Aplicaciones Web III

CC5325 - Taller de Hacking Competitivo
Diego Vargas

Contenido

- Pérdida de control de acceso
  - Principio del privilegio mínimo
  - IDOR
  - Forced browsing
- Demo

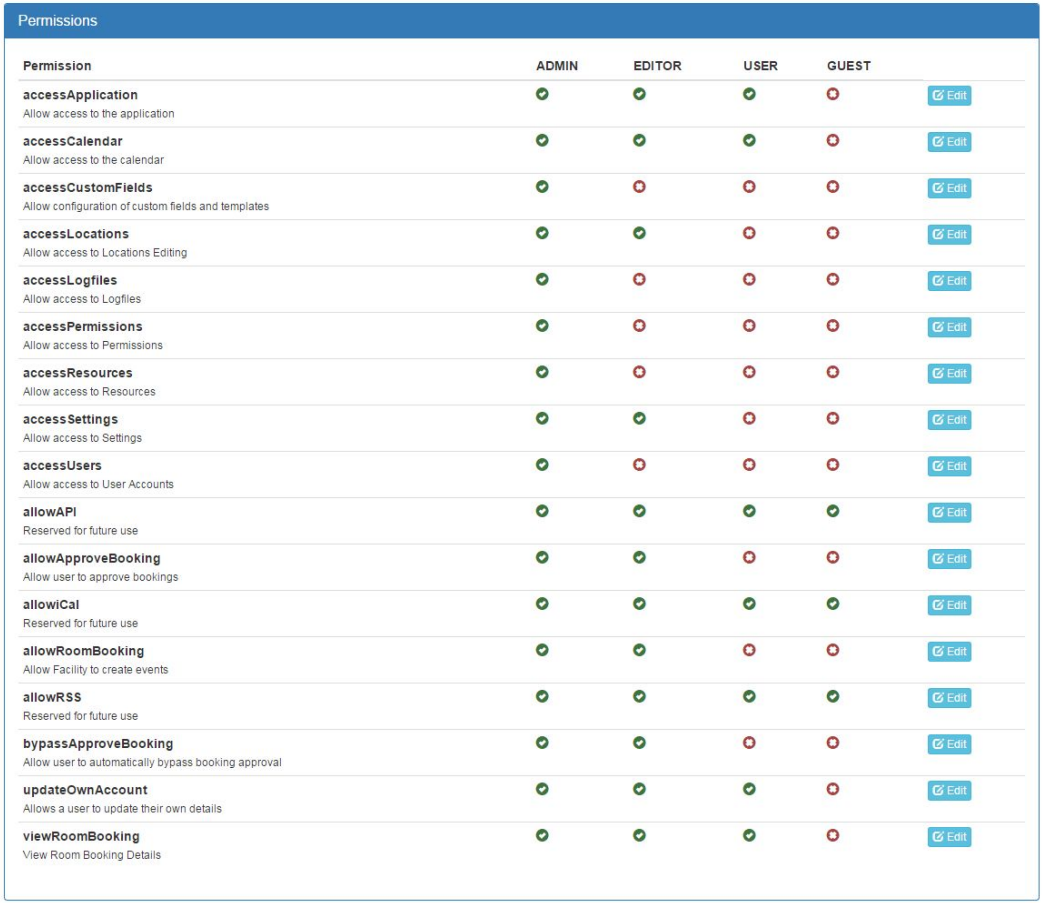
Pérdida de control de acceso

Principio del privilegio mínimo

Principio del Privilegio Mínimo (PoLP)

Objetivo:

- Permisos estrictamente necesarios.
- Prevenir accesos no autorizados.
- Limitar alcance de ataques.



Permissions

Permission	ADMIN	EDITOR	USER	GUEST	
accessApplication Allow access to the application	✓	✓	✓	✗	Edit
accessCalendar Allow access to the calendar	✓	✓	✓	✗	Edit
accessCustomFields Allow configuration of custom fields and templates	✓	✗	✗	✗	Edit
accessLocations Allow access to Locations Editing	✓	✓	✗	✗	Edit
accessLogfiles Allow access to Logfiles	✓	✗	✗	✗	Edit
accessPermissions Allow access to Permissions	✓	✗	✗	✗	Edit
accessResources Allow access to Resources	✓	✗	✗	✗	Edit
accessSettings Allow access to Settings	✓	✓	✗	✗	Edit
accessUsers Allow access to User Accounts	✓	✗	✗	✗	Edit
allowAPI Reserved for future use	✓	✓	✓	✓	Edit
allowApproveBooking Allow user to approve bookings	✓	✓	✗	✗	Edit
allowiCal Reserved for future use	✓	✓	✓	✓	Edit
allowRoomBooking Allow Facility to create events	✓	✓	✗	✗	Edit
allowRSS Reserved for future use	✓	✓	✓	✓	Edit
bypassApproveBooking Allow user to automatically bypass booking approval	✓	✓	✗	✗	Edit
updateOwnAccount Allows a user to update their own details	✓	✓	✓	✗	Edit
viewRoomBooking View Room Booking Details	✓	✓	✓	✗	Edit

Access Control List (ACL)

Causas de falla en el PoLP

- Mal diseño del ACL
- Permisos demasiado amplios
- Falta de revocación de permisos

Cómo probar fallas en el PoLP

- Conocer privilegios esperados
- Conocer funcionalidades del sistema
- Acceder a funcionalidades no permitidas

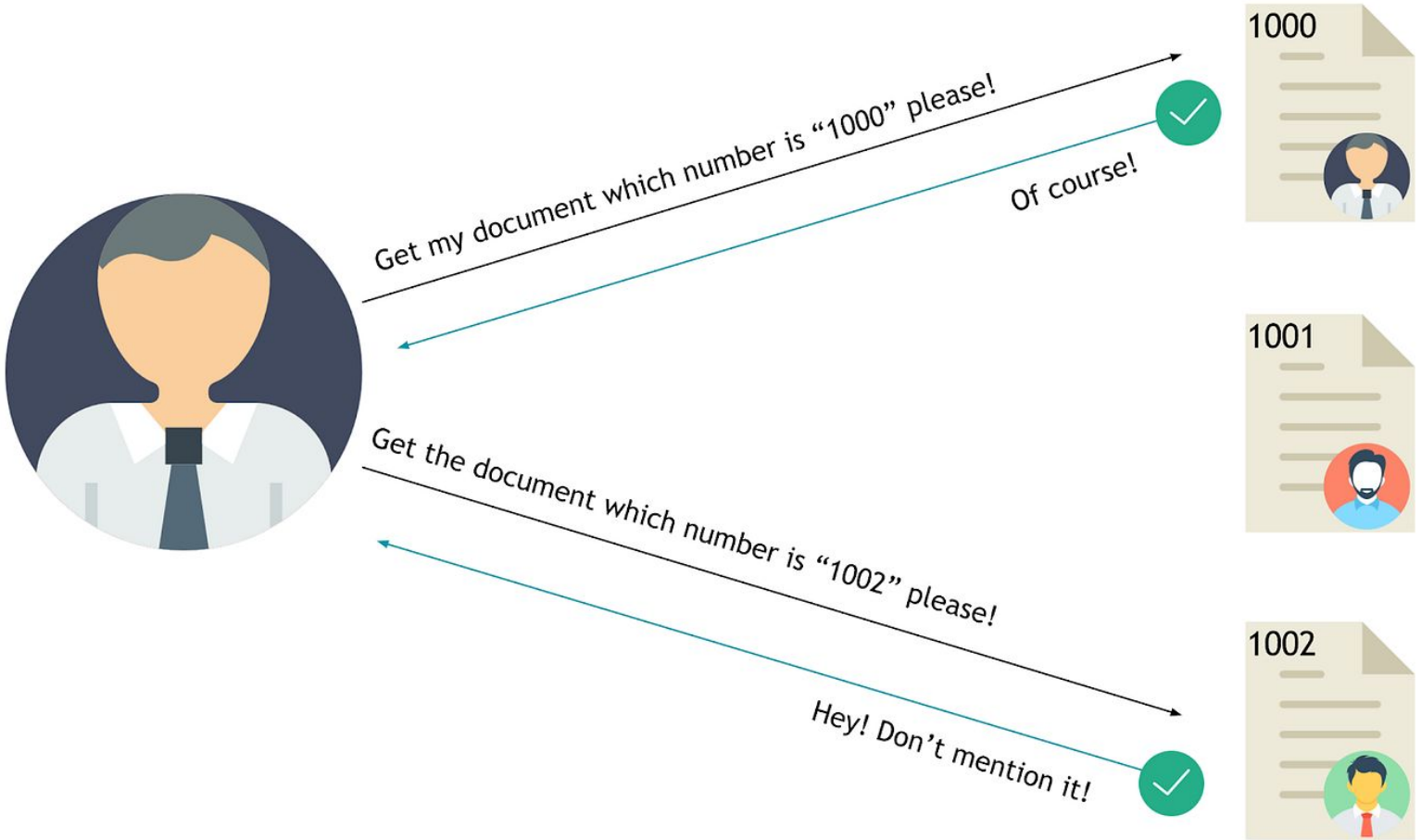
Pérdida de control de acceso

Insecure Direct Object Reference

Insecure Direct Object Reference (IDOR)

Descripción:

- Acceso directo a objetos por medio de su ID.
- Posible alcance:
    - Lectura de datos
    - Modificación de datos
    - Creación de datos
    - Destrucción de datos


Get my document which number is “1000” please!
Of course!
Get the document which number is “1002” please!
Hey! Don’t mention it!
1000
1001
1002

- /api/v1/document?id=1000
- /profile?username=cc5325
- /data/12345678-5
- /cart
  {“cartId”:10}

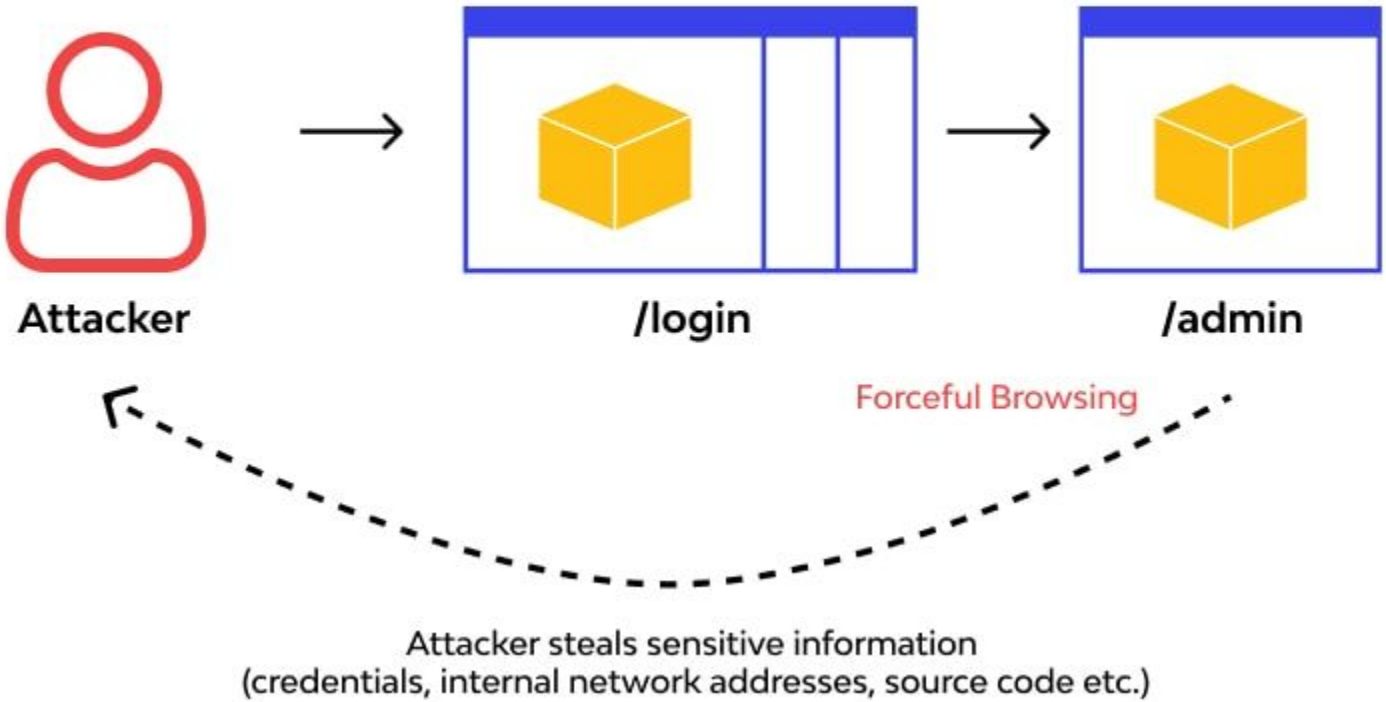
Pérdida de control de acceso

Forced Browsing

Forced Browsing

Descripción:

- Acceso directo a una URL restringida.
- Control de acceso implementado en frontend.
- Ejemplos:
    - /admin
    - /private
    - /system
    - /logs


Website / App Directory
Attacker
/login
/admin
Forceful Browsing
Attacker steals sensitive information
(credentials, internal network addresses, source code etc.)

Cómo encontrar Forced Browsing

- Tratar de acceder a endpoints comunes
- Enumerar accesos
- Saltarse pasos en flujos del sistema
- Revisar JS, HTML y comentarios

Demo

Herramientas

- Burp
- Dirsearch (https://github.com/maurosoria/dirsearch)