Instituto Superior de Engenharia de Lisboa
LEIC, LEIRT, LEIM
Segurança Informática
Terceira série de exercícios, Semestre de Inverno de 20/21
Entregar até 24 de janeiro de 2021

1. No contexto do protocolo *OpenID Connect*:

   1.1. Que elementos foram adicionados em relação à *framework* OAuth 2.0?

   1.2. Se a aplicação cliente (*relying party*) usar 2 fornecedores de identidade, e tiver um total de 100 utilizadores, quantos `client_id` tem de gerir?

2. Tendo em conta as abordagens de controlo de acessos estudadas, lista de controlo de acessos (ACL) e lista de capacidades, indique em que tipo de controlo se pode enquadrar a estrutura `access_token` da *framework OAuth 2.0*.

3. Considere os diferentes níveis do modelo RBAC.

   3.1. De que forma são suportados os princípios de segurança *Least Privilege* e *Separation Of Duty*?

   3.2. É possível existir uma sessão associada ao utilizador u e com o *role* r activo, sem que (u, r) esteja na relação *user assignment* (UA)?

4. Considere a bibliteca de autorização Casbin [1]:

   4.1. Explique de que forma uma aplicação consegue através desta biblioteca configurar um modelo de segurança e a concretização de uma política.

   4.2. Considere a seguinte política definida usando o modelo $RBAC_1$:

   - $U = \{u_1, u_2\}$, $R = \{r_0, r_1, r_2, r_3\}$, $P = \{p_0, p_2, p_3\}$
   - $\{r_0 \preceq r_1, r_0 \preceq r_2, r_2 \preceq r_3\} \subseteq RH$
   - $UA = \{(u_1, r_1), (u_2, r_2), (u_3, r_3)\}$
   - $PA = \{(r_0, p_0), (r_2, p_2), (r_3, p_3)\}$

   Note que a expressão $r_0 \preceq r_1$ significa que o *role* r_1 é sénior do *role* r_0.

   Tendo em conta a documentação da biblioteca [3], e usando o editor *online* em `https://casbin.org/editor`, apresente: i) a política acima na linguagem do Casbin, ii) dois pedidos permitidos e iii) dois pedidos negados.

5. Descreva sucintamente os seguintes aspetos sobre a CVE-2020-8962 [4].

   5.1. Qual o tipo de vulnerabilidade;

   5.2. Que tipo de *software* é alvo do ataque;

   5.3. Como pode a vulnerabilidade ser explorada.

6. Considere a aplicação web *Google Gruyere* [5], a qual é propositadamente vulnerável a vários ataques.

   6.1. Inicie uma instância da aplicação [6] e indique o *id* no relatório da série.

   6.2. Realize o desafio de *Cross-site Request Forgery* (CSRF) [8] descrevendo como configurou a aplicação de ataque. Apresente também um esquema/diagrama com a solução proposta para resolver a vulnerabilidade na aplicação Gruyere.

   6.3. Considere que o atacante controla uma aplicação *web* que recebe pedidos HTTP GET no endereço `https://europe-west3-si-2020-2021-299801.cloudfunctions.net/si2021serie3`. Descreva como é que, explorando a vulnerabilidade de *Cross-site Scripting* (XSS) refletido [7], o atacante pode receber na aplicação controlada por ele os *cookies* de utilizadores da aplicação Gruyere.

   Para completar com sucesso esta alínea, o pedido à aplicação do atacante tem de incluir 3 parâmetros na *query string*:

   i) `group` com o formato `G<nn><t>`, em que `<nn>` é o número do grupo (ex: 01, 02, 03, ...), `<t>` é a turma (5XD para as turmas diurnas ou 51N);
   ii) `cookie` com o conjunto de *cookies* da vítima;
   iii) `gkey` com uma chave fornecida pelos docentes a cada grupo.

Exemplo dos parâmetros a indicar na *query string*: `group=G995XDcookie=xyzgkey=111`.
Pode consultar se o ataque teve sucesso através do endereço:
`https://europe-west3-si-2020-2021-299801.cloudfunctions.net/si2021serie3-result?group=X&gkey=Y`, procurando no resultado pelo *cookies* da vítima.

4 de janeiro de 2021

Referências

[1] Casbin - `https://casbin.org/`

[2] RBAC: Hierarchical Role Based Access Control - `https://www.npmjs.com/package/rbac`

[3] Casbin RBAC model - `https://casbin.org/docs/en/rbac`

[4] CVE-2020-8962 - `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8962`

[5] Google Gruyere - Web Application Exploits and Defenses - `https://google-gruyere.appspot.com`

[6] Google Gruyere - start new instance - `https://google-gruyere.appspot.com/start`

[7] Google Gruyere - Cross-site Scripting - `https://google-gruyere.appspot.com/part2#2__xss_challenge`

[8] Google Gruyere - Cross-site Request Forgery - `https://google-gruyere.appspot.com/part3#3__cross_site_request_forgery`