|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 6 Report |

Table of Contents

[1.0 Introduction –Common Attack Types - Insecure Direct Object Reference (IDOR) & Directory Traversal 3](#_Toc147689936)

[1.1 Lab Results – Common Attack Types - Insecure Direct Object Reference (IDOR) & Directory Traversal 4](#_Toc147689937)

[2.0 References: 13](#_Toc147689938)

[3.0 Activity Log 14](#_Toc147689939)

# Introduction –Common Attack Types - Insecure Direct Object Reference (IDOR) & Directory Traversal

During the execution of this lab, an evaluation was done to test attacks in IDOR. IDOR is an access control vulnerability that looks to find objects that are on the internal several that are open to accessibility. Through these attacks, attackers can extract information from the internal object itself. The other focus was around Directory traversal, which is an attack that is used to find restricted directories on a server and access them. This attack uses misconfigured permissions on the actual server which can be exploited by potential attackers to access critical files as well as modify them to gain access to the server itself.

Through the usage of OWASP Zap, attacks can be emulated on localhost environments through dynamic SSL certificates to emulate actual websites in a lab environment. Once that was completed, an emulated site of Bwapp was used to attempt different types of attack vectors on an insecure site. The vulnerability executions done included both web request modifications and injected Linux commands. Since the data itself was never sanitized as well as the permission modules on the objects/directories were never properly set, attackers could use the web application to access these files and folders. Through this access, attackers can traverse the server as if they were on it using the permission model that is on the actual web application.

To avoid these types of attacks, proper permissions must be implemented on both the objects as well as the directories for reading and writing permissions. Improper permissions allow attackers to use the host's own web application against them to escalate and traverse through their server.

# 1.1 Lab Results – Common Attack Types - Insecure Direct Object Reference (IDOR) & Directory Traversal

A screenshot of a computer

Description automatically generated

Figure 1.0 – Start the OWASP Zap application.

A screenshot of a computer

Description automatically generated

Figure 1.1 – Create and save a local SSL certificate.

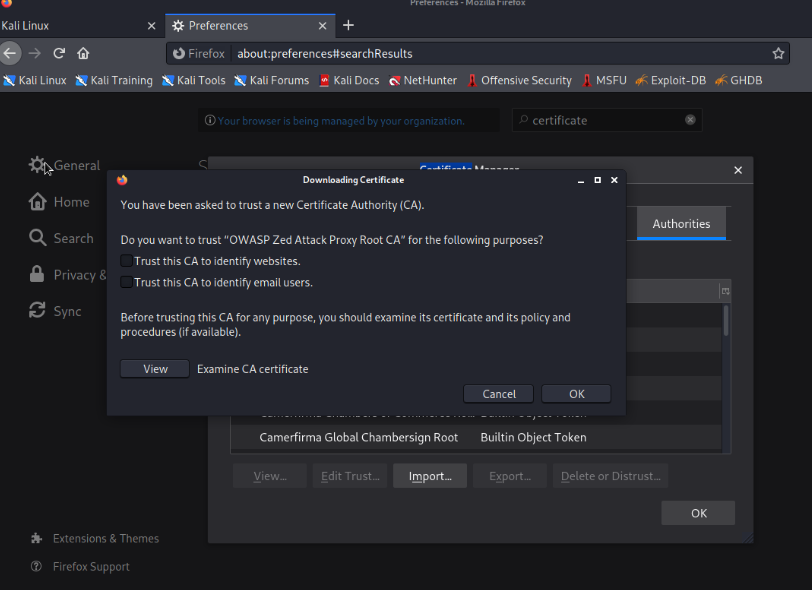


Figure 1.2 – Add the certification to your local browser.

A screenshot of a computer

Description automatically generated

Figure 1.3 – Modify your proxy to be the local host for resolution sites.

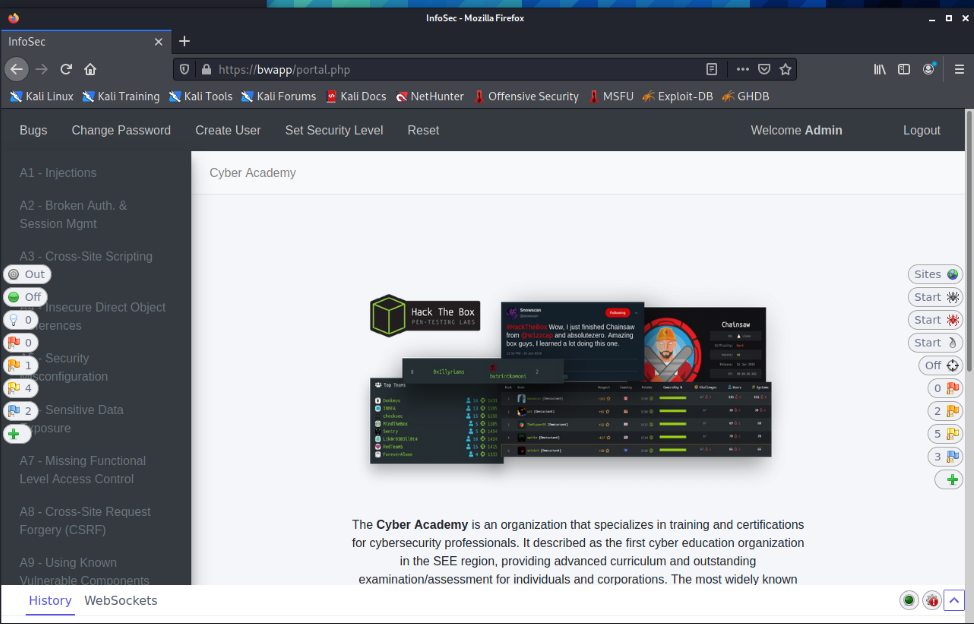


Figure 1.4 – Log into the bwapp website.

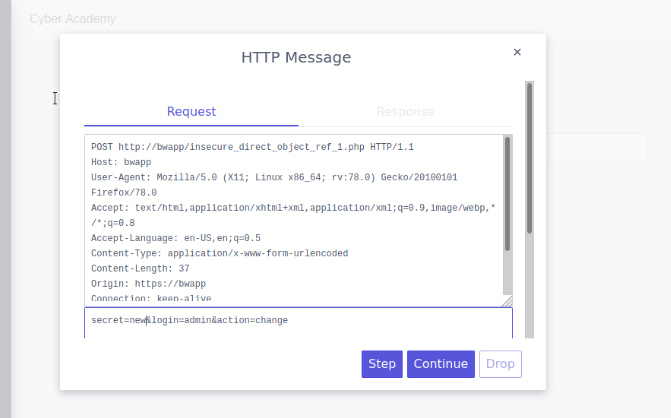


Figure 1.5 – Break on the POST Request, change the payload secret to ‘new’.

A screenshot of a computer

Description automatically generated

Figure 1.6 – Secret was changed to ‘new’ successfully.

A screenshot of a computer

Description automatically generated

Figure 1.7 – Change the login to be bob from admin.

A screenshot of a computer

Description automatically generated

Figure 1.8 – Bobs password was changed without him knowing.

A screenshot of a computer

Description automatically generated

Figure 1.9 - Change the page variable and delete it. We can see it is still looking for a file that does not exist now.

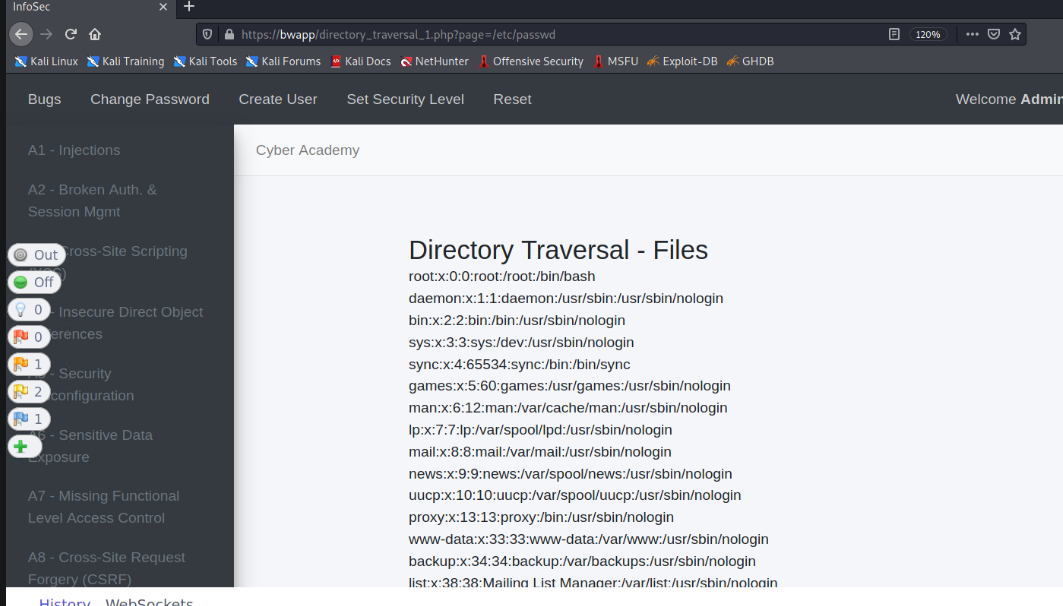


Figure 1.10 - Change the page variable to /etc/passwd. The site returns the file through file escalation.

A black screen with white text

Description automatically generated

Figure 1.11 – We can also attempt to use /../../../../ to traverse through file structures as well in the variable, giving us the ability to mimic cd commands on the actual Linux server.

# 2.0 References:

[1] Insecure Direct Object Reference Prevention · OWASP Cheat Sheet Series. (2013). Owasp.org. https://cheatsheetseries.owasp.org/cheatsheets/Insecure\_Direct\_Object\_Reference\_Prevention\_Cheat\_Sheet.html

[2] WSTG - Latest | OWASP. (n.d.). Owasp.org. <https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References>

[3] OWASP. (n.d.). Path Traversal | OWASP. Owasp.org. https://owasp.org/www-community/attacks/Path\_Traversal

[4] PortSwigger. (2019). What is directory traversal, and how to prevent it? Portswigger.net. https://portswigger.net/web-security/file-path-traversal

‌

‌

‌

‌

# 3.0 Activity Log

| **Member Name** | **Task Date** | **Task Details** |
| --- | --- | --- |
| Carl Laneave | 10/08/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |