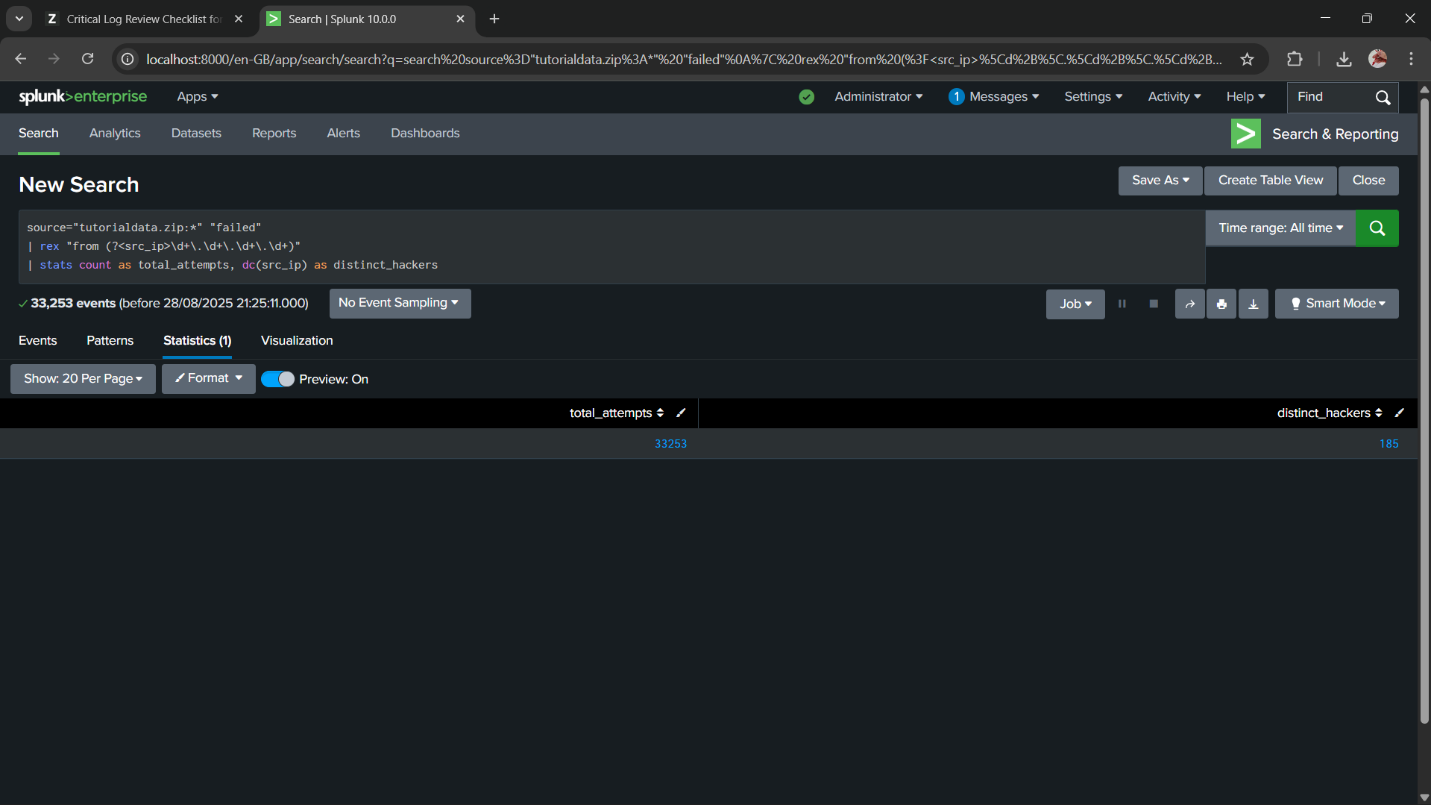
Com Sec Act 2 Splunk

Q1. How many hackers are trying to get access to our servers? And how many

attempts are there? Explain/define how you count distinct hackers.

ANS: #hacker=185, #attempt=33253

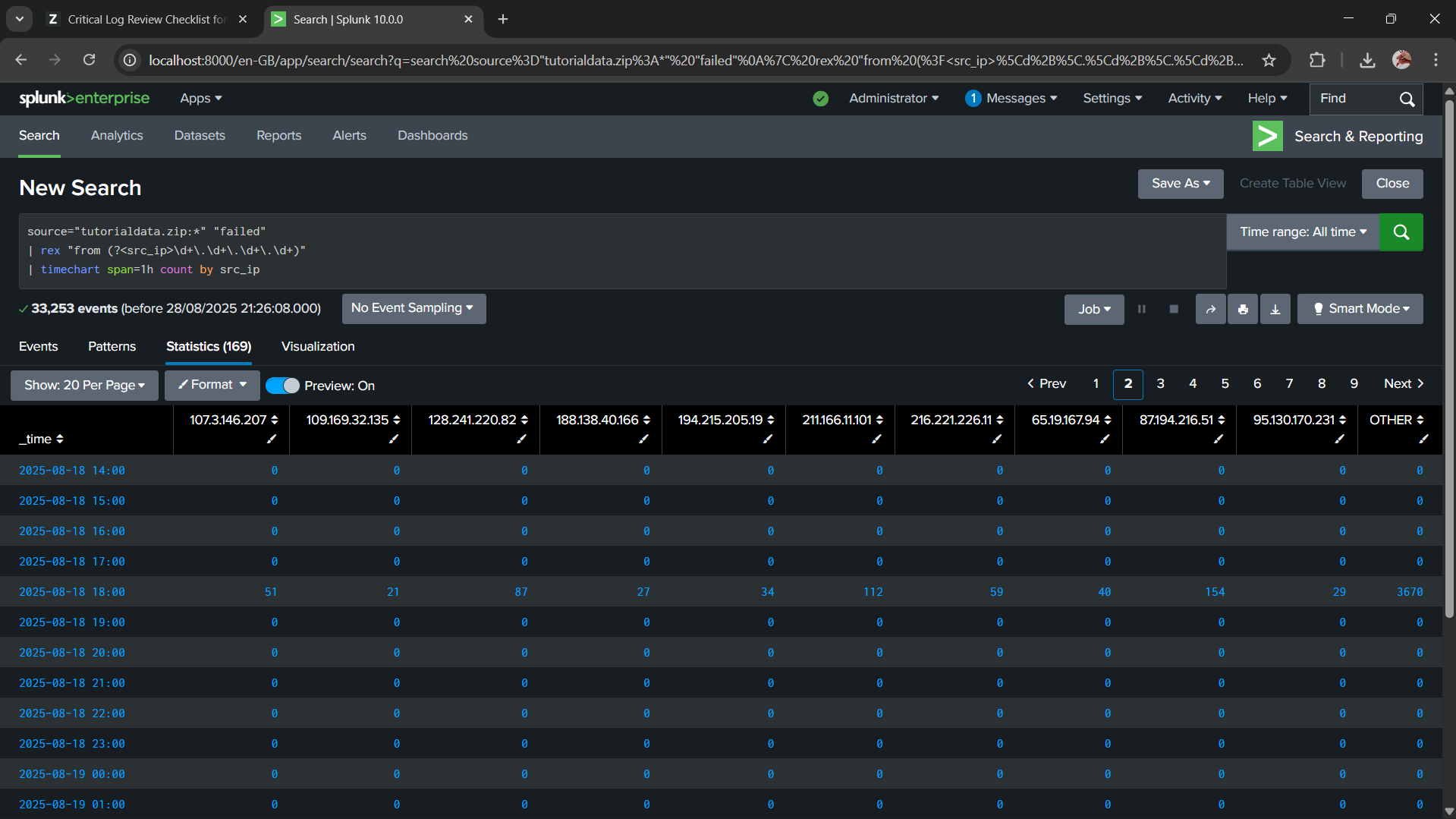
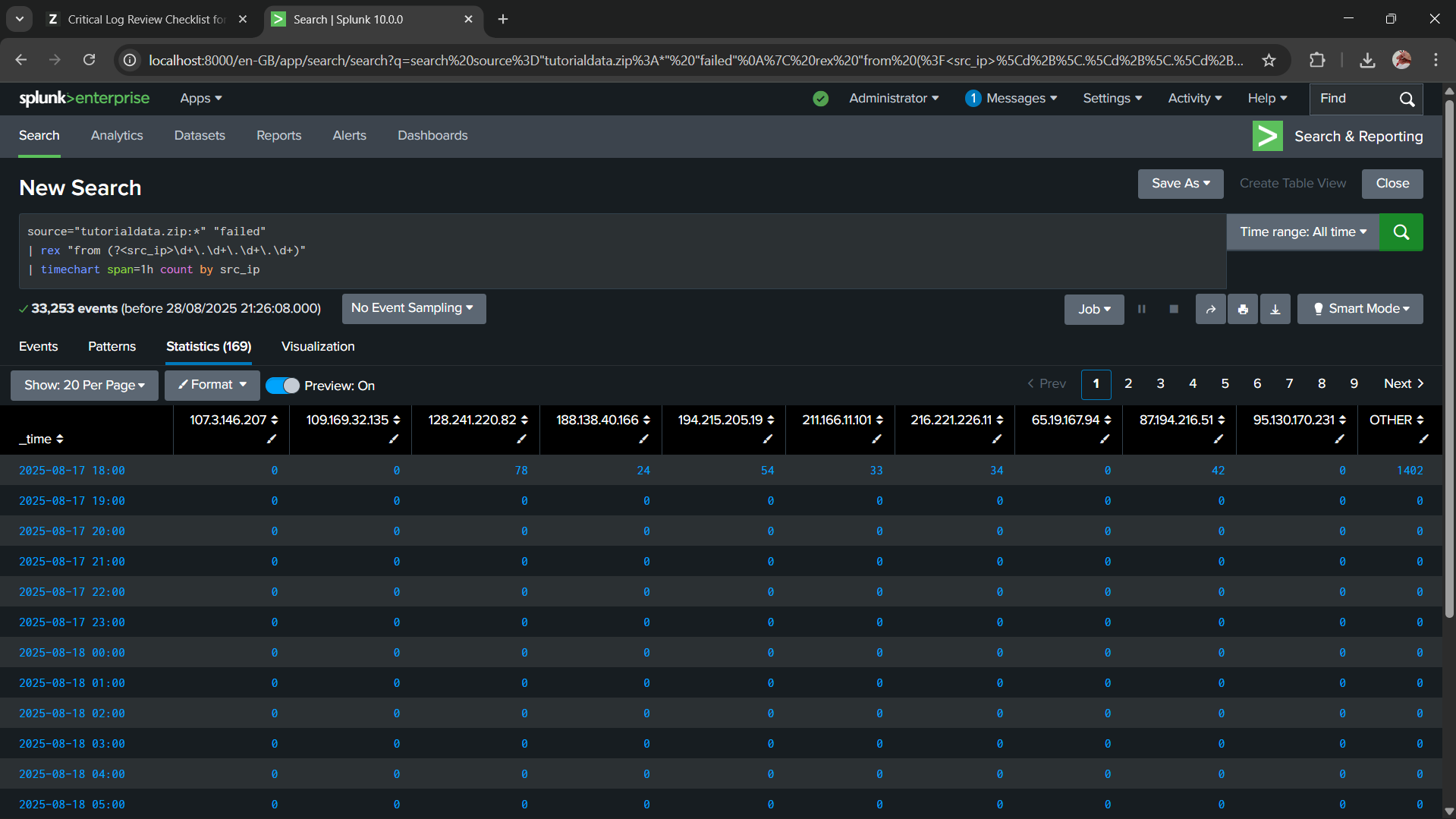


Q2. What time do hackers appear to try to hack our servers?

ANS: 2025-08-17 18:00, 2025-08-18 18:00, 2025-08-19 18:00,

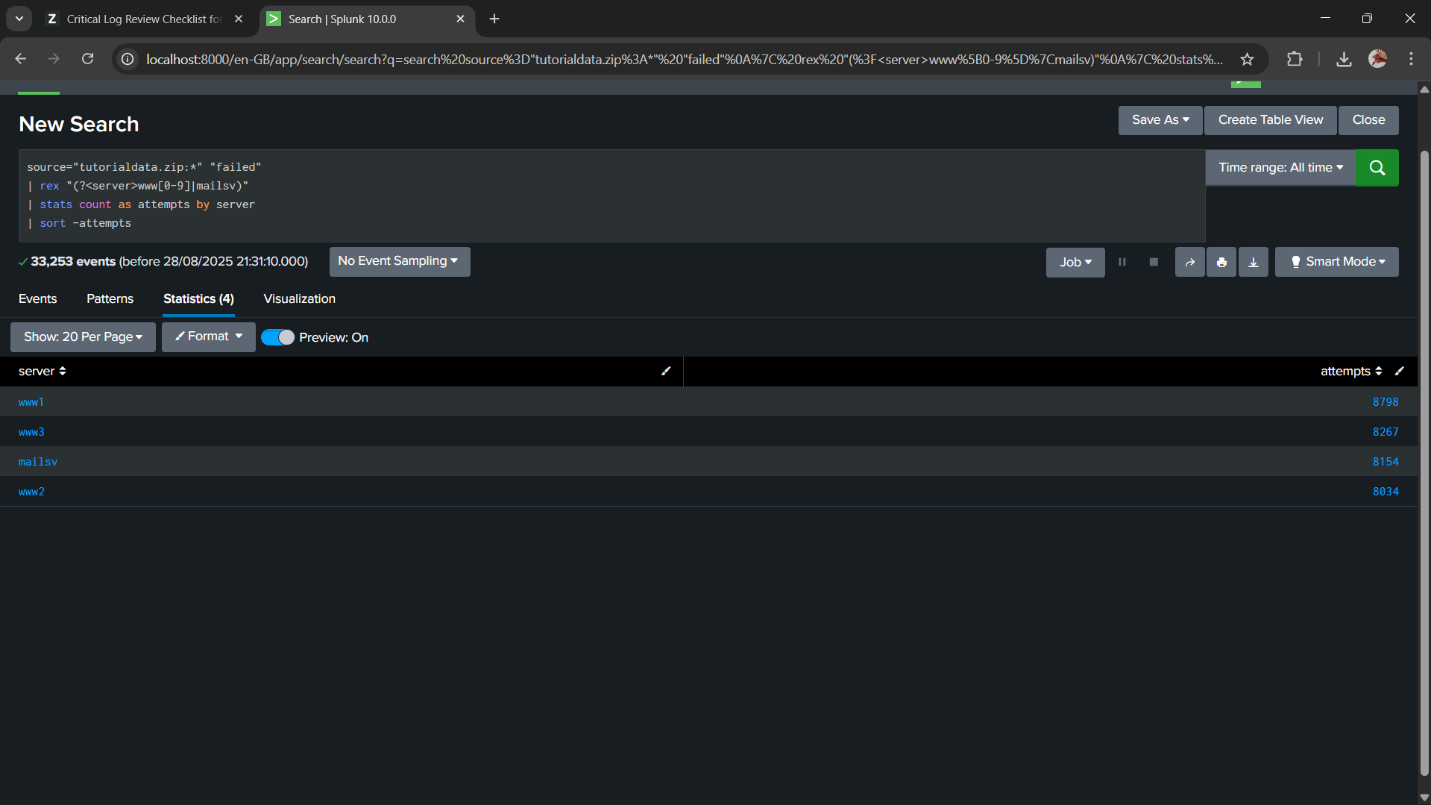
2025-08-20 18:00, 2025-08-21 18:00, 2025-08-22 18:00,

2025-08-23 18:00, 2025-08-24 18:00



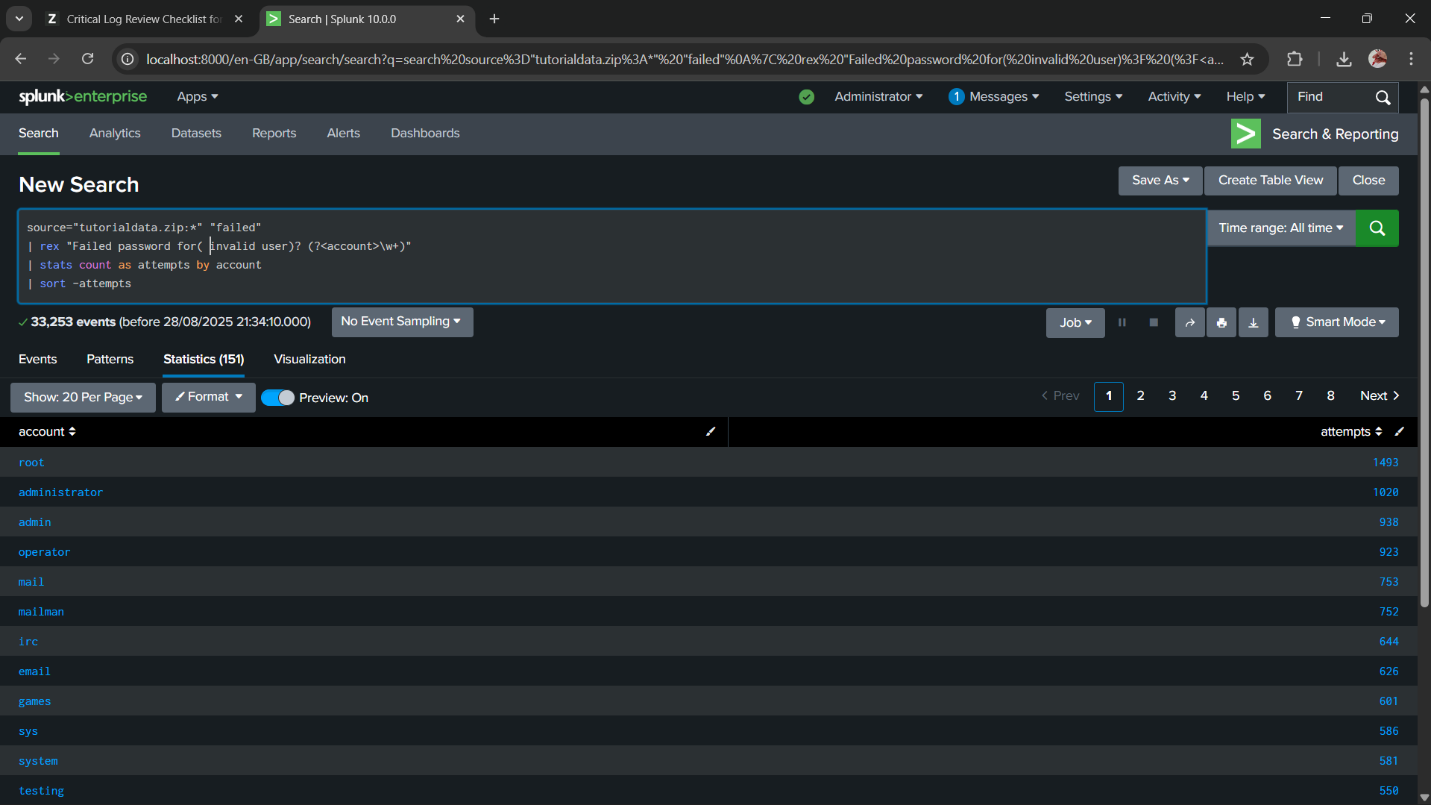
Q3. Which server (mailsv, www1, www2, www3) had the most attempts?

ANS: www1



Q4. What is the most popular account that hackers use to try to break in?

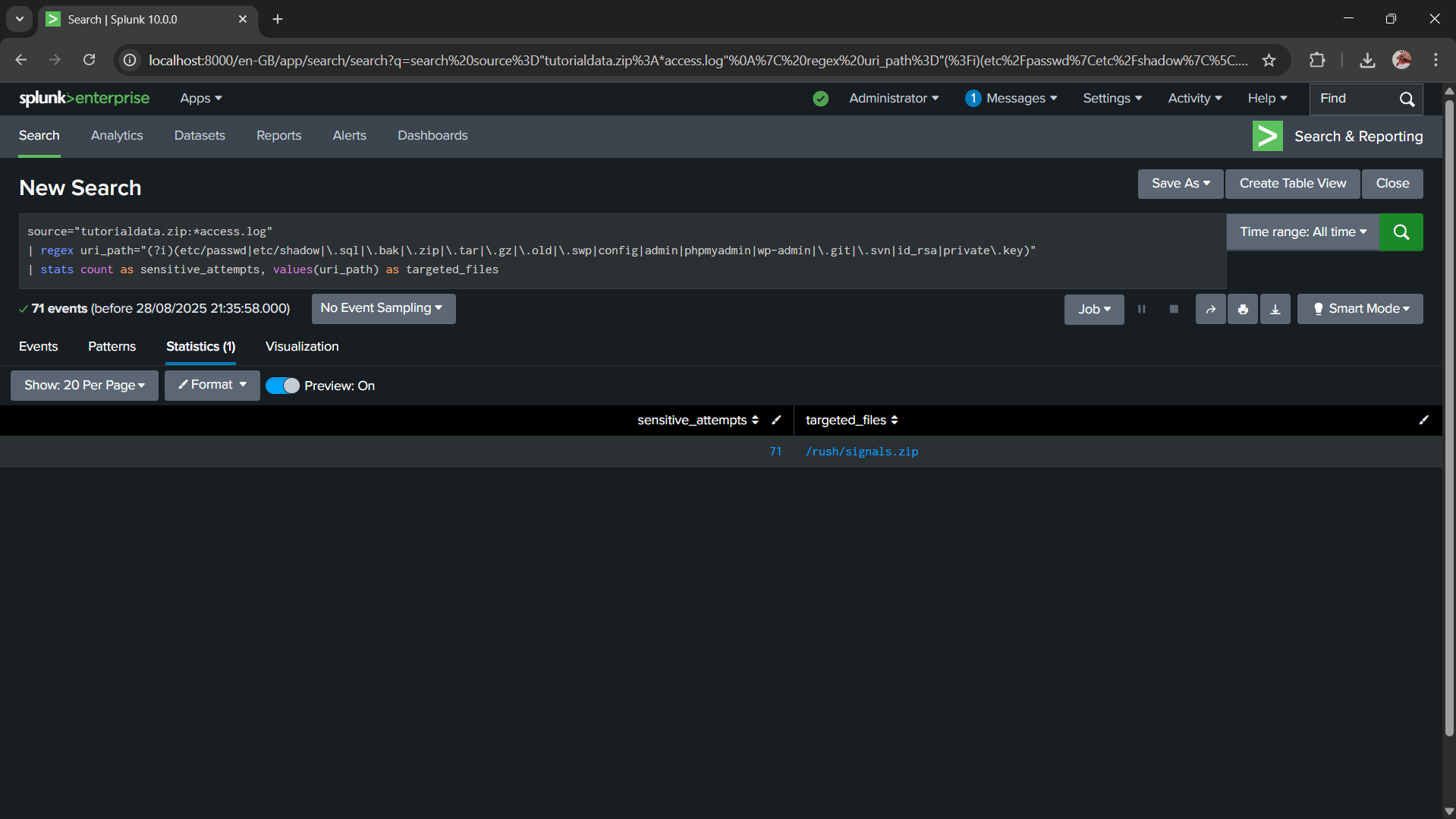
ANS: root



Q5. Can you find attempts to get access to sensitive information from our web

servers? How many attempts were there?

ANS: 71 times

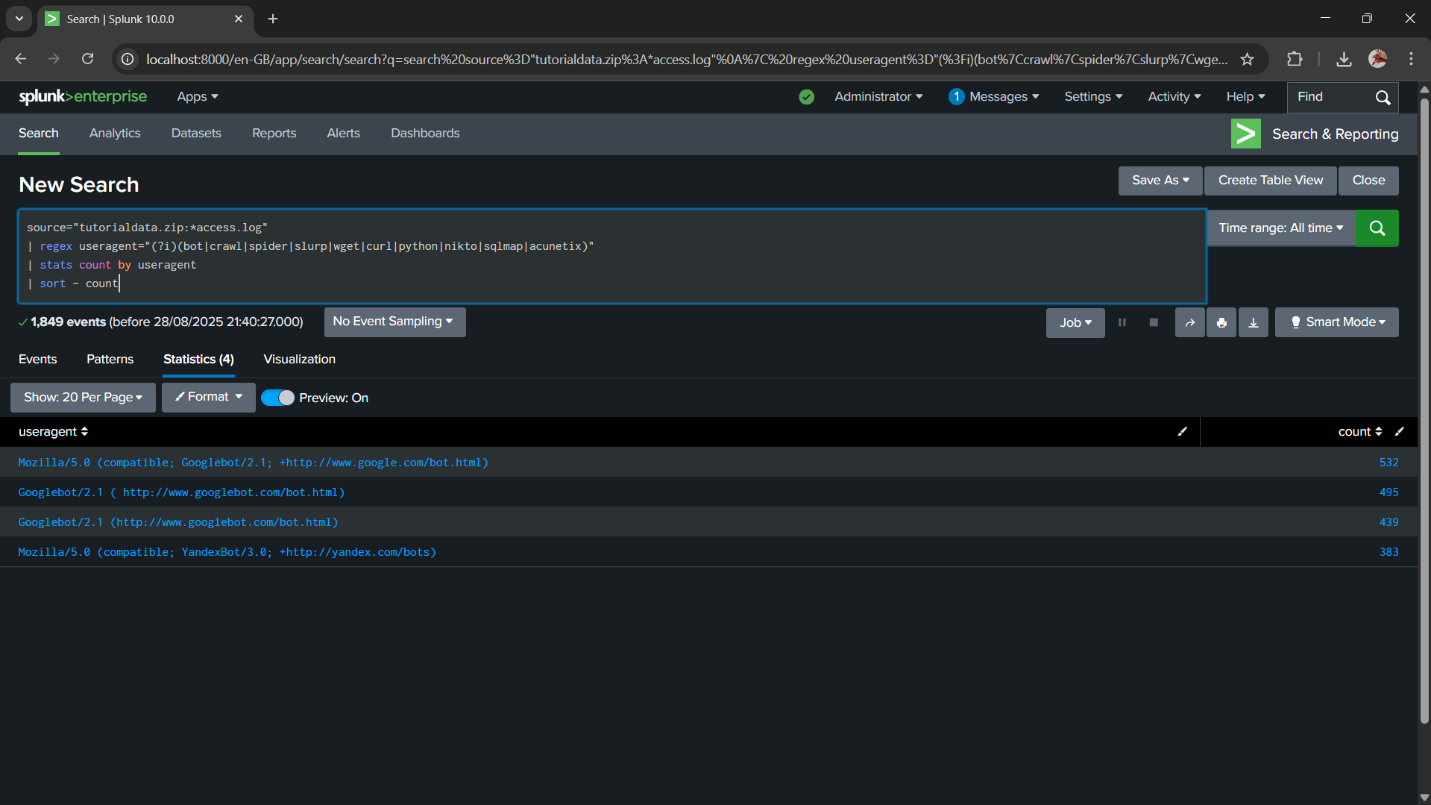


Q6. What resource/file are hackers looking for?

ANS: /rush/signals.zip

Q7. Can you find any bots crawling our websites?

ANS: YES



Q8. What are they doing on the site? (Hint: Look for User-Agent in the web access.logs.)

ANS: Bots are crawling the site to index pages for search engines.