The World of Broken Access Control

In this article, you'll learn the concept of Broken Access Controls.

What We'll Be Learning

Web applications are everywhere. Web applications are used daily, whether a website is visited online or a mobile app with a web application interface. Therefore, the Open Web Application Security Project (OWASP) devotes to building awareness and solutions for securing web applications. One of the top areas that require hardened security in web applications is A01 Broken Access Controls. In this article, we will:

- Review what Access Controls are.
- Define and understand Broken Access Controls.
- Learn the three aspects of successful access controls.
- Understand how breaks in access controls happen.
- Understand why broken access controls are dangerous.

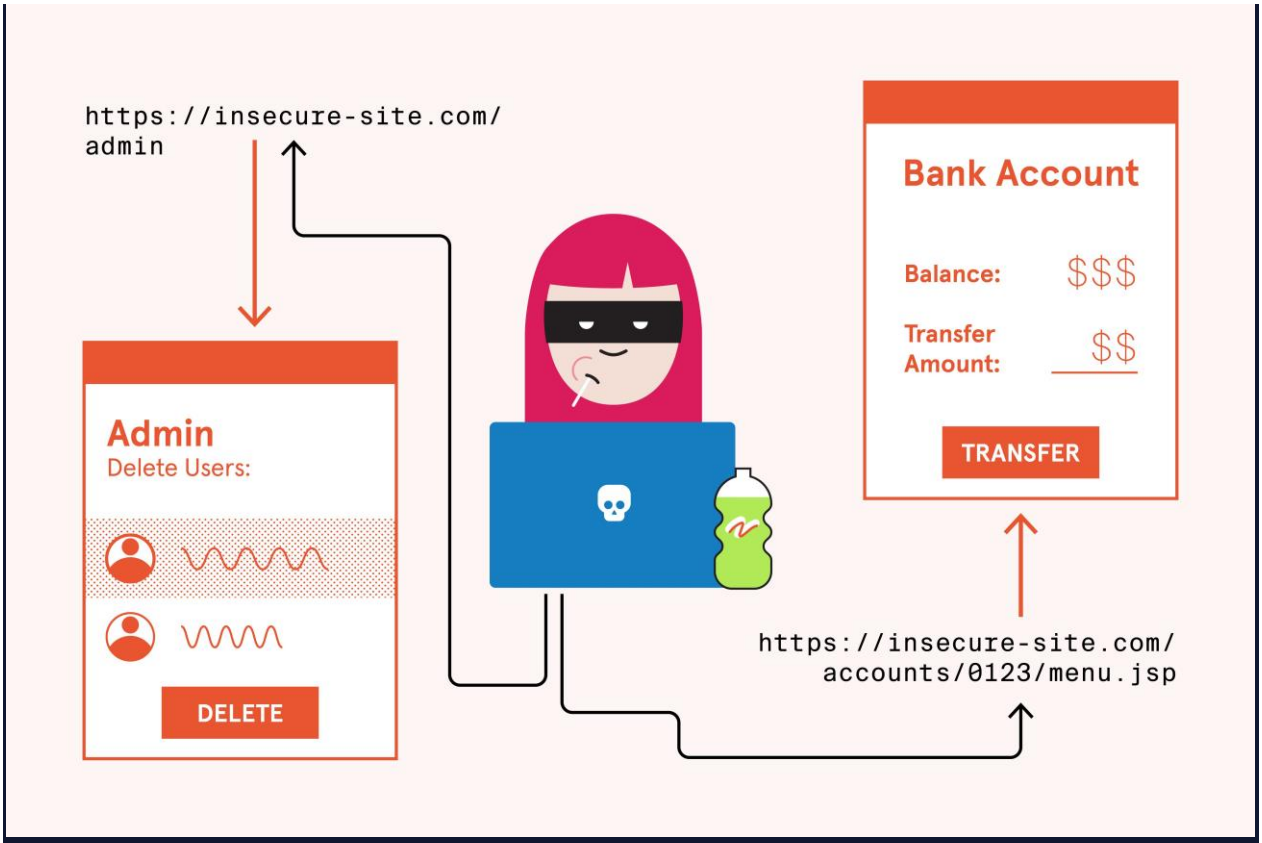
What are Broken Access Controls?

Access Controls

Access controls are designed to enforce security policies that prevent users from acting outside their intended permissions. Strong access controls will maintain the principle of least privilege and deny any action a user cannot perform. Failures in access controls will lead to unauthorized access to information and may allow the unauthorized modification or destruction of data and critical systems.

Broken Access Controls

The #1 *OWASP Top 10* category as of 2021 is *A01 Broken Access Controls*. Broken Access Controls are critical security vulnerabilities that attackers may exploit to perform any action not intended by an application's permissions. Access control is considered broken when it is either improperly implemented (i.e, misconfigured or not configured), is easily circumvented, and/or allows unauthorized actions without an in-place check or block.



How Do Broken Access Controls Come to Be?

Three Key Aspects of Web Application Access Controls

Access controls in web applications rely on three key aspects: authentication, authorization, and permissions checks. Access controls break due to the lack of proper implementation of these three key aspects and are mostly highly technical implementations. OWASP lists a few common access control vulnerabilities that allow exploitation:

- Failure to properly implement the *principle of least privilege* grants an authenticated user ONLY the minimal permissions they need to perform their tasks.
- Unblocked *escalation of privilege* within the application where a user performs actions of a higher level user.
- Misconfiguration of API access (CORS) allows access from untrusted origins.
- Access control bypass through modified URLs to other areas in a web application.
- Insecure direct object references, such as accessing other users' profiles using their identifier.
- Metadata manipulation to abuse JSON Web Tokens (JWT).

Why are Broken Access Controls Dangerous?

Broken Access Control Scenario

A property management company's web portal requires users to authenticate through a login page: `properties.com/signin`.

An attacker finds a web page that circumvents access controls when directly accessed via URL: `properties.com/accounts`.

The accounts page lists each property portfolio, including bank account information, the user's full name, social security number, and address.

In this above example, access controls were bypassed by modifying the URL of the `properties.com` website to navigate to another site's web page in an unauthorized fashion. The information made available to the unauthorized user is sensitive in nature and should maintain confidentiality from such users. A social security number may be used to steal an identity. Bank information could lead to fraud and theft of hard-earned funds. It is important to secure people's personally identifiable and financial information online. This is one example that demonstrates why broken access controls are dangerous.

Conclusion

Access controls play an important role in the authentication and authorization of web applications. Along with permission checks built into a web application's access controls, these three key aspects make for effective web access controls. Broken access controls are the leading security category in modern web applications. There are methods to mitigate the vulnerabilities of broken web applications, but broken access controls are dangerous to web applications and their users when exposed.