

Standardrapport for udført sårbarhedsscanning

**Tilladelses-  
indehaver**

Navn

Telefonnummer

Adresse

Postnr. og by

CVR-/SE-nr.

Kontaktperson/Mailadresse

**Certificeringsdato**

Forrige scanning

Nuværende scanning

Forventet dato for *næste* scanning

**Testvirksomhed**

Navn

Telefonnummer

Adresse

Postnr. og by

CVR-/SE-nr.

Kontaktperson/Mailadresse

Har testvirksomheden en gyldig akkreditering?

Ja \_\_\_\_

Nej \_\_\_\_

**NB: Dokumentation for akkreditering skal vedlægges.  
Alternativt indsættes link til akkreditering her:**

Link til akkreditering:

**Testvirksomhe-  
dens underleve-  
randør**

Skal kun udfyldes hvis  
testvirksomheden har  
brugt en underleve-  
randør

Navn

Adresse

Postnr. og by

De ansatte skal sørge for, at certificeringen bliver udført fagligt forsvarligt og skal supervisere og attestere certificeringsklæringen. Flere ansatte, som til sammen opfylder kravene, kan i fællesskab supervisere og attestere certificeringen. Udfyld nedenstående sektion med informationer om en supervisor, der opfylder kravene for hver af sektionerne (a, b og c). Det kan være én supervisor, der opfylder samtlige krav eller en forskellig supervisor for hver sektion.

### Krav supervisor

a) Personen, der superviserer og/eller attesterer denne rapport skal have en relevant uddannelse eller andre relevante kvalifikationer

|                           |               |
|---------------------------|---------------|
| Navn                      | Telefonnummer |
| E-mail adresse            |               |
| Uddannelse                | Periode       |
| Relevante kvalifikationer | Periode       |

b) Personen, der superviserer og/eller attesterer denne rapport skal være certificeret:

Navn

| Navn på certificering                            | Sæt kryds |
|--|-----------|
| EC-Council, Certified Ethical Hacker (CEH)       |           |
| EC-Council, Licensed Penetration Tester (LPT)    |           |
| IACRB Certified Penetration Tester (CPT)         |           |
| GIAC Certified Penetration Tester (CPEN)         |           |
| CESG CHECK Team Leader                           |           |
| CESG CHECK Team Member                           |           |
| CREST Infrastructure Certification               |           |
| CREST Registered Tester                          |           |
| Tiger Scheme Senior Security Tester              |           |
| Tiger Scheme Qualified Security Tester           |           |
| Offensive Security Certified Professional (OSCP) |           |

### Tilladelsesindehavers underleverandører

Det er tilladelsesindehaverens ansvar, at deres underleverandør(-er) får foretaget sårbarhedsscanninger i overensstemmelse med certificeringsprogrammet. Testvirksomheden skal sikre sig, at tilladelsesindehaverens underleverandør(-er) har en gyldig sårbarhedsscanning. I skemaet nedenfor anføres oplysninger om eventuelle underleverandørers sårbarhedsscanninger.

| Navn på underleverandør | Dato for sårbarhedsscanning (DD-MM-YYYY) | Er scanning bestået: Ja/Nej |
|-------------------------|--|-----------------------------|
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |
|                         |  |                             |

---

**Sårbarheds-  
scanning**

Er sårbarhedsscanningen gennemført og bestået?

Ja \_\_\_\_\_ Ja, fejl er rettet \_\_\_\_\_ Nej \_\_\_\_\_

NB: Hvis en enkelt underleverandørs sårbarhedsscanning ikke er bestået, så kan den samlede sårbarhedsscanning heller ikke bestå. Hvis sårbarhedsscanningen ikke er bestået, skal der, i bilaget til rapporten, beskrives en plan for udbedring af sårbarhederne samt beskrives hvilke kompenserende kontroller, der udføres, indtil sårbarhederne er udbedret.

---

**Intern funktion** Er sårbarhedsscanningen foretaget af en intern funktion hos tilladelsesindehaver?

Ja \_\_\_\_\_ Nej \_\_\_\_\_

---

**Andre oplysninger** Øvrige oplysninger, som er relevante for Spillemyndigheden skal I oplyse i bilaget.

---

**Erklæring og underskrift**

Jeg erklærer ved min underskrift, at de oplysninger, der er afgivet på denne certificeringsrapport er korrekte. Jeg er indforstået med, at manglende oplysninger eller bevidste fejl i oplysningerne, kan medføre at certificeringsrapporten bliver afvist. Hvis der sker ændringer i de afgivne oplysninger, skal I straks underrette Spillemyndigheden.

Dato

Navn

Underskrift

\_\_\_\_\_

\_\_\_\_\_

.....

Dato

Navn

Underskrift

\_\_\_\_\_

\_\_\_\_\_

.....