Veiligheidsrisico’s

Zwakte in Clientauthenticatie

Clientauthenticatie is het proces waarbij een applicatie (de "client") bewijst dat deze legitiem is en bevoegd om toegang te vragen tot een resource. Dit gebeurt meestal door middel van **client credentials** zoals een client-ID en een geheim (client secret).

Aanvallers kunnen zwakke client credentials bemachtigen, wat leidt tot datalekken, imitatie van legitieme clients, en massaal misbruik van resources.

Best Practices:

1. **Encryptie van clientsecrets:** Gebruik versleuteling om clientcredentials te beschermen, en vermijd opslag in front-end-code of openbare locaties.
2. **PKCE (Proof Key for Code Exchange):** Maak gebruik van PKCE in plaats van traditionele clientsecrets, vooral voor publieke clients zoals mobiele apps.
3. **HTTPS voor communicatie:** Zorg ervoor dat alle communicatie via een beveiligde verbinding loopt.

Clientimitatie

Bij client imitatie maakt een aanvaller een applicatie die lijkt op een legitieme client en misleidt gebruikers om deze toegang te geven.

Best Practices:

1. **Whitelist van redirect URI's**: Beperk de redirect URI's tot vooraf goedgekeurde en vertrouwde domeinen.
2. **Bewustwording bij gebruikers**: Informeer gebruikers over het herkennen van legitieme applicaties en phishingaanvallen.

Autorisatiecodes

Een autorisatiecode is een unieke, tijdelijke code die een client ontvangt nadat een gebruiker toestemming heeft gegeven via de autorisatieserver. De client gebruikt deze code vervolgens om een access token aan te vragen.

Autorisatiecodes die niet beveiligd zijn (bijvoorbeeld via HTTP of zonder PKCE) kunnen onderschept en hergebruikt worden, wat leidt tot ongeoorloofde toegang.

Best Practices:

1. **PKCE verplicht stellen**: PKCE voorkomt dat onderschepte codes kunnen worden gebruikt door aanvallers.
2. **Korte levensduur van codes**: Beperk de geldigheidsduur van autorisatiecodes tot enkele minuten.

Access Tokens

Een access token is een korte, veilige string die wordt gebruikt om toegang te krijgen tot een beveiligde API of resource. Het token is meestal tijdgebonden en kan specifieke toegangsrechten bevatten.

Tokens die via onveilige kanalen worden verzonden of slecht worden opgeslagen, kunnen door aanvallers worden onderschept en misbruikt.

Best Practices:

1. **Gebruik van TLS**: Encryptie tijdens transmissie voorkomt onderschepping.
2. **Beveiligde opslaglocaties**: Gebruik veilige opslagmethoden, zoals Secure Storage op mobiele apparaten.
3. **Scope en geldigheidsduur beperken**: Minimaliseer toegangsrechten en maak tokens tijdgebonden.
4. **Rotatie van tokens**: Maak gebruik van refresh tokens en vernieuw access tokens regelmatig.

Redirect URI-manipulatie

Bij manipulatie van de redirect URI verandert een aanvaller de URI die in de autorisatieaanvraag wordt opgegeven. Hierdoor wordt de autorisatiecode of het access token naar een kwaadaardige server gestuurd in plaats van naar de legitieme client.

Best Practices:

1. **Exacte validatie**: Sta alleen exacte overeenkomsten toe met vooraf geregistreerde URI's.
2. **Geen wildcards gebruiken**: Wildcards verhogen het risico op manipulatie aanzienlijk.
3. **Gebruik HTTPS**: Sta alleen veilige URI's toe om de communicatie te beschermen.

Endpoint Authenticiteit

Endpoint authenticiteit verwijst naar de zekerheid dat een server die beweert een autorisatieserver te zijn, ook daadwerkelijk is wie hij beweert te zijn.

Zonder een geldig TLS-certificaat kan een aanvaller een nep-autorisatieserver inzetten, wat de data van de gebruiker in gevaar brengt.

Best Practices:

1. **TLS-certificaten verplicht stellen**: Gebruik alleen vertrouwde certificaten van erkende certificaatautoriteiten (CA's).
2. **Certificaatauthenticatie**: Controleer certificaatketens om nepservers te voorkomen.
3. **HSTS implementeren**: Dwing het gebruik van HTTPS af via HTTP Strict Transport Security.

Phishing

Phishing-aanvallen zijn een van de meest. Aanvallers misleiden gebruikers om hun gegevens in te voeren op een nep-autorisatieserver, waardoor gevoelige informatie zoals wachtwoorden en autorisatiecodes in handen van kwaadwillenden komt.

Best Practices:

1. **Strikte validatie van redirect URI's**: Sta alleen vooraf goedgekeurde URI's toe.
2. **Indicatoren van vertrouwen**: Gebruik visuele signalen in de interface die aangeven dat de gebruiker op een legitieme autorisatieserver zit.