



Lesson 18

SECURITY AND AUDITING

Hikmah Nisya - 1103184094
Radzis Araaf Jaya Jamaludin - 1103184234
Raudhatul Rafiqah Assyahiddini - 1103180225

Audit

Audit merupakan proses peninjauan terhadap code kita dengan berfokus pada keamanan untuk mencari apakah ada masalah dengan code kita. Ketika kita mengirimkan kode, kita tidak boleh hanya mengatakan kepada seorang auditor bahwa bisakah melakukan pemeriksaan dan memastikan bahwa code ini sudah benar, karena hal itu menyebabkan kurangnya informasi yang diterima oleh auditor. Auditor harus mengetahui dengan mudah tentang apa fungsi dari code yang telah dibuat, serta seperti apa cara kerja dari code tersebut. Jika code sangat buruk, maka auditor pasti akan mengetahui semua kesalahan-kesalahan yang ada.

Alasan untuk melakukan audit keamanan.

1. untuk mengidentifikasi masalah dan celah keamanan serta kesalahan sistem.
2. untuk mematuhi kebijakan keamanan organisasi internal.
3. untuk mematuhi persyaratan peraturan eksternal.
4. untuk mengetahui apakah adanya pelatihan mengenai keamanan sudah memadai.
5. untuk identifikasi sumber daya yang tidak diperlukan.
6. untuk menetapkan dasar-dasar tentang keamanan yang dapat dibandingkan dengan audit untuk masa mendatang.

Types Of Security and Audits

1. Internal Audits

Pebisnis menggunakan sumber dayanya sendiri dan departemen internal digunakan Ketika sebuah kelompok ingin melakukan validasi sistem bisnis pada kepatuhan keijakan dan prosedur yang ada.

2. External Audits.

Kelompok yang berasal dari luar dibawa kedalam untuk melakukan proses audit, dimana audit eksternal ini juga dilakukan Ketika sebuah kelompok perlu memastikan bahwa suatu hal itu sudah sesuai dengan standar industry dan peraturan pemerintah.

What system does an audit cover

Beberapa sistem yang sebelumnya akan digunakan, dapat dilakukan pemeriksaan kerentanan pada beberapa area seperti berikut:

1. network vulnerabilities.
2. security controls.
3. encryption.
4. software systems.
5. architecture management capabilities.
6. Telecommunications controls.
7. systems development audit.
8. information processing.

An Auditors Process

1. melakukan atau menjalankan test.
2. membaca spesifikasi atau dokumen.
3. menjalankan tools (seperti slither, linter, analisis statis, dll).
4. melakukan analisis secara manual.
5. menjalankan tools (seperti echidna, manticore, eksekusi simbolis, dan mitosX)
6. mendiskusikan (jika ada step yang perlu di ulangi, maka silahkan diulangi sesuai kebutuhan).
7. menulis laporan.

Membuat Slither

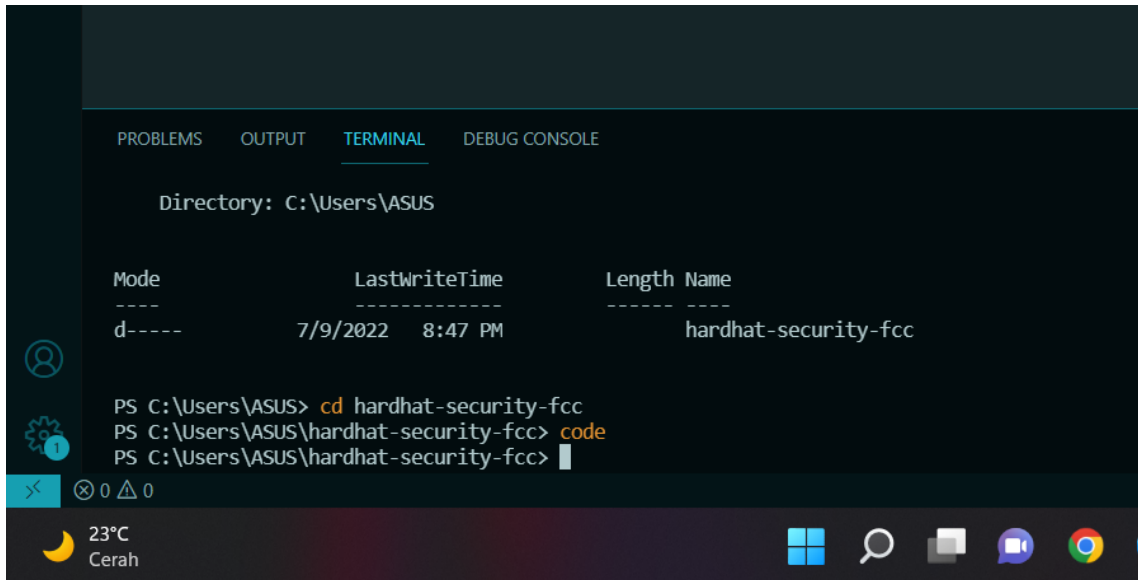
Pertama kita perlu membuka VsCode.

Kedua kita membuat direktori baru dengan perintah “mkdir hardhat-security-fcc”, setelah itu kita perlu masuk ke direktori tersebut dan membuat code.

Selanjutnya melakukan clone, gunakan perintah “git clone

<https://github.com/PatrickAlphaC/hardhat-security-fcc>.”

Maka selanjutnya kita akan menemukan apapun yang kita inginkan di dalam direktori tersebut.



The screenshot shows a Windows terminal window with the following content:

```
Directory: C:\Users\ASUS
```

Mode	LastWriteTime	Length	Name
d-----	7/9/2022 8:47 PM		hardhat-security-fcc

```
PS C:\Users\ASUS> cd hardhat-security-fcc
PS C:\Users\ASUS\hardhat-security-fcc> code
PS C:\Users\ASUS\hardhat-security-fcc>
```

The terminal window also shows the Windows taskbar at the bottom with the date 7/9/2022, time 8:47 PM, and weather 23°C Cerah.

Step involved in a security audit

1. agree in goals (melibatkan semua kepentingan yang ada dalam proses diskusi tentang apa yang harus dicapai saat proses audit.
2. define the scioe of the audit (membuat daftar semua asset yang akan diaudit, termasuk peralatan komputer, dokumentasi internal dan data yang diproses.
3. conduct the audit and identify threats (membuat daftar potensi ancaman yang terkait dengan setiap ancaman dapat mencakup hilangnya data, alat, atau catatan lainnya.
4. evaluate security and risks (menilai risiko dari setiap ancaman yang teridentifikasi.