++

Common Vulnerabilities and How to Find Them

e-Commerce and Financial Trading Applications

William Jardine

Bristol University – 30/11/2018

++

Whoami/Whatisthis/Etc.

- William Jardine
- Security Consultant, MWR, ~2 years
- First time at Bristol Uni!
- Previously gave this talk at OWASP Day Poland
- Developed by myself and Anthony Fielding

++

What?

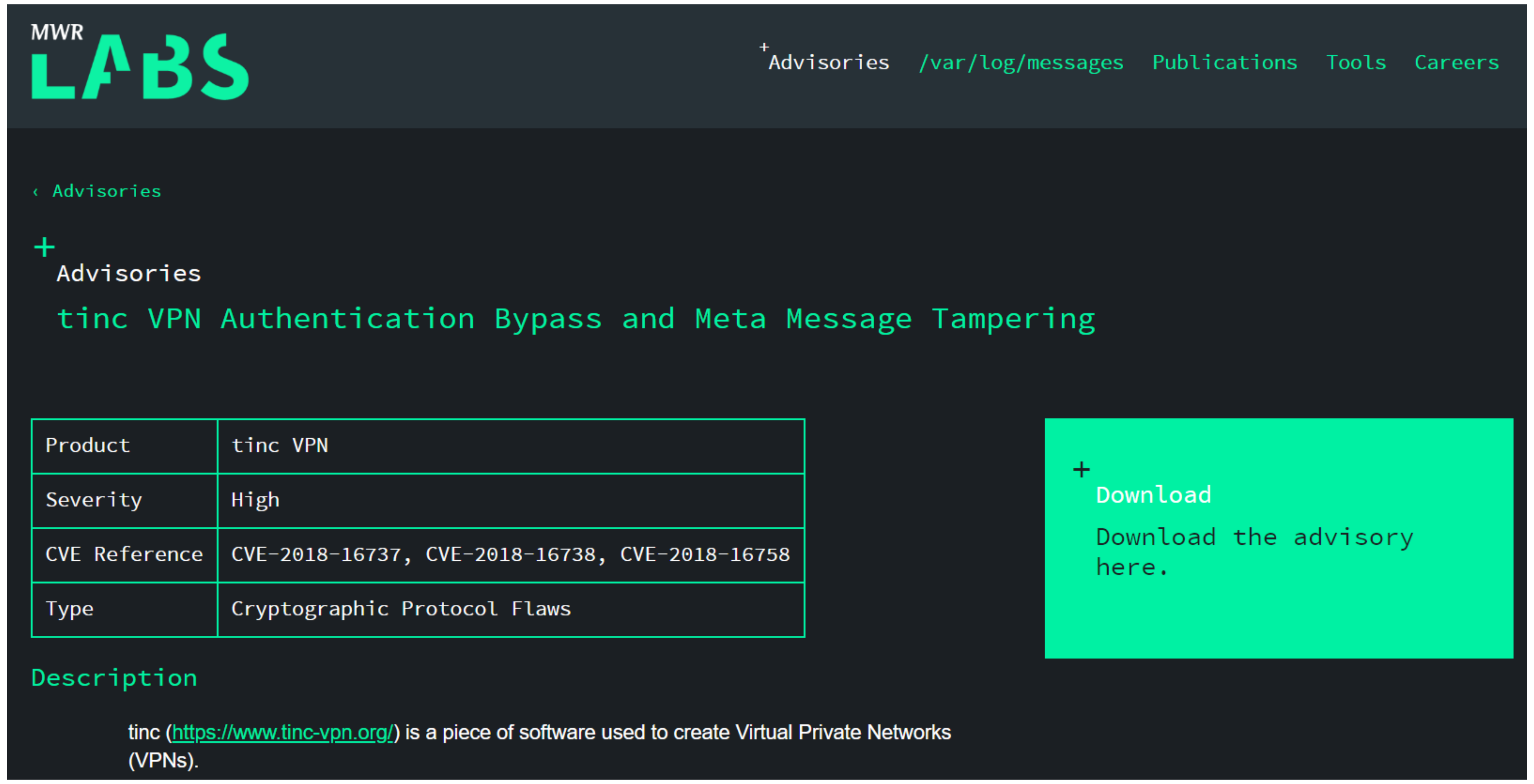
- An internship scheme run by MWR
- Supervised and mentored by some of our most talented consultants
- Shadow real pentesting, security research, etc.
- Award winning!

PRINCESS ROYAL TRAINING AWARD 2018

++

Why?

- A good start in the industry
- Do your own research
  - https://labs.mwrinfosecurity.com/blog/debugging-released-xamarin-android-applications/
  - https://labs.mwrinfosecurity.com/advisories/tinc-vpn/



+ Advisories

tinc VPN Authentication Bypass and Meta Message Tampering

Product	tinc VPN
Severity	High
CVE Reference	CVE-2018-16737, CVE-2018-16738, CVE-2018-16758
Type	Cryptographic Protocol Flaws

+ Download

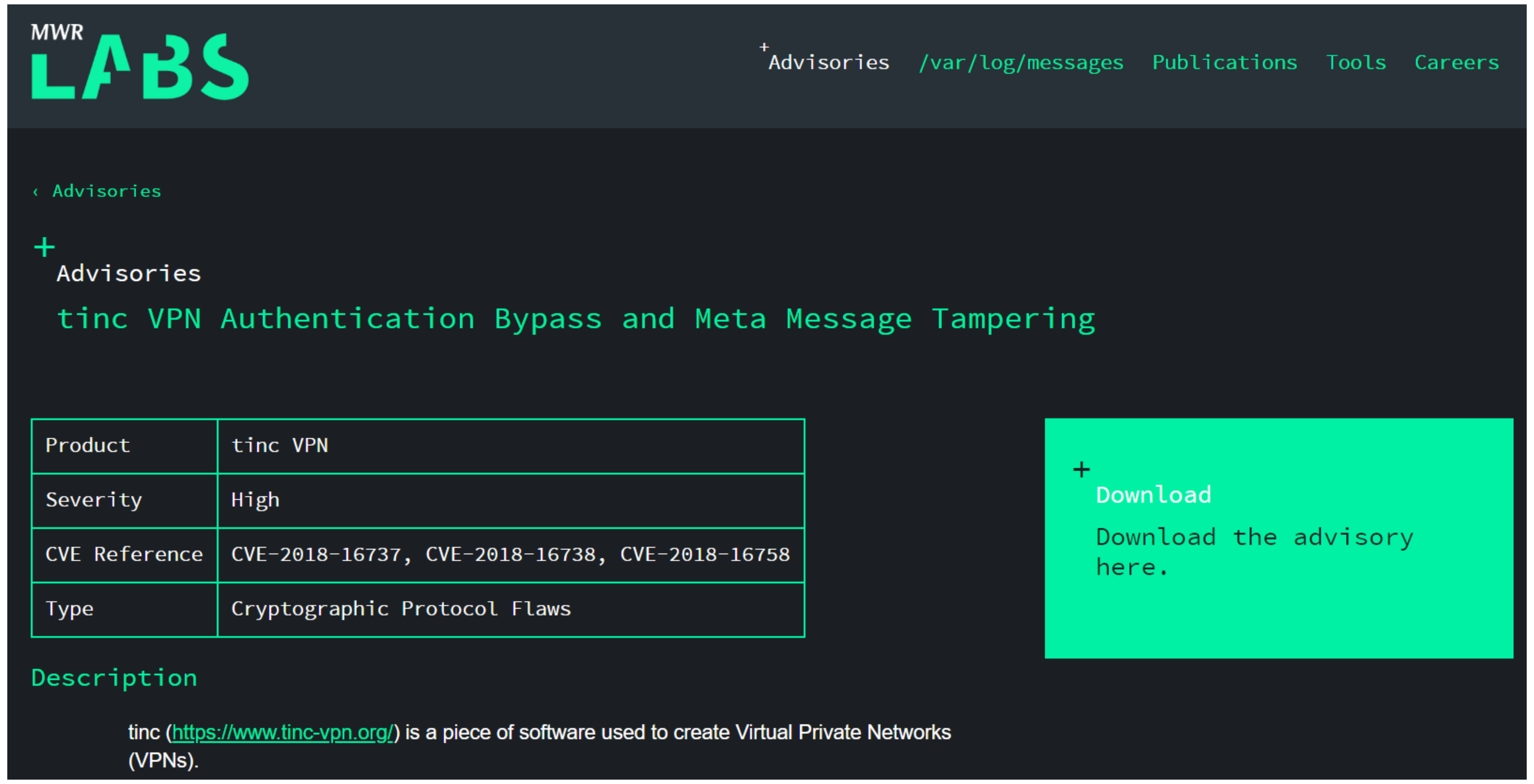
Download the advisory here.

Description

tinc (https://www.tinc-vpn.org/) is a piece of software used to create Virtual Private Networks (VPNs).

++
Why?

- A good start in the industry
- Do your own research
  - https://labs.mwrinfosecurity.com/blog/debugging-released-xamarin-android-applications/
  - https://labs.mwrinfosecurity.com/advisories/tinc-vpn/
- Some people have made it a success…
  - 1x Managing Consultant



+
Advisories

tinc VPN Authentication Bypass and Meta Message Tampering

Product	tinc VPN
Severity	High
CVE Reference	CVE-2018-16737, CVE-2018-16738, CVE-2018-16758
Type	Cryptographic Protocol Flaws

+
Download

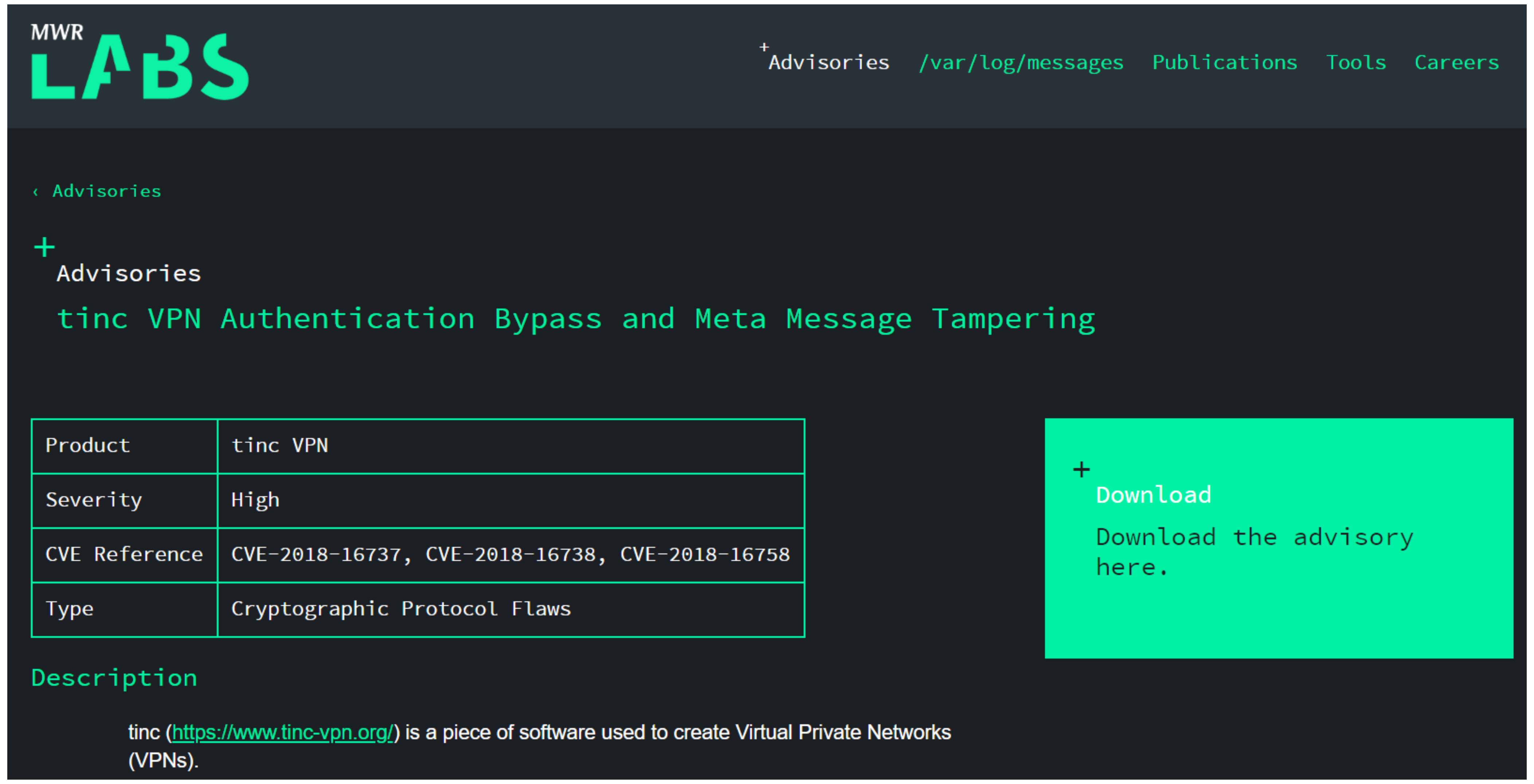
Download the advisory here.

Description

tinc (https://www.tinc-vpn.org/) is a piece of software used to create Virtual Private Networks (VPNs).

++
Why?

- +A good start in the industry
- +Do your own research
  - – https://labs.mwrinfosecurity.com/blog/debugging-released-xamarin-android-applications/
  - – https://labs.mwrinfosecurity.com/advisories/tinc-vpn/
- +Some people have made it a success…
  - – 1x Managing Consultant
  - – 1x Associate Director



+
Advisories

tinc VPN Authentication Bypass and Meta Message Tampering

Product	tinc VPN
Severity	High
CVE Reference	CVE-2018-16737, CVE-2018-16738, CVE-2018-16758
Type	Cryptographic Protocol Flaws

+
Download

Download the advisory here.

Description

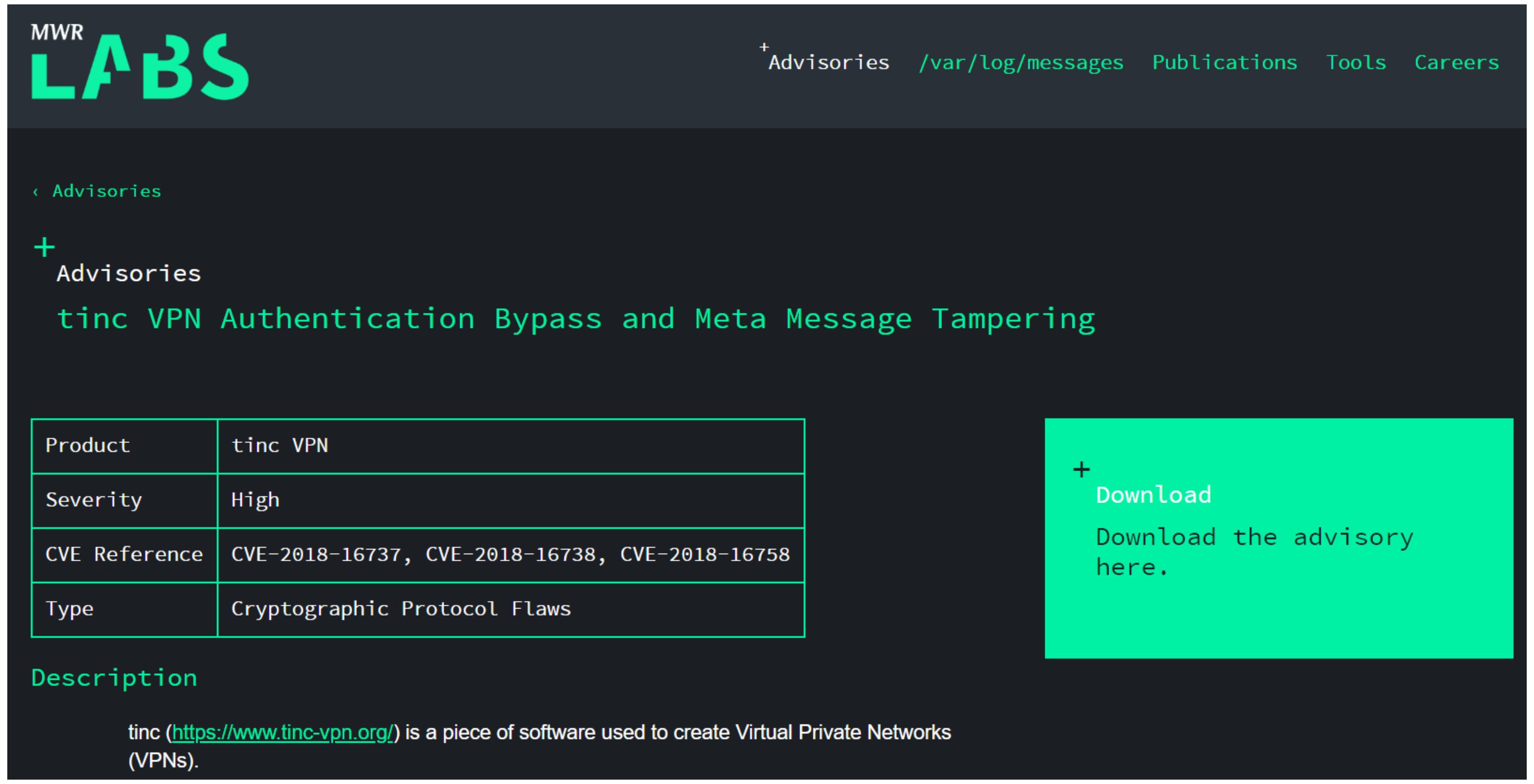
tinc (https://www.tinc-vpn.org/) is a piece of software used to create Virtual Private Networks (VPNs).

++

Why?

- +A good start in the industry
- +Do your own research
  - – https://labs.mwrinfosecurity.com/blog/debugging-released-xamarin-android-applications/
  - – https://labs.mwrinfosecurity.com/advisories/tinc-vpn/
- +Some people have made it a success…
  - – 1x Managing Consultant
  - – 1x Associate Director
  - – 1x Managing Director

Not that we're saying we'll make you MD… ;)



+
Advisories

tinc VPN Authentication Bypass and Meta Message Tampering

Product	tinc VPN
Severity	High
CVE Reference	CVE-2018-16737, CVE-2018-16738, CVE-2018-16758
Type	Cryptographic Protocol Flaws

+
Download

Download the advisory here.

Description

tinc (https://www.tinc-vpn.org/) is a piece of software used to create Virtual Private Networks (VPNs).

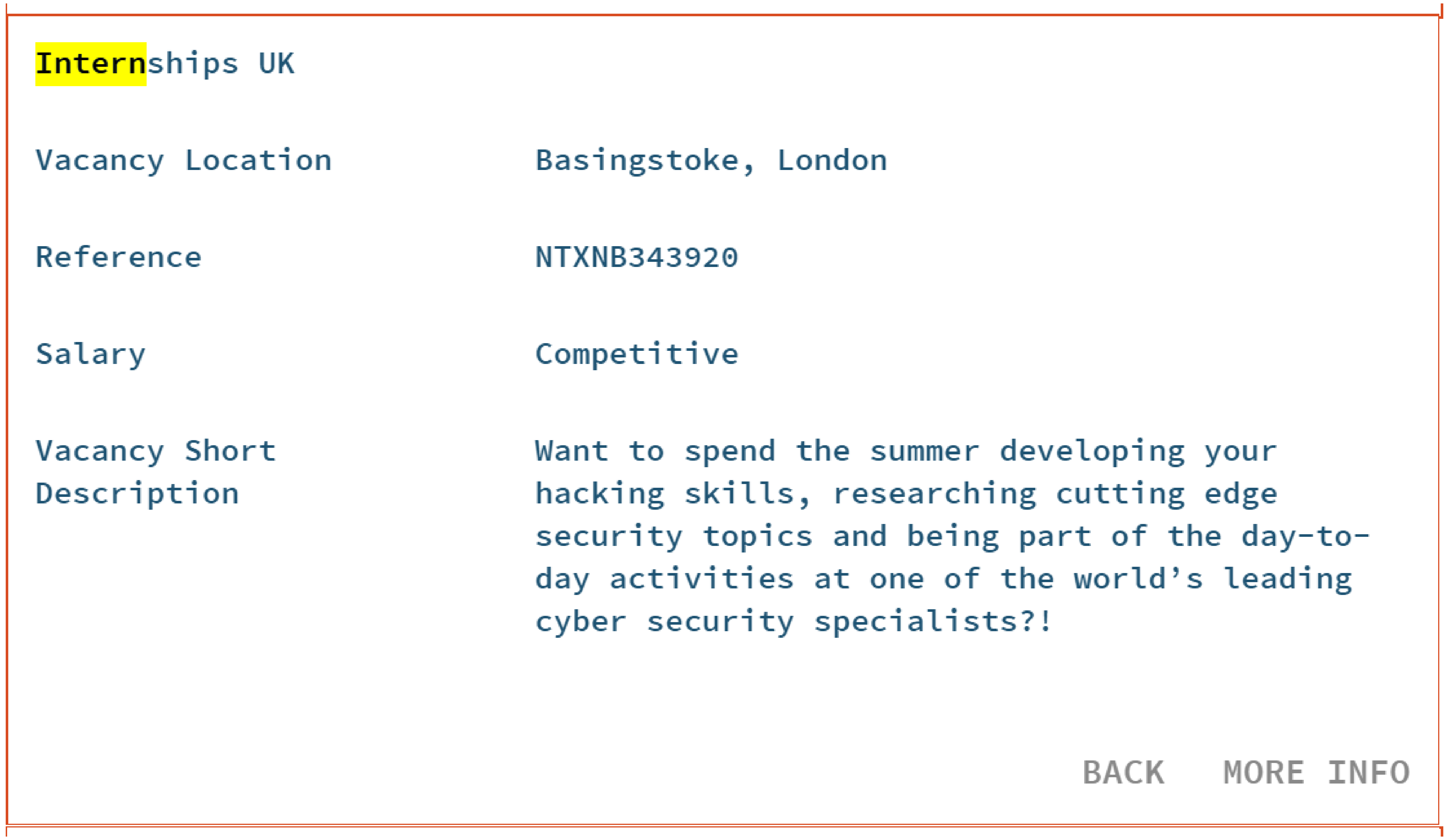
++

When?

- This (and every) summer
- 10 weeks
- Accepting applications now!

++
How?

+https://careers.mwrinfosecurity.com/Jobs/Advert/1413090?cid=1642&FromSearch=False



Internships UK

Vacancy Location	Basingstoke, London
Reference	NTXNB343920
Salary	Competitive
Vacancy Short Description	Want to spend the summer developing your hacking skills, researching cutting edge security topics and being part of the day-to-day activities at one of the world's leading cyber security specialists?!

++
Is and Isn't

Isn't: Intended to be new or groundbreaking techniques

Is: A summary of the currently observed threats against these 2 sectors

++

Is and Isn't

Isn't: Intended to be new or groundbreaking techniques

Is: A summary of the currently observed threats against these 2 sectors

Isn't: Hardcore war stories

Is: Simple, real-world, prevalent examples (arguably even scarier)

++

Is and Isn't

Isn't: Intended to be new or groundbreaking techniques

Is: A summary of the currently observed threats against these 2 sectors

Isn't: Hardcore war stories

Is: Simple, real-world, prevalent examples (arguably even scarier)

Isn't: A guide on how to fix

Is: A guide on how to (quickly) find

Obligatory Intro Spiel

Key Points

1. OWASP Top 10 is valuable
2. But we need context of the specific app domain
3. Whitebox testing leads to more effective results
4. Quick, easy tests can pick up low-hanging fruit

++

e-Commerce industry summary

- An online shop – generally we mean a big one
- E.g. apps like Amazon, eBay, etc.
- Open source
  - Lots of known vulnerabilities in many of these

++

e-Commerce industry summary

- An online shop – generally we mean a big one
- E.g. apps like Amazon, eBay, etc.
- Open source
    - Lots of known vulnerabilities in many of these
- More often using COTS $$$ solutions
    - Less open source and explored
    - More nuanced/complex installations…

++

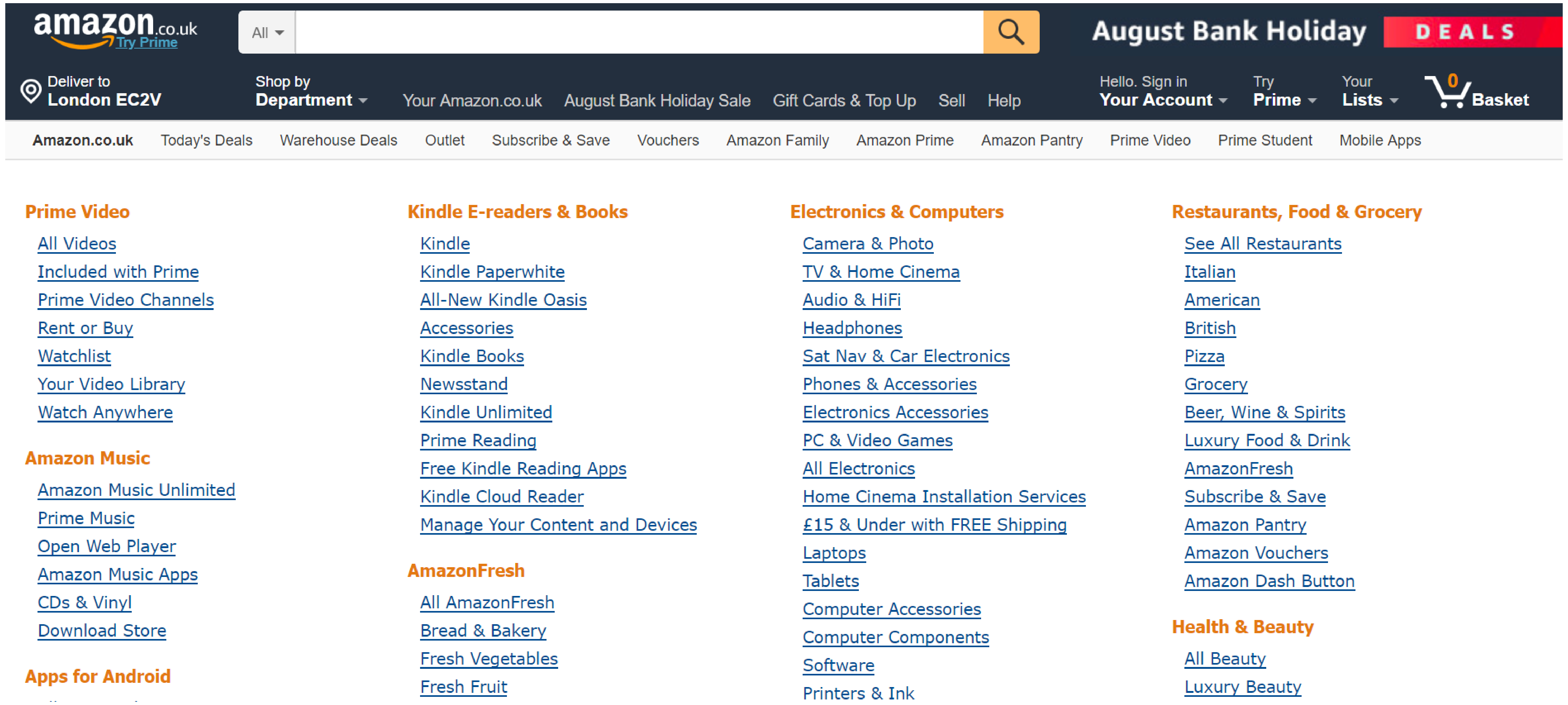
e-Commerce functionality

- Search
- PDP vs. PLP
- Add to basket
- Flat user model (i.e. no real admin functionality)
- Payments
- AJAX
- Large product catalogues

++

e-Commerce flow

+CLP: Category List Page



Prime Video

- All Videos
- Included with Prime
- Prime Video Channels
- Rent or Buy
- Watchlist
- Your Video Library
- Watch Anywhere

Amazon Music

- Amazon Music Unlimited
- Prime Music
- Open Web Player
- Amazon Music Apps
- CDs & Vinyl
- Download Store

Apps for Android

Kindle E-readers & Books

- Kindle
- Kindle Paperwhite
- All-New Kindle Oasis
- Accessories
- Kindle Books
- Newsstand
- Kindle Unlimited
- Prime Reading
- Free Kindle Reading Apps
- Kindle Cloud Reader
- Manage Your Content and Devices

AmazonFresh

- All AmazonFresh
- Bread & Bakery
- Fresh Vegetables
- Fresh Fruit

Electronics & Computers

- Camera & Photo
- TV & Home Cinema
- Audio & HiFi
- Headphones
- Sat Nav & Car Electronics
- Phones & Accessories
- Electronics Accessories
- PC & Video Games
- All Electronics
- Home Cinema Installation Services
- £15 & Under with FREE Shipping
- Laptops
- Tablets
- Computer Accessories
- Computer Components
- Software
- Printers & Ink

Restaurants, Food & Grocery

- See All Restaurants
- Italian
- American
- British
- Pizza
- Grocery
- Beer, Wine & Spirits
- Luxury Food & Drink
- AmazonFresh
- Subscribe & Save
- Amazon Pantry
- Amazon Vouchers
- Amazon Dash Button

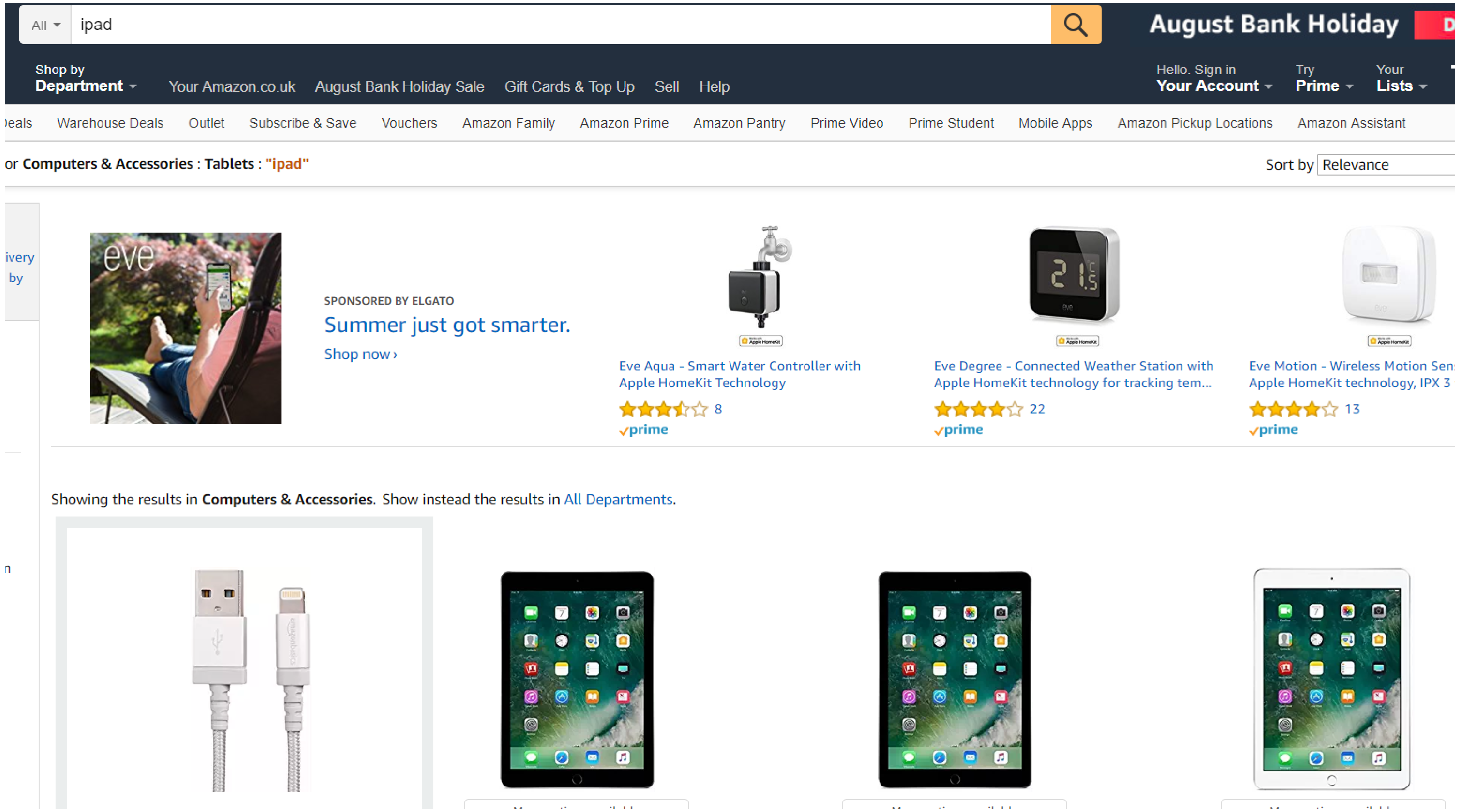
Health & Beauty

- All Beauty
- Luxury Beauty

++

e-Commerce flow

- CLP: Category List Page
- PLP: Product List Page



All ipad

August Bank Holiday

Shop by Department · Your Amazon.co.uk · August Bank Holiday Sale · Gift Cards & Top Up · Sell · Help

Hello. Sign in Your Account · Try Prime · Your Lists

eals · Warehouse Deals · Outlet · Subscribe & Save · Vouchers · Amazon Family · Amazon Prime · Amazon Pantry · Prime Video · Prime Student · Mobile Apps · Amazon Pickup Locations · Amazon Assistant

or Computers & Accessories : Tablets : "ipad"

Sort by Relevance

SPONSORED BY ELGATO

Summer just got smarter.

Shop now ›

Eve Aqua - Smart Water Controller with Apple HomeKit Technology
8
prime

Eve Degree - Connected Weather Station with Apple HomeKit technology for tracking tem...
22
prime

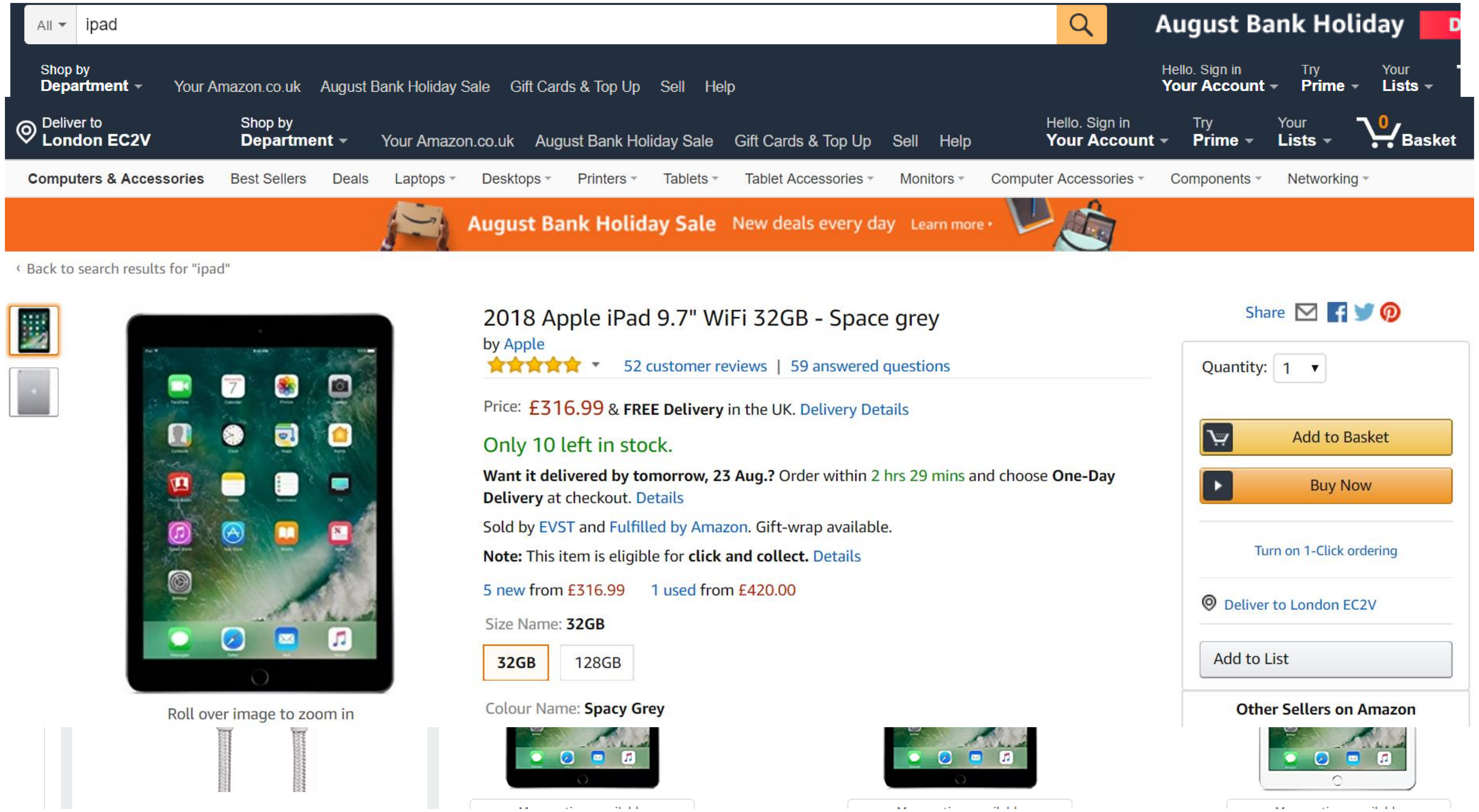
Eve Motion - Wireless Motion Sen Apple HomeKit technology, IPX 3
13
prime

Showing the results in **Computers & Accessories**. Show instead the results in All Departments.

++

e-Commerce flow

- +CLP: Category List Page
- +PLP: Product List Page
- +PDP: Product Display Page



2018 Apple iPad 9.7" WiFi 32GB - Space grey

by Apple

52 customer reviews | 59 answered questions

Price: £316.99 & FREE Delivery in the UK. Delivery Details

Only 10 left in stock.

Want it delivered by tomorrow, 23 Aug.? Order within 2 hrs 29 mins and choose **One-Day Delivery** at checkout. Details

Sold by EVST and Fulfilled by Amazon. Gift-wrap available.

Note: This item is eligible for **click and collect.** Details

5 new from £316.99   1 used from £420.00

Size Name: **32GB**

Colour Name: **Spacy Grey**

++

Selective CSRF in PLP pages

+PLP lists ~1000 items

+1000 “add to basket” buttons

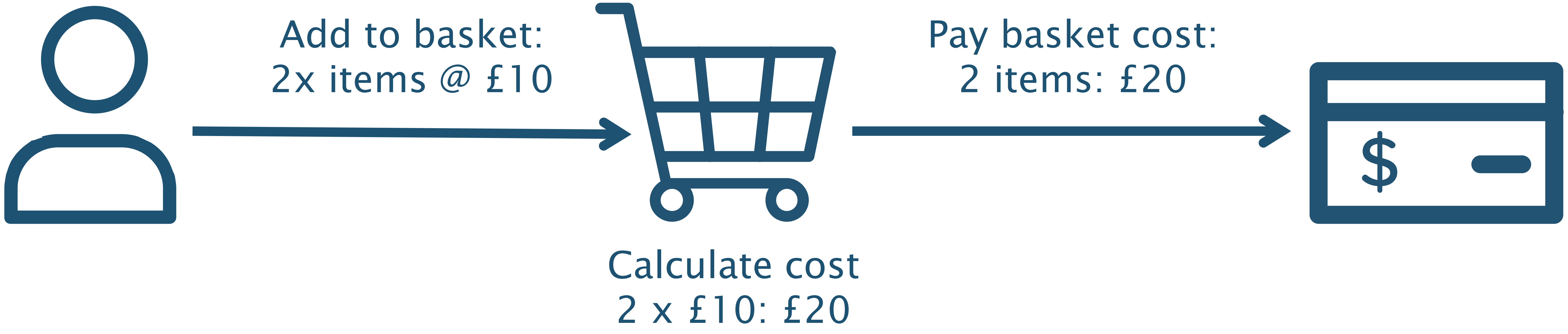
+Devs don’t want to have to list and verify 1000 unique CSRF tokens

+And if a PLP page is cached, CSRF tokens would become stale…

++

Payment flow abuse

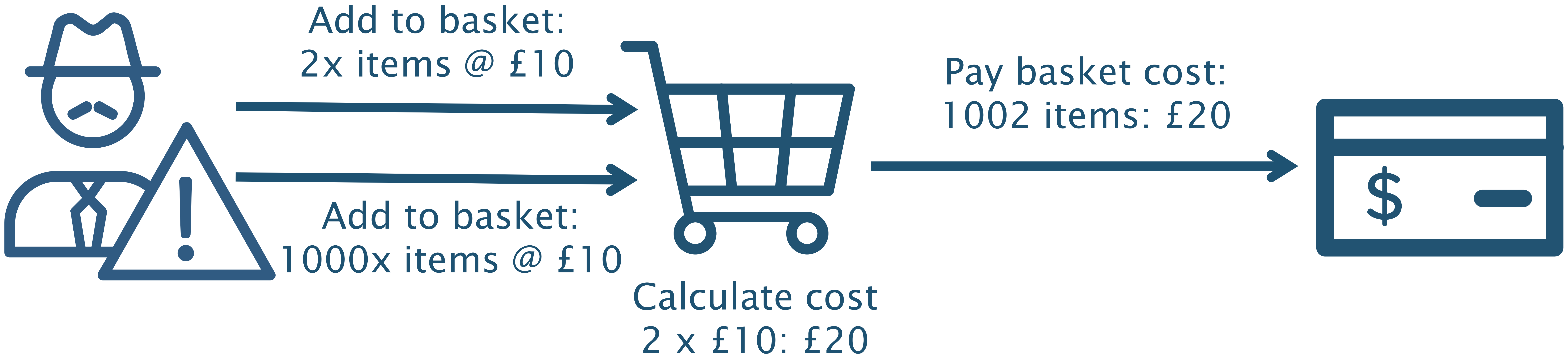
+Legitimate flow



++

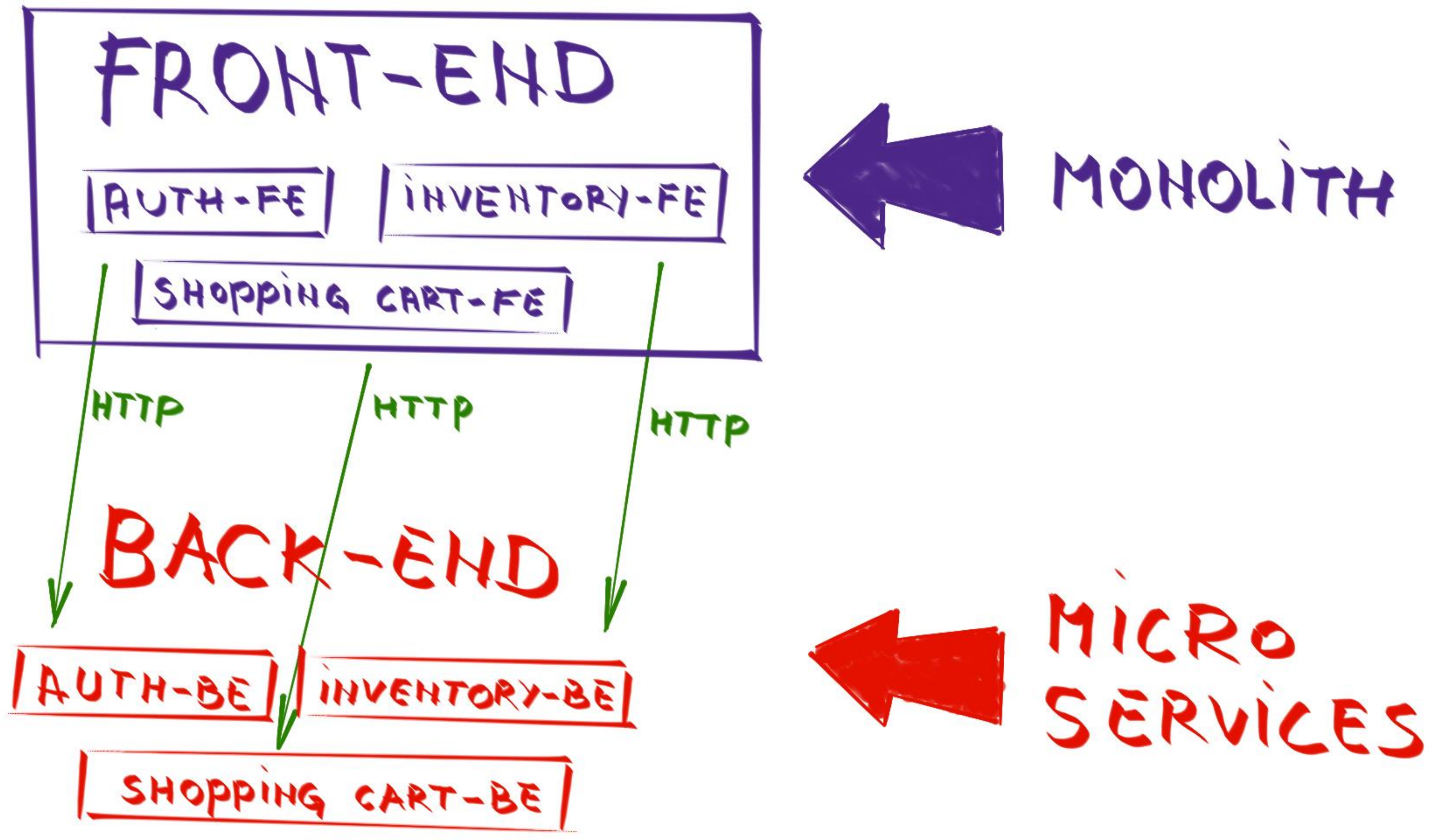
Payment flow abuse

- Malicious flow
- Occurs due to faulty business logic / lack of secure 3rd party vendor



++ Micro-service architectures

- Front-end is monolithic
- Back-end comprises several “micro-services”
- Auth service, payment service, enterprise search service, etc.
- Obviously this can become quite complex…

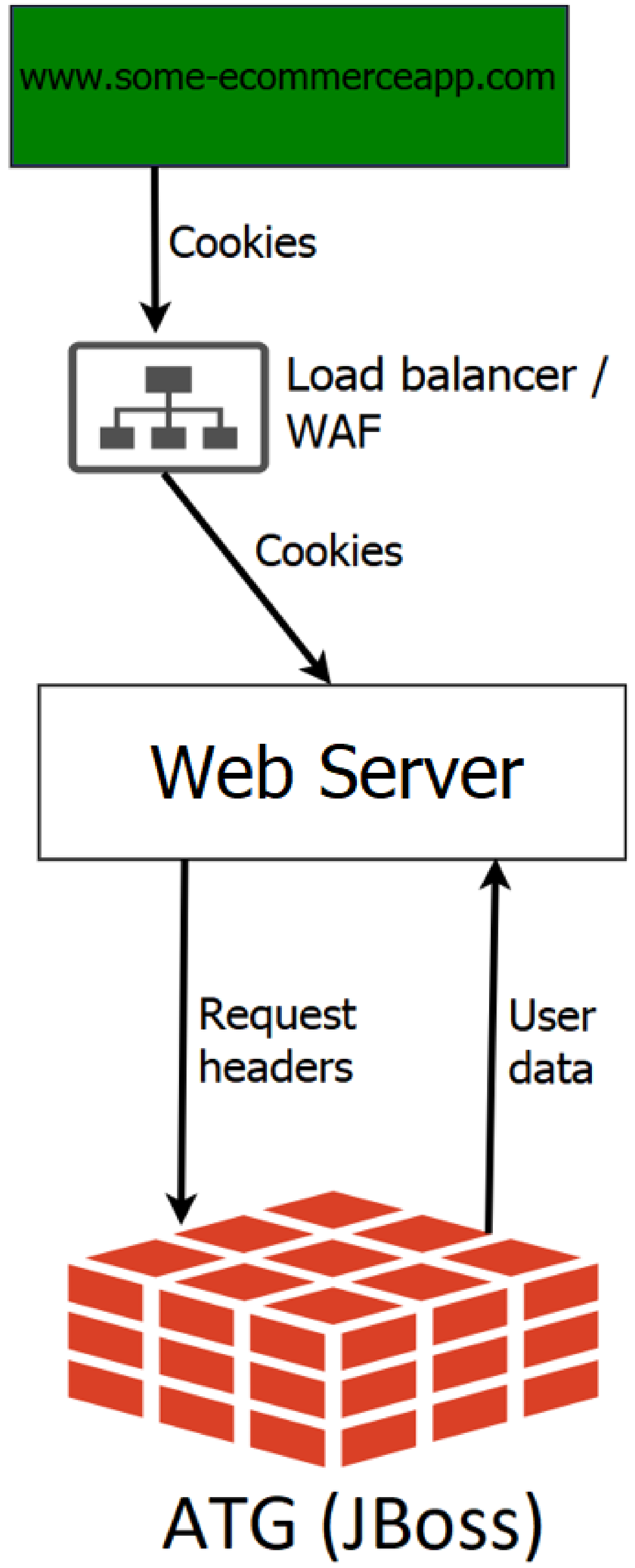


- https://technologyconversations.com/2015/08/09/including-front-end-web-components-into-microservices/

++

Micro-service A/C bypass nuances #1

+ Something like:



++

Micro-service A/C bypass nuances #1

- Cookies store some identifying session info
- Encrypted with a server-side session key

```
SomeCookie=LFfTTadH2MnC3ae9exhYr1jauab3ssORTQuPrpJzHlKGpCeB6T4er
JKco6rYJO/FraIn3W9ZYjVc4MbyciJiFA==
```

- ** in this case, just the AES encrypted form of:*

  userid=1;sessioncookie=1234;someotherstuff=2;test

++

Micro-service A/C bypass nuances #1

- The web server (Apache, IIS, whatever) then decrypts the cookies
- And creates request headers, which it uses to authenticate to back-end services

```
UserID: 1234
EmailAddress: test@example.com
```

++

Micro-service A/C bypass nuances #1

+ We can just send these headers in the initial web app request…

```
GET / HTTP/1.1
Host: www.some-ecommerceapp.com
SomeCookie=some-value
UserID: 1234
EmailAddress: test@example.com
Connection: close
```

++

Micro-service A/C bypass nuances #2

+ Observed on several occasions
+ Where apps are overly reliant on something else
  - API Gateway
  - WAF
+ Or where they’re not sticking to centralised procedures properly
+ E.g. Checking the HTTP code, not the actual body…

++

Micro-service A/C bypass nuances #2

+ Request with valid cookies

```
HTTP /1.1 200 OK
...

{"Response": "Authenticated"}
```

++

Micro-service A/C bypass nuances #2

- Request with valid cookies

```
HTTP /1.1 200 OK
...

{"Response": "Authenticated"}
```

✓

- Request with **invalid** cookies

```
HTTP /1.1 200 OK
...

{"Response": "Unauthenticated"}
```

✓ …

++

Micro-service auth note

- "Abstraction of security" can be a good thing
- But beware a lack of context
- Defence-in-depth!

++

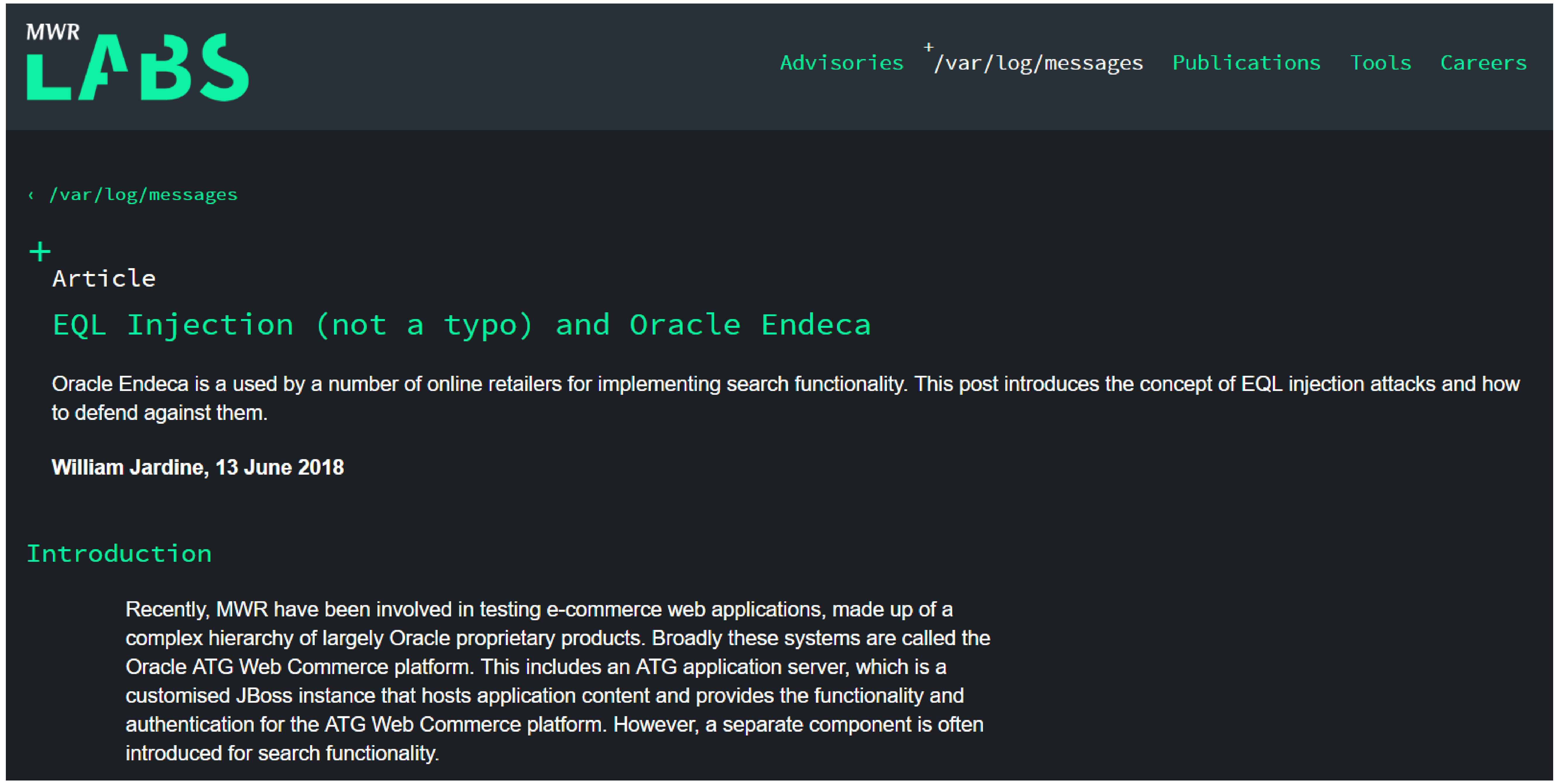
Niche search back-end

- +9 pentests out of 10 will just spam ‘or 1=1
- +And the top 100 SQLi payloads
- +Is a large product catalogue really going to be stored in an SQL DB?
- +Is the question even asked a lot of the time?

++

Oracle Endeca injection demo

- Or EQLi™ (© William Jardine 2018)
- https://labs.mwrinfosecurity.com/blog/eql-injection-and-oracle-endeca/



Article

EQL Injection (not a typo) and Oracle Endeca

Oracle Endeca is a used by a number of online retailers for implementing search functionality. This post introduces the concept of EQL injection attacks and how to defend against them.

William Jardine, 13 June 2018

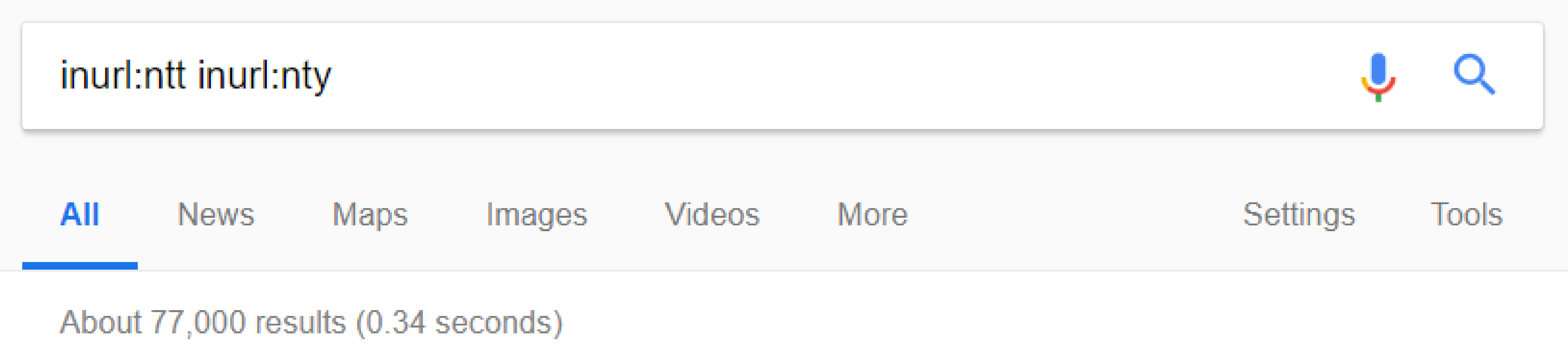
Introduction

Recently, MWR have been involved in testing e-commerce web applications, made up of a complex hierarchy of largely Oracle proprietary products. Broadly these systems are called the Oracle ATG Web Commerce platform. This includes an ATG application server, which is a customised JBoss instance that hosts application content and provides the functionality and authentication for the ATG Web Commerce platform. However, a separate component is often introduced for search functionality.

++

Oracle Endeca injection demo

- +Common in Oracle ATG e-Commerce installations
- +E.g. Google:
  - inurl:ntt inurl:nty
  - inurl:ntk inurl:p_price



inurl:ntt inurl:nty

About 77,000 results (0.34 seconds)

++

Oracle Endeca payloads

```
Nrs=collection()/record[LISTING_ID%3D "T123456"]

Nrs=collection()/record[endeca:matches(.,"P_Marked_For_Emergency_Withdrawal ","Y")]

Ns=P_Stock_Availability|0||P_Best_Seller|0

Ntt=someitem&Ntk=All
```

++

Summary: Context

Vulnerability	Severity	Frequency	Complexity
Payment flow vulnerabilities	High	Rarely*	Medium
Insecure direct object references	Medium	Sometimes	Low
Niche search injections	Medium	Sometimes	Medium
Nuanced broken access control	High	Sometimes	High
Selective CSRF	Low**	Frequent	Medium
Insecure CORS/CSP settings	Low	Frequent	Low

+ * Rarely in broadly secure apps that use 3DSecure
+ ** Low on its own; higher impact if chained with other things

++

Financial industry summary

+ Online banking and trading platforms
+ Complex, big systems with lots of functionality
+ Exciting words like butterfly trades, swaps, bonds, forex, etc…
+ Developed in-house over 6 months to many years
+ Mix of old (Silverlight, Flash) and new technologies e.g. AngularJS Single Page Application (SPA)

spring by Pivotal

ADOBE FLASH

Microsoft Silverlight

++

Financial functionality

- Limited or read-only functionality for regular users
- Highly customisable and rich user experience
  - Spreadsheet import/export
  - Extensive reporting capabilities
  - Visualisations and live data
- Create trades, transfer funds, approve payments

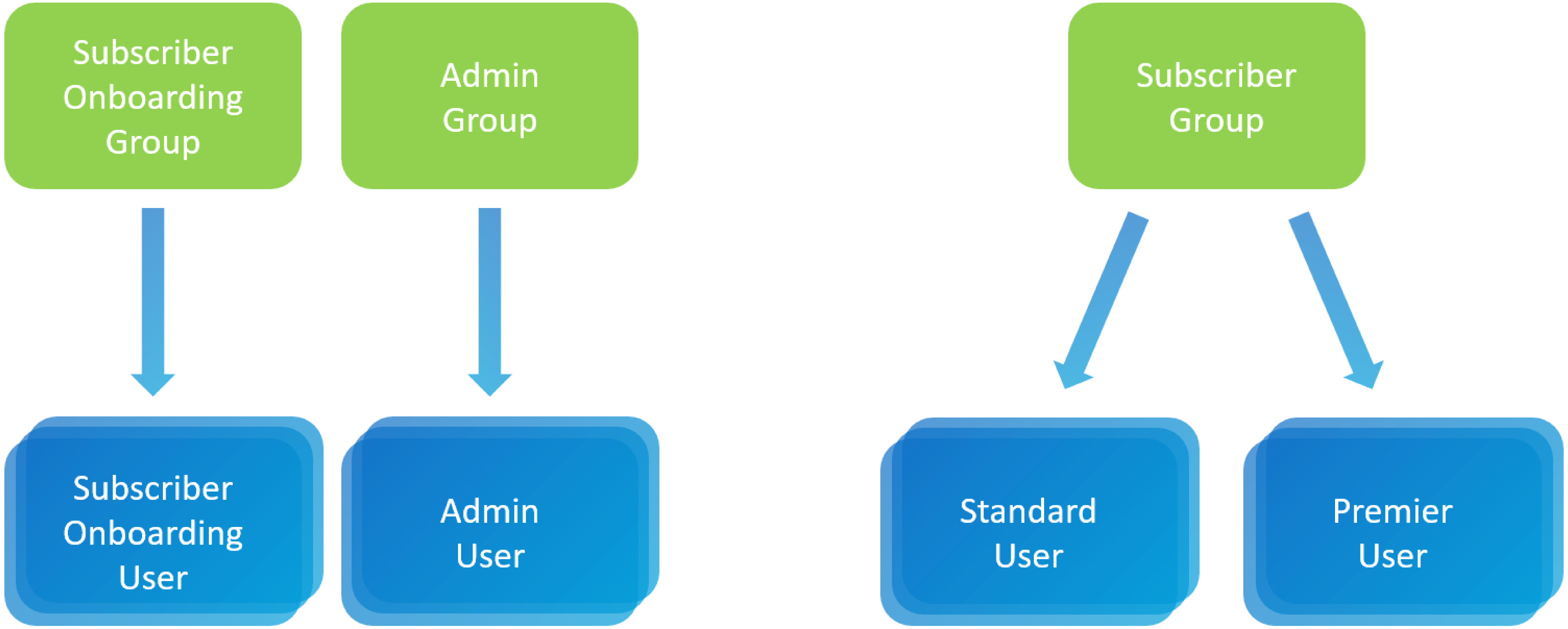
++

Financial functionality

- Complex user model
- Workflow heavy
- Upstream dependencies and downstream dependents
  - Many departments involved
  - Apps within apps
- Often use Single Sign-On (SSO) for authentication
- Prevalence of Single Page Application (SPA)s e.g. AngularJS

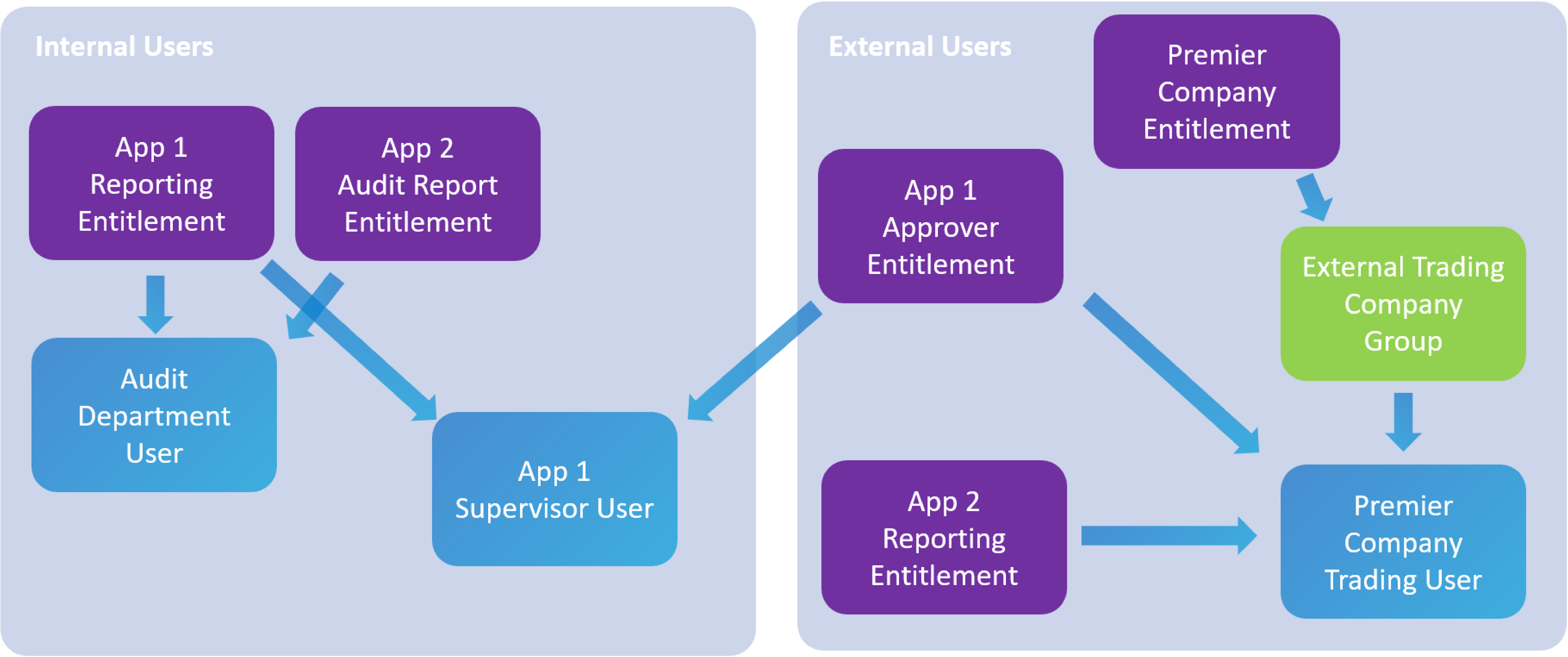
++

Simple user model



++

Finance user model


Internal Users
App 1 Reporting Entitlement
App 2 Audit Report Entitlement
Audit Department User
App 1 Supervisor User
External Users
Premier Company Entitlement
App 1 Approver Entitlement
External Trading Company Group
App 2 Reporting Entitlement
Premier Company Trading User

++

What do we find?

- Broken access control
  - Primarily horizontal privilege escalation
  - Reliance on “out of scope” SSO
- More and more hardened against Cross-Site Scripting (XSS)
  - Old: Due to age
  - New: Use of AngularJS
  - Still find relatively frequently though
- User-targeted Remote Code Execution (RCE) via formula injection
  - Output encoded (in browser) so we’re fine, right…?

Formula injection payloads

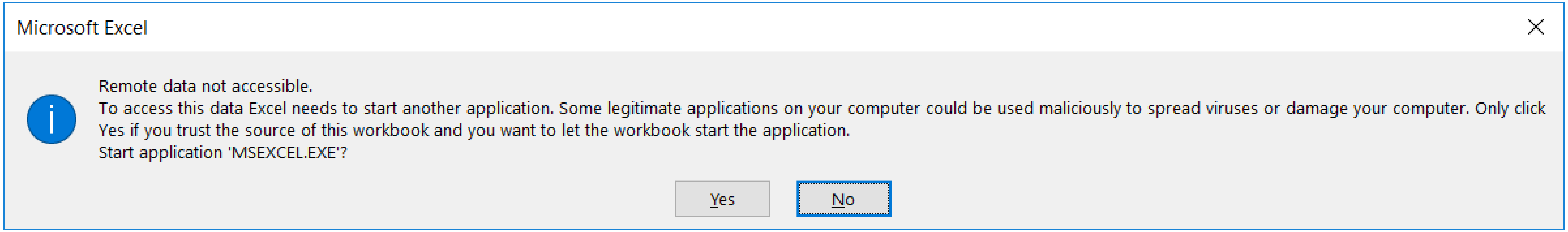
- The following payloads test for this vulnerability:

```
=cmd|' /C calc'!A0
+cmd|' /C calc'!A0
@SUM(1+1)*cmd|' /C calc'!A0
DDE ("cmd";"/C calc";"!A0")A0

+MSEXCEL|'\..\..\..\Windows\System32\cmd /c calc'!A0
```

Formula injection payloads

- The following payloads test for this vulnerability:

```
=cmd|' /C calc'!A0
+cmd|' /C calc'!A0
@SUM(1+1)*cmd|' /C calc'!A0
DDE ("cmd";"/C calc";"!A0")A0

+MSEXCEL|'\..\..\..\Windows\System32\cmd /c calc'!A0
```



Microsoft Excel

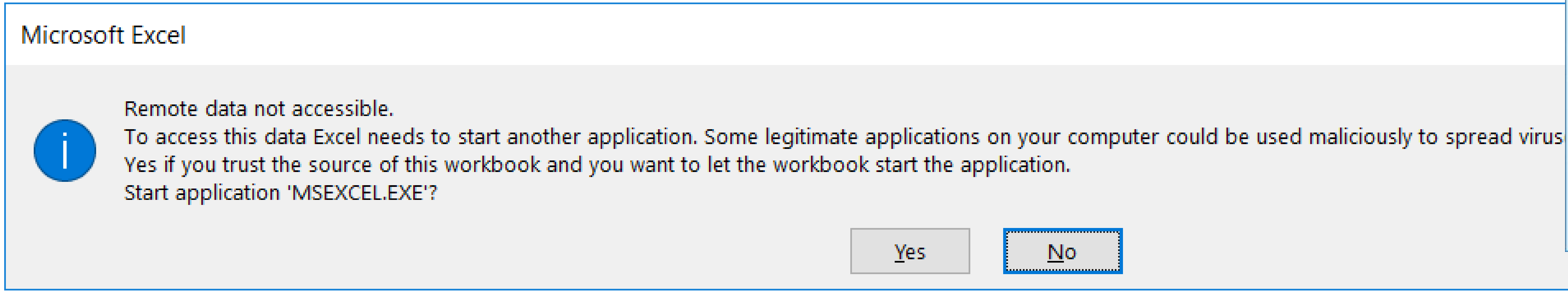
Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'MSEXCEL.EXE'?

++

Formula injection payloads

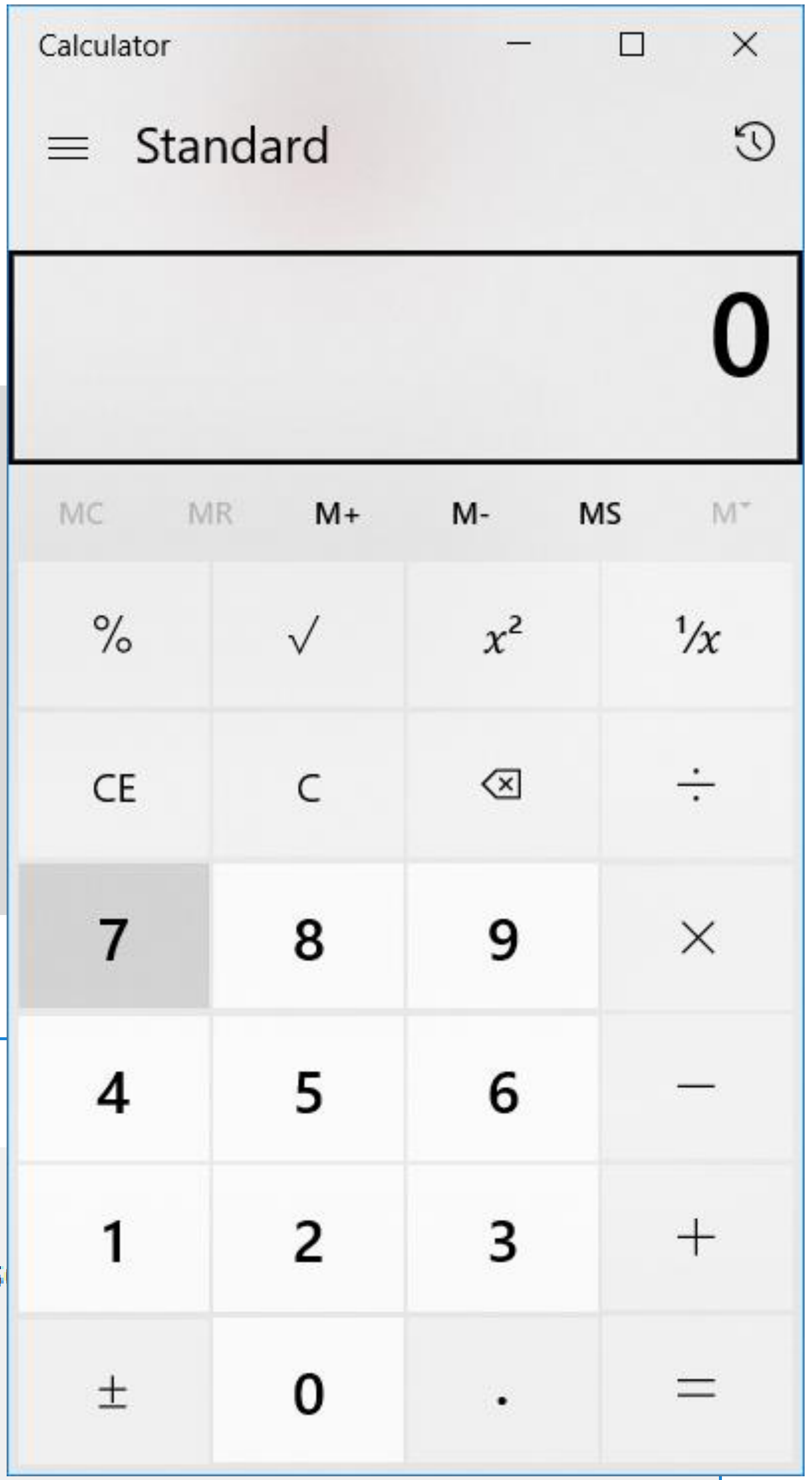
+ The following payloads test for this vulnerability:

```
=cmd|' /C calc'!A0
+cmd|' /C calc'!A0
@SUM(1+1)*cmd|' /C calc'!A0
DDE ("cmd";"/C calc";"!A0")A0

+MSEXCEL|'\..\..\..\Windows\System32\cmd /c calc'!A0
```



Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread virus
Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'MSEXCEL.EXE'?



++

What do we find?

- +Occasionally direct SQL query access on back-end panels
  - – Retired and long forgotten systems still in production
- +Insecure Direct Object References
  - – E.g. **https://sometradingapp.com/export?DocumentID=11**
- +Client-Side Template Injection (CSTI)
  - – Test for **{{7*7}}**
  - – **{{constructor.constructor('alert(1)')()}}**
- +Missing headers and poor cookie configuration
- +Out of date and vulnerable software
- +No or broken CSRF protection

++

MEGABANK demo

Sign in to
MEGABANK

Customer ID
User ID
Password
Token
Sign in

++

Summary: Context

Vulnerability	Severity	Frequency	Complexity
Formula injection	Medium	Frequent	Medium
Broken access control	High	Frequent	Medium
Insecure direct object references	High	Sometimes	Medium
CSTI	Medium	Sometimes	Medium
XSS	Medium	Sometimes	Medium
Direct SQL query execution	High	Rarely	Low
Lack of CSRF protection	Low	Frequent	Low
Insecure cookies	Low	Frequent	Low

++ Overlap (frequency)

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent

++

Overlap (frequency)

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent
3. Formula injection	N/A	Frequent

++

Overlap (frequency)

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent
3. Formula injection	N/A	Frequent
4. Insecure CORS/CSP settings	Frequent	N/A
5. Insecure cookies	N/A	Frequent

++

Overlap (frequency)

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent
3. Formula injection	N/A	Frequent
4. Insecure CORS/CSP settings	Frequent	N/A
5. Insecure cookies	N/A	Frequent
6. Insecure direct object references	Sometimes	Sometimes
7. Search injections	Sometimes	Rarely
8. XSS	N/A	Sometimes
9. CSTI	N/A	Sometimes

++

Overlap (frequency)

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent
3. Formula injection	N/A	Frequent
4. Insecure CORS/CSP settings	Frequent	N/A
5. Insecure cookies	N/A	Frequent
6. Insecure direct object references	Sometimes	Sometimes
7. Search injections	Sometimes	Rarely
8. XSS	N/A	Sometimes
9. CSTI	N/A	Sometimes
10. Payment flow vulnerabilities	Rarely*	N/A

++
Huh... That’s 10...

OWASP Top 10 Vulnerability	Higher/Lower
A1. Injection	▼
A2. Broken Authentication	N/A
A3. Sensitive Data Exposure	N/A
A4. XXE	N/A
A5. Broken Access Control	▲
A6. Security Misconfigurations	▲
A7. XSS	▼
A8. Insecure Deserialization	N/A
A9. Components w/ Known Vulns	N/A
A10. Insufficient Logging/Monitoring	N/A

Vulnerability	Frequency (e-Commerce)	Frequency (financial trading)
1. Some lack of CSRF protection	Frequent	Frequent
2. Broken access control	Sometimes	Frequent
3. Formula injection	N/A	Frequent
4. Insecure CORS/CSP settings	Frequent	N/A
5. Insecure cookies	N/A	Frequent
6. Insecure direct object references	Sometimes	Sometimes
7. Search injections	Sometimes	Rarely
8. XSS	N/A	Sometimes
9. CSTI	N/A	Sometimes
10. Payment flow vulnerabilities	Rarely*	N/A

++

Very rough hit-list

Vulnerability	How to find?
1. Some lack of CSRF protection	Burp CSRF PoC; is it in a cookie? Is it JSON?
2. Broken access control	Burp Repeater w/ different cookies; check response codes
3. Formula injection	=cmd|’ /C calc’!A0
4. Insecure CORS/CSP settings	DevTools fetch(); OPTIONS; all 3rd party resources
5. Insecure cookies	HttpOnly and Secure; domains; age
6. Insecure direct object references	e.g. DocumentID=2
7. Search injections	What DB is used? Audit code
8. XSS	<img src=x onerror=alert(1)>
9. CSTI	{{7*7}}
10. Payment flow vulnerabilities	Re-send requests after basket calculation

Key Points

1. OWASP Top 10 is valuable
2. But we need context of the specific app domain
3. Whitebox testing leads to more effective results
4. Quick, easy tests can pick up low-hanging fruit

Questions?

- (Other than why this slide is so orange)

- william.Jardine@mwrinfosecurity.com
- @williamkjardine
- https://www.linkedin.com/in/williamjardine