Aula TP - 09/Abr/2018

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 16/Abr/2018. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Exercícios

1. Vulnerabilidade de codificação

Experiência 1.1 - *Common Weakness Enumeration* (CWE)

A *Common Weakness Enumeration* (CWE) classifica classes de vulnerabilidade, atribuindo a cada classe de vulnerabilidades um identificador.

Aceda a https://cwe.mitre.org/ e veja quais as vulnerabilidades que são identificadas como:

- vulnerabilidades de projeto, introduzidas durante a fase de projeto do software (obtenção de requisitos e desenho) - https://cwe.mitre.org/data/definitions/701.html
- vulnerabilidades de codificação, introduzidas durante a programação do software - https://cwe.mitre.org/data/definitions/702.html
- vulnerabilidade operacional, causadas pelo ambiente no qual o software é executado ou pela sua configuração - https://cwe.mitre.org/data/definitions/16.html.

Veja ainda quais as vulnerabilidades identificadas como:

- *CWE/SANS Top 25 Most Dangerous Software Errors* (2011) - https://cwe.mitre.org/top25/
- *OWASP Top Ten* (2017) - https://cwe.mitre.org/data/definitions/1026.html

Experiência 1.2 - *Common Vulnerabilities and Exposures* (CVE)

A *Common Vulnerabilities and Exposures* (CVE) identifica vulnerabilidades (de projeto e codificação) existentes em software comercial ou aberto, com identificador com formato CVE-AAAA-NNNN, sendo AAAA o ano em que a vulnerabilidade foi catalogada e NNN o seu número.

Aceda a https://cve.mitre.org/ e verifique:

- o detalhe da vulnerabilidade mais recente;
- as vulnerabilidades identificadas no Google Chrome;
- as vulnerabilidades identificadas no Facebook.

Experiência 1.3 - *Common Vulnerability Scoring System* (CVSS)

O *Common Vulnerability Scoring System* (CVSS) disponibiliza um modelo quantitativo para definir as características e impacto das vulnerabilidades, garantindo uma medição precisa e repetível para gerar pontuações de impacto de vulnerabilidade.

Dois usos comuns do CVSS são a priorização das atividades de correção de vulnerabilidades e, o cálculo da gravidade das vulnerabilidades descobertas.

Explore o calculador de vulnerabilidades em https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

Experiência 1.4 - *National Vulnerability Database* (NVD)

A *National Vulnerability Database* (NVD) é o repositório de vulnerabilidades gerido pelo NIST. Baseia-se no CVE, mas inclui a gravidade da vulnerabilidade, de acordo com o CVSS (*Common Vulnerability Scoring System*)

Aceda a https://nvd.nist.gov/ e verifique:

- qual é a vulnerabilidade mais recente identificada?
- essa vulnerabilidade é a mesma vulnerabilidade mais recente encontrada na experiência 1.2 (CVE)? Qual poderá ser o motivo?
- as vulnerabilidades identificadas no Google Chrome;
- as vulnerabilidades identificadas no Facebook.

Pergunta P1.1

Em https://informationisbeautiful.net/visualizations/million-lines-of-code/ encontra (algumas são estimativas) o número de linha de código (*SLOC - Source Lines Of Code*) de alguns pacotes/plataformas de software.

1. Estime o número de bugs do Facebook, software de automóveis, Linux 3.1 e de todos os serviços Internet da Google.
2. Quantos desses bugs são vulnerabilidades?

Pergunta P1.2

Considere os três tipos de vulnerabilidades: de projeto, de codificação e operacional. Apresente para cada um deles dois exemplos e discuta a dificuldade de correção.

Pergunta P1.3

O que é que distingue uma vulnerabilidade diz-zero de outra vulnerabilidade de codificação que não seja de dia-zero?

Experiência 1.5 - *Exploit Database*

O *Exploit Database* contém um arquivo de *exploits* públicos, identificando o CVE da vulnerabilidade e/ou software que explora, para utilização por investigadores de vulnerabilidades e *penetration testers*.

Aceda a https://www.exploit-db.com/ e verifique:

- qual é o *exploit* mais recente identificado?
- o que é que o *exploit* relativo ao CVE-2016-6515 lhe permite fazer?

Experiência 1.6 - *Google Hacking Database*

O *Google Hacking Database* é um arquivo de Google *dorks* (*query* de pesquisa que retorna a informação sensível) que embora sendo uma forma de *exploits*, são também utilizados para criar novos *exploits*.

Aceda a https://www.exploit-db.com/google-hacking-database/ e verifique:

- qual é o *dork* mais recente identificado?

- explore alguns *dorks*.

Experiência 1.7 - *BugTraq*

A *BugTraq* é uma lista de correio eletrónico, com moderadores, na qual são discutidas vulnerabilidades recém-descobertas (entre outros assuntos relacionados com a segurança): o que são, como as explorar e, como as corrigir.

Aceda a https://www.securityfocus.com/ e explore algumas discussões.

Experiência 1.8 - Linguagem C

Tal como visto na aula teórica, a linguagem C é uma linguagem compilada em que cada instrução C é traduzida para instruções em linguagem máquina.

Utilizando a máquina virtual, compile um programa C com o `gcc` com a opção `-S`, de forma a produzir o código assembly correspondente ao código binário/executável (o código assembly fica no ficheiro com extensão .s). Verifique o ficheiro .s e compare-o com o ficheiro .c original.

Como exemplo utilize o seguinte código C:

```
#include <stdio.h>

void main()
{
  printf("Hello World\n");
}
```

Projeto de desenvolvimento de software

Os alunos deverão utilizar o resto desta aula TP para continuarem o projeto de desenvolvimento de software.

O projeto 1 (Leilões online) será efetuado, em conjunto, pelos grupos 1, 6, 10, 11, 12.

O projeto 2 (Gestor de passwords com base em QrCodes) será efetuado, em conjunto, pelos grupos 2, 3, 4, 5, 7, 8, 9.

- Projeto 1 – Leilões online
  - Leilões online, com entrega de propostas em "carta fechada";
  - Pode ser uma extensão para software open source de leilões online.
- Projeto 2 – Gestor de passwords com base em QrCodes
  - Gestor de passwords, em que com base em QrCode apresentado pelo site, o telemóvel lê o QrCode e envia o user + password para desbloquear o acesso;
  - Pode ser uma extensão para software open source de gestão de passwords.

Nesta primeira fase, os dois grupos de projeto devem definir em traços gerais o projeto e as suas funcionalidades, e pensarem de que modo serão utilizado as técnicas criptográficas no projeto.

Como output desta fase, deverão ter um primeiro draft de:

- definição do projeto e suas funcionalidades,
- etapas e fluxos de comunicação / mensagens, podendo utilizar como exemplo o formato visto no segundo exemplo do voto eletrónico, na aula teórica. Esta componente deve conter um diagrama e uma parte textual de explicação do diagrama,
- identificar os passos efetuados para a concepção e desenvolvimento do projeto, de forma a seguir os princípios de "*privacy by design*" e "*data minimization*" do RGPD (Regulamento Geral de Proteção de Dados);
- identificar de que modo o software garante os direitos do titular dos dados, de acordo com o RGPD.

Estes pontos deverão fazer parte do relatório final do projeto.