Aplicacions web i ciberseguretat

Laia Subirats Maté

Barcelona Activa
Ajuntament de Barcelona

Missió

Barcelona Activa vol contribuir a la millora de la qualitat de vida de les persones promovent la competitivitat econòmica de la ciutat i el reequilibri dels territoris, a través del foment de l'ocupació de qualitat, l'impuls a l'emprenedoria i el suport a un teixit empresarial plural, divers i sostenible, des d'una perspectiva econòmica, social i ambiental.

Visió

Les accions de l'entitat es regeixen per la voluntat de fer de Barcelona una ciutat de referència internacional per treballar, emprendre i viure amb valors socials i ambientals.

Valors

L'activitat de Barcelona Activa es desenvolupa al voltant d'aquests 4 valors:

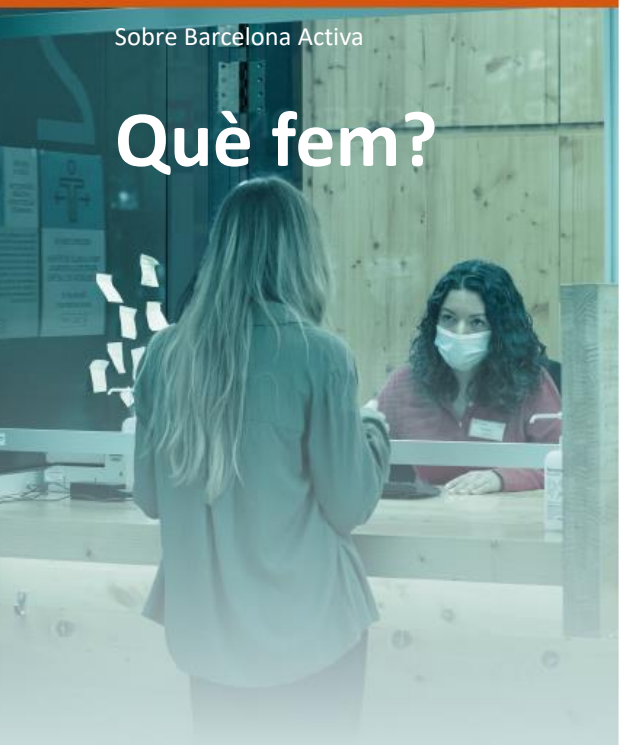
1. Igualtat d'oportunitats i progrés social

2. Cooperació dins l'organització i amb altres

3. Economia al servei de les persones: social i sostenible

4. Esperit de servei públic i ètica professional i personal

Què fem?



Acompanyem les persones que cerquen feina durant tot el procés

barcelonactiva.cat/treball

Donem suport a les persones emprenedores per fer realitat la seva idea de negoci

barcelonactiva.cat/emprenedoria

Ajudem les empreses i organitzacions a impulsar la seva activitat

barcelonactiva.cat/empreses

Oferim formació a les persones que cerquen feina, emprenedores i professionals.

barcelonactiva.cat/formacio

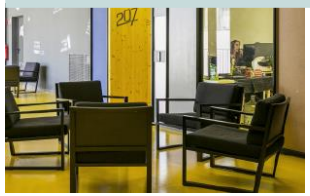
PROXIMITAT, INNOVACIÓ I IGUALTAT

Seu Central
de Barcelona Activa

Incubadora Glòries
Acull empreses de nova creació

Oficina d’Atenció a les Empreses
L’espai de referència per a les empreses i pimes de Barcelona

Porta22
2.000 m^2 per a l’ocupació i la carrera professional



Incubadora Almogàvers
Incubadora publicoprivada per a empreses innovadores

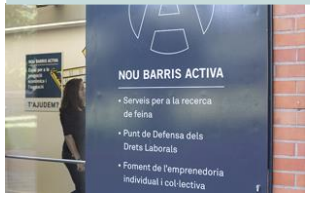
Parc Tecnològic
Clúster d’innovació i capacitació tecnològica al nord de la ciutat

Convent de Sant Agustí
Centre referent en ocupació per a joves a Ciutat Vella

Incubadora MediaTIC
Allotja empreses d’alt impacte tecnològic

Cibernàrium 22@
Centre de capacitació tecnològica i IT Academy

Ca n’Andalet
Espai per a la formació i l’ocupació a Horta-Guinardó



Nou Barris Activa
L’espai de referència per a la promoció econòmica i l’ocupació a Nou Barris

InnoBA
Centre municipal per a la Innovació socioeconòmica

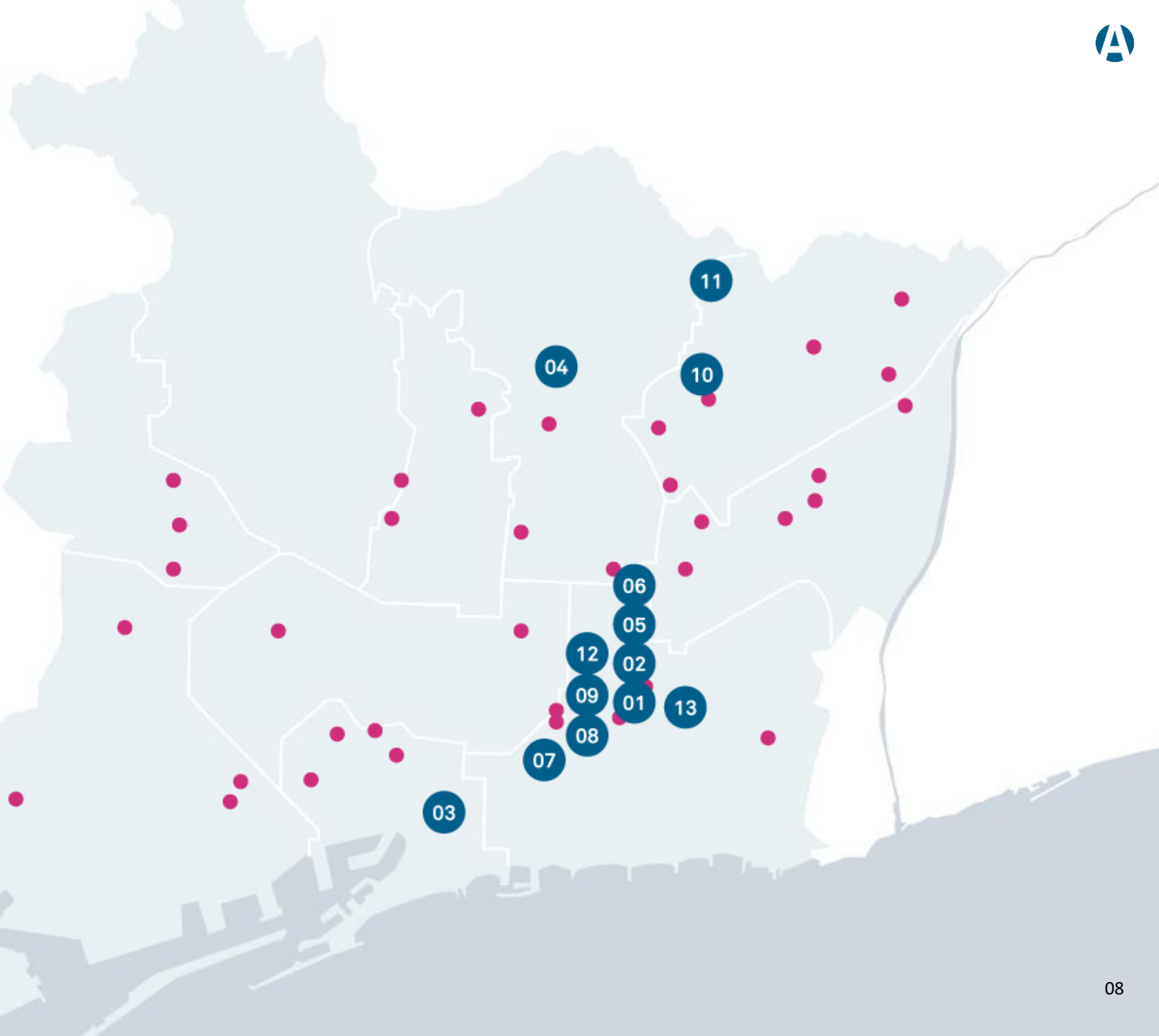
Centre per a la Iniciativa Emprenedora Glòries
L’equipament per emprendre a la ciutat

Cibernàrium Nou Barris
Centre de formació digital d’iniciació ubicat al Parc Tecnològic

Xarxa d’equipaments de Barcelona Activa

Barcelona Activa està present a **48** punts de la ciutat.

1. **Seu Central**
2. **Porta22**
3. **Convent de Sant Agustí**
4. **Ca n’Andalet**
5. **Centre per a la Iniciativa Emprenedora Glòries**
6. **Incubadora Glòries**
7. **Incubadora Almogàvers**
8. **Incubadora MediaTIC**
9. **Oficina d’Atenció a les Empreses**
10. **Parc Tecnològic i Cibernàrium Nou Barris**
11. **Nou Barris Activa**
12. **Cibernàrium 22@**
13. **InnoBA**



Punts d’atenció a la ciutat

Índex

0. Presentació ponent
1. Confidencialitat, Integritat i Disponibilitat
2. Control d’accés: autenticació i autorització
3. Cas d’ús
4. Federated authorization
5. Construir la seguretat en el disseny de l’aplicació
6. OWASP Top 10: les vulnerabilitats més comunes
7. Altres consideracions de seguretat de backend
8. Miscel·lània

Laia Subirats

Experiència laboral:

- **Investigadora @ Eurecat (2009-Actualitat)**
- **Consultora @ Universitat Oberta de Catalunya (2016-Actualitat)**
- Consultora @ Universitat Pompeu Fabra (Estiu 2011, Estiu 2012)
- Estudiant @ Google Summer of Code (Estiu 2008)
- Estudiant d'estiu @ European Organization for Nuclear Research (CERN) (Estiu 2007)
- Becària @ Telefónica I+D (2006-2008)

Estudis:

- Doctorat en Informàtica @ Universitat Autònoma de Barcelona (2009-2015)
- Màster en Telemàtica @ Universitat Politècnica de Catalunya (2008-2009)
- Enginyeria de Telecomunicacions @ Universitat Pompeu Fabra (2003-2008)

Objectius

- Com protegir les dades privades de l'accés d'usuaris no autoritzats?
- Com protegir les dades d'accés o modificació per part d'usuaris que no tenen els privilegis adequats?
- Les millors pràctiques utilitzades durant la implementació de comprovacions d'autenticació i autorització.
- Com avaluar millor els riscos als quals es podria exposar la vostra aplicació?

1. Confidencialitat, integritat i disponibilitat

Confidencialitat:

La confidencialitat és el valor de fer complir que les dades només estan disponibles per al seu públic, i no per a tothom.

La confidencialitat de les dades pot ser pública, restringida o confidencial.

Moltes companyies tenen els seus nivells de confidencialitat per etiquetar documents i recursos.

La pèrdua de confidencialitat pot tenir un impacte de pèrdua de valor.

Integritat

- Les dades han de ser veraces per conservar el seu valor. Si les dades es corrompeixen com a conseqüència d'una manipulació incorrecta o per un procés defectuós, perdran el seu valor.Perquè les dades conservessin la seva integritat, només haurien de ser modificades pel públic definit pel seu nivell de confidencialitat i mitjançant els processos esperats (per exemple, si s'esperava que les dades s'emmagatzemen com a fitxer binari, s'haurien de serialitzar i deserialitzar amb les eines adequades).
- Les dades perdran la seva integritat si són modificades per actors fora del seu públic previst; o quan sigui modificat per processos que no siguin els prevists pels titulars de les dades i l'aplicació.La integritat no només està relacionada amb com es modifiquen les dades, sinó amb com no. Les dades en repòs no haurien de canviar ni ser corrompudes per elements externs, com ara actors maliciosos (per exemple, pirates informàtics) o infraestructures defectuoses (per exemple, discs durs dolents sense redundància).

Disponibilitat

- Les dades han d’estar disponibles a no ser que hi hagi moments específics (per exemple de manteniment), els usuaris esperen un servei continuat.
- Atac: Distributed Denial-of Service (DDoS)

2. Autenticació i autorització

Autenticació:

L'autenticació consisteix a comprovar que qui intenta accedir a un conjunt concret de dades o realitzar alguna acció és qui diu ser.
Definim les identitats dels usuaris dins d'un context d'aplicació mitjançant un identificador o "ID".
Problemes amb els passwords: qwerty o fàcils d’endevinar.
Atacs de força bruta o atacs de diccionari(provar múltiples combinacions de paraules que s'utilitzen habitualment a les contrasenyes, fent que endevinar una contrasenya sigui un procés fàcil si no hi ha prou proteccions de contrasenya)

Autenticació

- Compromís entre fàcil de recordar i no massa fàcil de deduir.
- **The U.S. National Institute of Standards and Technology (NIST) describes in its "Digital Identity Guidelines" document some guidelines for memorized secrets or passwords**:
- Enforce a minimum password length of 8 characters for user-chosen passwords, or 6 character length for randomly-generated numeric PINs.
- All printing ASCII and Unicode characters as well as the space character should be acceptable.
- Authentication services may replace multiple consecutive space characters into a single space character, to account for user typing errors.
- Random password generators should be cryptographically strong (a list of advised generators is provided in the NIST document).
- When creating new passwords, the authentication service should compare the password with a deny-list consisting of commonly used or compromised passwords. This list contains dictionary words, or context-specific words like the user's username.

Autenticació

- No hints should be provided to unauthenticated users about the password. This can provide helpful information to malicious users to guess existing users' passwords.
- Limit the number of failed authentication attempts to not more than 100. This is to prevent online brute force or dictionary attacks which aim to guess the password. The number of tries shouldn't be small enough that causes users to be locked out due to human error.
- After reaching a specific number of failed authentication attempts, impose a wait of 30 seconds up to an hour. This is also to discourage online guessing attacks.
- Consider the use of tools like CAPTCHA which discourage automated access to the application.
- Allow copy-paste into the password field. This encourages users to use password managers which increase the likelihood of users creating strong and unique passwords.
- Don't require other composition rules like requiring special characters or numbers. Don't enforce periodical password updates. Research has found that these limitations do little to prevent password leaks or guessing, while at the same time, they are a common cause of users having bad password practices (for example, using repeated or easy to guess passwords).
- Prefer "pass phrases" consisting of multiple words separated by spaces, over single words. They are harder to guess by brute-force attacks and easier to remember by users.
- Passwords should be encrypted in traffic (for example, while being sent through the network) and in the rest (while being stored in a database).

Autenticació

- Passwords should never be stored in plain-text. A strong hashing algorithm must be used to create a hash derived from the password. The application then can compare the generated hash with the stored hash to confirm the password is correct.
- Hi ha moltes consideracions per a la gestió de contrasenyes. No és fàcil fer complir totes aquestes regles per nosaltres mateixos, per això la majoria de vegades hauríem de preferir utilitzar proveïdors d'autenticació existents especialitzats en seguretat d'aplicacions en lloc d'implementar l'autenticació per nosaltres mateixos.

Autenticació multi-factor

- Codi d’un sol ús enviat a un correu o a un móvil
- L'autenticació multifactor no és perfecta. Els usuaris maliciosos han trobat maneres de segrestar el codi enviat a correus electrònics o telèfons mòbils; també han utilitzat atacs d'enginyeria social per enganyar la gent perquè els proporcioni aquests secrets. És gràcies a la combinació de moltes mesures de seguretat imperfectes que aconseguim una solució millor i en capes.

Single Sing-on (SSO)

- Els serveis SSO redirigeixen els usuaris a un formulari d'autenticació només una vegada: quan intenten accedir per primera vegada a una aplicació que forma part de l'organització.
- Un cop l'usuari s'ha autenticat, es comparteix un testimoni de seguretat amb la resta d'aplicacions de la mateixa organització, permetent que l'usuari hi pugui accedir sense haver de tornar a iniciar sessió.
- SSO requereix una inversió addicional en infraestructura, però facilita la vida dels usuaris alhora que els permet mantenir polítiques de contrasenyes segures.

Autorització

- Una vegada l'usuari s'ha autenticat correctamente, s'assignen els privilegis per acceder a les dades.

User	Resource ID	Read	Edit	Delete
User 1	1232	☑		
User 2	1232	☑	☑	☑
User 3	1232	☑		

- Rols i groups → tenen propietat transitiva
- Un usuari pot ser membre de varis rols o grups.

Autorització

- Millor práctica: donar el nivel d’autorització més Baix per fer la feina.

3. Cas d’ús: autenticació i autorització d’un servei de pizzes

https://miro.com/welcomeonboard/RWJGS0tnbUxTSERUNXZySk9GaDdwbkMzOGhpMEcxdTJmUndSbHJocG5IVWxGVld2dW1UbmhTTlNpUXRYOUhPVXwzNDU4NzY0NTIwNTA4MDI0NzE4fDI=?share_link_id=355906348396

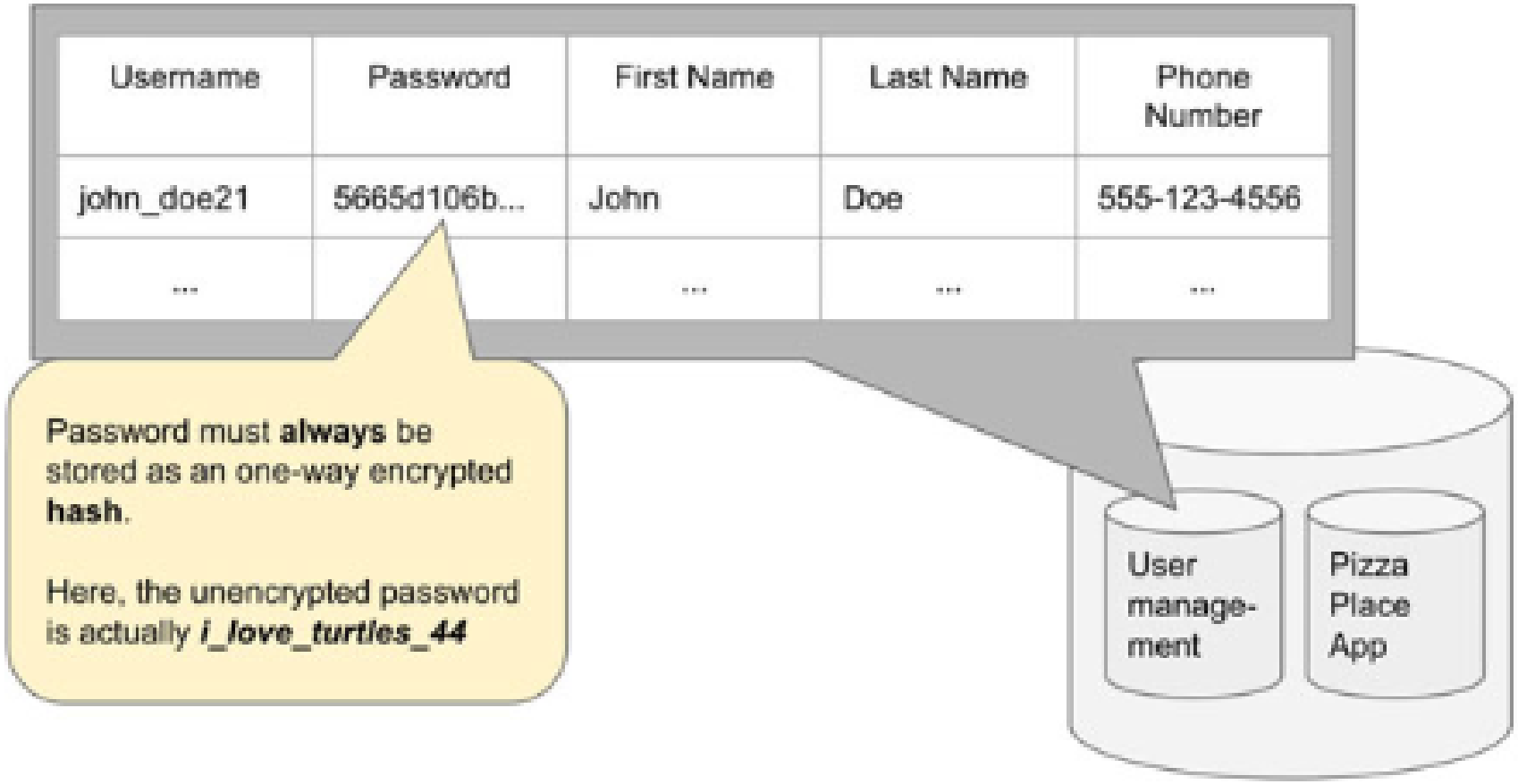
3. Cas d'ús: autenticació i autorització d'un servei de pizzes

Identificar rols:

- Usuaris anònims
- Usuaris registrats
- Administradors
- Propietaris del negoci

Role	Read-Menu	Create Order	Redeem-Rewards	Update-Menu	Read financial-report
AnonymousCustomer	☑	☑			
Customer	☑	☑	☑		
Admin	☑	☑		☑	
Manager	☑	☑		☑	☑

Definir l’emmagatzemament



Definir proteccions de contrasenyes

- L'algorisme més comú que s'utilitza actualment per a aquest xifratge és SHA-256, però és important que facis la teva pròpia investigació per esbrinar quin és el millor algorisme que pots utilitzar en aquest moment per crear la teva aplicació.
- Recuperació de contrasenyes: Un desavantatge de no poder desxifrar una contrasenya és que no podem proporcionar als usuaris reals les seves pròpies contrasenyes si les obliden. El millor que podem fer és restablir la contrasenya substituint el hash existent per un generat a partir d'una nova contrasenya de text sense format i donar la nova contrasenya a l'usuari perquè pugui iniciar sessió i actualitzar la contrasenya de nou.

HTTP cookies

- Les galetes són petites dades que es transmeten entre el navegador d'un client i el servidor. Les galetes s'utilitzen habitualment per emmagatzemar informació que cal enviar en cada sol·licitud, com ara galetes de sessió, tokens d'autorització o preferències de l'usuari com l'idioma.

HTTP cookies

- Alguns servidors opten per emmagatzemar les dades de l'usuari directament a la galeta, mentre que altres prefereixen emmagatzemar les dades de l'usuari en una base de dades i només utilitzen la galeta per emmagatzemar l'ID de sessió per recuperar el registre. Hi ha diverses compensacions per a aquests enfocaments, però la majoria de vegades és més difícil emmagatzemar totes les dades de sessió a la galeta, ja que implica signar-la criptogràficament per assegurar-se que un usuari maliciós no l'ha manipulat i limitar-ne la quantitat. de dades que pot emmagatzemar, per tal de no frenar el trànsit afegint massa informació a cada sol·licitud.

Testejar el control d’accés

- Tests unitaris manuals o automàtics.

Federated authentication

- A l'autenticació federada, utilitzeu un servei de gestió d'usuaris o un proveïdor d'identitats (identity provider en anglès o IP) independent per autenticar els vostres usuaris. La IP s'encarrega d'emmagatzemar els usuaris i les seves dades. Una vegada que la IP validi que un usuari és qui diu que és, li donarà un testimoni que els usuaris utilitzaran per fer saber a la vostra aplicació que realment estan autenticats.

Autenticació federada

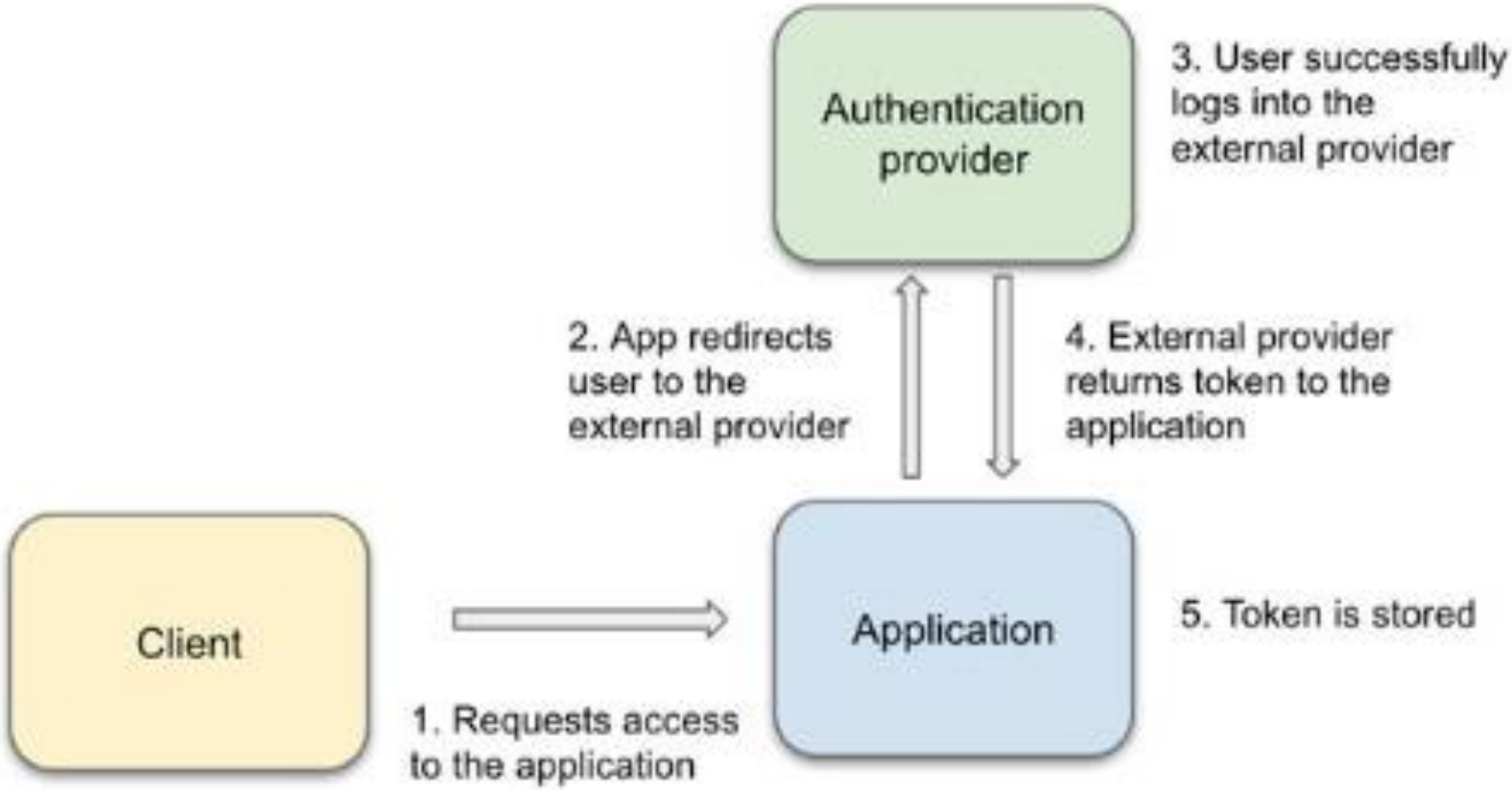


Figure 6.8: Authentication flow when integrating with an external provider

Identity provider (IP)

- Tens diverses opcions a l'hora de triar una IP:
  - Podeu crear la vostra pròpia IP. Realment no s'aconsella, tret que siguis una empresa gran o que tinguis previst oferir serveis IP tu mateix. Requereix massa feina.
  - Instal·leu una solució disponible com WSO2 Identity Server o Keycloak. Podeu comprar una llicència per a aquests productes i instal·lar-los a la vostra xarxa privada.
  - Utilitzeu serveis públics basats en núvol. L'autenticació federada és un dels principals serveis d'empreses especialitzades com Okta o Auth0; però grans empreses com Facebook, LinkedIn o Google ofereixen els seus propis serveis IP als quals us podeu integrar.

Avantatges i inconvenients de federated authentication

- Els múltiples avantatges d'utilitzar l'autenticació federada són:
  - Es pot integrar perfectament amb aplicacions internes i externes. Sempre que totes les aplicacions implicades confiïn en el proveïdor d'identitat (IP).
  - Millor separació de preocupacions. Els desenvolupadors que treballen en la IP poden concentrar-se en la creació de totes les últimes funcions de l'aplicació secundària, així com en el compliment de regulacions com HIPAA i GDPR.
  - El servei IP pot evolucionar i créixer independentment de totes les aplicacions que el consumeixen. Només consumirà els recursos que realment necessita, en lloc de compartir-los amb una aplicació.
- D'altra banda, alguns dels inconvenients són:
  - Augmenta la complexitat de l'aplicació. Això és cert per a qualsevol implementació que requereixi que l'aplicació es distribueixi entre diferents servidors.
  - Es requereixen mesures addicionals per confirmar que totes les dades d'autenticació i d'autorització són correctes i fiables. Aquestes mesures solen significar passos de comunicació addicionals entre l'aplicació i la IP, així com l'ús de claus criptològiques per assegurar-se que tots els testimonis són correctes i no manipulats.

Com que l'autenticació federada implica la integració i la comunicació de múltiples aplicacions i serveis, és important utilitzar protocols i estàndards ben definits. Els més utilitzats són SAML (madur, permet comunicar-se amb proxies) i OpenID.

5. Construir la seguretat en els disseny de l’aplicació

- Descomposar l’aplicació
- Determinar i prioritzar amenaces
- Determinar mesures de mitigació i prevenció

Descomposar l’aplicació

- Punts d'entrada que poden ser utilitzats per usuaris maliciosos per accedir i potencialment atacar l'aplicació.
- Actius que poden ser d'interès per a usuaris maliciosos, com ara bases de dades, registres que contenen informació sensible, etc.
- Enumereu les possibles vulnerabilitats comunes al tipus d'aplicació que estem creant (per exemple, aplicacions web, mòbils o d'escriptori).
- Els privilegis d'accés per a rols i actors.

Determinar i prioritzar amenaces

Model STRIDE de Microsoft:

- Spoofing identity: Illegally impersonate another user. Tampering with data. Any action which negatively impacts the integrity of data at any point in the application.
- Repudiation: Repudiation is the capability of malicious users to deny and hide their malicious actions. These vulnerabilities happen when there are no records which can prove a user performed a malicious action.
- Information disclosure: Violations to the confidentiality levels of data within the application.
- Denial of service: Violations to the availability of data within the application.
- Elevation of privilege: Cases where unprivileged users gain access to parts or data of the application which they shouldn’t have access to, like admin features.

Determinar i **prioritzar** amenaces

DREAD:

- Damage: How bad would an attack be?
- Reproducibility: How easy is it to reproduce the attack?
- Exploitability: How much work is it to launch the attack?
- Affected users: How many people will be impacted?
- Discoverability: How easy is it to discover the threat?

Mitigar

DREAD:

- Arregleu aquelles vulnerabilitats que es poden solucionar.
- Mitigar les vulnerabilitats que no es poden solucionar.
- Accepteu vulnerabilitats que no es poden mitigar o suprimiu les característiques que les contenen si no es poden acceptar.

6. OWASP: les vulnerabilitats més comunes

- OWASP: Open Web Application Security Project
- The OWASP Top 10 for 2021 is:
- Broken Access Control: OWASP: “Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, *modification, or destruction of all data or performing a business function outside the user’s limits.*”

OWASP

- **Cryptographic failures**: These vulnerabilities cover failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **Injection**: Injection vulnerabilities are those where, due lack of correct validation or sanitization of data incoming into the application, malicious users are able to pass parameters or execute code remotely to retrieve sensitive information or gain privileged access to parts of the application.
- **Insecure design**: These vulnerabilities involve "*missing or incorrect control design*", which is the lack of consideration of application security features, constrains, and analysis like threat modeling while designing the application.
- **Security misconfiguration**: Applications and servers which rely on configuration files to retrieve settings during runtime are vulnerable when those configurations contain factory settings like known or default passwords and keys, or excessively permissive configurations in things like firewalls, open ports, and other network configurations.

OWASP

- **Vulnerable and outdated components**: During the lifetime of most code libraries and dependencies, users and developers find vulnerabilities which then are fixed in future versions. When applications don’t update these components in time, they open themselves to those well-known vulnerabilities.
- **Identification and authentication failures**: Several vulnerabilities exist which cause the incorrect use and implementation of the authentication and authorization flows we discussed in this chapter. Other situations which compromise authentication are those where we expose sensitive data like access tokens or client secrets.
- **Software and data integrity failures**: These are vulnerabilities which fail to guarantee the integrity of the application and the data that is used by it.
- **Security logging and monitoring failures**: One critical aspect of application security is the system’s capability of detecting and monitoring intrusions and attacks. Without an adequate logging and monitoring implementation, attacks can be led successfully without us having the chance to try to stop or mitigate them, or at least recover from them.

OWASP

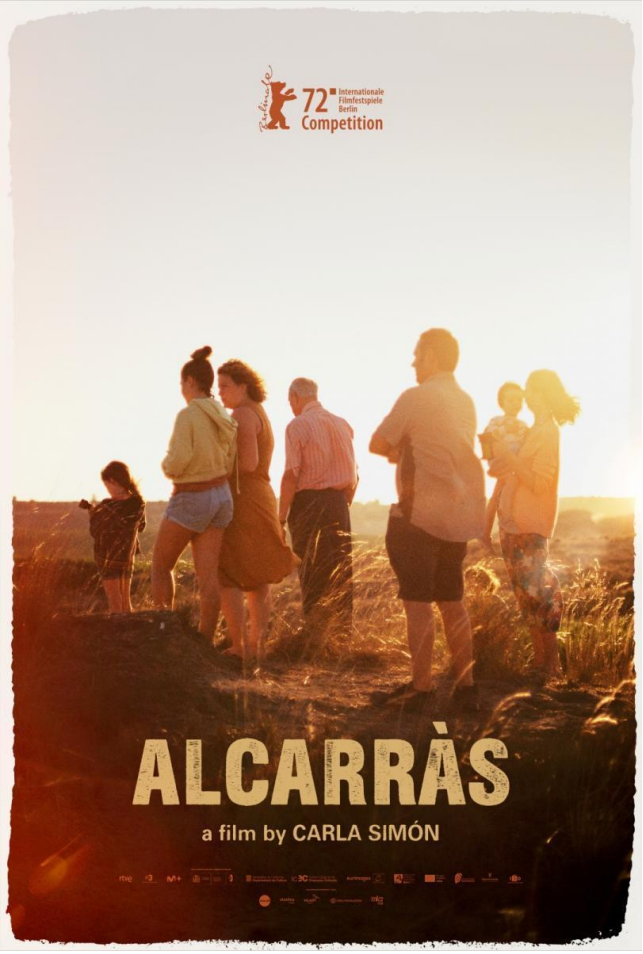
- **Server-side request forgery**: This specific vulnerability exists when *a web application is fetching a remote resource without validating the user-supplied URL*. This lack of validation can lead to the server making requests to malicious resources through an insecure channel.

The OWASP website includes more complete descriptions of these categories, as well as some examples of the most common vulnerabilities. Feel free to jump in and get a better idea of how hackers take advantage of poorly implemented applications. Then, use this knowledge to build better software.

Exercici

- Pick two different apps you use on a semi-daily basis. Then, for each of those applications, answer the following questions: What part or parts of the application do you think malicious users target the most? How do you think they try to "*hack*" these applications? Is there a part of the application which might be especially vulnerable?

Exercici


72 Internationale Filmfestspiele Berlin
Competition
ALCARRÀS
a film by CARLA SIMÓN

Recursos

- Study about the impact of data breaches: **https://www.verizon.com/business/resources/reports/dbir/**
- NIST Digital Identity Guidelines: **https://pages.nist.gov/800-63-3/sp800-63b.html**
- STRIDE model: **https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)**

Bibliografia

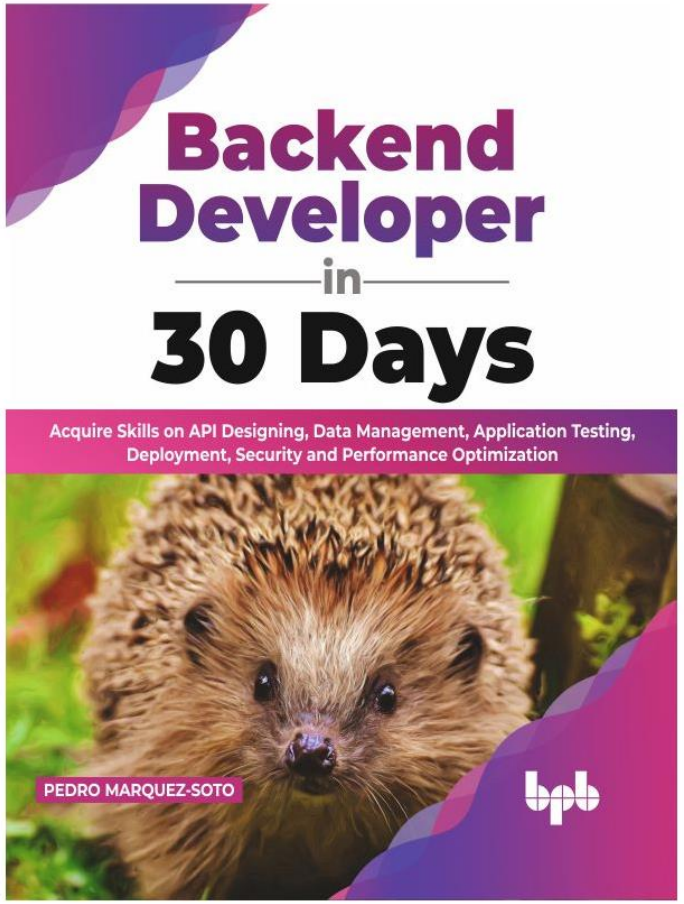
Adobe Digital Editions - Backend Developer in 30 Days: Acquire Skills on Api Designing, Data Management, Application Testing, Deployment, Security and Performance Optimization

Archivo Edición Lectura Ayuda

Biblioteca

Tabla de contenido

- Cover Page
- Title Page
- Copyright Page
- Dedication Page
- About the Author
- Acknowledgement
- Preface
- Errata
- Table of Contents
- 1. Building Multi-User Apps
- 2. The Client-Server Architecture
- 3. Designing APIs
- 4. End-to-End Data Management
- 5. Automating Application Testing
- 6. Securing Applications
  - Structure
  - Objectives
  - The CIA triad: Confidentiality, Integrity, and Availability
    - Confidentiality
      - Loss of confidentiality
    - Integrity
    - Availability
  - Access Control: Authentication and authorization
    - Authentication
    - Authorization
  - Use case: Implementing basic authentication and authorization for the
  - Federated authorization
  - Building security into the application's design
  - OWASP Top 10: The most common vulnerabilities
  - Conclusion
  - Questions
  - Resources
- 7. Handling Errors
- 8. Adopting Frameworks
- 9. Deploying Applications
- 10. Creating High-performance Apps
- 11. Designing a System



1 / 2689

Exercici Kahoot

- https://kahoot.it

7. Altres consideracions de seguretat de backend

- Sql Injection: https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
- Uso de capa https (encrypt) https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto
- Uso de JWT con sellado de tiempo
- CORS
- Gestión de perfiles correcta (Access Control)
- Encriptación de passwords y almacenamiento
- Deserialización segura

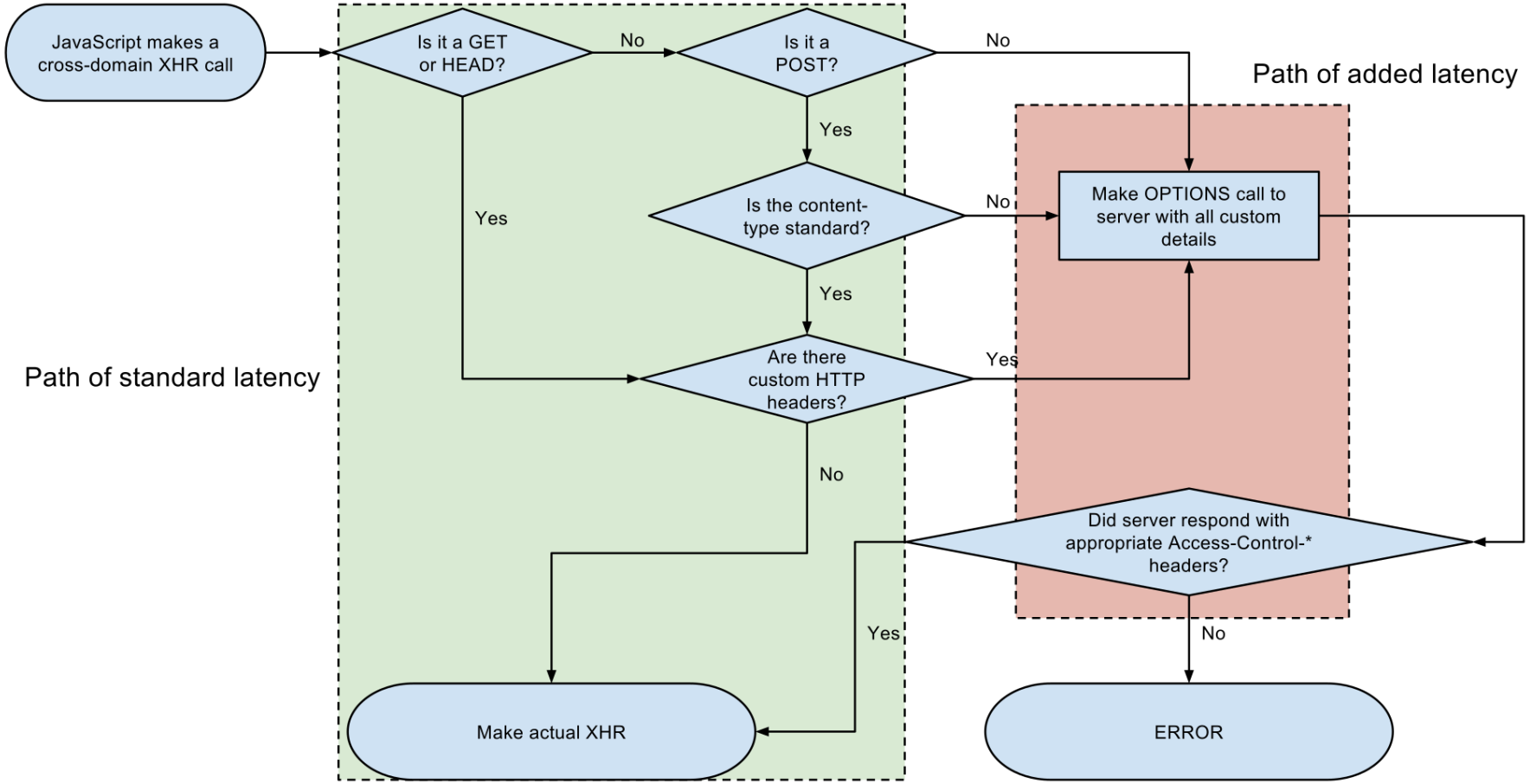
JWT con sellado de tiempo

- JWT es el medio principal de autenticación en servicios de tipo REST, es un medio compacto y autocontenido para enviar datos de manera segura entre las partes en formato JSON.
- Un JWT puede ser firmado tanto con un algoritmo simétrico como uno asimétrico.
- Los JWT consisten de tres partes separadas por puntos (.), las cuales son: cabecera (header), cuerpo (payload) y la firma (signature).
- Se debe considerar el cifrado de los datos del cuerpo si estos se consideran sensibles, véase el punto (Confidencialidad).
- Por su facilidad de implementación al trabajar con un servicio REST, se recomienda siempre utilizar JWT, sin olvidar que muchas veces es necesario revocar un token, por lo cual se sugiere que como mínimo esta implementación soporte la revocación además del tiempo de expiración del JWT.

CORS (Cross-origin resource sharing)

- L'ús compartit de recursos entre orígens (CORS) és un mecanisme que permet que els recursos restringits d'una pàgina web es sol·licitin des d'un altre domini fora del domini des del qual es va servir el primer recurs.
- Una pàgina web pot incrustar lliurement imatges d'origen creuat, fulls d'estil, scripts, iframes i vídeos. La política de seguretat del mateix origen prohibeix de manera predeterminada determinades sol·licituds "entre dominis", especialment les d'Ajax.
- CORS defineix una manera en què un navegador i un servidor poden interactuar per determinar si és segur permetre la sol·licitud d'origen creuat. Permet més llibertat i funcionalitat que les sol·licituds purament del mateix origen, però és més segur que simplement permetre totes les sol·licituds d'origen creuat.

CORS (Cross-origin resource sharing)

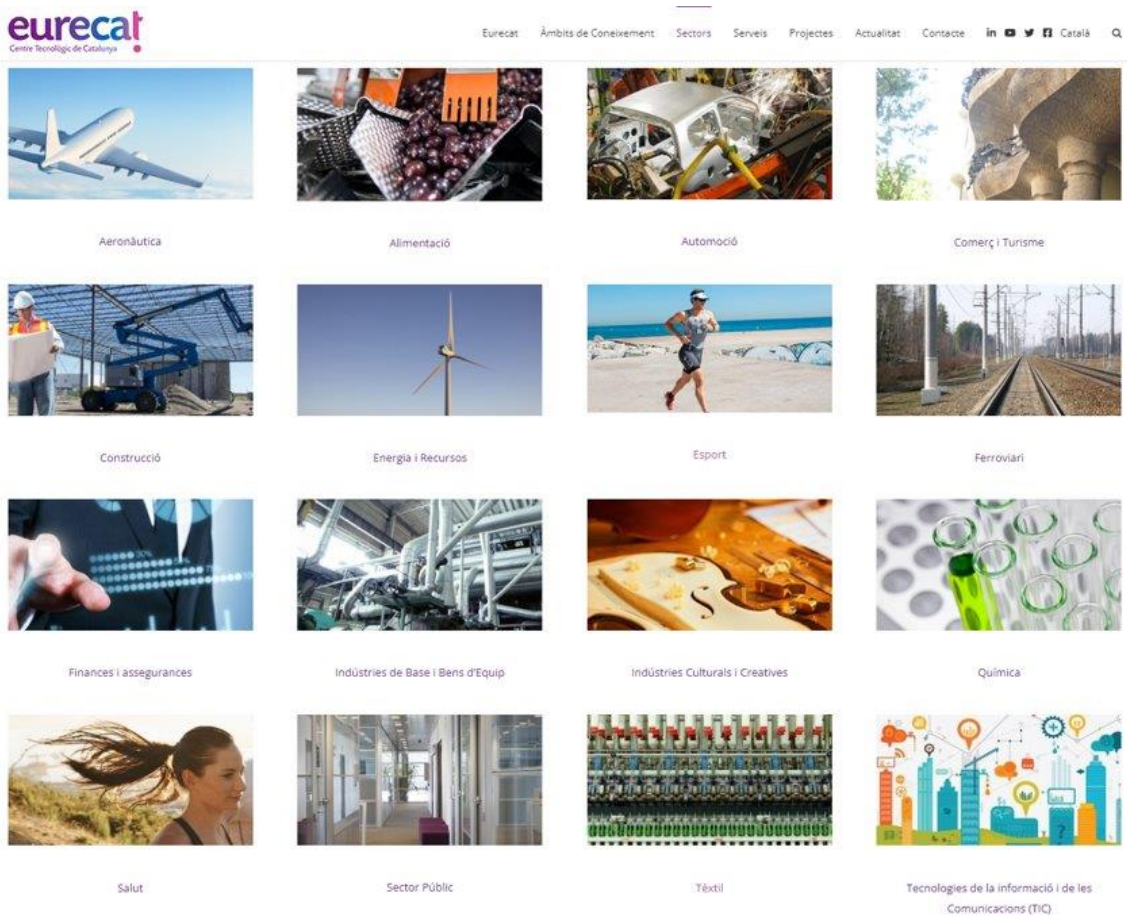


Páginas relevantes

- https://blog.hackmetrix.com/insecure-deserialization/
- https://securitytrails.com/blog/backend-security-risks
- https://geekflare.com/web-backend-security-risk

8. Miscel·lània

Camps d’aplicació



Tipus de seguretat en les dades

https://www.fortinet.com/resources/cyberglossary
https://www.fortinet.com/resources/cyberglossary/data-security

Encryption

Data Erasure: More secure than standard data wiping, data erasure uses software to completely overwrite data on any storage device. It verifies that the data is unrecoverable.

Data Masking: By masking data, organizations can allow teams to develop applications or train people using real data. It masks personally identifiable information (PII) where necessary so that development can occur in environments that are compliant.

Data Resiliency: Resiliency is determined by how well an organization endures or recovers from any type of failure

Best Practices for Ensuring Data Security and Privacy

Why is data security important? Primarily, it keeps your data secure and builds confidence among your customers. Here are some best practices that have been effective for other organizations:

1. **Secure your information:** This means managing who has access and encrypting your data. Only people who need it to perform essential functions should have access, and information should be encrypted as it goes back and forth between the database and their computer or device.
2. **Prepare ahead of time for threats:** You can get ready for a potential data security incident by testing your system, educating employees, devising an incident management plan, and creating a data recovery plan.
3. **Delete data you are not using:** You should get rid of both digital and physical copies of data you no longer need. In this way, you reduce the chances of a hacker discovering it and using it for profit.

Solucions

Data discovery and classification tools
Data and file activity monitoring
Vulnerability assessment and risk analysis tools
Automated compliance reporting

Criteris i procediments en l'emmagatzematge de dades

Estratègies:

Physical security of servers and user devices
Access management and controls
Application security and patching
Backups
Employee education
Network and endpoint security monitoring and controls

Tendències de seguretat en les dades

AI
Multicloud security
Quantum

Interacció

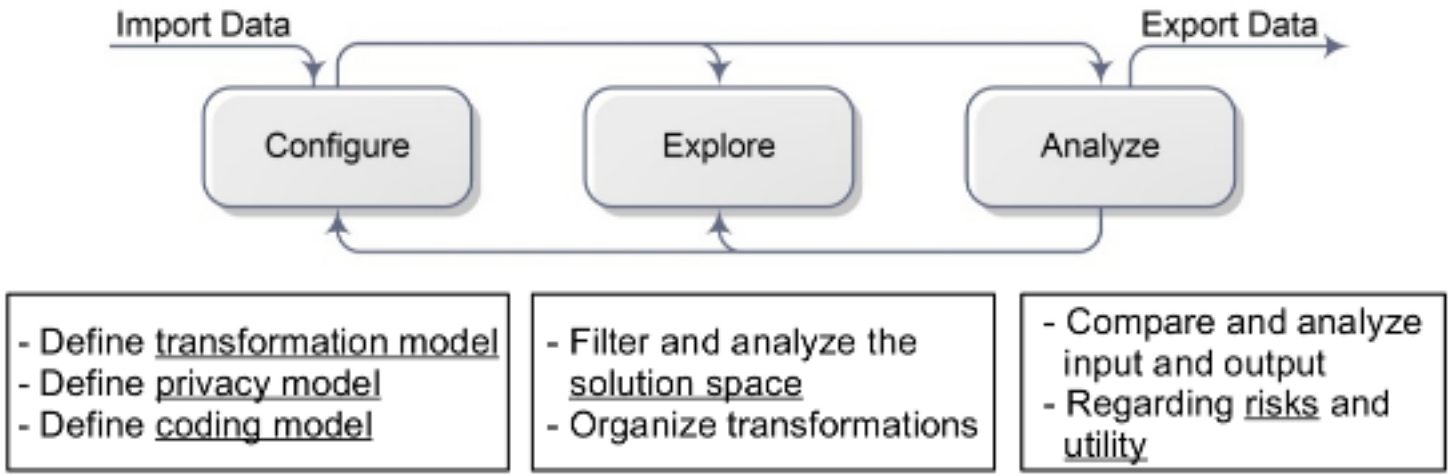
Achieving enterprise-grade data security
Data security and the cloud
Data security and BYOD (Bring your own Device)

Data security, privacy and protection solutions

Data security solutions
Data security devices
Homomorphic encryption
Storage data backup (Github) and recovery
Data encryption solutions
Data privacy
Ransomware protection
Zero trust security
Flash storage solutions
GDPR

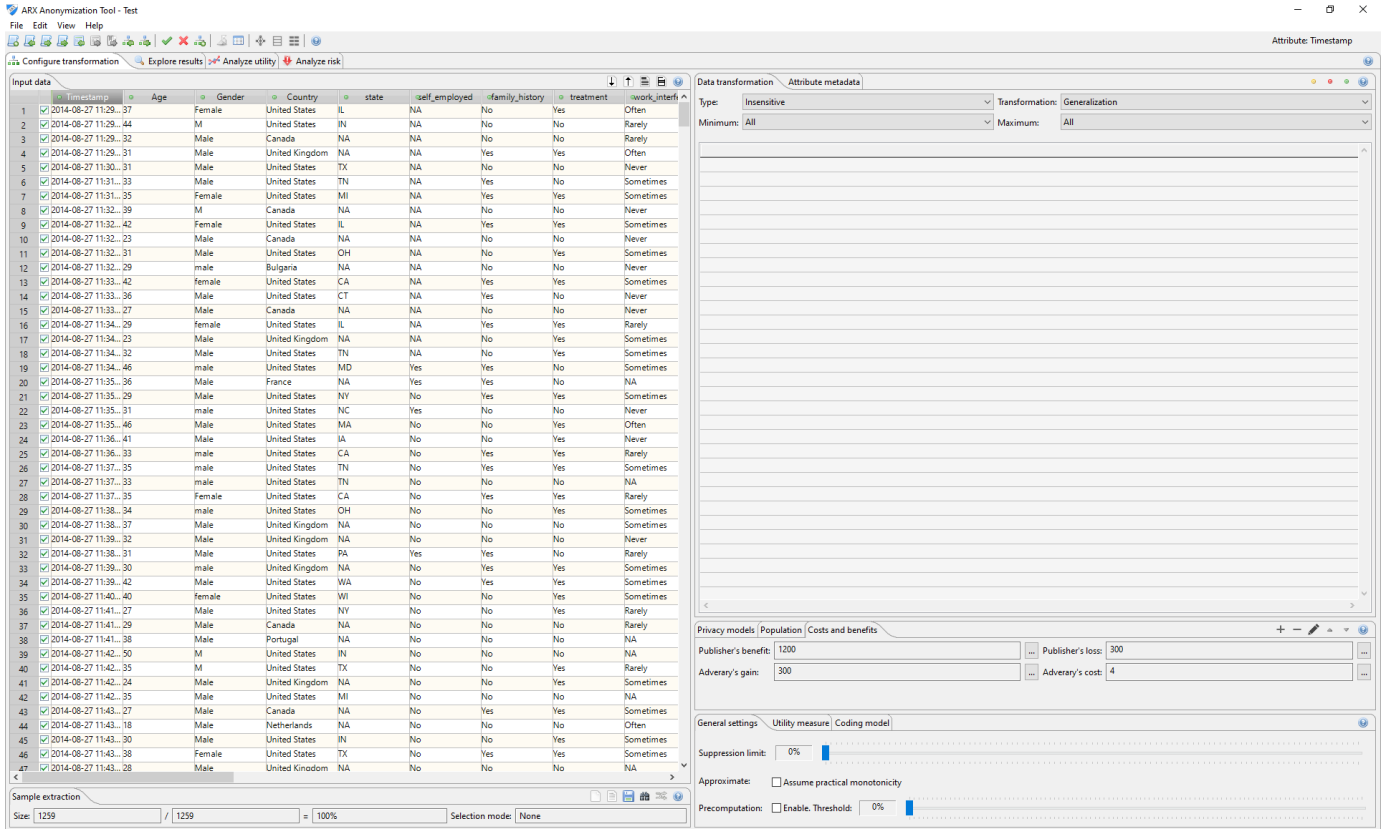
ARX Data anonymization tool

https://arx.deidentifier.org

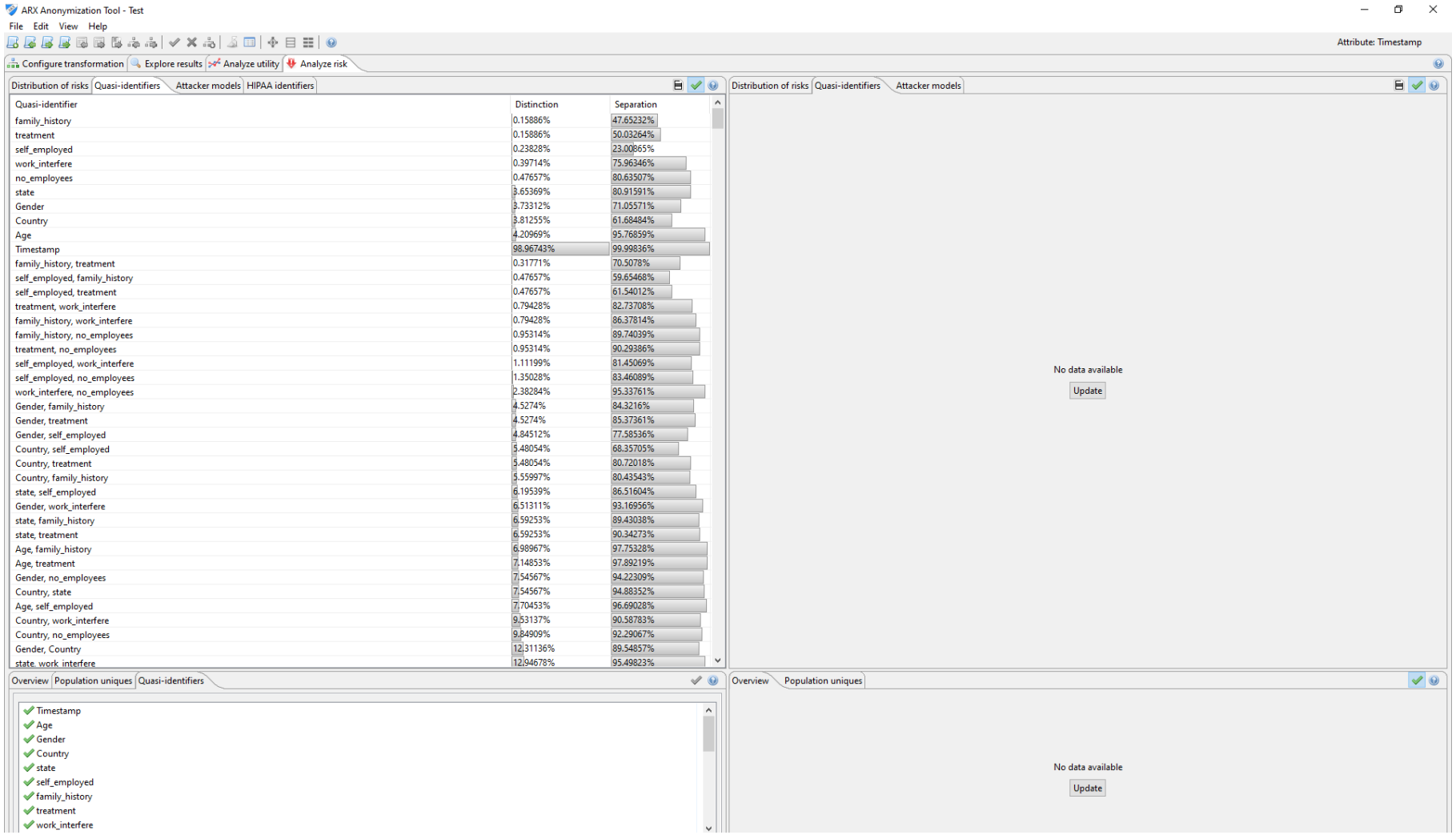


Exemple pràctic ARX anonymization tool

Carreguem dades de:
https://www.kaggle.com/datasets/osmi/mental-health-in-tech-survey



Exemple pràctic ARX anonymization tool



What Are the Components of Access Control?

Access control is managed through several components:

Authentication

Authentication is the initial process of establishing the identity of a user. For example, when a user signs in to their email service or online banking account with a username and password combination, their identity has been authenticated. However, authentication alone is not sufficient to protect organizations' data.

Authorization

Authorization adds an extra layer of security to the authentication process. It specifies access rights and privileges to resources to determine whether the user should be granted access to data or make a specific transaction.

For example, an email service or online bank account can require users to provide two-factor authentication (2FA), which is typically a combination of something they know (such as a password), something they possess (such as a token), or something they are (like a biometric verification). This information can also be verified through a 2FA mobile app or a thumbprint scan on a smartphone.

Access

Once a user has completed the authentication and authorization steps, their identity will be verified. This grants them access to the resource they are attempting to log in to.

Manage

Organizations can manage their access control system by adding and removing the authentication and authorization of their users and systems. Managing these systems can become complex in modern IT environments that comprise cloud services and on-premises systems.

Audit

Organizations can enforce the principle of least privilege through the access control audit process. This enables them to gather data around user activity and analyze that information to discover potential access violations.

How Does Access Control Work?

Access control is used to verify the identity of users attempting to log in to digital resources. But it is also used to grant access to physical buildings and physical devices.

Physical Access Control

Common examples of physical access controllers include:

Barroom Bouncers

Bouncers can establish an access control list to verify IDs and ensure people entering bars are of legal age.

Subway Turnstiles

Access control is used at subway turnstiles to only allow verified people to use subway systems. Subway users scan cards that immediately recognize the user and verify they have enough credit to use the service.

Keycard or Badge Scanners in Corporate Offices

Organizations can protect their offices by using scanners that provide mandatory access control. Employees need to scan a keycard or badge to verify their identity before they can access the building.

Logical/Information Access Control

Logical access control involves tools and protocols being used to identify, authenticate, and authorize users in computer systems. The access controller system enforces measures for data, processes, programs, and systems.

Signing Into a Laptop Using a Password

A common form of data loss is through devices being lost or stolen. Users can keep their personal and corporate data secure by using a password.

Unlocking a Smartphone With a Thumbprint Scan

Smartphones can also be protected with access controls that allow only the user to open the device. Users can secure their smartphones by using biometrics, such as a thumbprint scan, to prevent unauthorized access to their devices.

Remotely Accessing an Employer’s Internal Network Using a VPN

Smartphones can also be protected with access controls that allow only the user to open the device. Users can secure their smartphones by using biometrics, such as a thumbprint scan, to prevent unauthorized access to their devices.

What Is the Difference Between Authentication and Authorization?

Authentication and authorization are crucial to access control in security. Authentication is the process of logging in to a system, such as an email address, online banking service, or social media account. Authorization is the process of verifying the user's identity to provide an extra layer of security that the user is who they claim to be.

Importance of Access Control in Regulatory Compliance

Access control is crucial to helping organizations comply with various data privacy regulations. These include:

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that protects the payment card ecosystem. An access control system is crucial to permitting or denying transactions and ensuring the identity of users.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was created to protect patient health data from being disclosed without their consent. Access control is vital to limiting access to authorized users, ensuring people cannot access data that is beyond their privilege level, and preventing data breaches.

SOC 2

Service Organization Control 2 (SOC 2) is an auditing procedure designed for service providers that store customer data in the cloud. It ensures that providers protect the privacy of their customers and requires organizations to implement and follow strict policies and procedures around customer data. Access control systems are crucial to enforcing these strict data security processes.

ISO 27001

The International Organization for Standardization (ISO) defines security standards that organizations across all industries need to comply with and demonstrate to their customers that they take security seriously. ISO 27001 is the ISO's gold standard of information security and compliance certification. Implementing access controls is crucial to complying with this security standard.

What Are the Different Types of Access Controls?

There are various types of access controls that organizations can implement to safeguard their data and users. These include:

Attribute-based Access Control (ABAC)

ABAC is a dynamic, context-based policy that defines access based on policies granted to users. The system is used in identity and access management (IAM) frameworks.

Discretionary Access Control (DAC)

DAC models allow the data owner to decide access control by assigning access rights to rules that users specify. When a user is granted access to a system, they can then provide access to other users as they see fit.

Mandatory Access Control (MAC)

MAC places strict policies on individual users and the data, resources, and systems they want to access. The policies are managed by an organization's administrator. Users are not able to alter, revoke, or set permissions.

Role-Based Access Control (RBAC)

RBAC creates permissions based on groups of users, roles that users hold, and actions that users take. Users are able to perform any action enabled to their role and cannot change the access control level they are assigned.

Break-glass Access Control

Break-glass access control involves the creation of an emergency account that bypasses regular permissions. In the event of a critical emergency, the user is given immediate access to a system or account they would not usually be authorized to use.

Rule-based Access Control

A rule-based approach sees a system admin define rules that govern access to corporate resources. These rules are typically built around conditions, such as the location or time of day that users access resources.

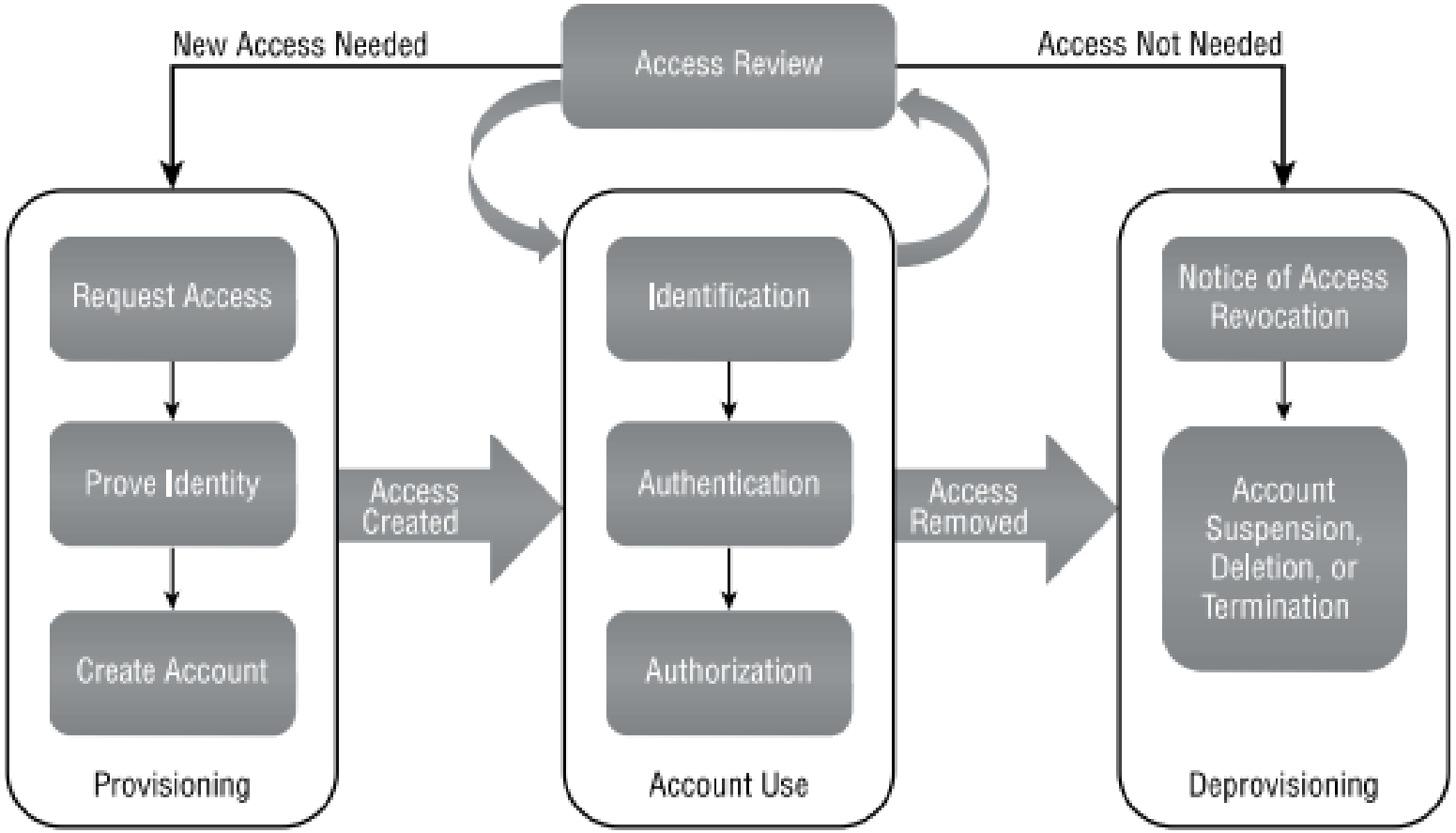


FIGURE 5.1 **The access management lifecycle**

https://es.wikipedia.org/wiki/OpenID

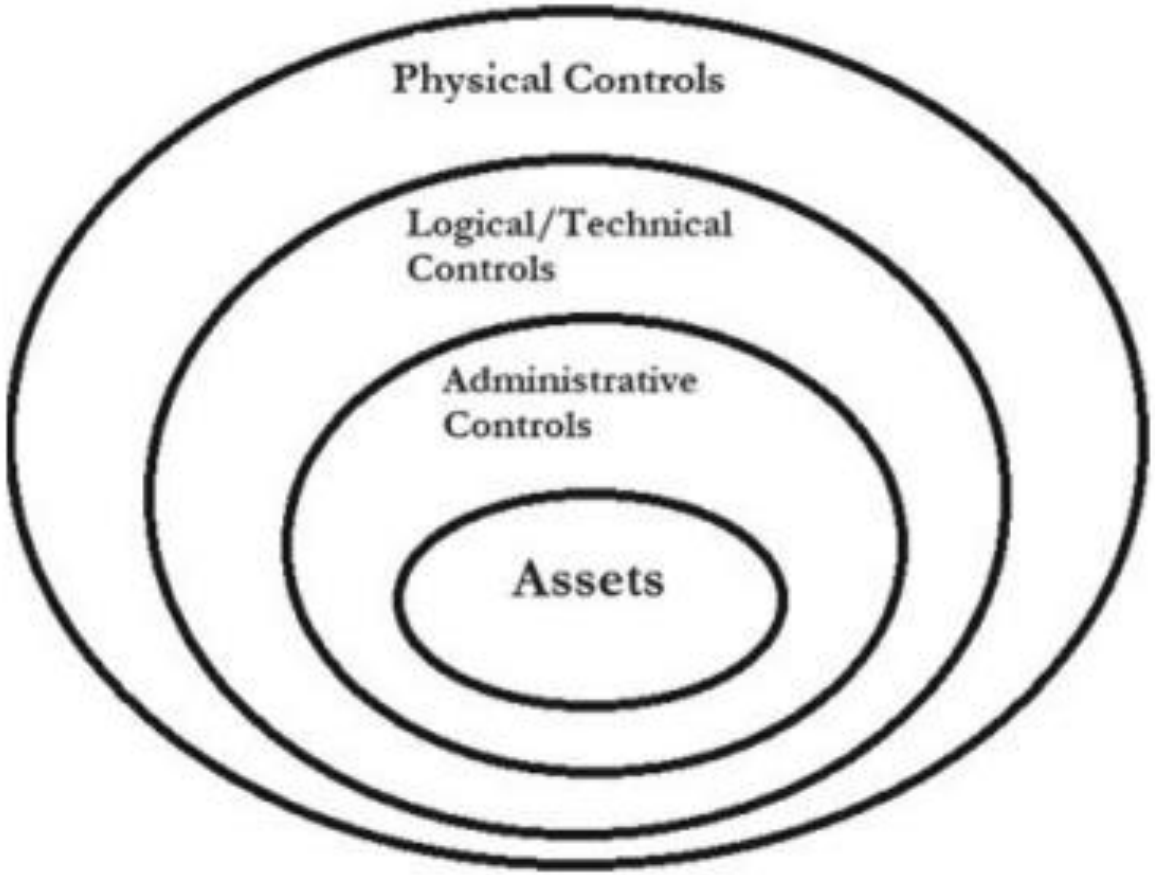


Fig. 9.1 Defense-in-depth implementation in security controls

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Certification **Exam Outline**

Effective Date: May 1, 2021

Figure 9: Placing the ECSF role profiles in the context of a management circle

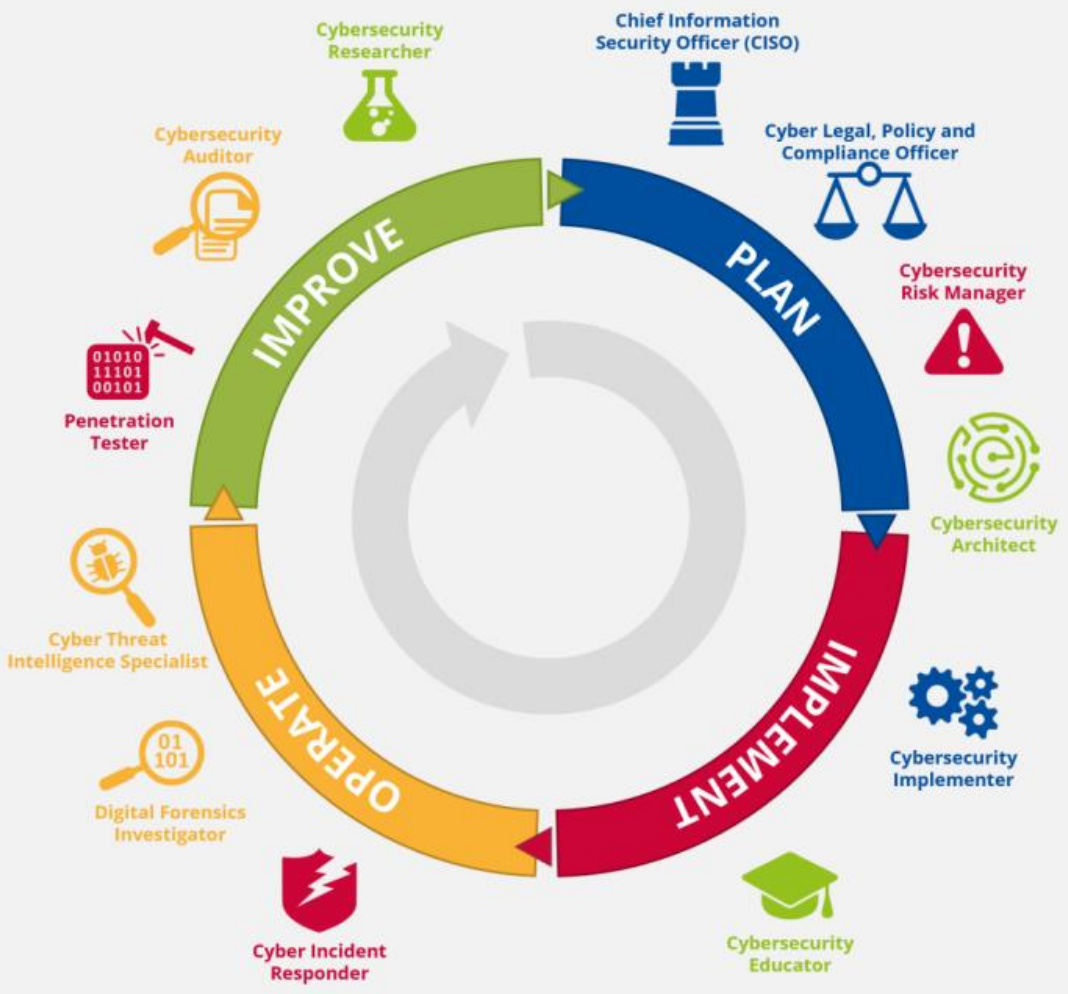


Table 5: The ESCO profiles and the ECSF profiles relationships

ESCO code	ESCO Occupation	Relationship	ECSF role profile
2149.2.8	Research engineer	might include	Cybersecurity Researcher
2310.1	Higher education lecturer	might include	Cybersecurity Educator
2356	Information technology trainer	might include	Cybersecurity Educator
2511.18	IT auditor	might include	Cybersecurity Auditor
2519.2	ICT auditor manager	might include	Cybersecurity Auditor
2529.1	Chief ICT security officer	is	Chief Information Security Officer (CISO)
2529.2	Digital forensic expert	is	Digital Forensics Investigator
2529.3	Embedded system security engineer	might be included	Cybersecurity Implementer
2529.4	Ethical hacker	is	Penetration Tester
2529.6	ICT Security administrator	might be included	Cybersecurity Implementer
2529.7	ICT security engineer	might be included	Cybersecurity Architect
2529.7	ICT security engineer	might be included	Cybersecurity Implementer
2619.4	Data protection officer	is	Cyber Legal, Policy & Compliance Officer

https://esco.ec.europa.eu/en/classification/occupation_main

Hacking for dummies

- Cracker
- White hat
- Black hat
- Gray hat
- Green hat
- Red hat
- Blue hat

Key loggers, SQL injection attack, distributed denial of service, ethical hacking

Seguretat dades

Tabla 2. Clasificación según el impacto de seguridad de los datos

Objetivo de seguridad	Impacto bajo	Impacto moderado	Impacto alto
Confidencialidad	La divulgación no autorizada de información puede tener un efecto adverso **limitado** en la organización.	La divulgación no autorizada de información puede tener un efecto adverso **grave** en la organización.	La divulgación no autorizada de información puede tener un efecto adverso grave o **catastrófico** en la organización.
Integridad	La modificación o destrucción no autorizada de la información puede tener un efecto adverso **limitado** en la organización.	La modificación o destrucción no autorizada de la información puede tener un efecto adverso **grave** en la organización.	La modificación o destrucción no autorizada de la información puede tener un efecto adverso grave o **catastrófico** en la organización.
Disponibilidad	La interrupción del acceso o uso de la información o un sistema de información puede tener un efecto adverso **limitado** en la organización.	La interrupción del acceso o uso de la información o un sistema de información puede tener un efecto adverso **grave** en la organización.	La interrupción del acceso o uso de la información o un sistema de información puede tener un efecto adverso grave o **catastrófico** en la organización.

Exercici

- El propietari d'una perruqueria perd accidentalment una carpeta que contenia les factures dels seus proveïdors dels tres últims mesos.

- Un empleat d'una assessoria legal obre accidentalment un correu que conté *ransomware* al seu ordinador portàtil, que està connectat exclusivament a Internet.

- Similar a el cas anterior, però aquesta vegada l'empleat està utilitzant el PC de la seva oficina que té accés a Internet i a la intranet corporativa.

Qualitat de les dades

- Exactitut
- Completitut
- Consistència
- Puntualitat
- Unicitat
- Validesa

OEIAC
Observatori d'Ètica en Intel·ligència Artificial de Catalunya

Qui som | Com funciona | A qui va dirigit | Senzillesa | Informe | Registre | **Model d'autoavaluació PIO**

Model d'autoavaluació PIO

Presentem el model d'autoavaluació PIO (Principis, Indicadors i Observables) per avançar en l'avaluació ètica de dades i sistemes d'intel·ligència artificial a través d'un formulari de verificació o checklist

Iniciar Formulari

Avaluem

Proporcionem una eina per la

Revisem

Portem a terme una revisió

Aconsellem

T'oferim la possibilitat de rebre

https://oeiac.cat

Springer Link

Search Log in

Textbook | © 2023

Cybersecurity and Identity Access Management

Authors: Bharat S. Rawal, Gunasekaran Manogaran, Alexender Peter

Discusses the different third-party attacks and hacking processe

Maximizes reader insights into effective cyber security, malware, firewalls and cryptography

Simplifies a complicated picture into hacking and penetration testing

1933 Accesses

Sections

Table of contents
About this book
Keywords
Authors and Affiliations
About the authors
Bibliographic Information

This is a preview of subscription content, access via your institution.

Access via your institution →

eBook EUR 85.59

Price includes VAT (Spain)

- ISBN: 978-981-19-2658-7
- Instant PDF download
- Readable on all devices
- Own it forever
- Exclusive offer for individuals only
- Tax calculation will be finalised during checkout

Buy eBook

Hardcover Book EUR 103.99

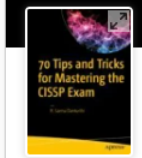
Learn about institutional subscriptions

https://link.springer.com/book/10.1007/978-981-19-2658-7

Springer Link

Search Log in

Introducing new learning courses and educational videos from Apress. Start watching



Book | © 2020

70 Tips and Tricks for Mastering the CISSP Exam

Apress®

Authors: R. Sarma Danturthi

Shows you how to read an exam question and correctly pick an answer from a set of solutions

Provides tips and tricks to tackle the verbiage given in an exam question, quickly eliminate wording that is not required, get the gist of the question, and find the solution without spending too much time

Teaches you how words such as MOST, BEST, FIRST, and LAST are used in exam questions and how to discern the correct answer to a question when multiple options look close as possible solutions

3931 Accesses

Sections

Table of contents
About this book
Keywords
Authors and Affiliations

Access via your institution →

eBook EUR 36.99

Price includes VAT (Spain)

- ISBN: 978-1-4842-6225-2
- Instant PDF download
- Readable on all devices
- Own it forever
- Exclusive offer for individuals only
- Tax calculation will be finalised during checkout

Buy eBook

Softcover Book EUR 46.79

Learn about institutional subscriptions

https://link.springer.com/book/10.1007/978-1-4842-6225-2

Enllaços d’interès

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679
https://www.iispv.cat/es/ceim/comite-etic-dinvestigacio-amb-medicamets-ceim-institut-dinvestigacio-sanitaria-pere-virgili/
https://ticsalutsocial.cat/
https://web.gencat.cat/ca/seu-electronica/sobre-la-seu/proteccio-de-dades
https://salutweb.gencat.cat/ca/el_departament/proteccio-de-dades/
https://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/
https://www.cloudflare.com/es-es/
https://snyk.io/
https://www.incibe.es/
https://www.is4k.es/
https://www.osi.es/es
https://www.incibe.es/protege-tu-empresa/blog
https://www.incibe.es/protege-tu-empresa/blog/transforma-tu-pyme-ciberresiliencia-siguiendo-los-consejos-enisa
https://archive.org/
https://tryhackme.com/
https://www.amazon.es/El-arte-invisibilidad-T%C3%ADtulos-Especiales/dp/8441540616
https://storage.cdn.eurecat.org/CIDAI/WhitePapers/ACC_CIDAI_AICiberseguretat.pdf
https://krebsonsecurity.com
http://cybercat.eu/
https://www.cyberseek.org/
https://ciberseguretat.gencat.cat/ca/Resums-mensuals-de-Tendencies-en-Ciberseguretat/index.html
https://www.futurepedia.io/

Adreça de contacte per dubtes

cibernarium@barcelonactiva.cat

Ajuntament de Barcelona

Barcelona Activa

barcelonactiva.cat