Web application security - onderzoek

Sten Hulsbergen

1. web applicatie beveiliging

1.1. Injectieaanvallen

1.1.1. SQL-injectie

- Gebruik parameterized queries of prepared statements om SQL-injectie te voorkomen.
- Gebruik een web kwetsbaarheden scanner om SQL injectie kwetsbaarheden snel te vinden.
- Het gebruik van mysqli_real_escape_string gaat SQL-injection tegen, maar is een van de minst goede maatregelen tegen SQL-injection. Het beveiligt niet in alle gevallen de query.

1.1.2. Opdrachtinjectie

- Het is belangrijk om de juiste maatregelen te nemen om injectieaanvallen te voorkomen door gebruikersinvoer te valideren en te ontsmetten.
- Gebruik veilige API's die automatisch commando-injectie voorkomen.
- Beperk de rechten van applicatie-accounts om de impact van een succesvolle aanval te minimaliseren.

1.1.3. Uitvoering van externe code

- Gebruik de nieuwste versies van alle software, inclusief besturingssystemen, webbrowsers en plug-ins.
- Schakel onnodige functies en componenten uit om het aanvalsoppervlak te verkleinen.
- Gebruik een web application firewall (WAF) om bekende aanvalspatronen te blokkeren.

1.1.4. Kwetsbaarheden bij bestandsuploads

- Beperk het type bestanden dat kan worden geüpload.
- Scan geüploade bestanden op malware.
- Sla geüploade bestanden op in een locatie buiten de webroot of in een database.

1.2 Cross-site scripting aanvallen (XSS)

1.2.1. Opgeslagen Cross-Site Scripting Aanvallen

- Output Encoding: Gebruik output encoding om speciale karakters zoals <, >, ", ' te vervangen door HTML-entiteiten. Dit voorkomt dat de browser de geïnjecteerde code uitvoert.
- Content Security Policy (CSP): Gebruik CSP om te bepalen welke bronnen van scripts zijn toegestaan en welke niet. Dit helpt bij het blokkeren van ongewenste scripts.

1.2.2. Gereflecteerde Cross-Site Scripting Aanvallen

- Input Validatie: Valideer gebruikersinvoer grondig en sta alleen specifieke tekens toe. Filter speciale karakters die kunnen worden gebruikt in XSS-aanvallen.

- Output Encoding: Gebruik output encoding om speciale karakters zoals <, >, ", ' te vervangen door HTML-entiteiten. Dit voorkomt dat de browser de geïnjecteerde code uitvoert.

1.2.3. DOM-Gebaseerde Cross-Site Scripting Aanvallen

- Input Validatie: Valideer gebruikersinvoer grondig en sta alleen specifieke tekens toe. Filter speciale karakters die kunnen worden gebruikt in XSS-aanvallen.
- Output Encoding: Gebruik output encoding om speciale karakters zoals <, >, ", ' te vervangen door HTML-entiteiten. Dit voorkomt dat de browser de geïnjecteerde code uitvoert.
- DOM Sanitization: Gebruik DOM sanitization om onveilige HTML-elementen en attributen te verwijderen of te ontsmetten. Dit voorkomt dat de browser de geïnjecteerde code uitvoert.

1.3. Cross-Site Request Forgery (CSRF) aanvallen

- CSRF Token: Gebruik een uniek, willekeurig en onvoorspelbaar token dat wordt gegenereerd voor elke sessie en verzoek. Dit token moet worden gevalideerd door de server om te controleren of het verzoek legitiem is.
- Same-Site Cookie: Gebruik de SameSite-attribuut om te voorkomen dat cookies worden verzonden bij cross-site verzoeken. Dit helpt bij het voorkomen van CSRF-aanvallen.
- Re-authenticatie: Vraag de gebruiker om opnieuw te authenticeren voor gevoelige acties, zoals het wijzigen van wachtwoorden of het overmaken van geld. Dit helpt bij het voorkomen van CSRF-aanvallen.

1.4. Session Hijacking

- HTTPS: Gebruik HTTPS om de communicatie tussen de client en de server te versleutelen. Dit voorkomt dat aanvallers de sessiegegevens onderscheppen of wijzigen.
- Session Timeout: Stel een sessie timeout in om de sessie automatisch te beëindigen na een periode van inactiviteit. Dit voorkomt dat aanvallers de sessie overnemen als de gebruiker de browser niet sluit.
- Session Regeneration: Genereer een nieuw sessie-ID bij elke aanmelding of uitloggen. Dit voorkomt dat aanvallers het oude sessie-ID gebruiken om toegang te krijgen tot de sessie.
- Het implementeren van deze maatregelen helpt bij het verminderen en voorkomen van de risico's geassocieerd met XSS, CSRF en session hijacking. Vergeet niet regelmatig beveiligingsaudits uit te voeren en op de hoogte te blijven van nieuwe beveiligingspraktijken en kwetsbaarheden.

2. MQTT

2.1. Authenticatie en Autorisatie

Standaard biedt MQTT alleen basisauthenticatie met gebruikersnaam en wachtwoord, die in platte tekst worden verzonden. Dit is niet altijd voldoende om de identiteit van de client of de broker te garanderen, vooral als de verbinding niet versleuteld is. Een aanvaller kan de gebruikersnaam en het wachtwoord onderscheppen, wijzigen of vervalsen, en zich voordoen als een client of broker.

2.2. Versleuteling

Standaard biedt MQTT geen versleuteling van de berichten die worden verzonden tussen de clients en de brokers. Dit betekent dat een aanvaller die de verbinding kan afluisteren, de inhoud van de berichten kan zien of manipuleren.

2.3. Quality of Service (QoS)

MQTT heeft drie niveaus van QoS:

- QoS 0: hoogstens eenmaal. Berichten worden alleen verstuurd zonder dat het uitmaakt of het bericht verloren raakt.
- QoS 1: ten minste eenmaal. Dit is een hoger niveau, waarbij een bericht wordt verzonden en moet een bevestiging ontvangen omdat dit soort berichten niet verloren mogen raken.
- QoS 2: precies eenmaal. Dit is het hoogste niveau, waarbij de zender en de ontvanger een reeks van vier berichten uitwisselen om te bevestigen dat het bericht precies eenmaal is afgeleverd.

2.4. Broker Security

Broker security omvat verschillende aspecten, zoals:

- Encryptie: Dit is het proces van het versleutelen van de communicatie tussen de broker en de apparaten, zodat alleen de beoogde ontvangers de berichten kunnen lezen.
- Authenticatie: Dit is het proces van het verifiëren van de identiteit van de apparaten die verbinding maken met de broker. Authenticatie voorkomt ongeautoriseerde toegang tot de broker en de berichten.
- Autorisatie: Dit is het proces van het bepalen van de toegangsrechten van de apparaten tot de broker en de topics. Autorisatie beheert de toegang tot de bronnen en voorkomt misbruik of sabotage van de berichten.
- Monitoring: Dit is het proces van het verzamelen en analyseren van de gegevens over de activiteiten en de prestaties van de broker en de apparaten.

2.5 Message Payload Security

Er zijn verschillende methoden en algoritmen die kunnen worden gebruikt voor message payload security, zoals:

- AES: Advanced Encryption Standard, een symmetrisch versleutelingsalgoritme dat dezelfde sleutel gebruikt voor versleuteling en ontsleuteling.
- ECC: Elliptic Curve Cryptography, een asymmetrisch versleutelingsalgoritme dat publieke en private sleutels gebruikt voor versleuteling en ontsleuteling.
- ChaCha20: Een symmetrisch versleutelingsalgoritme dat een nonce en een sleutel gebruikt voor versleuteling en ontsleuteling.
- XXTEA: XTEA in eXtended mode, een symmetrisch versleutelingsalgoritme dat een sleutel gebruikt voor versleuteling en ontsleuteling.
- RSA: Rivest-Shamir-Adleman, een asymmetrisch versleutelingsalgoritme dat publieke en private sleutels gebruikt voor versleuteling en ontsleuteling.
- HMAC: Hash-based Message Authentication Code, een MAC-algoritme dat een hashfunctie en een geheime sleutel gebruikt om een code te genereren die de identiteit van de afzender en de integriteit van de gegevens kan verifiëren.

2.6. Netwerkbeveiliging

Netwerkbeveiliging omvat verschillende aspecten, zoals:

- Firewall: Een firewall is een apparaat of software die de inkomende en uitgaande netwerkverkeer controleert en filtert op basis van vooraf gedefinieerde regels. Een firewall helpt bij het voorkomen van ongeautoriseerde toegang tot de MQTT-broker of de apparaten, en het blokkeren van schadelijke verzoeken of aanvallen.
- VPN: Een VPN (Virtual Private Network) is een technologie die een beveiligde verbinding tot stand brengt tussen twee of meer apparaten via een openbaar netwerk, zoals het internet. Een VPN kan worden gebruikt om de MQTT-communicatie te beveiligen, vooral als de apparaten zich op verschillende locaties bevinden of gebruik maken van onbetrouwbare netwerken.
- IPsec: IPsec (Internet Protocol Security) is een protocol dat de communicatie tussen twee of meer apparaten op het IP-niveau beveiligt. IPsec kan worden gebruikt om de MQTT-communicatie te beveiligen, vooral als de apparaten zich in hetzelfde lokale netwerk bevinden of gebruik maken van betrouwbare netwerken.

2.7. Beheer van IoT-apparaten

Beheer van IoT-apparaten omvat verschillende processen, zoals:

- Inrichting: Dit is het proces van het toewijzen van een unieke identiteit en configuratie aan elk apparaat dat verbinding maakt met het MQTT-netwerk.
- Monitoring: Dit is het proces van het verzamelen en analyseren van de gegevens over de status, de prestaties en de activiteiten van de apparaten.
- Update: Dit is het proces van het bijwerken van de software of firmware van de apparaten om de functionaliteit, de compatibiliteit of de beveiliging te verbeteren.
- Onderhoud: Dit is het proces van het uitvoeren van preventieve of correctieve acties om de apparaten in goede staat te houden.

3. Reflectie

Om alle informatie te vinden heb ik zelf zitten zoeken en ook copilot (m.a.w. ChatGPT in Edge) gebruikt aangezien deze op het internet ook de bronnen kan voorzien wat heel erg helpt met het opzoeken. Hierdoor ben ik veel te weten gekomen over de verschillende soorten security riscs als het aankomt over web applications en de hoeveelheid risicos waaraan gedacht moet worden is enorm.

Over MQTT is al veel bekend, aangezien wij voor IoT project dit moeten gebruiken en daarvoor ook security moeten toevoegen met namelijk een SSL-key. Daarnaast zijn er heel wat dingen die ik nog niet wist en door deze opdracht nu wel.

4. Bronnen

https://www.avg.com/nl/signal/sql-injection https://www.one.com/nl/website-beveiliging/wat-is-sql-injection https://www.itfaq.nl/website-beveiligen-tegen-sql-injection-aanvallen/ https://geekflare.com/nl/prevent-os-command-injection/ https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_NL_DP6.pdf https://support.microsoft.com/nl-nl/topic/ms14-082-beveiligingsproblemen-in-microsoft-office-kunnen-leiden-tot-uitvoering-van-externe-code-9-december-2014-ce315417-ff86-8c0e-ead5-2ea1c9bba243 https://support.microsoft.com/nl-nl/topic/ms13-098-beveiligingsproblemen-in-windows-kunnen-leiden-tot-uitvoering-van-externe-code-10-december-2013-529ed5d9-3666-1a93-16ac-7129b13e7406 https://www.infomil.nl/onderwerpen/ruimte/omgevingsthema/externe-veiligheid/maatregelen/ https://www.beswic.be/nl/themas/arbeidsplaatsen/atex https://co-prev.be/wp-

content/uploads/2022/05/vernieuwde-guideline-2021-versie-5-nov-2021.pdf
https://websetnet.net/nl/remote-code-execution-attacks-and-prevention-steps/ https://www.techidee.nl/het-vertrouwen-in-de-beveiliging-van-het-uploaden-van-bestanden-is-alarmerend-laag-waarom/1823/
https://bctsoftware.com/nl/informatiebeveiliging-waarom-is-het-zo-belangrijk-en-wat-kunnen-we-doen/
https://www.kpn.com/zakelijk/blog/website-beschermen-tegen-kwetsbaarheden.htm
https://support.microsoft.com/nl-nl/windows/windows-update-veelgestelde-vragen-8a903416-6f45-0718-f5c7-375e92dddeb2 https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2013/ms13-098?redirectedfrom=MSDN https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2014/2915720?redirectedfrom=MSDN