# **CTF Topic: URL FIZZING**

# **Introduction**

In this CTF challenge, participants will perform URL fizzing, also known as directory brute forcing or URL enumeration, a technique used in penetration testing to discover hidden directories and files within a web server. This is often accomplished by trying out common directory and file names to see if they exist. The goal is to uncover potentially vulnerable or sensitive information not intended to be public.

# **Tools and requirements**

* [Pentest Tool](https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files)

# **Link (File)**

Target: <http://testphp.vulnweb.com/>

# **Scenario**

Imagine you are a penetration tester assigned to perform a security assessment of a web application hosted at http://testphp.vulnweb.com/. Your task is to discover hidden directories and files using URL fuzzing techniques.

# **Process to Perform**

* Go through the pentest too which is linked above on the tool and requirement section
* Then input the target which is on the link and answer according to the question

# **Let's Begin The Challenge**

# **Question**

Flag 1: What is the project version?

Answer: 4

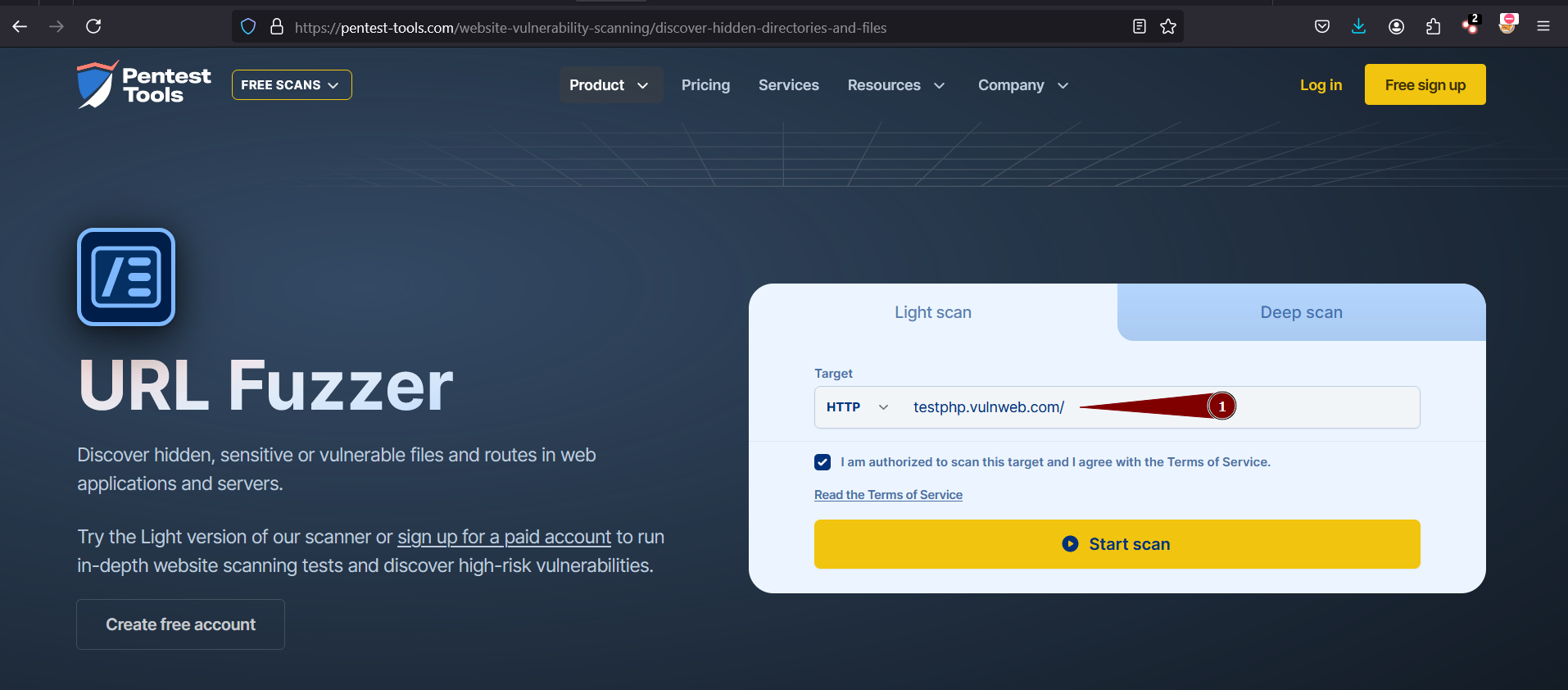
Flag 3: How many artists are registered on the website?

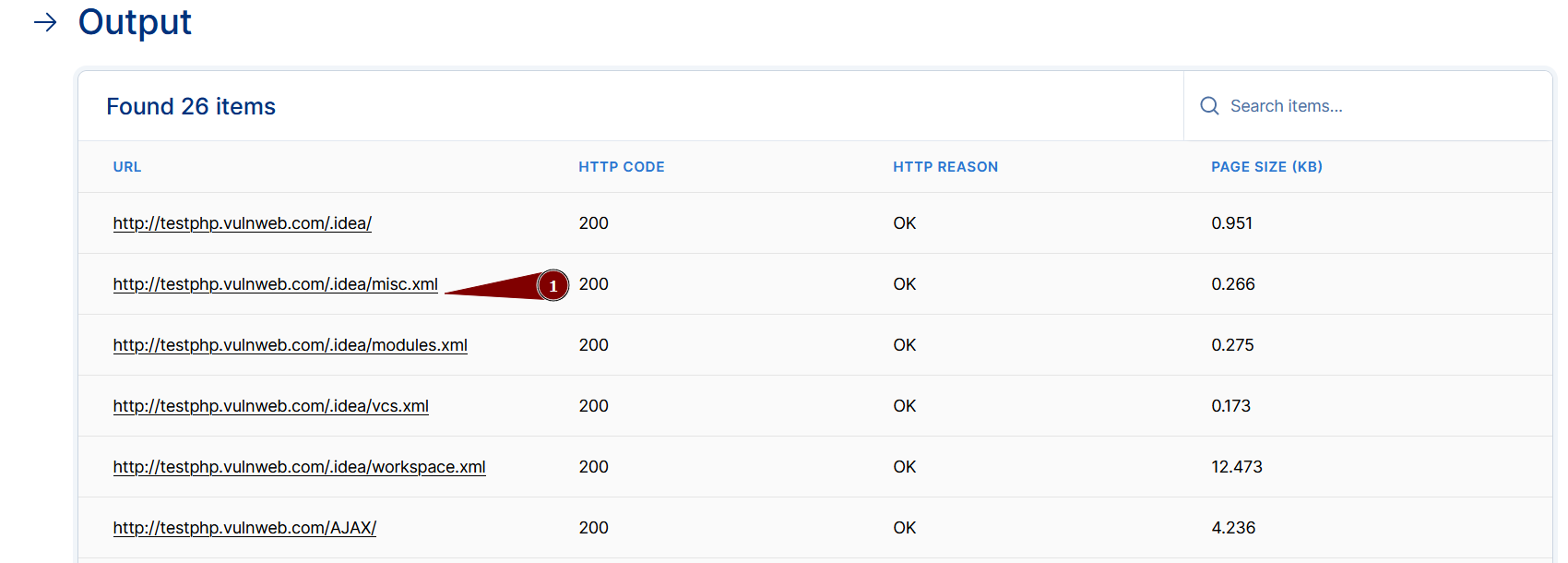
Answer: 3

flag3: In which directory is the credentials.txt file stored?

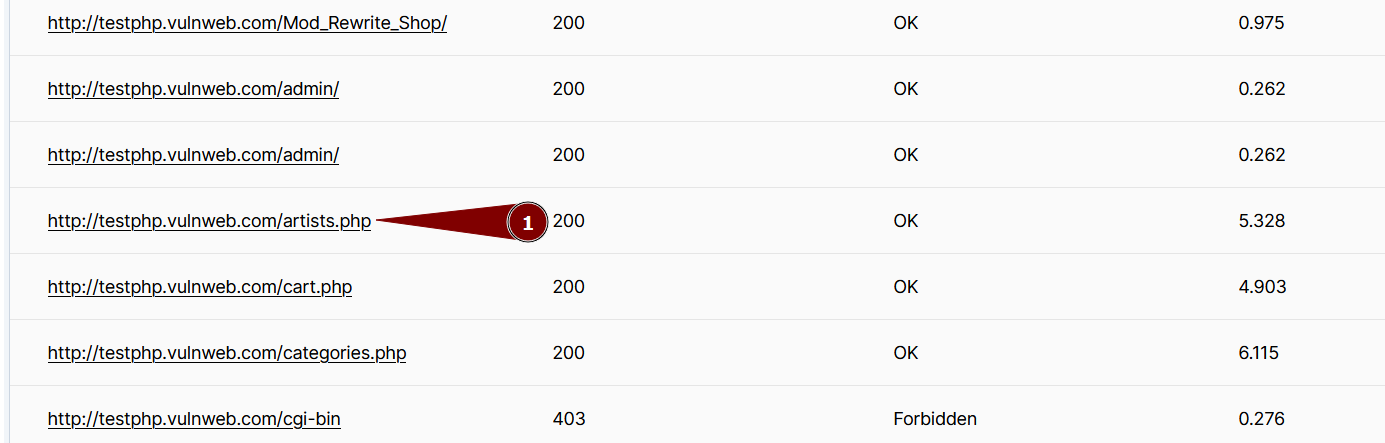
Answer: picture

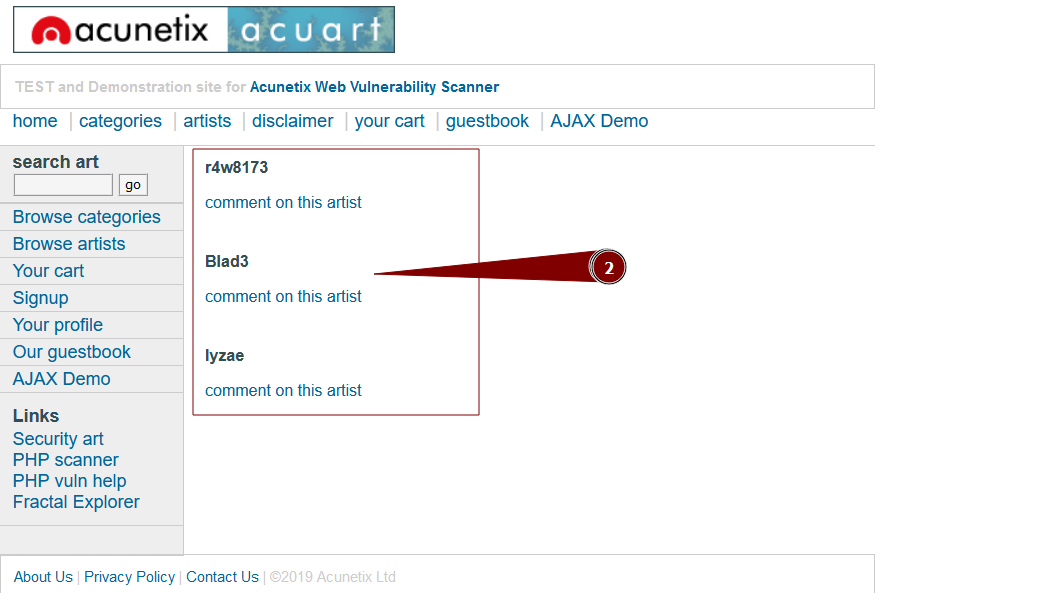
# **Hint**

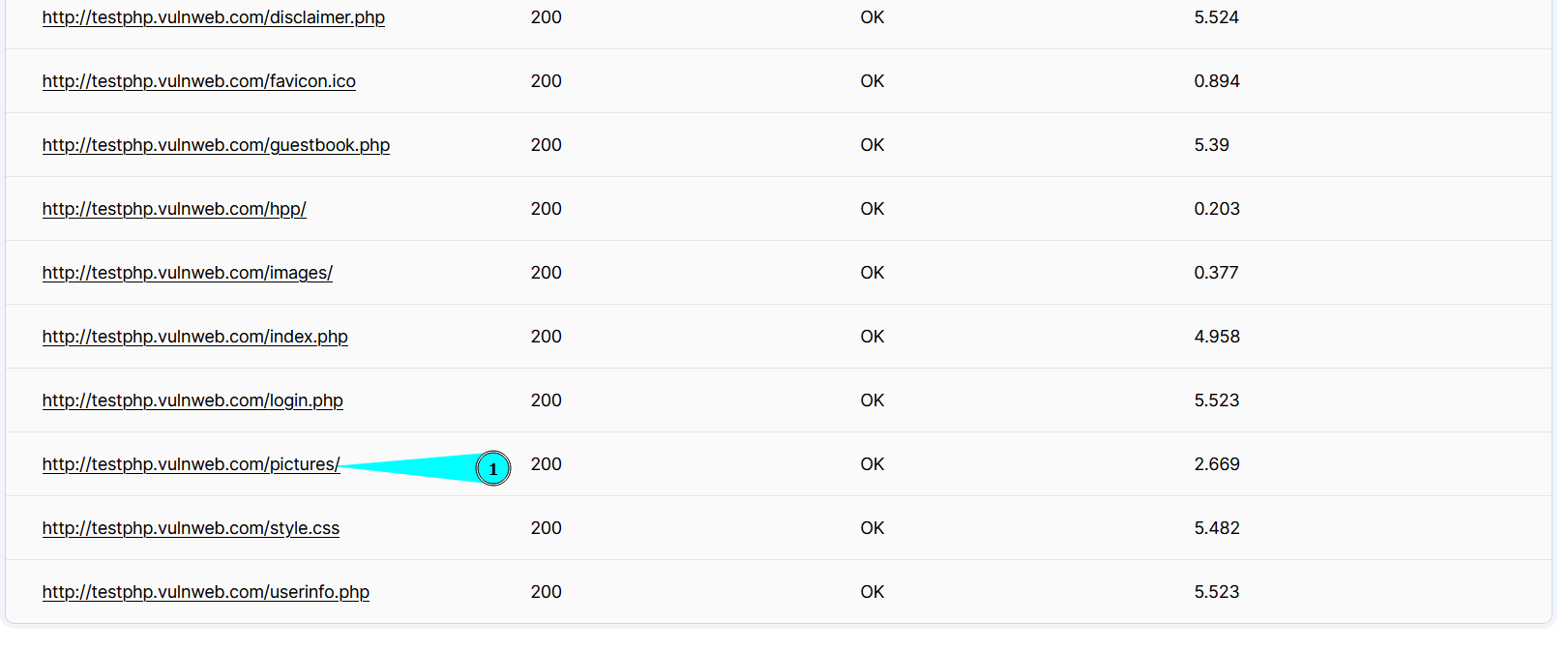


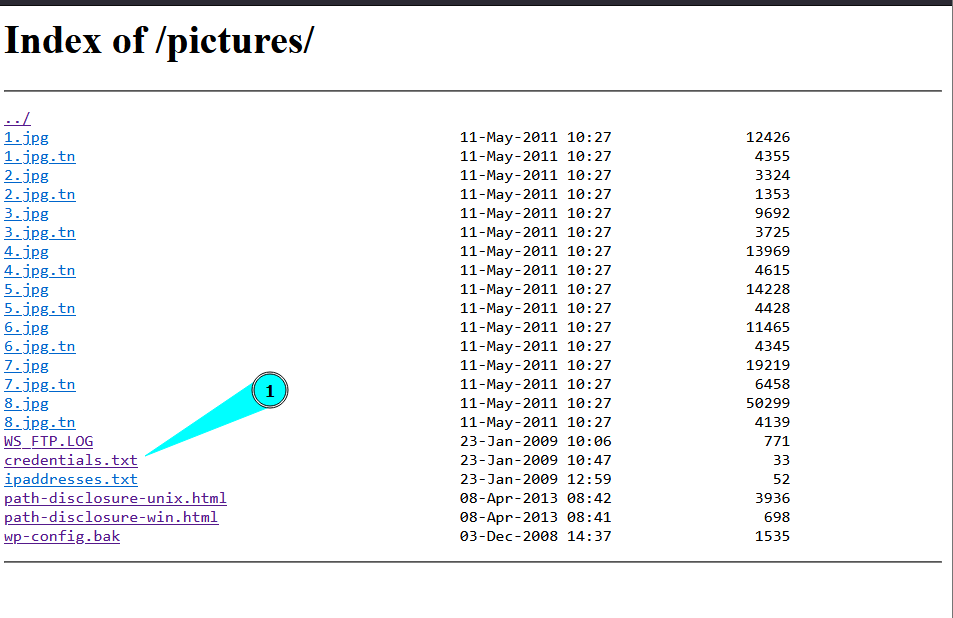
****

****

****

****

****

****