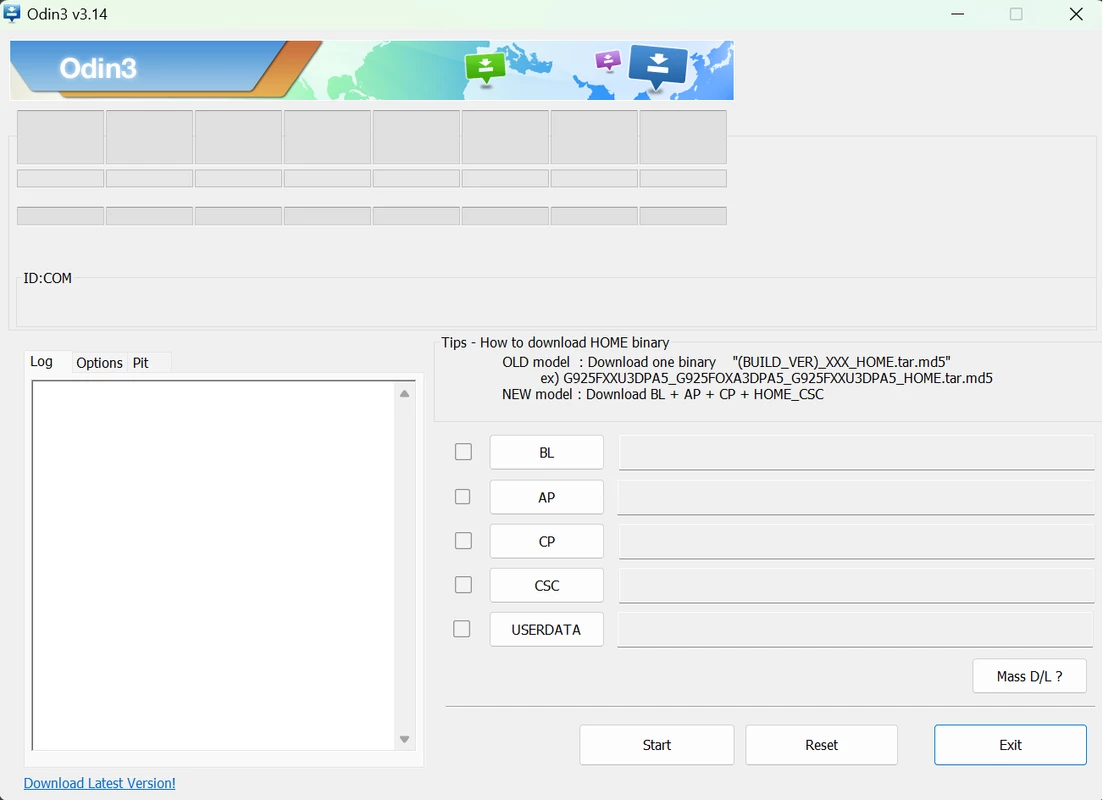
# **CTF Topic: Scanning Target With ODIN**



# **Introduction**



In Capture The Flag (CTF) challenges and real-world cybersecurity assessments, scanning a target system is a critical detail. ODIN is a comprehensive tool that can perform a wide range of scans to gather information about a target system. This guide will explain how to use ODIN to scan a specific target.

# **Tools and requirements**

* [ODIN](https://getodin.com/)

# **Link**

Target: 65.61.137.117

# **Scenario**

In this scenario, we will use ODIN to perform a comprehensive scan on the target IP address 65.61.137.117. The goal is to gather as much information as possible about the targets.

# **Process to Perform**

* Go through the ODIN tool which is linked above in the tool and requirement section
* Click on the search
* then enter the target IP on the search box

# **Let's Begin The Challenge**

# **Question**

Flag1: What is the version used by the HTTP service Apache Tomcat/Coyote JSP engine?

Answer: 1.1

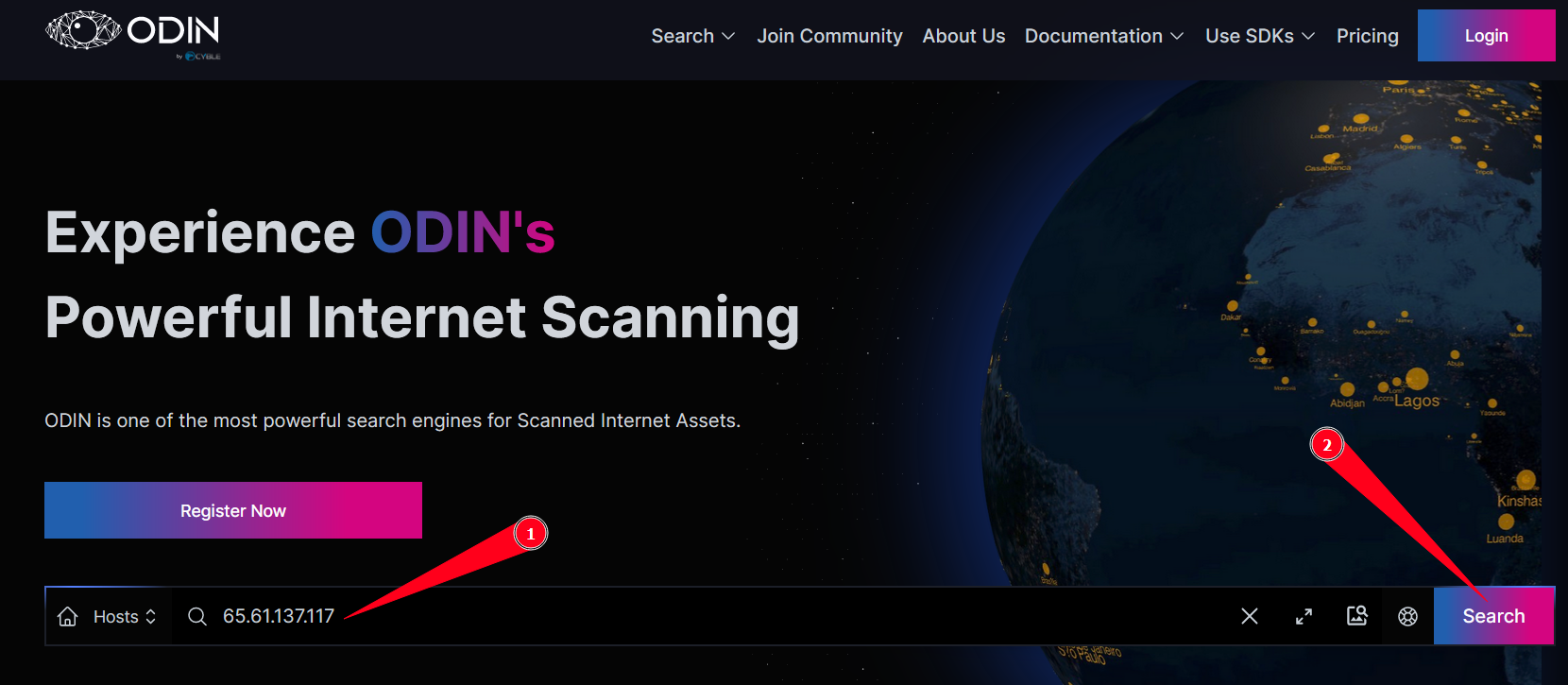
Flag 2: what is the code of asn organization?

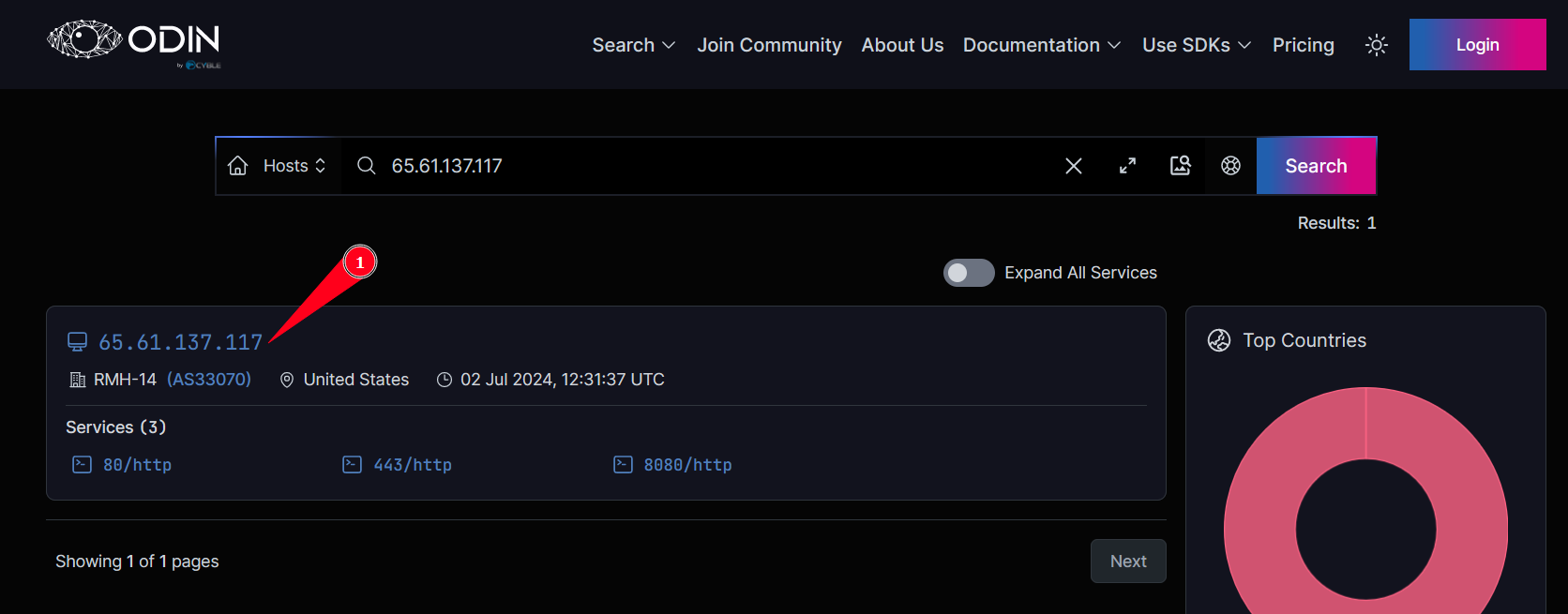
Answer: RMH-14

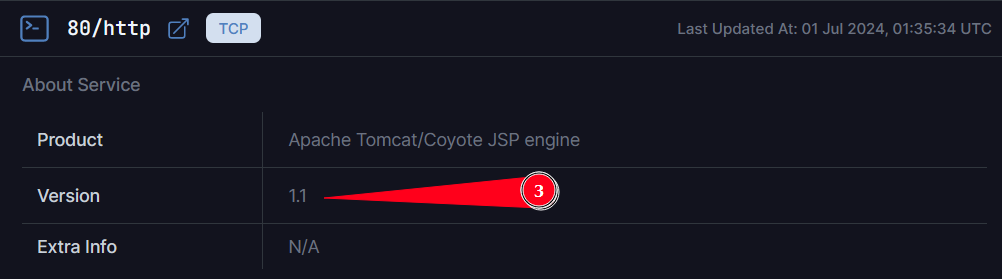
Flag 3: What is the Body SHA256 Hash of a target?

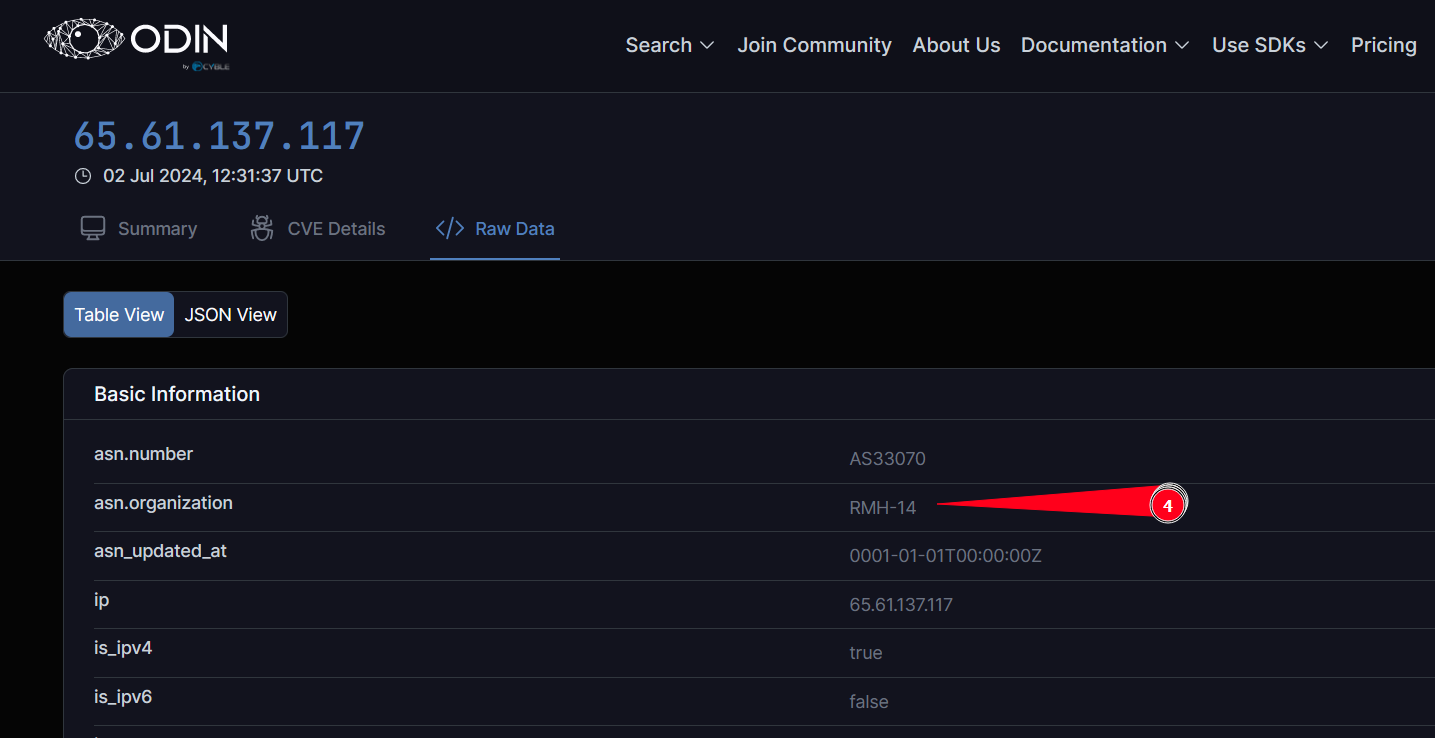
Answer:ab96445e2230ac2e6fe13654ac058dc051f3d49655821f9fa09b5a22863cf635

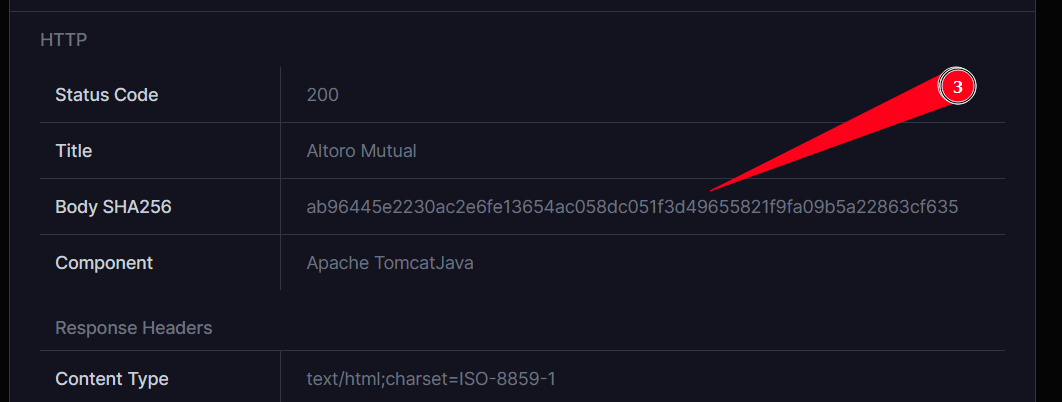
# **Hint**



****

****

****

****