Security research

Tim Meijvogel
S3 DB01

Inhoud

Context

Wat wil ik weten?

Waarom zou je een authenticatie service gebruiken in plaats van een eigen login systeem?

Waarom wil ik dit weten?

In mijn game wil ik gebruik maken van accounts, zodat ik speler data op kan slaan. Om deze reden heb ik aan mijn applicatie auth0 toegevoegd. Ik had er voor kunnen kiezen een eigen database te maken met speler en hun accountgegevens. Deze had ik natuurlijk dan zelf moeten beveiligen, in plaats van dat ik dit door de authenticatie service zou laten doen. Toen ik dit onderwerp bedacht vroeg ik me af.

Voor deze research ga ik uit van auth0 aangezien dit is wat ik heb gebruikt in mijn applicatie.

Hoe ga ik dit doen?

Ik ga dit onderzoeken door te kijken naar wat een authenticatie service doet, welke voordelen dit biedt en wat de gevaren kunnen zijn wanneer je geen authenticatie service gebruikt. Ik kijk hierbij naar bestaande producten, research en gebeurtenissen. Ik maak dus gebruik van library research.

Wat doet een authenticatie service?

Authenticatie services zorgen ervoor dat de gebruikers van je app kunnen inloggen met hun gebruikersnaam/email en wachtwoord. Er zijn ook services die het toelaten om in te loggen met social media accounts. De authenticatie service zorgt er achter de schermen voor dat dit op een veilige manier gebeurd. Een authenticatie service kan ook op andere manieren bevestigen dat jij bent wie je zegt dat je bent, namelijk: door fysieke spullen, zoals een telefoon of sleutel. Een andere manier is door biometrie (vingerafdruk scanner of iris scanner). Ze beveiligen zoals eerder gezegd ook je applicatie. Een aantal manieren zijn:

1. Anomaly detection

Dit is wanneer de service oplet of er abnormaal gedrag wordt vertoond door een gebruiker van je applicatie. Dit kan worden gebruikt om kwaadaardige inlogpogingen te stoppen voordat ze plaatsvinden.

2. Brute-Force Protection

Om je applicatie tegen een brute force attack te beschermen worden (in het geval van auth0) 2 shields gebruikt. De eerste is na 10 gefaalde log in pogingen van een account vanaf hetzelfde ip adres, de tweede na 100 gefaalde log in pogingen van 1 ip adres in 24 uur of na 50 gefaalde log in pogingen van 1 ip adres in 1 minuut. wanneer het tweede shield wordt geactiveerd word het ip adres geblokkeerd.

3. Breached-password detection

Dit is wanneer de service denkt dat een gebruikers email is gecomprimeerd in een security breach. De gebruiker kan niet inloggen totdat zijn wachtwoord is aangepast. Hier krijgt de gebruiker een bericht over.

Wat zijn de voordelen van een authenticatie service?

Er zijn veel voordelen aan een authenticatie service. Een aantal grote voordelen zijn: Dat het je tijd bespaart wanneer je er een gebruikt, aangezien dit een deel is van je applicatie dat je niet zelf meer hoeft te maken. Een ander groot voordeel is de beveiliging die je kunt instellen. Wanneer je zelf een inlog systeem zou maken met een eigen database waar je gebruikersinformatie op zou slaan zijn er veel security issues waar je rekening mee moet houden. Een authenticatie service kent deze issues al en heeft deze al opgelost. Sommige authenticatie services laten mensen inloggen met social media accounts, dit is fijn voor de gebruiker, aangezien ze nu niet door het proces van het creëren van een account hoeven te lopen.

Wat zijn de gevaren van een eigen login systeem/user database?

Zoals eerder verteld zijn er veel security issues met een eigen login systeem, als je hier geen rekening mee houdt kunnen hackers makkelijk bij de gegevens van je gebruikers. Een aantal gevaren zijn:

SQL injection:
Hierdoor zouden mensen vanuit je frontend sql queries uitvoeren. Hiermee kunnen ze alle gegevens van alle accounts in de database in de frontend te zien krijgen. Een voorbeeld hiervan is Adobe Flash.

Het opslaan van gevoelige informatie in javascript files of server responses:
Wanneer je dit doet kan een hacker proberen een manier te vinden om de inloggegevens uit de respons- of javascript-bestanden te halen.

Geen Brute-force protection:
Dit is een risico waar ik eerder over heb geschreven. Wanneer dit niet aanwezig is kunnen hacker door trial and error proberen aan logingegevens of andere gevoelige informatie te komen.

Respons manipulatie:
Vaak wordt opgemerkt dat de toepassing van "success":false of "success":true wordt gegeven wanneer ongeldige/geldige inloggegevens worden ingevuld. Als de applicatie de bevestiging aan de serverzijde niet goed uitvoert, is het mogelijk om de reactie te manipuleren, door bijvoorbeeld "success":false in "success":true te veranderen. Een aanvaller kan dan toegang krijgen tot het account van een van jouw gebruikers. Deze aanval is vaak effectief wanneer de authenticatietoken of de logica voor het genereren van cookies aan de clientzijde ligt, dit is een slechte gewoonte.

Conclusie

Dus Waarom zou je een authenticatie service gebruiken in plaats van een eigen login systeem?
Authenticatie stelt organisaties dus in staat hun netwerken veilig te houden door alleen geverifieerde gebruikers of processen toegang te geven tot hun beschermde bronnen. Dit kunnen computersystemen, netwerken, databases, websites en andere netwerkgebaseerde toepassingen of diensten zijn. Dit kan ook gedaan worden met een eigen inlog systeem, maar tenzij je dit maakt met een cyber security expert is de kans groot dat je iets over het hoofd zal zien, waardoor je gebruikersdata of beschermde bronnen in gevaar brengt.
Is het dan verstandig om een eigen login service te maken als je met een cyber security expert zou werken en het resultaat is volledig veilig? Mijn mening is dat dit niet het geval is. Tenzij je 100% controle wilt over je inlog systeem is er geen reden om het wiel opnieuw uit te vinden.

Bronnen

Bothra, H.(2021, 10 juni)10 Most Common Security Issues Found in Login Functionalities. RedHuntLabs.
https://redhuntlabs.com/blog/10-most-common-security-issues-found-in-login-functionalities.html

Xano(2021, 15 december)5 Reasons To Use Auth0 For Authentication In Your Application. Xano.
https://www.xano.com/blog/5-reasons-to-use-auth0-for-authentication-in-your-application/

Guevare, H.(2020, 29 juli) What is an authentication server? Auth0.
https://auth0.com/blog/what-is-an-authentication-server/

Poza, D.(2018, 29 juli)How Auth0 Makes Your Apps More Secure. Auth0.
https://auth0.com/blog/how-auth0-makes-your-apps-more-secure/

Shacklett, M.E.(2021, september) authentication. TechTarget.
https://www.techtarget.com/searchsecurity/definition/authentication

Vince Vintage(2022, 14 juni) This Toy illegally Spied on 6.4 Million Children. Youtube
https://www.youtube.com/watch?v=gkJ4qv5RLRc