Auxiliar 2:
Pérdidas de control de acceso

Prof. Auxiliar: Natalia Quinteros

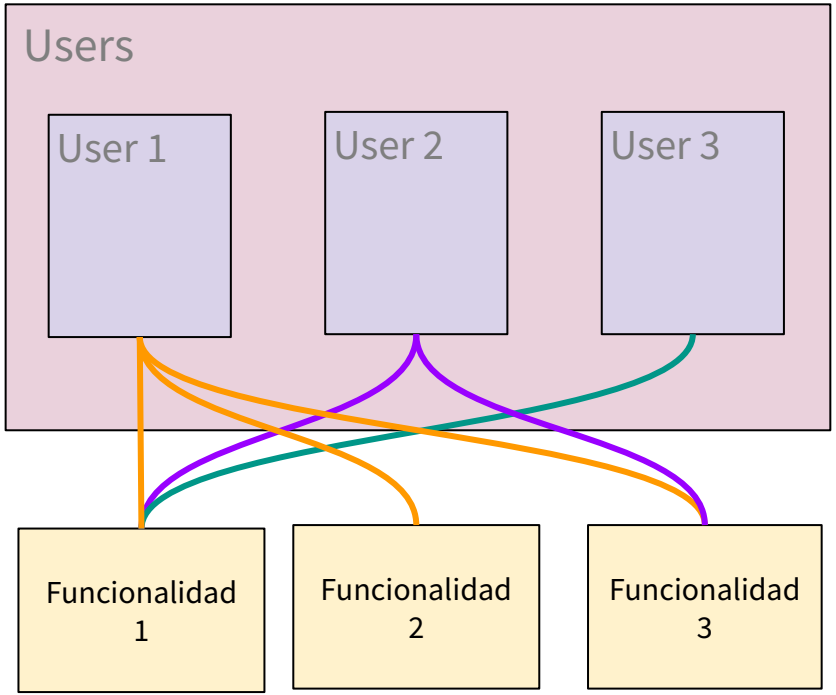
Otoño 2024

dcc CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE CHILE

Contenidos

- Controles de acceso
- Broken access control
- Principio del privilegio mínimo (PoLP)
- Insecure Direct Object Reference (IDOR)
- Forced Browsing

Control de acceso



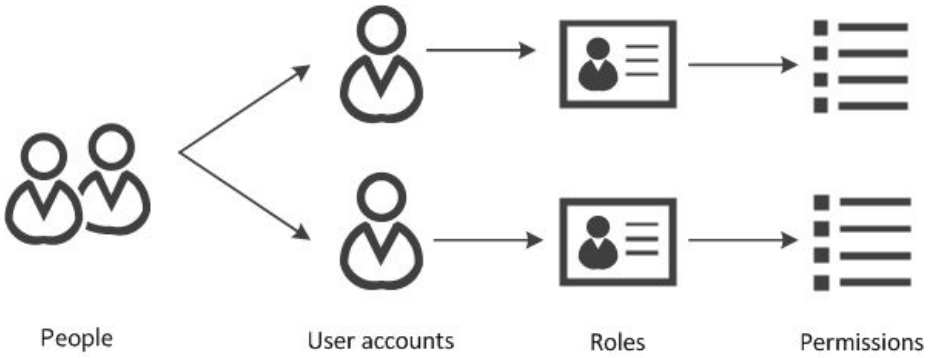
- Manera de administrar la forma en la que los usuarios acceden a un sistema, mediante autenticación y gestión de permisos

Broken access control

- Ocurre cuando un usuario puede acceder a una sección o funcionalidad, a la que no debiese poder acceder.

- Debido al poder que otorga esta vulnerabilidad, resulta uno de los principales focos de los atacantes.

Principio del privilegio mínimo



- Se concentra en asignar los permisos estrictamente necesarios a cada usuario
- En caso de no seguir PoLP nos arriesgamos a:
  - Manejo indeseado de información
  - Movimientos laterales (escalamiento de privilegios)

Fuente imagen: cert.govt.nz
https://www.cert.govt.nz/it-specialists/critical-controls/principle-of-least-privilege/

Insecure Direct Object Reference (IDOR)

- Vulnerabilidad que se presenta solo cuando hay ausencia de control de acceso.

- Ocurre al acceder a objetos mediante identificadores únicos. (por ejemplo, obtener información de otro usuario solo haciendo una modificación del id que se encuentra en una URL)

Forced Browsing

- Muchas páginas solo entregan la url una vez que el usuario ha pasado algunas páginas de verificaciones. Qué sucede si de alguna forma obtenemos esa url?

- Formas de encontrarla:
  - Realizando enumeración con una sesión de usuario:
    `dirsearch -u 'http://localhost/' --cookie 'SESSION=cookie'`
  - Revisando referencias de los archivos JS del sitio web.

P1

Link al problema:

https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter

P2

Link al problema:

https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references

P3

Link al problema:

https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality-with-unpredictable-url

P4

Link al problema:

https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile