Pentest Rapport

[naam applicatie]

|  |  |
| --- | --- |
| Versie |  |
| Datum |  |
| Naam |  |
| Studentnummer |  |

Inhoud

[[Uitleg bij dit sjabloon] 3](#_Toc105736046)

[Aanbevelingen 4](#_Toc105736047)

[Scope/Bereik 5](#_Toc105736048)

[Uitgevoerde tests 6](#_Toc105736049)

[Gevonden kwetsbaarheden 7](#_Toc105736050)

# [Uitleg bij dit sjabloon]

[

Het is de bedoeling dat je met dit sjabloon je eigen pentest rapport maakt. In dit sjabloon wordt uitleg gegeven over hoe je de onderwerpen kan beschrijven.

Het is de bedoeling dat je de uitleg verwijderd en je eigen inhoud toevoegt.

**Alles wat in dit document tussen blokhaken staat [], moet verwijderd worden als je het document inlevert. Ook deze pagina met uitleg moet je vewijderen.**

**Vergeet ook niet om de inhoudsopgave bij te werken!**

]

# Aanbevelingen

*[*

*Nadat je de pentest hebt uitgevoerd schijf je je aanbevelingen op. Dit is een lijst met punten die je de klant/gebruiker aanbeveelt om uit te voeren of te verbeteren]*

***Voorbeeld:***

***Er is vastgesteld dat teveel ongebruikte poorten openstaan. Ik beveel aan om de volgende poorten te sluiten: 21, 8080***

*]*

# Scope/Bereik

[

Hier beschrijf je wat de scope (bereik) is van je test. Als je bijvoorbeeld alleen een bepaald deel van het netwerk hebt getest, dan beschrijf je welk deel dat is.]

**Voorbeeld**

|  |  |
| --- | --- |
| **Network** | **Toelichting** |
| 10.0.1.0/24 | Het netwerk waarbinnen de geteste computer valt. |

|  |
| --- |
| **Software** |
| MySQL  Apache  ssh |

]

# Uitgevoerde tests

[

Hier komt een lijst met tests en bevindingen.

Voorbeeld:

|  |  |
| --- | --- |
| **Test** | **Bevinding** |
| In de applicatie kan een document worden geupload. Geprobeerd is om een PHP bestand met schadelijke code te uploaden. | Het was niet mogelijk om PHP bestanden te uploaden |

]

# Gevonden kwetsbaarheden

[

Hier schrijf je op welke kwetsbaarheden je hebt gevonden. Het kan gaan om kwetsbaarheden in de software, maar ook bijvoorbeeld in de toegang tot de server. Hier komen dus alle punten uit de bovenstaande lijst met tests die niet goed door de test kwamen.

Alle kwetsbaarheden die je hier beschrijf komen ook weer terug bij de aanbevelingen aan het begin van het document.

Per gevonden kwetsbaarheid beschrijf je:

* Hoe je de kwetsbaarheid hebt vastgesteld
* Wat het risico is van de kwestbaarheid (hoog, medium, laag)
* Wat de impact is van het oplossen (moeilijk, medium, eenvoudig)]

Voorbeeld:

**SSH Toegang**

Er kan met ssh ingelogd worden door gebruik te maken van username en password. Dit geeft een veiligheidsrisico omdat de server met brute force attacks aangegevallen kan worden.

Risico: hoog

Oplossingsmoeilijkheid: eenvoudig

]