**Lab: Reflected XSS into HTML context with most tags and attributes blocked**

Problem: in the search functionality but uses a web application firewall (WAF) to protect against common XSS vectors.

Goal: perform a [cross-site scripting](https://portswigger.net/web-security/cross-site-scripting) attack that bypasses the WAF and calls the print() function.

Solution:

1-

A screenshot of a web page

Description automatically generated

A black rectangular object with white text

Description automatically generated

2-dosen’t work

A screenshot of a computer

Description automatically generated

A screenshot of a social media post

Description automatically generated

3-

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

4-

A screenshot of a computer

Description automatically generated

A screenshot of a computer

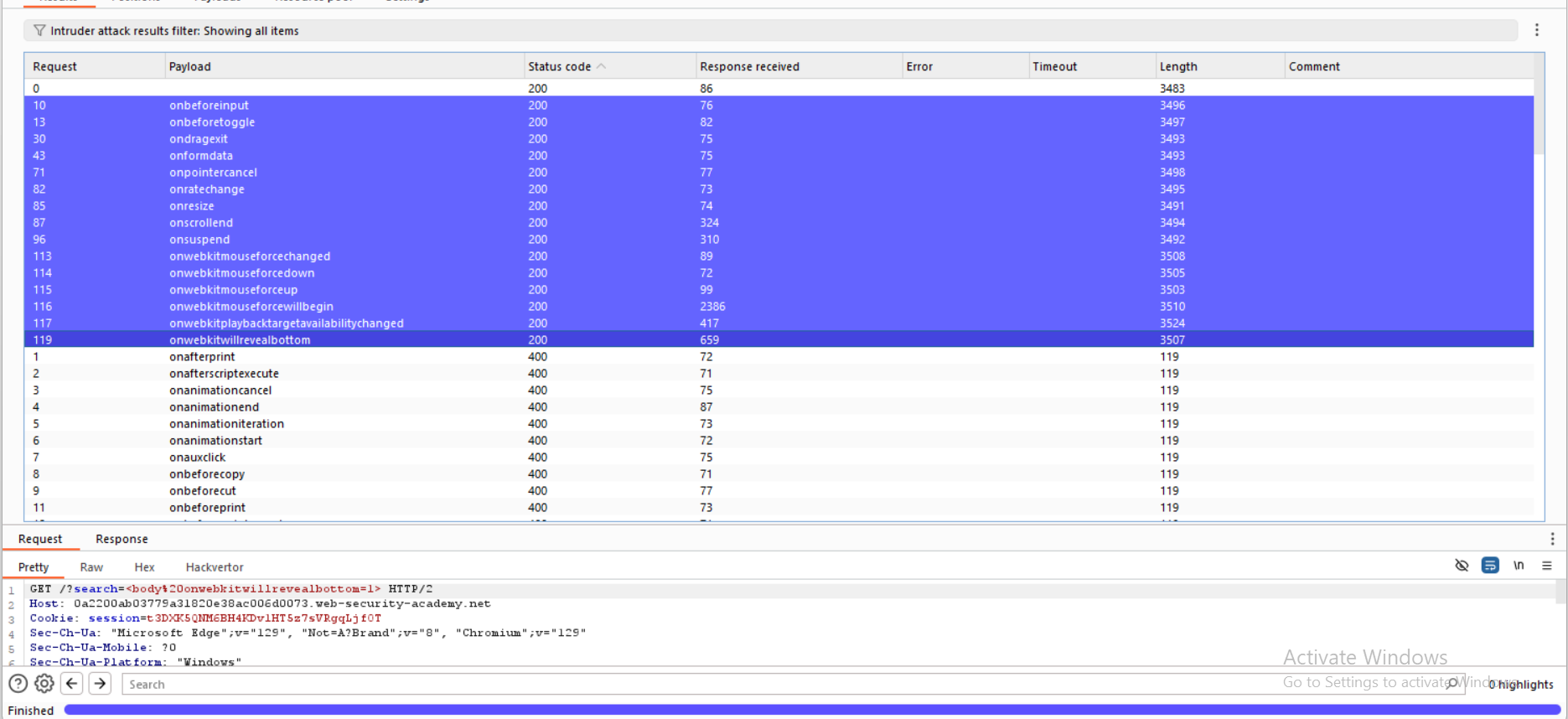
Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



5-

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated