API Security Bootcamp
Hands-On OWASP Top 10 for APIs

Dr. Sunny Wear

2023

#3 Excessive Data Exposure

Finding secrets, passwords, API tokens

Excessive Data Exposure

Definition: Exposure of all object properties containing individual sensitivity

Examples: Responses showing secrets, passwords, access tokens

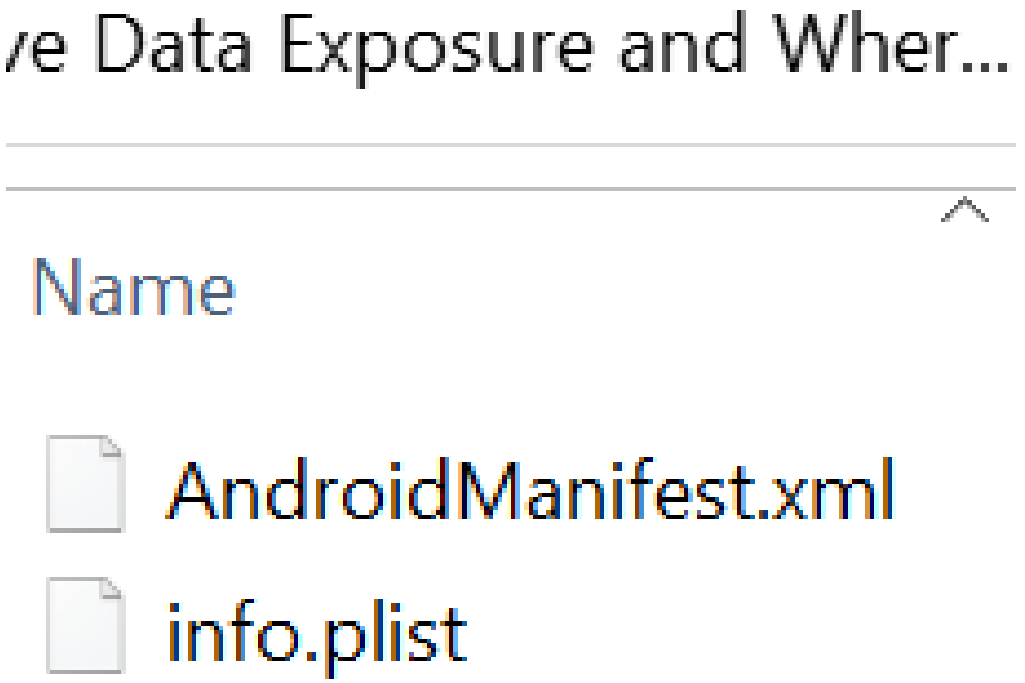
Mobile Health Apps Systematically Expose PII and PHI Through APIs, New Findings from Knight Ink and Approov Show

- "Of the 30 popular apps Knight Ink tested, 77 percent contained hardcoded API keys, some of which don't expire, and seven percent contained hardcoded usernames and passwords."
- *https://www.bloomberg.com/press-releases/2021-02-09/mobile-health-apps-systematically-expose-pii-and-phi-through-apis-new-findings-from-knight-ink-and-approov-show*

Excessive Data Exposure

Exercise 3-1: Find the Data Exposure Issues

- Unzip the Exercise1_Files zip file
- Open each file in Notepad++ and try to identify the excessive data exposure issue



Code 39 Bytes

```
1  req.Header.Add("x-api-key", "[redacted]")
```

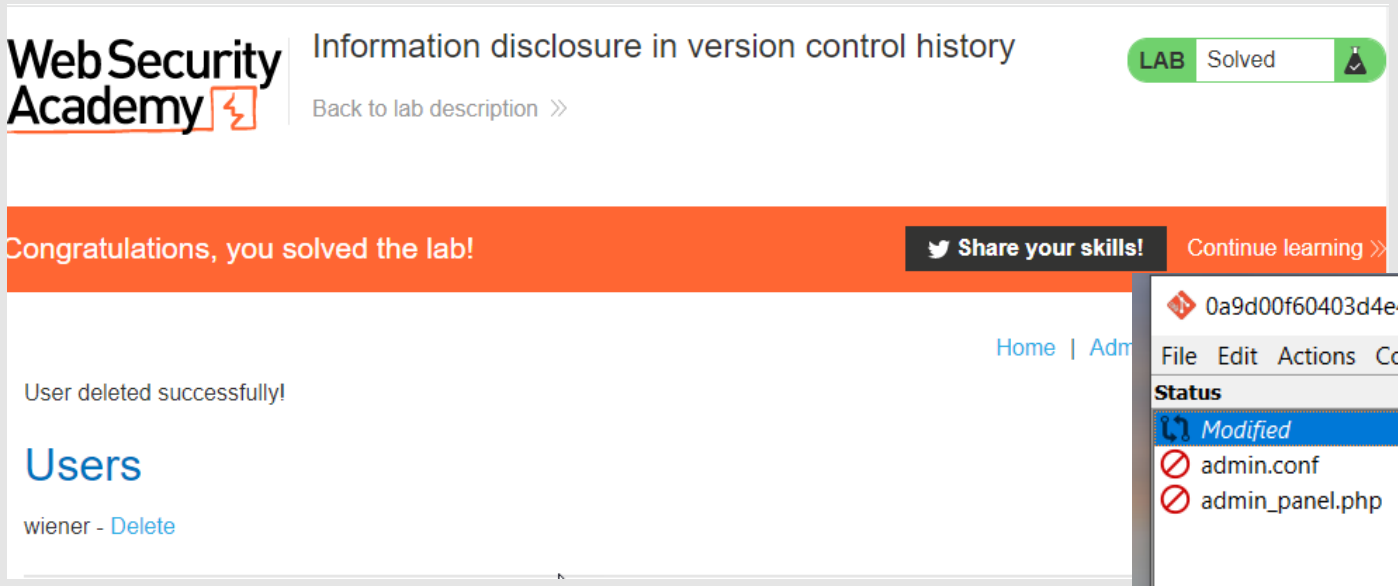
Hard coded API Keys in Source Code

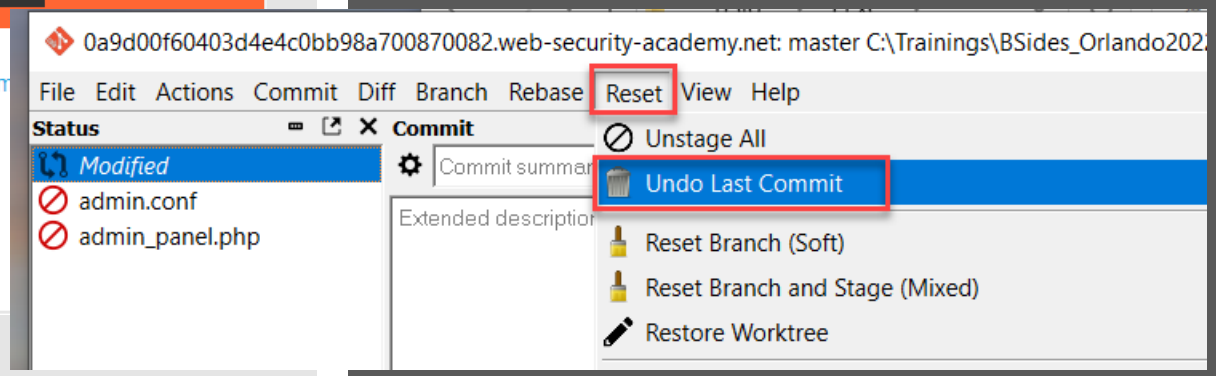
- If software is open-sourced, check github
- Check config files when reverse engineering mobile apps
- Attempt path traversal to try to view/download config files

```
        <meta-data
            android:name="io.fabric.ApiKey"
            android:value="12ac6e94f850aaffcdf[redacted]415d06a43" />
    </application>

</manifest>
```

Exercise 3-2: Information Disclosure in Version Control History





- Burp Web Academy lab found in the **Information Disclosure** labs
- You will need wget and git cola (zip files available)

Exercise 3-3: Sensitive Data Exposure

Lab: User ID controlled by request parameter with data leakage in redirect

APPRENTICE

This lab contains an access control vulnerability where sensitive information is leaked in the body of a redirect response.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.