Secure Software Development November 2022

« Collaborative Discussion 1: UML flowchart

Ashok Kumar Shanmugam

Initial Post

29 days ago

1 reply

Last 1 hour ago

Broken authentication is one of the weaknesses that OWSAP has found. Broken authentication is risky because authentication is the first line of defence against attacks. Authentication is usually considered by the application to be a legitimate user.

Only authorised users should be able to access data or functionality thanks to access control mechanisms. Any flaw that makes it possible for an attacker to avoid access restrictions or that disregards the least privilege principle falls under the group of vulnerabilities known as "broken access control." By changing the specified URL, a user of a web application, for instance, would be able to access another

user's account. (Checkpoint, #1 Broken Access Control).

Broken access control rises from fifth place in A01:2021; 94% of applications were examined for broken access control in some way. Applications had the highest frequency of the 34 Common Weakness Enumerations (CWEs) assigned to Broken Access Control.

Example Attack Scenarios

Scenario #1: The application uses unverified data in a SQL call that is accessing account information:

pstmt.setString(1, request.getParameter("acct"));

ResultSet results = pstmt.executeQuery( );

An attacker simply modifies the browser's 'acct' parameter to send whatever account number they want. If not correctly verified, the attacker can access any user's account.

https://example.com/app/accountInfo?acct=notmyacct

Scenario #2: An attacker simply forces browses to target URLs. Admin rights are required for access to the admin page.

https://example.com/app/getappInfo

https://example.com/app/admin_getappInfo

If an unauthenticated user can access either page, it's a flaw. If a non-admin can access the admin page, this is a flaw.

A sequence diagram just shows how objects interact with each other in the order that these interactions happen. We can also call a sequence diagram an event diagram or an event scenario. Sequence diagrams show how objects in a system work and in what order. Geeksforgeeks, (2022).

References:

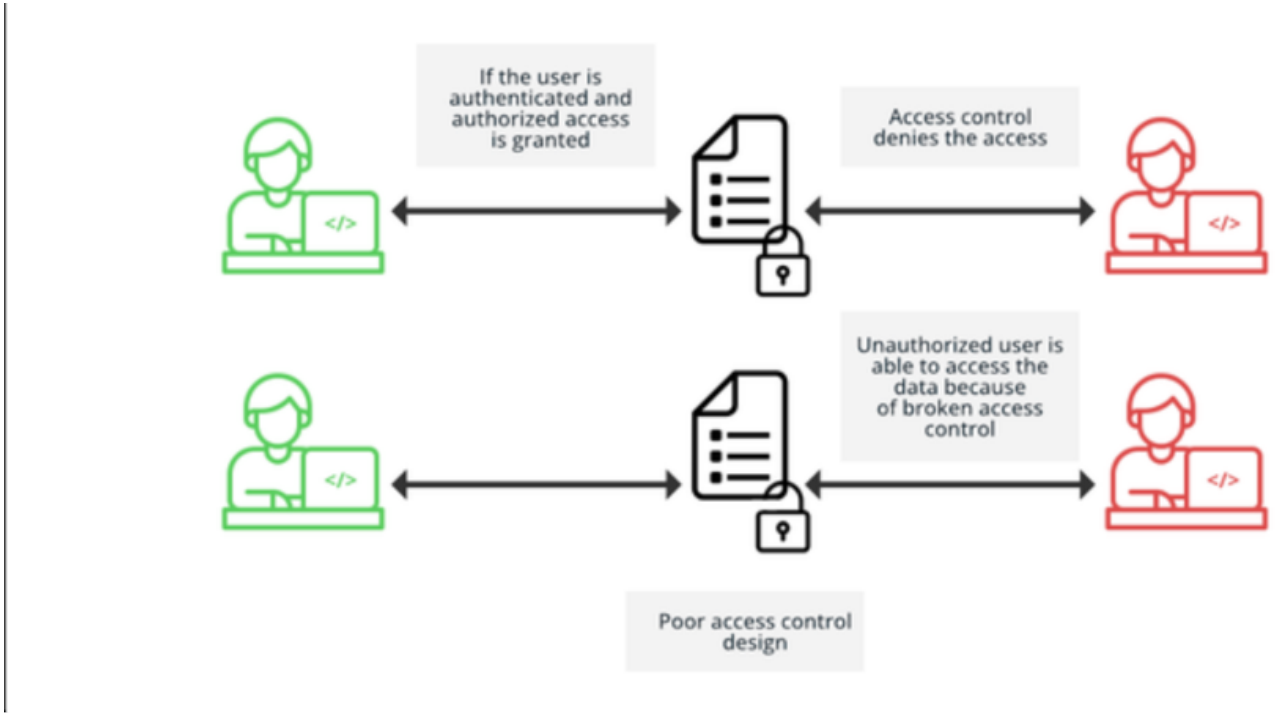
Checkpoint (2022) #1. Broken Access Control Available at: **https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/** (Accessed

November 20, 2022).

OWASP Top 10 Web Application Security Risks Available at: **https://owasp.org/www-project-top-ten/** (Accessed November 20, 2022).

OWASP Example Attack Scenarios Available at: **https://owasp.org/Top10/A01_2021-Broken_Access_Control/** (Accessed November 20, 2022).

Geeksforgeeks, (2022). Unified Modelling Language (UML) Sequence Diagrams Available at **https://www.geeksforgeeks.org/unified-modeling-language-uml-sequence-diagrams/?ref=gcse** (Accessed November 20, 2022)



Reply

Maximum rating: -

1 reply

1

Post by **Shailender Kudachi**

Peer Response

1 hour ago

I find myself in agreement with your essay, and in fact, I have decided to make Broken Authentication the topic of my initial post. The Open Web Application Security Project identifies it as one of the top security vulnerabilities. A security flaw known as "broken authentication" refers to any weaknesses that may exist inside the authentication procedure of a given system. It is possible for it to take place when an adversary is successful in evading the authentication procedure in order to obtain unauthorized access to a system or network. The Open Web Application Security Project, or OWASP for short, is a non-profit organization that offers tools and direction for furthering the cause of enhancing the safety of web applications. Identifying and fixing widespread security flaws and vulnerabilities in online applications is one of the primary focuses of the Open Web Application Security Project (OWASP). Broken authentication is one of the top 10 vulnerabilities recognized by OWASP. This vulnerability can allow attackers to obtain access to critical information and systems and is therefore one of the most dangerous vulnerabilities. I like you used a nice sequence UML diagram which depicts Access control method and the affect of not having a

proper access control.

Reply

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

Older discussion

Initial Post