Mock Exam Web Security

Wees duidelijk, en kort maar krachtig in je antwoorden. Succes!

1. Waarom is het beter een POST dan een GET request te gebruiken als sommige parameters confidentieel zijn, ook al kan een aanvaller die het netwerkverkeer afluistert in beide gevallen al deze data voorbij zien komen?

2. Hoe werkt HSTS? Leg bij je antwoord ook uit tegen welke soort aanvallen het bescherming biedt, en hoe.

3. Wat is het verschil tussen gewone en blind SQL injection?

4. Misbruikt CSRF het vertrouwen van een website in de client of het vertrouwen van de client/gebruiker in een website? Motiveer je antwoord.

5. XSS aanvallen maken soms ook gebruik van CSRF. Schets een voorbeeld van een XSS aanval waarbij geen sprake is van CSRF, en schets een voorbeeld van een XSS aanval waarbij óók sprake is van CSRF.

6. Beschouw de onderstaande webpagina die een andere webpagina als iframe opneemt en een knopje aanbiedt om de JavaScript functie `f` van deze binnenste webpagina aan te roepen

```
<html> <body>
   <iframe src="http://xx.com/x.html"> </iframe>
   <input type="button" value="Roep f aan op iframe above"
          onclick="frames[0].f();">
</body></html>
```

   a) Onder welke voorwaarden zal de aanroep van `f` toegestaan zijn, en wanneer niet?

   b) Wat is de motivatie voor deze voorwaarden, vanuit oogpunt voor security? Met andere woorden, wat voor attacks hoopt men met deze voorwaarden te voorkomen?

7. Wat is het verschil tussen een cookie `secure` maken en een cookie `HttpOnly` maken?

8. a) Wat is een path traversal aka file name injection attack?

   b) Noem tenminste twee tegenmaatregelen tegen zulke aanvallen, en leg uit hoe ze werken.

9. Met SSL stripping kan een aanvaller een HTTPS tunnel tussen de browser en de server proberen open te breken, en vervangen door hetzij (i) een HTTP verbinding tussen de browser en hemzelf en een HTTPS verbinding tussen hemzelf en de server, of door (ii) een HTTPS verbinding tussen de browser en hemzelf en een HTTPS verbinding tussen hemzelf en de server. over tweede geval.

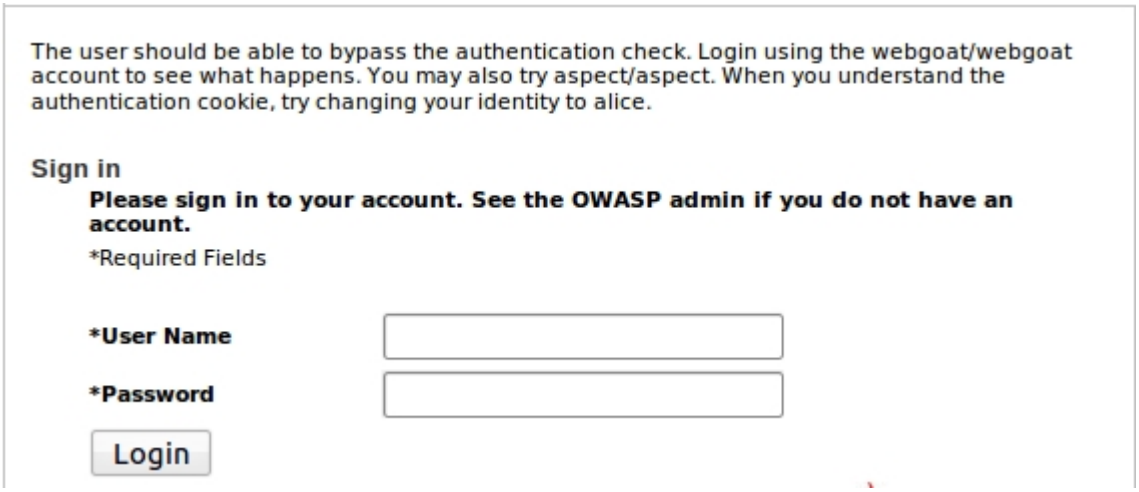
   Wat zijn voor- en nadelen van de eerste type aanval ten opzichte van het tweede type aanval, vanuit het perspectief van de aanvaller?

10. Hoe werkt een Remote File Inclusion aanval op een PHP web applicatie?

11. Stel iemand heeft geen Facebook-account. Is het mogelijkheid dat er toch een privacy risico is, waarbij er informatie lekt aan Facebook?

    Motiveer je antwoord. Leg hierbij uit waarom dit gevaar er (mogelijk/altijd) wel of niet is, en zoja, welke informatie er lekt, en wat de gebruiker hier nog tegen zou kunnen doen.

12. Deze vraag gaat over de WebGoat opdracht om een authenticatie cookie te spoofen.



Als je op deze web inlogt met user name 'webgoat' en wachtwoord 'webgoat' set server een sessie cookie met daarin `AuthCookie=65432ubphcfx`. Als je uitlogt, en opnieuw inlogt, maar nu met user name 'aspect' en wachtwoord 'aspect', dan staat er in het cookie `AuthCookie=65432udfqtb`.

Hou kon je nu als user 'bob' inloggen zonder het password van bob te kennen?

Welke tools (of soort tools) heb je nodig om deze aanval uit te voeren, zowel om te achterhalen hoe een en ander werkt, en om de aanval daadwerkelijk uit te voeren.

13. Bij twee van de practicumopdrachten bij `websecurity.cs.ru.nl` moest je een cookie stelen. Beschrijf kort de stappen er in zo'n aanval zitten, en welke infrastructuur de aanvaller hierbij nodig heeft.