Broken Authentication

Overview

- Broken Authentication là lỗ hổng bảo mật đứng thứ 2 trên bảng xếp hạng Top 10 Owasp năm 2017. Broken Authentication thường là do chức năng xác thực và quản lí phiên người dùng thực hiện kém. Các cuộc tấn công nhằm mục đích chiếm 1 hay nhiều tài khoản mang lại cho kẻ tấn công các đặc quyền tương tự như người dùng bị tán công. Broken Authentication giúp cho kẻ tấn công có thể xâm phạm mật khẩu, khoá hoặc mã thông báo phiên, thông tin tài khoản người dùng và các chi tiết để xác định danh tính người dùng.

Impact

- Nếu tin tặc đăng nhập thành công bằng cách đánh cắp thông tin đăng nhập của bạn bằng bất kỳ kỹ thuật brocken authentication nào được đề cập, họ có thể lạm dụng đặc quyền của bạn và ảnh hưởng đến bạn như chiếm quyền truy cập phiên để có quyền truy cập vào hệ thống bằng cách giả mạo dữ liệu phiên, chẳng hạn như cookie và đánh cắp thông tin đăng nhập.

Type: chủ yếu chia làm 2 phần chính: Session management và credential management

- Session management là một chuỗi các giao dịch mạng được liên kết với cùng một người dùng trong một khoảng thời gian. Các ứng dụng web phát hành mỗi người dùng 1 session id duy nhất cho mỗi lần truy cập. Các id này thường là dạng cookie hay thông số URL.

    (Session management attack thường chia làm 3 loại)

    - Session Hijacking: Những kẻ tán công thường dùng session id bị đánh cắp để mạo danh người dùng. Ví dụ đơn giản nhất về chiếm quyền điều khiển phiên là người dùng quên đăng xuất khỏi ứng dụng và sau đó rời khỏi thiết bị của họ. Tin tặc sau đó có thể tiếp tục phiên của họ

- Session ID URL Rewriting: Một cách phổ biến khác để chiếm đoạt phiên là "viết lại URL". Trong trường hợp này, ID phiên của một cá nhân xuất hiện trong URL của một trang web. Bất kì ai cũng có thể thấy nó điều này làm cho tin tặc dễ dàng lợi dụng

- Session Fixation: Nếu ứng dụng web vẫn duy trì trạng thái xác thực của nạn nhân trong phiên, kẻ tấn công có thể sử dụng ID phiên được xác định trước đó để mạo danh nạn nhân sau khi nạn nhân đăng nhập. Cho dù kẻ tấn công hoặc nạn nhân trình bày ID phiên đó cho máy chủ, máy chủ sẽ thiết lập rằng ID phiên tương ứng với một phiên được xác thực và cấp quyền truy cập vào các tài nguyên được bảo vệ.

- Credential management: những kẻ tấn công đã phát hiện ra rằng cách dễ nhất để truy cập các hệ thống ngoài giới hạn là đăng nhập bằng thông tin đăng nhập của người khác. Các tác nhân độc hại sử dụng nhiều phương pháp khác nhau để đánh cắp, đoán hoặc lừa người dùng tiết lộ mật khẩu của họ.

    - **Credential Stuffing:** Những kẻ tấn công sử dụng botnet cho các cuộc tấn công vũ phu kiểm tra thông tin đăng nhập bị đánh cắp từ một trang web trên các tài khoản khác nhau. Chiến thuật này thường hoạt động vì mọi người thường sử dụng cùng một mật khẩu trên các ứng dụng.

    - **Password Spraying:** hơi giống như nhồi nhét thông tin xác thực, nhưng thay vì làm việc với cơ sở dữ liệu mật khẩu bị đánh cắp, nó sử dụng một bộ mật khẩu yếu hoặc phổ biến để đột nhập vào tài khoản của người dùng. Password Spraying là một loại tấn công vũ phu, nhưng nó thường trượt bằng khóa tự động chặn địa chỉ IP sau quá nhiều lần đăng nhập thất bại. Nó thực hiện điều này bằng cách thử cùng một mật khẩu, một người dùng tại một thời điểm, thay vì thử mật khẩu sau mật khẩu trên một người dùng duy nhất.

    - **Phishing Attacks:** Những kẻ tấn công thường lừa đảo bằng cách gửi cho người dùng một URL giả vờ là từ một nguồn đáng tin cậy và sau đó lừa người dùng chia sẻ thông tin đăng nhập của họ hoặc các thông tin liên quan khác.

Protect

Các cuộc tấn công broken authentication rất nguy hiểm và phổ biến, nhưng chúng cũng có khả năng ngăn chặn rất cao. Bằng cách áp dụng một số biện pháp bảo vệ

- **Update Session Management**
    - **Control Session Length:** Mỗi ứng dụng web tự động kết thúc phiên tại một số thời điểm, sau khi đăng xuất, một khoảng thời gian không hoạt động hoặc một khoảng thời gian nhất định. Điều chỉnh độ dài phiên của bạn theo loại người dùng và ứng dụng họ đang sử dụng
    - **Rotate and Invalidate Session IDs:** cách tốt nhất để ngăn chặn cố định phiên là phát hành người dùng với ID phiên mới sau khi đăng nhập. Tương tự, phiên và mã thông báo xác thực phải ngay lập tức bị vô hiệu hóa sau khi phiên kết thúc, vì vậy kẻ tấn công không thể tái sử dụng chúng.
    - **Don’t Put Session IDs in URLs:** Có rất nhiều cách để viết lại URL có thể làm lộ ID phiên, vì vậy đặt cược an toàn nhất của bạn là không đi theo con đường đó. Sử dụng cookie được tạo bởi trình quản lý phiên an toàn.
- **Tighten Password Policies**
    - **Implement Multi-Factor Authentication (MFA):** Cách số 1 để bảo đảm khỏi broken authentication là triển khai xác thực đa yếu tố để ngăn chặn các cuộc tấn công tái sử dụng thông tin đăng nhập tự động, thông tin xác thực, vũ phu và đánh cắp thông tin đăng nhập.

- **Don’t Permit Weak Passwords:**Một mật khẩu yếu thì rất dễ bị những kẻ tấn công dò ra được bằng 1 số công cụ chuyên môn.
- **Don’t Store Passwords in Cleartext:** 1 mật khẩu an toàn là 1 mật khẩu đươc mã hoá đúng cách với khả năng chỉ đọc 1 chiều và hash là điều như vậy. Không nên lưu mật khẩu dưới dạng plaintext vì rất dễ để dò tìm ra mật khẩu
- **Use Breached Password Protection:** Sử dụng nền tảng quản lý danh tính và truy cập (IAM) với bảo vệ mật khẩu bị vi phạm. Khi nền tảng phát hiện ra bộ nhớ cache thông tin đăng nhập bị xâm phạm, nó sẽ thông báo cho bạn nếu bất kỳ người dùng nào của bạn bị xâm phạm. Những người dùng đó sẽ bị khóa cho đến khi họ thay đổi mật khẩu của họ, vì vậy những kẻ tấn công không thể sử dụng mật khẩu bị xâm phạm của họ chống lại bạn trong một cuộc tấn công nhồi nhét thông tin xác thực.

- **Guard Against Attacks**
  - **Implement Brute-Force Protection:** trong một cuộc tấn công nhồi nhét thông tin đăng nhập thì lưu lượng truy nhập có thể tăng 1 cách kinh ngạc vì vậy bảo vệ brute-force là điều tuyệt đối phải thực hiện. Nó hoạt động bằng cách giới hạn số lần một địa chỉ IP cụ thể có thể cố gắng đăng nhập, vì vậy bot không thể làm ngập hệ thống của bạn.
  - **Employ anomaly detection:** Một hệ thống IAM tinh vi không chỉ xem xét thông tin đăng nhập và ID phiên để xác định xem người dùng là hợp pháp hay độc hại. Nó cũng nên gắn cờ các loại hành vi đáng ngờ khác
  - **Conduct Workplace Phishing Training:**

Reference

- https://auth0.com/blog/what-is-broken-authentication/
- https://owasp.org/www-project-topten/2017/A2_2017Broken_Authentication.html