Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Licenciatura em Engenharia Informática, Redes e Telecomunicações

Segurança Informática

Terceira série de exercícios, Semestre de Inverno de 19/20

Data limite de entrega: 20 de dezembro de 2019

1. No contexto dos sistemas de controlo de acessos, distinga entre modelos e políticas. Dê um exemplo no âmbito de um sistema operativo.

2. Considere os modelos RBAC:

   2.1. No RBAC_1, 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)?

   2.2. Qual a relação entre o princípio de privilégios mínimos e o conceito de sessão?

3. Explique sucintamente de que forma a vulnerabilidade CVE-2019-9766 [1] pode levar a que um atacante consiga executar código arbitrário no computador da vítima.

4. O que têm em comum as vulnerabilidades de *buffer overflow* e *cross-site scripting* (XSS)?

5. Admita que a aplicação cliente que fez na segunda série tem uma vulnerabilidade de *cross site request forgery* no URL de *callback* da Google. De um exemplo de como essa vulnerabilidade pode ser explorada por um atacante.

6. Considere a aplicação web vulnerável Gruyere (`https://google-gruyere.appspot.com/`), alojada no serviço de *cloud* AppEngine da Google.

   6.1. Inicie uma instância da aplicação para utilização pelo grupo: `https://google-gruyere.appspot.com/part1#1__setup`. Inclua no relatório o identificador da aplicação na forma (*https://google-gruyere.appspot.com/*`<id>`*/*)

   6.2. Realize os primeiros três desafios da categoria *XSS Challenges*: *File Upload XSS*, *Reflected XSS* e *Stored XSS*. Em cada ataque tente injetar no *browser* código para apresentar uma caixa de alerta com os *cookies* da vítima. Os *cookies* que o *browser* mantém para o domínio a que pertence a página onde o *script* é executado podem ser obtidos em *javascript* com `document.cookie` [2].

   6.3. Considere que o atacante controla uma aplicação web que recebe pedidos HTTP GET no endereço `https://europe-west1-cn-ver1819.cloudfunctions.net/si1920serie3`. Descreva como é que através de um dos métodos da alínea anterior o atacante pode receber na aplicação controlada por si os *cookies* de utilizadores da aplicação Gruyere.

   Para completar com sucesso esta alínea, o pedido à aplicação do atacante tem de incluir três 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 (51D, 52D 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=G9951D&cookie=xyz&gkey=111`

   Pode consultar se o ataque teve sucesso através do endereço:
   `https://europe-west1-cn-ver1819.cloudfunctions.net/siserie3-result?group=X&gkey=Y`

7. Considere o laboratório do projeto SEED sobre *cross-site request forgery* (CSRF) [3]. Verifique que o sistema está corretamente configurado (ponto 2 do guião) acedendo aos URLs das aplicações alvo e atacante.

   7.1. Realize as alíneas 3.1 e 3.2. Apresente um sumário das ações realizadas e os *screenshots* relevantes.

   7.2. Aceda à aplicação vulnerável e à do atacante em máquinas virtuais diferentes [4], ou ligando-se à máquina virtual através de um computador na rede (ver modo *bridge* [5]). Apresente um *screenshot* que demonstre o sucesso do ataque.

Referências

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9766

[2] https://developer.mozilla.org/en-US/docs/Web/API/Document/cookie

[3] https://seedsecuritylabs.org/Labs_16.04/PDF/Web_CSRF_Elgg.pdf

[4] http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf

[5] https://www.virtualbox.org/manual/ch06.html#networkingmodes

ISEL, 2 de dezembro de 2019.