Journey to Low Code / No Code App Security

Learn how to secure your application & data with a low code or no code approach!

24th September – 6 PM-8 PM (GST)
Secure your single page web app with low code on IBM Cloud
https://www.crowdcast.io/e/journey-to-low-code-no-code-app-security-1

28th September – 6 PM-8 PM (GST)
Easily Secure your Spring Boot app with Low code / No code
https://www.crowdcast.io/e/journey-to-low-code-no-code-app-security-2

30th September – 6 PM-8 PM (GST)
Securely Manage access to your Application Sensitive Data on IBM Cloud
https://www.crowdcast.io/e/journey-to-low-code-no-code-app-security-3

GISPP

ELLE/TECH
WOMEN IN TEAMS

BUSINESS INNOVATION

REHNUMAA
lead the way...

OpenUAE

SKYSNAG

ArabWIC

Secure your single page web app with low code on IBM Cloud

Asna Javed
Lead Developer Advocate, IBM PAK

Divya S
Security Consultant, IBM India

Get Started here: https://ibm.biz/appsecurity

Frequently Asked Questions

All sessions are recorded automatically and **Recording** will be available instantly when live broadcast will end.

You do need a basic understanding of **Programming & security.**

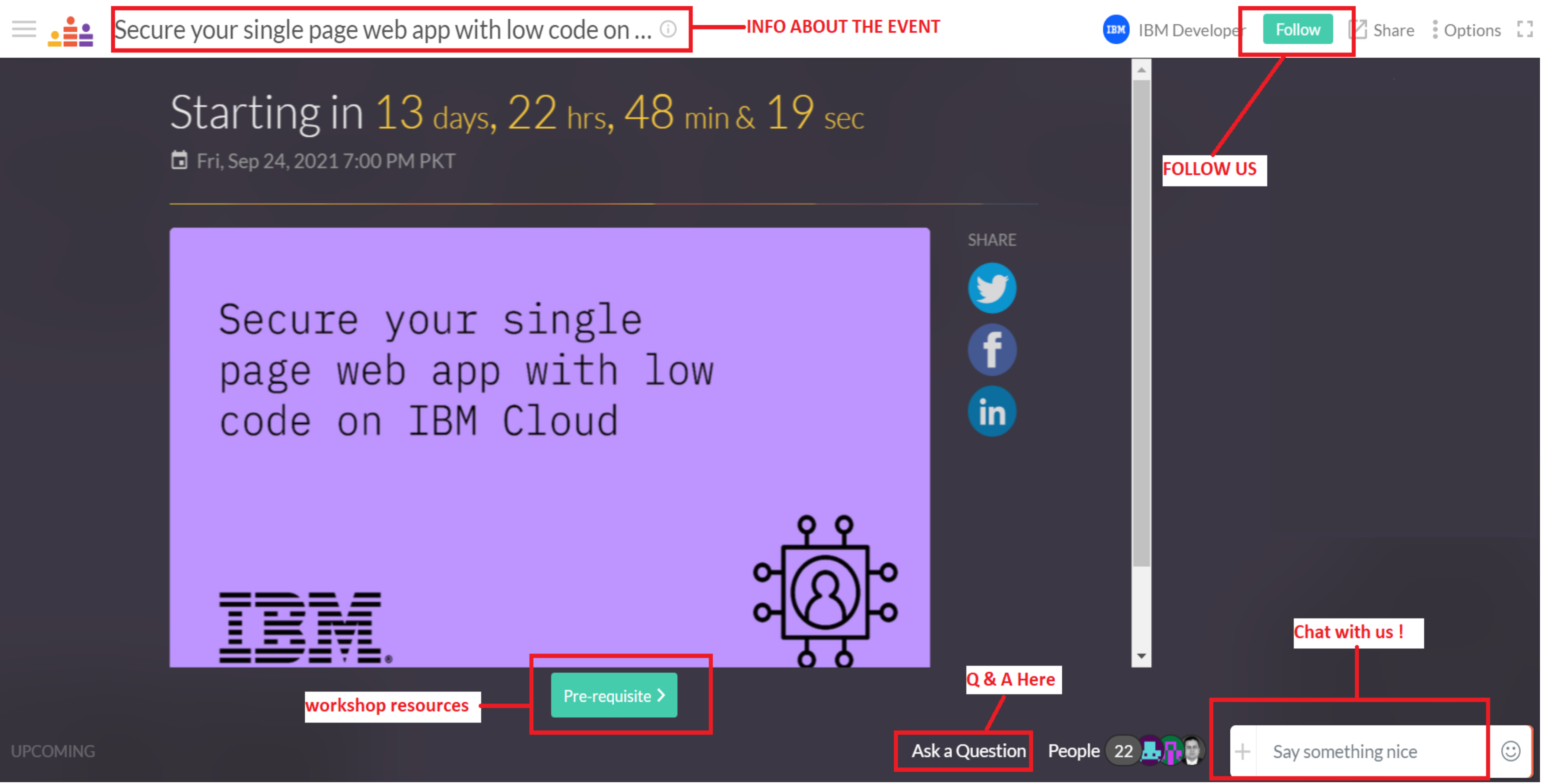
Just log in or create your **IBM Cloud Account** from https://ibm.biz/appsecurity and you're good to go!

Yes, **Certificate** will be given within two weeks of completion of series.

Q&A session will happen at the end. Stay tuned!

How to join the IBM Developer Community? **Join our Facebook community**

https://www.facebook.com/groups/ibmdevelopermea/



Secure your single page web app with low code on ...

Starting in 13 days, 22 hrs, 48 min & 19 sec

Fri, Sep 24, 2021 7:00 PM PKT

Secure your single page web app with low code on IBM Cloud

INFO ABOUT THE EVENT

FOLLOW US

workshop resources

Q & A Here

Chat with us !

Get your Certificate!

To get your participation certificate email us with the following info:

1. First Name
2. Last Name
3. Email ID you used to create your cloud account
4. Email ID you used to attend the live workshops on crowdcast.

Let's get started

- Sign up/Login to IBM Cloud: https://ibm.biz/appsecurity

- Follow along with the hands-on: https://github.com/IBMDeveloperMEA/Secure-your-single-page-web-app-with-low-code-on-IBM-Cloud

Get Started here: https://ibm.biz/appsecurity

Agenda

- Intro to low code/ No code Application Security
- Why we should learn Application security
- Recent developments
- AppID: What, Why & How
- Using AppID and What Does the Flow Looks Like?
- Authentications vs authorization
- Managing authentication
- Understanding the flow of Single-page apps
- Hands-on

https://meetingking.com/how-to-create-a-meeting-agenda/

Guest Speaker:

Ayesha Iftikhar

- Researcher & Co-founder and Mentor

Muhammad Nadeem

- Application Security Consultant

Get Started here: https://ibm.biz/appsecurity

Introduction to low-code/ no-code Application Security

Get Started here: https://ibm.biz/appsecurity

The evolving digital economies

- To survive in the digital economy:
- we need digital transformation at digital speed
- connect data, people and processes to compete, scale and win
- smooth app capabilities across multiple devices
- business and IT must work together
- hence, need for more powerful, faster, and business-friendly digital platforms

Why low-code/ no-code app development?

Get Started here: https://ibm.biz/appsecurity

- low-code can be a game changer:
- tools/ digital platforms that create applications with visual programming capabilities
- drag-and-drop elements with no hardcore programming involved
- use a number of approaches to automate and abstract app development
- supports faster and reliable app development without any coding
- these platforms need a varying level of technical expertise

Get Started here: https://ibm.biz/appsecurity

Low-code/ no-code app development benefits

- Improved agility
- Decreased costs
- Higher productivity
- Better customer experience
- Effective risk management and governance
- Change easily
- Faster transformation
- Drag-and-drop interfaces
- Instant mobility
- Declarative tools
- Security and scalability

Get Started here: https://ibm.biz/appsecurity

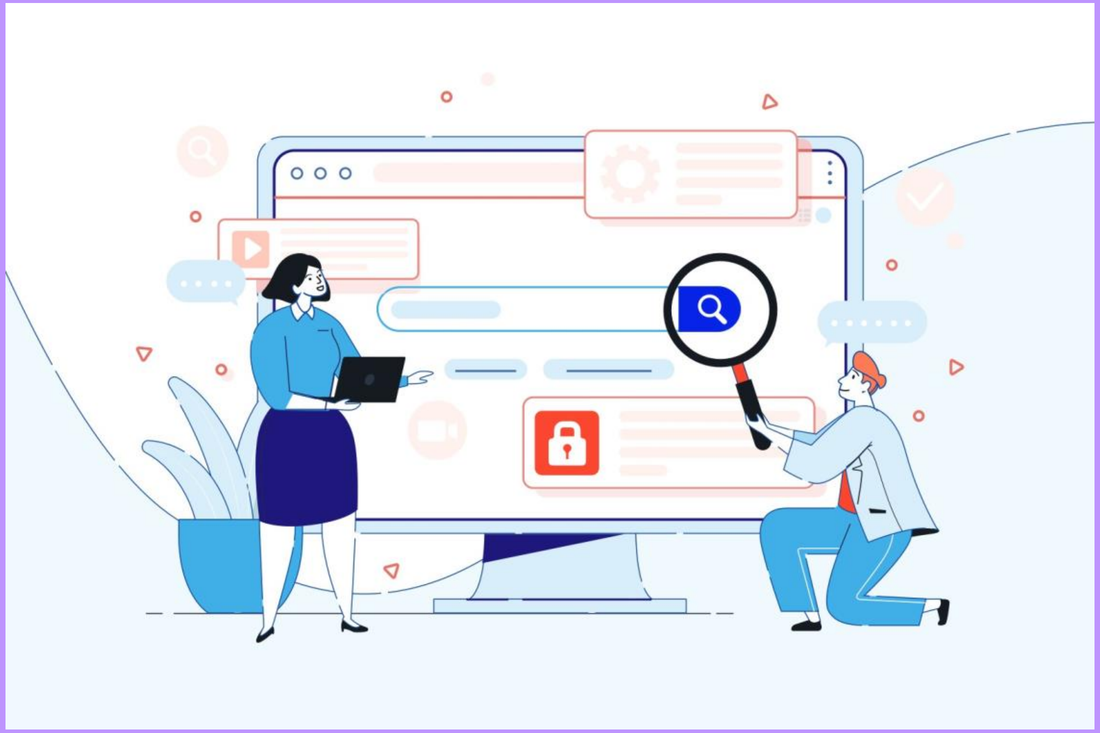
App security with low-code/ no-code development approach

- Low-code/no-code tools are powerful, fast and user friendly BUT,
- security is a critical aspect
- if its not secure, it is not a practical solution
- the success of a business now lies in a secure eco-system
- make sure that the platforms is able to protect the system and the platform both

Get Started here: https://ibm.biz/appsecurity

Security implications in low-code/ no-code

- These platforms impose major security challenges:
- handling power to less-security-aware and non-technical people is risky
- there may exist compromised libraries and leverage APIs that may cause sensitive data breaches
- may also facilitate an increase in shadow IT
- there is a potential for backdoors
- pose growing security risks



Get Started here: https://ibm.biz/appsecurity

Security concerns in low-code/ no-code

- Investigation reports have concluded that 43% of all data breaches are results of vulnerabilities at application layer
- Proprietary software's used in low-code/no-code platforms can have hidden vulnerabilities
- Trusting a platforms means placing faith in vendor for security processes
- Lack of security trainings to citizen developers impose a major threat

Get Started here: https://ibm.biz/appsecurity

Hardening low-code/ no-code environments

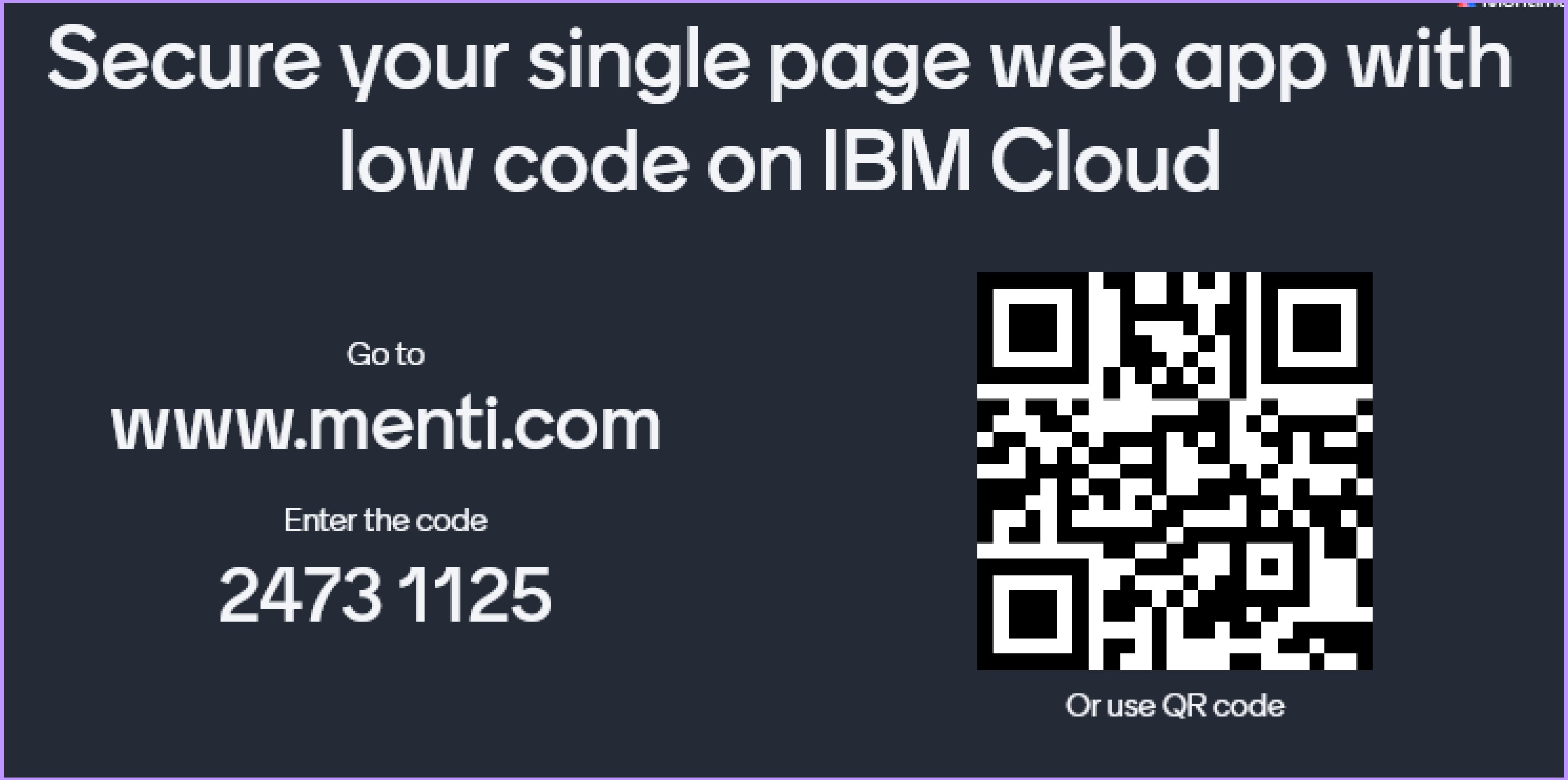
- Perform code analysis
- Examine/audit proprietary libraries
- Trusted partners
- APIs security tests
- Compartmentalize
- Security exercises for citizen developers
- Access control

Get Started here: https://ibm.biz/appsecurity

Developing responsible attitude towards security

- Secure all applications even if they are intended for internal use only
- Level up security understandings within the organizations
- Low-code/no-code platform users must be aware of the associated security threats and must have plans to address accordingly
- Vendors must arm their platforms sufficiently against associated threats
- Vendors must have vulnerability disclosure programs
- Establish means to accept bugs from white hat researchers for your products

Why should I learn security?



Secure your single page web app with low code on IBM Cloud

Go to

www.menti.com

Enter the code

2473 1125

Or use QR code

Get Started here: https://ibm.biz/appsecurity

Are you facing any of these challenges?

- I am not sure if my source code is secure?
- We are not sure whose responsibility, is it?
- We are not sure how to initiate software security program?
- I am incorporating security, but I am not sure if I am doing right/ enough
- We are using automated tools but there is a steady trend in detection of issues

Statistically speaking…

Get Started here: https://ibm.biz/appsecurity

- Global cybercrime losses to exceed $1 trillion annually(1)
- Average interruption to operations at 18 hours(2)
- The average cost is more than half a million dollars per incident(2)
- Two-thirds of surveyed companies reported cyber incident in 2019(2)
- Damage also includes downtime, brand reputation, and reduced efficiency(2)
- 56% organizations lack a plan to prevent/ respond to cyber attack(2)

[1] Report by mcafee.com, 2020

[2] https://www.businesswire.com/

Recent incidents…

SolarWinds breach

- A hardcoded password in an API [2020]
- Microsoft, US govt organizations, and many others affected

Bypassing PayPal’s 2FA

- By manipulating request parameters [2017]

Zoom’s enumerable meeting IDs

- Anyone could join meeting by entering IDs [2020]

A few question…

Get Started here: https://ibm.biz/appsecurity

Can a vulnerable software function without producing any errors?

- *Yes, it can function even for several months or years before the vulnerability is disclosed*

Can we add security to a software once it is ready to ship?

- *Security must not be an after thought*

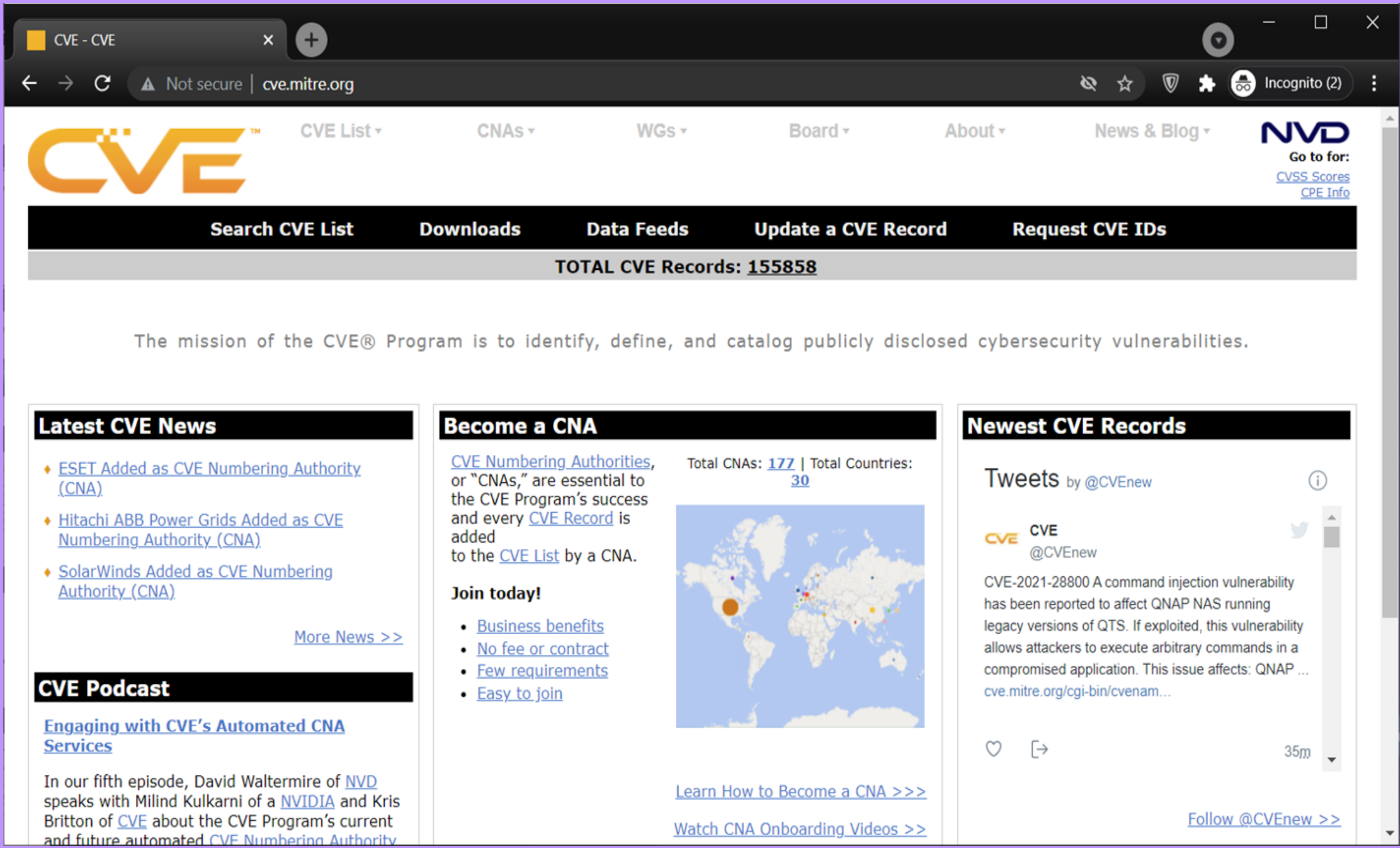
What is the trend in discovery of security vulnerabilities?

- *See graph on next slide*

The CVE repository

Get Started here: https://ibm.biz/appsecurity

~155,000 vulnerable components (Jun 2021)



TOTAL CVE Records: 155858

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Latest CVE News

- ESET Added as CVE Numbering Authority (CNA)
- Hitachi ABB Power Grids Added as CVE Numbering Authority (CNA)
- SolarWinds Added as CVE Numbering Authority (CNA)

More News >>

CVE Podcast

Engaging with CVE's Automated CNA Services

In our fifth episode, David Waltermire of NVD speaks with Milind Kulkarni of a NVIDIA and Kris Britton of CVE about the CVE Program's current and future automated CVE Numbering Authority

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Total CNAs: 177 | Total Countries: 30

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records

Tweets by @CVEnew

CVE @CVEnew

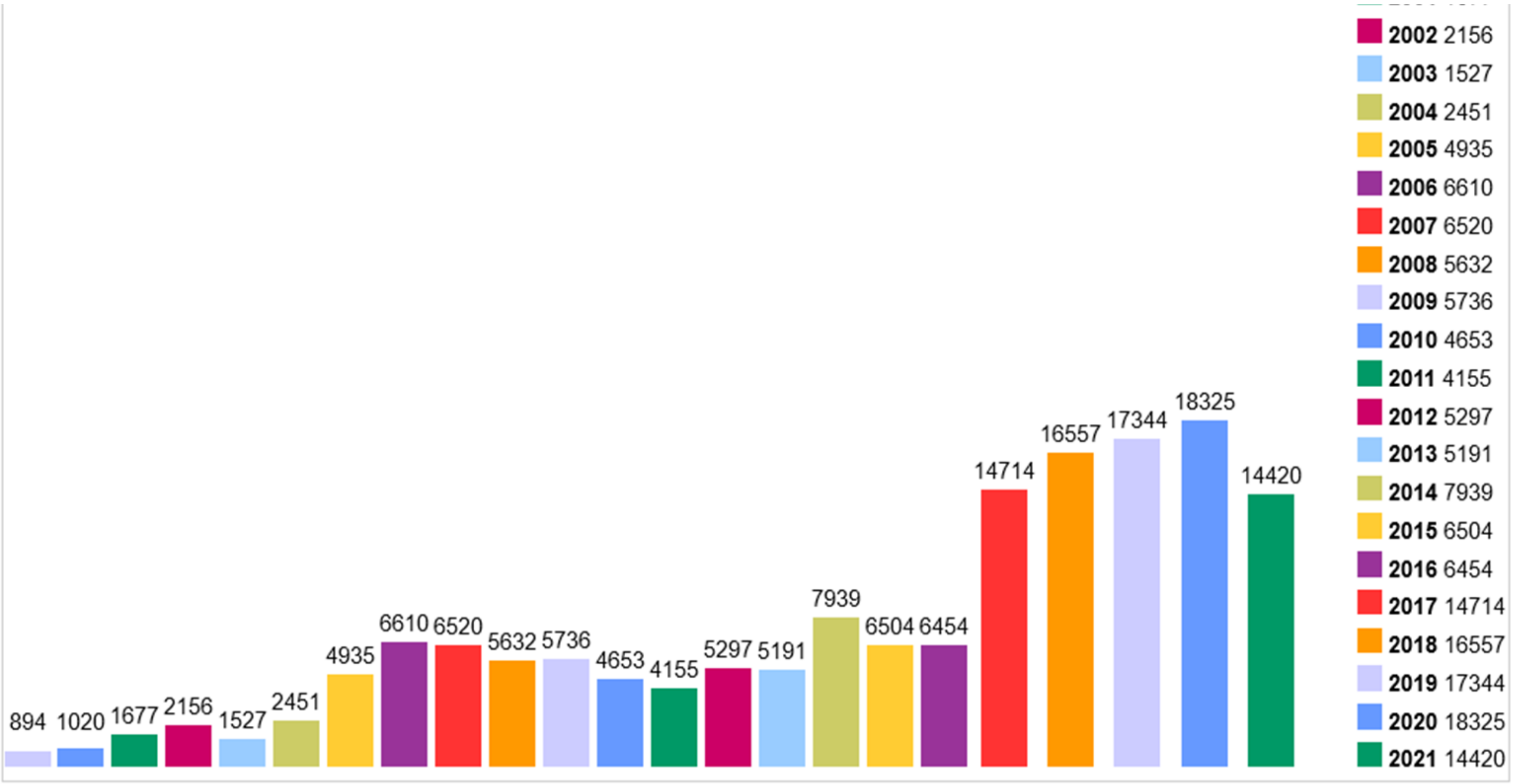
CVE-2021-28800 A command injection vulnerability has been reported to affect QNAP NAS running legacy versions of QTS. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP ... cve.mitre.org/cgi-bin/cvenam...

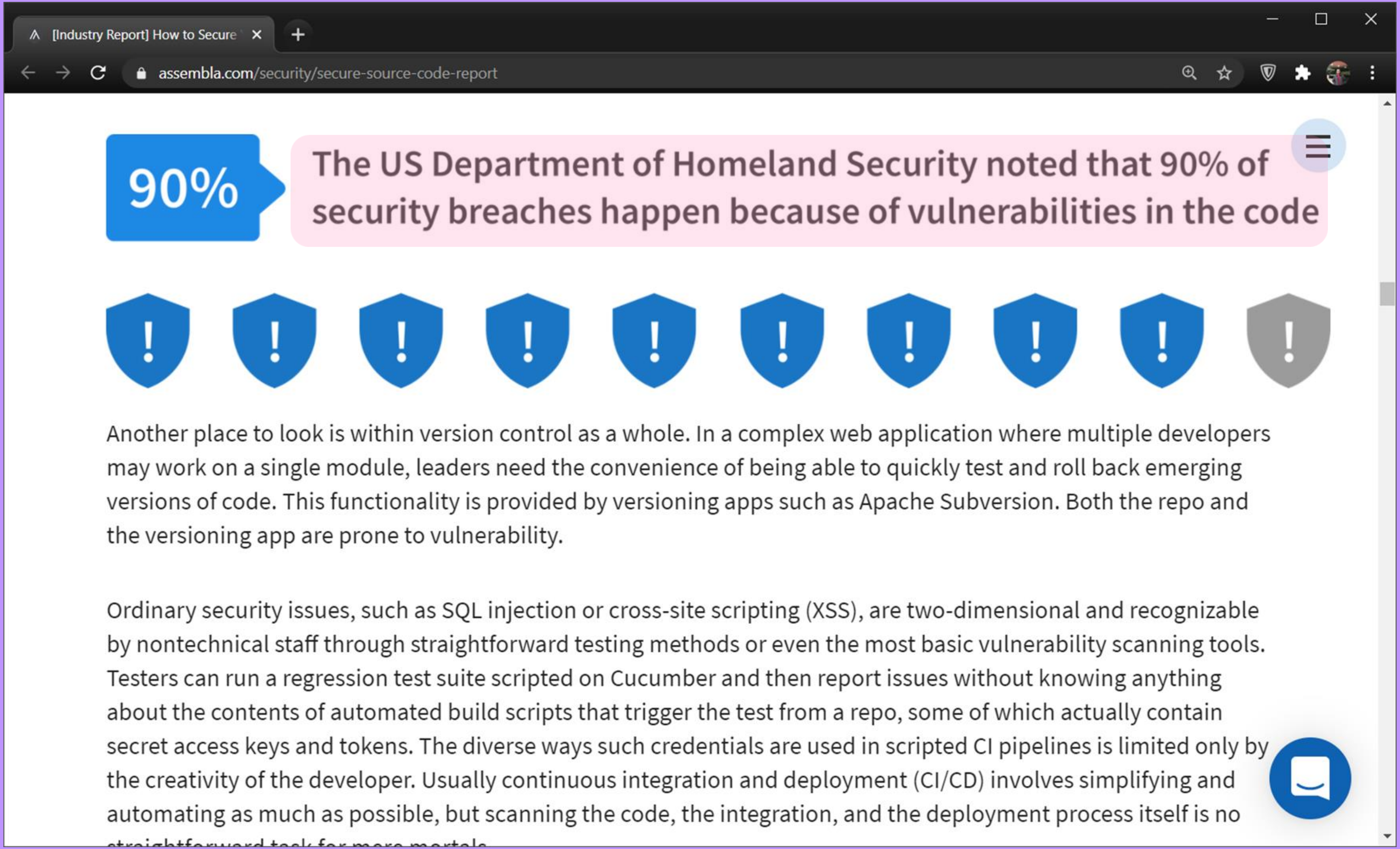
35m

Follow @CVEnew >>

Vulnerabilities by Year

Reference: https://www.cvedetails.com/browse-by-date.php




[Industry Report] How to Secure
assembla.com/security/secure-source-code-report

90%

The US Department of Homeland Security noted that 90% of security breaches happen because of vulnerabilities in the code

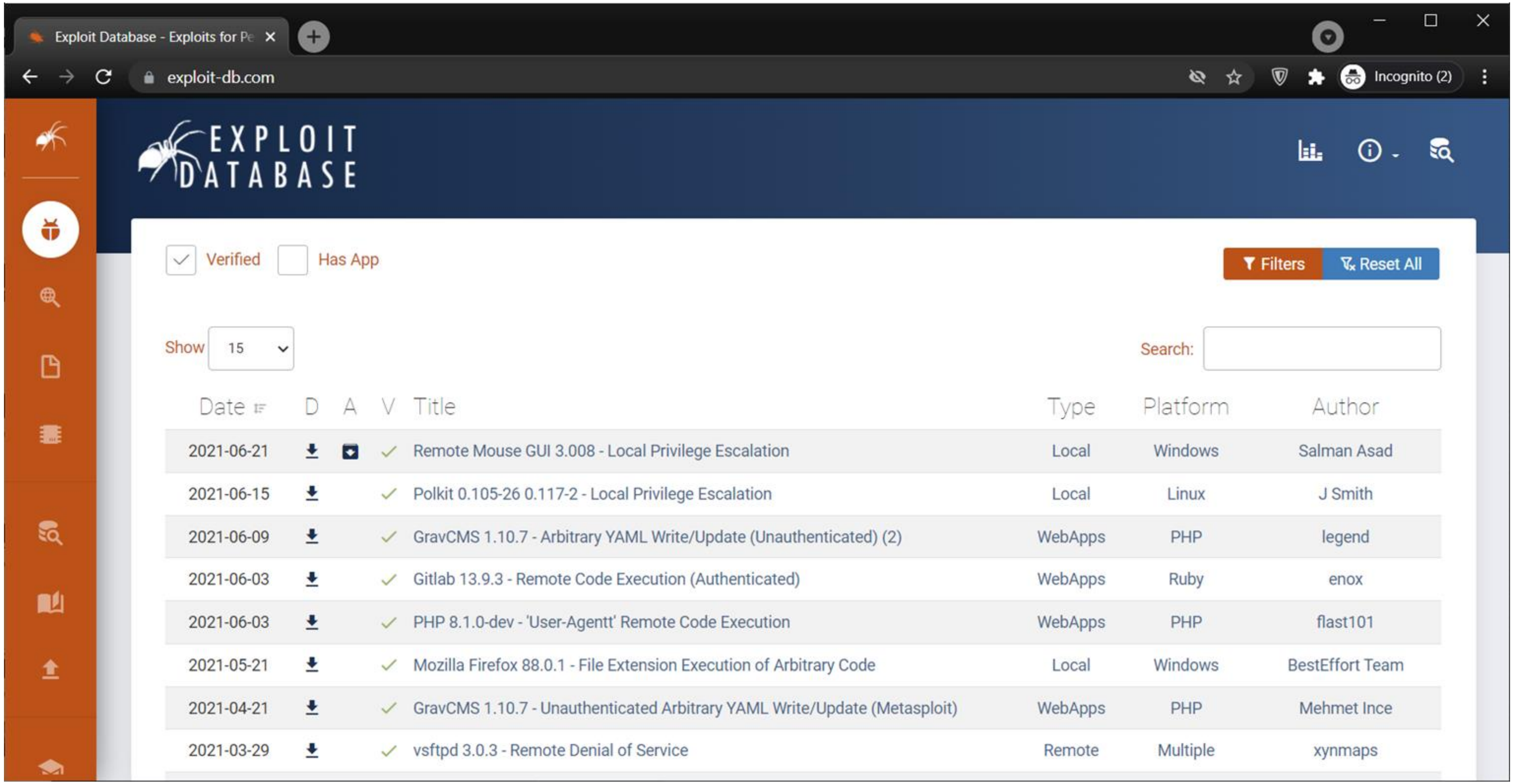
Another place to look is within version control as a whole. In a complex web application where multiple developers may work on a single module, leaders need the convenience of being able to quickly test and roll back emerging versions of code. This functionality is provided by versioning apps such as Apache Subversion. Both the repo and the versioning app are prone to vulnerability.

Ordinary security issues, such as SQL injection or cross-site scripting (XSS), are two-dimensional and recognizable by nontechnical staff through straightforward testing methods or even the most basic vulnerability scanning tools. Testers can run a regression test suite scripted on Cucumber and then report issues without knowing anything about the contents of automated build scripts that trigger the test from a repo, some of which actually contain secret access keys and tokens. The diverse ways such credentials are used in scripted CI pipelines is limited only by the creativity of the developer. Usually continuous integration and deployment (CI/CD) involves simplifying and automating as much as possible, but scanning the code, the integration, and the deployment process itself is no straightforward task for mere mortals.

The Exploits-DB

Get Started here: https://ibm.biz/appsecurity

More than 44,000 exploits



☑ Verified □ Has App

Show 15

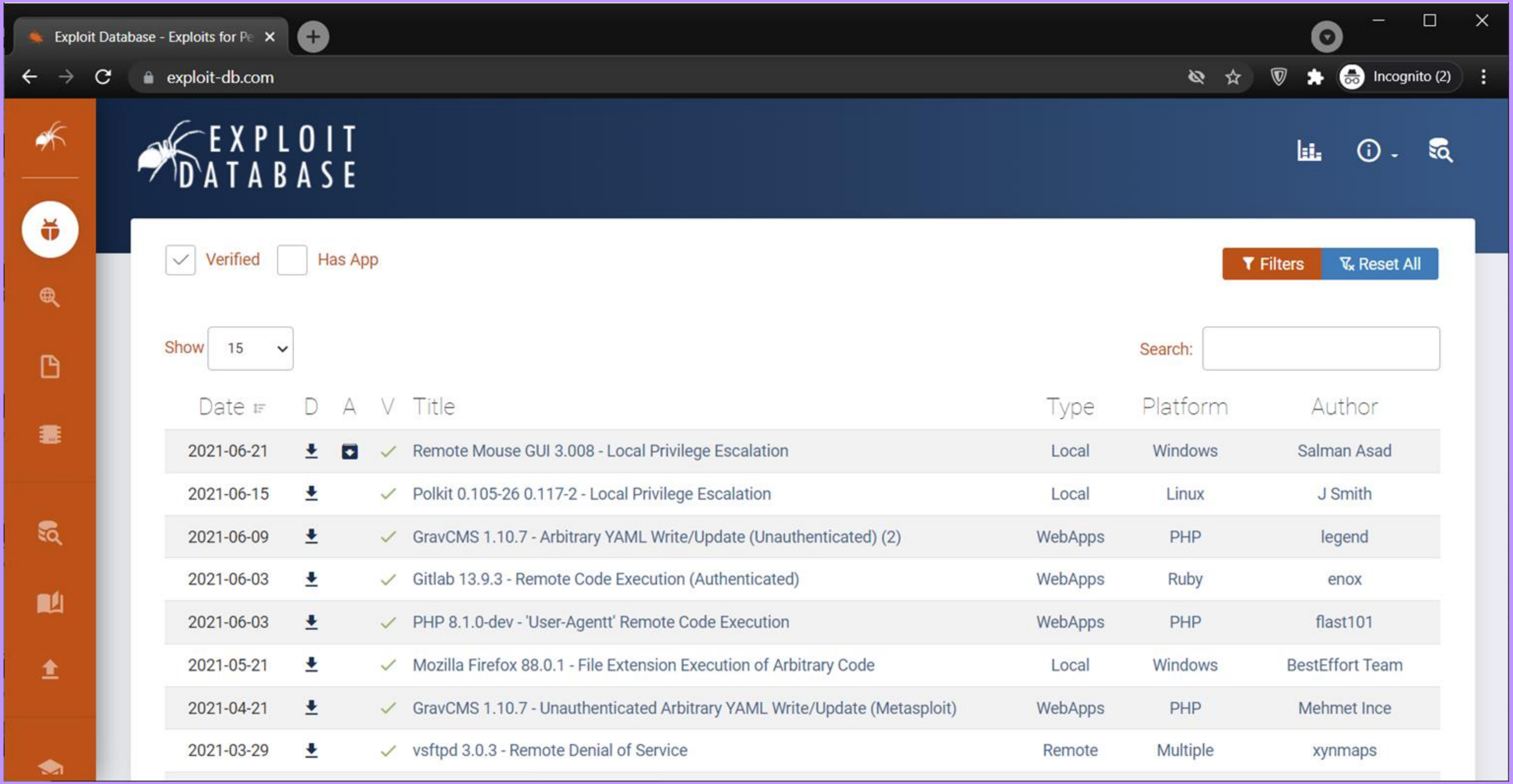
Search:

Date	D	A	V	Title	Type	Platform	Author
2021-06-21	↓	▣	✓	Remote Mouse GUI 3.008 - Local Privilege Escalation	Local	Windows	Salman Asad
2021-06-15	↓		✓	Polkit 0.105-26 0.117-2 - Local Privilege Escalation	Local	Linux	J Smith
2021-06-09	↓		✓	GravCMS 1.10.7 - Arbitrary YAML Write/Update (Unauthenticated) (2)	WebApps	PHP	legend
2021-06-03	↓		✓	Gitlab 13.9.3 - Remote Code Execution (Authenticated)	WebApps	Ruby	enox
2021-06-03	↓		✓	PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution	WebApps	PHP	flast101
2021-05-21	↓		✓	Mozilla Firefox 88.0.1 - File Extension Execution of Arbitrary Code	Local	Windows	BestEffort Team
2021-04-21	↓		✓	GravCMS 1.10.7 - Unauthenticated Arbitrary YAML Write/Update (Metasploit)	WebApps	PHP	Mehmet Ince
2021-03-29	↓		✓	vsftpd 3.0.3 - Remote Denial of Service	Remote	Multiple	xynmaps

Get Started here: https://ibm.biz/appsecurity

The Exploits-DB

More than 33,000 verified exploits

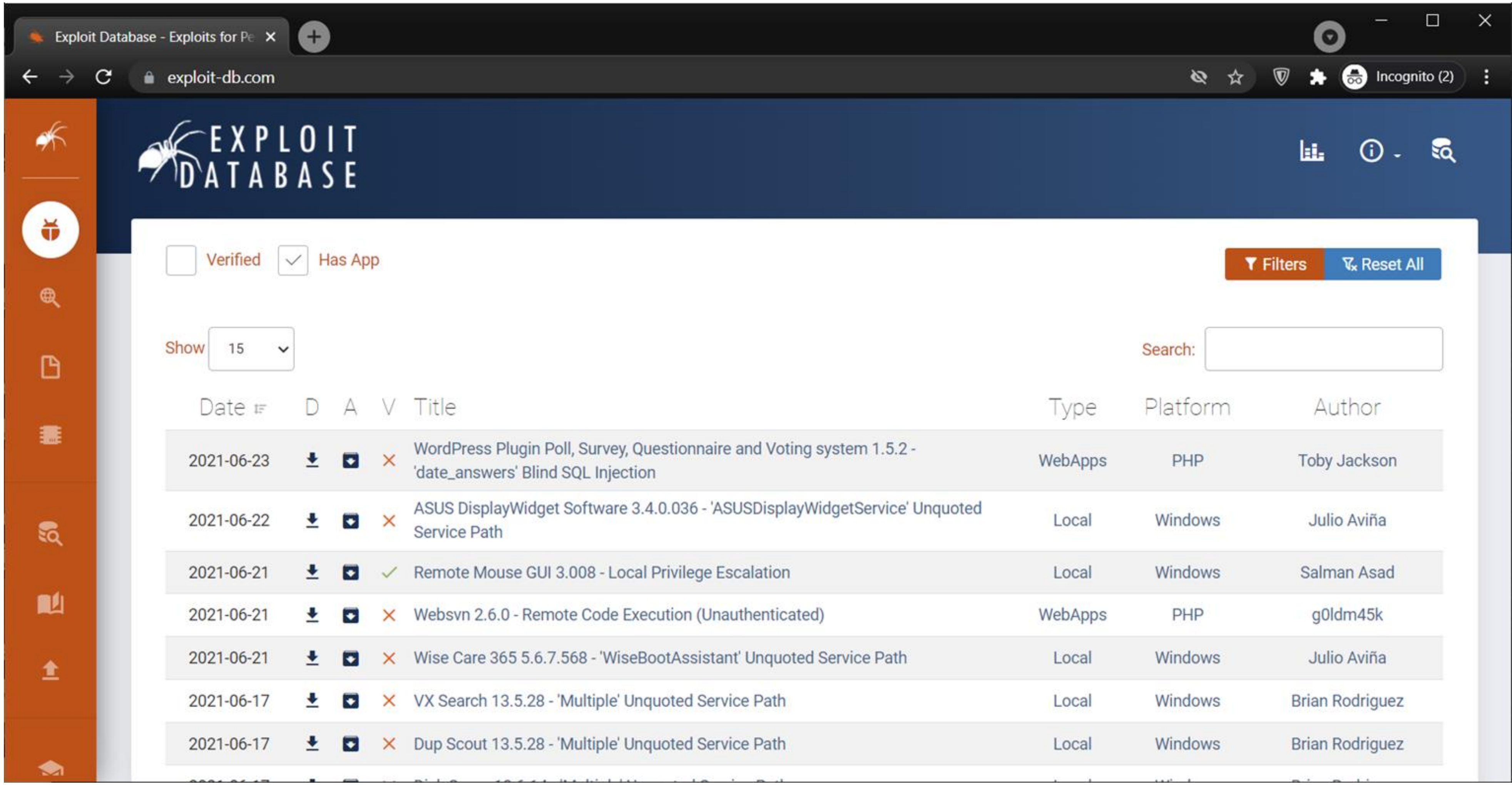


Date	D	A	V	Title	Type	Platform	Author
2021-06-21	⬇	●	✓	Remote Mouse GUI 3.008 - Local Privilege Escalation	Local	Windows	Salman Asad
2021-06-15	⬇		✓	Polkit 0.105-26 0.117-2 - Local Privilege Escalation	Local	Linux	J Smith
2021-06-09	⬇		✓	GravCMS 1.10.7 - Arbitrary YAML Write/Update (Unauthenticated) (2)	WebApps	PHP	legend
2021-06-03	⬇		✓	Gitlab 13.9.3 - Remote Code Execution (Authenticated)	WebApps	Ruby	enox
2021-06-03	⬇		✓	PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution	WebApps	PHP	flast101
2021-05-21	⬇		✓	Mozilla Firefox 88.0.1 - File Extension Execution of Arbitrary Code	Local	Windows	BestEffort Team
2021-04-21	⬇		✓	GravCMS 1.10.7 - Unauthenticated Arbitrary YAML Write/Update (Metasploit)	WebApps	PHP	Mehmet Ince
2021-03-29	⬇		✓	vsftpd 3.0.3 - Remote Denial of Service	Remote	Multiple	xynmaps

The Exploits-DB

Get Started here: https://ibm.biz/appsecurity

Almost 8,000 exploits with an app



□ Verified ☑ Has App

Filters Reset All

Show 15

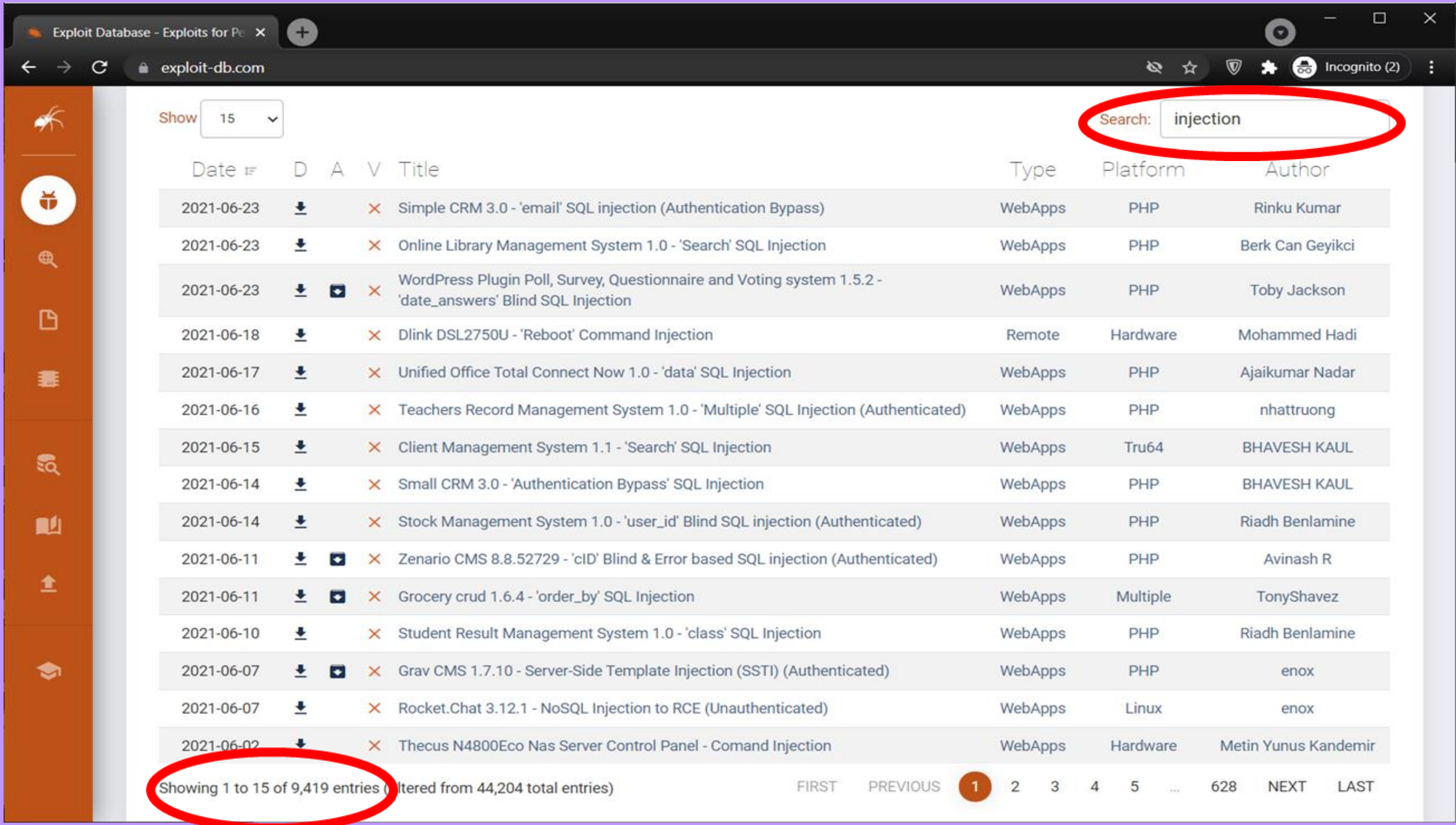
Search:

Date	D	A	V	Title	Type	Platform	Author
2021-06-23	⬇	▣	✗	WordPress Plugin Poll, Survey, Questionnaire and Voting system 1.5.2 - 'date_answers' Blind SQL Injection	WebApps	PHP	Toby Jackson
2021-06-22	⬇	▣	✗	ASUS DisplayWidget Software 3.4.0.036 - 'ASUSDisplayWidgetService' Unquoted Service Path	Local	Windows	Julio Aviña
2021-06-21	⬇	▣	✓	Remote Mouse GUI 3.008 - Local Privilege Escalation	Local	Windows	Salman Asad
2021-06-21	⬇	▣	✗	Websvn 2.6.0 - Remote Code Execution (Unauthenticated)	WebApps	PHP	g0ldm45k
2021-06-21	⬇	▣	✗	Wise Care 365 5.6.7.568 - 'WiseBootAssistant' Unquoted Service Path	Local	Windows	Julio Aviña
2021-06-17	⬇	▣	✗	VX Search 13.5.28 - 'Multiple' Unquoted Service Path	Local	Windows	Brian Rodriguez
2021-06-17	⬇	▣	✗	Dup Scout 13.5.28 - 'Multiple' Unquoted Service Path	Local	Windows	Brian Rodriguez

Get Started here: https://ibm.biz/appsecurity

The Exploits-DB

More than 9,000 exploits related to injections

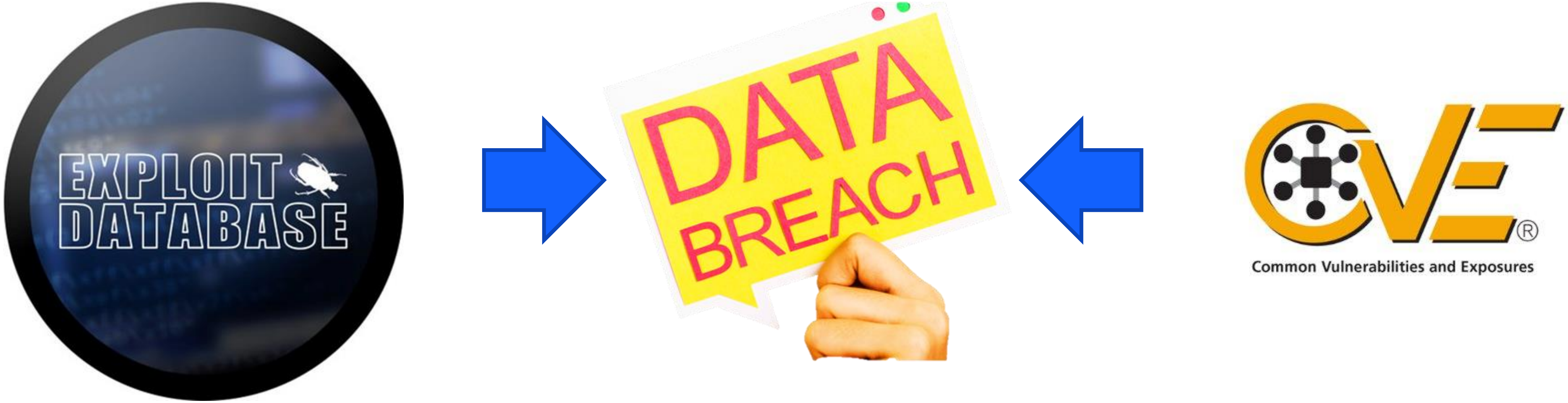


Show 15

Search: injection

Date	D	A	V	Title	Type	Platform	Author
2021-06-23	⬇		✕	Simple CRM 3.0 - 'email' SQL injection (Authentication Bypass)	WebApps	PHP	Rinku Kumar
2021-06-23	⬇		✕	Online Library Management System 1.0 - 'Search' SQL Injection	WebApps	PHP	Berk Can Geyikci
2021-06-23	⬇	▣	✕	WordPress Plugin Poll, Survey, Questionnaire and Voting system 1.5.2 - 'date_answers' Blind SQL Injection	WebApps	PHP	Toby Jackson
2021-06-18	⬇		✕	Dlink DSL2750U - 'Reboot' Command Injection	Remote	Hardware	Mohammed Hadi
2021-06-17	⬇		✕	Unified Office Total Connect Now 1.0 - 'data' SQL Injection	WebApps	PHP	Ajaikumar Nadar
2021-06-16	⬇		✕	Teachers Record Management System 1.0 - 'Multiple' SQL Injection (Authenticated)	WebApps	PHP	nhattruong
2021-06-15	⬇		✕	Client Management System 1.1 - 'Search' SQL Injection	WebApps	Tru64	BHAVESH KAUL
2021-06-14	⬇		✕	Small CRM 3.0 - 'Authentication Bypass' SQL Injection	WebApps	PHP	BHAVESH KAUL
2021-06-14	⬇		✕	Stock Management System 1.0 - 'user_id' Blind SQL injection (Authenticated)	WebApps	PHP	Riadh Benlamine
2021-06-11	⬇	▣	✕	Zenario CMS 8.8.52729 - 'cID' Blind & Error based SQL injection (Authenticated)	WebApps	PHP	Avinash R
2021-06-11	⬇	▣	✕	Grocery crud 1.6.4 - 'order_by' SQL Injection	WebApps	Multiple	TonyShavez
2021-06-10	⬇		✕	Student Result Management System 1.0 - 'class' SQL Injection	WebApps	PHP	Riadh Benlamine
2021-06-07	⬇	▣	✕	Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated)	WebApps	PHP	enox
2021-06-07	⬇		✕	Rocket.Chat 3.12.1 - NoSQL Injection to RCE (Unauthenticated)	WebApps	Linux	enox
2021-06-02	⬇		✕	Thecus N4800Eco Nas Server Control Panel - Comand Injection	WebApps	Hardware	Metin Yunus Kandemir

Showing 1 to 15 of 9,419 entries (filtered from 44,204 total entries)


EXPLOIT DATABASE
DATA BREACH
CVE®
Common Vulnerabilities and Exposures

Get Started here: https://ibm.biz/appsecurity

Recent developments…

Get Started here: https://ibm.biz/appsecurity

AppSec got a lot of attention recently!

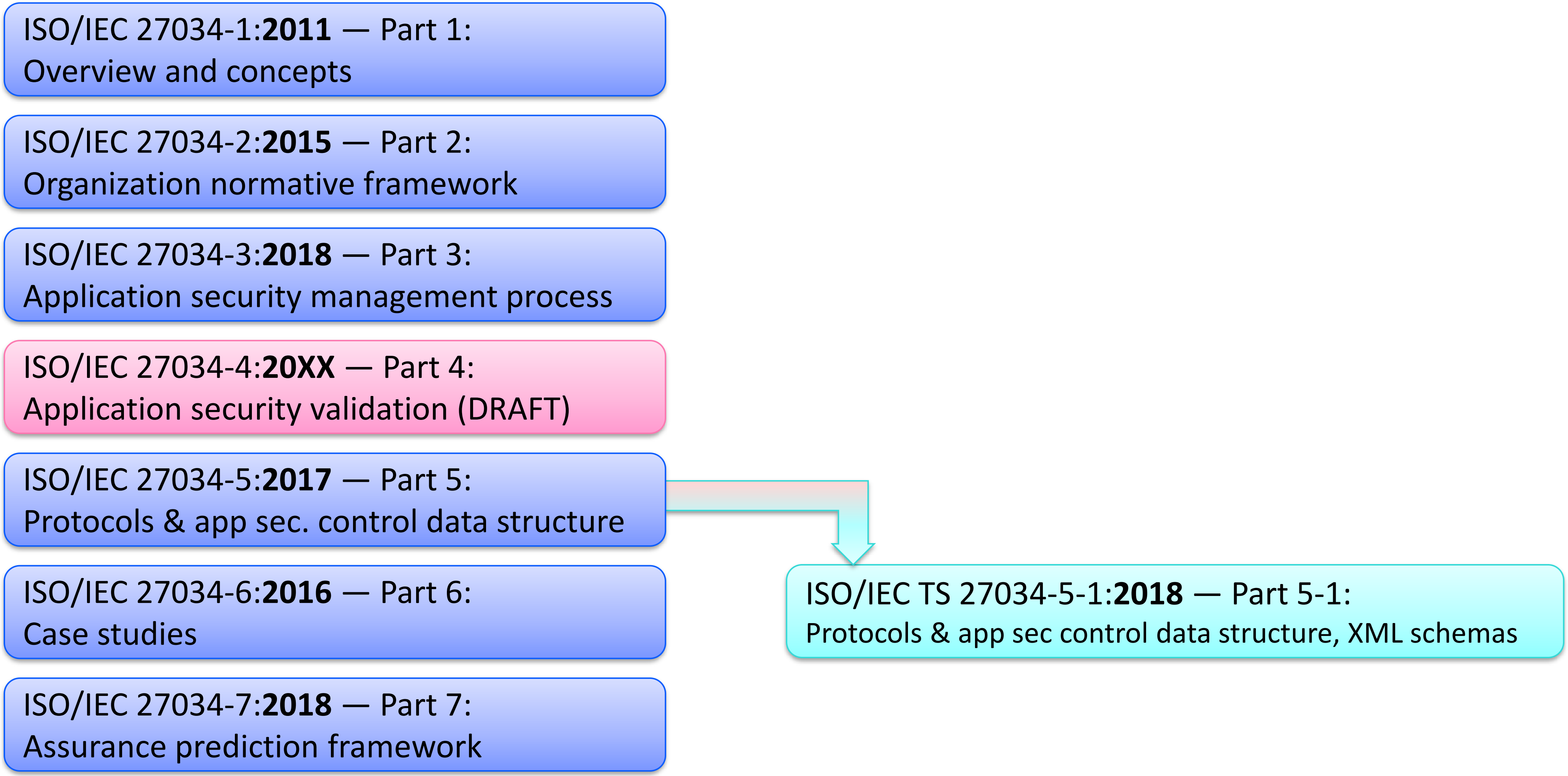
- PCI Software Security Framework (SSF) – (2019-2020)

  ❑ Secure SLC Standard

  ❑ Secure Software Standard

- ISO/ IEC 27034 – (2011 – 2018) [still incomplete]
- Software Assurance Maturity Model (SAMM) ver. 2.0 – (2020)
- Built Security In Maturity Model (BSIMM) ver. 11 – (2019)
- NIST's Secure Software Development Framework (SSDF) (2020)

ISO/ IEC 27034



ISO/IEC 27034-1:**2011** — Part 1:
Overview and concepts

ISO/IEC 27034-2:**2015** — Part 2:
Organization normative framework

ISO/IEC 27034-3:**2018** — Part 3:
Application security management process

ISO/IEC 27034-4:**20XX** — Part 4:
Application security validation (DRAFT)

ISO/IEC 27034-5:**2017** — Part 5:
Protocols & app sec. control data structure

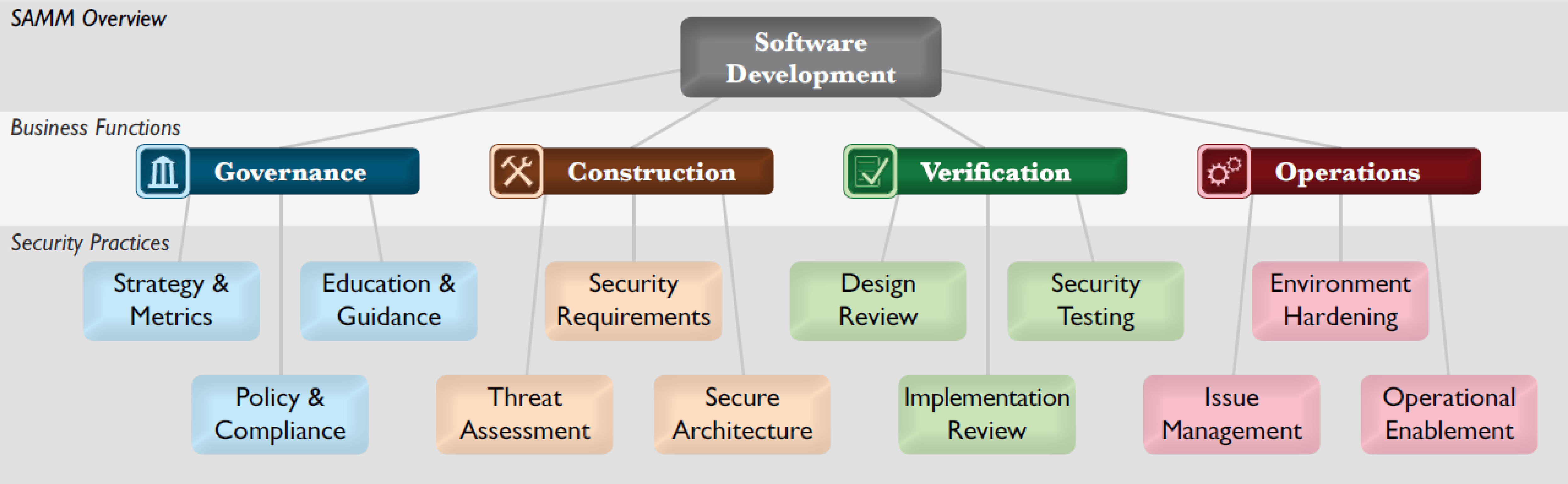
ISO/IEC TS 27034-5-1:**2018** — Part 5-1:
Protocols & app sec control data structure, XML schemas

ISO/IEC 27034-6:**2016** — Part 6:
Case studies

ISO/IEC 27034-7:**2018** — Part 7:
Assurance prediction framework

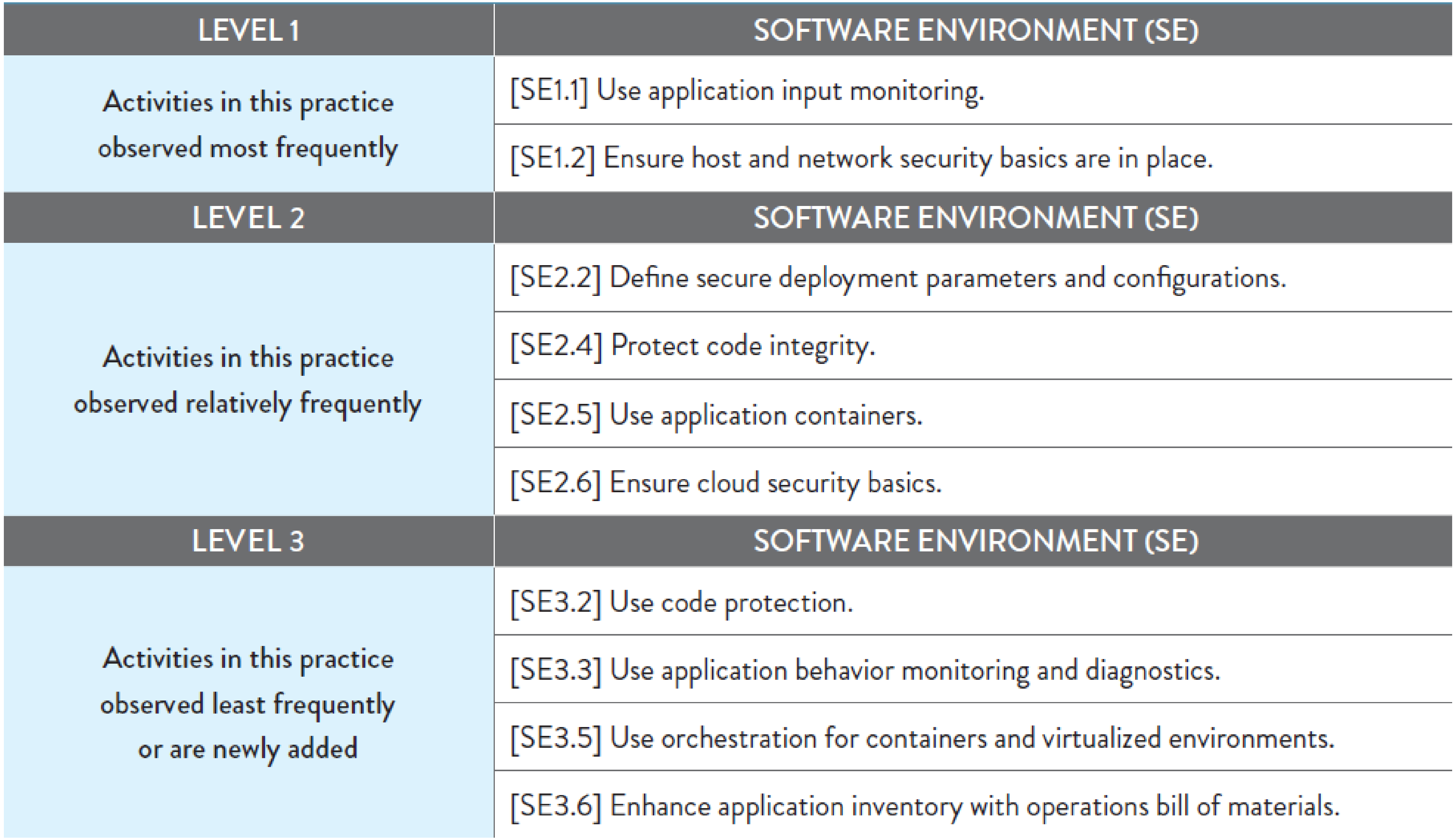
OWASP SAMM ver. 1.5

Get Started here: https://ibm.biz/appsecurity



Get Started here: https://ibm.biz/appsecurity

BSIMM ver. 11



LEVEL 1	SOFTWARE ENVIRONMENT (SE)
Activities in this practice observed most frequently	[SE1.1] Use application input monitoring.
	[SE1.2] Ensure host and network security basics are in place.
LEVEL 2	**SOFTWARE ENVIRONMENT (SE)**
Activities in this practice observed relatively frequently	[SE2.2] Define secure deployment parameters and configurations.
	[SE2.4] Protect code integrity.
	[SE2.5] Use application containers.
	[SE2.6] Ensure cloud security basics.
LEVEL 3	**SOFTWARE ENVIRONMENT (SE)**
Activities in this practice observed least frequently or are newly added	[SE3.2] Use code protection.
	[SE3.3] Use application behavior monitoring and diagnostics.
	[SE3.5] Use orchestration for containers and virtualized environments.
	[SE3.6] Enhance application inventory with operations bill of materials.

Get Started here: https://ibm.biz/appsecurity

App ID

Get Started here: https://ibm.biz/appsecurity

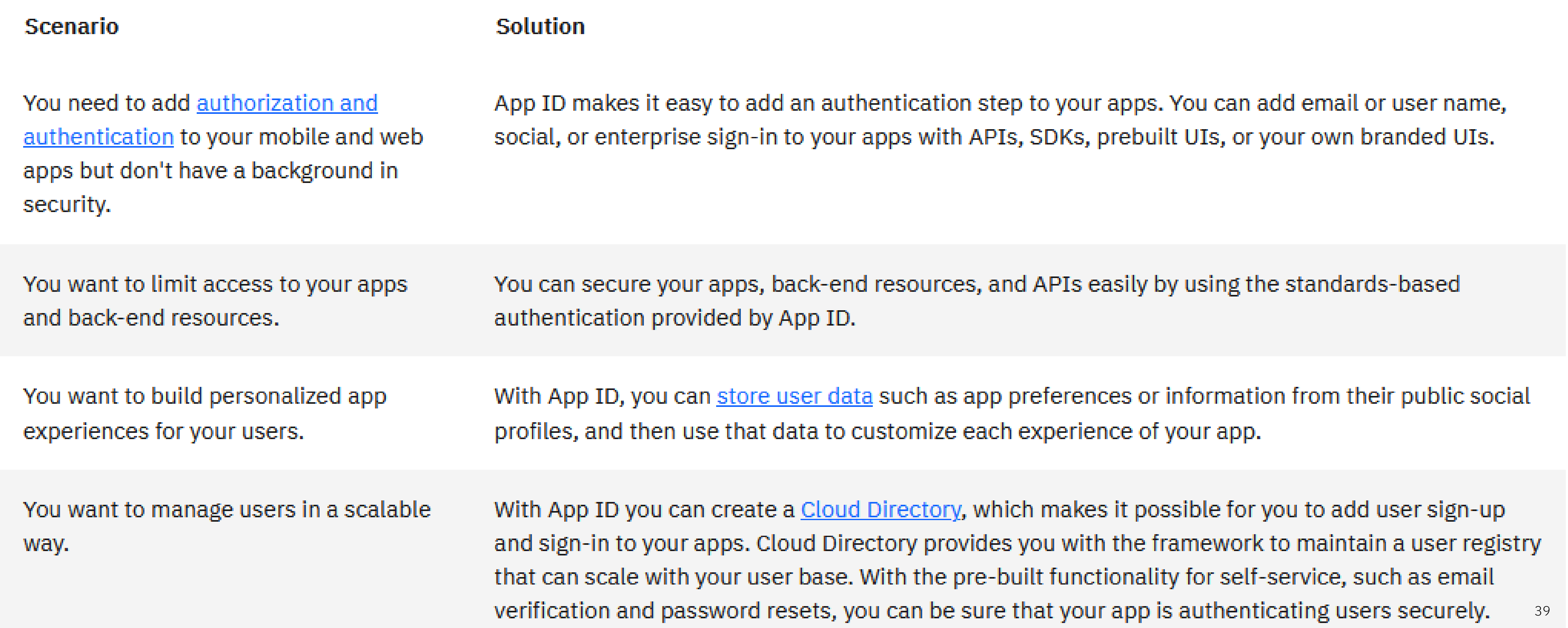
What is AppID

Application security can be incredibly complicated. For most developers, it's one of the hardest parts of creating an app. How can you be sure that you are protecting your user's information? By integrating IBM Cloud™ App ID into your apps, you can secure resources and add authentication; even when you don't have a lot of security experience.

By requiring users to sign into your app, you can store user data such as app preferences or information from the public social profiles, and then use that data to customize each experience of your app. App ID provides a framework for you, but you can also bring your own branded sign in screens when working with cloud directory.

Why Do We Need AppID

Get Started here: https://ibm.biz/appsecurity



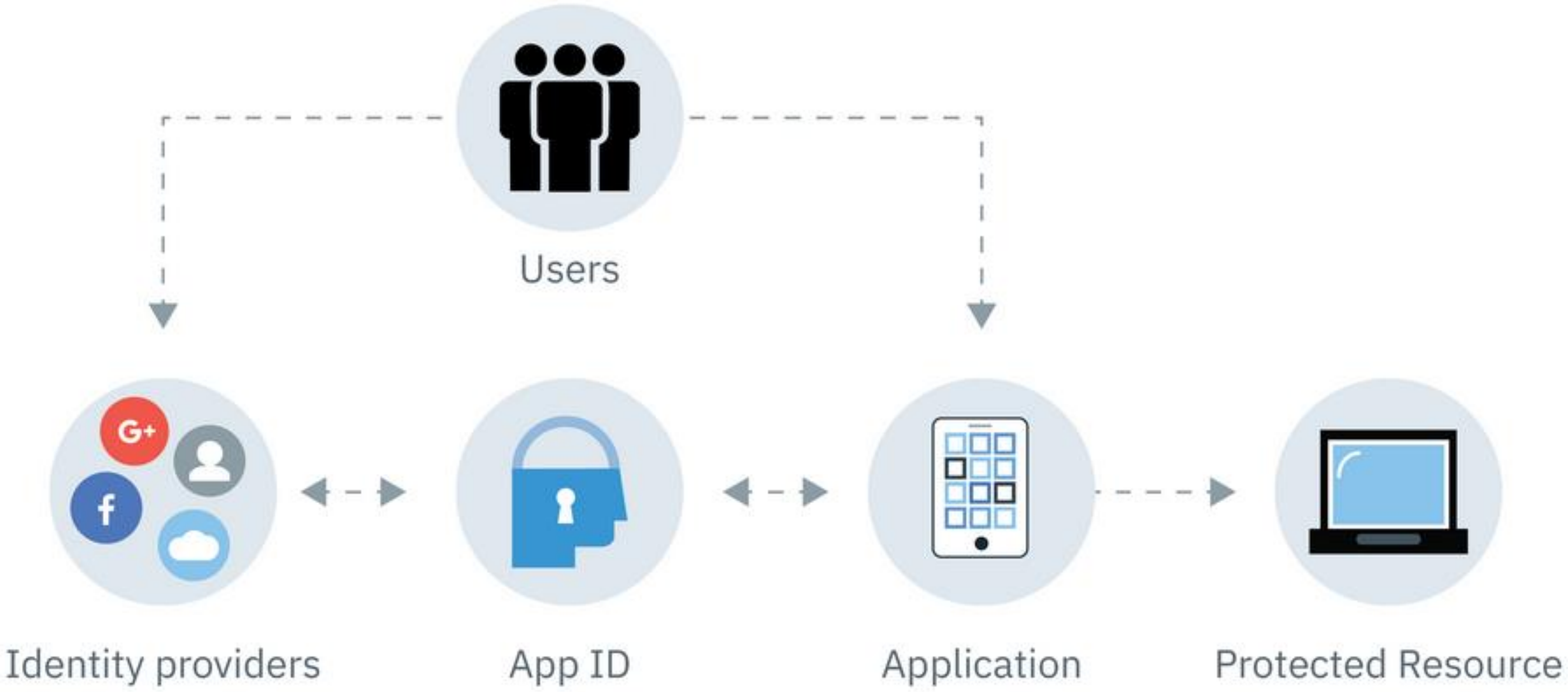
Scenario	Solution
You need to add authorization and authentication to your mobile and web apps but don't have a background in security.	App ID makes it easy to add an authentication step to your apps. You can add email or user name, social, or enterprise sign-in to your apps with APIs, SDKs, prebuilt UIs, or your own branded UIs.
You want to limit access to your apps and back-end resources.	You can secure your apps, back-end resources, and APIs easily by using the standards-based authentication provided by App ID.
You want to build personalized app experiences for your users.	With App ID, you can store user data such as app preferences or information from their public social profiles, and then use that data to customize each experience of your app.
You want to manage users in a scalable way.	With App ID you can create a Cloud Directory, which makes it possible for you to add user sign-up and sign-in to your apps. Cloud Directory provides you with the framework to maintain a user registry that can scale with your user base. With the pre-built functionality for self-service, such as email verification and password resets, you can be sure that your app is authenticating users securely.

How it Works

Get Started here: https://ibm.biz/appsecurity

With App ID, you can add a level of security to your apps by requiring users to sign in. You can also use the server SDK o APIs to protect your back-enc resources.

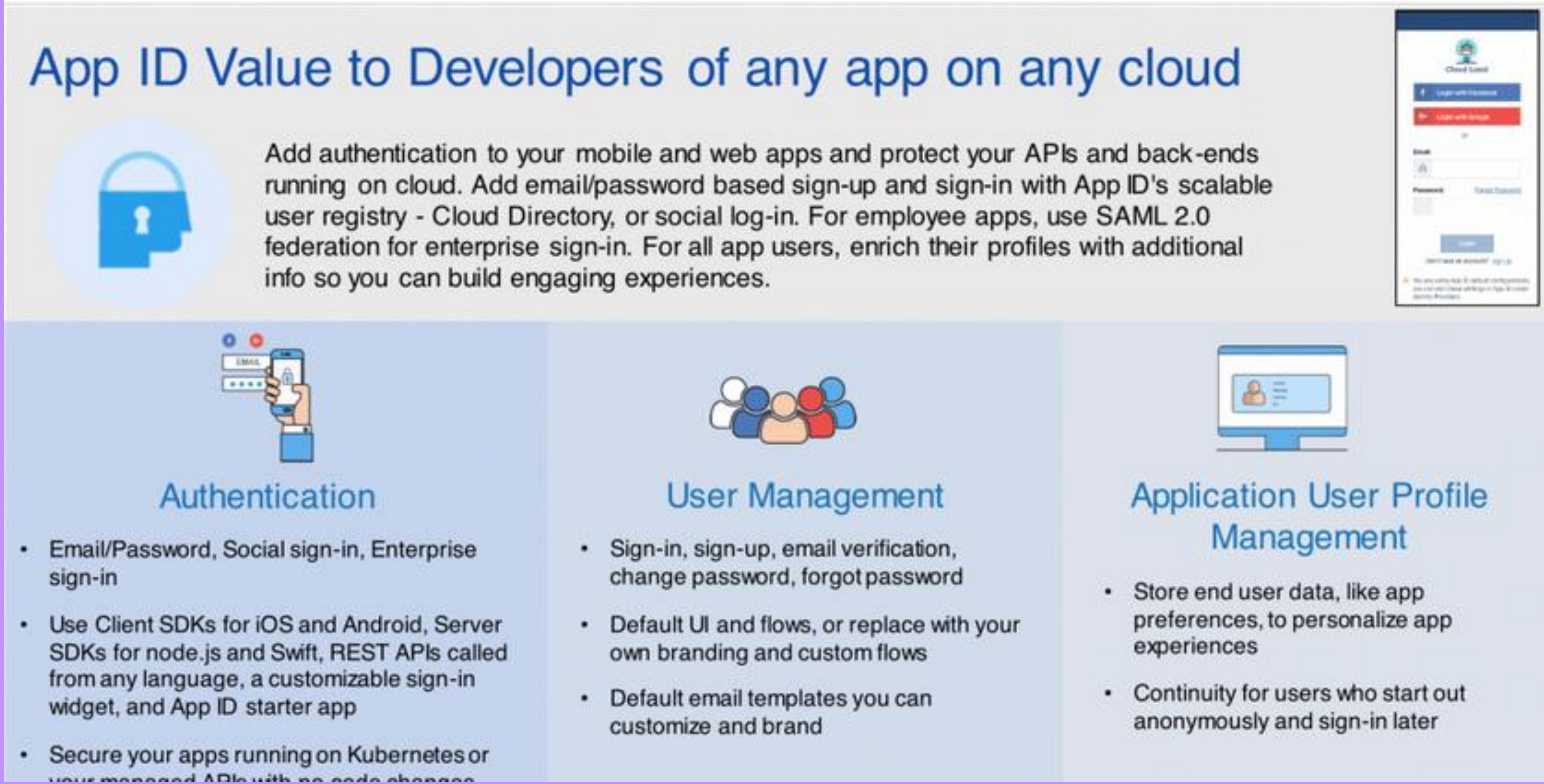
- Application
- Server SDK:
- Client SDK:
- IBM Cloud
- App ID:
- Cloud Directory:
- External (third party)



Integrations

Get Started here: https://ibm.biz/appsecurity

- Kubernetes Service
- Cloud Functions and API Connect
- Cloud Foundry
- Activity Tracker
- iOS Programming Guide
- Node.js programming guide



App ID Value to Developers of any app on any cloud

Add authentication to your mobile and web apps and protect your APIs and back-ends running on cloud. Add email/password based sign-up and sign-in with App ID's scalable user registry - Cloud Directory, or social log-in. For employee apps, use SAML 2.0 federation for enterprise sign-in. For all app users, enrich their profiles with additional info so you can build engaging experiences.

Authentication

- Email/Password, Social sign-in, Enterprise sign-in
- Use Client SDKs for iOS and Android, Server SDKs for node.js and Swift, REST APIs called from any language, a customizable sign-in widget, and App ID starter app
- Secure your apps running on Kubernetes or your managed APIs with no code changes

User Management

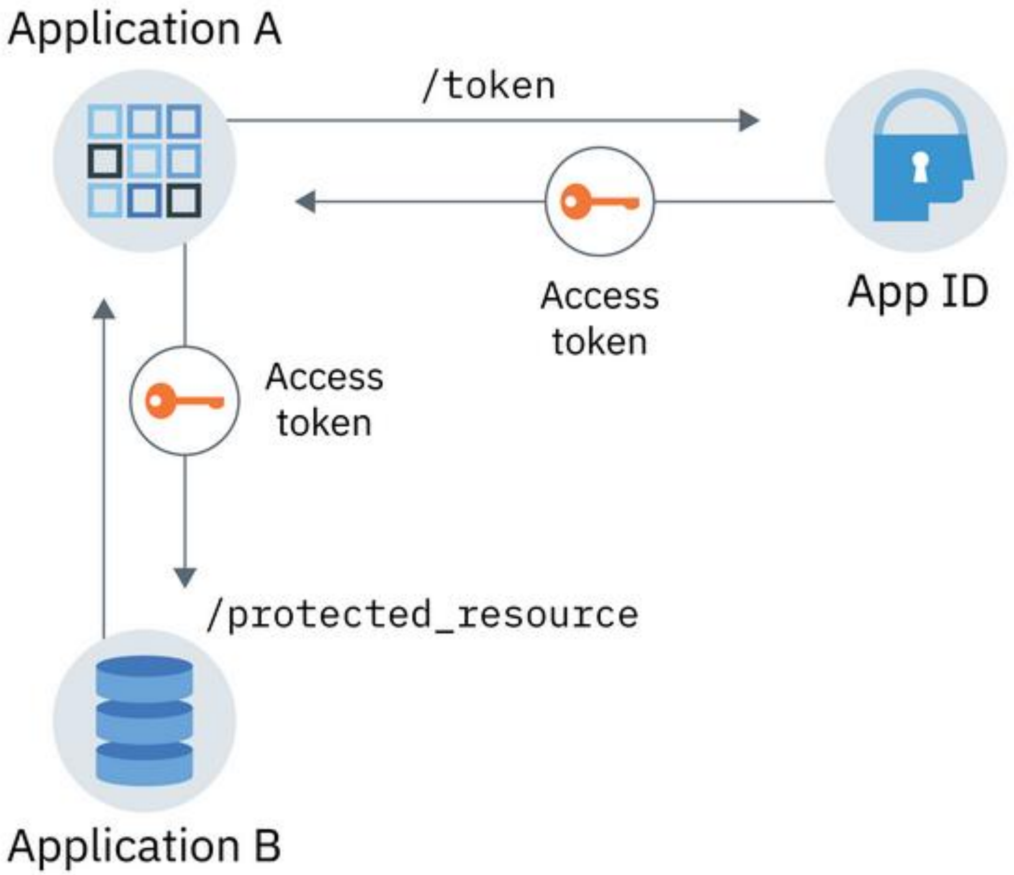
- Sign-in, sign-up, email verification, change password, forgot password
- Default UI and flows, or replace with your own branding and custom flows
- Default email templates you can customize and brand

Application User Profile Management

- Store end user data, like app preferences, to personalize app experiences
- Continuity for users who start out anonymously and sign-in later

How App ID works: What Does the Flow Looks Like?

Get Started here: https://ibm.biz/appsecurity



1.You register the application that needs to authenticate to access a protected resource with App ID.

2.Application A registers with App ID to obtain a client ID and secret.

3.Application A makes a request to the App ID authorization server /token endpoint by sending the credentials retrieved in the previous step.

4.App ID validates the request, authenticates the app, and returns a response to Application A that contains an access token.

5.Application A is now able to use the valid access token to send requests to protected resources such as Application B.

Managing authentication

Get Started here: https://ibm.biz/appsecurity

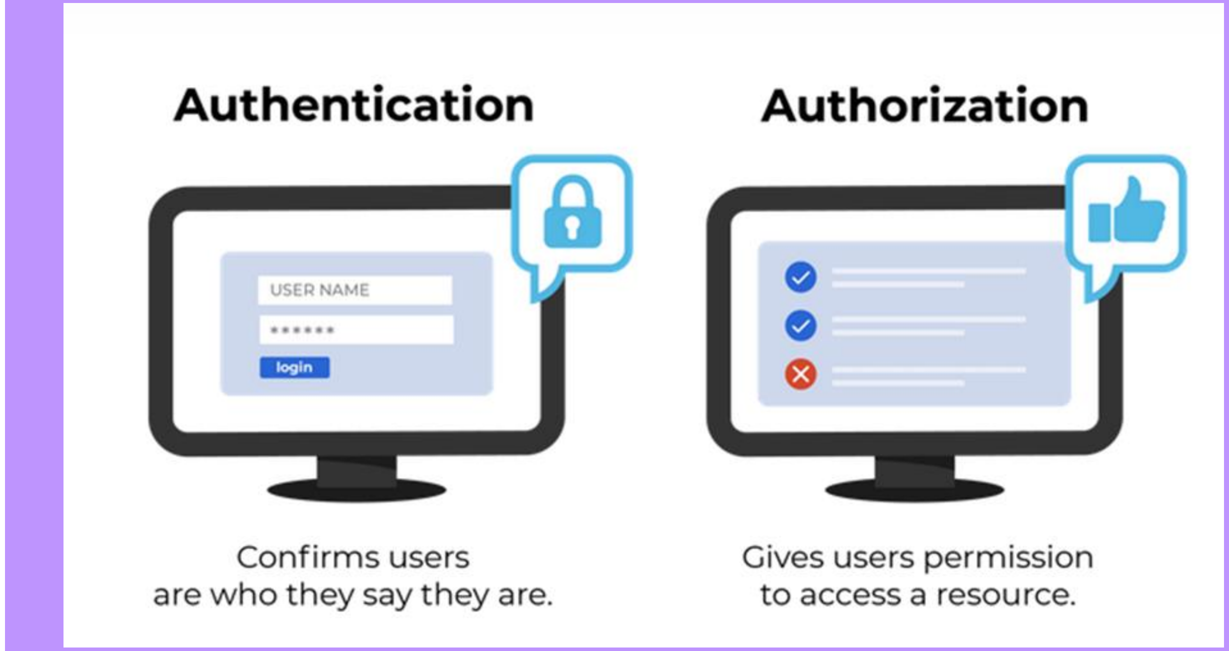
Identity provider	Type	Description
Cloud Directory	Managed registry	You can maintain your own user registry in the cloud. When a user signs up for your app, they are added to your directory of users. This option gives your users more freedom to manage their own account within your app.
SAML	Enterprise	You can create a single sign-on experience for your users.
Facebook	Social	Users can sign into your app by using their Facebook credentials.
Google+	Social	Users can sign into your app by using their Google credentials.
Custom	Custom	If none of the provided options fit your specific need, you can configure your own identity flow to work with App ID.

Get Started here: https://ibm.biz/appsecurity

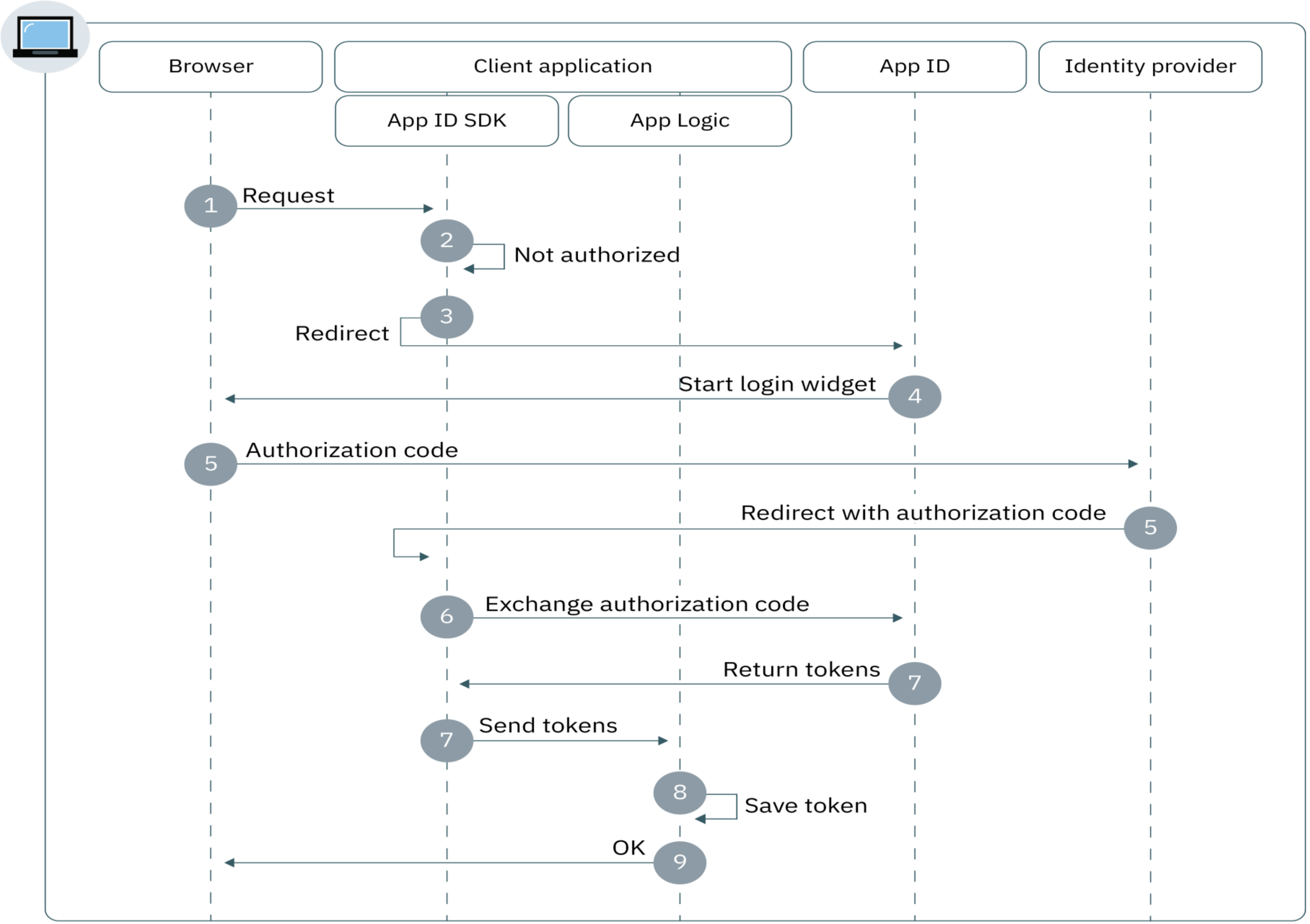
Difference Authentication and Authorization

- **Authentication**, in the form of a key. The lock on the door only grants access to someone with the correct key in much the same way that a system only grants access to users who have the correct credentials.

- **Authorization**, in the form of permissions. Once inside, the person has the authorization to access the kitchen and open the cupboard that holds the pet food. The person may not have permission to go into the bedroom for a quick nap.


Authentication
Authorization
USER NAME
******
login
Confirms users are who they say they are.
Gives users permission to access a resource.

Understanding the flow Single-page apps



Hands On

Get Started here: https://ibm.biz/appsecurity

- Sign up/Login to IBM Cloud: https://ibm.biz/appsecurity
- Follow along with the hands-on: https://github.com/IBMDeveloperMEA/Secure-your-single-page-web-app-with-low-code-on-IBM-Cloud

Summary:

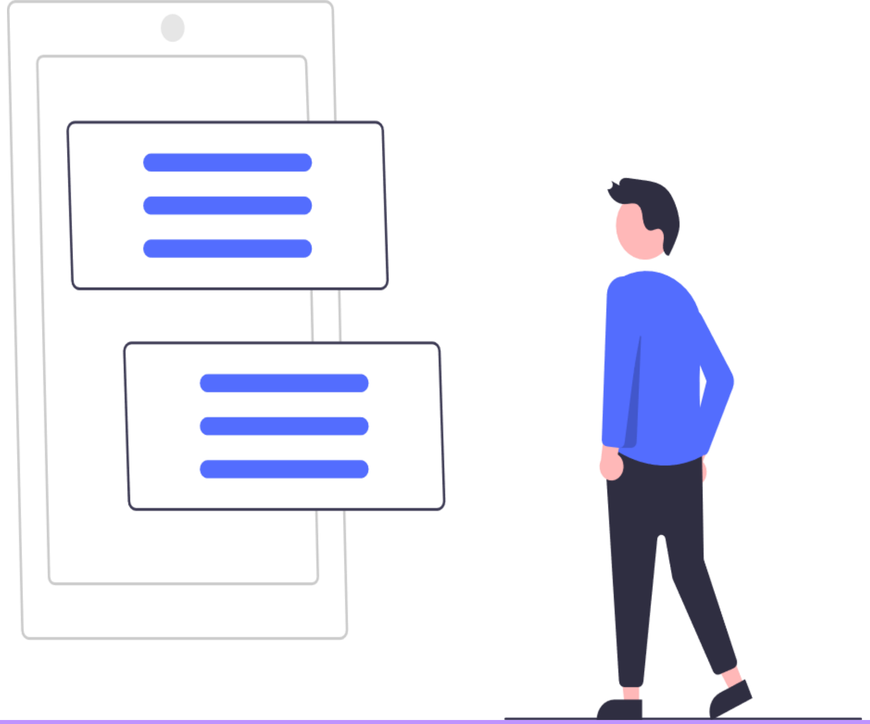
Get Started here: https://ibm.biz/appsecurity

we learned about:

- Intro to low code/ No code Application Security
- Why is it important to adapt security in Application development
- Recent developments
- What is AppID, how does it work and why we should use it.
- Benefits of AppID
- Difference between Authentications vs authorization
- Managing authentication

Let us know how we are doing!

SCAN ME



Survey link

https://ibm.biz/appsecurity-survey

Get Started here: https://ibm.biz/appsecurity

Join our Facebook Community

Join here:

https://www.facebook.com/groups/ibmdevelopermea/

Get Started here: https://ibm.biz/appsecurity

A big thank you to our partners!

SKYSNAG

OpenUAE

GISPP

REHNUMAA
lead the way...

BUSINESS INNOVATION

ELLE/TECH®
WOMEN IN TEAMS

ArabWIC

Journey to Low Code / No Code App Security

The next workshop in the series!

28th September – 6 PM-8 PM (GST)
Easily Secure your Spring Boot app with Low code / No code
https://www.crowdcast.io/e/journey-to-low-code-no-code-app-security-2

Thank you!

Asna Javed
Lead Developer Advocate, PAK
asna.javed1@ibm.com

Divya S
Security Consultant, India

Ayesha Iftikhar
Researcher & Co-founder and Mentor

Muhammad Nadeem
Application Security Consultant

linkedin.com/in/mn338

Let us know how we did!

Survey link:
https://ibm.biz/appsecurity-survey