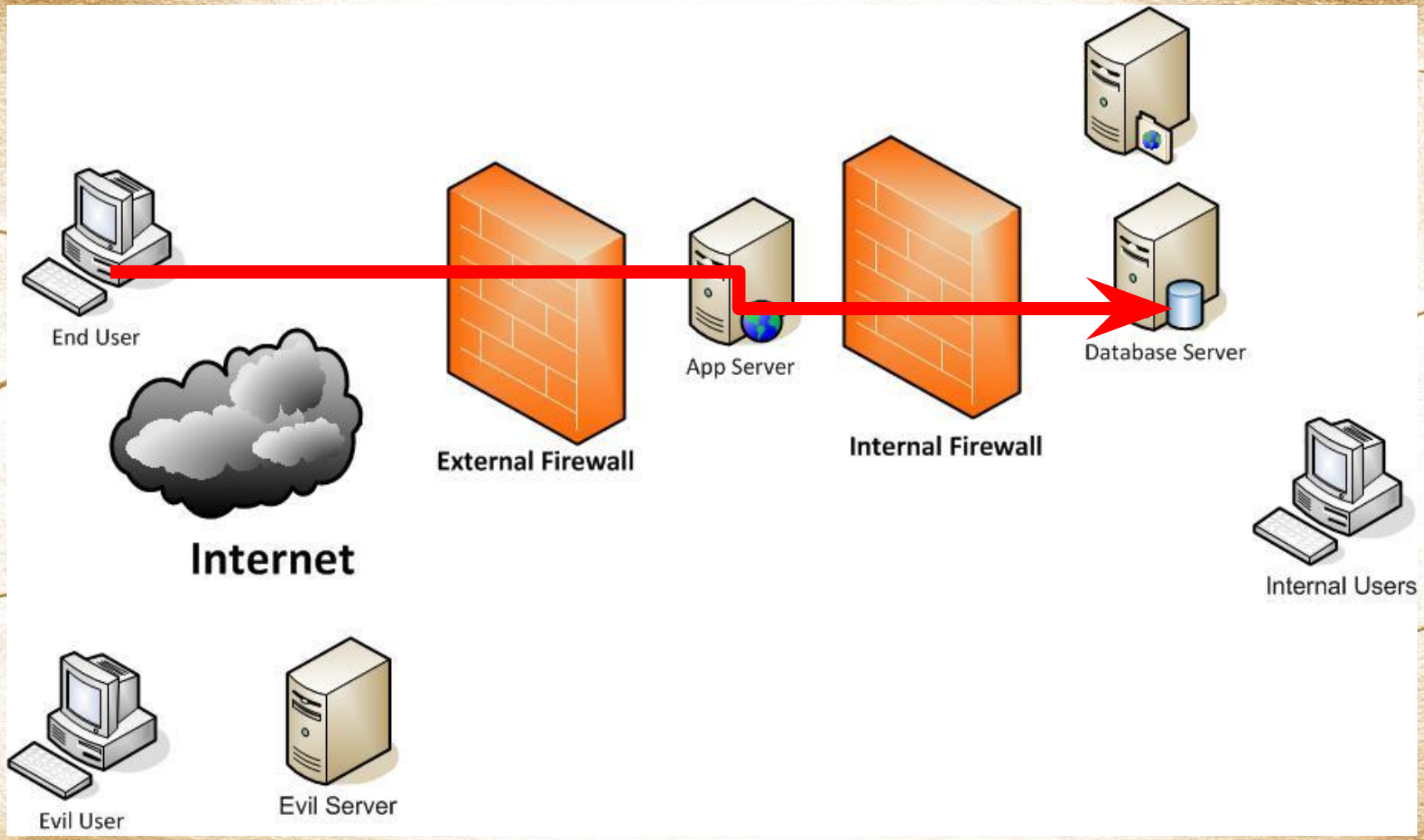
- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Components With Known Vulnerabilities
- Insufficient Logging and Monitoring



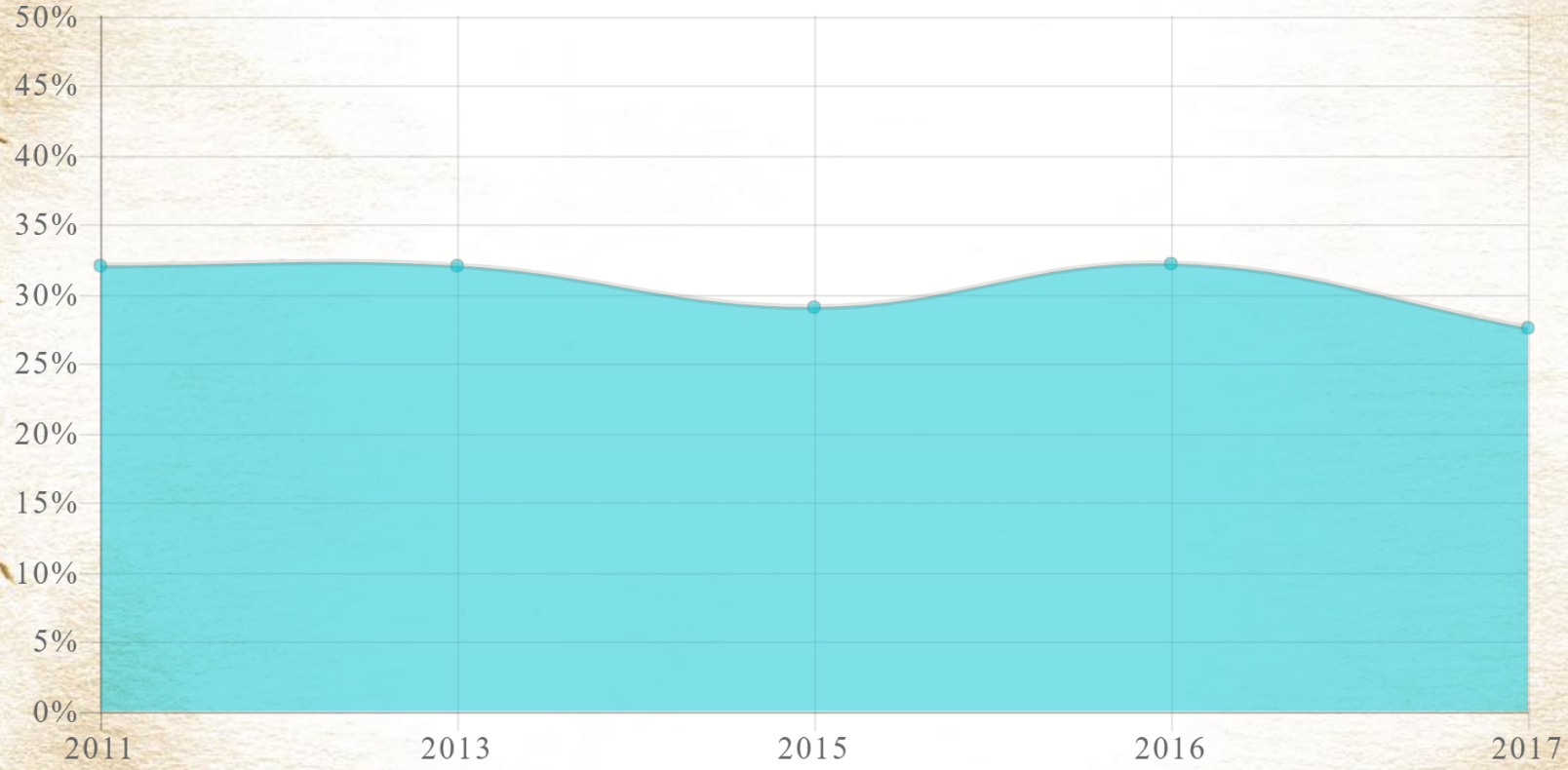


Source:
Web Hacking Incident Database
http://tinyurl.com/AppAttackStats

https://www.flickr.com/photos/colmmcsky/6300431678/



SQL INJECTION TREND
Percentage of Applications Affected



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

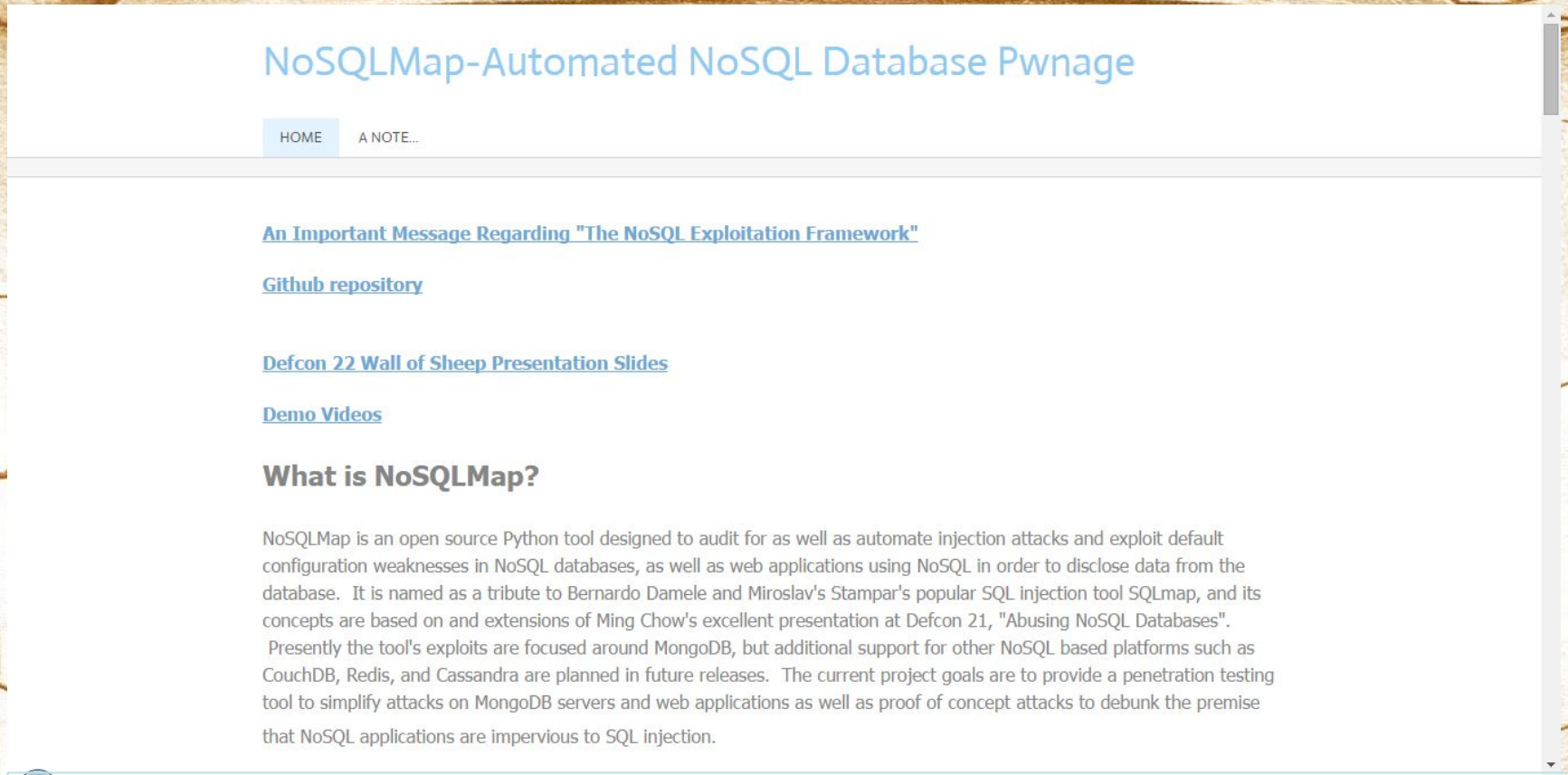
https://codecurmudgeon.com/wp/sql-injection-hall-of-shame/

Company	Date	Results	Reference
IIT-Delhi	2018-03	potential access to student data	Kerala youth picks security flaw in IIT-Delhis web server
BSNL	2018-03	47,000 employees data taken by hacker to prove problem. Second time for this site in 2 years. Fixed.	Security researcher hacks BSNL intranet, leaks details of 47,000 employees
Telangana NREGA portal (India)	2018-02	hack exposed data to show security flaw	Hacker exposes major security flaw in Telangana governments NREGA website
Joomla	2018-02	Joomla CMS sqli bugs (patch available)	Joomla 3.2.4 release addresses three XSS and SLI Injection vulnerabilities
Zoho	2018-01	Helpdesk software vulnerable to blind SQLi	Multiple critical flaws found in Zoho MANAGEENGINE
Hetzner South Africa	2017-11	Over 40,000 customer details including bank accounts leaked.	Hetzner hack - top south african web host hit
Wordpress	2017-10	SQLi vulnerability in plugins - patched in v4.8.3	If your websites use WordPress, put down that coffee and upgrade to 4.8.3
GoDaddy	2017-10	Researcher showed site security tool is easily bypassed to allow sqli	This bug let a researcher bypass GoDaddy's site security tool
Inmarsat	2017-10	AmosConnect satellite communications for ships is vulnerable.	mosConnect: Maritime Communications Security Has Its Flaws
Equifax	2017-10 (long term)	Personal data for over 145 million people compromised	Equifax was warned
Jigsaw Holding in South Africa	2017-10	75m database records available for download	Revealedthe real source of SAs massive data breach
Catholic United Financial	2017-10	personal info for over 130k users.	Data breach at Arden Hills-based Catholic financial services provider affects nearly 130k accounts
BPC Banking - SmartVista software	2017-10	numerous vulnerable ecommerce sites	Vendor BCP Baking Silent on Patching SQL Injection in SmartVista Ecommerce Software
EMC	2017-07	multiple vulnerabilities found, some fixed.	EMC products hit by multiple vulnerabilities including SQL injection
Wordpress Statistics plugin	2017-07	vulnerability in wordpress plugin	SQL injection vulnerability found in popular WordPress plugin, again
Siemens	2017-06	vulnerability in AMT industrial products patched after CERT warning	Siemens patches critical Intel AMT flaw in industrial products
Illinois State Board of Elections	2017-06	voter registration system breached - reported in 2017-06 but occurred in 2016	Illinois chapter in the Russian hacking saga
Peplink	2017-06	vulnerable routers - now patched	Peplink patches SD-WAN routers

4.8 Million parents
6.3 Million children

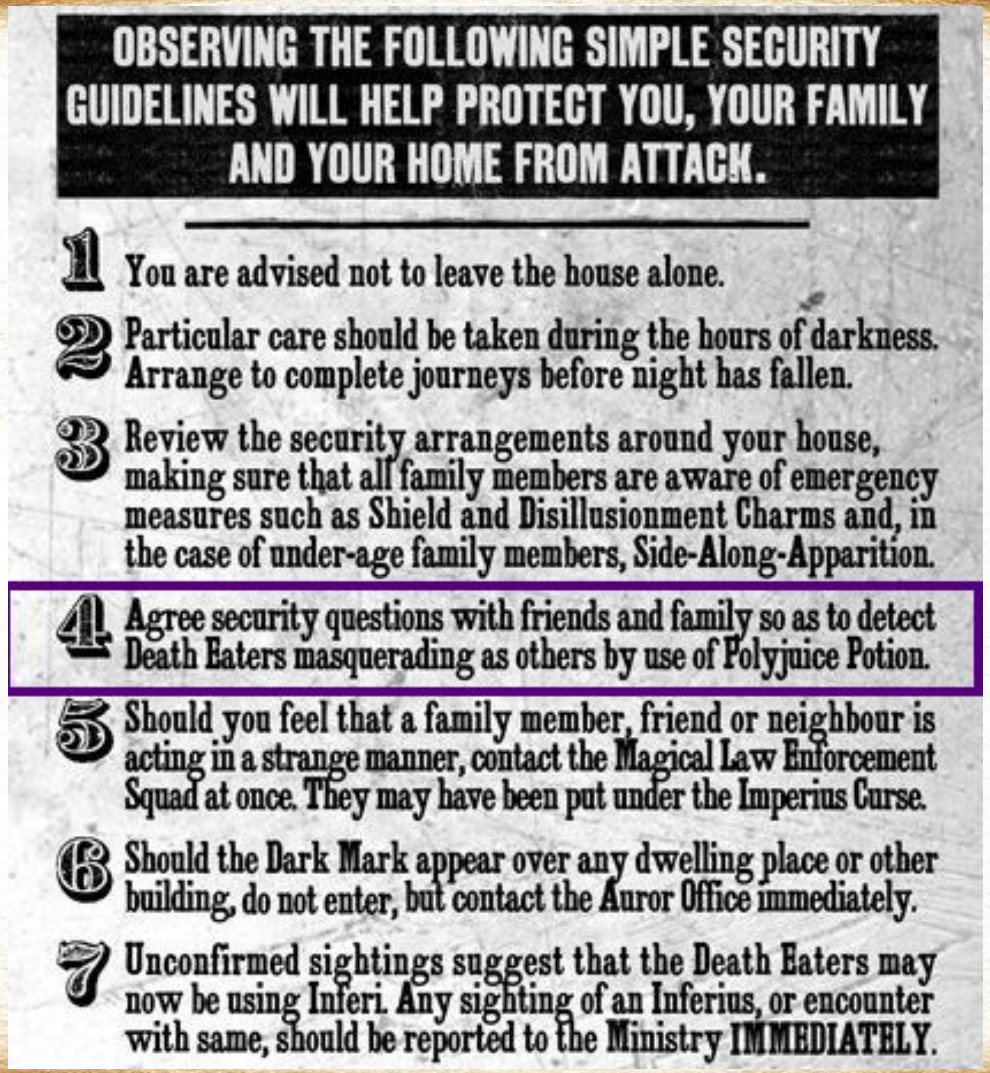
http://motherboard-images.vice.com/content-images/article/28241/1448640227075896.jpg

```
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
        is_avatar_created
          false
```




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

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



OBSERVING THE FOLLOWING SIMPLE SECURITY GUIDELINES WILL HELP PROTECT YOU, YOUR FAMILY AND YOUR HOME FROM ATTACK.

1. You are advised not to leave the house alone.
2. Particular care should be taken during the hours of darkness. Arrange to complete journeys before night has fallen.
3. Review the security arrangements around your house, making sure that all family members are aware of emergency measures such as Shield and Disillusionment Charms and, in the case of under-age family members, Side-Along-Apparition.
4. Agree security questions with friends and family so as to detect Death Eaters masquerading as others by use of Polyjuice Potion.
5. Should you feel that a family member, friend or neighbour is acting in a strange manner, contact the Magical Law Enforcement Squad at once. They may have been put under the Imperius Curse.
6. Should the Dark Mark appear over any dwelling place or other building, do not enter, but contact the Auror Office immediately.
7. Unconfirmed sightings suggest that the Death Eaters may now be using Inferi. Any sighting of an Inferius, or encounter with same, should be reported to the Ministry IMMEDIATELY.

https://www.pinterest.com/pin/785315872270483328/

https://www.flickr.com/photos/foilman/27016860369/

@jkuemerle / www.kuemerle.com

https://haveibeenpwned.com/

412	8,513,925,254	103,309	123,092,693
pwned websites	pwned accounts	pastes	paste accounts

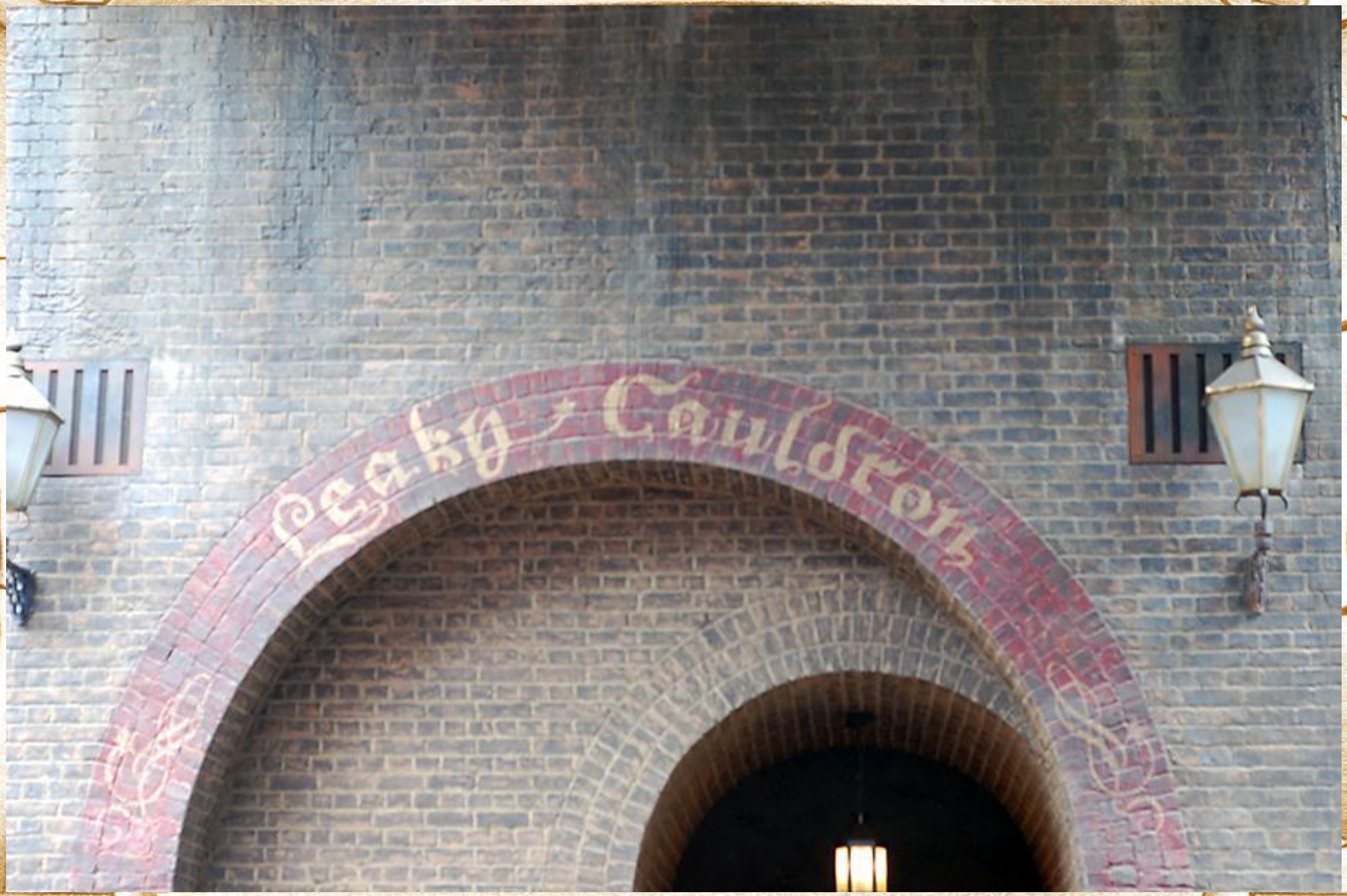
Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts

Recently added breaches

6,002,694	ToonDoo accounts
686,899	Vedantu accounts
290,955	Hookers.nl accounts
71,407	Zooville accounts
988,230	StreetEasy accounts
780,073	Sephora accounts
23,165,793	Wanelo accounts
15,453,048	Lumin PDF accounts
4,606	KiwiFarms accounts
396,533	Minehut accounts

https://www.flickr.com/photos/bryanalexander/17611523750/



https://www.flickr.com/photos/rdh-photo/36725534450/

@jkuemerle / www.kuemerle.com

https://www.flickr.com/photos/yaketyyakyak/73259939128/

@jkuemerle / www.kuemerle.com

https://graph.facebook.com/1138975844

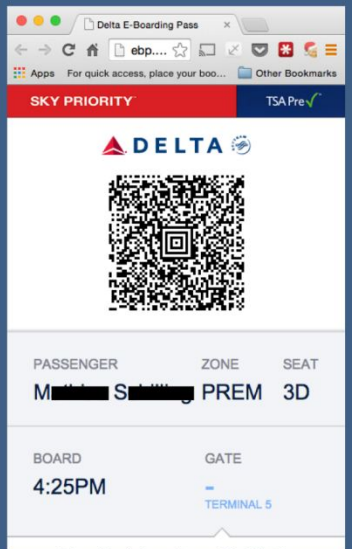
That's me, obviously.


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


https://graph.facebook.com/1138975845

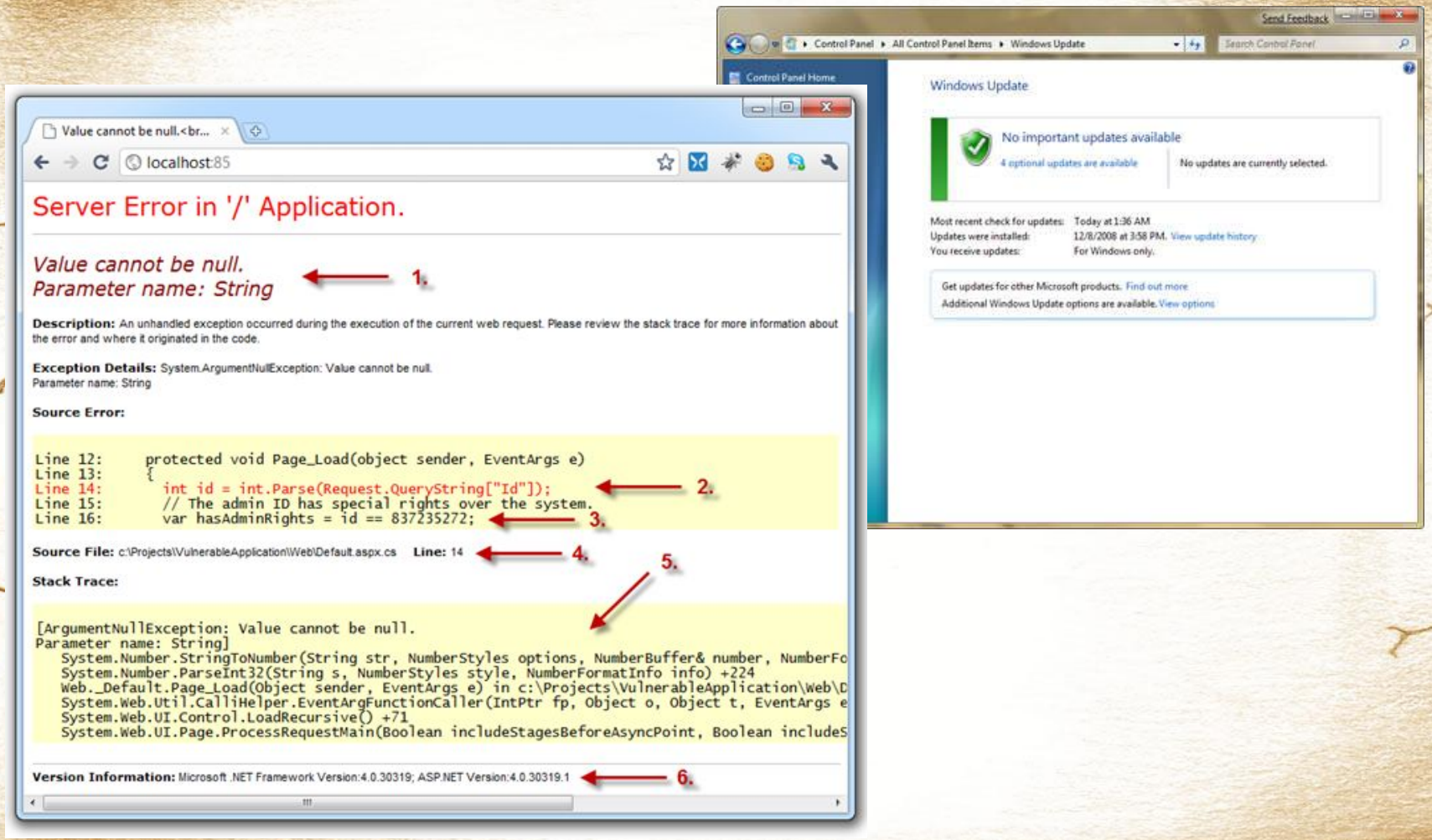
That could get interesting.


```
{
   "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"
}
```

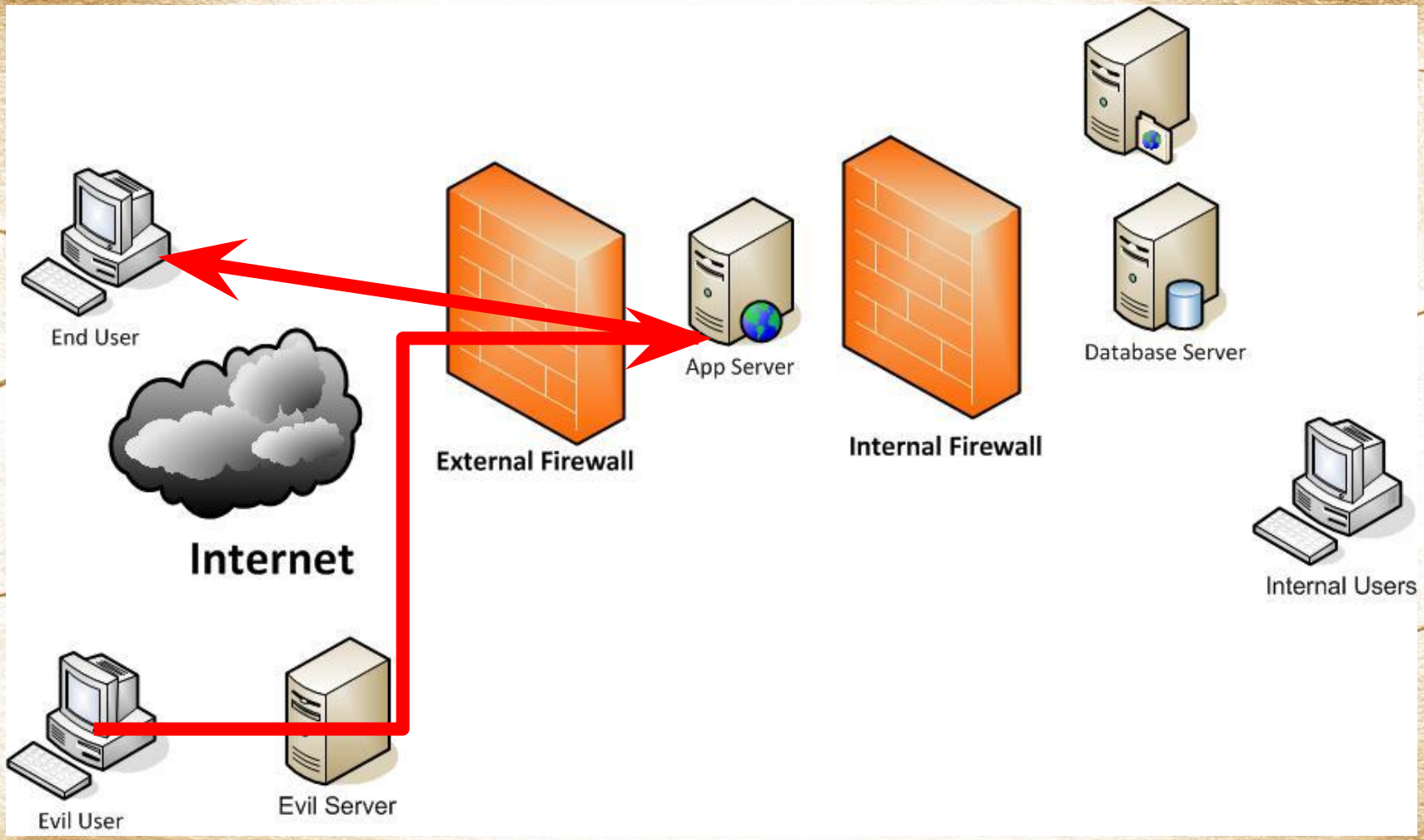



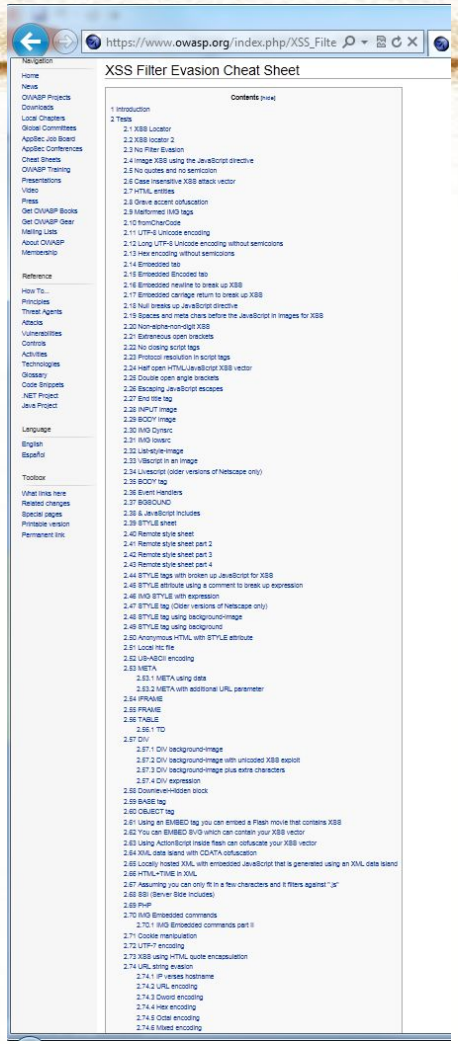
http://www.itnews.com.au/News/398892,delta-site-flaw-lets-passengers-access-other-boarding-passes.aspx

https://www.flickr.com/photos/saeru/872702709/



https://www.pinterest.com/pin/299911656412432748/





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

https://www.flickr.com/photos/yaketyyakyak/7306685420/

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

p-value = 0.441

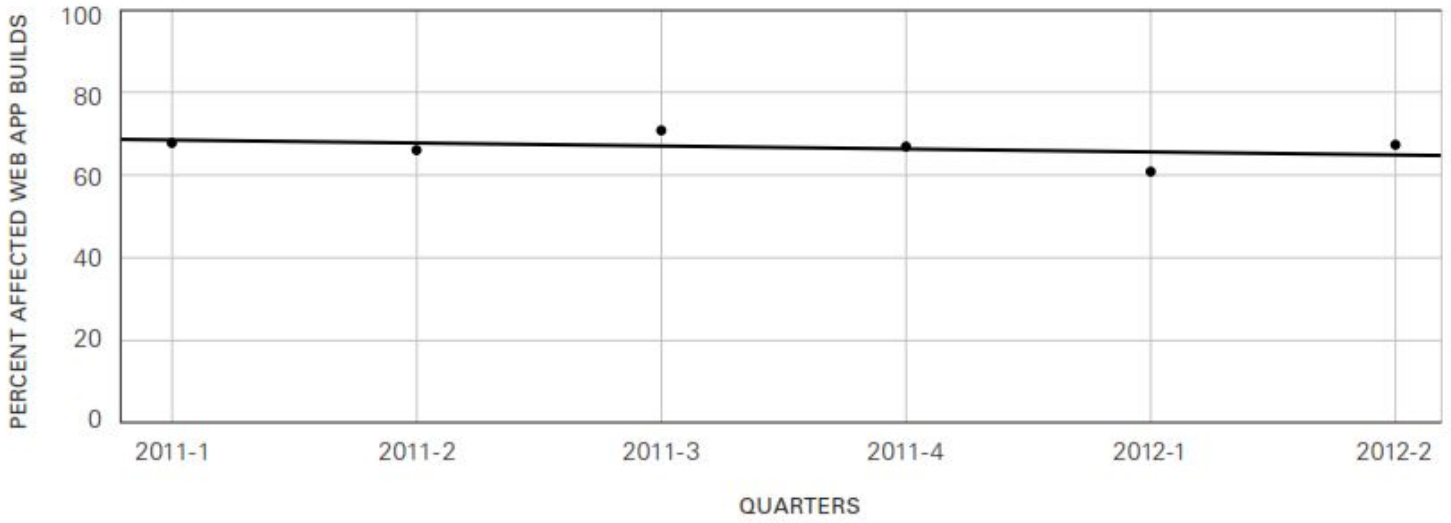


Figure 27: Quarterly Trend for Cross-Site Scripting (XSS) Prevalence (Percentage of Affected Web Applications)

Vulnerability Prevalence in ColdFusion Applications (Percentage of Applications Affected)

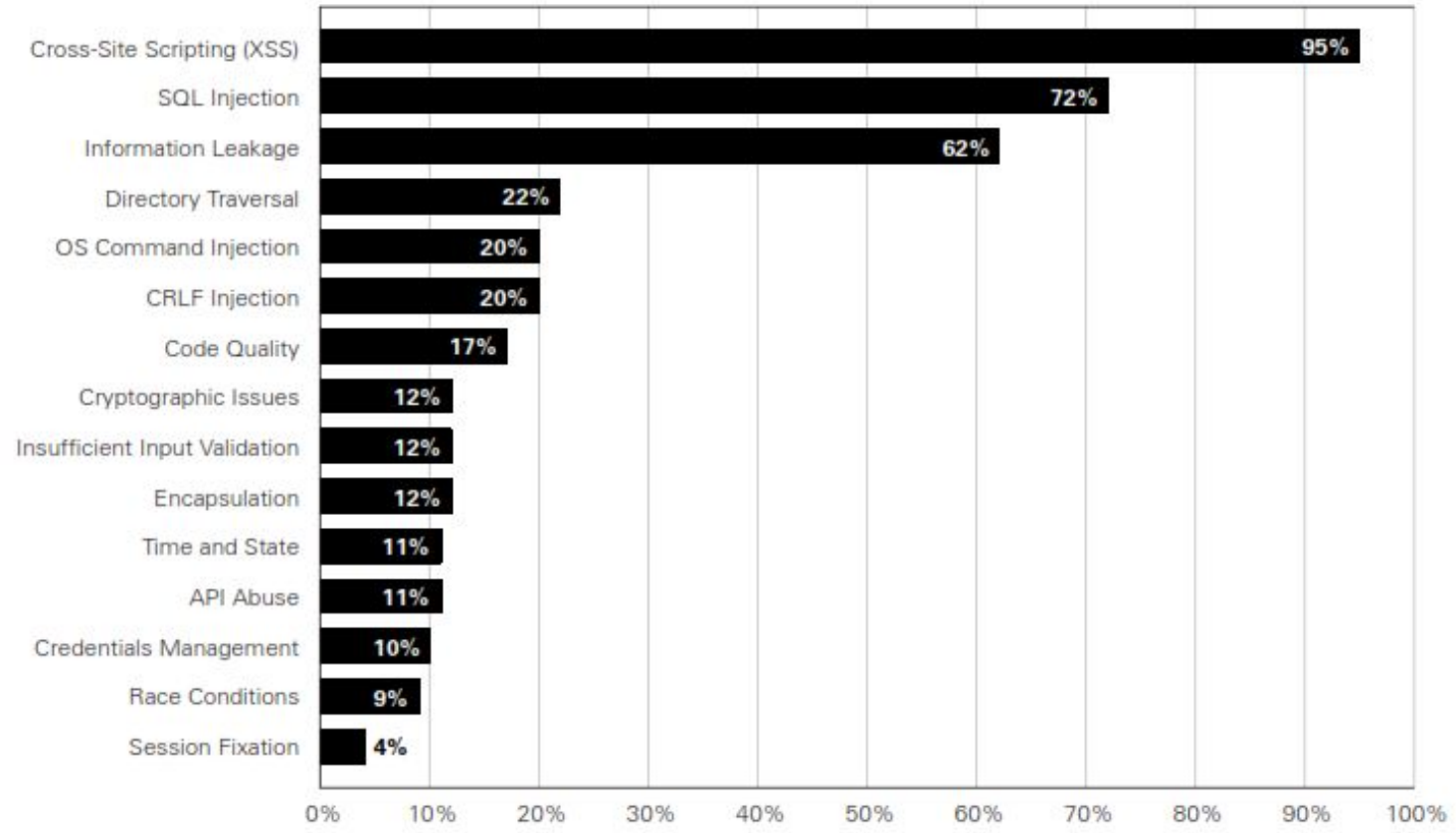
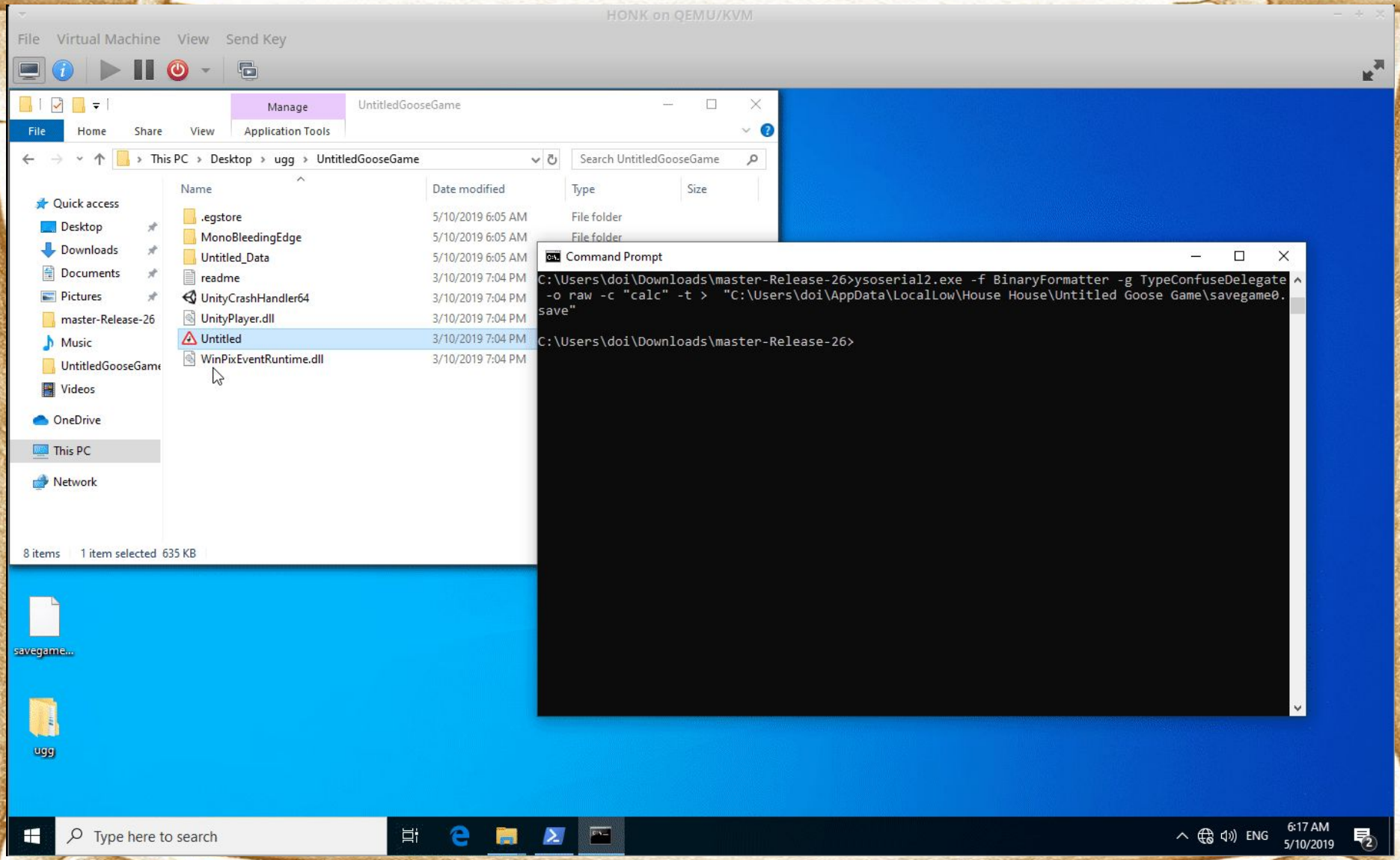


Figure 19: Vulnerability Prevalence in ColdFusion Applications (Percentage of Applications Affected)

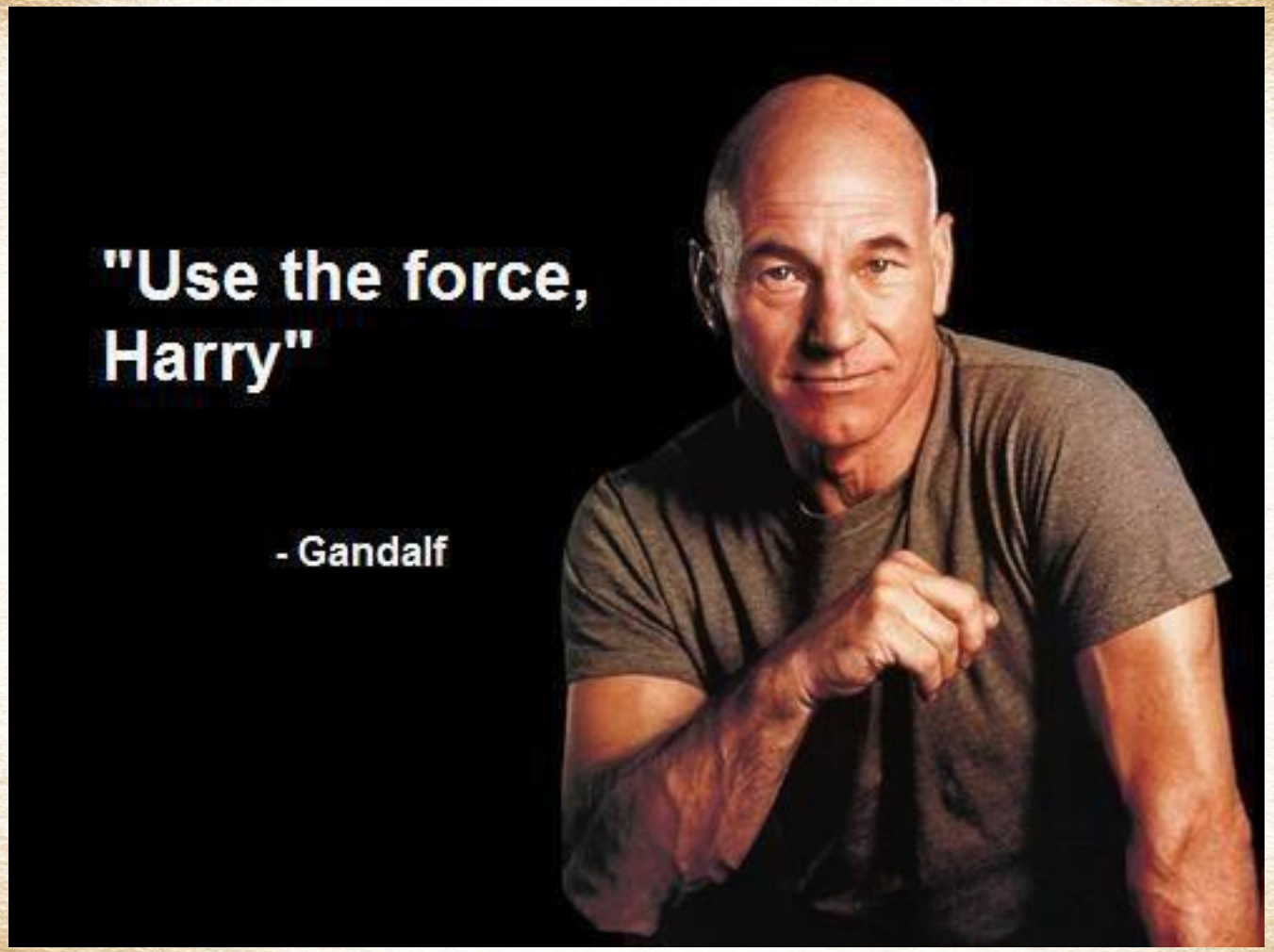
https://www.flickr.com/photos/20656268@N00/2094726257



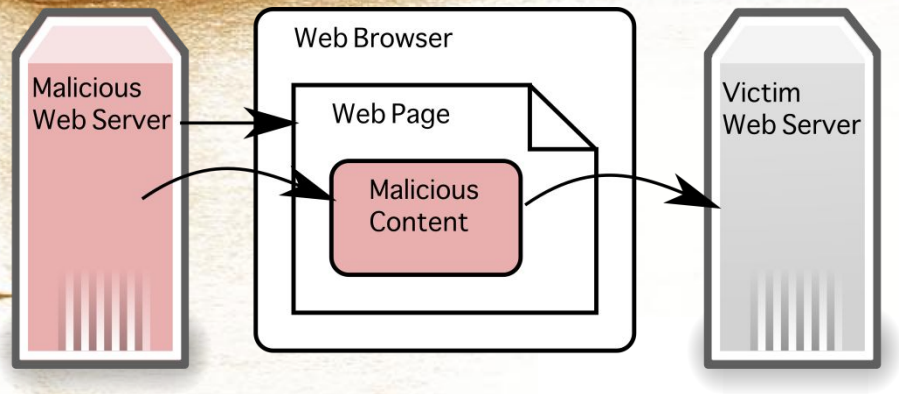
https://www.flickr.com/photos/justinhoch/5417977222/

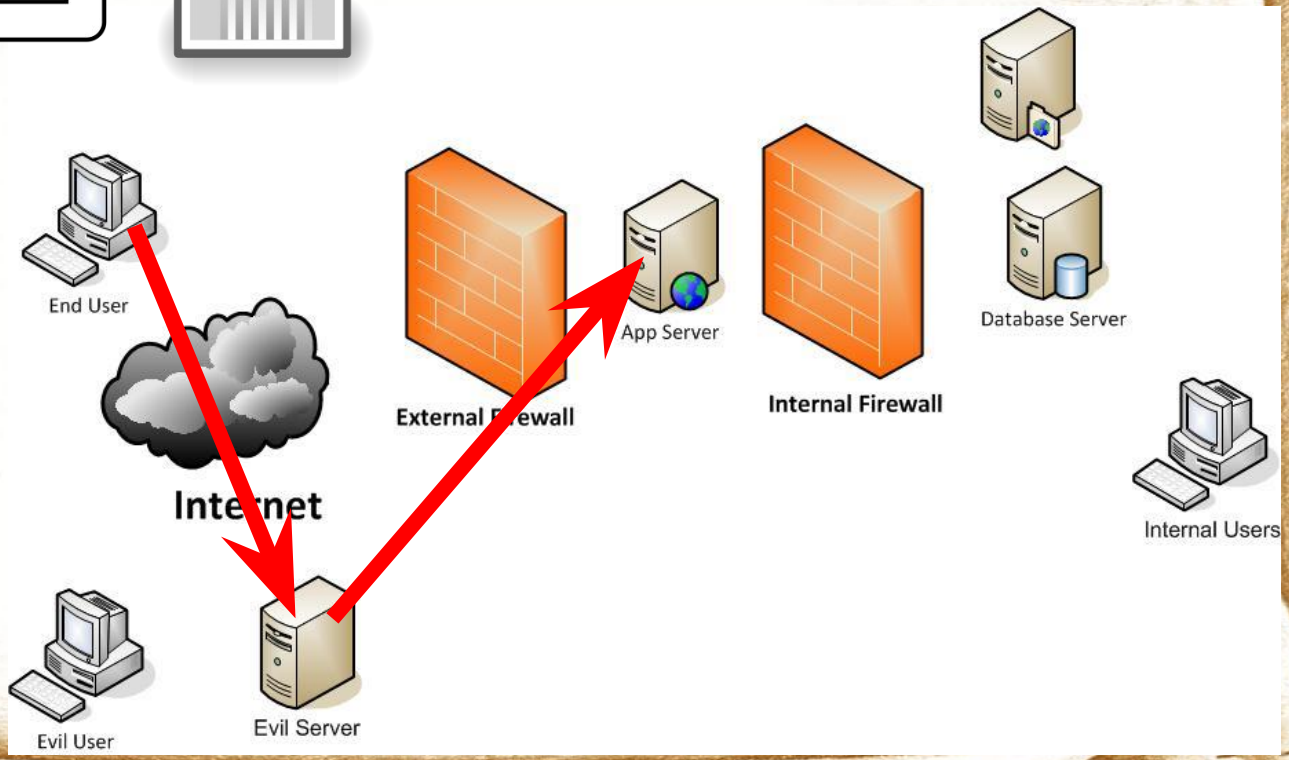
https://www.flickr.com/photos/pheezy/3769080979/

https://www.flickr.com/photos/foilman/38557740656/



https://www.pinterest.com/pin/481885228855703308/





www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Components With Known Vulnerabilities
- Insufficient Logging and Monitoring

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

M1 - Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2 - Insecure Data Storage	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management
M5 - Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
M6 - Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.
M7 - Client Code Quality	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
M8 - Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
M9 - Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
M10 - Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

Vulnerability Distribution for Mobile Platforms (Share of Total Vulnerabilities Found)

Android		iOS		Java ME	
CRLF Injection	37%	Information Leakage	62%	Cryptographic Issues	47%
Cryptographic Issues	33%	Error Handling	20%	Information Leakage	47%
Information Leakage	10%	Cryptographic Issues	7%	Directory Traversal	3%
SQL Injection	9%	Directory Traversal	6%	Insufficient Input Validation	2%
Time and State	4%	Buffer Management Errors	3%	Credentials Management	<1%

Figure 20: Vulnerability Distribution for Mobile Platforms (Share of Total Vulnerabilities Found)

Android Vulnerability Prevalence (Percentage of Applications Affected)

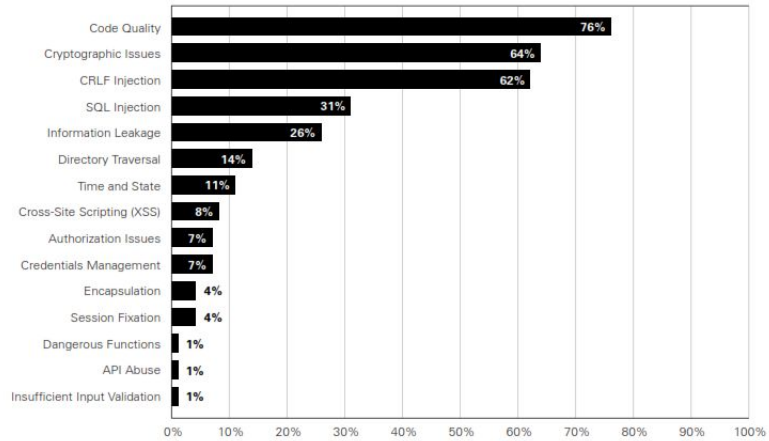


Figure 21: Android Vulnerability Prevalence (Percentage of Applications Affected)

iOS (ObjectiveC) Vulnerability Prevalence (Percentage of Applications Affected)

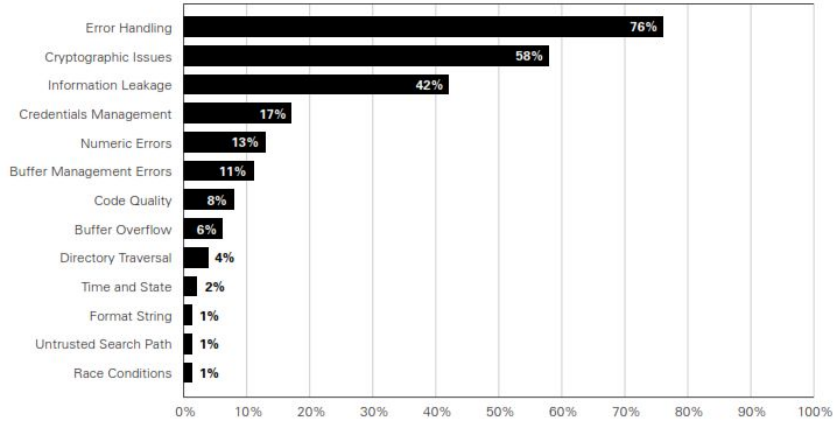
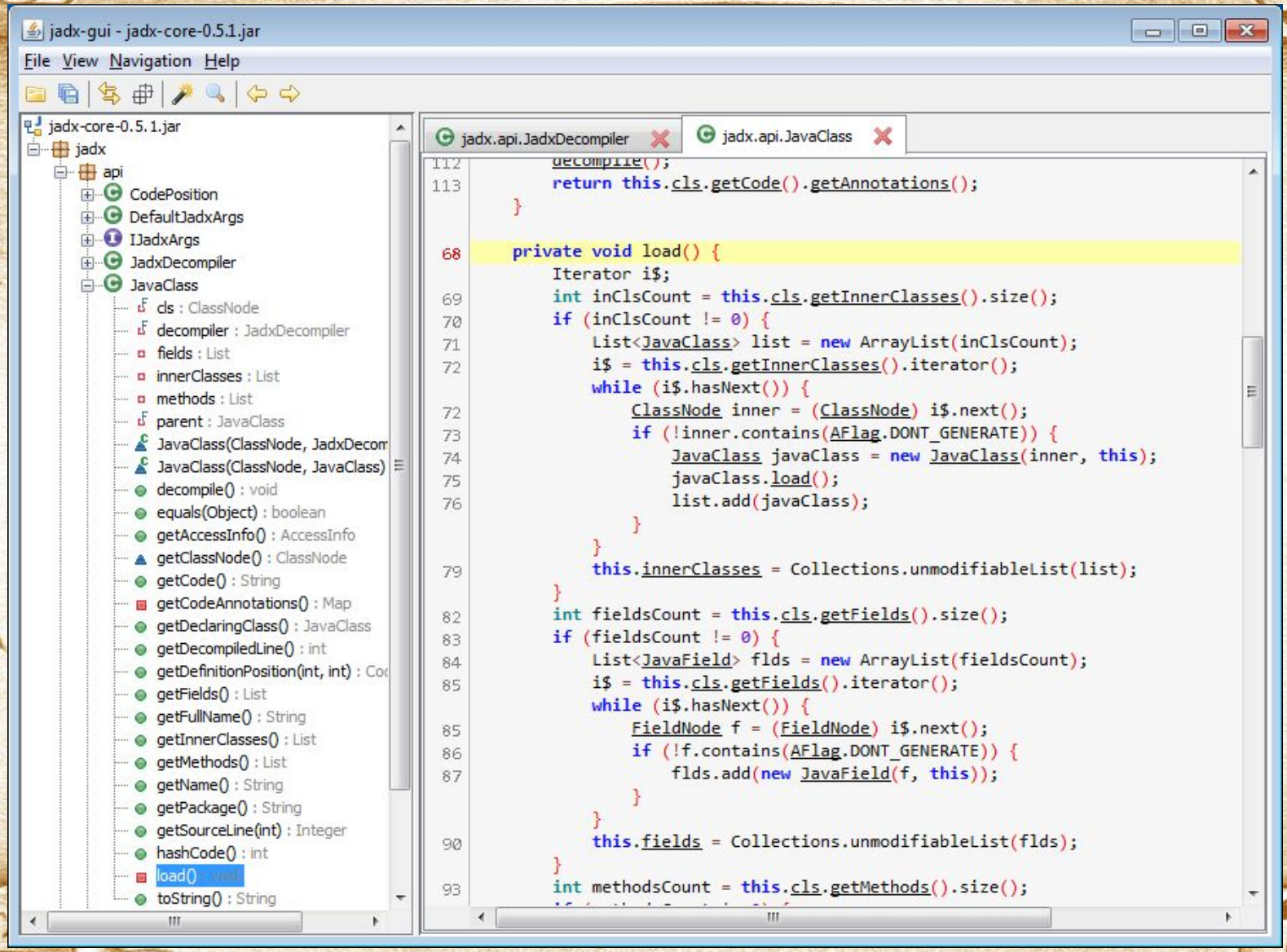
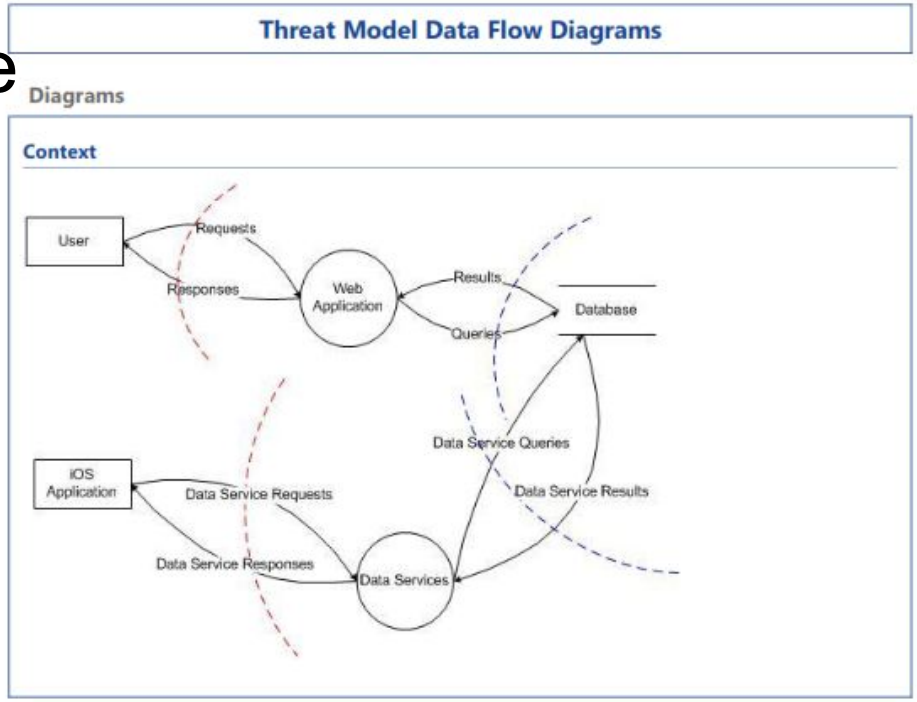


Figure 22: iOS (ObjectiveC) Vulnerability Prevalence (Percentage of Applications Affected)

https://github.com/skylot/jadx



Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege



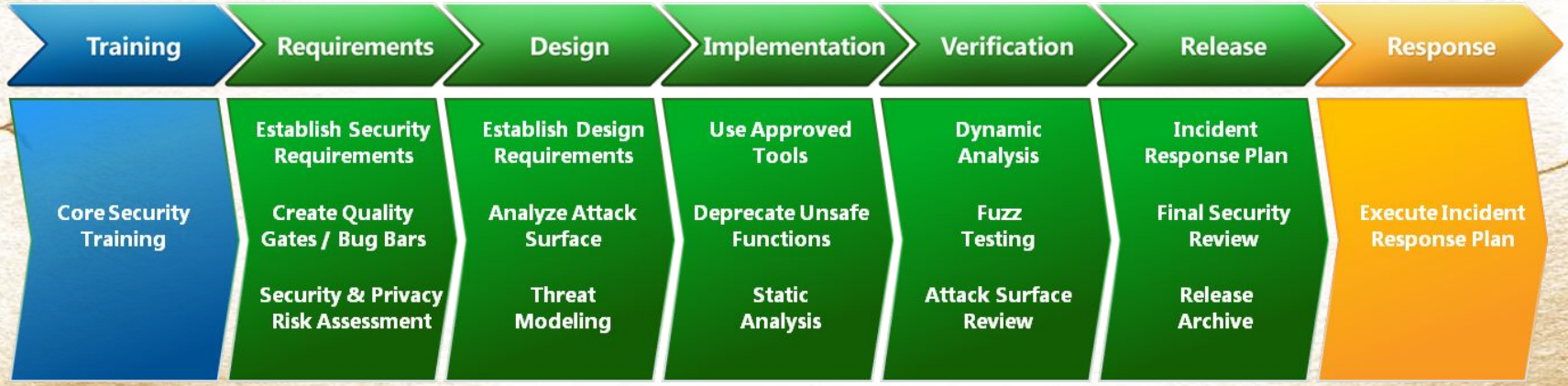
Microsoft | Security Blog

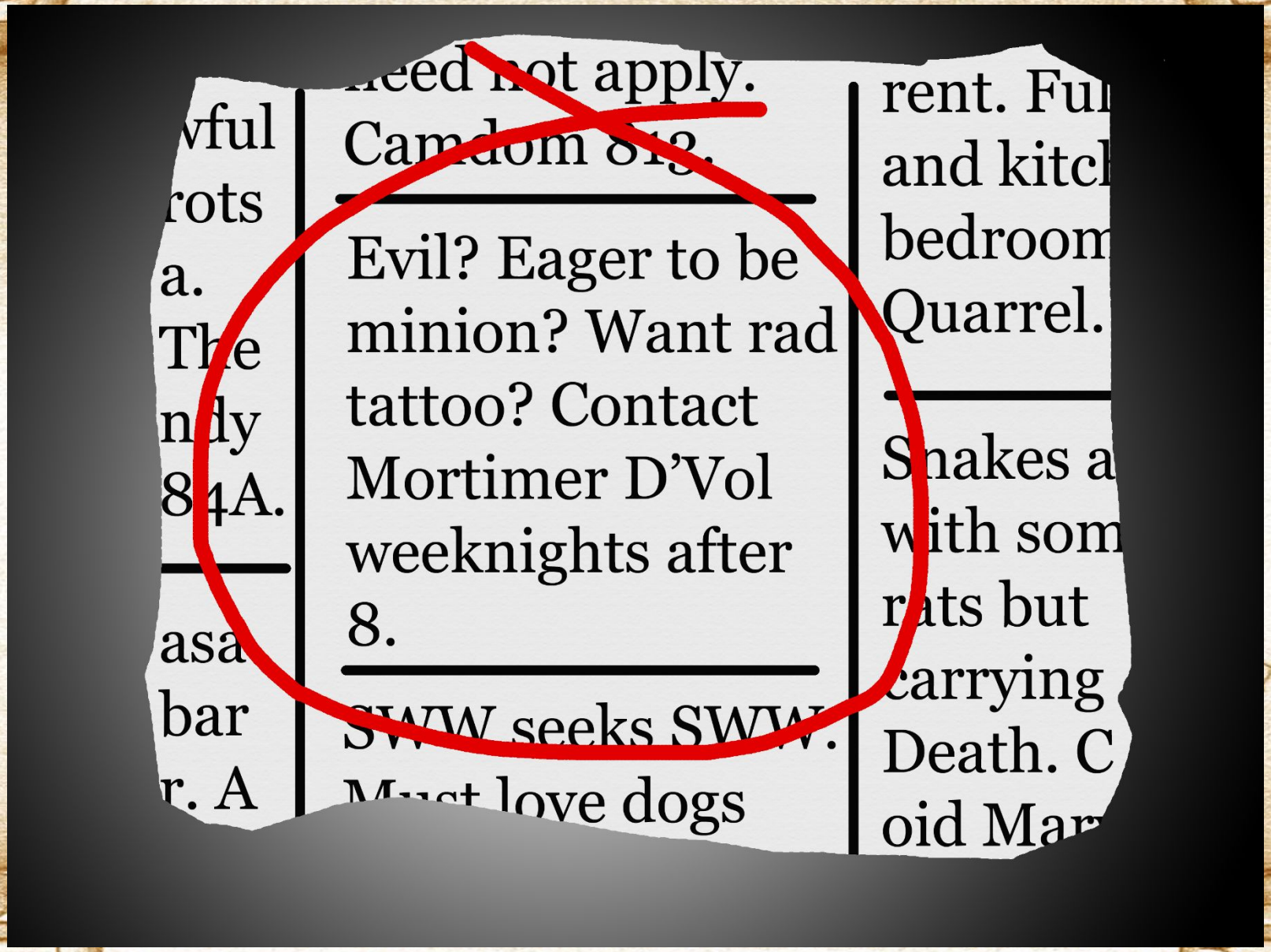
DEFENSIVE SECURITY PODCAST

BSIMM

OWASP Podcast

Exploring Information Security podcast,

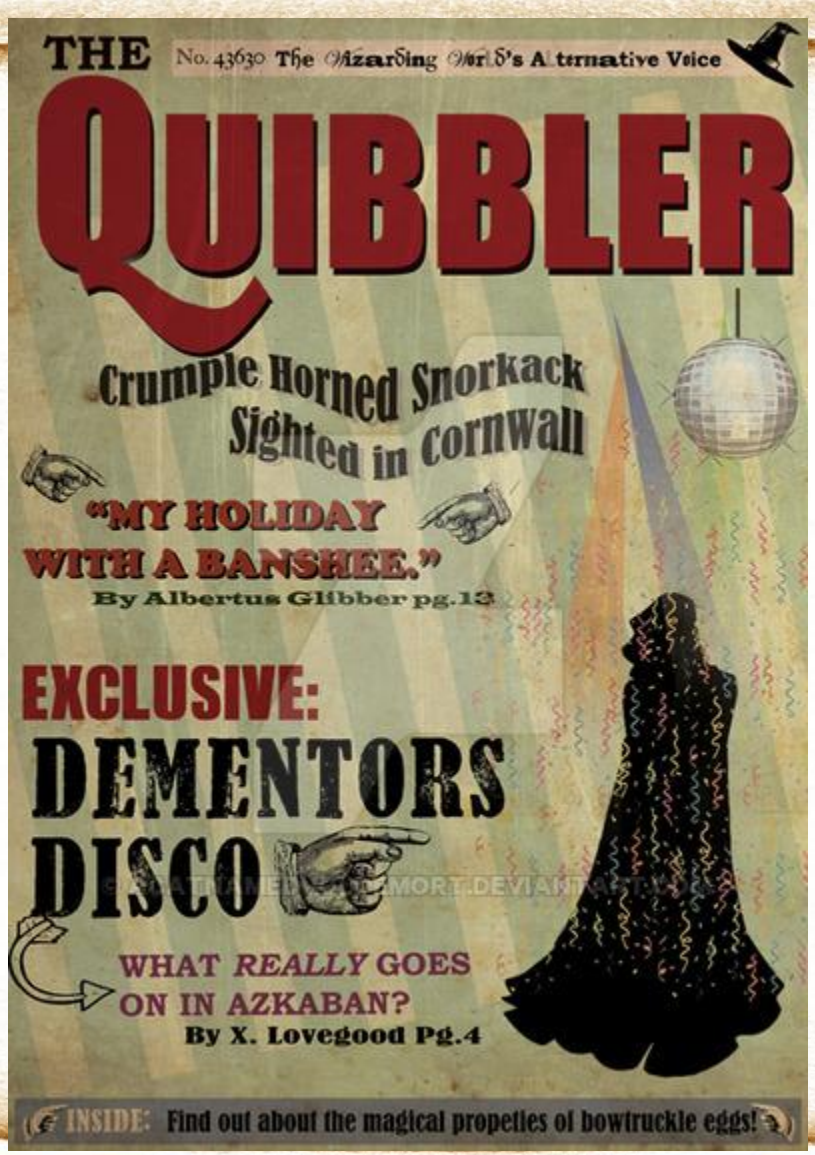




https://www.flickr.com/photos/tuba/53933899/

https://www.youtube.com/watch?v=JzPoz2safPI

http://www.potterworldmc.com/forum/m/23366915/viewthread/24561719-quibbler



References

- http://www.troyhunt.com
  - http://www.troyhunt.com/2011/12/free-ebook-owasp-top-10-for-net.html
- http://www.owasp.org
  - http://www.youtube.com/user/AppsecTutorialSeries?feature=watch
- http://www.microsoft.com/security/sdl/default.aspx
- http://blogs.msdn.com/b/sdl
- http://bsimm.com
- http://www.amazon.com/Writing-Secure-Second-Michael-Howard/dp/0735617228
- http://www.nosqlmap.net/index.html
- http://www.veracode.com/resources/state-of-software-security

Tools

- https://www.kali.org/
- OWASP ZAP https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://www.microsoft.com/en-us/download/details.aspx?id=49168 (Threat Model designer)
- JuiceShop https://github.com/bkimminich/juice-shop
- ysoserial.NET https://github.com/pwntester/ysoserial.net