



## Værktøj til analyse af source code:

### Baggrund:

En af Forsvarets opgaver er at sikre data og it-systemer. Disse it-systemer kan være alt fra open source til proprietære systemer. Fælles for disse er at de skal analyseres for evt. sikkerhedsbrister, således at en kompromittering kan undgås.

Et af de programmeringssprog der ligger til grund for vores it-systemer er PHP.

PHP er et scripting-sprog, der i høj grad bruges til dynamiske hjemmesider. Sproget er som sådan meget udbredt og danner grundlag for en lang række programmer, hvoraf nogle bliver brugt indenfor Forsvaret.

### Opgaven:

Der ønskes udarbejdet et program, der kan analysere PHP-kode og udarbejde en rapport der redegør for evt. fejl eller mulige svagheder i koden, der kan medføre kompromittering af information.

Niveauet af opgave kan variere, men de mest gængse kompromitteringer så som SQL injections, RFI/LFI samt andre ”lette fejl” skal som minimum kunne findes. I rapportdelen ønskes en funktionalitet, der kan spore evt. sårbarheder gennem koden.

Opgaven kan udvides til at finde andre potentielle exploits som ligger uden for PHP så som XSS, AJAX ol.

### Krav:

Opgaven skal skrives i Python.

Rapportgenerering skal være i et tilgængeligt format, f.eks. XML, HTML eller lignende.

Det er et krav fra opgavestillers side at de studerende underskriver en NDA.

### Bidrag:

- Forsvaret bidrager med hostning af opgaven
  - Subversion
  - TracBackup skal selv varetages af de studerende
- Møder med slutbrugere fra forsvaret