Instituto Superior de Engenharia de Lisboa
Licenciatura/Mestrado em Engenharia Informática e de Computadores
Segurança Informática
Terceira série de exercícios, Semestre de Inverno de 16/17
Data de entrega: 13 de Janeiro de 2016

---

1. No contexto do OpenID Connect, e usando o *implicit flow* [1], porque motivo é essencial que o cliente valide a assinatura do *ID Token*?

2. Considere o modelo RBAC_1.

   2.1. É possível que a adição de um utilizador a um *role* diminua as suas permissões?

   2.2. Apesar de não haver permissões negativas, que mecanismo do modelo pode ser usado para limitar a associação entre *roles* e permissões? Dê um exemplo.

   2.3. Seja u um utilizador, p uma permissão e dois *roles*, r_1 e $r_2 \in R$, tais que $r_2 \geq r_1$. Se $(u, r_2) \in UA$ e $(p, r_1) \in PA$, isso significa que qualquer sessão s com $user(s) = u$ tem acesso à permissão p?

3. O que é que um atacante consegue obter ao realizar com sucesso um ataque de *cross-site scripting*? Forneça pelo menos um exemplo concreto.

4. Quais as diferenças entre as soluções "Synchronizer (CSRF) Tokens" e "Double Submit Cookie" propostas pela OWASP [2] para evitar ataques de CSRF?

5. Implemente um componente (e.g. biblioteca de classes ou módulo NPM) para realizar as funções de *Policy Decision Point* (PDP) com os seguintes requisitos:

   - Suporte para o modelo $RBAC_1$, em que os utilizadores, *roles* e permissões são definidos por *strings*.
   - Utilização de ficheiros de configuração ou de outro repositório alternativo (e.g. base de dados) para o armazenamento da política.
   - Suporte para realização de interrogações sobre a política (e.g. permissões de um dado utilizador numa sessão).

6. Pretende-se desenvolver um *Policy Enforcement Point* (PEP) para testar o PDP realizado na alínea anterior. Use a componente de autenticação da aplicação web desenvolvida na alínea 7 da segunda série. Acrescente à aplicação um conjunto de rotas cuja decisão de acesso é delegada no PDP, usando uma política RBAC_1 que inclua uma hierarquia de *roles* com dois ou mais níveis de herança.

7. Elabore um documento, até 2500 palavras, com base num dos seguintes temas:

   - *Passwords* gráficas - `https://goo.gl/ccPi17`, `https://goo.gl/Gbx2p2`;
   - Ataques ao OAuth 2.0 - `https://goo.gl/Msh20u`;
   - Especificação *User-Managed Access* (UMA) - `https://goo.gl/pbRnPO`;
   - Vulnerabilidades de injecção de comandos em aplicações web - `https://goo.gl/wQh45z`;
   - Código malicioso escondido em imagens - `https://goo.gl/6AZvtz`, `https://goo.gl/Q21R5H`.

   Tendo por base o tema escolhido e o(s) artigo(s)/norma a ele associado, organize o documento em quatro secções, com a seguinte estrutura: i) qual a motivação do assunto / o que se pretende resolver; ii) o que outros fizeram na área; iii) qual a metodologia usada; iv) quais os resultados;

   Recomenda-se o uso do template IEEE [3].

Referências

[1] `http://openid.net/specs/openid-connect-core-1_0.html#ImplicitFlowSteps`, visitado a 6 de dezembro de 2016.

[2] `https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet`, visitado a 6 de dezembro de 2016.

[3] `https://www.ieee.org/conferences_events/conferences/publishing/templates.html`, visitado a 6 de dezembro de 2016.

ISEL, 9 de Dezembro de 2016.