**Report 1**

**Brute force attack using zaproxy**

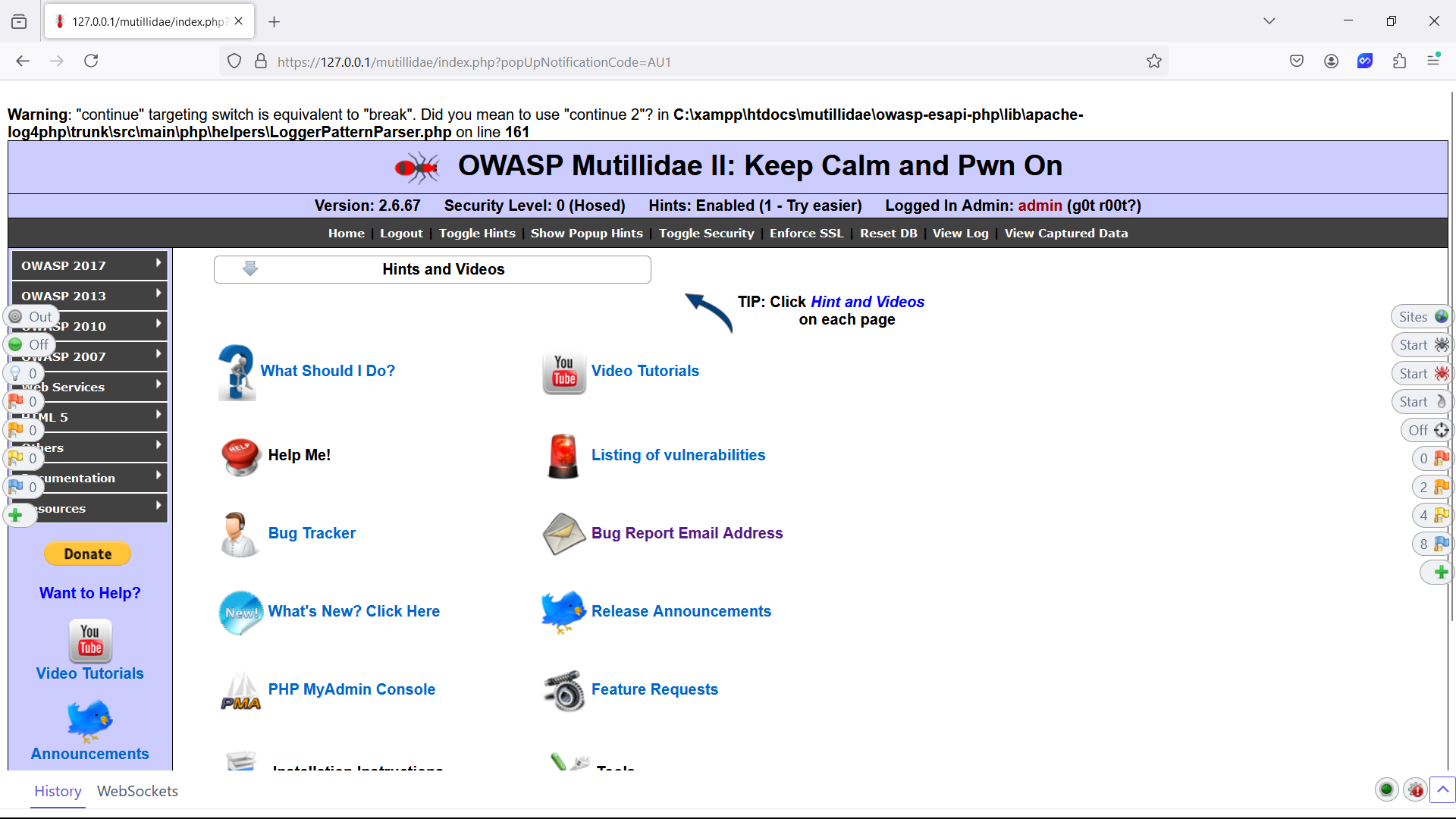
**Definition:**

A brute force attack is a method used to gain unauthorized access to systems or data by systematically trying all possible combinations until the correct one is found. In the context of passwords, for example, a brute force attack involves trying every possible password combination until the right one is discovered

**Website used**

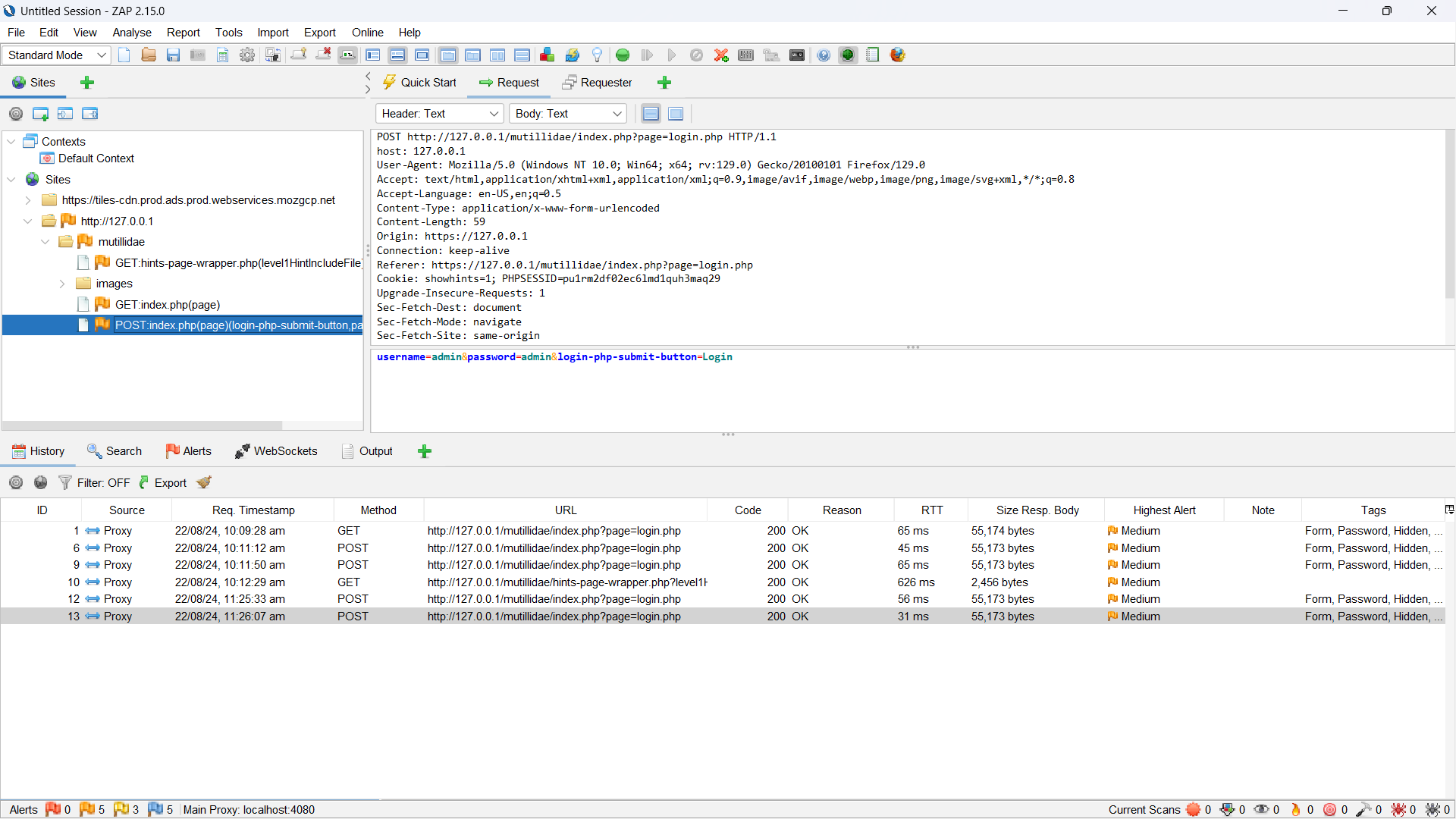
Mutillidae2:

It is a vulnerable site specifically created for pen testers



**Zaproxy version 15.01**

* Zap is a pen testing tool created by Simon Bennettsin 2010
* OWASP ZAP is an open-source security tool designed for finding vulnerabilities in web applications. It is maintained by the Open Web Application Security Project (OWASP). ZAP acts as a proxy between the user's browser and the web application, allowing it to intercept and analyze the traffic between them.

**Explanation:**

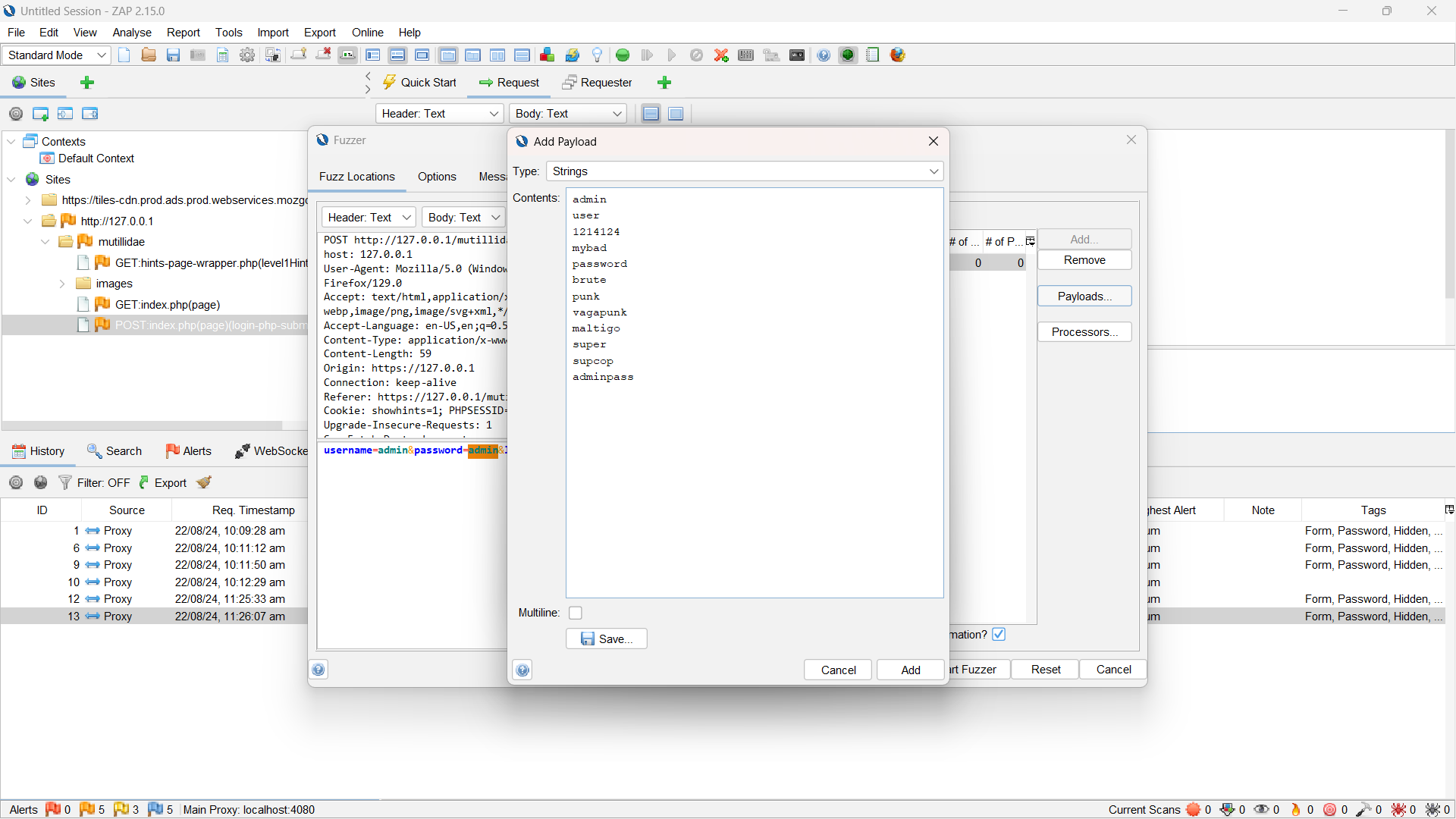
**Step1:**

Started with capturing the request by login with dummy id and

Password after that capturing the POST request from the browser

Injecting payload file to the browser

**Step2:**



After injecting payload file analyze the header of the response

If header length varies from another or different from sequence order

Can say that password have been found

