# **CTF Topic: Web Info gathering with urldna**



# **Introduction**



In this Capture The Flag (CTF) challenge, you will be using the tool urldna to perform web information gathering on the target. The objective is to explore the site and gather as much useful information as possible that could help in identifying potential vulnerabilities or gaining insights into the structure and content of the website.

# **Scenario**



Your task is to use urldna to gather detailed information about the target site. This includes identifying technologies used, extracting metadata, and more. Follow the steps below to perform the process effectively.

# **Process to Follow while Performing CTF**

Strep 1: Go through the ODIN tool which is linked above in the tool and requirement section: [**https://urldna.io/**](https://urldna.io/)

Step 2: Enter the target URL [**http://altoro.testfire.net**](http://altoro.testfire.net)

Step 3: Now identify the flag and solve it

# 

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the user agent used by the target website?

Answer: **Mozilla**

Flag 2: Which ISP is hosting the target website?

Answer: **Rackspace**

Flag3: Which server is running on the target system?

Answer: **Apache Coyote 1.1**

Flag 4: is there any vulnerability on the server version, if yes what is that vulnerability?

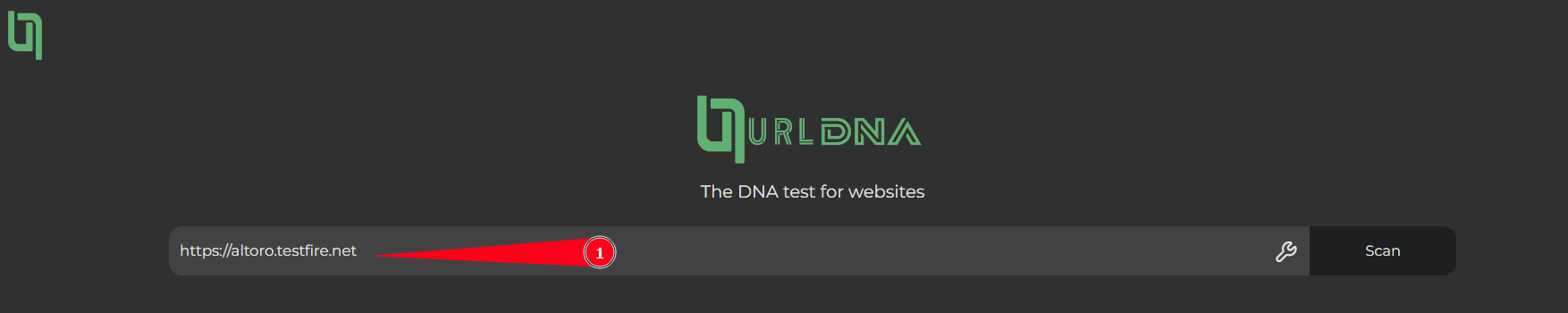
Answer: **remote attack**

Flag 5: which programming language is used by the target website?

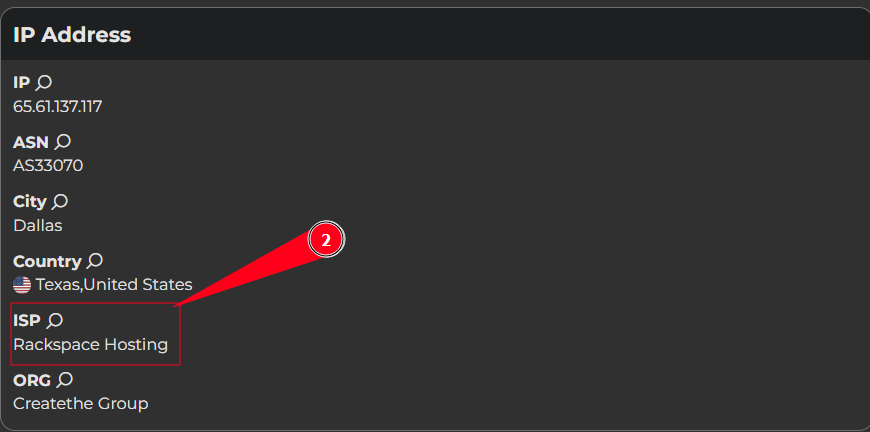
Answer: **Java**

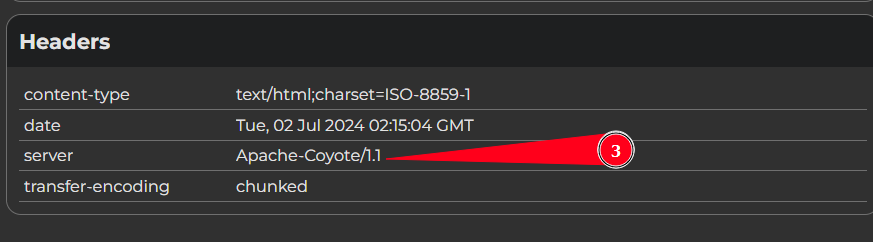
# 

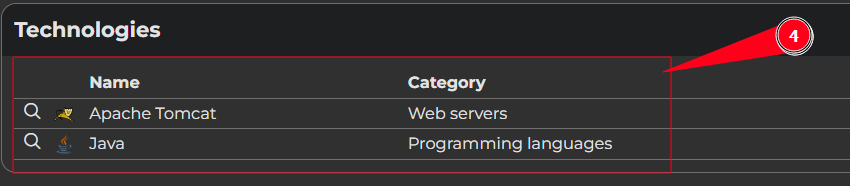
# **Hint**

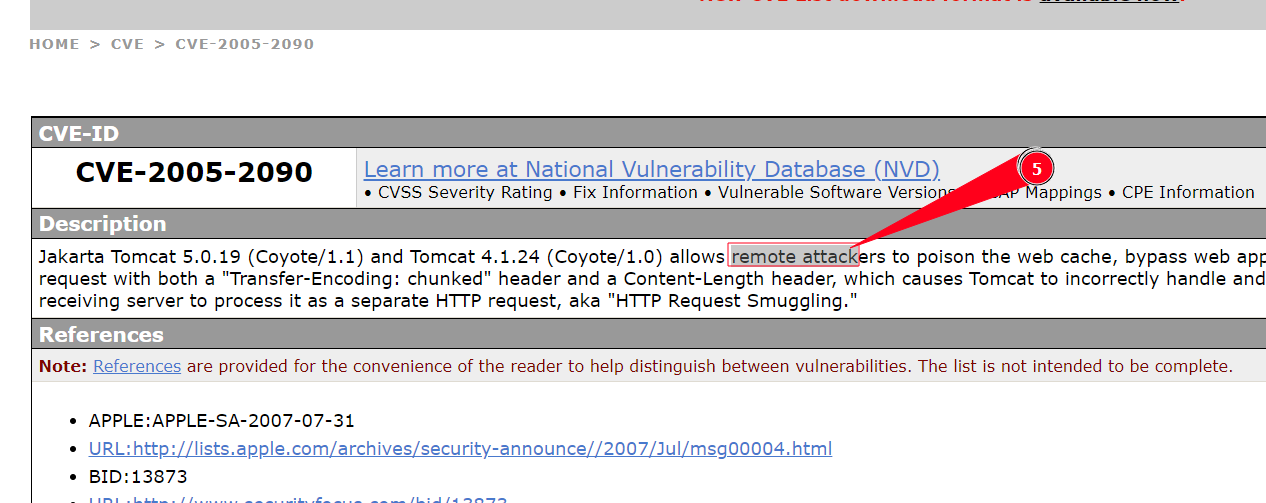










****