****

**MÔN SOA204**

**PHẦN MỀM MIỄN PHÍ VÀ MÃ NGUỒN MỞ**

**BÁO CÁO**

**LAB 01**

**GVHD:**Lê Thanh Huy

**SVTH: DaoXuanHung**

**MSSV: PS32367**

**TPHCM - 2024**

**Câu 1:** So sánh giữa **phần mềm mã nguồn mở và phần mềm độc quyền**

* Liệt Kê
* Kẻ bảng (\*\*\*)

|  |  |  |
| --- | --- | --- |
| Tính năng | Phần mềm mã nguồn mở | Phần mềm độc quyền |
| Độ tương thích với nhiều nền tảng | Có thể cao hơn | Có thể thấp hơn |
| Tính bảo mật | Có thể cao hơn | Có thể thấp hơn |
| Tính thẩm mỹ | Có thể thấp hơn | Có thể cao hơn |
| Tính dễ sử dụng | Có thể khó sử dụng hơn | Dễ sử dụng hơn |
| Tính ổn định | Có thể cao hơn | Có thể thấp hơn |
| Khả năng tùy biến | Cao | Thấp |
| Khả năng cập nhật sửa lỗi | Tốt hơn | Có thể kém hơn |

**Câu 2:** Lý do gì khiến phần mềm mã nguồn mở có tính ổn định và bảo mật cao

….

Có hai lý do chính khiến phần mềm mã nguồn mở có tính ổn định và bảo mật cao:

* Kiểm tra mã nguồn bởi cộng đồng người dùng

Mã nguồn của phần mềm mã nguồn mở có thể được xem xét và kiểm tra bởi bất kỳ ai. Điều này giúp phát hiện các lỗi và lỗ hổng bảo mật. Một cộng đồng người dùng lớn sẽ có nhiều khả năng phát hiện các lỗi và lỗ hổng bảo mật hơn một nhóm người nhỏ.

* Quy trình phát triển cộng tác

Phần mềm mã nguồn mở thường được phát triển bởi một cộng đồng người dùng. Điều này giúp đảm bảo rằng phần mềm được phát triển và duy trì một cách cẩn thận. Cộng đồng người dùng có thể đóng góp ý kiến và phản hồi, giúp cải thiện chất lượng của phần mềm.

Dưới đây là một số ví dụ cụ thể về cách cộng đồng người dùng đã giúp phát hiện và sửa chữa các lỗ hổng bảo mật trong phần mềm mã nguồn mở:

* Năm 2017, một lỗ hổng bảo mật trong trình duyệt web Firefox đã được phát hiện bởi một người dùng bình thường. Lỗ hổng này có thể khiến tin tặc chiếm quyền kiểm soát máy tính của người dùng.
* Năm 2018, một lỗ hổng bảo mật trong hệ điều hành Linux đã được phát hiện bởi một nhóm nghiên cứu bảo mật. Lỗ hổng này có thể khiến tin tặc chiếm quyền kiểm soát máy tính của người dùng.
* Năm 2020, một lỗ hổng bảo mật trong hệ điều hành Android đã được phát hiện bởi một nhóm nghiên cứu bảo mật. Lỗ hổng này có thể khiến tin tặc chiếm quyền kiểm soát điện thoại thông minh của người dùng.

Tất nhiên, không phải tất cả phần mềm mã nguồn mở đều có tính ổn định và bảo mật cao. Tuy nhiên, nói chung, phần mềm mã nguồn mở có xu hướng có tính ổn định và bảo mật cao hơn phần mềm độc quyền.

**Câu 3:** **(câu hỏi trên group zalo)**

Bước 1: Tải source code từ github

**<dán hình:** chụp cả màn hình có thời gian>

