

TAREA 4 – TEST DE PENETRACION

JHON SEBASTIAN ZUÑIGA LOPEZ

TUTOR SERGIO LUIS LUDO ARGUMEDO

GRUPO 55

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA  
INGENIERIA EN SISTEMAS  
Argelia – Cauca  
febrero 2022

## **Objetivo**

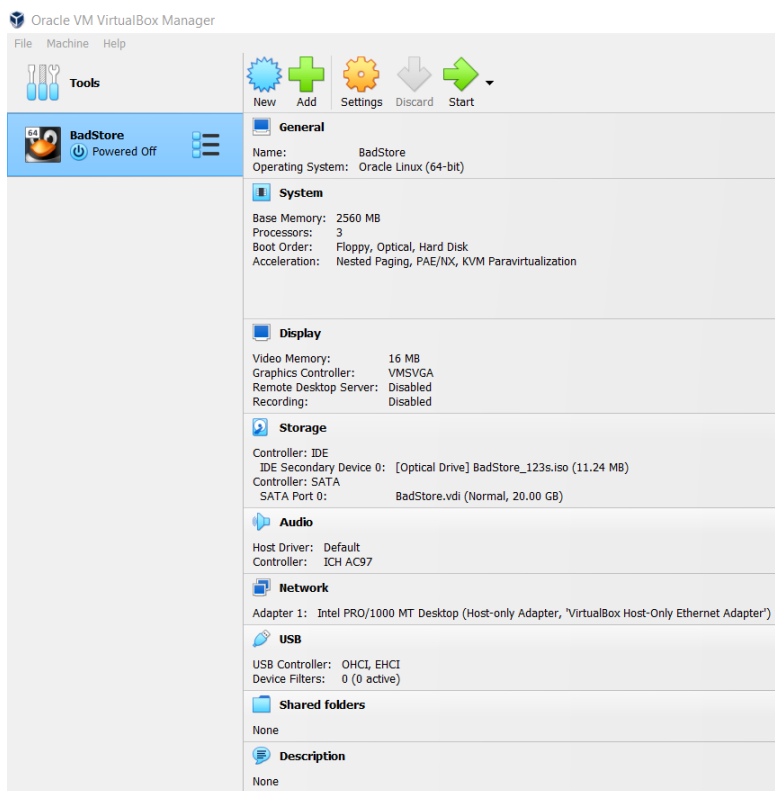
El objetivo es realizar un exhaustivo análisis de seguridad en la aplicación web alojada en la máquina virtual "badstore", utilizando la herramienta de prueba de penetración OWASP ZAP. Este análisis buscará identificar y evaluar posibles vulnerabilidades de seguridad, incluyendo, inyecciones SQL, vulnerabilidades XSS y otras amenazas comunes. A través de este proceso, se pretende mejorar la resistencia y la integridad de la aplicación web al identificar y corregir posibles brechas de seguridad, garantizando así un entorno en línea más seguro y confiable para los usuarios finales.

**Link de la presentación:** [https://www.canva.com/design/DAGFCz7o1LA/wGTI9-IP8lhjMPfuUDmFUg/edit?utm\\_content=DAGFCz7o1LA&utm\\_campaign=designshare&utm\\_medium=link2&utm\\_source=sharebutton](https://www.canva.com/design/DAGFCz7o1LA/wGTI9-IP8lhjMPfuUDmFUg/edit?utm_content=DAGFCz7o1LA&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton)

## Procedimiento de prueba

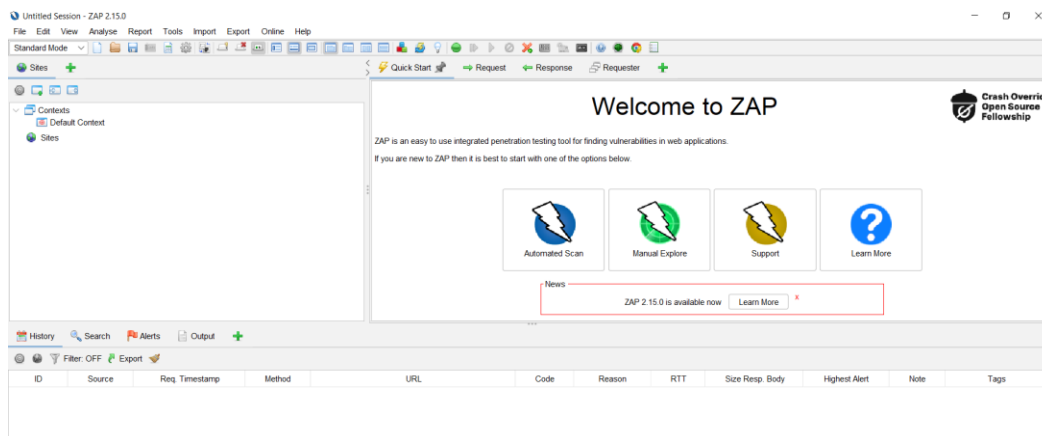
### configuración de la máquina virtual

Una vez descargada la imagen ISO de la badStore se procede a crear la máquina virtual especificando cantidad de memoria RAM, capacidad de disco entre otras cosas.



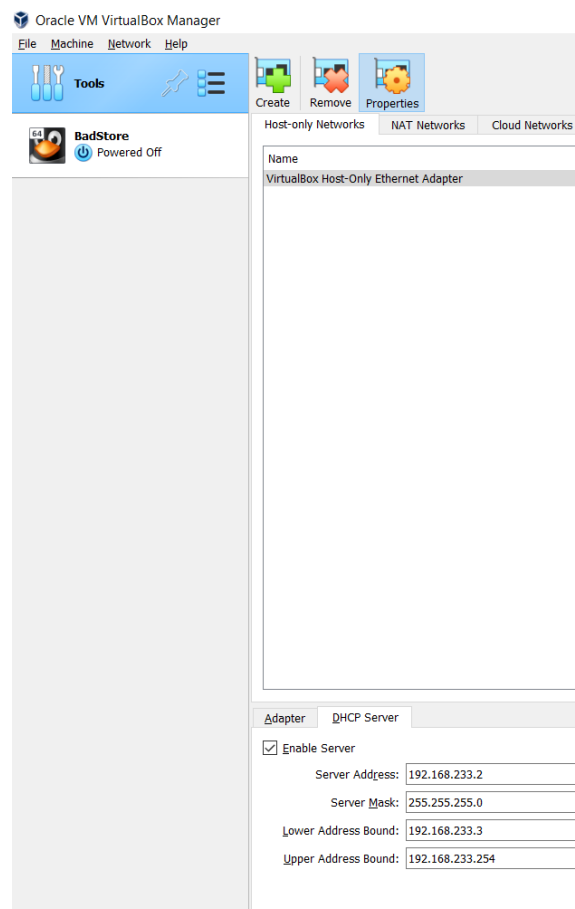
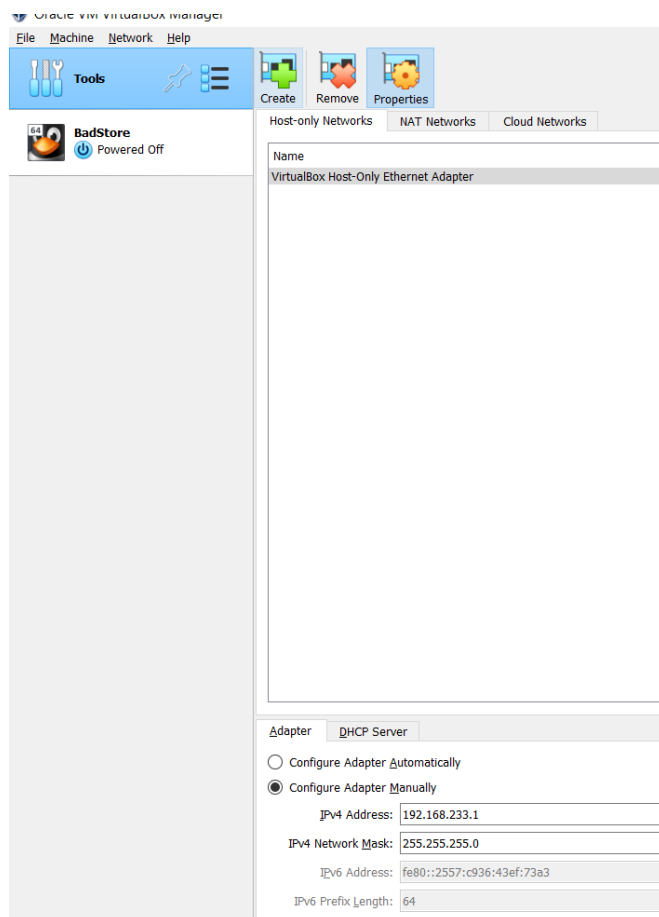
### Instalación de la herramienta OWASP ZAP.

Después de descargar la aplicación se procede a realizar la instalación. La instalación se realiza mediante el sistema de instalación de Windows lo que hace que sea sencilla. Una vez terminada la instalación se obtiene la interfaz del aplicativo.

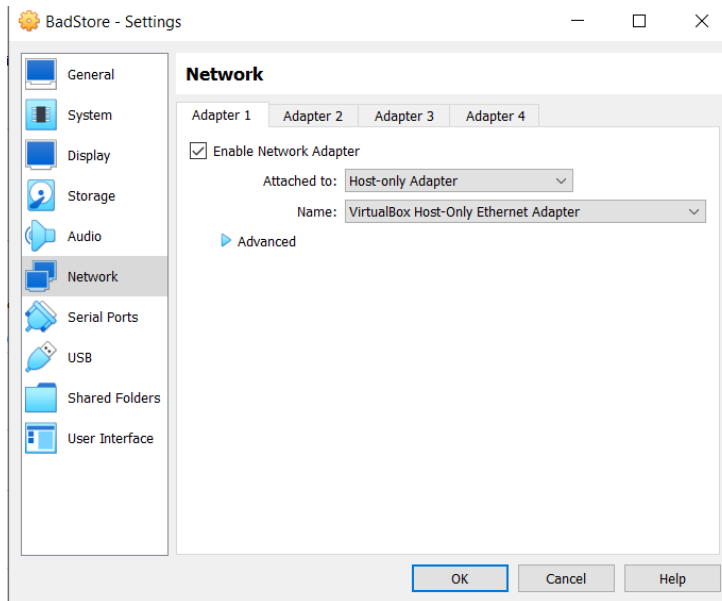


## Configuración de la maquina badstore.

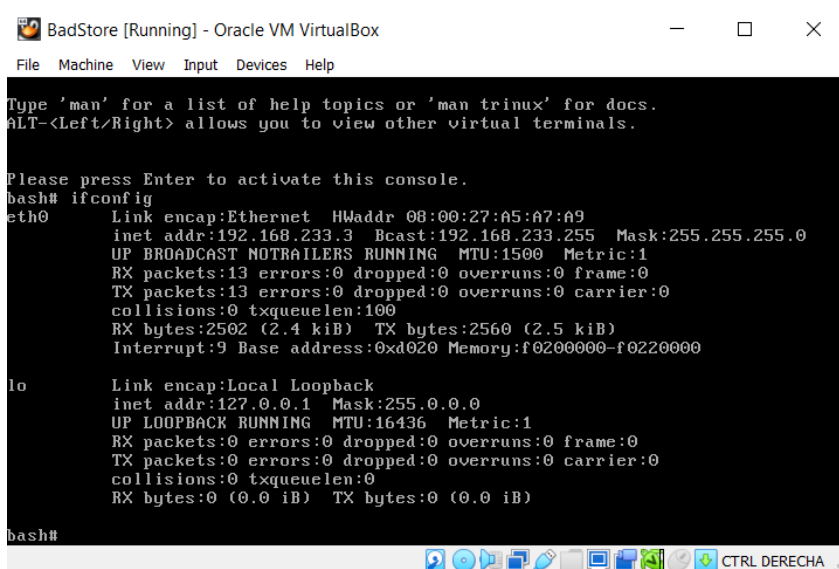
A continuación, se configura la red virtual teniendo en cuenta la dirección IP de la máquina virtual creada anteriormente. Se configura el adaptador y el servidor DHCP.



En las configuraciones de red se debe asegurar que este seleccionada la opción Host-only adapter.



Para obtener la dirección IP de la maquina se inicializa la misma y en consola se ejecuta el comando **ifconfig**.



## Configuración del proxy en el navegador

Para poder acceder a el badstore mediante un nombre de dominio y no directamente desde una IP se agrega la dirección IP de la máquina virtual a un archivo llamado **hosts** que se encuentra en la dirección C:\Windows\System32\drivers\etc\hosts

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
# Added by Docker Desktop
10.10.15.222 host.docker.internal
10.10.15.222 gateway.docker.internal
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
192.168.233.3 www.badstore.net
# End of section
```

## Ataque 1 – Spider

Untitled Session - ZAP 2.15.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites

DoingBusiness  
GET:DoingBusiness  
GET:Procedures  
Procedures  
GET:UploadProc.html  
GET:UploadProc\_files  
UploadProc\_files

Quick Start

## Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

History Search Alerts Output Spider Active Scan

New Scan Progress: 2: http://www.badstore.net 100%

Current Scans: 0 URLs Found: 86 Nodes Added: 4 Export

Processed	Method	URI	Seed
●	GET	http://www.badstore.net	Seed
●	GET	http://www.badstore.net/robots.txt	Seed
●	GET	http://www.badstore.net/sitemap.xml	Seed
●	GET	http://www.badstore.net/?action=search&searchquery=ZAP	Seed
●	GET	http://www.badstore.net/BadStore_net_v1_2_Manual.pdf	Seed
●	GET	http://www.badstore.net/DoingBusiness	Seed
●	GET	http://www.badstore.net/DoingBusiness/contract.doc	Seed
●	GET	http://www.badstore.net/Procedures	Seed
●	GET	http://www.badstore.net/Procedures/UploadProc.html	Seed
●	GET	http://www.badstore.net/Procedures/UploadProc_files	Seed
●	GET	http://www.badstore.net/Procedures/UploadProc_files/filelist.xml	Seed
●	GET	http://www.badstore.net/backup	Seed
●	GET	http://www.badstore.net/cardvrfy.js	Seed
●	GET	http://www.badstore.net/cgi-bin	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=cartview	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=doguestbook	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=cartadd	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=moduser	Seed
●	GET	http://www.badstore.net/cgi-bin/badstore.cgi?action=login	Seed

## Ataque 2 – escaneo

Untitled Session - ZAP 2.15.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites

GET:badstore.cgi  
GET:badstore.cgi?action  
POST:badstore.cgi?action  
POST:badstore.cgi?action/Add Items to Cart, cartitem  
POST:badstore.cgi?action/DelMod, email, pwdhint  
POST:badstore.cgi?action/Login\_email, password  
POST:badstore.cgi?action/Place Order, cartitem  
POST:badstore.cgi?action/Register\_email, fullname, password, pwdhint, role

Header Text Body Text

POST http://www.badstore.net/cgi-bin/badstore.cgi?action=login HTTP/1.1  
host: www.badstore.net  
Proxy-Connection: keep-alive  
content-length: 33  
Cache-Control: max-age=0  
email=<password=<login"> or 2=1 />

History Search Alerts Output Spider Active Scan Fuzzer

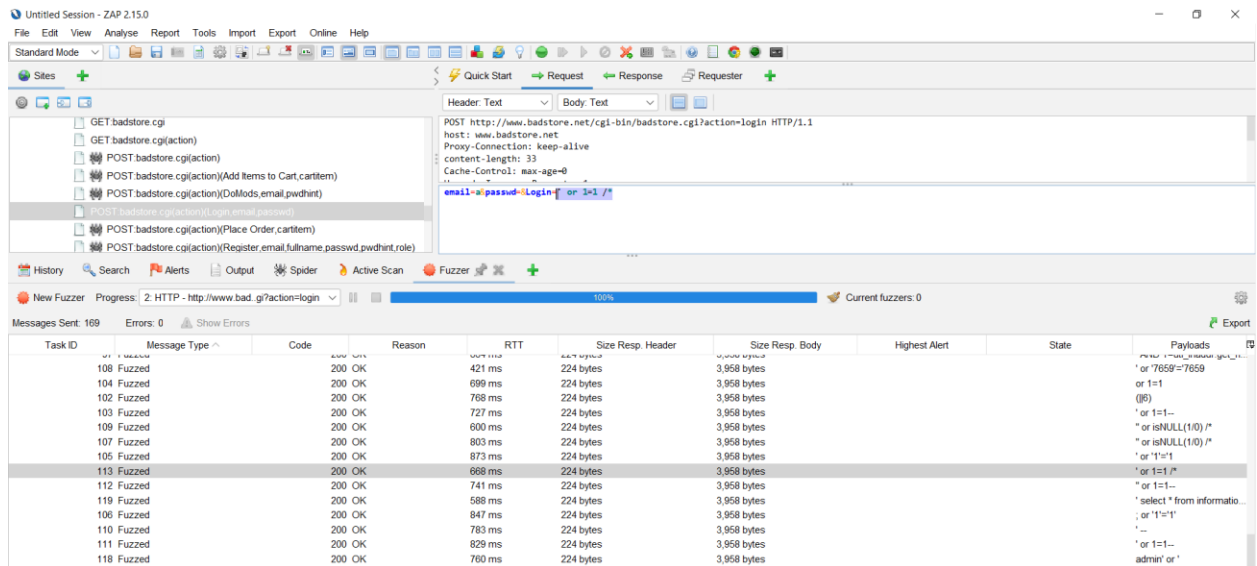
New Scan Progress: 3: http://www.badstore.net 100%

Current Scans: 0 Num Requests: 7 New Alerts: 0 Export

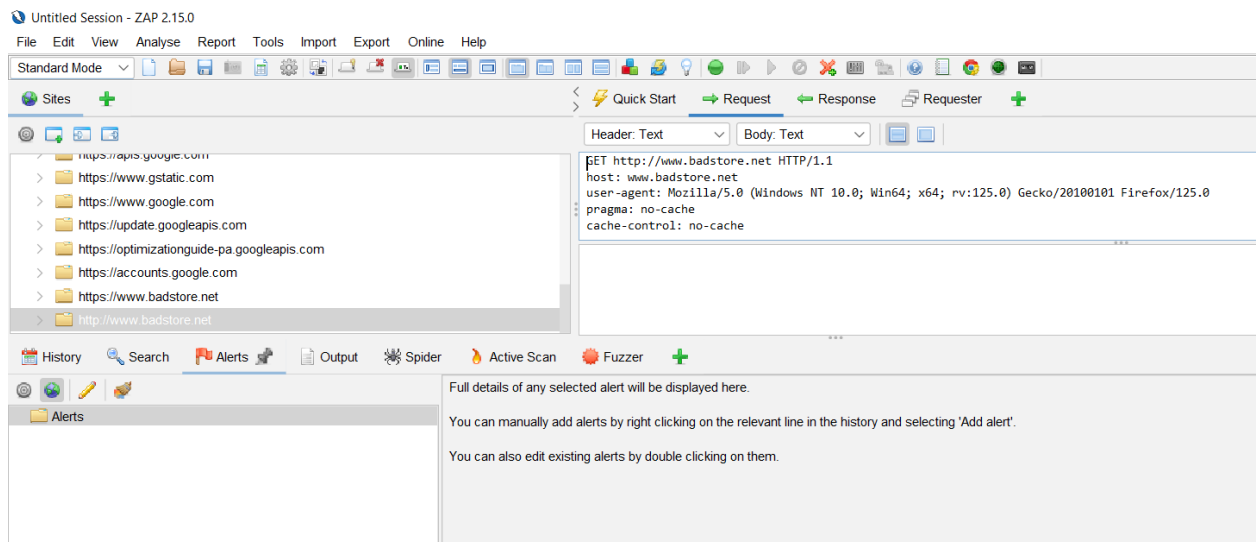
ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
360	5/11/24, 9:07:14 PM	5/11/24, 9:07:14 PM	GET	http://www.badstore.net/7260699051608850759	404	Not Found	136 ms	189 bytes	283 bytes
362	5/11/24, 9:07:14 PM	5/11/24, 9:07:14 PM	GET	http://www.badstore.net/DoingBusiness/1100373909056522	404	Not Found	102 ms	189 bytes	287 bytes
364	5/11/24, 9:07:14 PM	5/11/24, 9:07:14 PM	GET	http://www.badstore.net/Procedures/17676309508327715	404	Not Found	105 ms	189 bytes	294 bytes
366	5/11/24, 9:07:14 PM	5/11/24, 9:07:15 PM	GET	http://www.badstore.net/Procedures/UploadProc_files/2161	404	Not Found	101 ms	189 bytes	311 bytes
368	5/11/24, 9:07:15 PM	5/11/24, 9:07:15 PM	GET	http://www.badstore.net/cgi-bin/6507707569040646113	404	Not Found	106 ms	189 bytes	291 bytes
370	5/11/24, 9:07:15 PM	5/11/24, 9:07:15 PM	GET	http://www.badstore.net/images/1724266891820302251	404	Not Found	104 ms	189 bytes	290 bytes
372	5/11/24, 9:07:15 PM	5/11/24, 9:07:15 PM	GET	http://www.badstore.net/scanbot/351625204556738565	404	Not Found	129 ms	189 bytes	290 bytes

## Ataque 3 - inyección SQL

Se realiza la prueba mediante inyección SQL y se identifica que la cláusula '**or 1=1** /\*' permite el ingreso a la aplicación.



Los escaneos no generan alertas, sin embargo, se debe tener en cuenta que mediante de inyección de código SQL se logró iniciar sesión, lo cual es un fallo de seguridad muy elevado. Para ello se deben tomar medidas correctivas y preventivas como lo son la validación de caracteres, el escape de caracteres especiales, actualización de los sistemas y directamente desde código separar los valores ingresados de la consulta SQL.





## Referencias Bibliográficas

OWASP (2020). [Web Application Penetration Testing](https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies). [https://owasp.org/www-project-web-security-testing-guide/latest/3-The\\_OWASP\\_Testing\\_Framework/1-Penetration\\_Testing\\_Methodologies](https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies)

OWASP (2021). [TOP TEN](https://owasp.org/Top10/es/). <https://owasp.org/Top10/es/>

Ramachandran, M. (2012). [Software Security Testing](https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=602994&lang=es&site=eds[1]live&scope=site&ebv=EB&ppid=pp_151). En Nova (Eds), Software Security Engineering : Design and Applications (pp. 151-164). Nova Science Publishers, Inc. [https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=602994&lang=es&site=eds\[1\]live&scope=site&ebv=EB&ppid=pp\\_151](https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=602994&lang=es&site=eds[1]live&scope=site&ebv=EB&ppid=pp_151)