عنوان مقاله : احراز هویت و احراز دسترسی

امین محمد خوارزمی

دانشگاه آزاد اسلامی واحد کاشمر

amiin.kharazmii@gmail.com

چکیده:

احراز هویت و احراز دسترسی دو موضوع پر اهمیت در حوزه امنیت می باشد. در این مقاله به تعریف و شناسایی این دو موضوع، چگونگی کارکرد آنها در سیستم های مختلف و همچنین هدف به کارگیری آنها خواهیم پرداخت.

به اختصار، احراز هویت به مجموعه روش هایی گفته می شود که بیان می کند آیا هویت فرد با آنچه اعلام می کند یکسان است یا خیر! صراحتا در صورت عدم انجام صحیح این مورد، امنیتی برای اطلاعات هر فرد شکل نگرفته لذا ممکن است اطلاعات زیادی از افراد گوناگون در سراسر جهان آشکار شود که خود زمینه ساز سوءاستفاده های متعدد در شرایط مختلف از داده های افراد است.

پیرو موضوع مهم احراز هویت، احراز دسترسی نیز امروزه اهمیت های فراوانی دارد. احراز دسترسی یا کنترل دسترسی یعنی دادن مجوز های لازم برای استفاده از منابع و داده ها به کارابرانی که قبلا احراز هویت شده اند.

کلمات کلیدی:

هویت، شناسایی، اعتبارسنجی، مدیریت دسترسی، سیاست دسترسی، مجوز، کاربر

مقدمه:

در گذشته استفاده از کامپیوتر و شبکه های اطلاعاتی به مراتب کمتر از حال بود زیرا استفاده کنندگان اغلب محدود و مشخص بودند، همچنین تجربه کاربری محیط های دیجیتال نیز به اندازه زمان حال پیچیده نبود و نیاز مبرمی به احراز هویت اشخاص نبود. با گذر زمان مسائل احراز هویت و احراز دسترسی از اهمیت زیادی برخوردار شد، یعنی درست از زمان ایجاد اینترنت، توسعه فناوری‌های احراز هویت و احراز دسترسی به طور همزمان با رشد فناوری و ارتباطات پیش رفت.

احراز هویت و احراز دسترسی به ویژه در عصر دیجیتال و انتقال اطلاعات از روی سیم‌های فیزیکی به شبکه‌های بی‌سیم و ابری، از اهمیت بیشتری برخوردار شد، زیرا تهدیدات امنیتی نیز با پیشرفت فناوری رشد کردند و توانستند اطلاعات حیاتی و حساس را تهدید کنند.

هدف احراز هویت و احراز دسترسی:

به طور کلی برقراری امنیت در هر بستری جزو اصلی ترین اهداف سازمان ها می باشد، در این خصوص فاکتورهای تاثیرگذار بسیاری وجود دارد که یکی از مهمترین عوامل در مدیریت امنیت اطلاعات، احراز هویت است. به همین منظور اکثر سرویس ها و یا برنامه ها برای ارائه خدماتشان به کاربران اقدام به ایجاد حساب های کاربری می نمایند درواقع ساده ترین احراز هویتی که وجود دارد تعریف یک نام کاربری و یک رمز عبور منحصر به فرد به ازای هر کاربر می باشد. هدف اصلی از احراز هویت افراد در واقع ایجاد محیطی امن برای حفظ اطلاعات سازمانی و جلوگیری از خطرات احتمالی از تهدیدات خارجی (مانند هکرها، نرم افزارهای مخرب و غیره) یا تهدیدهای داخلی مانند مخرب های داخلی محافظت کنند.

کنترل های دسترسی، اقدامات امنیتی هستند که دسترسی به منابع، سیستم ها و داده ها را محدود و کنترل می کنند. آنها اطمینان می دهند که فقط کاربران مجاز می توانند به اطلاعات یا منابع حساس دسترسی داشته باشند و از دسترسی غیرمجاز، تغییر یا تخریب داده ها جلوگیری کنند. به طور کلی، فناوری های کنترل دسترسی در تضمین امنیت منابع، سیستم ها و داده ها بسیار مهم هستند. انتخاب فناوری های کنترل دسترسی مناسب به نیازهای امنیتی خاص و الزامات برنامه بستگی دارد.

بدنه اصلی:

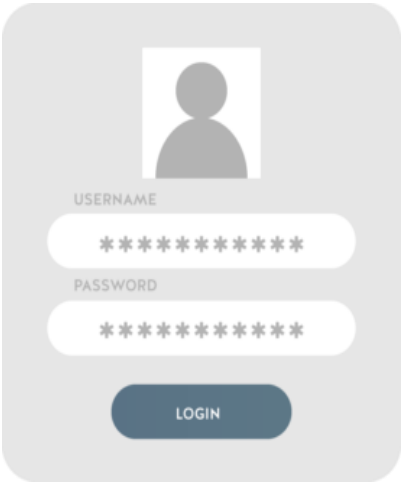
به طور معمول برای استفاده از خدمات یک سامانه و یا سازمان، اطلاعات منحصر به فردی به ازای هر کاربر صادر می گردد که این اطلاعات همان هویت ما در سازمان مربوطه را مشخص می نماید، در واقع یک شناسه برای ما تعریف می گردد که ما با استفاده از آن از خدمات بهره مند می شویم، این روند شناسایی ما درسامانه یا سازمان و یا هر بستر دیگری را احراز هویت می نامند. به عبارت دیگر احراز هویت یا Authentication به روندی گفته می شود که در آن هویت فردی که قصد ورود به سیستم را دارد، بررسی شده و در صورت تأیید شدن هویت اینکه آیا واقعا این فرد همان فردی است که قابلیت ورود را دارد، وارد سیستم می شود. یعنی در این فرایند ثابت می شود کسی هستیم که می گوییم!
به عنوان مثال، اگر کاربر نیاز به دسترسی به یک سیستم داشته باشد از او خواسته می‌شود اطلاعات اعتباری خود را وارد کند (مثلا نام کاربری و رمزعبور)؛ سپس این اطلاعات در یک پایگاه داده مشخص بررسی می‌شوند. پس از این مرحله، در صورت مطابقت داده‌های ارسالی کاربر، به وی اجازه ورود به سیستم داده می‌شود.

بعد از اینکه معنا و مفهوم احراز هویت را درک کردیم حال باید به اهمیت و علت اینکه این مسأله از اهمیت بالایی برخوردار است بپردازیم. برقراری امنیت یکی از مهم‌ترین و البته چالش برانگیزترین موضوعاتی است توسعه دهندگان باید آن را پیاده‌سازی کنند. برقراری امنیت برای یک وب سایت از راه‌های مختلفی انجام می‌شود اما همواره یکی از ثابت‌ترین و البته مهم‌ترین بخش‌های برقراری امنیت، ایجاد قابلیت‌های احراز هویت است.

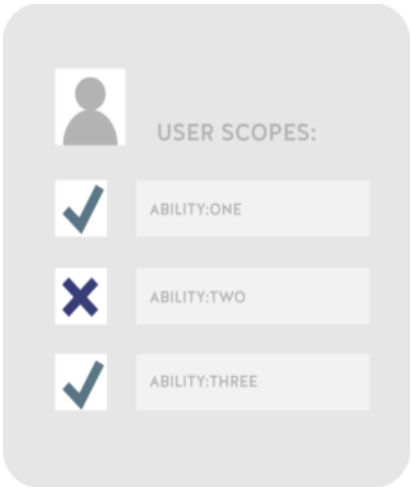
در یک سازمان که می تواند هر مدلی از سیستم های گوناگون باشد، برای هر فردی که از مرحله احراز هویت عبور می کند می بایست مجوز هایی تعیین کرد که وی فقط به همان داده ها و یا فقط به همان منابع دسترسی دارد؛ واضح است که هر فرد درون یک سیستم مجوز ها و اختیارات متفاوتی با دیگر افراد دارد!

احراز دسترسی، کنترل های دسترسی، اعتبارسنجی و یا Authorization، اقدامات امنیتی هستند که دسترسی به منابع، سیستم ها و داده ها را محدود و کنترل می کنند. آنها اطمینان می دهند که فقط کاربران مجاز می توانند به اطلاعات یا منابع حساس دسترسی داشته باشند و از دسترسی غیرمجاز، تغییر یا تخریب داده ها جلوگیری کنند.

در واقع احراز دسترسی مرحله بعد از احراز هویت است لذا احراز هویت می گوید که " فرد چه کسی است؟ " اما احراز دسترسی می گوید که "فرد می تواند چنین کاری را انجام دهد؟ ". پس بنابراین موضوع احراز دسترسی هم مانند احراز هویت اهمیت زیادی دارد که توسعه دهندگان باید به آن توجه کنند.



شکل ۱ – احراز هویت



شکل۲ – احراز دسترسی

«مجوز» از برخی تنظیمات ایجاد شده و مدیریت شده توسط شرکت پیروی می‌کند در حالی‌که «احراز هویت» از رمزعبور یا داده‌های بیومتریک برای تائید هویت یک کاربر استفاده می‌کند. هنگامی که از فرآیند احراز دسترسی صحبت می‌شود، ابتدا احراز هویت مورد بحث است سپس مجوز به دنبال آن می‌آید.

از دیگر تفاوت‌های این دو موضوع این است که احراز هویت فرایندی قابل مشاهده توسط کاربر است، اما احراز دسترسی قابل مشاهده نیست زیرا تنظیماتی است که از قبل بر روی سیستم اعمال شده است.

هر دو فرایند باید بصورت سینرژی (یعنی در کنار هم به صورت همکاری) عمل کنند، زیرا در صورت شکست یکی، درها به روی شکاف‌های امنیتی باز می‌شود. هدف اصلی احراز هویت، احراز دسترسی و همکاری با یکدیگر، جلوگیری از حملات سایبری است که شامل افشای اطلاعات است.

روش های احراز هویت و احراز دسترسی و پیاده سازی آنها :

احراز هویت بر چهار پایه اصلی می باشد و با این چهار ورش می توان احراز هویت را در سیستم های مختلف پیاده سازی کرد :

۱- هر آنچه کاربر دارد. برای مثال احراز هویت هر فرد با کارت ملی یا هویتی خود صورت بگیرد!
۲- هر آنچه کاربر می داند. مثلا هویت هر فرد با یک رمز عبور یا گذرواژه که قبلا خود در داخل سیستم تعیین کرده است تأیید شود.
۳- هر آنچه کاربر است. یعنی تمام افراد دارای ویژگی های منحصر به فردی هستند که به کمک آن ها می توان هویت آنها را تأییدکرد، مانند اثر انگشت یا هر ویژگی بیومتریکی دیگری که افراد مختلف دارای آن ها هستند.
۴- هر آنچه کاربر می تواند. برای مثال سیستم ها قادر هستند با نحوه راه رفتن یا تایپ کردن و دیگر ویژگی های رفتاری هویت افراد را مشخص کنند.

احراز دسترسی نیز با چهار روش یا شیوه می تواند در یک سیستم پیاده سازی شود:

۱- احراز دسترسی مبتنی بر صفت. اختصاص دادن منابع به فرد طبق صفات و ویژگی هایی که دارد مانند اثر انگشت!

۲- احراز دسترسی مبتنی بر سطح. در سیستم‌های اطلاعاتی، دسترسی به منابع و داده‌ها بر اساس سطح دسترسی کاربر تنظیم می‌شود. به عنوان مثال، کارمندان در یک سازمان ممکن است به منابعی که برای مدیران در دسترس است، دسترسی نداشته باشند!

۳- احراز دسترسی مبتنی بر سیاست. احراز دسترسی بر اساس سیاست های از پیش تعیین شده در یک سازمان؛ برای مثال نیاز به احراز دو مرحله ای یا زمان تغییر رمز عبور!

۴- احراز دسترسی مبتنی بر نقش. کنترل دسترسی بر اساس نقش هر فرد صورت می گیرد، مثلا در سیستم های مدیریت محتوا دسترسی به بخش های مختلفی از سایت بر اساس نقش کاربر تعیین می شود لذا مدیران ممکن است دسترسی به تنظیمات سایت را داشته باشند در حالی که کاربران معمولی این دسترسی را ندارند!

شکل ۳ – Authentication&Authorization

اگر با خودمان روراست باشیم، بخاطر مشکلات اینترنتی و مسائلی مانند تحریم‌های بین‌المللی، خطا های اینترنتی و خطاهای مختلف جزئی از روتین‌های وب شده است و داشتن اطلاعات در مورد دلیل نمایش و همچنین چگونگی ایجاد آنها برای تمامی کاربرانی که می‌خواهند در وب حرفه‌ای باشند و یا می‌خواهند کسب‌وکار اینترنتی خود را راه‌اندازی کنند ضروری می‌باشد.

دو نمونه از خطا هایی که در ارتباط با بحث احراز هویت و احراز دسترسی می باشند و نیاز است که راجع به آنها اطلاعاتی بیان شود، خطا های Unauthorized401 و همچنین Forbidden403 می باشند!

خطای Unauthorized401 به معنی غیرمجاز است. این خطا زمانی نشان داده می‌شود که کاربر یک URL را درخواست کرده اما به درستی احراز هویت (Authentication) نشده است. پس ابتدا باید کاربر وارد سایت شود و سپس درخواست خود را مجددا انجام دهد. در این صورت، معمولاً پیام خطا Unauthorized401 نمایش داده می‌شود.

به عبارتی خطای Unauthorized401 یک خطا از خطا های سمت کاربر می باشد که در آن به ما اعلام می‌شود که اصالت‌سنجی کاربر با مشکل مواجه شده است و مجوز دسترسی به صفحه موردنظر صادر نشده است! نکته اصلی که در مورد این خطای کلاینت وجود دارد این است که این خطا زمانی به وجود می‌آیند که المان HTTP Authentication عیب و ایراد خاصی را تشخیص دهد؛ HTTP Authentication یکی از اولین و ساده‌ترین پروتکل‌هایی است که برای انتقال داده های حساس به‌صورت رمزنگاری شده و امن ارائه شد. به عبارتی وقتی مکانیزم HTTP Authentication نتواند تاییدیه اینکه شخص کاربر این سایت است را بدهد و او را تایید شده بداند خطای Unauthorized 401 به شخص نمایش داده خواهد شد. در واقع خطای Unauthorized 401 می‌گوید که کاربر برای صفحه‌ای که می‌خواهد به آن دسترسی پیدا کند از سطح دسترسی لازم برخوردار نیست.

اما خطای Forbidden403 به معنی دسترسی غیرمجاز است. این خطا زمانی به کاربر نشان داده می‌شود که مجوز دسترسی به آن بخش سایت را ندارد. حتی اگر کاربر احرازهویت (Authentication) شده باشـــــد، ممکن است مجوز لازم (Authorization) برای مشاهده یا عملیات در آن بخش را نداشته باشد. در این صورت، معمولاً پیام خطا Forbidden403 نمایش داده می‌شود.

در تعریف خطای Forbidden403 باید به این نکته توجه داشت که خطای Forbidden403 نوعی کد وضعیت HTTP است که نشان می‌دهد وب سرور درخواست کاربر را دریافت کرده اما اجازه اتصال آی‌پی وی به صفحه موردنظر را نمی‌دهد؛ یعنی دسترسی او به وب‌سایت موردنظر مجاز نبوده یا منبع موردنظر درحال‌حاضر در دسترس نیست!

بعضی از دلایل خطای Forbidden403 در HTTP به دلیل برخی اشتباهات دسترسی در سمت کلاینت هستند که به معنای آن است که معمولاً می توان مشکل را حل کرد.

یکی از عوامل شایع ایجاد این خطا، تنظیمات مجوز فایل یا پوشه ها است که کنترل کننده کسانی هستند که می توانند فایل یا پوشه را بخوانند، بنویسند و اجرا کنند. در این مورد دو احتمال وجود دارد: یا صاحب وب سایت تنظیمات را به گونه ای ویرایش کرده است که ما نمی توانیم به منابع دسترسی داشته باشیم، یا او مجوزهای صحیح را تنظیم نکرده است.

نتیجه گیری:

حال با شناخت احراز هویت و احراز دسترسی به طور خلاصه، به سوال های پیش آمده در این مورد با خواندن مقاله پاسخ داده می شود.

* **تعریف Authentication چیست؟**

به روند بررسی و تأیید هویت فرد قبل از ورود به سیستم احراز هویت یا Authentication می گویند.

* **تعریف Authorization چیست؟**

به فرایند های امنیتی برای کنترل دسترسی منابع و داده ها به کاربران سیستم که هویت آن ها تأیید شده، احراز دسترسی یا Authorization می گویند.

* **روش های احراز هویت را نام ببرید.**

آنچه کاربر دارد – آنچه کاربر می داند – آنچه کاربر است – آنچه کاربر می تواند

* **چهار شیوه کنترل دسترسی را نام ببرید.**

احراز دسترسی مبتنی بر سطح – احراز دسترسی مبتنی بر نقش – احراز دسترسی مبتنی بر صفت – احراز دسترسی مبتنی بر سیاست

* **مفهوم خطای Forbidden403 چیست؟**

دسترسی غیر مجاز، زمانی نمایش داده می شود که کاربر به بخشی از سیستم دسترسی ندارد.

مراجع:

1.https://www.sid.ir/search/journal/paper/%d8%a7%d8%ad%d8%b1%d8%a7%d8%b2%20%d9%87%d9%88%db%8c%d8%aa/fa?str=%d8%a7%d8%ad%d8%b1%d8%a7%d8%b2+%d9%87%d9%88%db%8c%d8%aa&page=1&sort=0&fgrp=all&ftyp=all&fyrs=all

2.https://payvast.com/%DA%86%D8%B1%D8%A7-%D8%A7%D8%AD%D8%B1%D8%A7%D8%B2-%D9%87%D9%88%DB%8C%D8%AA-%D8%A7%D9%87%D9%85%DB%8C%D8%AA-%D8%AF%D8%A7%D8%B1%D8%AF-%D8%9F/

3.https://www.shahrsakhtafzar.com/fa/articles-guides/security/38468-face-iris-fingerprint-password-pin-most-secure

4.https://shopingserver.net/45111/%D9%87%D9%85%D9%87-%DA%86%DB%8C%D8%B2-%D8%AF%D8%B1-%D9%85%D9%88%D8%B1%D8%AF-%DA%A9%D9%86%D8%AA%D8%B1%D9%84-%D9%87%D8%A7%DB%8C-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C/

5.https://tebyansmart.com/%D8%AA%D9%81%D8%A7%D9%88%D8%AA-%D8%A7%D8%AD%D8%B1%D8%A7%D8%B2-%D9%87%D9%88%DB%8C%D8%AA-%D8%AF%D8%B1-%D9%85%D9%82%D8%A7%D8%A8%D9%84-%D9%85%D8%AC%D9%88%D8%B2-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C/

6.https://blog.u-id.net/authentication-and-access-control

7.https://roocket.ir/articles/authentication-vs-authorization