

The most painful way to implement GDPR

BASED ON 40+ CUSTOMER GDPR PROJECTS I MADE


Marcin Spychała
Senior Security Architect

25.05.2018

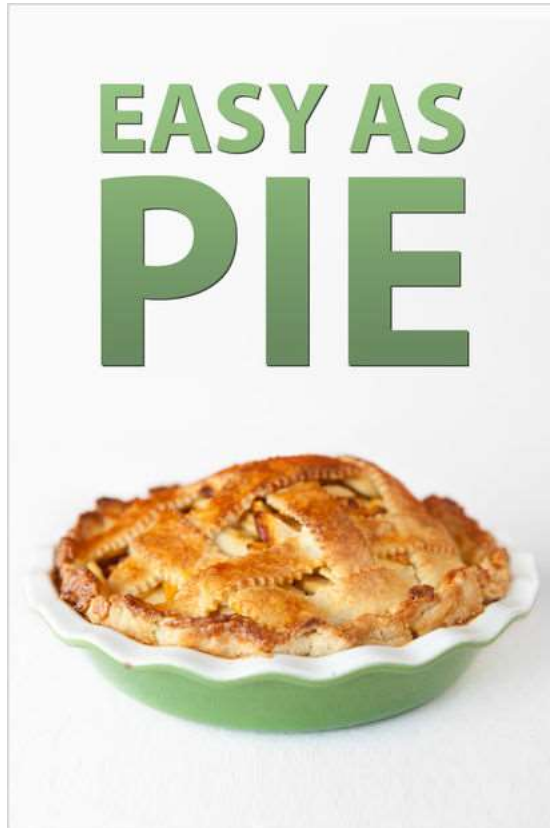


THE FOLLOWING SCENARIO HAS BEEN APPROVED FOR
RESTRICTED CYBERSECURITY AUDIENCES ONLY
BY THE IBM SECURITY FINANCIAL SERVICES TEAM OF AMERICA

IT HAS BEEN RATED

S	Scarily Realistic
	THIS CONTENT REQUIRES THAT EXECUTIVES AND BUSINESS UNIT LEADERS BE ACCOMPANIED BY AN ARCHITECT OR SOC LEADER
HARSH REALITIES, GRAPHIC BREACHES	


I just hackedYOU



Why so late?

Interest over time

Google Trends

Interest by region 

Region    



1	Jersey	92	
2	St Helena	75	
3	Czechia	64	
4	Luxembourg	59	
5	United Kingdom	50	

Include low search volume regions

< Showing 1-5 of 51 regions >

24 Apr 2016

10 Sep 2017



GDPR Ready? Take our Questionnaire

will appear automatically at the foot of the page. Please be sure to answer all

12/27/2001
GENERAL DATA PROTECTION
REGULATION
SELF-ASSESSMENT



pointed a Data Protection Officer (DPO)?

Yes No

GDPR?

Yes No

Yes No

Yes No

Yes No

Data Protection

Yes No

Obtain consent

Yes No

Managing

Yes No

subject data access requests?

[\[click here for more\]](#)

Have processes been developed to allow individuals to amend or delete their personal data?

[\[click here for more\]](#)

Have data retention and destruction procedures been reviewed for all data (including offline) as used by your organisation?

[\[click here for more\]](#)

Have you re-assessed your suppliers and supplier contracts in relation to the GDPR?

Yes No

Yes No

Yes No

Classic GDPR readiness approach....and its consequences

- Legal layer

- “Lets review our Ts&Cs, consent and make sure we are covered from legal perspective”
- And why is that important?



- Process layer

- Let's hire EY, KPMG, PWC, Accenture you name it... to get proper data management process description and book of conduct
- And why it is useless?

Finally...

- IT layer
 - 20 years of data protection legislation
 - Audit based compliance
 - Snapshot based data repository



2 key concepts

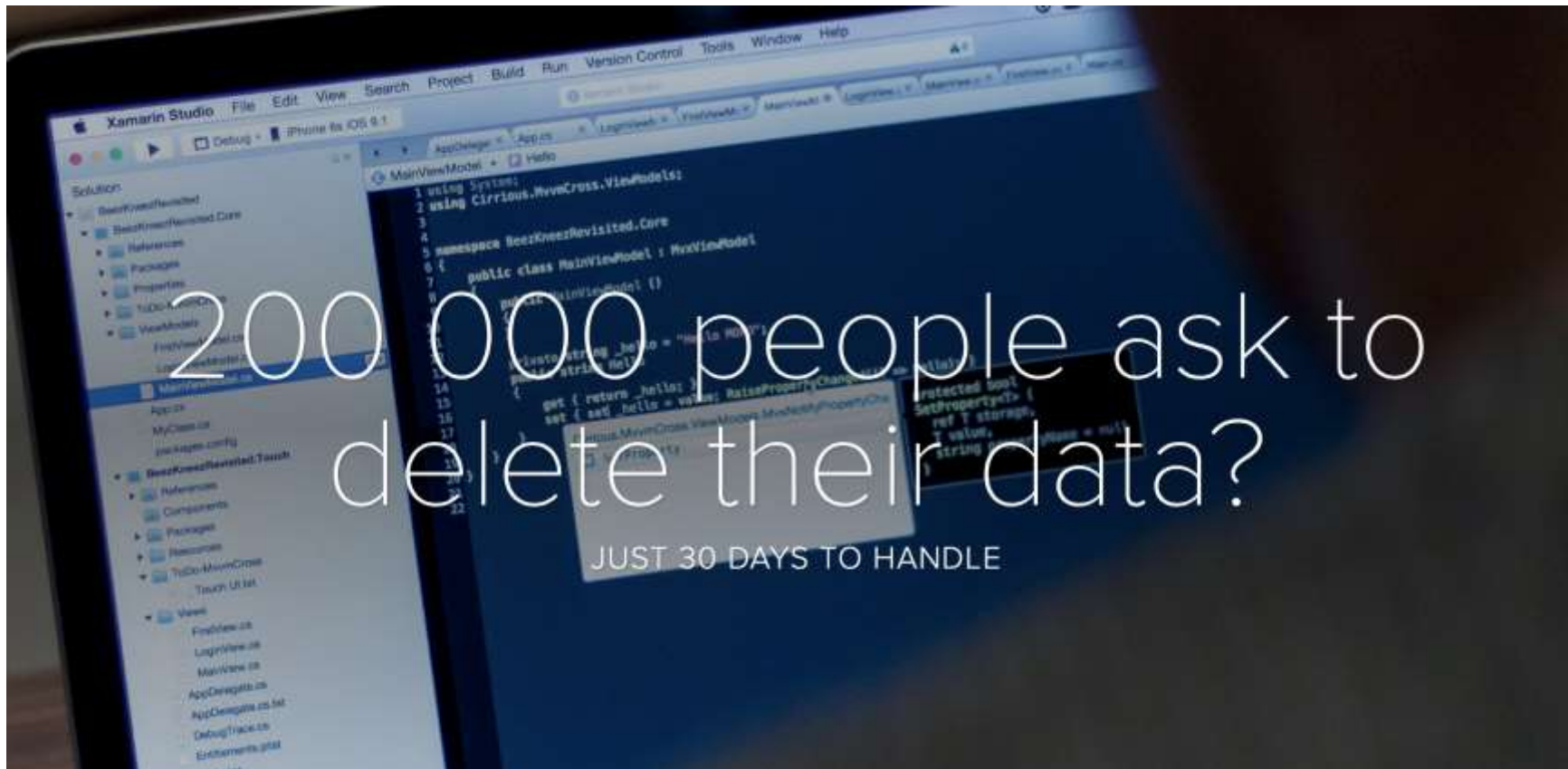
Data dynamics

Typical example: „Anna, could you quickly send me an extract of our customers emails for marketing campaign I plan to run? Oh its that late? Ok – send it to my Dropbox account.”

Data entropy

Nothing is typical here – yet here is the story...

Real life consequences – data access, data move



Real life consequences – data exfiltration



FULL INSTAGR
MERIDIA747

Mastercard Hacked. DUMP!
ANONL30N MAY 26TH, 2015 22,336 NEVER

SHARE
TWEET

Not a member of Pa

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 10.37 KB

text 31.61 KB

raw download clone embed report print

Obvious fraud

1. INSTAGRAM LEAKE
2.
3. Here is the lin
4.
5. >>> https://goo
6.
7.
8. This leak inclu
9. Just open up th
10.
11. Proof of conten
12. (Format is emai
13.
14. root@kali-linux:
15. sumonzool@yahoo
16. nomad__ss@hotmail
17. rkcarpenter@gmail
18. nurrudin44@yahoo
19. rufusrichardson
20. fateschild60@ho
21. ilsevandenheuve
22. koyelnimur@gmail
23. dizzvin@gmail

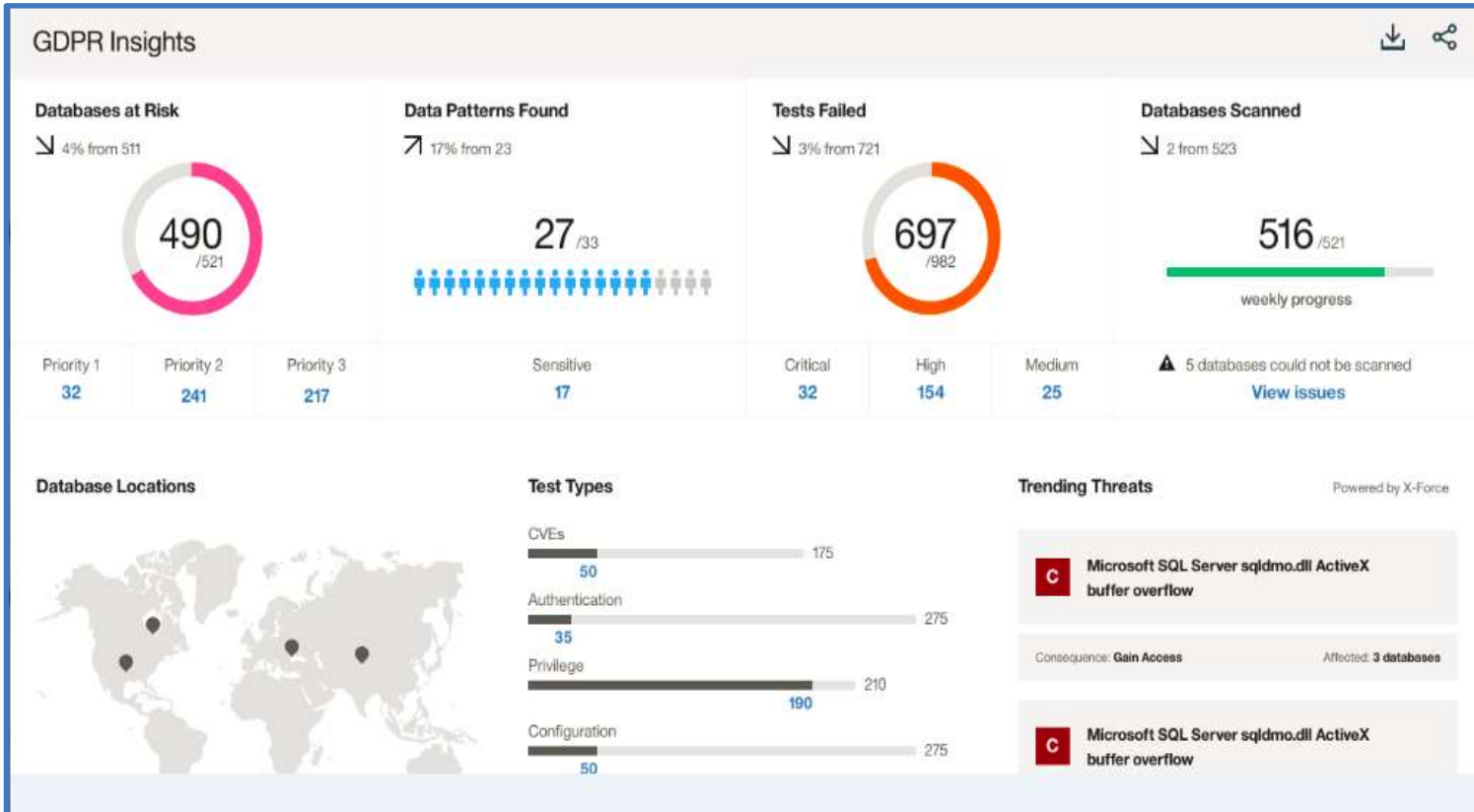
Credit Cards hacked 26 May 2015
#####HURR My Last leak got down in less than 1 hour...THIS PASTE WILL EXPIRE IN 1 DAY#####
#Fuck #The #Government
#cyber #will #lead

5205-85505
FULL LIST DOWNLOAD : http://cur.lv/md2hf #####
FULL LIST DOWNLOAD : http://cur.lv/md2hf #####
5205-85505
#####HURRY My Last leak got down in less than 1 hour...THIS PASTE WILL EXPIRE IN 1 DAY#####

-----+| AnonL30N |----- FULL LIST DOWNLOAD : http://cur.lv/md2hf #####
17. First Name : SMADAR
18. Last Name : HAVER CONFINO
19. Date of Birth : 16/9/1973
20. C... .. SUAM 00

What if...

You could: Find GDPR-relevant data. Uncover risks. Take action.



Data Patterns Found

↗ 17% from 23

GDPR Insights

27 / 33

Tests Failed

↘ 3% from 721

Databases Scanned

↘ 2 from 523

at Risk ⓘ

View all



Tests / Are the number of failed log-in attempts limited to 3?

Scanned yesterday | Scanning weekly

Search



Priority ↓	Databases	Personal Records	Patterns	Days Open	First Found
Priority 1	Dependable_MobileApp_Prod...	632.5M	4	37	13 Sept 2017
Priority 2	Premiere_Customer_Account...	488.4M	7	35	27 Month 2017
Priority 2	This_Isalong_DB_Name...	776.2M	9	43	4 Month 2017
Priority 2	WebApp_Services_Settings...	615.9M	3	2	30 Month 2016
Priority 2	CustomerBudgetsServiceApp...	537.7M	5	3	13 Month 2017
Priority 3	Dependable_MobileApp_Prod...	272.6M	1	3	27 Month 2017
Priority 3	Dept_Sit_Noctateur_Property...	321.4M	2	1	30 Month 2016

End of results

Dependable_MobileApp_Prod

Priority 1 | 632.5M personal records | 60 vulnerabilities

New Authentication Vulnerability

MAX_DAYS_SINCE_LOGIN is not set, or is set to an ... read more

Test Description

Enable common criteria compliance enabled option for MSSQL 2005... read more

Fix Recommendation

Security best practices recommend setting this to 90 days; however, this value may be customized to meet... read more

Progress: 6/10 (60%) | Last Fixed: August 30, 2017

Example Command

```
ALTER LOGIN POLICY ROOT MAX_DAYS_SINCE_LOGIN
```

Mark as Fixed

Priority 3

217

Risk ⓘ ↓

Databases
450 (94%)

Priority 1 | Dependable_MobileApp_Prod...

Priority 1 | Premiere_Customer_Account...

Priority 1 | This_Isalong_DB_Name...

Priority 1 | WebApp_Services_Settings...

Priority 1 | CustomerBudgetsServiceApp...

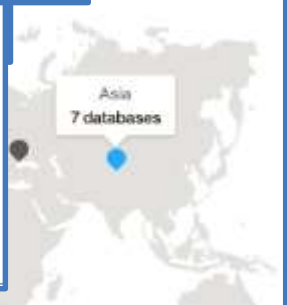


C Microsoft SQL Server sqldmo.dll ActiveX buffer overflow

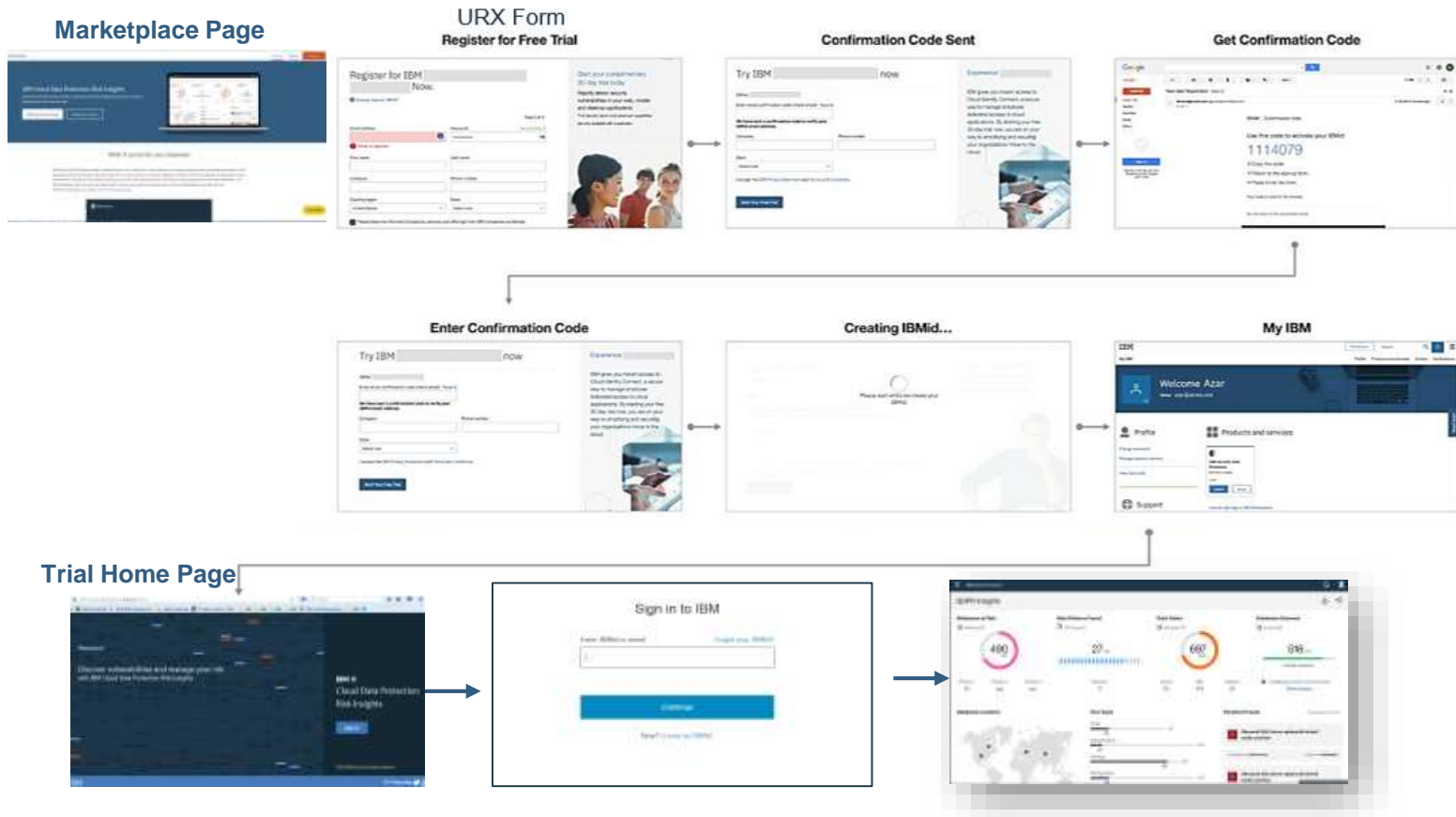
Consequence: Gain Access

Affected: 3 databases

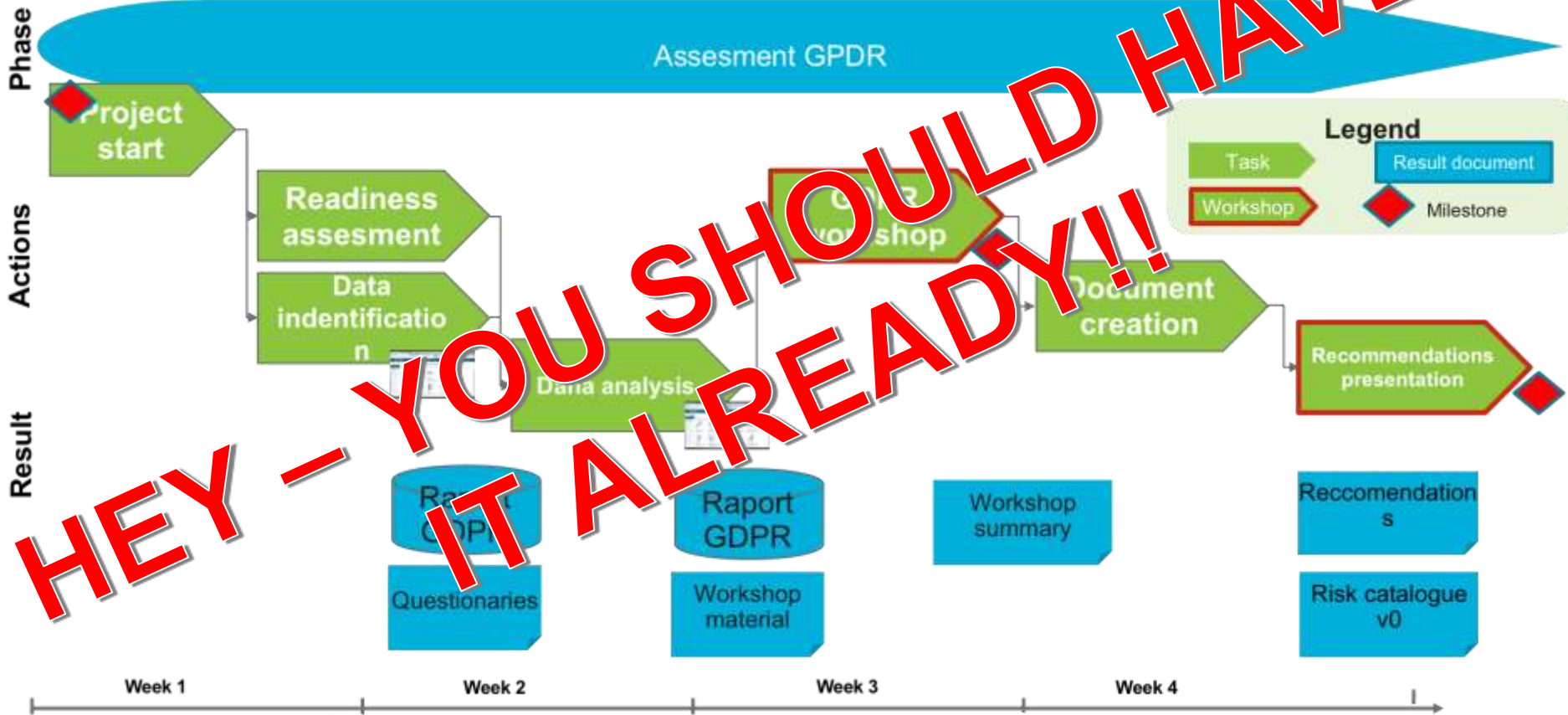
C Microsoft SQL Server sqldmo.dll ActiveX buffer overflow



- How can you get started?
Sign up for our Free 30-Day Trial (*available starting June 5, 2018*)



Alternatively...




CONTACT US!





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.