SECURITY AUDIT REPORT

Evaluation of Authentication and Session Cookie Management in Web Applications

Author: **Luis Aparicio**

Role: **QA Tester - Security Testing**

Date: **December 2025**

Abstract

This report documents the results of a technical assessment focused on analyzing authentication and session management mechanisms across various web platforms. The study centered on identifying potential weaknesses related to password policies, account recovery processes, session persistence, and the handling of authentication cookies.

During the analysis, registration, activation, and password recovery flows were reviewed, as well as the behavior of session cookies generated by the evaluated systems. The reliance on tokens stored in the browser as the primary identity validation mechanism was also examined.

While no critical vulnerabilities immediately exploitable were identified, implementing best practices aligned with OWASP standards would significantly strengthen the security posture and reduce the attack surface in scenarios involving session hijacking or credential compromise.

Overall, the identified risk level can be classified as moderate, primarily dependent on the correct configuration and management of the session lifecycle.

Scope of Analysis

The evaluation was conducted using a non-intrusive, client-side assessment approach, employing web browser developer tools (Google Chrome and Mozilla Firefox) in controlled environments.

The scope included:

- Review of the registration and account creation process.
- Analysis of the email activation flow.
- Evaluation of the password recovery mechanism.
- Inspection of cookie and session token storage.
- Observation of active session behavior and session invalidation upon closure.
- Analysis of security attributes associated with cookies (Secure, HttpOnly, SameSite).
- Exploratory evaluation of session persistence and identifier reuse.

The analysis was limited to client-side observable behavior, reflecting exclusively technical observations derived from system behavior during controlled test sessions.

Introduction

This report documents the results of a technical audit aimed at evaluating the authentication and session management mechanisms on various publicly accessible web platforms. The main objective of the analysis was to identify potential weaknesses in the processes of registration, password recovery, session persistence, and the handling of authentication cookies.

The evaluation was carried out through controlled manual testing using developer tools in web browsers (Google Chrome and Firefox), under a non-intrusive exploratory analysis approach. The scope included a review of the Single Sign-On (SSO) authentication flow, password policy validation, account recovery on the elpais.com.uy website, and analysis of the session cookie lifecycle on the capacitacion.ces.com.uy and rappi.com.uy platforms.

The study was conducted using industry best practices and guidelines established in standards such as OWASP, with particular attention to risks related to authentication failures, session hijacking, and credential exposure.

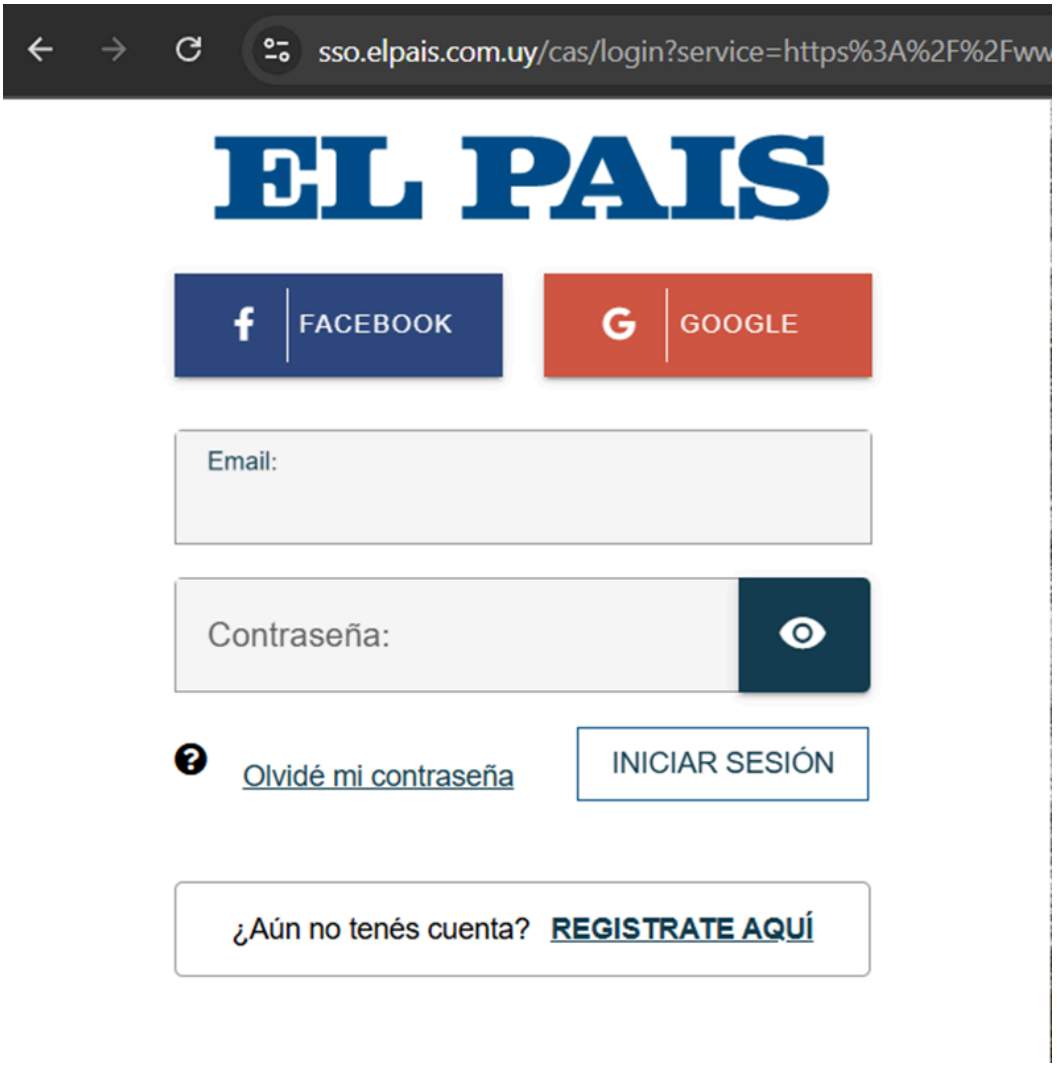
Authentication System

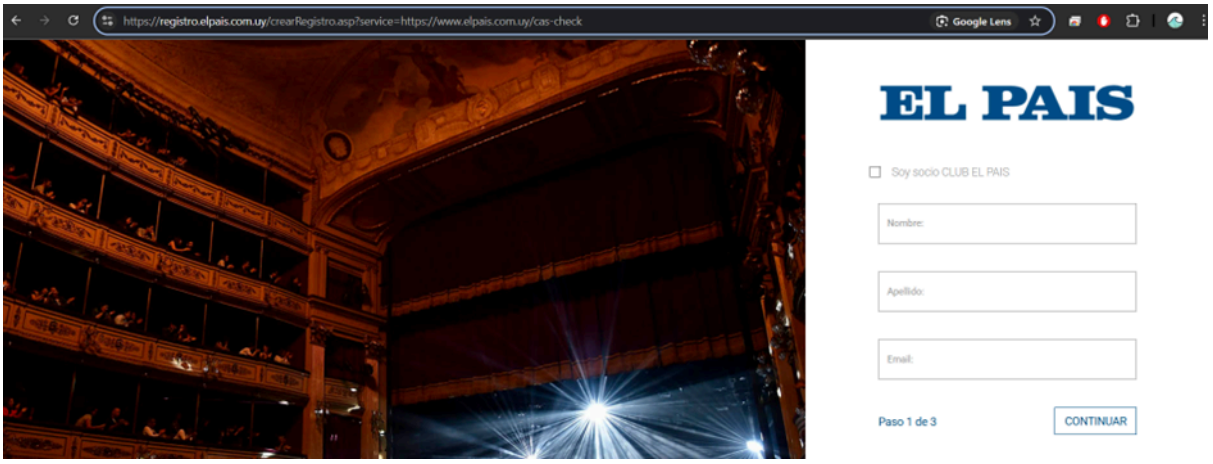
During the audit of elpais.com.uy's authentication system, the implementation of a centralized Single Sign-On (SSO) mechanism was identified. This model allows users to access multiple services associated with the domain using a single set of credentials.

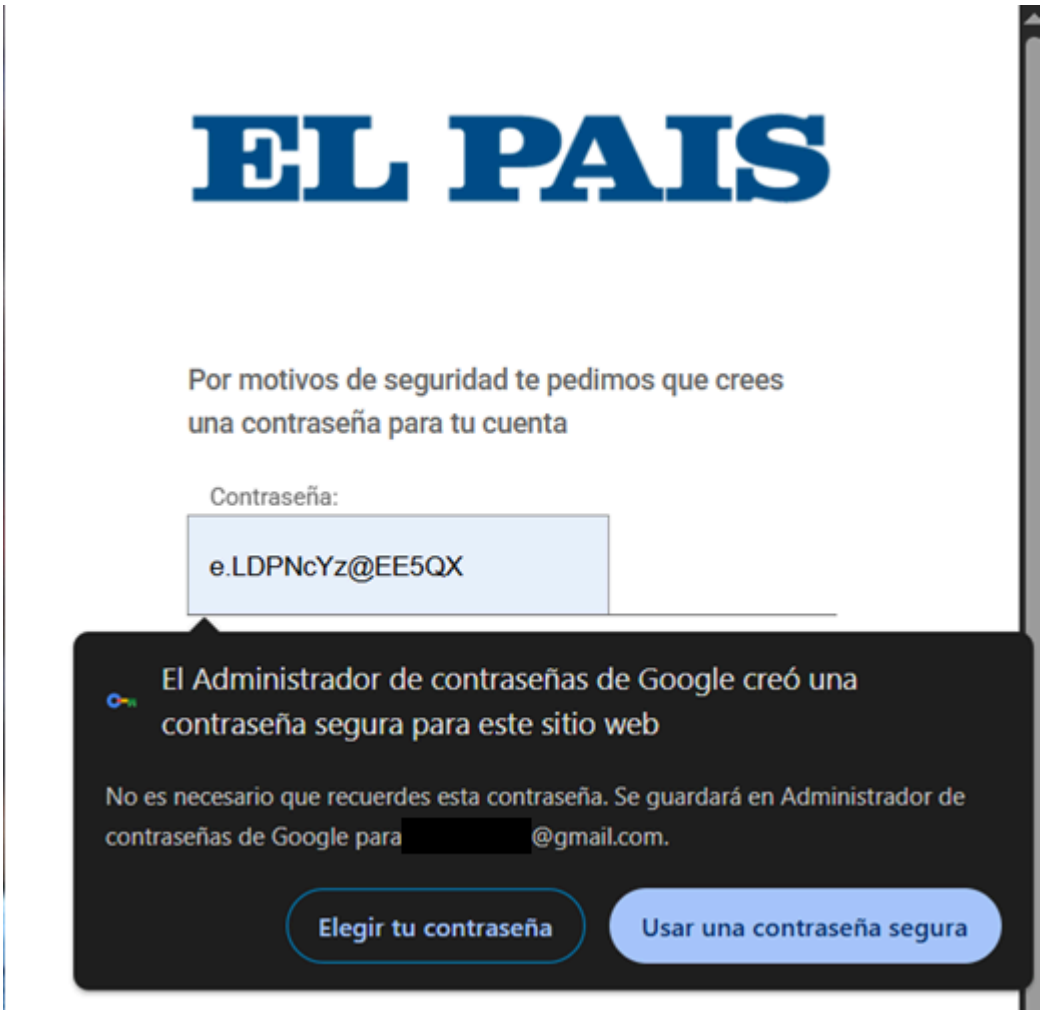
The system includes traditional authentication via email and password, as well as external providers such as Google and Facebook, with interaction between the identity provider and service providers.

The registration process requests first name, last name, and email address, followed by password creation. Subsequently, additional data such as phone number and date of birth are requested.

During password creation, the browser suggests strong passwords using Google's password manager; however, the system does not visibly display the minimum security requirements (length, complexity, specific restrictions) nor does it explicitly validate against databases of compromised passwords.




https://registro.elpais.com.uy/crearRegistro.asp?service=https://www.elpais.com.uy/cas-check
Google Lens
EL PAIS
Soy socio CLUB EL PAIS
Nombre:
Apellido:
Email:
Paso 1 de 3
CONTINUAR


EL PAIS
Por motivos de seguridad te pedimos que crees una contraseña para tu cuenta
Contraseña:
e.LDPNcYz@EE5QX
El Administrador de contraseñas de Google creó una contraseña segura para este sitio web
No es necesario que recuerdes esta contraseña. Se guardará en Administrador de contraseñas de Google para [redacted]@gmail.com.
Elegir tu contraseña
Usar una contraseña segura


EL PAIS
Teléfono celular:
Tu fecha de nacimiento:
5
5
Año
Hombre
Mujer
Paso 3 de 3
Volver
FINALIZAR


¿Quieres guardar la contraseña?
Nombre de usuario
[redacted]@gm
Contraseña
Guardar
Nunca
Puedes usar las contraseñas guardadas en cualquier dispositivo. Se guardan en Administrador de contraseñas de Google para [redacted]@gmail.com.
AIS
ólo falta un
e enviamos a tu

Account Activation Process

Once registration is complete, the system sends a confirmation email. The link received redirects to the main portal instead of explicitly directing you to an authentication screen or technical confirmation of your account status.

While the process functionally fulfills the activation, the direct redirection to the main page can create ambiguity regarding the actual status of the session and the verification process.

Password Recovery Flow Evaluation

During the analysis of the "Forgot your password" flow, it was observed that the system sends a self-generated password directly to the registered user's email address, with an estimated delivery time of approximately 80 seconds.

This practice presents significant weaknesses, as the new password is stored in plain text within the email, posing a risk if the user's mailbox is compromised. The system does not exclusively use a one-time, time-limited password, which could increase the vulnerability of the credentials.

From a modern security perspective, sending credentials directly via email is not considered a best practice.

Olvidé mi contraseña

Ingresá el correo con el cual te registraste y te enviaremos una nueva clave autogenerada, luego podrás cambiarla en tu perfil por una que vos prefieras.

[redacted]@gmail.com

Se han enviado su **Usuario** y **Contraseña** a la casilla de correo ingresada.

ENVIARME NUEVA CONTRASEÑA

EL PAIS

Hola Luis.

Hemos recibido una solicitud para restablecer tu contraseña de El País. Ingresa con la siguiente contraseña autogenerada y luego podrás cambiarla en tu perfil.

Usuario: [redacted]@gmail.com

Contraseña: FC5IB6FM

Identified Risks

Poorly Visible Password Policy:

- The system does not clearly communicate the minimum required criteria. This can facilitate the use of weak or reused passwords.
- Absence of Multi-Factor Authentication (2FA):
    - The implementation of a second authentication factor was not identified, which increases the risk of account hijacking in the event of a breach or reuse of credentials.
- Possible User Enumeration:
    - Differentiated messages in the recovery process could allow inferences to be made about whether an email address is registered.
- Persistent Session Management:
    - The "remember me" option was identified, suggesting persistent sessions. It could not be explicitly validated whether these are automatically invalidated after a password change, which could represent an additional risk.
- Direct Password Delivery via Email:
    - This represents a significant weakness compared to current security standards.

The evaluated authentication system has a suitable functional architecture based on SSO; However, weaknesses were identified in password recovery practices and in the disclosure of security policies to end users.

The lack of multi-factor authentication and the sending of self-generated passwords via email represent the main risk points detected.

While no critical vulnerabilities for direct exploitation were identified during the analysis, implementing modern measures aligned with OWASP standards would significantly strengthen system security and reduce the likelihood of account compromise.

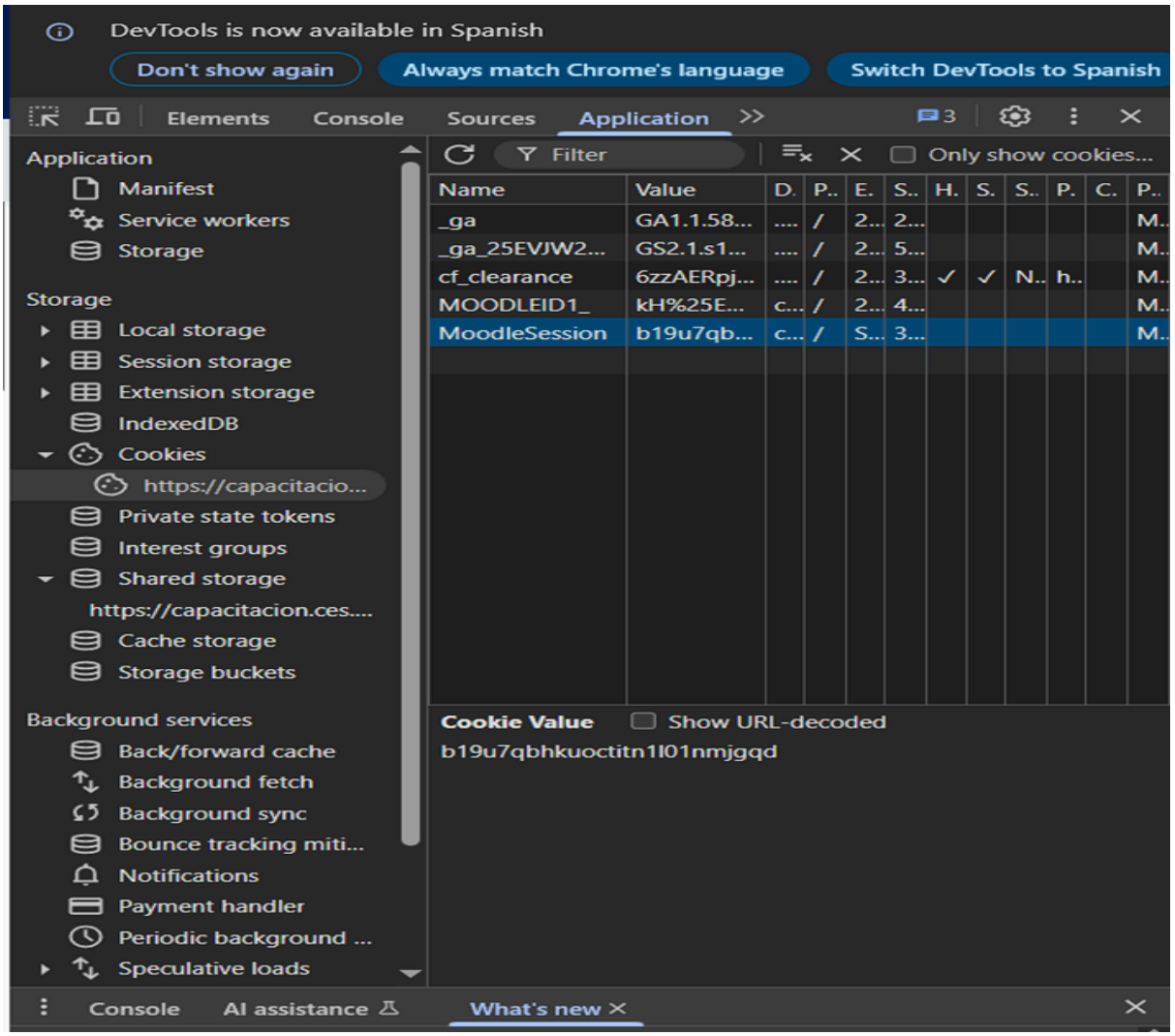
Cookie and Session Management

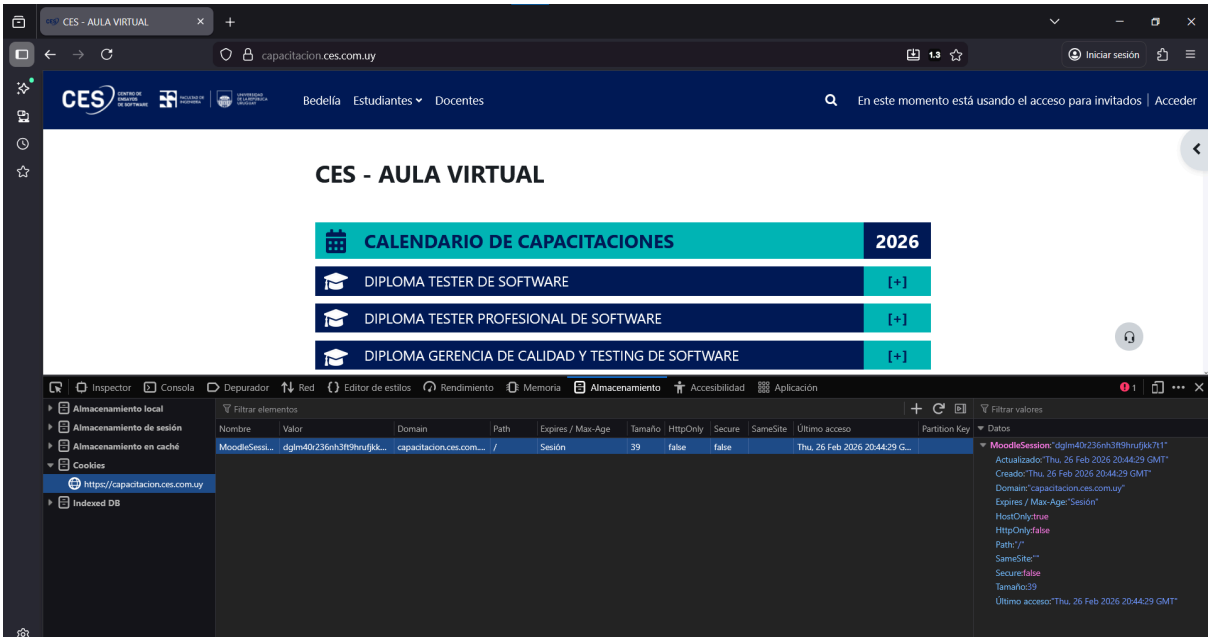
In this second phase of the audit, the session management mechanism was evaluated on various web platforms, such as capacitacion.ces.com.uy and rappi.com.uy, focusing on session cookie generation, authentication persistence, token reuse, and user-side dependency for identity validation. This analysis was performed by inspecting the browser storage of Google Chrome and Firefox (Devtools) during controlled browsing sessions.

During the evaluation of the capacitacion.ces.com.uy session management system, the cookie named “MoodleSession,” automatically generated upon accessing the site, was identified. It was observed that the session cookie is created even before authentication; upon logging in with valid credentials, the cookie's value is updated and associated with the user's session value.

In controlled tests, it was verified that, while the session remained active, the cookie's value represented the only element necessary to maintain user authentication.

Likewise, when logging out of the main browser, the system correctly invalidated the session, causing access to expire in other active contexts.



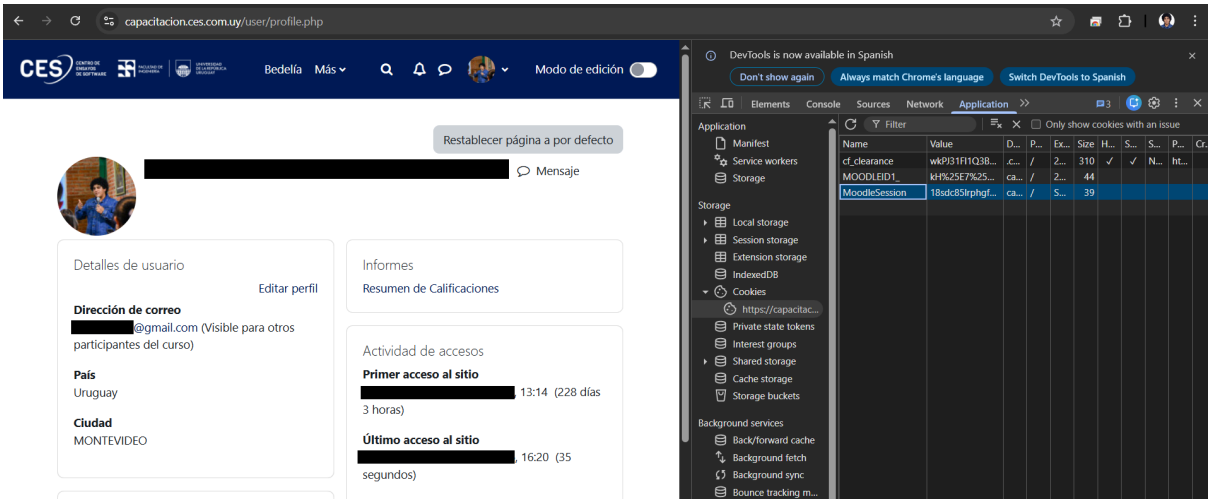


Risk Analysis

The observed behavior indicates that the system relies heavily on the session cookie to validate user identity. This model is standard in many web applications; however, without additional controls, it can pose risks in scenarios such as:

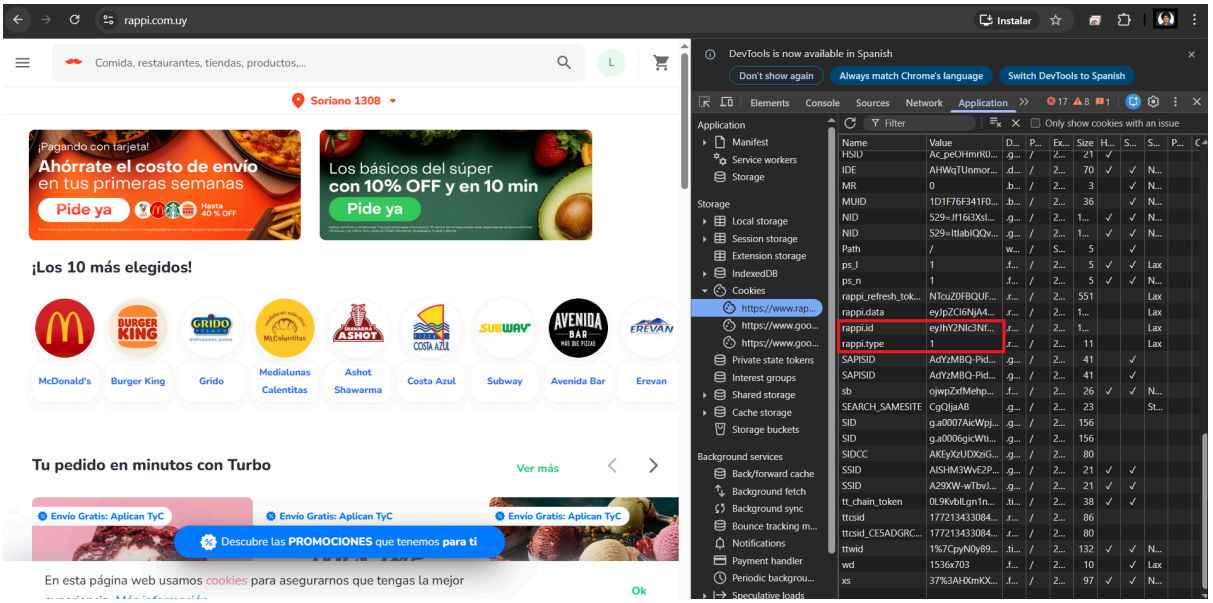
- Exposure of cookies in shared environments.
- Interception via Man-in-the-Middle attacks (if a strict secure transport configuration is not in place).
- Session hijacking via physical access or malware on the user's device.

Reusing the session identifier while it remains active can facilitate a session hijacking scenario if its value is compromised, with a potentially high impact and significant risk to session management.



During the exploratory analysis of the rappi.com.uy platform, similar patterns were observed in session management, such as the presence of cookies associated with user identification, authentication tokens stored in the browser, session persistence after prolonged browsing, and cookies identifiable by developer tools such as rapi.id and rapi.type.

No critical flaws requiring immediate invalidation were identified; however, the observed architecture suggests a strong reliance on client-side tokens for continuous session validation.



Technical Analysis

In modern architectures based on JWT or signed session cookies, authentication commonly relies on a valid token stored in the browser. The risk lies not in the existence of the token itself, but in the configuration of security attributes (Secure, SameSite), the absence of session rotation, and the lack of validation for critical account changes.

If an attacker gains access to the token's value by compromising the user's environment, they could potentially use it while it remains valid. Therefore, it is recommended to implement ID rotation after authentication, strict configuration of the aforementioned cookies (HttpOnly, SameSite=Strict), a short expiration period with secure token refresh, and monitoring of concurrent sessions.

Comparative Table of Detected Vulnerabilities

ID	Platform	Vulnerability	Affected Mechanism	Potential Impact	Risk
SB-001	rappi.com.uy	Reuse of session cookies	Cookies `rappi.id` `rappi.type`	Unauthorized access to user account	High
SB-002	capacitacion.ces.com.uy	Reuse of session cookies	Cookie `MoodleSession`	Unauthorized access to academic profile	High

Comparative Analysis

The identified vulnerabilities share similar characteristics in that they rely exclusively on the identifier stored in the browser, allowing the cookie value to be reused while the session remains active. However, the impact varies depending on the platform. In the case of rappi.com.uy, the potential risk includes exposure of personal information and the execution of actions with financial repercussions. In the case of capacitacion.ces.com.uy, the impact is concentrated on the exposure of academic information and personal data. Nevertheless, both vulnerabilities are classified as Session Management weaknesses according to OWASP guidelines.

Conclusion

The audit identified that the analyzed platforms have a functional architecture aligned with modern authentication models based on SSO and validation using tokens or session cookies. However, significant opportunities for improvement were detected in security, particularly in password recovery processes, visibility of complexity policies, implementation of multi-factor authentication, and advanced session management.

In the case of the evaluated authentication system, the sending of auto-generated passwords via email and the absence of a second authentication factor represent the main points of risk. Likewise, in the platforms where session management was analyzed, a strong dependence on the session identifier stored in the browser as the primary validation mechanism was observed.

While this model is widely used in modern web applications, its security depends strictly on the correct configuration of cookie attributes, session rotation, timely invalidation in the event of critical events, and the implementation of complementary controls.

No critical vulnerabilities immediately exploitable were identified. However, adopting practices aligned with OWASP standards and secure session management guidelines would significantly reduce the attack surface and strengthen protection against session hijacking or account compromise scenarios.