28 de Outubro de 2015



**Shuttle Reservation System with User Reputation**

Segurança Informática em Redes e Sistemas

Grupo 4 – Alameda

|  |  |
| --- | --- |
| 75522 | Daniel Sil |
| 75714 | Miguel Pasadinhas |
| 76012 | Carlos Carvalho |

# Motivação

Com este projeto pretendemos potenciar os nossos conhecimentos acerca da segurança de sistemas informáticos. Para tal iremos desenvolver um sistema de reservas num shuttle. Este sistema permitirá dar prioridade a utilizadores com um maior karma (reputação associada a uma pessoa). Neste sistema a segurança é um aspeto de grande relevância pois é necessário que a integridade do sistema seja mantida. Em caso oposto o sistema de reputação poderá ser abusado por utilizadores com intenções maliciosas. Neste relatório, continuaremos a explorar os possíveis ataques a este sistema e formas de nos defendermos dos mesmos.

# Objetivos

No final deste projeto tencionamos ter desenvolvido um sistema seguro tendo em conta os recursos disponíveis. De seguida apresentamos uma lista de objetivos (ordenados do mais simples para o mais desafiante):

* Garantir que o sistema permite a reserva de lugares num shuttle, baseada na reputação do utilizador;
* Garantir a confidencialidade e integridade das comunicações com a web application;
* Impedir ataques à aplicação web, como XSS, CSRF e Code Injection;
* Garantir que o sistema dá reputação aos utilizadores de forma justa e balanceada;
* Garantir a confidencialidade e integridade dos dados críticos na base de dados;
* Garantir que cada pessoa apenas consegue ter uma conta;
* Impedir ataques de *Brute Force* ao sistema de autenticação;
* Garantir que o sistema de reputação não pode ser abusado através de ações legitimas;
* Minimizar o impacto de ataques feitos a partir do interior;
* Impedir o acesso aos servidores por pessoas não autorizadas;
* Minimizar o impacto de ataques de *Denial of Service*.

# Solução Proposta



A aplicação a desenvolver será uma web application. A mesma será executada num único servidor centralizado. Existirão duas vistas da aplicação – uma para os utilizadores que pretendem reservar um lugar no shuttle e outra para o registo das presenças no shuttle. Para tentar assegurar uma maior segurança do servidor aplicacional, este estará protegido por uma firewall em software. A base de dados rá apenas acessível a partir do servidor. Os utilizadores terão uma conta única no sistema, sendo isso garantido pelo uso de um documento oficial de identificação (Cartão de Cidadão, Passaporte, etc). Serão então necessários leitores de Cartão de Cidadão e, eventualmente, de outros documentos semelhantes. Para assegurar confidencialidade e integridade da comunicação na internet, será usado o protocolo HTTPS. A firewall permitirá resistir a alguns ataques de DoS e Brute Force vindos do mesmo IP e tentar impedir o acesso indevido ao servidor. Para minimizar o impacto de ataques feitos a partir do interior, será mantido um log das ações realizadas pelos Bus Drivers (utilizadores com privilégios elevados). O servidor aplicacional terá um mecanismo de atribuição de karma aos utilizadores, permitindo que utilizadores com um maior karma tenham vantagens (precedência) na reserva de lugares. Para assegurar a autenticidade das máquinas presentes nos autocarros, cada uma terá uma chave secreta. A chave será adicionada manualmente no servidor aplicacional. Para além disso o servidor aplicacional terá as suas próprias chaves para encriptação da informação da base de dados.

# Plano de Trabalho

|  |  |  |  |
| --- | --- | --- | --- |
| Semana | Daniel Sil | Miguel Pasadinhas | Carlos Carvalho |
| 2-Nov – 8-Nov | Desenho | Desenho | Desenho |
| 9-Nov – 15-Nov | Implementação da funcionalidade do sistema | Implementação da funcionalidade do sistema | Implementação da funcionalidade do sistema |
| 16-Nov – 22-Nov | Configuração dos mecanismos de protecção contra XSS, CSRF, Code Injection e outros | Garantir a integridade e confidencialidade dos dados críticos na base de dados | Implementação do sistema de logs de ações |
| 23-Nov – 29-Nov | Implementar sistema de prevenção de ataques Brute Force ao sistema de autenticação | Configuração da Firewall | Configuração do HTTPS |
| 30-Nov – 4-Dec | Testes de penetração | Testes de penetração | Testes de penetração |

# Referencia de Ferramentas

Serão usadas as seguintes ferramentas:

* Laravel – esta Framework MVC escrita em PHP oferece mecanismos elegantes de tratar a persistência, bem como ferramentas de MVC tradicionais. Para além disso oferece suporte para minimizar as vulnerabilidades relacionadas com XSS, CSRF e Code Injection. Esta Framework tem também implementações de vários algoritmos de encriptação;
* fail2ban – esta ferramenta lê os logs do sistema (e.g. logs do web server ou logs de acesso ssh) e permite banir IPs com comportamento suspeito;
* nginx – web server para correr a aplicação;