

# OWASP ZAP

## Task 1 Intro to ZAP

## Task 2 Disclaimer

## Task 3 Installation

## Task 4 How to perform an automated scan

## Task 5 Manual Scanning

## Task 6 Scanning an Authenticated Web Application

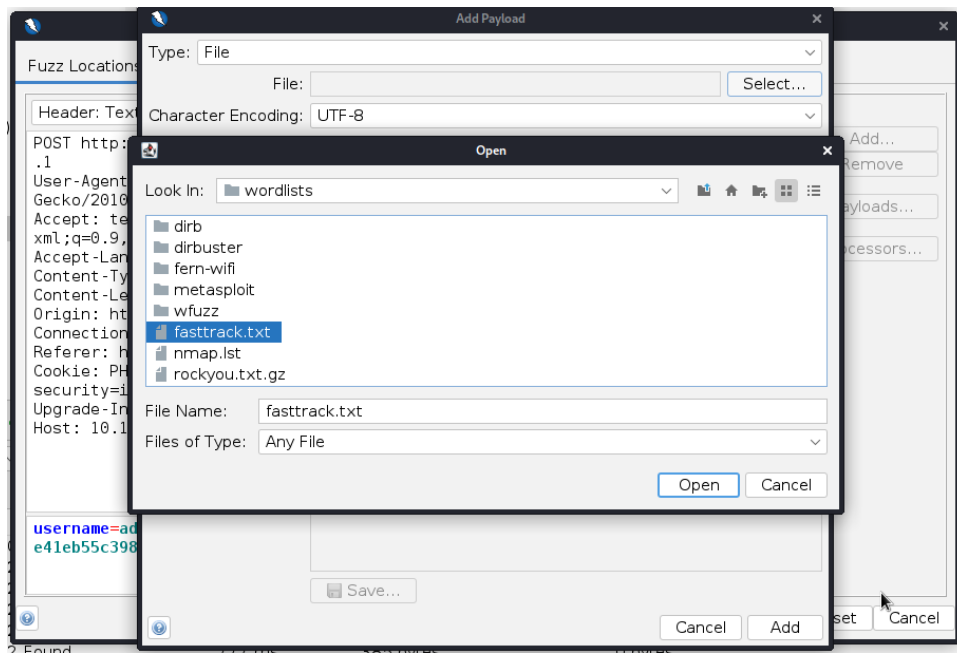
## Task 7 Brute-force Directories

Set the DVWA security is low

Go to the Brute Force page then send a request

The image shows two screenshots. The top screenshot is of the DVWA (Damn Vulnerable Web Application) interface, specifically the 'Vulnerability: Brute Force' page. The left sidebar contains a menu with options: Home, Instructions, Setup / Reset DB, Brute Force (highlighted), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, and SQL Injection (Blind). The main content area has a 'Login' form with 'Username:' and 'Password:' input fields and a 'Login' button. Below the form, a red error message states: 'Username and/or password incorrect. Alternative, the account has been locked because of too many failed logins. If this is the case, please try again in 15 minutes.' The bottom screenshot is of the OWASP ZAP (Zed Attack Proxy) interface, showing the 'Request' tab. The request is a POST to 'http://10.10.41.85/vulnerabilities/brute/' with a body containing login credentials and a token. The request headers include '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: 83', 'Origin: https://10.10.41.85', 'Connection: keep-alive', and 'Referer: https://10.10.41.85/vulnerabilities/brute/'. The request body is 'username=admin&password=aaa&Login=Login&user\_token=e41eb55c398d17110aca6c69e2408f3a'.

Click right mouse to the request -> attack -> fuzz and import file contain payload



Observe the payload that it is marked “ reflected “

☀ Reflected	password
	test
	testing
	Password1
	P@ssw0rd
	Password1!
	Password12
☀ Reflected	security
	security3

*Answer the questions below*

Use ZAP to bruteforce the DVWA 'brute-force' page. What's the password?

password

Correct Answer

## Task 9 ZAP Extensions

Set up add-on HUNT extension : Done

## Task 10 Further Reading