**Voorbereiden**

**Handmatig Pentest Plan**

1. **Verkennen en Informatie Verzamelen**
   * **Doel:** Begrijpen van de applicatie, ontdekking van alle eindpunten en functies.
   * **Methoden:** Gebruik van OWASP ZAP voor interceptie en exploratie van verkeer. Handmatig door de applicatie navigeren.
2. **Input Validatie Testen**
   * **Doel:** Controleren of de applicatie correct omgaat met verschillende soorten invoer.
   * **Methoden:** Handmatig invoeren van speciale tekens, scripts en grote hoeveelheden data in alle invoervelden.
     + **SQL Injection:** Proberen van klassieke SQL-injectiepatronen (' OR '1'='1).
     + **Cross-site Scripting (XSS):** Invoeren van <script>alert('XSS')</script> in verschillende velden.
3. **Authenticatie en Autorisatie Testen**
   * **Doel:** Controleren van sterkte van authenticatie- en autorisatiecontroles.
   * **Methoden:** Proberen van brute-force aanvallen op login eindpunten, testen van zwakke wachtwoorden, en controleren van toegang tot gevoelige gegevens zonder juiste rechten.
4. **Beveiligingsheaders Testen**
   * **Doel:** Verifiëren of alle aanbevolen beveiligingsheaders correct zijn ingesteld.
   * **Methoden:** Handmatig inspecteren van HTTP-headers met OWASP ZAP.
5. **API Security Testen**
   * **Doel:** Controleren van de beveiliging van API-eindpunten.
   * **Methoden:** Verzenden van handmatige API-verzoeken met ongeoorloofde methodes, verkeerde content-types, en zonder juiste API-sleutels.

**Geautomatiseerd Pentest Plan**

1. **Verkennen en Informatie Verzamelen**
   * **Tool:** OWASP ZAP
   * **Acties:** Crawlen van de applicatie om alle eindpunten en pagina's te ontdekken.
2. **Vulnerability Scanning**
   * **Tool:** OWASP ZAP
   * **Acties:** Automatische scan uitvoeren voor bekende kwetsbaarheden zoals SQL-injectie, XSS, en ontbrekende beveiligingsheaders.
3. **API Security Testing**
   * **Tool:** OWASP ZAP
   * **Acties:** Automatische testen van API-eindpunten voor kwetsbaarheden zoals injecties, ongeoorloofde toegang en verkeerde content-types.

**Uitvoeren**

**Handmatige Pentest Uitvoering**

1. **Verkennen en Informatie Verzamelen**
   * Navigeren door de applicatie met OWASP ZAP ingeschakeld voor verkeer interceptie.
   * Identificeren van alle eindpunten, formulieren, en functionaliteiten.
2. **Input Validatie Testen**
   * Invoeren van SQL-injectie patronen in zoekvelden, loginvelden, en andere invoervelden.
   * Invoeren van XSS payloads in verschillende invoervelden en observeren van de reacties.
   * Testen van grote hoeveelheden data invoer en speciale tekens.
3. **Authenticatie en Autorisatie Testen**
   * Uitvoeren van brute-force aanvallen op login eindpunten met tools zoals OWASP ZAP.
   * Proberen van zwakke wachtwoorden en standaard gebruikersnamen.
   * Handmatig testen van toegang tot admin-functies zonder in te loggen.
4. **Beveiligingsheaders Testen**
   * Inspecteren van HTTP-headers voor beveiligingsheaders zoals X-Content-Type-Options, Content-Security-Policy, en Strict-Transport-Security.
5. **API Security Testen**
   * Verzenden van handmatige API-verzoeken met OWASP ZAP.
   * Proberen van ongeoorloofde methodes zoals DELETE en PUT.
   * Verzenden van verzoeken zonder API-sleutels en controleren van de reacties.

**Geautomatiseerde Pentest Uitvoering**

1. **Verkennen en Informatie Verzamelen**
   * Gebruik OWASP ZAP om de applicatie te crawlen en alle eindpunten te ontdekken.
   * Configureren van de scan om alle pagina's en API-eindpunten te verkennen.
2. **Vulnerability Scanning**
   * Uitvoeren van een volledige kwetsbaarheidsscan met OWASP ZAP.
   * Analyseren van de resultaten en identificeren van alle gevonden kwetsbaarheden.
3. **API Security Testing**
   * Configureren van OWASP ZAP om beveiligingstests uit te voeren op API-eindpunten.
   * Uitvoeren van automatische testen met OWASP ZAP op API-eindpunten.

De raporten zijn de pdf die in de zelfde map zitten

(kon geen sql-map doen het lukt me niet)