Questões de Segurança em Engenharia de Software 2018/19

1º Trabalho

Descrição geral

Neste trabalho pretende-se que analise e modifique uma aplicação web feita em Java e Java Server Pages, a Java Vulnerable Lab (JVL), disponibilizada na forma de um projecto Maven na página da disciplina.

Deve detectar e corrigir vulnerabilidades de segurança na JVL, fazendo uso da ferramenta SpotBugs para análise estática de código em conjunto com o "plugin" FindSecBugs, e ainda da ferramenta Zed Attack Proxy (ZAP) para testes de penetração.

O uso destas ferramentas deverá guiar a análise e modificação a operar no código da JVL. Para mais detalhes sobre o projecto de código e ferramentas a utilizar veja a página da disciplina. Os detalhes conceptuais de elaboração do trabalho são descritos na próxima página deste documento.

São sugeridas também algumas tarefas adicionais que pode levar a cabo para análise de vulnerabilidades da JVL.

Valorização

Peso de 4 valores na nota final.

Elaboração

O trabalho pode ser realizado individualmente ou em grupos de 2 alunos.

Entrega

Data: 5 / Novembro / 2018

Envie ao docente (`edrdo@dcc.fc.up.pt`) um email com os seguintes anexos:

- o seu relatório em formato PDF;
- o projecto Maven (modificado) num arquivo ZIP;

Análise e correcção de vulnerabilidades

Dada a grande quantidade de vulnerabilidades da JVL que poderão ser reportadas via SpotBugs e ZAP, o foco do trabalho será restrito a um conjunto restrito de vulnerabilidades e de funcionalidades da JVL. Em termos de classes de vulnerabilidade, deverá considerar apenas as questões relacionadas com:

- "SQL injection" (SQLi);
- "Cross-site scripting" (XSS);
- Uso inseguro de cookies.

Relativamente a funcionalidades da DVL, deverá considerar 4 grupos da JVL à sua escolha, tais como;

- `Login` – `login.jsp` e `LoginValidator.java` (em conjunto);
- `Register` – `Register.jsp` e `Register.java` (em conjunto);
- `Forum` – `vulnerability/forum.jsp` e `forumposts.jsp` (em conjunto);
- `My Profile` – `myprofile.jsp`;
- Uma das servlets accionadas na página de "My Profile" (visível depois do login).
- Aceda ao menu `Vulnerabilities` para explorar algumas outras possibilidades.

Para cada uma das funcionalidades que escolheu e classes de vulnerabilidade:

- Indique no relatório que vulnerabilidades detectou e de que forma; uma vulnerabilidade poderá ser detectada tanto pelo SpotBugs e/ou ZAP, mas às vezes apenas por uma das ferramentas.
- Explique também de que forma as vulnerabilidades em causa podem ser exploradas comprometendo a segurança da aplicação, por exemplo através da interacção pedido/resposta via ZAP.
- Ajuste a aplicação seguindo as orientações dadas pelas ferramentas, em particular os conselhos do SpotBugs para correcção de código. Recompile e volte a validar a aplicação novamente via SpotBugs e ZAP para verificar se a vulnerabilidade se mantém.
- Faça um sumário no relatório das mudanças operadas no código.

Notas:

- A análise SpotBugs emitirá vários avisos relativos a XSS que poderão ser ignorados, em particular o valor input `err` usado para funcionamento interno e outros dados relativos a dados básicos de sessão HTTP guardados no servidor (desde que não relevem informação sensível). Será relevante considerar apenas os avisos que dizem respeito a reflexão de dados de "forms" ou provenientes da bases de dados.
- Quando considerar necessário um passo de sanitisação no código, será útil empregar métodos da classe org.apache.commons.text.StringEscapeUtils para "escaping" de uma string em HTML ou outro formato. Após a incorporação de código de sanitisação a análise SpotBugs poderá continuar a assinalar a vulnerabilidade, dado a análise poder ser "cega" ao efeito da sanitisação (mas não o ZAP em princípio!).

Tarefas adicionais

Depois de fazer o trabalho base (descrito anteriormente) não há razões para ficar sossegado com a JVL. Afinal a aplicação é (bastante) vulnerável e assim continuará. Será que ...

- É possível conduzir um ataque CSRF a alguma funcionalidade da JVL?
- De entre as funcionalidades que analisou ou outras, se conseguem vislumbrar vulnerabilidades não reportados pelo SpotBugs ou ZAP?
- A configuração do SpotBugs está preparada para apenas reportar vulnerabilidades de SQLi, XSS, ou uso de cookies. No entanto se comentar/remover a secção `<Match>` do ficheiro `config/spotbugs/exclude.xml` verá que o Spotbugs passa a reportar (muitos) outros avisos de segurança. Alguns dos avisos (considere um apenas) chama a sua atenção para uma potencial vulnerabilidade?

Para um ou mais dos itens acima, no relatório explique e exemplifique como um ataque pode ser conduzido e possivelmente como poderia ser prevenido/mitigado.