

# Beveiligingsaspecten van webapplicatie ontwikkeling met PHP

---

Versie 1.0

Wouter van Kuipers

7-7-2008

## 1 Inhoud

|     |                        |   |
|-----|------------------------|---|
| 1   | Inhoud .....           | 2 |
| 2   | Inleiding.....         | 2 |
| 3   | Probleemgebied.....    | 3 |
| 3.1 | Doelstelling .....     | 3 |
| 4   | Onderzoeksvraag .....  | 3 |
| 4.1 | Deelvragen .....       | 3 |
| 5   | Verantwoording .....   | 4 |
| 6   | Werkwijze .....        | 4 |
| 6.1 | Literatuurstudie ..... | 4 |
| 6.2 | Dataverzameling .....  | 4 |
| 6.3 | Data-analyse .....     | 4 |
| 7   | Producten.....         | 5 |
| 8   | Planning .....         | 6 |

## 2 Inleiding

Deze afstudeeropdracht zal worden uitgevoerd in opdracht van de Radboud Universiteit Nijmegen, afdeling Digitale Security (DS), onder begeleiding van dhr. E. Poll (Erik)

Contactgegevens student      Wouter van Kuipers s652830 [w.vankuipers@student.ru.nl](mailto:w.vankuipers@student.ru.nl)

De belangrijkste doelstellingen van het onderzoeksplan zijn:

- Welke probleemstelling en opdracht het afstuderen omvat;
- Welke producten er opgeleverd zullen worden;
- Welke randvoorwaarden van belang zijn;
- Hoe het project georganiseerd wordt;
- Welke uitgangssituatie zich voordoet;
- Volgens welke planning het project uitgevoerd wordt.

In hoofdstuk 3 wordt het probleemgebied beschreven en zal de probleemstelling worden afgebakend. In hoofdstuk 4 word de onderzoeksvraag en bijbehorende subvragen besproken. Hoofdstuk 5 beschrijft de verantwoording en in hoofdstuk 6 zal worden ingegaan op de werkwijze. Hoofdstuk 7 zal de op te leveren producten beschrijven waarna in hoofdstuk 8 de planning wordt besproken.

### 3 Probleemgebied

Het onderzoek zal gericht zijn op de security aspecten die van toepassing zijn vóór, tijdens en na het ontwikkelingsproces van PHP applicaties. Hierbij wordt gekeken waarom er voor PHP gekozen is en voor welke versie van PHP. Daarnaast wordt ook gekeken hoe er om wordt gegaan met de beveiliging van de applicatie tijdens de verschillende stadia van het ontwikkelproces en in latere stadia tijdens het ontwikkelproces. Ook zal gekeken worden welke externe factoren zoals Operating Systems en Webserver invloed hebben op de veiligheid van de applicatie en of er al standaard oplossingen zijn in de vorm van frameworks of (ISO) standaarden. Dit alles wordt vergeleken met de gevaren die lokale (intranet) en globale (internet) applicaties lopen.

#### 3.1 Doelstelling

Het doel van het onderzoek is het onderzoeken van en eventueel aanpassen/opstellen van een verzameling richtlijnen waarmee gewerkt kan worden tijdens en na het ontwikkelproces van een applicatie in PHP. Dit ontwikkelproces is globaal in te delen in drie stadia;

1. **Ontwerp**

Tijdens dit stadium wordt de applicatie ontworpen, dit kan zijn omdat er een nieuwe applicatie moet komen aan de hand van een idee of wens van de opdrachtgever of omdat een bestaande applicatie moet worden omgezet naar een webapplicatie.

2. **Ontwikkelstadia**

Tijdens dit stadium wordt de applicatie ontwikkeld.

3. **Beheerstadia**

Tijdens dit stadium wordt de applicatie beheerd en worden aanpassingen gedaan die tijdens het ontwikkelproces niet (goed) zijn geïmplementeerd (bugs) of die later door de opdrachtgever worden aangedragen (verbeteringen).

### 4 Onderzoeksvraag

- *Hoe wordt binnen de Radboud Universiteit omgegaan met beveiliging van Web applicaties, in het bijzonder PHP applicaties, tijdens de verschillende stadia van het ontwikkelproces?*

#### 4.1 Deelvragen

- *Welke gevaren zijn er op het gebied van beveiliging van Web applicaties, in het bijzonder PHP applicaties, tijdens de verschillende stadia van het ontwikkelproces?*
- *Welke richtlijnen zijn er binnen de Radboud Universiteit op het gebied van beveiliging van Web applicaties, in het bijzonder PHP applicaties, tijdens de verschillende stadia van het ontwikkelproces?*
- *Zijn de richtlijnen van de Radboud Universiteit op het gebied van beveiliging van Web applicaties, in het bijzonder PHP applicaties, tijdens de verschillende stadia van het ontwikkelproces volledig/voldoende om de kwaliteit van deze applicaties te kunnen garanderen?*
- *Zijn er andere/betere richtlijnen die de kwaliteit van Web applicaties, in het bijzonder PHP applicaties, op het gebied van security kunnen verbeteren?*

## 5 Verantwoording

In het dagelijks leven ben ik freelance PHP programmeur voor diverse kleine en middelgrote ondernemingen. Tijdens deze werkzaamheden en mijn HBO en WO studie kom ik steeds vaker webapplicaties tegen die gevoelige informatie verwerken die vroeger alleen lokaal op een server binnen een beveiligd netwerk zouden draaien. Doordat deze applicaties zijn omgezet in een webapplicatie treden er echter allerlei security problemen op die vroeger niet aan de order waren.

Deze problemen worden vaak onderschat. Als er al een ontwikkelaar is die aangeeft dat er ook op het security aspect geïnvesteerd moet worden met behulp van tijd en geld, dan wordt er vaak voor gekozen om met een minimale investering door te gaan. Hierbij wordt de aandacht die aan de beveiliging van de applicatie wordt besteed tot een minimum beperkt.

Op het HBO heb ik de minor webdevelopment gevolgd. Deze minor die gericht was in het ontwikkelen bevatte ook een onderdeel over security waardoor ik mij voor het eerst bewust werd over de gevaren die webapplicaties lopen. Tijdens de bachelor fase van de Master ben ik, ondermeer door het vak Security dermate in deze materie geïnteresseerd geraakt, dat ik met dit scriptieonderwerp naar de afdeling Digitale Security ben gegaan en in overleg met de heer Poll deze opdracht heb geformuleerd.

## 6 Werkwijze

Het onderzoek zal worden opgesplitst in de volgende drie fasen:

### 6.1 Literatuurstudie

Tijdens deze fase zal er literatuur bestudeerd worden die te maken heeft met de beveiliging van Web applicaties, en in het bijzonder PHP applicaties. De literatuur die bestudeerd zal worden zal gebruikt worden om de kennis over het probleemgebied te vergroten en om de conclusie te kunnen onderbouwen.

### 6.2 Dataverzameling

Tijdens deze fase zal er informatie verzameld worden over de wijze waarop binnen de Radboud Universiteit Web applicaties, en in het bijzonder PHP applicaties, worden ontwikkeld. Hiervoor zullen onder meer de huidige applicaties en richtlijnen worden geanalyseerd en zullen er interviews worden gehouden met de ontwikkelaars van deze applicaties. Ook zal er tijdens deze fase een analyse gemaakt worden van de security threads die de applicaties op de RU lopen en zal er één of meerder PHP applicaties die binnen de RU zijn ontworpen worden onderzocht op beveiligingscomplicaties.

### 6.3 Data-analyse

Tijdens deze fase worden de bevindingen van de voorgaande fase geanalyseerd en verwerkt tot een conclusie. Aan de hand van deze conclusie zullen ook de nodige richtlijnen worden opgesteld en/of aangepast zodat er een duidelijk pakket met richtlijnen zal ontstaan waarmee beveiliging van Web applicaties, en in het bijzonder PHP applicaties, op de RU in het vervolg kunnen worden verbeterd.

## 7 Producten

Het onderzoek zal naast de scriptie ook de volgende producten opleveren;

- **Rapport met huidige richtlijnen**
  - Analyse van de huidige richtlijnen (of ideeën/inzichten die betrekking hebben op deze richtlijnen) die er op dit moment binnen de Radboud Universiteit gelden voor het ontwikkelen van Web applicaties. Dit document is met name bedoeld voor de interne ontwikkelaars van de RU, de inhoud zal geschikt zijn voor zowel ontwikkelaars al managers.
- **Rapport met mogelijke threads**
  - Analyse van de gevaren die Web applicaties binnen de Radboud Universiteit lopen. Wie zijn de stakeholders en welke belangen behartigen zij. Dit document is bedoeld voor beheerders van een webapplicatie die meer willen weten over de gevaren die hun applicatie loopt, de inhoud zal vooral geschikt zijn voor managers.
- **Analyserapport software**
  - Analyserapport van de geanalyseerde software. Welke (mogelijke) problemen zijn er gevonden tijdens de analyse en welke gevaren bieden deze problemen. Dit document is met name bedoeld voor de interne ontwikkelaars van de RU, de inhoud zal vooral geschikt zijn voor ontwikkelaars.
- **Verbetervoorstel richtlijnen**
  - Rapport met een voorstel voor het verbeteren van de richtlijnen ten opzichte van het ontwikkelen van een Web applicaties, en in het bijzonder PHP applicaties, binnen de Radboud Universiteit. Dit document is met name bedoeld voor de interne ontwikkelaars van de RU, de inhoud zal geschikt zijn voor zowel ontwikkelaars al managers.

Naast deze papieren/digitale producten is het wellicht interessant om eventuele bevindingen te presenteren aan geïnteresseerde partijen. Hierbij kan gedacht worden aan de PHP werkgroep van de RU (Peru, PHP Exchange RU) of The Open Web Application Security Project (OWASP). Daarnaast is er de mogelijkheid om een publicatie te schrijven van mijn bevindingen die gepubliceerd kan worden in vakgerelateerde tijdschriften en/of websites als CT, phpfreakz.nl, phphulp.nl en ppgg.nl.

## 8 Planning

| Product                            | Maand<br>Week | Juli |    |    |    |    | Augustus |    |    |    |    | September |    |    |    |    | Oktober |    |    |    | November |    |    |    | December |    |    |  | 1 |
|------------------------------------|---------------|------|----|----|----|----|----------|----|----|----|----|-----------|----|----|----|----|---------|----|----|----|----------|----|----|----|----------|----|----|--|---|
|                                    |               | 27   | 28 | 29 | 30 | 31 | 32       | 33 | 34 | 35 | 36 | 37        | 38 | 39 | 40 | 41 | 42      | 43 | 44 | 45 | 46       | 47 | 48 | 49 | 50       | 51 | 52 |  |   |
| Plan van aanpak & kickoff          |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
|                                    |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| <b>Literatuurstudie</b>            |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Verzamelen bronnen                 |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Analyse bronnen                    |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
|                                    |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| <b>Dataverzameling</b>             |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Verzamelen richtlijnen             |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Analyse richtlijnen                |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Analyserapport huidige richtlijnen |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Analyserapport threads             |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Analyserapport software            |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
|                                    |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| <b>Data-analyse</b>                |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Terugkoppeling bevindingen         |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Verbetervoorstel richtlijnen       |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Scriptie (voorlopige versie)       |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Scriptie (eindversie)              |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
|                                    |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |
| Terugkoppeling scriptie begeleider |               |      |    |    |    |    |          |    |    |    |    |           |    |    |    |    |         |    |    |    |          |    |    |    |          |    |    |  |   |

### Legenda

Definitieve versie

Geplande werkzaamheden

Vakantie