Hanzehogeschool Groningen
University of Applied Sciences

Instituut voor Communicatie, Media & IT

Thema 4.1 I:
Web Application Development

Opgaven week 4

1. Inleiding

In deze week staat beveiliging en oauth centraal. Bij de opgaven wordt uitgegaan van de energie-monitorsite die in de vorige weekopgaven is gemaakt. Mocht deze niet of onvoldoende afgerond zijn, dan volstaat het om met een dummy-site te werken.

Opgave 1: Beveiliging theorie

1. Bestudeer de owasp password storage cheat sheet. Hierin worden vier tips gegevens voor de opslag van wachtwoorden. Beschrijf deze vier en geef van elk een voor- en een nadeel.
2. Geef argumenten waarom een dergelijke beveiliging niet altijd noodzakelijk is.
3. Wat is SQL injection en op welke manier kan dat gebruikt worden om een database te kraken?
4. Op welke manier kan query parameterization gebruikt worden om sql-injectie tegen te gaan? Geef aan op welke manier dit in het toegewezen framework toegepast wordt.

5. Wat is session-hijacking en op welke manier kan dit gebruikt worden voor identity-theft?

```
<script>
     var initData = <%= data.to_json %>;
</script>
```

6. Bekijk het onderstaande code-fragment:

   Welk gevaar schuilt er in dit fragment en op welke manieren is dat te omzeilen?

7. Bestudeer het artikel Seven steps for building a secure web-application. Geef van de zeven stappen die hierin genoemd worden elk een voor- en een nadeel. Is het wenselijk om deze stappen in elke web-applicatie in te bouwen?

Opgave 2: flickr-feed

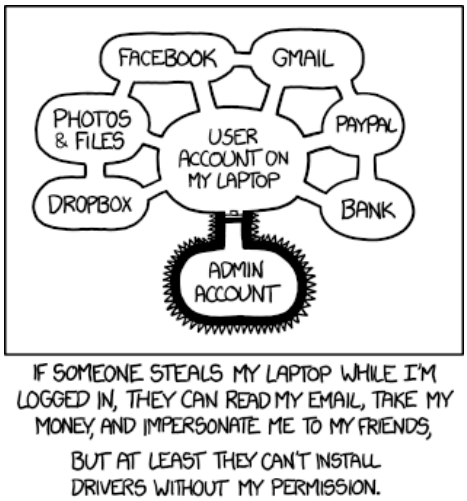
1. Maak gebruik van de publieke flick-api om foto's aan de energie-monitorsite toe te voegen. Zorg er hierbij voor dat de onderstaande functionaliteit wordt geïmplementeerd:

- ✓ Ergens op de pagina moet een foto te zien zijn die van flickr afkomstig is.
- ✓ De foto wordt automatisch elke vijf seconden vervangen door een andere foto; hierbij schuift de nieuw foto over de oude heen.
- ✓ De foto's die hier te zien zijn, hebben als onderwerp (tag) sustainability, urban gardening of solar panels.
- ✓ De titel van de foto en de datum waarop deze genomen is staan onder de foto.
- ✓ Wanneer op de foto geklikt wordt, wordt de op dat moment getoonde foto in flickr zelf in een nieuw tabblad geopend.
- ✓ De beheerder van de site kan de tags waarop de foto's geselecteerd worden en de snelheid waarmee deze worden getoond aanpassen.

2. Demonstreer het resultaat aan de practicumdocent.

Opgave 3: login met Facebook

1. Beschrijf een aantal voor- en nadelen van inloggen via een derde partij door gebruik te maken van OAuth.
2. Wat zijn de grote verschillen tussen OAuth 1.0 en OAuth 2.0?
3. Maak gebruik van OAuth 2.0 om inloggen in de site via een andere partij mogelijk te maken. Kies uit de lijst van service providers op wikipedia minimaal twee providers.
4. Demonstreer de werking en de code aan de practicum-docent.



Opgave 4: How to hack a website

1. Bekijk de presentatie van Susan Loveland, die op youtube te vinden is.
2. Zij geeft een aantal methoden en technieken weer waarop een website is te hacken. Noem hier een aantal van.
3. Geef van de genoemde punten weer in hoeverre dit een werkelijk probleem voor een website vormt.