Lab 6 Report

Jason Tolbert

The Pennsylvania State University

IST 894-001: Capstone Experience

Dr. Michael Bartolacci, Instructor

March 5th, 2025

Table of Contents

General Context

This lab introduces participants to two kinds of web vulnerabilities: insecure direct object references and directory traversal.

Insecure direct object references (IDOR) are possible when a web application trusts user-supplied identifiers – like user IDs in URLs — without validating whether the user is authorized to access the resource associated with that identifier. (Pratama & Rhusuli, 2022). For instance, let's say you have an account at *example.com*, and you can access your account's settings at *example.com/user/11037/settings*, where 11037 is your user ID. Now, let's say you change the user ID in the URL to 154064. Ideally, *example.com* would validate that you are user 154064 before letting you continue. But, if *example.com* was vulnerable to IDOR, it wouldn't perform that validation — it would simply let you access the modify the settings of that person's account.

Directory traversal is possible when websites display the contents of a file or directory provided in the URL but fail to limit the scope of files and directories that can be displayed (Chawda et al., 2021). For instance, say that going to *example.com/hello.txt* displays the contents of a file named *hello.txt*. If *example.com* was vulnerable to directory traversal, you could replace *hello.txt* with the path to *any* file or directory and *example.com* would display its contents — e.g., browsing to *example.com//etc/passwd* would show you sensitive information about the user accounts registered on the server where *example.com* is hosted.

In the lab, participants explore these vulnerabilities via bWAPP (**b**uggy **W**eb **App**lication), a locally-hosted web app that is deliberately susceptible to a wide range of vulnerabilities. bWAPP exists for the express purpose of teaching users about these vulnerabilities and their potential consequences and isn't quite reflective of the real-world web app security landscape, where modern frameworks, web servers, and cloud providers often block IDOR, directory traversal, and other common vulnerabilities out of the box. In the increasingly limited-number cases where this doesn't apply, there are other fairly easy methods of preventing these attacks — for example, robots that automatically crawl websites to detect potential IDOR vectors, or simple algorithms that stop directory traversal. (Flanders, 2019; Hadavi et al., 2021).

Technical Context

This lab introduces participants to indirect object reference (IDOR) and directory traversal vulnerabilities.

IDOR vulnerabilities are typically the consequences of improper access control enforcement at the object level. When an application relies solely on user-supplied identifiers in URLs, API requests, or other inputs without enforcing proper authorization, attackers can modify those identifiers to obtain unauthorized access. There are various strategies to mitigate IDOR; most common among them are role- and attribute-based access control. IDOR is also often mitigated by removing the need for identifiers in in user-supplied inputs entirely — for instance, instead of a website at *example.com* having distinct paths for every variation of */user/<USER_ID>/settings*, it would simply have a single path at */user/settings*, determine the user ID via a token cookie that was set on login, and render the settings page for the appropriate user.

Directory traversal attacks target improperly sanitized file inputs. Classic examples use query parameters, but any kind of input that takes a file path can be a vector for directory traversal, including forms and file uploads. In some cases, websites vulnerable to SQL injection can also be vulnerable to directory traversal by proxy, depending on the database interacts with the filesystem. The most standard prevention measure is simple whitelisting of the files and directories that can be accessed, though it is rare that prevention measures specific to directory traversal are needed at all — modern web frameworks, web servers, and cloud hosts will generally block directory traversal out of the gate.

The lab has users explore these vulnerabilities through bWAPP, a deliberately vulnerable web application designed to demonstrate web app vulnerabilities and their potential consequences. In the IDOR half of the lab, users use the Zed Attack Proxy to intercept a request and modify a user identifier in order to change the password for an account other their own; in the directory traversal half, users modify a file path query parameter to point to /etc/passwd.

References

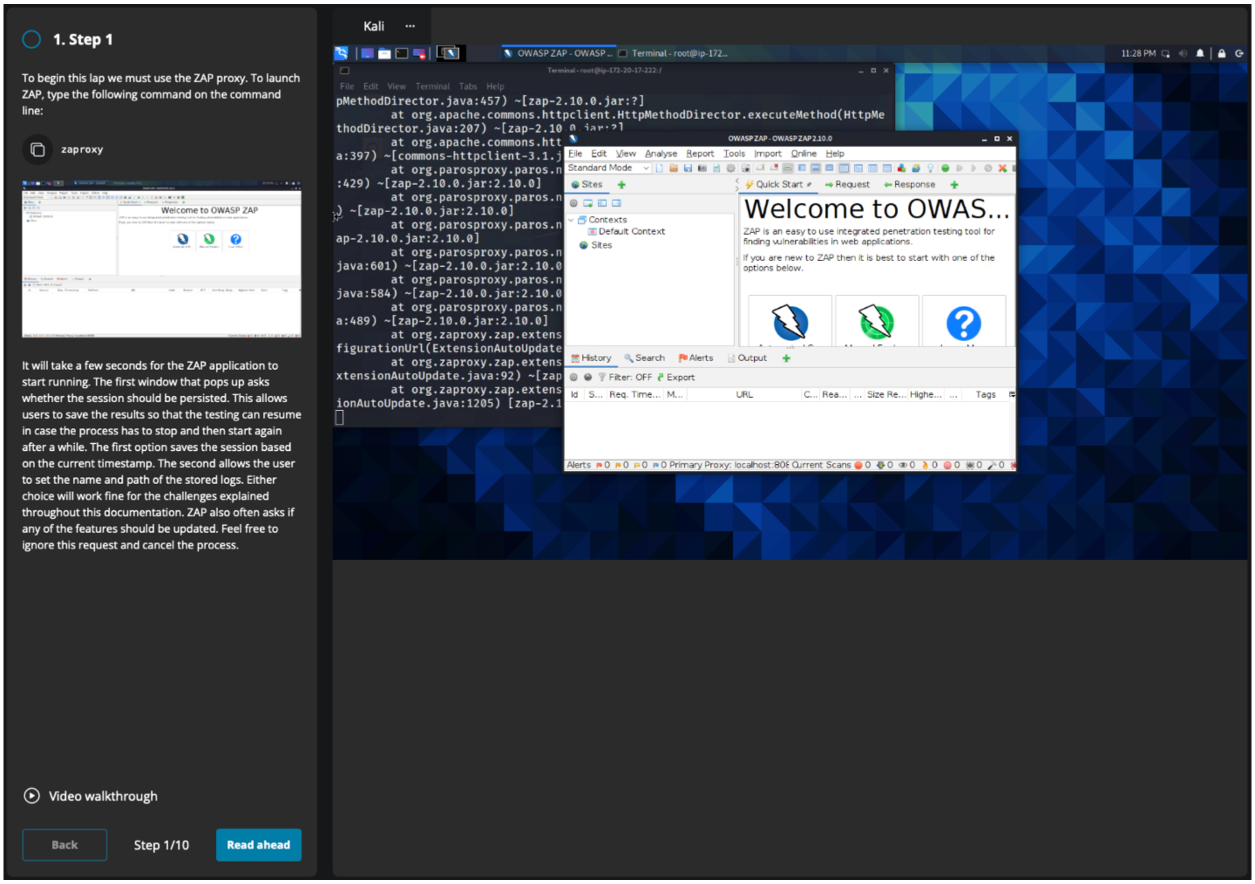
Chawda, M., Sharma, Dr. P., & Patel, Mr. J. (2021). Deep dive into directory traversal and file inclusion attacks leads to privilege escalation. *International Journal of Scientific Research in Science, Engineering and Technology*, 115–120. https://doi.org/10.32628/IJSRSET218384

Flanders, M. (2019). *A simple and intuitive algorithm for preventing directory traversal attacks* (No. arXiv:1908.04502). arXiv. https://doi.org/10.48550/arXiv.1908.04502

Hadavi, M. A., Bagherdaei, A., & Ghasemi, S. (2021). *IDOT: black-box detection of access control violations in web applications*.

Pratama, I. P. A. E., & Rhusuli, A. M. (2022). Penetration testing on web application using insecure direct object references (IDOR) method. *2022 International Conference on ICT for Smart Society (ICISS)*, 01–07. https://doi.org/10.1109/ICISS55894.2022.9915074

Screenshots



1. Step 1

To begin this lap we must use the ZAP proxy. To launch ZAP, type the following command on the command line:

```
zaproxy
```

It will take a few seconds for the ZAP application to start running. The first window that pops up asks whether the session should be persisted. This allows users to save the results so that the testing can resume in case the process has to stop and then start again after a while. The first option saves the session based on the current timestamp. The second allows the user to set the name and path of the stored logs. Either choice will work fine for the challenges explained throughout this documentation. ZAP also often asks if any of the features should be updated. Feel free to ignore this request and cancel the process.

Video walkthrough
Back
Step 1/10
Read ahead
Kali
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:28 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help

```
pMethodDirector.java:457) ~[zap-2.10.0.jar:?]
        at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMe
thodDirector.java:207) ~[zap-2.10.0.jar:?]
        at org.apache.commons.htt
a:397) ~[commons-httpclient-3.1.j
        at org.parosproxy.paros.n
:429) ~[zap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
) ~[zap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
ap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
java:601) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy.paros.n
java:584) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy.paros.n
a:489) ~[zap-2.10.0.jar:2.10.0]
        at org.zaproxy.zap.extens
figurationUrl(ExtensionAutoUpdate
        at org.zaproxy.zap.extens
xtensionAutoUpdate.java:92) ~[zap
        at org.zaproxy.zap.extens
ionAutoUpdate.java:1205) [zap-2.1
```

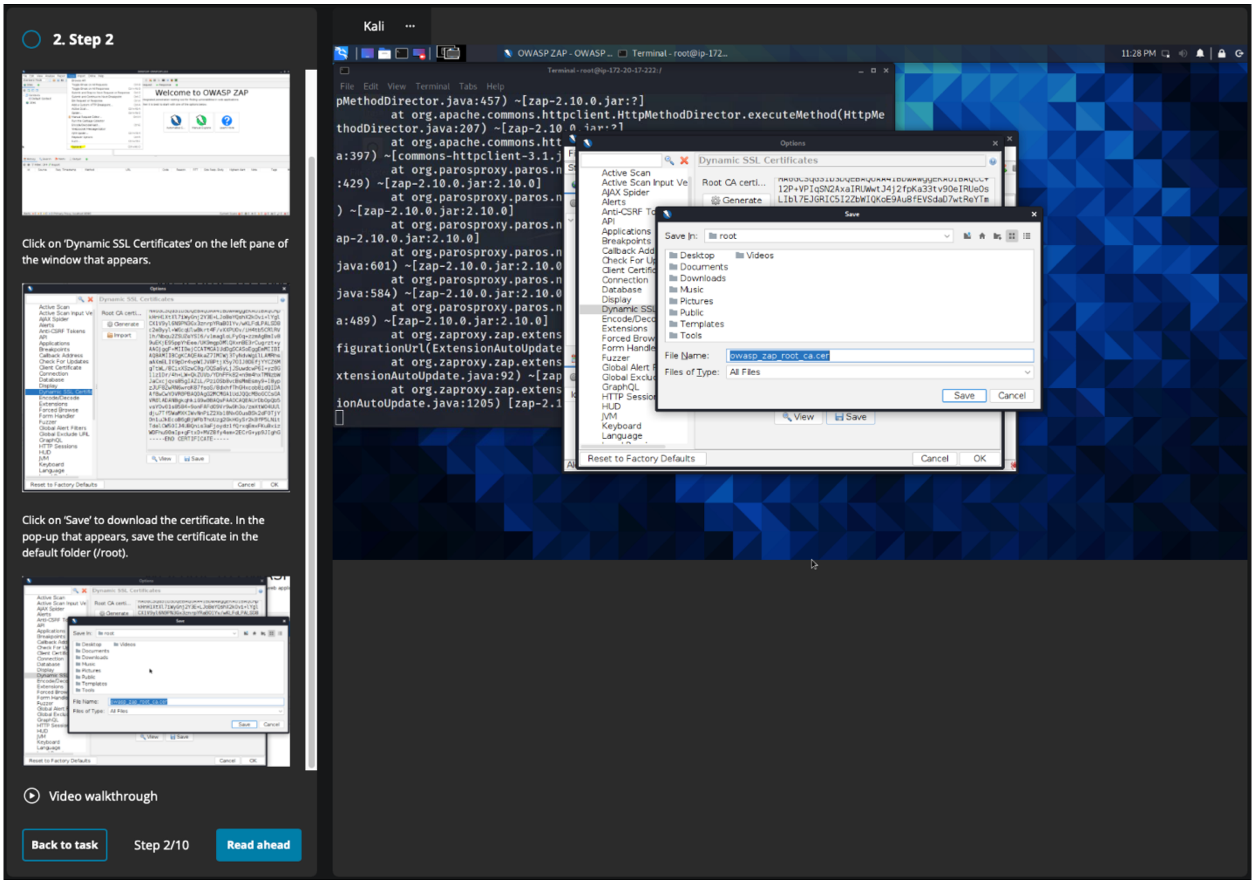
OWASP ZAP - OWASP ZAP 2.10.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites

Welcome to OWAS...

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Figure 1. Launching ZAP.



2. Step 2

Click on 'Dynamic SSL Certificates' on the left pane of the window that appears.

Click on 'Save' to download the certificate. In the pop-up that appears, save the certificate in the default folder (/root).

Video walkthrough

Back to task | Step 2/10 | Read ahead

Terminal - root@ip-172-20-17-222:/

```
pMethodDirector.java:457) ~[zap-2.10.0.jar:?]
        at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMe
thodDirector.java:207) ~[zap-2.10.0.jar:?]
        at org.apache.commons.htt
a:397) ~[commons-httpclient-3.1.j
        at org.parosproxy.paros.n
:429) ~[zap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
) ~[zap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
ap-2.10.0.jar:2.10.0]
        at org.parosproxy.paros.n
java:601) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy.paros.n
java:584) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy.paros.n
a:489) ~[zap-2.10.0.jar:2.10.0]
        at org.zaproxy.zap.extens
figurationUrl(ExtensionAutoUpdate
        at org.zaproxy.zap.extens
xtensionAutoUpdate.java:92) ~[zap
        at org.zaproxy.zap.extens
ionAutoUpdate.java:1205) [zap-2.1
```

Options – Dynamic SSL Certificates

Root CA certi...

```
12P+VPIqSN2AxaIRUWwtJ4j2fpKa33tv90eIRUeOs
LIbl7EJGRIC5I2ZbWIQKoE9Au8fEVSdaD7wtReYTm
```

Save

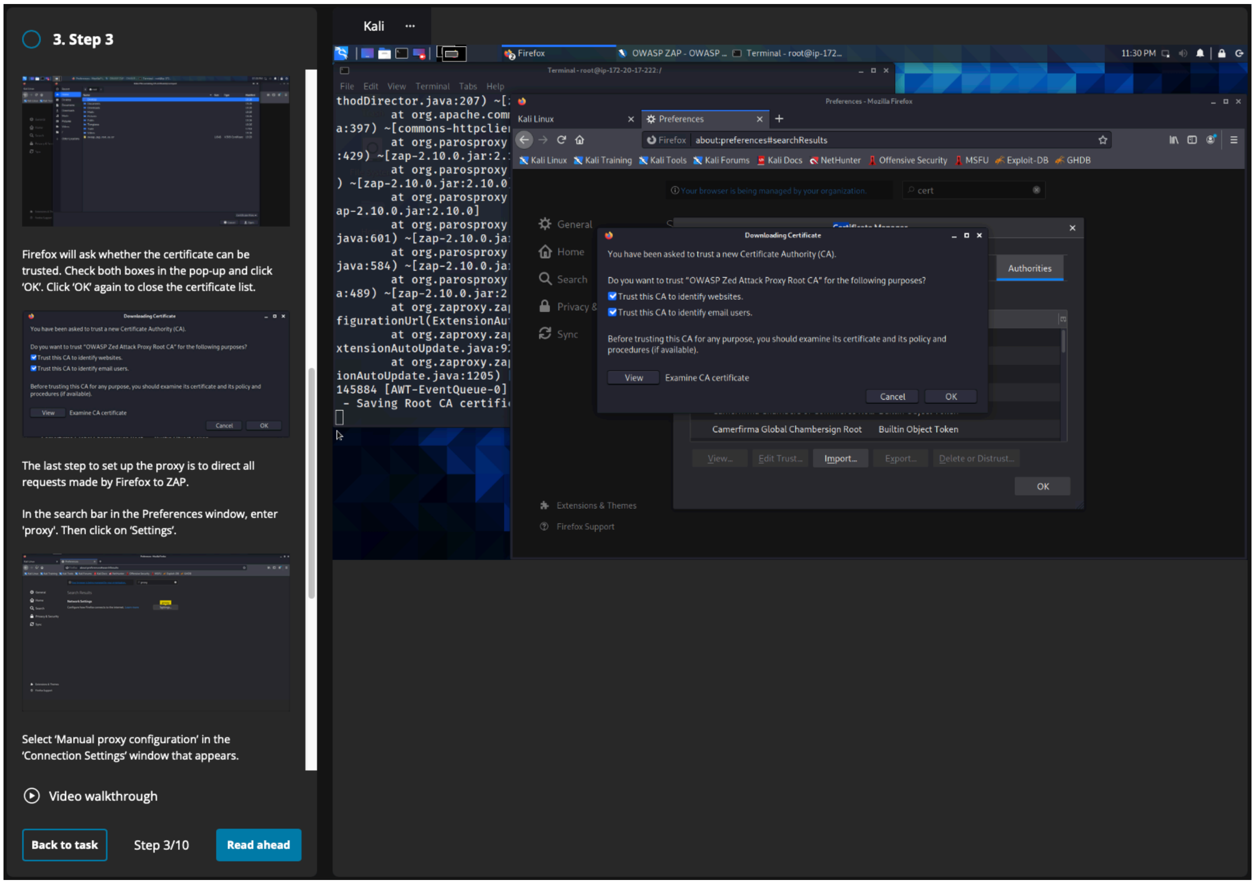
Save In: root

Desktop, Documents, Downloads, Music, Pictures, Public, Templates, Tools, Videos

File Name: owasp_zap_root_ca.cer

Files of Type: All Files

Figure 2. Downloading an SSL certificate from ZAP.



3. Step 3

Firefox will ask whether the certificate can be trusted. Check both boxes in the pop-up and click 'OK'. Click 'OK' again to close the certificate list.

The last step to set up the proxy is to direct all requests made by Firefox to ZAP.

In the search bar in the Preferences window, enter 'proxy'. Then click on 'Settings'.

Select 'Manual proxy configuration' in the 'Connection Settings' window that appears.

Video walkthrough
Back to task
Step 3/10
Read ahead
Kali
Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:30 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help

```
thodDirector.java:207) ~[:
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

Camerfirma Global Chambersign Root | Builtin Object Token

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "OWASP Zed Attack Proxy Root CA" for the following purposes?

☑ Trust this CA to identify websites.

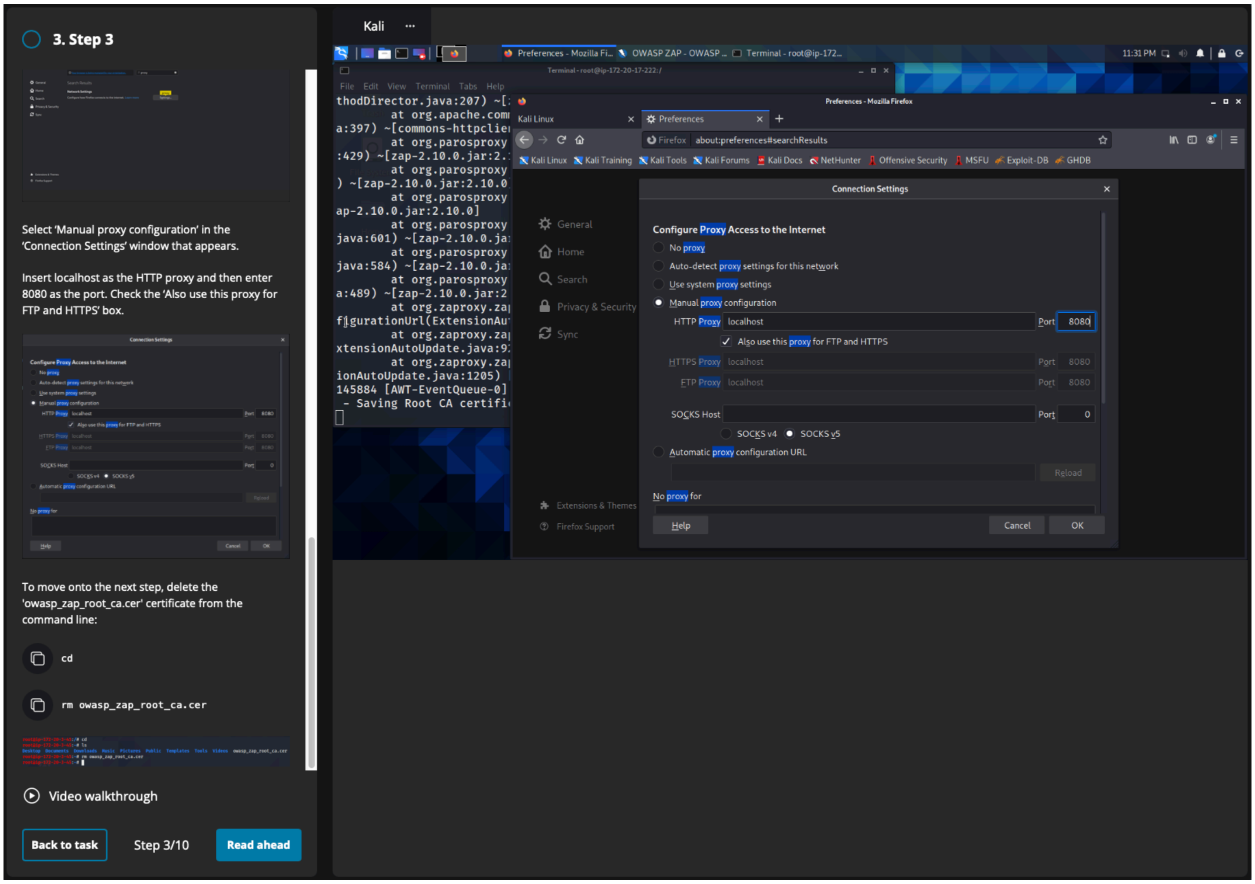
☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

Figure 3. Trusting the ZAP certificate in Firefox.



Select 'Manual proxy configuration' in the 'Connection Settings' window that appears.

Insert localhost as the HTTP proxy and then enter 8080 as the port. Check the 'Also use this proxy for FTP and HTTPS' box.

To move onto the next step, delete the 'owasp_zap_root_ca.cer' certificate from the command line:

```
cd
```

```
rm owasp_zap_root_ca.cer
```

Video walkthrough
Back to task
Step 3/10
Read ahead
Kali
Preferences - Mozilla Fi...
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:31 PM
File Edit View Terminal Tabs Help

```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy: localhost Port: 8080

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy: localhost Port: 8080

FTP Proxy: localhost Port: 8080

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5

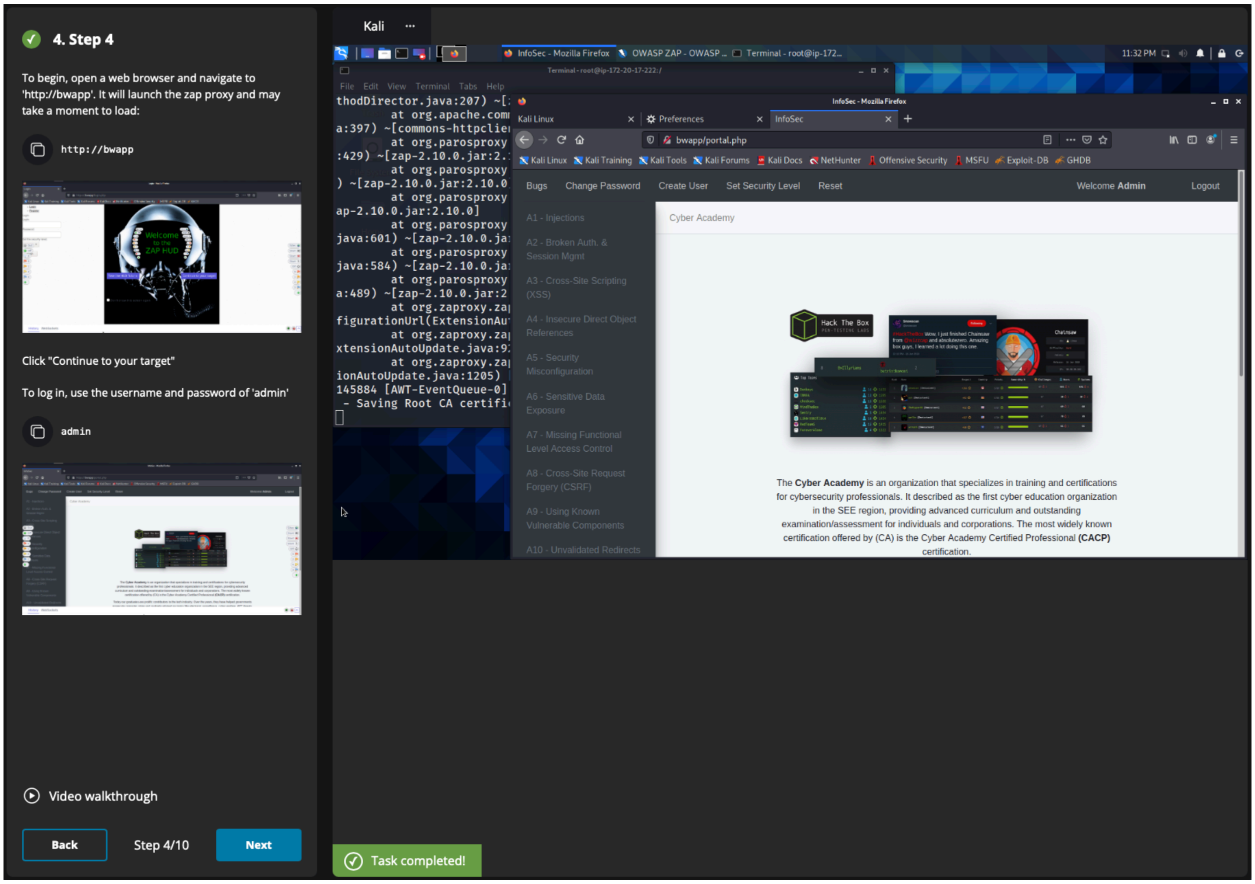
○ Automatic proxy configuration URL

Reload

No proxy for

Help Cancel OK

Figure 4. Configuring Firefox to direct all requests through ZAP.



4. Step 4

To begin, open a web browser and navigate to 'http://bwapp'. It will launch the zap proxy and may take a moment to load:

```
http://bwapp
```

Click "Continue to your target"

To log in, use the username and password of 'admin'

```
admin
```

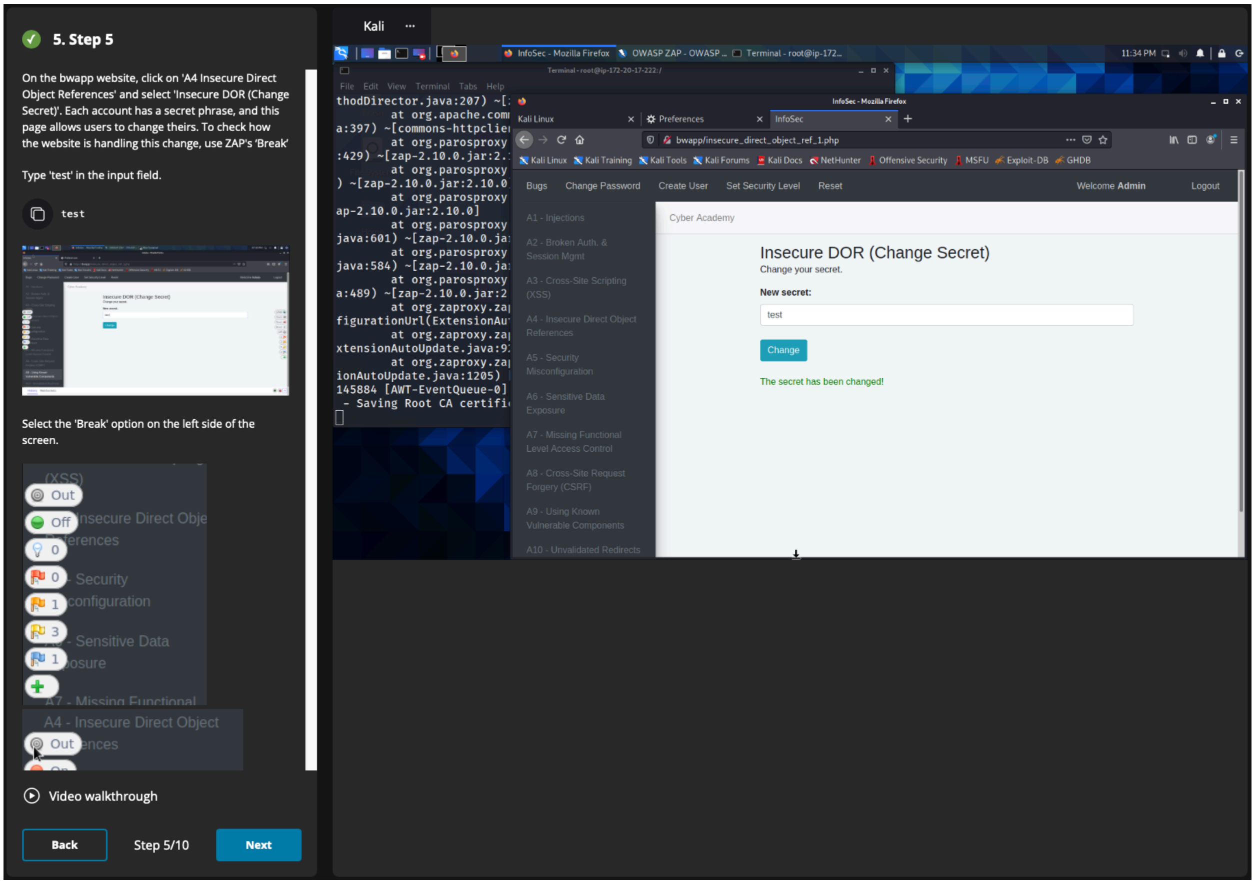
Video walkthrough
Back
Step 4/10
Next
Kali
InfoSec - Mozilla Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:32 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help

```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

InfoSec - Mozilla Firefox
Kali Linux
Preferences
InfoSec
bwapp/portal.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Bugs
Change Password
Create User
Set Security Level
Reset
Welcome Admin
Logout
A1 - Injections
A2 - Broken Auth. & Session Mgmt
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Functional Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Unvalidated Redirects
Cyber Academy
Hack The Box
PEN-TESTING LABS
Chainsaw

The **Cyber Academy** is an organization that specializes in training and certifications for cybersecurity professionals. It described as the first cyber education organization in the SEE region, providing advanced curriculum and outstanding examination/assessment for individuals and corporations. The most widely known certification offered by (CA) is the Cyber Academy Certified Professional **(CACP)** certification.

Figure 5. The bWAAP interface.



5. Step 5

On the bwapp website, click on 'A4 Insecure Direct Object References' and select 'Insecure DOR (Change Secret)'. Each account has a secret phrase, and this page allows users to change theirs. To check how the website is handling this change, use ZAP's 'Break'

Type 'test' in the input field.

```
test
```

Select the 'Break' option on the left side of the screen.

Out
Off
0
0
1
3
1
A4 - Insecure Direct Object
Out
Video walkthrough
Back
Step 5/10
Next
Kali
InfoSec - Mozilla Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:34 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help

```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

InfoSec - Mozilla Firefox
Kali Linux
Preferences
InfoSec
bwapp/insecure_direct_object_ref_1.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Bugs
Change Password
Create User
Set Security Level
Reset
Welcome Admin
Logout
A1 - Injections
A2 - Broken Auth. & Session Mgmt
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Functional Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Unvalidated Redirects
Cyber Academy

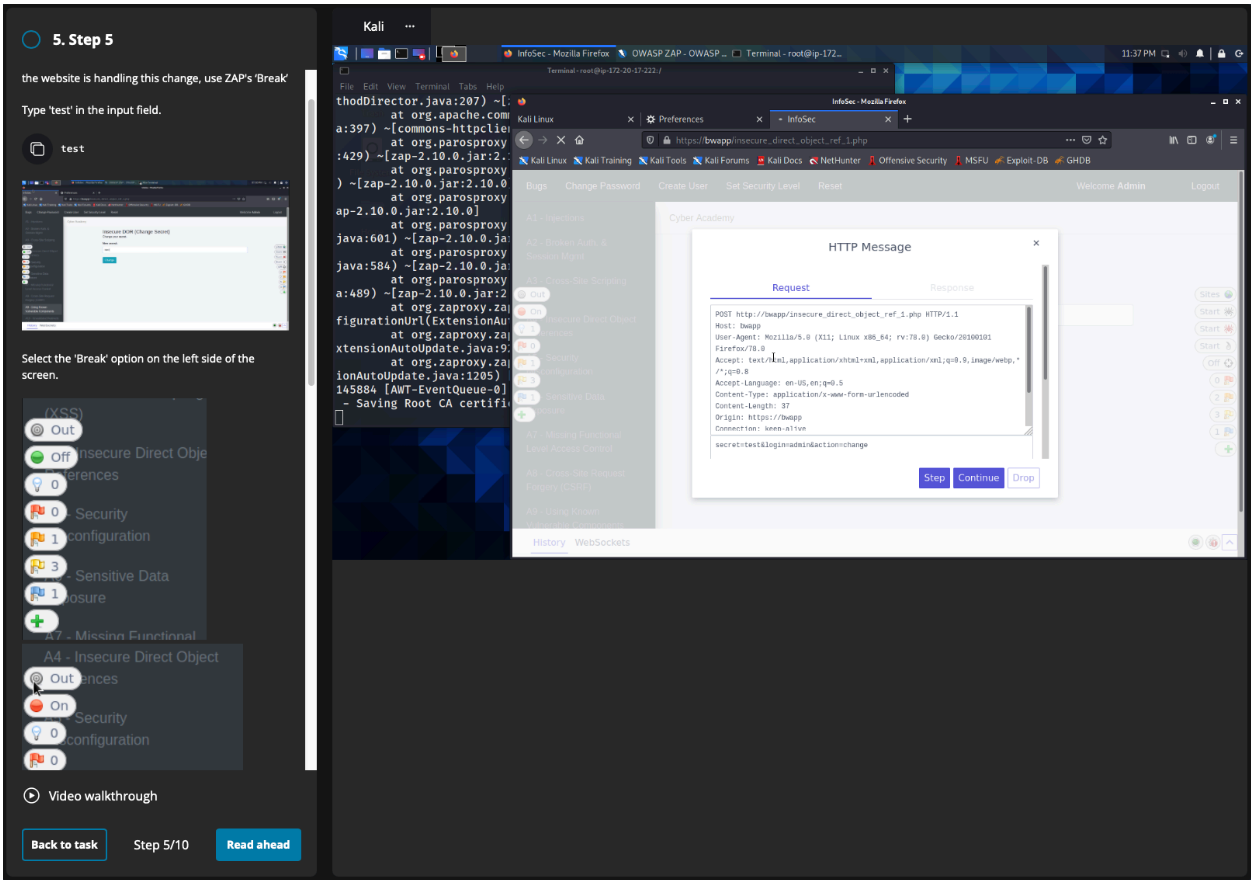
Insecure DOR (Change Secret)

Change your secret.

New secret: test

The secret has been changed!

Figure 6. Changing the account secret.



5. Step 5

the website is handling this change, use ZAP's 'Break'

Type 'test' in the input field.

```
test
```

Select the 'Break' option on the left side of the screen.

Step 5/10

```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

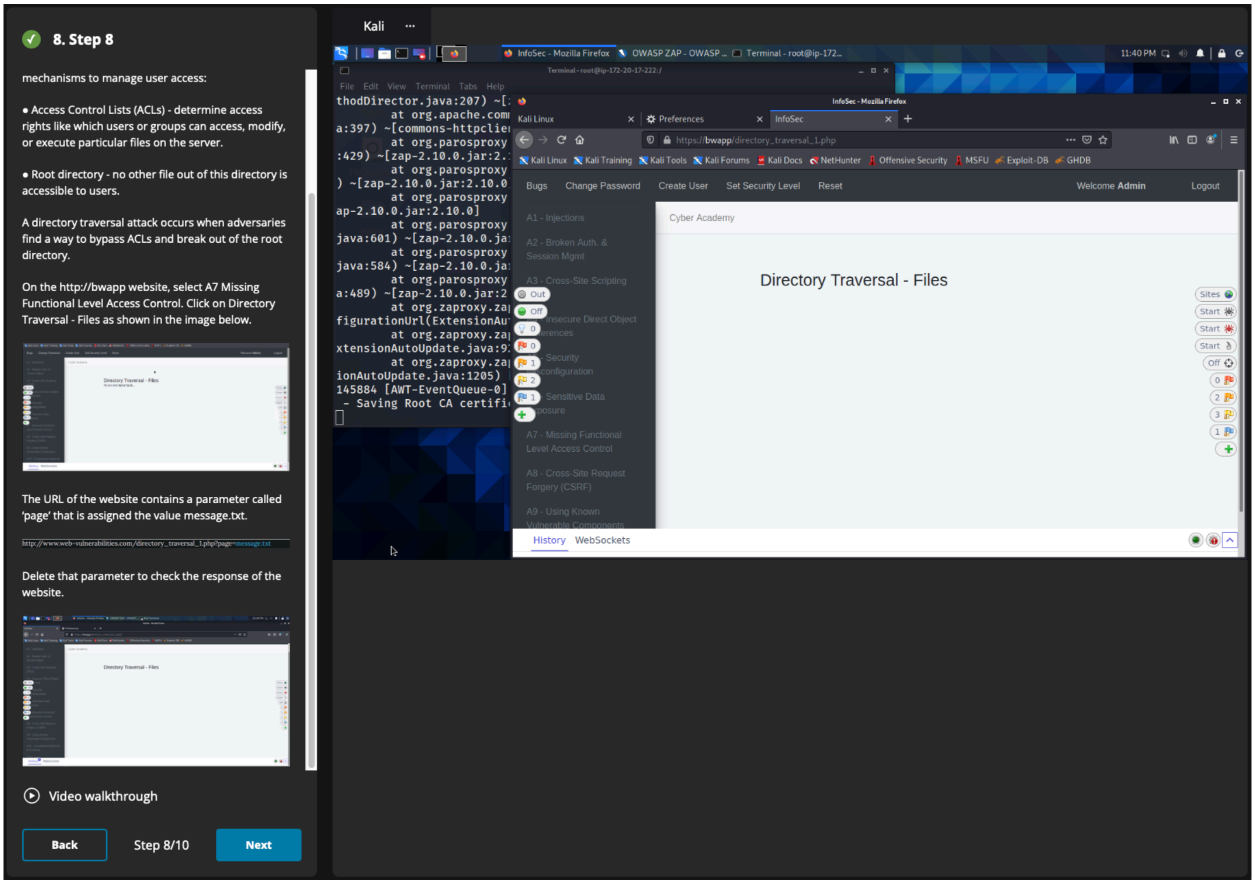
https://bwapp/insecure_direct_object_ref_1.php

HTTP Message

```
POST http://bwapp/insecure_direct_object_ref_1.php HTTP/1.1
Host: bwapp
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: https://bwapp
Connection: keep-alive
```

```
secret=test&login=admin&action=change
```

Figure 7. Examining the captured HTTP request from bWAPP.



8. Step 8

mechanisms to manage user access:

- Access Control Lists (ACLs) - determine access rights like which users or groups can access, modify, or execute particular files on the server.
- Root directory - no other file out of this directory is accessible to users.

A directory traversal attack occurs when adversaries find a way to bypass ACLs and break out of the root directory.

On the http://bwapp website, select A7 Missing Functional Level Access Control. Click on Directory Traversal - Files as shown in the image below.

The URL of the website contains a parameter called 'page' that is assigned the value message.txt.

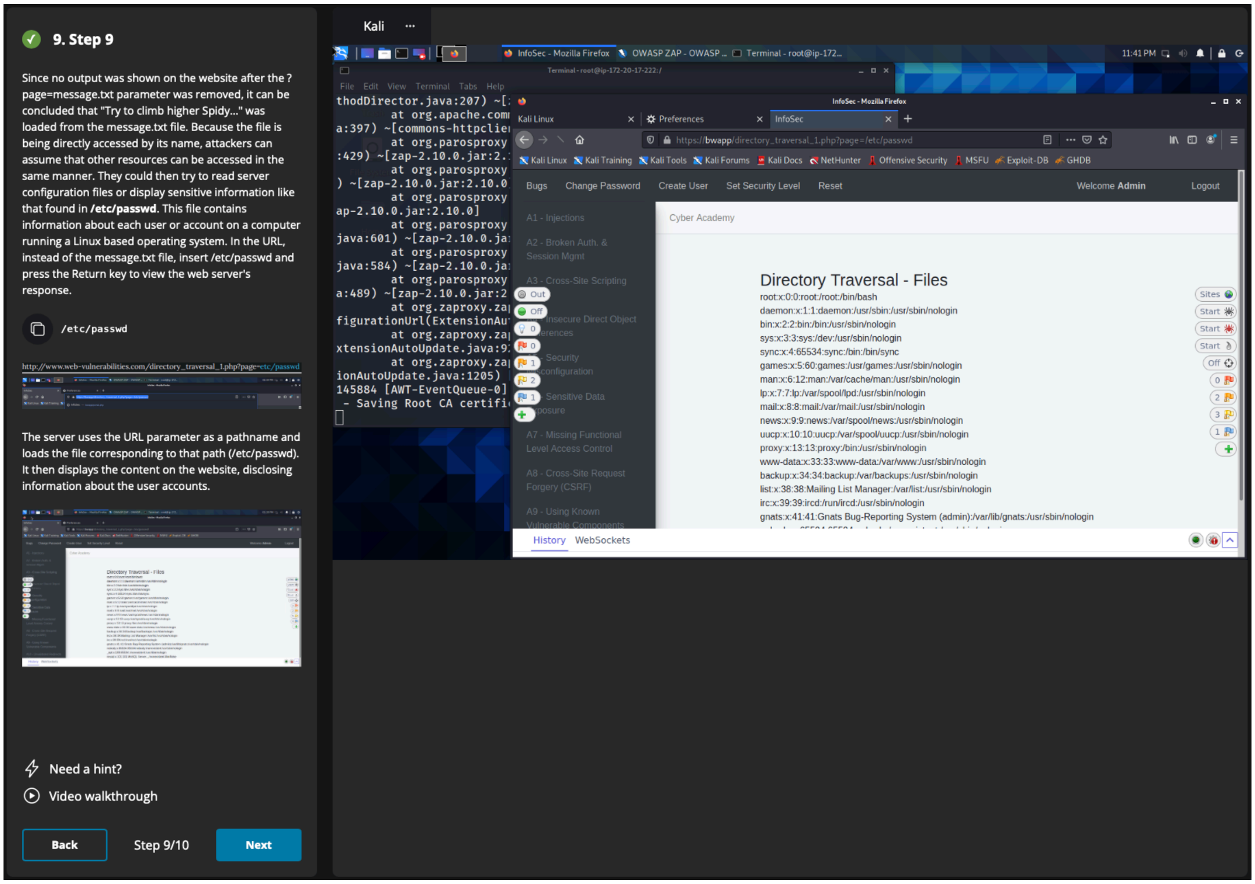
http://www.web-vulnerabilities.com/directory_traversal_1.php?page=message.txt

Delete that parameter to check the response of the website.

Video walkthrough
Back
Step 8/10
Next
Kali
InfoSec - Mozilla Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:40 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help
InfoSec - Mozilla Firefox
Kali Linux
Preferences
InfoSec
https://bwapp/directory_traversal_1.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Bugs
Change Password
Create User
Set Security Level
Reset
Welcome Admin
Logout
A1 - Injections
A2 - Broken Auth. & Session Mgmt
A3 - Cross-Site Scripting
Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
A7 - Missing Functional Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
Cyber Academy
Directory Traversal - Files
Out
Off
Sites
Start
Off
History
WebSockets

```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

Figure 8. The "Directory Traversal - Files" page after removing the "page" query parameter.



9. Step 9

Since no output was shown on the website after the ?page=message.txt parameter was removed, it can be concluded that "Try to climb higher Spidy..." was loaded from the message.txt file. Because the file is being directly accessed by its name, attackers can assume that other resources can be accessed in the same manner. They could then try to read server configuration files or display sensitive information like that found in **/etc/passwd**. This file contains information about each user or account on a computer running a Linux based operating system. In the URL, instead of the message.txt file, insert /etc/passwd and press the Return key to view the web server's response.

```
/etc/passwd
```

http://www.web-vulnerabilities.com/directory_traversal_1.php?page=etc/passwd

The server uses the URL parameter as a pathname and loads the file corresponding to that path (/etc/passwd). It then displays the content on the website, disclosing information about the user accounts.

Need a hint?
Video walkthrough
Back
Step 9/10
Next
Kali
InfoSec - Mozilla Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
11:41 PM
Terminal - root@ip-172-20-17-222:/
File Edit View Terminal Tabs Help

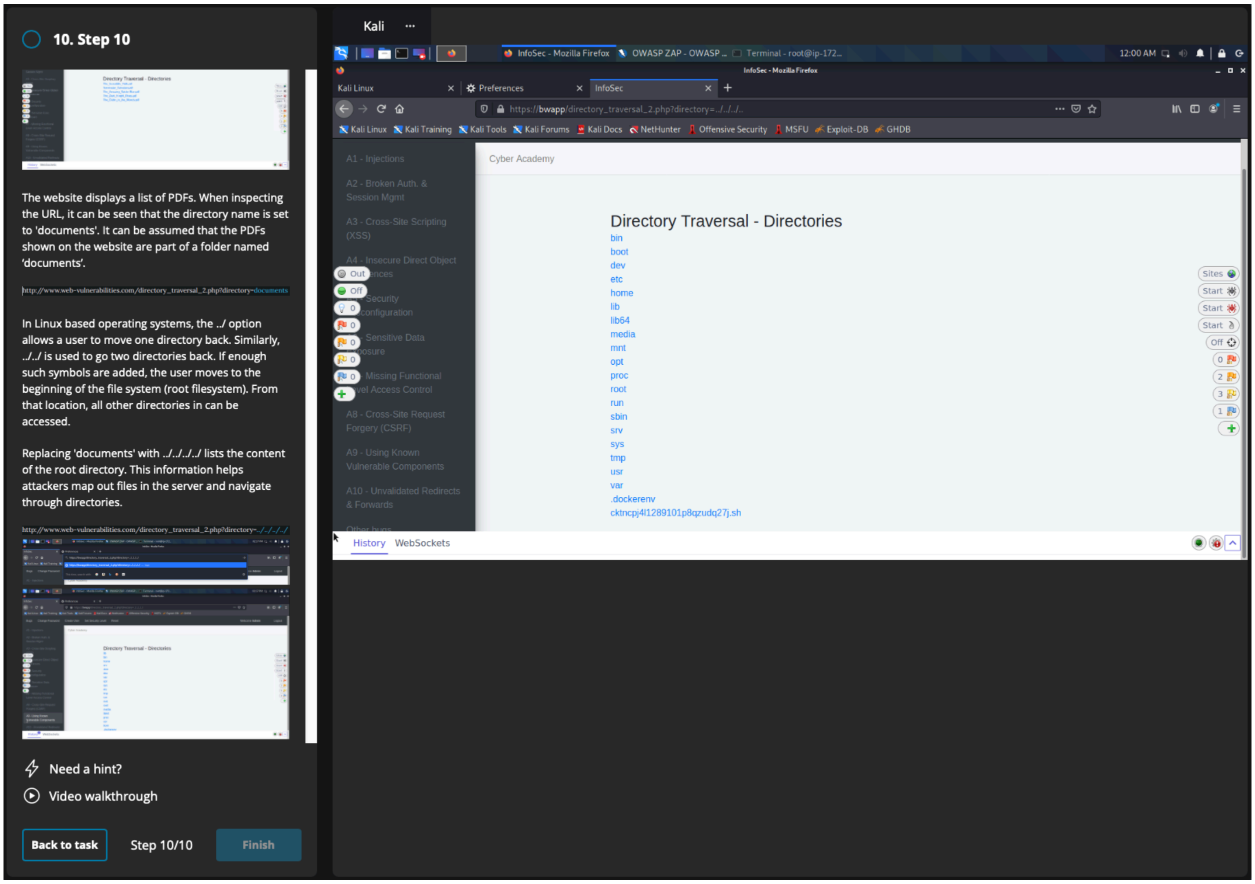
```
thodDirector.java:207) ~[
        at org.apache.comm
a:397) ~[commons-httpclie
        at org.parosproxy
:429) ~[zap-2.10.0.jar:2.
        at org.parosproxy
) ~[zap-2.10.0.jar:2.10.0
        at org.parosproxy
ap-2.10.0.jar:2.10.0]
        at org.parosproxy
java:601) ~[zap-2.10.0.ja
        at org.parosproxy
java:584) ~[zap-2.10.0.ja
        at org.parosproxy
a:489) ~[zap-2.10.0.jar:2
        at org.zaproxy.za
figurationUrl(ExtensionAu
        at org.zaproxy.za
xtensionAutoUpdate.java:9
        at org.zaproxy.za
ionAutoUpdate.java:1205)
145884 [AWT-EventQueue-0]
 - Saving Root CA certifi
```

InfoSec - Mozilla Firefox
Kali Linux
Preferences
InfoSec
https://bwapp/directory_traversal_1.php?page=/etc/passwd
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Bugs
Change Password
Create User
Set Security Level
Reset
Welcome Admin
Logout
A1 - Injections
A2 - Broken Auth. & Session Mgmt
A3 - Cross-Site Scripting
Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
A7 - Missing Functional Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
Cyber Academy
Out
Off
Sites
Start
History
WebSockets

Directory Traversal - Files

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

Figure 9. Exploiting directory traversal to view the contents of /etc/passwd.



10. Step 10

The website displays a list of PDFs. When inspecting the URL, it can be seen that the directory name is set to 'documents'. It can be assumed that the PDFs shown on the website are part of a folder named 'documents'.

```
http://www.web-vulnerabilities.com/directory_traversal_2.php?directory=documents
```

In Linux based operating systems, the ../ option allows a user to move one directory back. Similarly, ../../ is used to go two directories back. If enough such symbols are added, the user moves to the beginning of the file system (root filesystem). From that location, all other directories in can be accessed.

Replacing 'documents' with ../../../../ lists the content of the root directory. This information helps attackers map out files in the server and navigate through directories.

```
http://www.web-vulnerabilities.com/directory_traversal_2.php?directory=../../../../
```

https://bwapp/directory_traversal_2.php?directory=../../../..

Directory Traversal - Directories

bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
.dockerenv
cktncpj4l1289101p8qzudq27j.sh

Need a hint?
Video walkthrough
Back to task
Step 10/10
Finish
Kali
InfoSec - Mozilla Firefox
OWASP ZAP - OWASP ...
Terminal - root@ip-172...
12:00 AM
Kali Linux
Preferences
InfoSec
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
A1 - Injections
A2 - Broken Auth. & Session Mgmt
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
Missing Functional Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Unvalidated Redirects & Forwards
Cyber Academy
Out
Off
Sites
Start
History
WebSockets

Figure 10. Exploiting directory traversal to view the contents of the root directory.