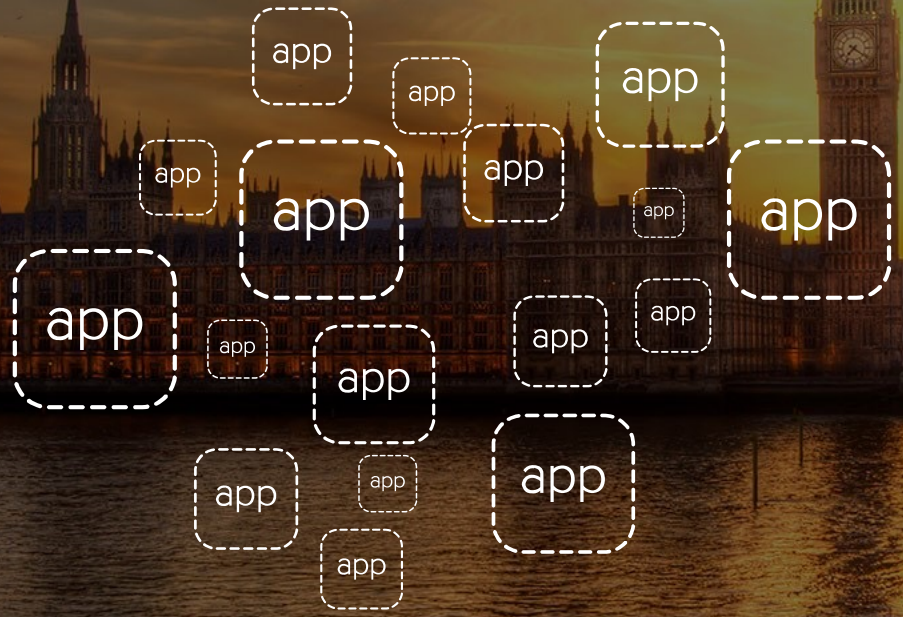
Don’t get stung by #OWASP Top 10

Shain Singh | Security Solutions Architect

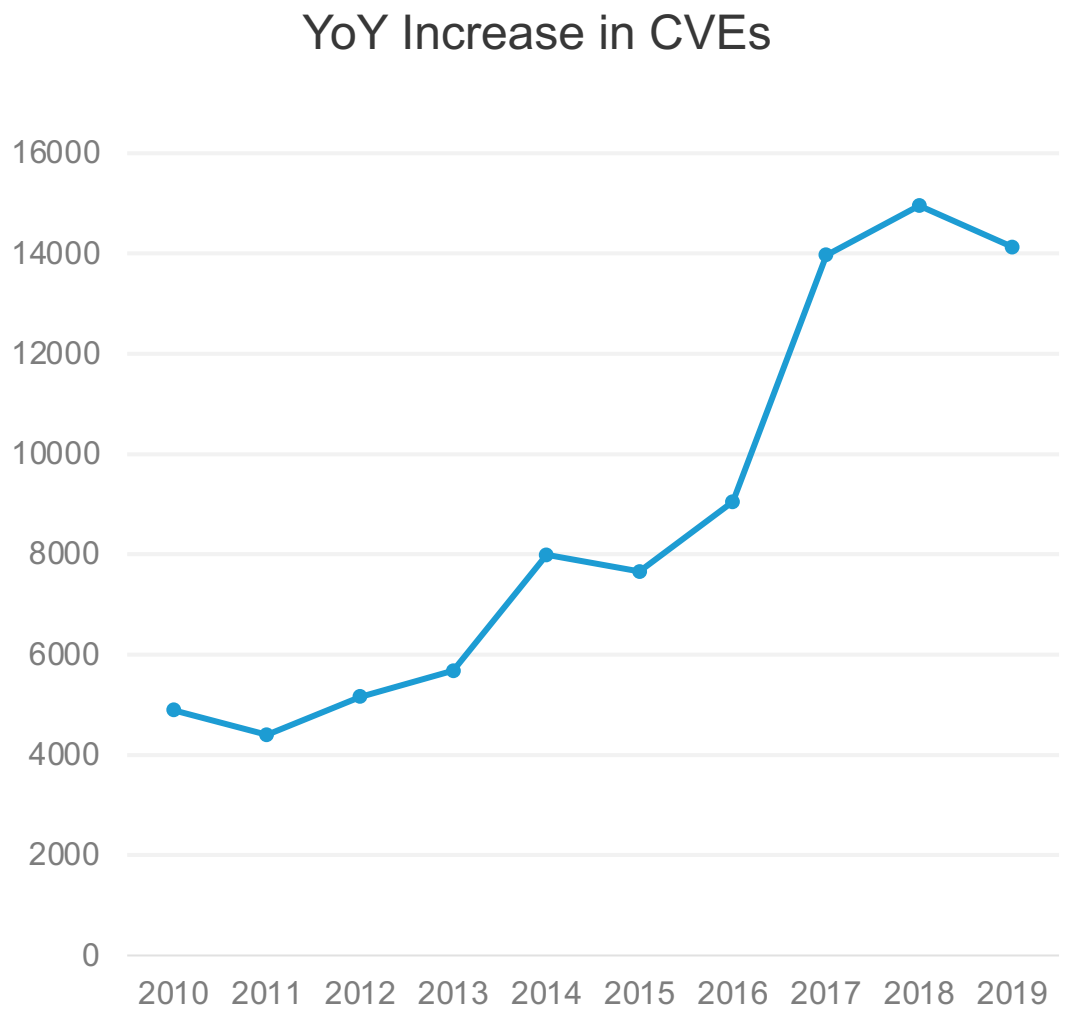
Shahnawaz Backer | Principal Security Advisor



The average organization uses 983 apps

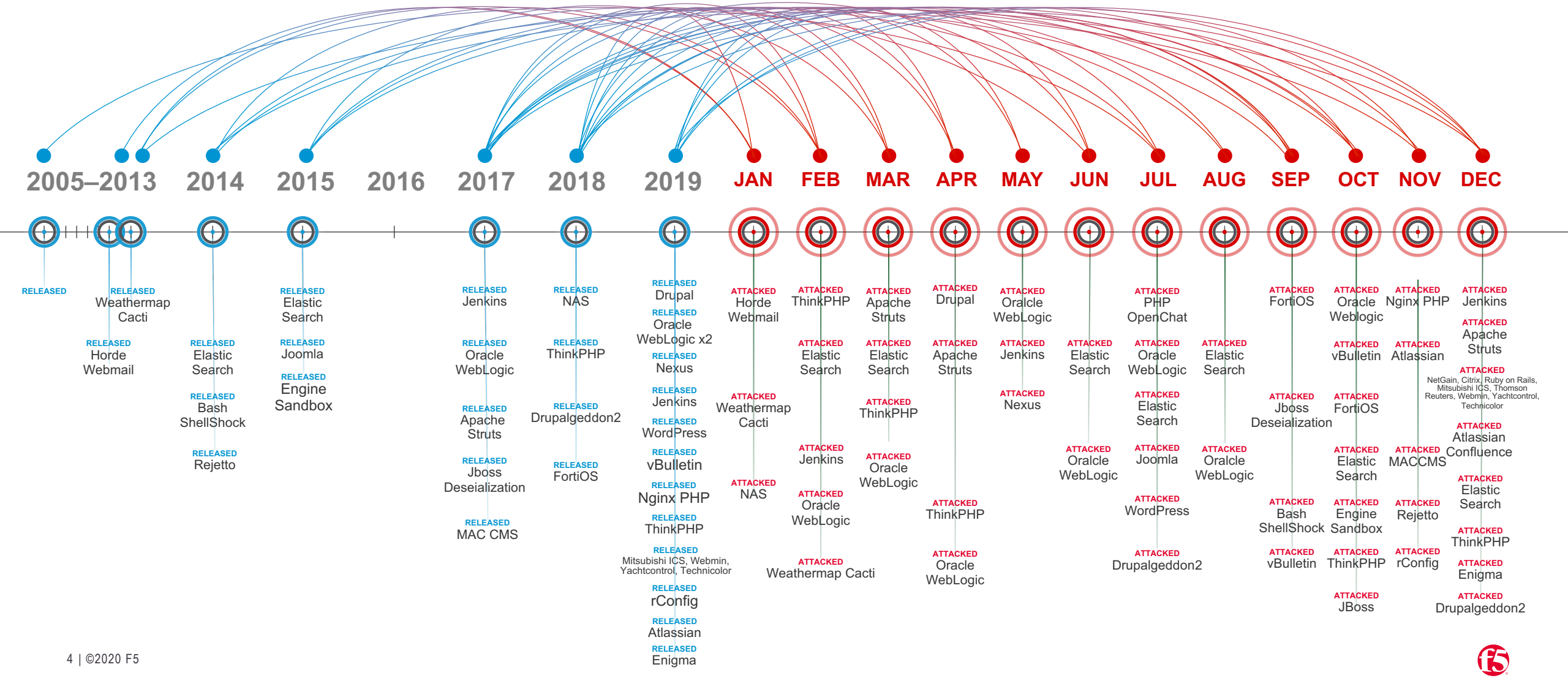
How many are mission critical?

New vulnerabilities are discovered in all manner of software all the time



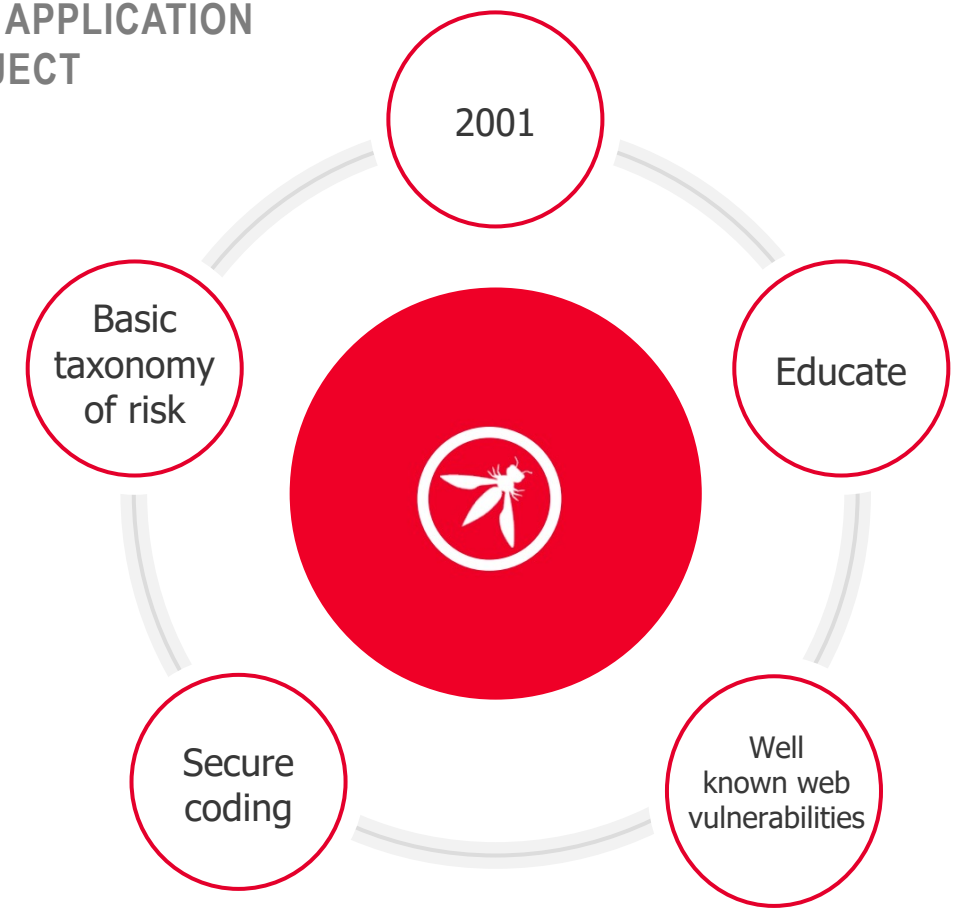
Note: Excludes any rejections or disputes

Vulnerability Release Date vs Active Attack Campaign



OWASP

THE OPEN WEB APPLICATION SECURITY PROJECT



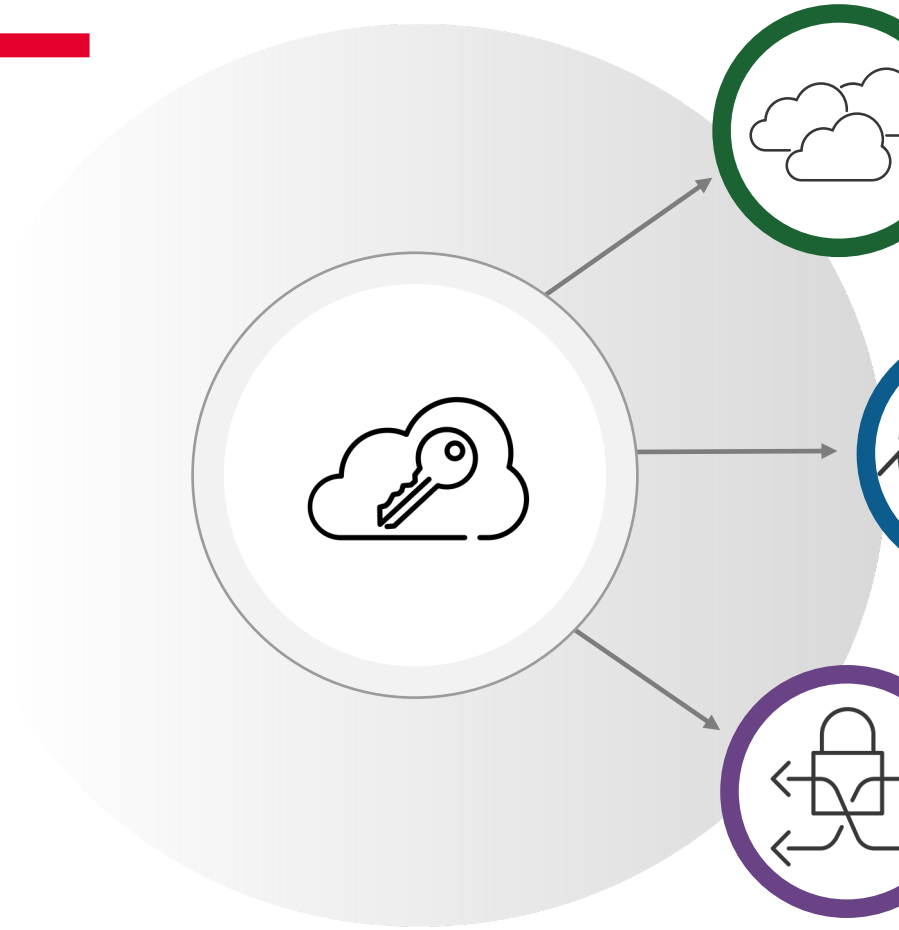
THE OWASP TOP 10

VULNERABILITIES AND MITIGATIONS

OWASP also publishes the API Security Top 10, the Mobile Top 10, the IoT Top 10, and the Automated Threats list

Security Challenges in Today's Multi-Cloud, App Driven World

RETHINKING APP SECURITY



Consistency

Deploying and managing a global application security policy across multiple cloud architectures.

Appropriate Controls

Sacrificing security for perceived convenience of cloud provider, "cloud-native" services.

Agility

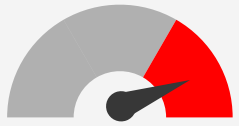
Enforce SecOps-authorized security smoothly in the Dev-Ops CI/CD process.

Don’t Trust the User. Ever.

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Injection

ATTACK VECTORS
Exploitability



SECURITY WEAKNESS
Prevalence

SECURITY WEAKNESS
Detectability

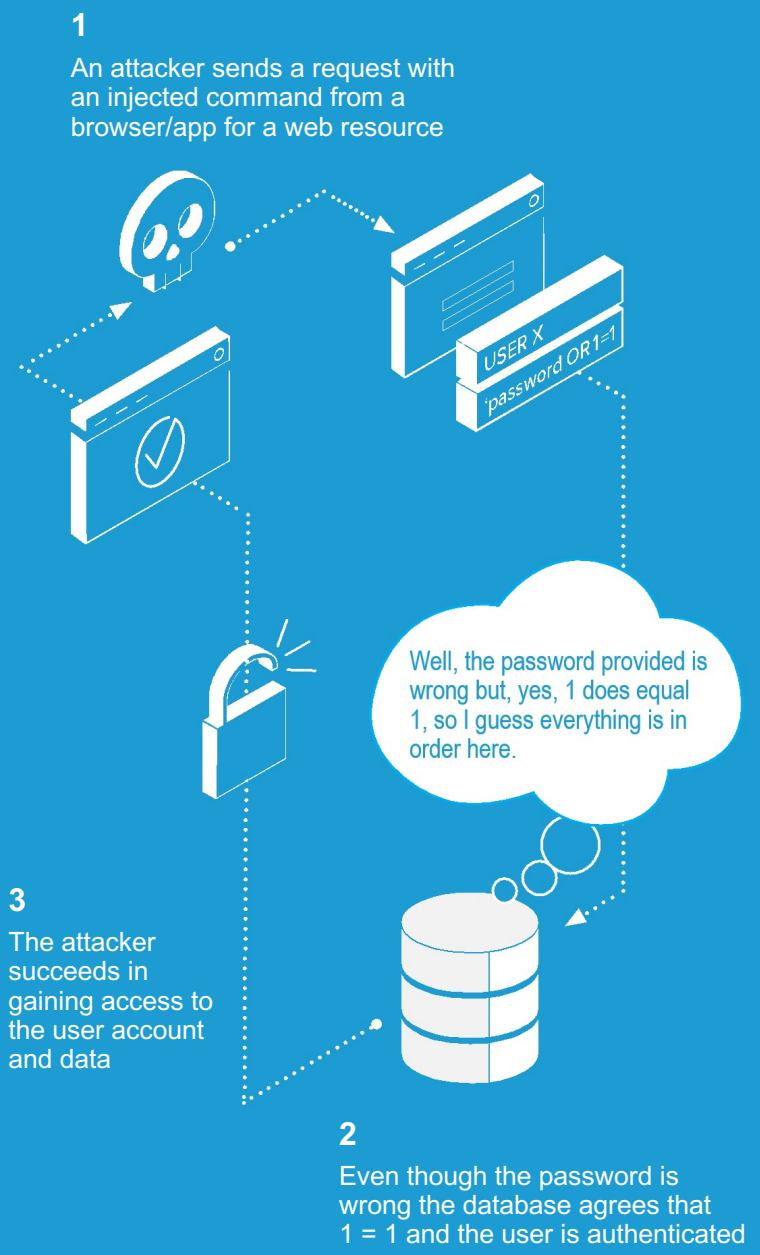
IMPACT
Technical

Vulnerable

- User-supplied data is not validated, filtered, or sanitised

Can lead to

- Data loss
- Data corruption
- Denial of service
- Remote code execution
- Host take over



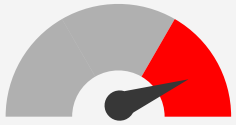
XML External Entity (XXE) Attacks

ATTACK VECTORS
Exploitability

SECURITY WEAKNESS
Prevalence

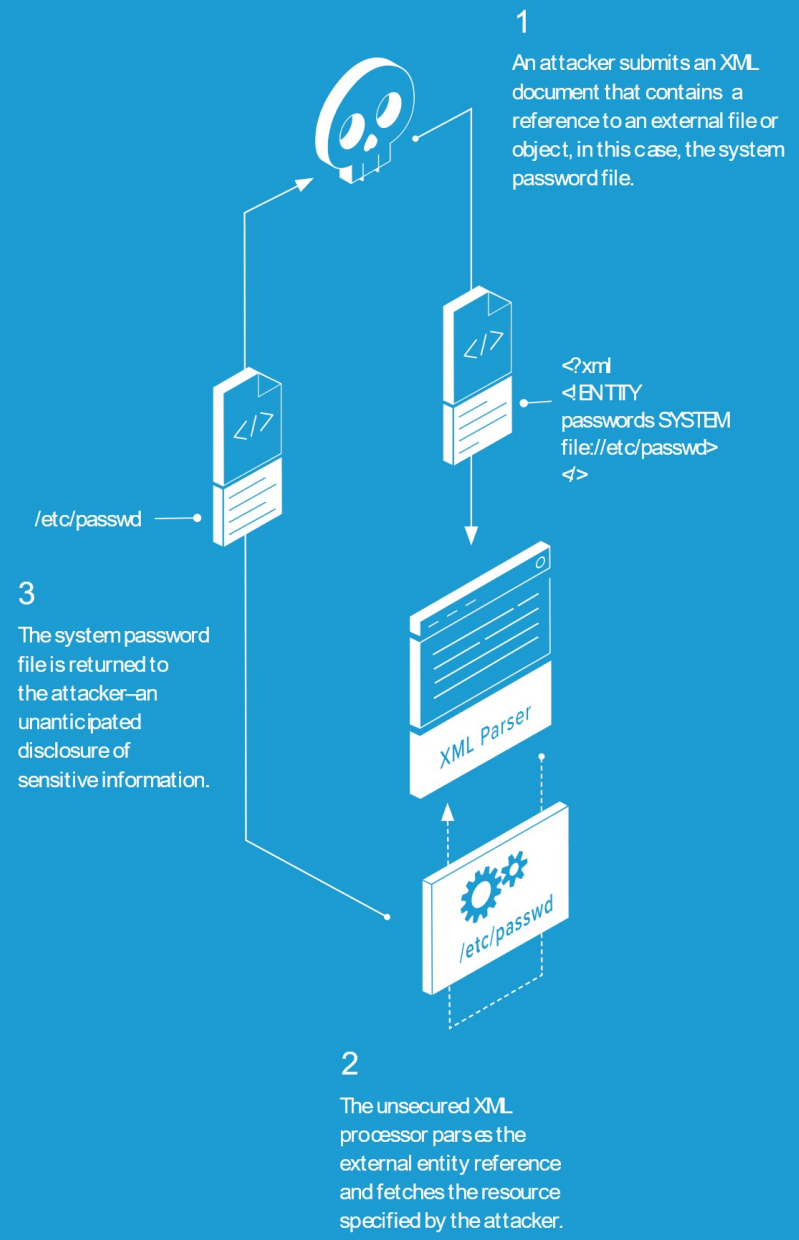
SECURITY WEAKNESS
Detectability

IMPACT
Technical



Vulnerable?

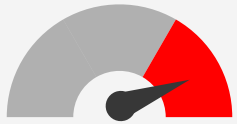
- XML directly or XML uploads
- XML processor has Document Type Definitions (DTDs) enabled
- Uses SOAP prior to version 1.2
- Not limited to web applications
- Valid functionality of the XML language



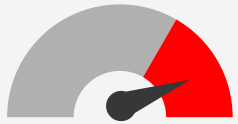
A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Cross-Site Scripting (XSS)

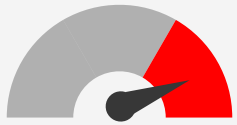
ATTACK VECTORS
Exploitability



SECURITY WEAKNESS
Prevalence



SECURITY WEAKNESS
Detectability



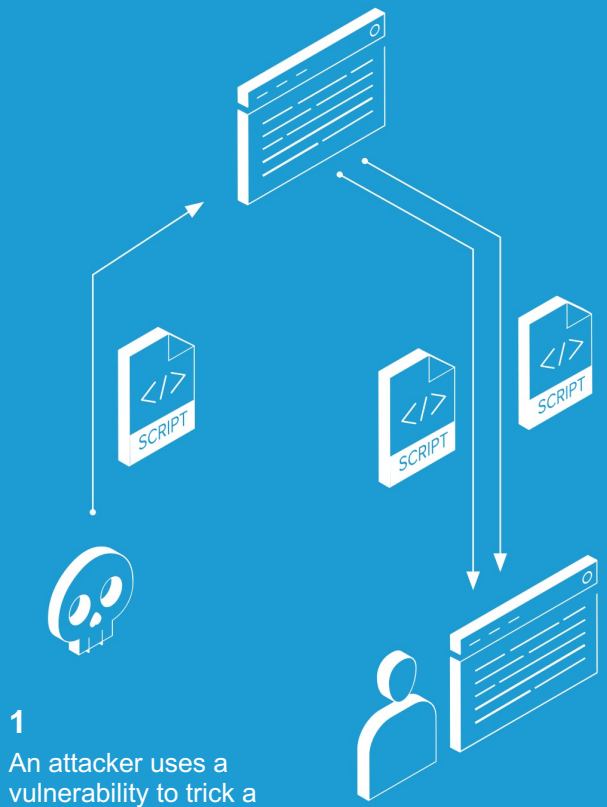
IMPACT
Technical

Three forms of XSS

- Reflected XSS
- Stored XSS
- Document Object Model (DOM) XSS

Can lead to

- Session hijacking
- Loss of data
- Fraudulent transactions
- Cross-Site Request Forgery (CSRF) defense avoidance



1
An attacker uses a vulnerability to trick a website in to running malicious code

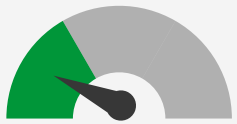
2
A visitor to the website makes a request for a normal web resource, for example, an image

3
The visitor unknowingly receives and executes the legitimate web resource as well as the attackers malicious code

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Insecure Deserialisation

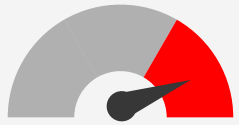
ATTACK VECTORS
Exploitability



SECURITY WEAKNESS
Prevalence

SECURITY WEAKNESS
Detectability

IMPACT
Technical

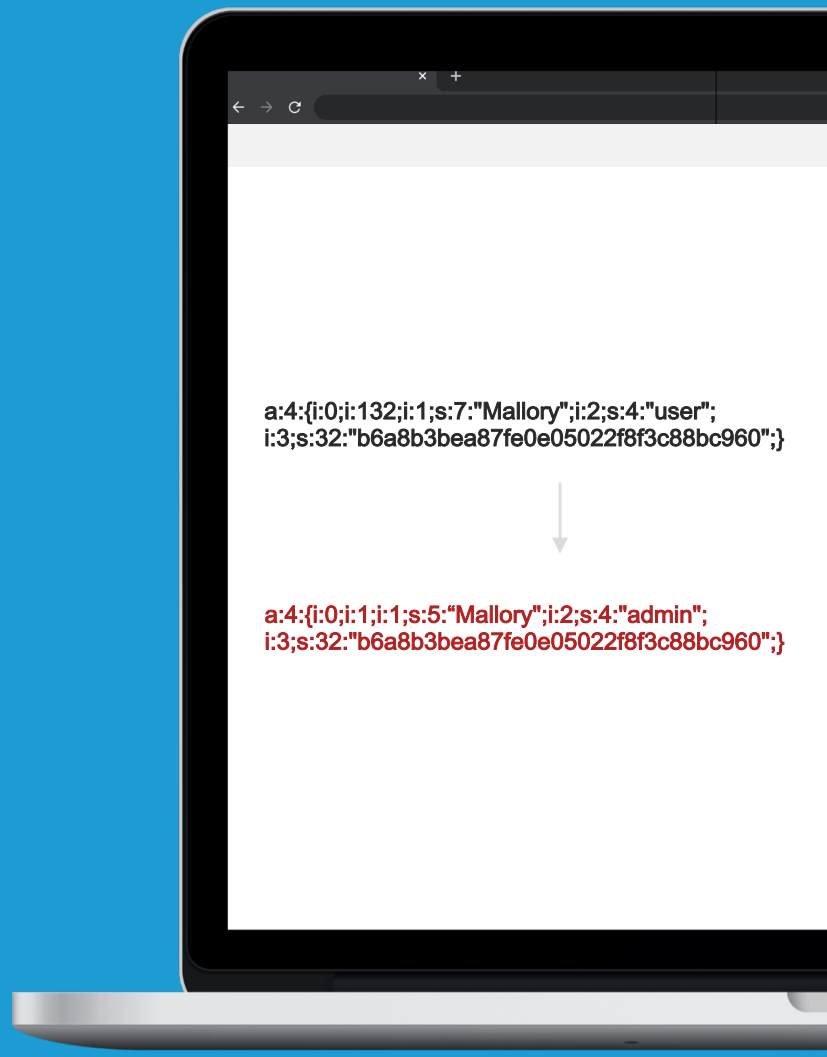


Vulnerable

- Serialised data treated as an object
- Not inspected and sanitised as other inputs

Can lead to

- Cross-site scripting, cookie theft
- Elevation of privileges
- Remote code execution



MITIGATING

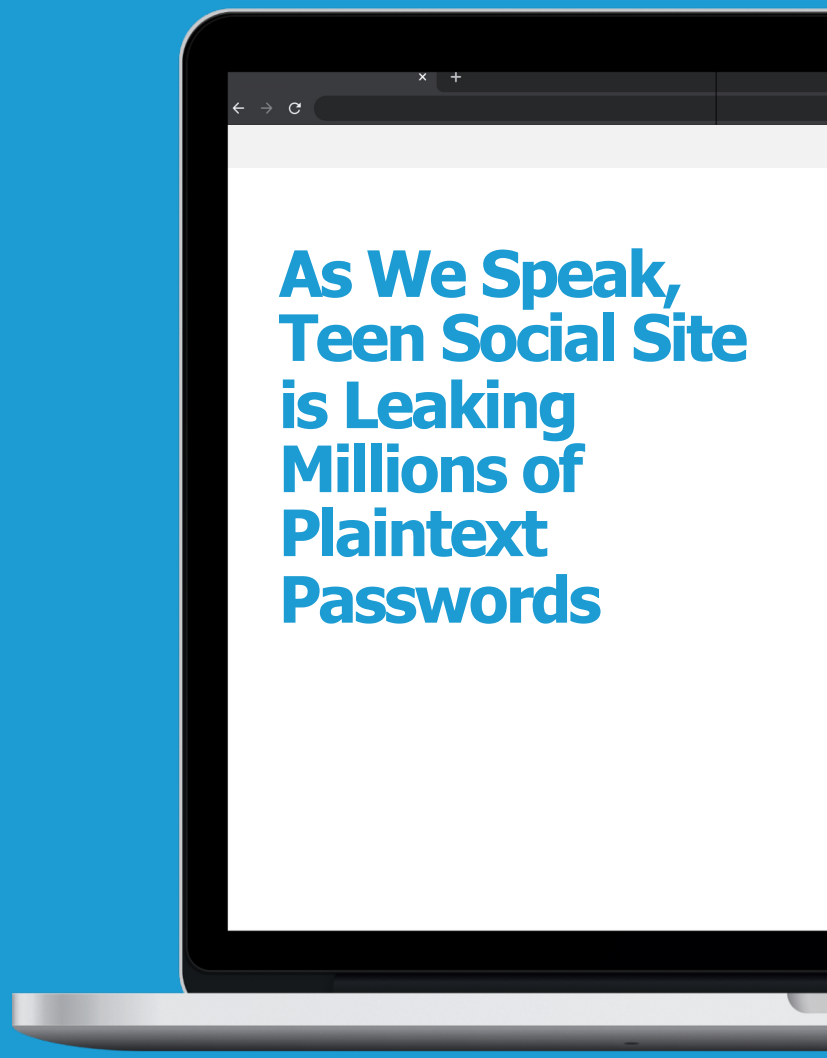
Injection

Prevention

- Keep data separate from commands and queries
- Use a safe API
- Whitelist server-side input validation
- Use LIMIT & other controls to prevent mass disclosure of records

Victims

- Country's Commission on Elections: 77,736,795 Records
- Teen Social Site: 5.5 Million Teenage Accounts
- Major University: 400,000 Names & email Addresses
- Midwest Urology Group: 521,659 Patients



MITIGATING

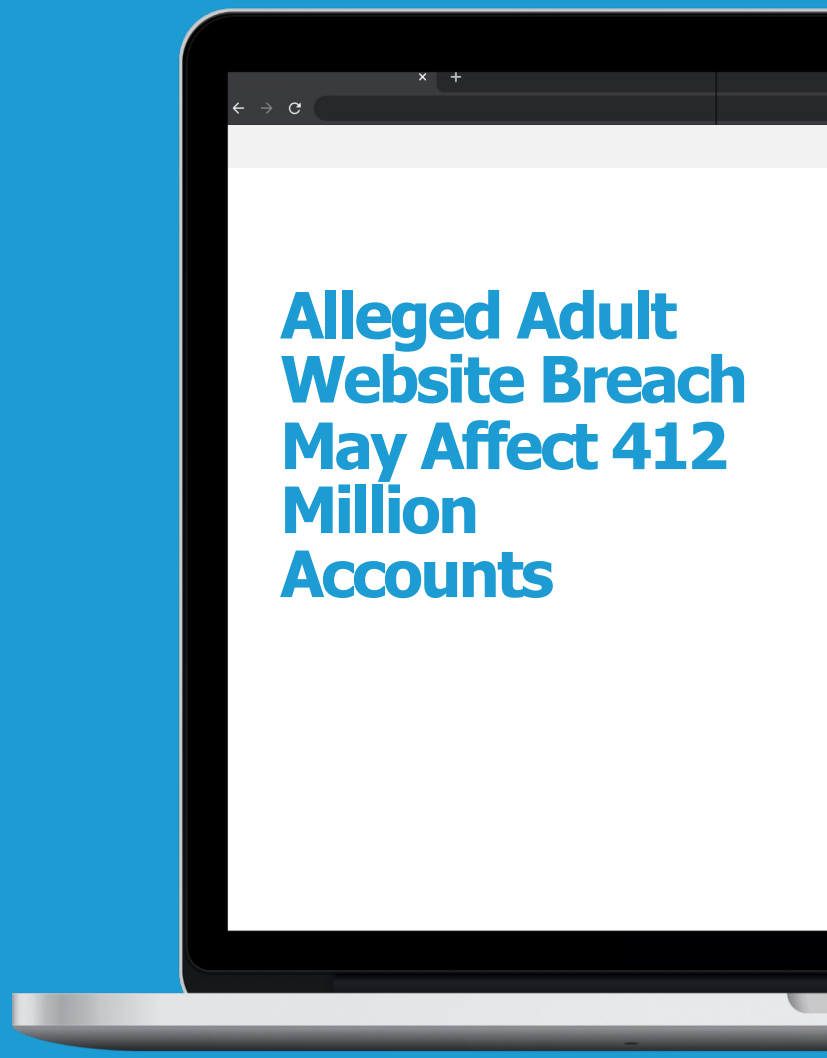
XML External Entity (XXE) Attacks

Prevention

- Dev Training
- Use less complex data formats: JSON
- Avoiding serialization of sensitive data
- Patch/upgrade all XML processors

Victims

- Multiple Adult Sites Hit: 3.5 million accounts



MITIGATING

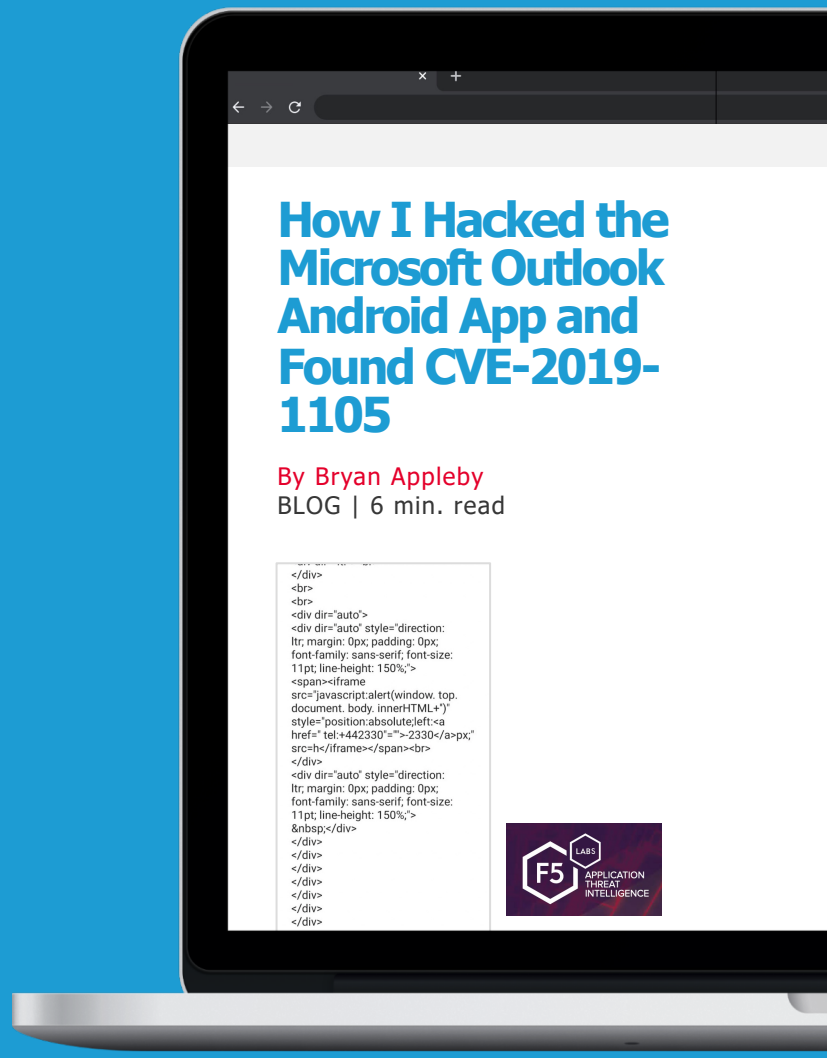
Cross-Site Scripting (XSS)

Prevention

- Separation of untrusted data from active browser content.
- Using frameworks that automatically escape XSS by design
- Escaping untrusted HTTP request data based on the context
- Context-sensitive encoding when modifying the browser document on the client side.
- Enabling a Content Security Policy as a DiD vs. XSS.

Victims

- Major European Airline: 380,000 booking transactions
- Social Messaging Site: Potentially 330 Million Accounts
- Online Auctioning/Sellers Site: Potentially 175 Million Accounts



[1] https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019--episode-3--web-injection-attacks
[2] https://www.f5.com/labs/articles/threat-intelligence/how-i-hacked-the-microsoft-outlook-android-app-and-found-cve-2019-1105

MITIGATING

Insecure Deserialization

CVE-2020-0688 (MS Exchange RCE) just landed to @metasploit, just needs a domain user with a mailbox for SYSTEM code exec

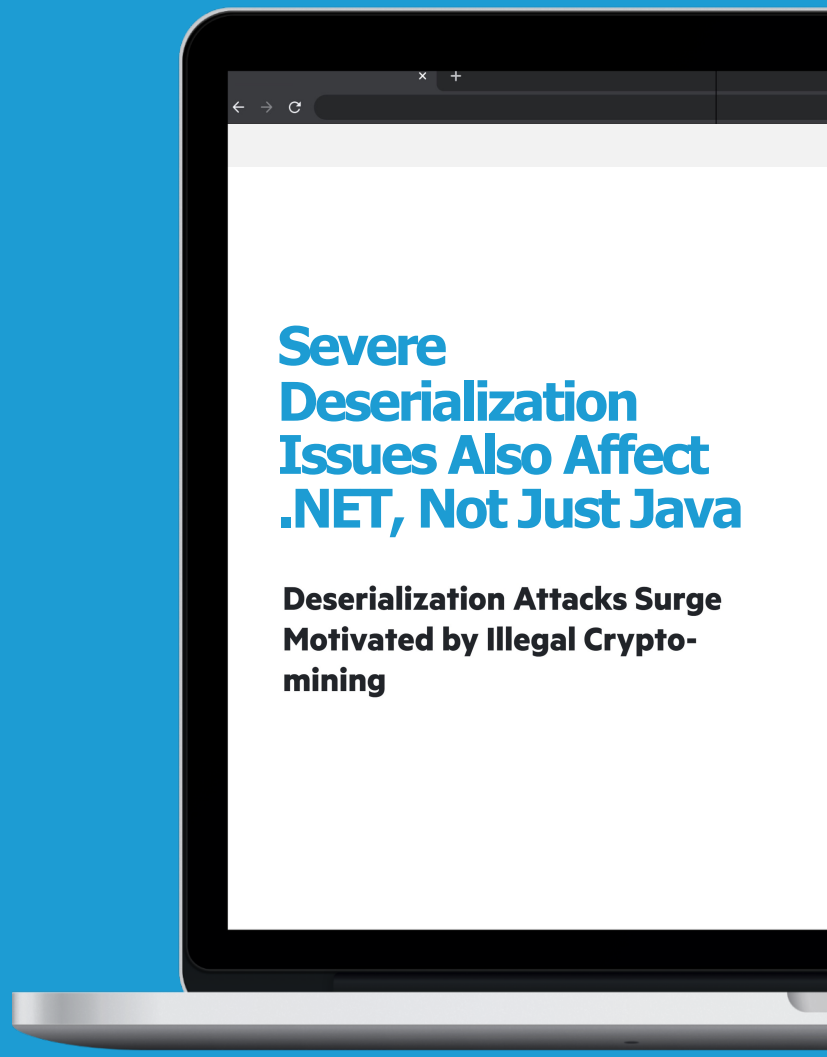
RAPID7 RAPID7 RAPID7 RAPID7

Add an exploit for Exchange ECP ViewState deserialization (...
This PR adds an exploit module for CVE-2020-0688 (Exchange ECP ViewState Deserialization). The viewstate ...
github.com

Prevention

"The only safe architectural pattern is not to accept serialized objects from untrusted sources or to use serialization mediums that only permit primitive data types."

- OWASP

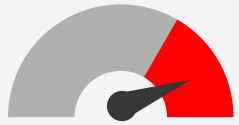


Let the Right One In

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Broken Authentication

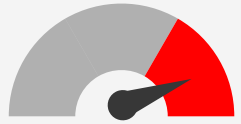
ATTACK VECTORS
Exploitability



SECURITY WEAKNESS
Prevalence

SECURITY WEAKNESS
Detectability

IMPACT
Technical



Can lead to

- Brute force / Credential stuffing
- Session high jacking
- Session fixation
- Cross Site Request Forgery (CSRF)
- Execution After Redirect (EAR)
- One-click attack

UK's National Cyber Security Centre (NCSC) the Top 10 most common passwords in 2019

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. Password1
10. 12345

National Cyber Security Centre

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

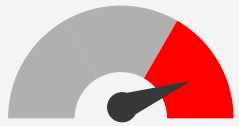
Sensitive Data Exposure

ATTACK VECTORS
Exploitability

SECURITY WEAKNESS
Prevalence

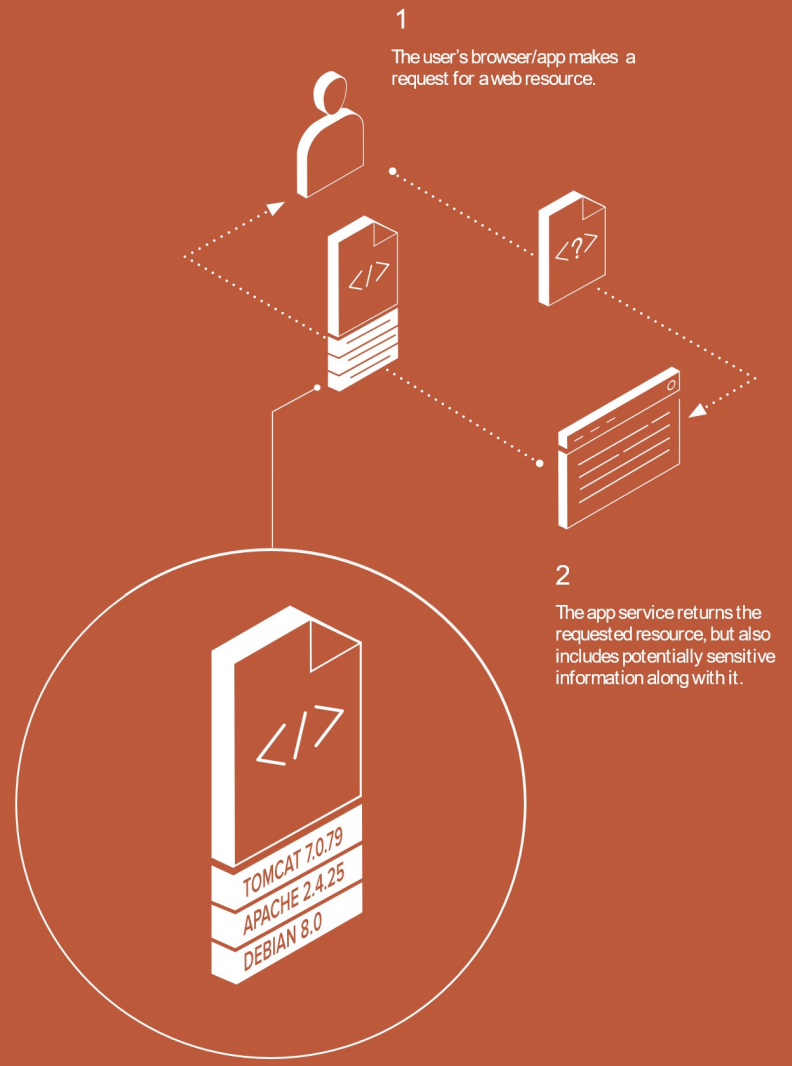
SECURITY WEAKNESS
Detectability

IMPACT
Technical



Vulnerable?

- Data transmitted in clear text
- Using old or weak cryptographic algorithms
- Default or weak crypto keys
- Encryption not enforced



A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

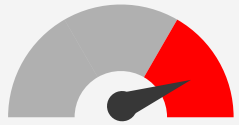
Broken Access Control

ATTACK VECTORS
Exploitability

SECURITY WEAKNESS
Prevalence

SECURITY WEAKNESS
Detectability

IMPACT
Technical



Fallout

- Unauthorised access to sensitive information
- Inappropriate creation or deletion of resources
- User impersonation
- Privilege escalation

Thousands of Amazon S3 buckets left open exposing private data

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

MITIGATING

Broken Authentication

Victims

- **Credit agency / Supermarket:** 431,000 tax and salary data
- **Payroll provider:** 550,000 clients
- **Video platform:** 30 million accounts
- **Ticket broker:** 1.5 million airline passengers

Prevention

- Multifactor
- No default credentials
- Weak password check
- Hardened registration and recovery
- Limit failed attempts
- SessionID

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

MITIGATING

Sensitive Data Exposure

Victims

- **Healthcare / insurance billing processor:** 1.7GB personal data / 90K
- **Pharmaceutical company:** 78,000 patients

Prevention

- Classify data (sensitive)
- Controls per class
- Discard after use
- Encrypt in transit / at rest
- Strong algorithms / protocols / keys
- Salt passwords

Report: Thousands of pharmaceutical records leaked in possible HIPAA* violation

*Health Insurance Portability and Accountability Act

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

MITIGATING

Broken Access Control

Victims

- Too many to count

Prevention

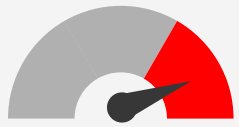
- Access control is only effective if enforced in trusted server-side code or server-less API
- Implement once and re-use them throughout the application
- Unique application business limit requirements
- Rate limit API and controller access
- Deny by default

Strong Basics

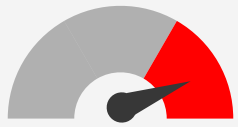
A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Security Misconfiguration

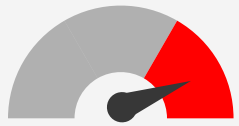
ATTACK VECTORS
Exploitability



SECURITY WEAKNESS
Prevalence



SECURITY WEAKNESS
Detectability



IMPACT
Technical

Fallout

- Brute force, credential stuffing
- Code injection
- Buffer overflow
- Command injection
- XSS
- Forceful browsing

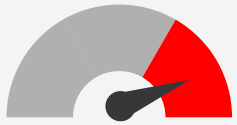
Security misconfiguration can leave apps vulnerable to multiple attacks

A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Using Components with Known Vulnerabilities

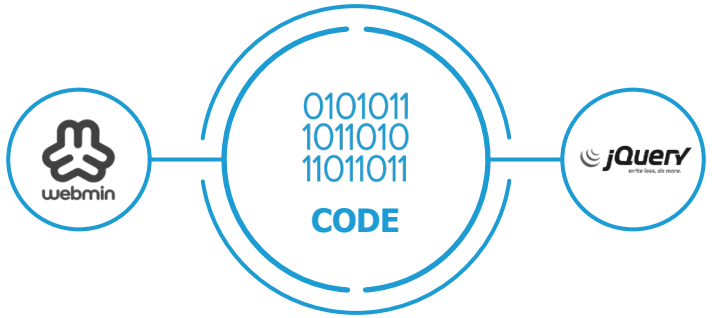
ATTACK VECTORS
Exploitability

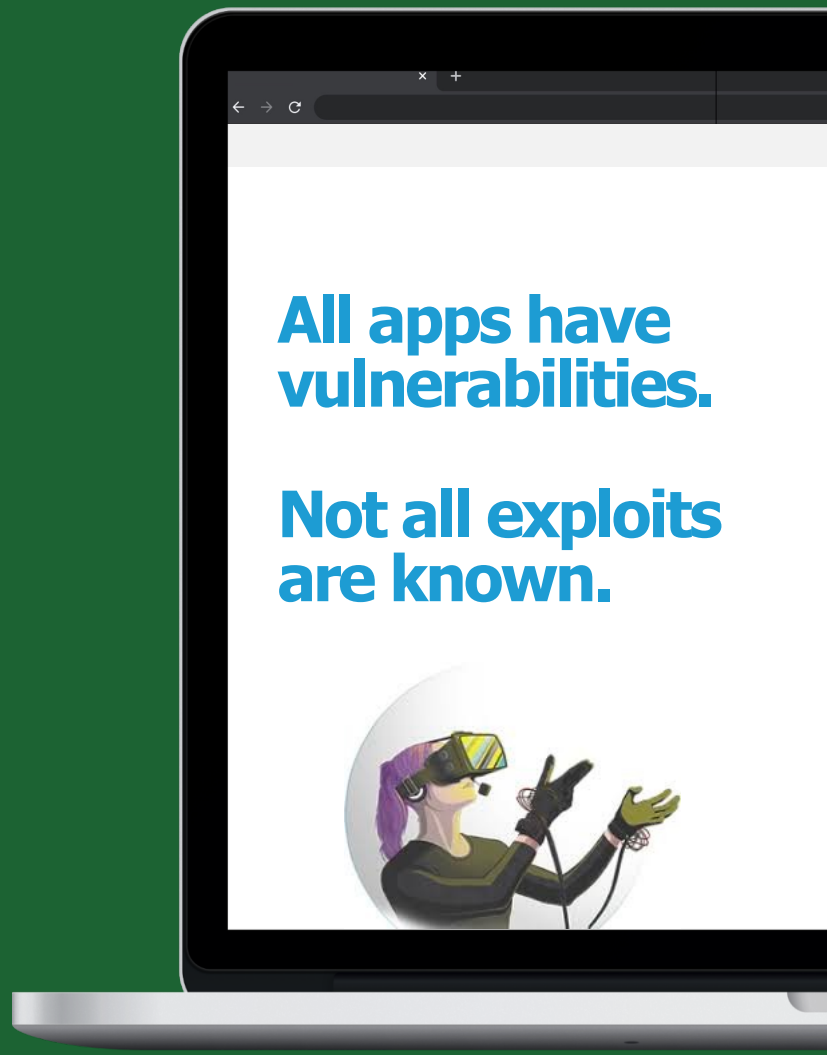
SECURITY WEAKNESS
Prevalence



SECURITY WEAKNESS
Detectability

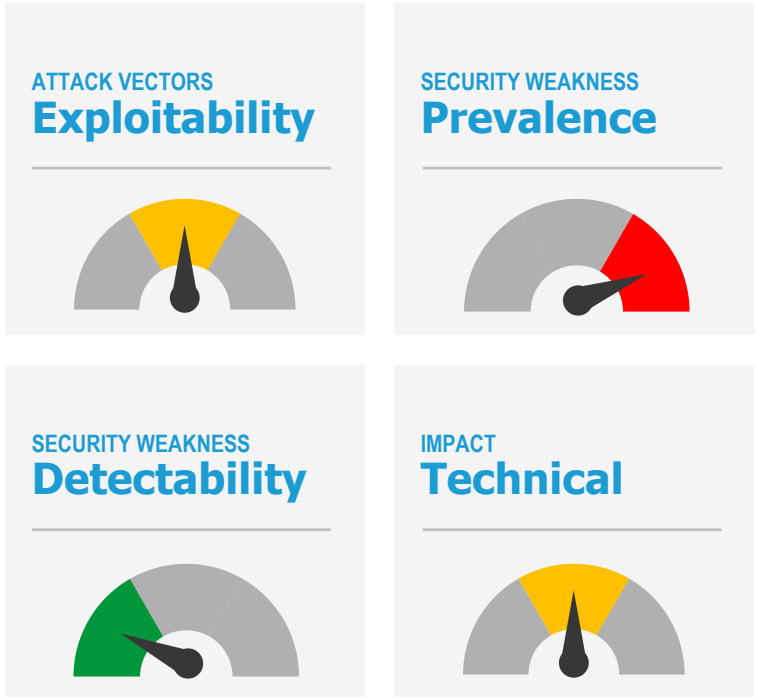
IMPACT
Technical





A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Insufficient Logging and Monitoring



Can lead to

- Code injection
- Buffer overflow
- Command injection
- XSS
- Forceful browsing

Attackers rely on complacency and blind spots to gain access to apps

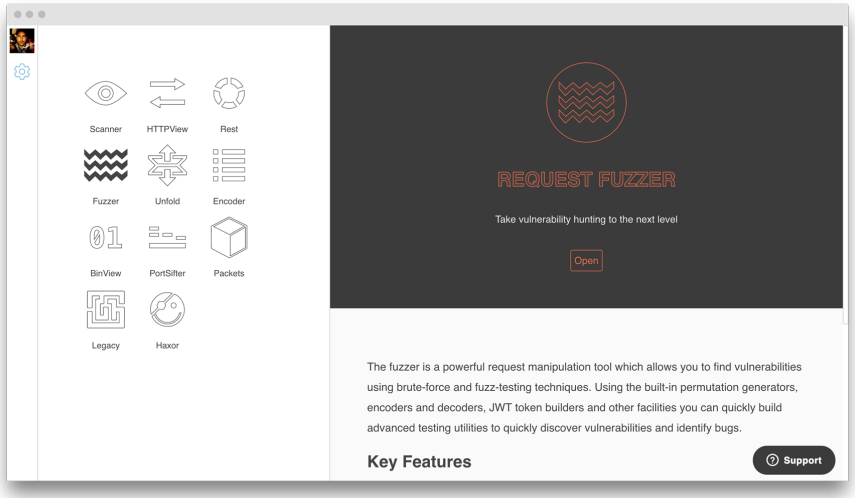
A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

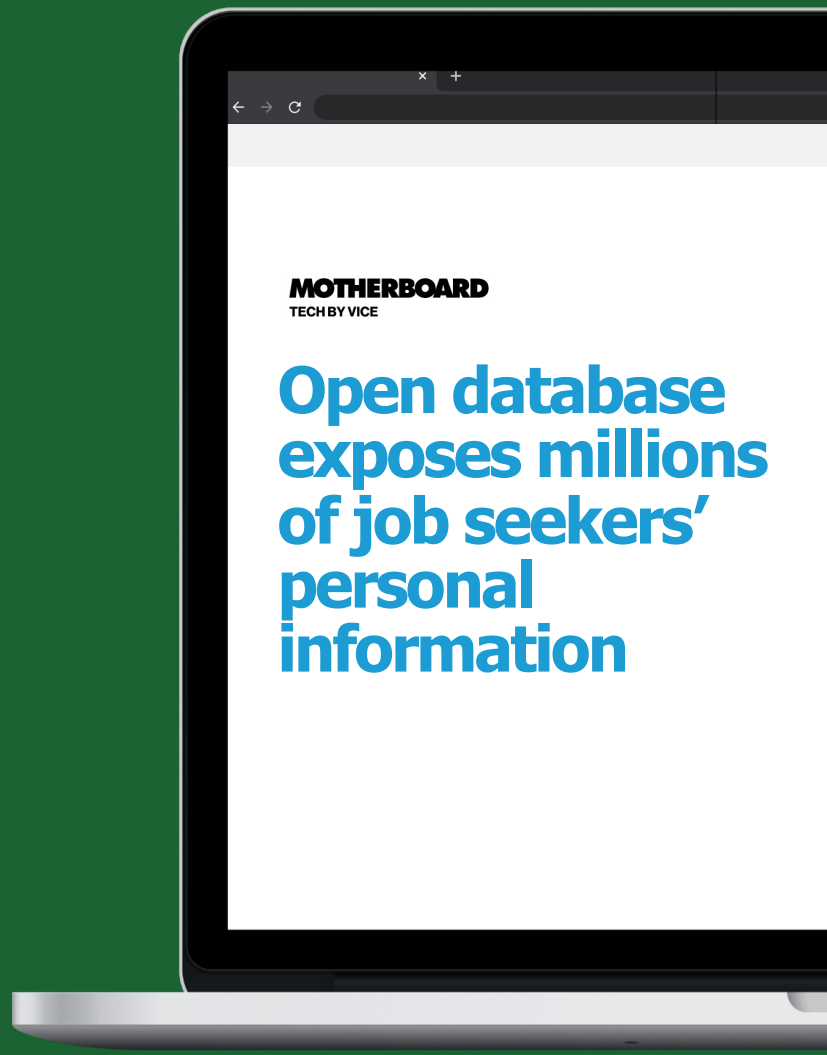
MITIGATING

Security Misconfiguration

Prevention

- Repeatable hardening
- Minimal platform and features
- Asset / inventory / patch management
- Segmented architecture
- Automate verification





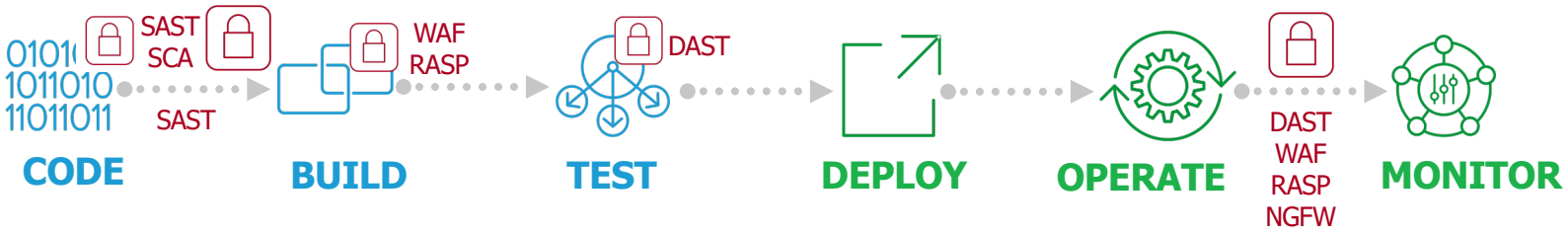
A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

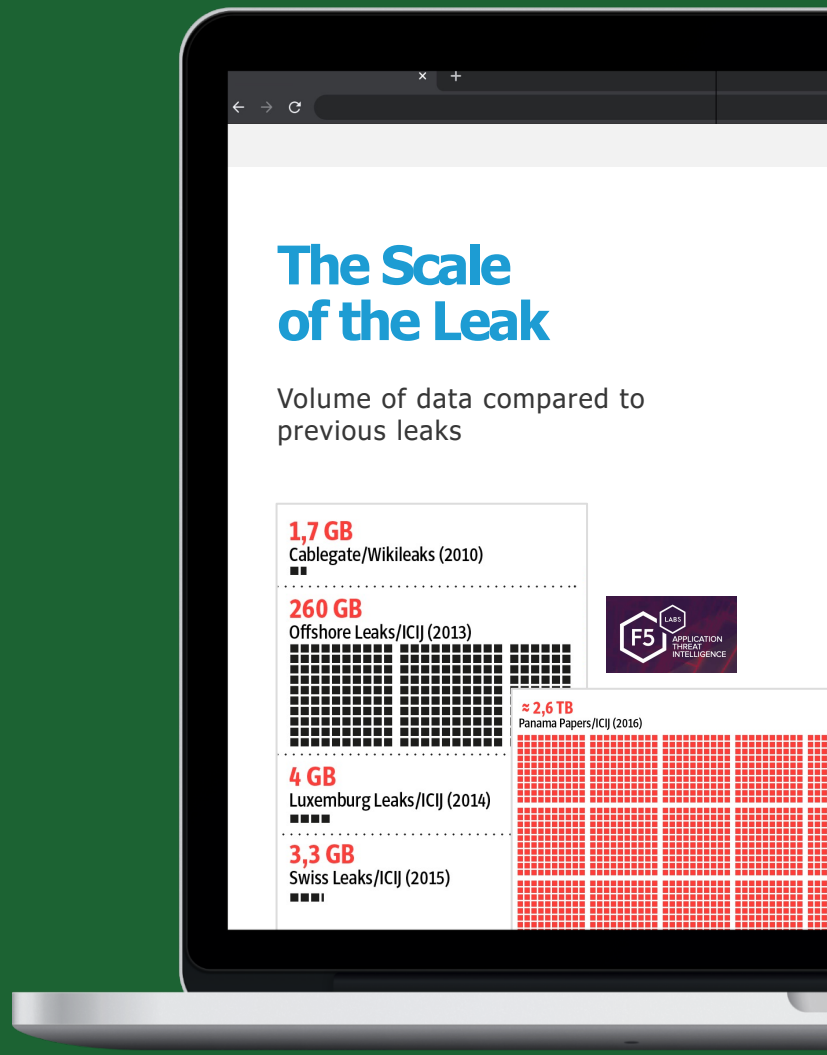
MITIGATING

Using Components with Known Vulnerabilities

What is the risk?

- Most common vulnerability in 2019 is jQuery XSS (CVE-2012- 6708)
- CVE-2017-5638 Apache Struts resulted in a major data breach





A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

MITIGATING

Insufficient Logging and Monitoring

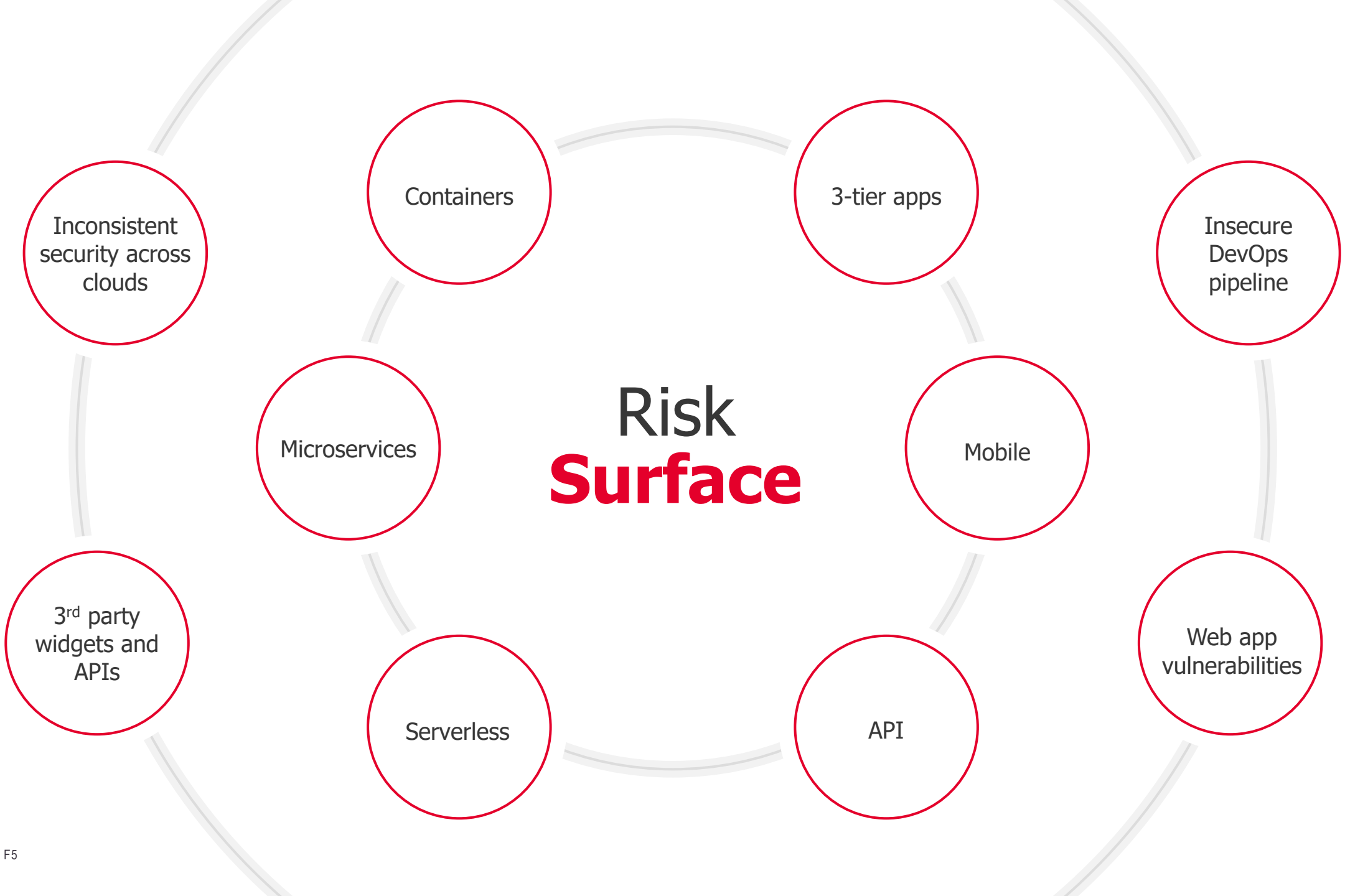
What could happen?

"Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%."

– **OWASP**

Applications and identities are cyber attackers' primary targets

Protect Every App


Risk
Surface
Containers
3-tier apps
Insecure DevOps pipeline
Inconsistent security across clouds
Microservices
Mobile
Web app vulnerabilities
3rd party widgets and APIs
Serverless
API