ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Seguretat en els testimonis de sessió: desafiaments i estratègies de protecció a l'entorn digital

TLP: WHITE

OCTUBRE 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	25/10/2024	30/10/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

En el món digital actual, **l'ús dels testimonis (tokens)** s'ha estès ràpidament en àrees com l'autenticació d'usuaris, la protecció d'actius digitals i el control d'accés a sistemes. Els testimonis han sorgit com una eina essencial per a la seguretat i l'autenticació en diverses aplicacions, des de la gestió de sessions fins a la protecció de dades confidencials.

Encara que aquesta tecnologia es va desenvolupar inicialment per als serveis de banca en línia, avui dia s'aplica en diversos sectors que cerquen optimitzar les operacions dels usuaris sense posar en risc la seva seguretat digital.

Aquest informe se centra en els **testimonis de sessió** perquè el robatori d'aquesta mena de testimonis pot tenir conseqüències greus, inclosos l'accés no autoritzat a informació confidencial, la manipulació de dades i la realització d'accions malicioses en nom de l'usuari compromès. Per tant, això s'ha convertit en una **amenaça significativa en l'àmbit de la ciberseguretat**, especialment en un entorn on les interaccions digitals són fonamentals per a les empreses i els usuaris.

Per abordar aquest tema, expliquem quin és el rol dels testimonis de sessió en la seguretat digital i quins són els riscos i vulnerabilitats als quals s'enfronten. En aquest sentit, oferim informació rellevant sobre els mètodes emprats pels ciberdelinqüents, com també les estratègies preventives que les organitzacions han d'implementar per minimitzar aquest risc creixent.

Cal destacar que quan un atacant aconsegueix obtenir un testimoni de sessió, pot suplantar la identitat de l'usuari legítim i accedir als seus recursos i dades personals. Aquesta mena d'atac pot succeir fins i tot si s'han implementat mesures d'autenticació multifactor (MFA), perquè el testimoni robat compleix amb els requisits d'autenticació.

Per tant, és crucial que s'entengui com es produeixen aquesta mena d'atacs, les tècniques que fan servir els atacants i les estratègies de mitigació per protegir els sistemes i les dades de les organitzacions.

3. CONCEPTES BÀSICS

Si bé aquest informe se centrarà en els testimonis de sessió, explicarem, en primer lloc, què és un testimoni, com funcionen els testimonis i quin tipus de testimonis existeixen.

3.1. Què és un testimoni (token)?

Un testimoni és un identificador o codi que segons el seu tipus i aplicació, pot autenticar un usuari, atorgar accés a recursos, representar actius digitals o protegir dades mitjançant criptografia. Els testimonis són essencials en la ciberseguretat i en diverses aplicacions digitals, perquè faciliten processos segurs i eficients.

3.2. Com funciona un testimoni?

Tal com hem esmentat, la finalitat del testimoni és ajudar a protegir dades delicades, com ara els números dels comptes bancaris, les targetes de crèdit o dèbit, o un altre tipus d'informació confidencial. Per a això, els testimonis funcionen de la manera següent:

1. **Substitució de dades delicades:** les dades delicades es reemplacen per un testimoni, que és un valor alfanumèric generat aleatòriament. El testimoni no té cap valor fora del sistema específic en el qual es fa servir, cosa que redueix el risc d'exposició de les dades originals.

2. **Emmagatzematge segur:** les dades originals s'emmagatzemen de manera segura en un servidor protegit, conegut com a 'volta de testimonis'. Només el sistema autoritzat pot fer el mapatge del testimoni de tornada a les dades originals quan calgui.

3. **Transmissió segura:** durant les transaccions, només es transmet el testimoni en lloc de les dades delicades. Això ens assegura que, si les dades són interceptades, no se'n pot fer ús sense tenir accés a la 'volta dels testimonis'.

4. **Reducció del risc de frau:** en fer servir els testimonis en lloc de les dades reals, es minimitza el risc de frau i de robatori de la identitat. Igualment, els testimonis es poden configurar per expirar després d'un cert temps o per ser vàlids en contextos específics.

5. **Compliment normatiu:** l'ús dels testimonis ajuda les organitzacions a complir amb les regulacions de protecció de dades, com ara el Reglament general de protecció de dades europeu (GDPR) i l'Estàndard de seguretat de dades del sector de targetes de pagament *(Payment Card Industry Data Security Standard, PCI DSS)*, que exigeixen la protecció d'informació delicada.

En resum, els testimonis proporcionen una capa addicional de seguretat en protegir les dades delicades mitjançant la seva substitució per valors que no tenen valor fora del sistema autoritzat. Això redueix significativament el risc d'exposició i l'ús indegut de la informació confidencial.

3.3. Tipus de testimonis

Hi ha diferents tipus de testimonis. En aquest apartat farem referència als testimonis de sessió, seguretat, accés i signatura. Cadascun té el seu propòsit i avantatges segons el context en el qual es faci servir.

- **Diferències pel que fa a les funcions:** els testimonis de sessió són temporals per mantenir l'autenticació mentre es navega; els de seguretat es fan servir per verificar la identitat en l'autenticació de dos factors (2FA); els d'accés permeten connectar-se a les API; i els de signatura, verifiquen documents.

- **Diferències pel que fa a la forma:** alguns testimonis són digitals (com els de sessió o accés) i d'altres poden ser físics (com els de seguretat o signatura).

- **Diferències pel que fa a durada:** la durada pot ser temporal (sessió o accés) o permanent (signatura electrònica o testimoni físic).

3.3.1 Testimoni de sessió

- **Objectiu:** mantenir l'autenticació d'un usuari mentre interactua amb un sistema, lloc web o aplicació.

- **Funcionament:** es genera després de l'inici de sessió, i permet que l'usuari navegui sense necessitat d'autenticar-se a cada sol·licitud.

- **Emmagatzematge:** usualment a les galetes o a la memòria del dispositiu.

- **Durada:** temporal, s'invalida en tancar la sessió o en expirar el temps de sessió.

3.3.2 Testimoni de seguretat

- **Objectiu:** ser una capa addicional en l'autenticació de dos factors (2FA) o multifactor (MFA) per verificar la identitat de l'usuari.

- **Funcionament:** pot ser un dispositiu físic (una espècie de clauer) o una aplicació que genera codis temporals per completar l'autenticació.

- **Durada:** es renova periòdicament i té una durada limitada, com els codis d'un sol ús (OTP).

3.3.3 Testimoni d'autenticació

- **Objectiu:** assegurar que només els usuaris autoritzats puguin accedir a un sistema.

- **Funcionament:** funciona de manera similar al testimoni de seguretat, però es pot fer servir exclusivament en entorns digitals, i generar un codi i clau única per validar la identitat de l'usuari.

- **Durada:** temporal (expira després d'un temps o quan es fa servir) o permanent (per a una autenticació recurrent).

3.3.4 Testimoni d'accés (OAuth)

- **Objectiu:** atorgar accés a recursos protegits en nom de l'usuari, sense necessitat de revelar credencials.

- **Funcionament:** a l'usuari se li atorga un testimoni d'accés després d'autenticar la seva identitat, que es pot fer servir per interactuar amb una API o servei en nom seu.

- **Durada:** temporal, expira després d'un període definit, però es pot renovar mitjançant un testimoni d'actualització.

3.3.5 Testimoni físic (maquinari)

- **Propòsit:** proporcionar un mètode segur per a l'autenticació de dos factors mitjançant un dispositiu físic.

- **Funcionament:** pot ser un clauer, una targeta intel·ligent o un USB que genera o conté un codi d'accés o clau criptogràfica.

- **Durada**: generalment no té una caducitat limitada, però té com a requisit tenir el dispositiu físic per poder-hi accedir.

3.3.6 Testimoni de signatura electrònica

- **Propòsit:** servir com una clau única per signar digitalment documents, i verificar la identitat del signatari.

- **Funcionament:** general una clau criptogràfica que s'associa amb el document, i n'assegura l'autenticitat i evita alteracions.

- **Durada:** específica per a cada transacció o document.

4. TESTIMONIS DE SESSIÓ

Els testimonis de sessió **són fonamentals per mantenir la seguretat i l'eficiència en aplicacions web i mòbils**, en proporcionar una capa addicional de protecció i millorar l'experiència de l'usuari. Pel que fa a aquest darrer punt, milloren la interacció entre l'usuari i el sistema en eliminar la necessitat d'autenticar-se a cada sol·licitud.

Malgrat els avantatges, els testimonis de sessió poden presentar riscos important si són robats. Els atacants poden fer servir un testimoni compromès per suplantar l'usuari legítim, i accedir a les dades o sistemes delicats de manera no autoritzada.

4.1. Què és un testimoni de sessió?

Un testimoni de sessió **és un valor alfanumèric generat pel servidor quan un usuari iniciar sessió en un lloc web o aplicació**. Aquest testimoni s'emmagatzema en el client (al navegador o l'aplicació) i s'envia amb cada sol·licitud al servidor per mantenir activa la sessió de l'usuari. És a dir, funciona com una 'clau' digital que en verifica la identitat i li atorga l'accés als recursos i funcionalitats específiques del sistema sense necessitat d'ingressar-ne les credencials repetidament. El testimoni de sessió també es pot emmagatzemar en forma de galeta assignada pel servidor, cosa que permet que el sistema recordi l'usuari i mantingui la sessió iniciada.

4.2. Rol que exerceixen els testimonis de sessió a la seguretat web

Els testimonis de sessió juguen un paper crucial per mantenir la seguretat de les aplicacions web i mòbils atès que representen una manera segura i eficient de gestionar l'autenticació d'usuaris. A més a més, en estar signats digitalment, garanteixen que no poden ser manipulats pels atacants. Tot seguit, s'explica com contribueixen a la seguretat:

- **Autenticació segura i continua**: els testimonis de sessió permeten que els usuaris romanguin autenticats durant un període determinat sense que calgui reintroduir les credencials, cosa que disminueix l'exposició de les contrasenyes i redueix el risc d'intercepció. A més, optimitzen l'experiència de l'usuari en eliminar la necessitat de gestionar contrasenyes de manera repetida.

- **Seguretat millorada**: en fer servir testimonis de sessió, les aplicacions poden evitar emmagatzemar contrasenyes a cada sol·licitud. Al seu lloc, el testimoni actua com una credencial temporal que és difícil d'interceptar i reutilitzar pels atacants.

- **Seguretat més gran**: atès que les aplicacions eviten l'emmagatzematge de contrasenyes a cada sol·licitud. D'aquesta manera, el testimoni actua com una credencial temporal, que és difícil d'interceptar i reutilitzar per qualsevol atacant.

- **Prevenció d'atacs:** els testimonis de sessió són eficaços per prevenir atacs com ara el segrest de sessions i el Cross-Site Request Forgery (CSRF). Gràcies al caràcter únic i el temps de vida limitat, redueixen les oportunitats d'explotació per part dels atacants.

- **Escalabilitat i flexibilitat:** en ser autònoms, els testimonis de sessió contenen tota la informació necessària per a l'autenticació. Això permet que els servidors siguin més escalables, atès que no els cal gestionar l'estat de la sessió de l'usuari.

- **Control detallat i transparent**: els testimonis de sessió permeten una gestió precisa de l'accés als recursos perquè inclouen dades sobre els permisos i els rols de l'usuari. Això facilita un control més bo i eficient en la gestió d'accessos.

4.3. Com funciona un testimoni de sessió?

Quan un usuari inicia sessió en un lloc web o aplicació, el sistema genera un testimoni de sessió vinculat al seu compte. Aquest testimoni sol ser una **cadena aleatòria de caràcters generada mitjançant algoritmes criptogràfics** que s'envia al dispositiu de l'usuari i s'emmagatzema, generalment com a una galeta o a la memòria del dispositiu. Aquests algoritmes es fan servir per tal d'assegurar que el testimoni sigui únic i difícil de predir.

A mesura que l'usuari navega o interactua amb l'aplicació, el testimoni de sessió es fa servir per verificar-ne la identitat i els permisos, i evitar que s'hagi d'autenticar contínuament, tal com hem explicat prèviament. El servidor valida el testimoni i accedeix a les dades de la sessió, que poden incloure el nom de l'usuari, les preferències i els drets d'accés.

Quan l'usuari tanca la sessió o la sessió caduca, el testimoni s'invalida i l'accés al compte queda revocat. El temps d'expiració del testimoni varia segons la configuració del lloc o de l'aplicació. En alguns casos, també es pot invalidar si es detecten canvis a l'adreça IP de l'usuari o activitat sospitosa, com a múltiples intents fallits d'inici de sessió.

Tot seguit, s'explica detalladament el procés.

1. **Inici de sessió:** quan un usuari introdueix les seves credencials (nom de l'usuari i contrasenya) en una aplicació, el servidor verifica aquesta informació.

2. **Generació del testimoni:** si les credencials són correctes, el servidor genera un testimoni de sessió únic. Aquest testimoni és un fragment petit de dades que contenen informació sobre la sessió de l'usuari i està signat digitalment per evitar manipulacions.

3. **Enviament del testimoni:** el servidor envia aquest testimoni al client (per exemple, el navegador web o l'aplicació mòbil) i el client l'emmagatzema, generalment a les galetes del navegador o a l'emmagatzematge local.

4. **Autenticació en sol·licituds posteriors:** a cada sol·licitud posterior al servidor, el client inclou el testimoni als encapçalaments de la sol·licitud. El servidor verifica el testimoni per assegurar-se que sigui vàlid i que no ha estat alterat.

5. **Manteniment de la sessió:** mentre el testimoni sigui vàlid, l'usuari no ha de tornar a introduir les seves credencials. El testimoni permet que el servidor identifiqui l'usuari i mantingui la sessió activa.

6. **Expiració del testimoni:** els testimonis de sessió solen tenir un temps de vida limitat per raons de seguretat. Una vegada que el testimoni expira, l'usuari ha de tornar a autenticar-se per obtenir un testimoni nou.

En teoria, aquest procés assegura que les sessions d'usuari siguin segures i que només els usuaris autenticats poden accedir als recursos protegits.

Si bé els testimonis de sessió tenen una vida útil limitada, en realitat poden continuar essent vàlids per períodes més llargs (generalment al voltant de 30 dies) o fins i tot indefinidament mentre es mantingui l'activitat.

4.4. Robatori de testimonis de sessió

Molts servidors web empren algoritmes personalitzats o patrons predefinits per generar identificadors de sessió. No obstant això, com més previsible sigui el testimoni de sessió, més vulnerable serà. Si els atacants aconsegueixen obtenir diversos identificadors i analitzar el seu patró, podrien ser capaços de predir un identificador de sessió vàlid. Aquest mètode es pot comparar amb un atac de força bruta, on s'explota la predictibilitat per comprometre la seguretat del sistema.

Tot seguit s'examinaran els mètodes d'atac que fan servir els ciberdelinqüents, com també les mesures preventives i correctores que les organitzacions han d'implementar per mitigar aquest risc creixent.

4.4.1 Mètodes de robatori de testimonis de sessió

Tal com ja hem esmentat, el **robatori de testimonis de sessió** és una tècnica que fan servir els atacants per segrestar la sessió d'un usuari i obtenir accés no autoritzat als seus comptes o sistemes. Hi ha diversos mètodes que els ciberdelinqüents empren per robar aquest tipus de testimonis:

- **Cross-site scripting (XSS)** (injecció indirecta de scripts): és un tipus de ciberatac web que permet executar codi JavaScript maliciós en el navegador d'una víctima a través d'una aplicació vulnerable. Les vulnerabilitats XSS poden variar, cosa que determina el tipus d'XSS que pugui ser executat.

  En un atac d'XSS, els atacants injecten scripts maliciosos en una pàgina web vulnerable per capturar testimonis de sessió. En trobar una possible vulnerabilitat XSS, un atacant l'ha de posar a prova i executar qualsevol mena de comandament en JavaScript. Un de molt comú és el d'executar una alerta al navegador, cosa que és útil per revisar que la vulnerabilitat existeixi i sigui explotable.

Quan un usuari visita la pàgina compromesa, l'script s'executa al seu navegador i pot capturar el testimoni de sessió emmagatzemat, i tot seguit l'envia a l'atacant. Amb aquest testimoni, l'atacant pot suplantar l'usuari i accedir a les seves dades.

- **Segrest de galetes (*cookie Hijacking*)**: com hem assenyalat prèviament, les galetes sovint es fan servir per emmagatzemar testimonis de sessió. Si un atacant aconsegueix interceptar les galetes d'un usuari, per exemple, mitjançant una connexió no segura (HTTP en lloc d'HTTPS), poden robar el testimoni de sessió i fer-lo servir per accedir al sistema en nom de l'usuari legítim.

- **Man-in-the-Middle (MitM):** en aquesta mena d'atac, un atacant intercepta la comunicació entre l'usuari i el servidor, i captura els testimonis de sessió que es transmeten. Si la comunicació no està xifrada, és a dir, si no es fa servir l'HTTPS, és més fàcil per als atacants dur a terme aquesta mena d'atac.

- **Cross-Site Request Forgery (CSRF):** en un atac de CSRF l'atacant enganya l'usuari per tal que faci una sol·licitud maliciosa des del seu navegador, i fa servir el testimoni de sessió de l'usuari legítim. El servidor, en rebre la sol·licitud des del navegador de l'usuari, assumeix que és legítima i la processa, cosa que permet l'atacant dur a terme accions en nom de l'usuari.

- **Força bruta o atacs predictius:** si els testimonis de sessió es generen mitjançant algoritmes dèbils o predictibles, els atacants poden intentar descobrir patrons en els identificadors de sessió, i llançar un atac de força bruta per generar un testimoni vàlid i accedir al compte de l'usuari.

- **Programari maliciós (*malware*)**: els atacants poden fer servir programari maliciós que infecta el dispositiu de la víctima, i capturar el testimoni de sessió directament des del seu emmagatzematge local, com ara les galetes o la memòria de l'aplicació. Això els permet reutilitzar el testimoni per obtenir accés no autoritzat.

- **Exposició de testimonis als URL:** algunes aplicacions envien testimonis de sessió a través d'URL, cosa que pot provocar que el testimoni quedi exposat en els registres de servidors, els historials de navegació o compartit si es reenvia l'enllaç. Els atacants poden aprofitar aquesta exposició per robar el testimoni.

4.4.2 Conseqüències del robatori de testimonis de sessió

El robatori de testimonis de sessió té un impacte significatiu en la seguretat dels sistemes i les dades dels usuaris. Això no només compromet la privacitat de l'usuari, sinó que també pot provocar l'exposició d'informació confidencial, l'alteració no autoritzada de dades i la realització d'accions malicioses en nom de l'usuari.

Entre les conseqüències, trobem les següents:

- **Suplantació d'identitat:** l'atacant pot accedir al compte d'un usuari sense que li calgui autenticar-se una altra vegada, perquè té el testimoni vàlid. Quan un atacant aconsegueix un testimoni de sessió vàlid, es pot fer passar per l'usuari legítim, i accedir als seus comptes i recursos sense que li calguin credencials addicionals.

- **Escalada de privilegis:** si l'atacant roba un testimoni d'un usuari amb privilegis administratius, pot dur a terme accions destructives o crítiques en el sistema.

- **Pèrdua de dades:** l'atacant podria accedir a dades delicades, modificar informació o fer transferències no autoritzades.

- **Danys reputacionals:** el robatori de testimonis pot comportar que la reputació de les empreses es vegi perjudicada, hi hagi pèrdues financeres i violacions de normatives de protecció de dades, com el GDPR. Per això, comprendre i mitigar aquest risc és essencial per garantir la seguretat dels sistemes i les aplicacions.

4.4.3 Mesures preventives i correctives a implantar

Tal com hem vist al llarg de l'informe, el robatori de testimonis de sessió és una amenaça seriosa per a la seguretat web i requereix una combinació de bones pràctiques per mitigar els seus riscos.

Tot seguit comentarem quines han de ser les mesures preventives i correctives que les organitzacions han d'implementar per prevenir possibles robatoris:

1. **Fer servir l'HTTPS:** s'ha de fer sevir sempre per xifrar el trànsit i que els testimonis no puguin ser capturats a través d'atacs de *sniffing*.

2. **Implementar la bandera HttpOnly a les galetes:** impedeix que JavaScript del costat de l'atacant accedeixi als testimonis.

3. **Regenerar testimonis de sessió:** canviar el testimoni de sessió després d'iniciar sessió o fer operacions delicades.

4. **Implementar seguretat contra les XSS:** censurar correctament els inputs i fer servir capçaleres de seguretat com ara Content-Security-Policy (CSP) per prevenir la injecció de scripts.

5. **Fer servir testimonis de sessió impredictibles:** assegurar-se que els testimonis siguin prou aleatoris i difícils d'endevinar.

6. **Establir una expiració de testimonis:** els testimonis de sessió haurien de tenir una vida útil limitada per minimitzar el temps d'atac per part dels ciberdelinqüents. En resum, reduir la vida útil de les sessions o reduir el temps de viabilitat d'un testimoni fa que la finestra d'actuació dels atacants sigui més curta.

7. **Implementar polítiques d'accés condicional**: amb això s'aplicarà l'MFA en cas d'accés des d'un lloc o un dispositiu no reconegut.

8. **Implementar solucions d'MFA**: aquestes han de ser resistents a la pesca informàtica (*phishing*).

9. **Segregar i segmentar rols i permisos d'usuaris**: fins i tot en diferents identitats per a diferents capacitats administratives.

Les recomanacions abans esmentades no són infal·libles de manera individual però sí que ajuden a fer més difícil l'accés als possibles atacants.

Igualment, la detecció també és molt important per resoldre possibles casos de frau que es puguin fer revisant els esdeveniments d'autenticació i les activitats sospitoses implicades. Per poder dur a terme aquesta detecció se solen monitorar els esdeveniments del sistema d'autenticació i les aplicacions relacionades, i en base a diferents regles (per exemple, correlació, comportament, entre d'altres) poder identificar situacions de risc. Aquests serien alguns dels punts rellevants a tenir en compte:

1. Correus amb fitxers o enllaços maliciosos que s'hagin identificat després del seu lliurament a l'usuari.

2. Manipulacions sospitoses a les bústies de correu (permisos delegats, redireccions, etc.).

3. Viatges impossibles: un usuari no pot iniciar sessió des d'Andorra i al cap de mitja hora fer-ho des de Nova Zelanda.

4. Activitat duta a terme des d'un país on no hi sol haver activitat.

5. Testimoni amb característiques anòmales.

6. Propietats d'inici de sessió anòmales.

5. CONCLUSIONS

El robatori de testimonis de sessió representa una amenaça greu per a la seguretat web i la protecció dels usuaris. A través del robatori de testimonis de sessió, els ciberdelinqüents poden obtenir accés no autoritzat a comptes i sistemes, i posar en risc informació confidencial i alhora exposar tant individus com organitzacions a conseqüències diverses, com ara pèrdues econòmiques, violació de normatives de privacitat i dany reputacional.

Si bé és cert que els testimonis de sessió permeten una experiència d'usuari fluida en evitar l'autenticació repetida, també els converteix en un objectiu atractiu per als ciberdelinqüents. Per a això, és fonamental implementar mesures de seguretat robustes, com ara el xifratge de les comunicacions, la protecció contra atacs d'XSS i CSRF, i l'ús de testimonis amb temps d'expiració curts. A més, les organitzacions han d'adoptar pràctiques com l'autenticació multifactor (MFA) i la utilització de galetes segures per minimitzar el risc de robatori.

La seguretat en la gestió dels testimonis de sessió és essencial per protegir els usuaris i mantenir la integritat dels sistemes. La prevenció i detecció precoç d'atacs relacionats amb el robatori de testimonis és clau per mitigar aquesta amenaça creixent a l'entorn digital actual.

6. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.