BugFeed – Uma Plataforma de Recompensa por Bugs

Tauan B. M. Matos1, Victor S. E. Brito1, Felipe G. Torres1

1Escola de Arquitetura, Engenharia e Tecnologia da Informação – Universidade Salvador (UNIFACS) – Salvador, BA, Brazil

144151034@unifacs.edu.br, 029151068@unifacs.edu.br, felipe.torres@unifacs.br

**Abstract.** This work describes a democratic platform that will function as a bridge between users and companies, where users are expert information security professionals. Users can report security breaches found in the products and services offered by these companies and be rewarded by them according to the severity of the reported flaw.

**Resumo.** Este trabalho descreve uma plataforma democrática que servirá como uma ponte entre usuários e empresas, onde usuários são especialistas em segurança da informação. Os usuários podem reportar falhas de segurança encontrados nos produtos e serviços oferecidos por essas empresas e serem recompensados pelas mesmas de acordo com a gravidade da falha reportada.

1. Introdução

De acordo com o Internet World Stats, site que coleta e classifica dados sobre o uso da internet mundial, mais da metade da população já está conectada à internet. A Statista, portal de estatísticas online, estima que a quantidade de downloads de aplicativos mobile ultrapasse 350 bilhões em 2021: um aumento de mais de 100% em relação aos números em 2016, que totalizavam cerca de 150 bilhões de downloads. Esta mesma estatística já possuía um número 200 bilhões de downloads no fim de 2017.

Porém, independentemente do quão bom o teste de software é, ou quão minuciosos os desenvolvedores são para não deixar o software vulnerável, não se pode garantir que nenhum desses produtos estão totalmente seguros.

Segundo seus sites oficiais, empresas como Facebook, Google, Samsung e Microsoft oferecem pagamentos diretos em troca de relatórios de alguns tipos de vulnerabilidades e técnicas de exploração, com o intuito de aperfeiçoar a segurança de seus produtos e proteger seus clientes. Essas empresas de grande escala têm condições de organizar e financiar um programa de recompensas, recrutar os pesquisadores de segurança e ainda consertar as falhas encontradas. Porém, uma empresa de pequeno-médio porte não costuma ter a infraestrutura necessária para ter um programa de recompensas em execução. A solução para esse problema seria usar um serviço que lidaria com todas as nuances de recrutamento de pessoal, filtragem de *bugs* reportados e análise dos *bugs*.

Com o propósito de minimizar o risco de ataques com más intenções, está sendo sugerido neste projeto uma plataforma de *bug bounty* (“caça aos bugs”). Uma plataforma de “recompensas por bugs” é um lugar centralizado, onde as empresas podem publicar seus programas de *bug bounty*. A comunidade, ao achar falhas nos produtos e serviços, poderá reportar esses problemas e ser recompensada de acordo com a gravidade das vulnerabilidades encontradas.

1. Justificativa

Existem inúmeros benefícios para esses programas, tais como a identificação e a correção de mais vulnerabilidades e uma infraestrutura mais segura. Segundo o Centro de Recursos de Roubo de Identidade (ITRC), dos Estados Unidos, houveram 1.339 vazamentos de dados apenas em 2017, expondo quase 200 milhões de registros de origens médicas, bancárias, empresariais, educacionais e governamentais. De acordo com a Akamai, uma plataforma que monitora e analisa dados da internet em tempo real, quase 50 milhões de ataques a sites e serviços online são realizados por dia, pondo em risco a disponibilidade e a confiabilidade que o usuário tem ao utilizar um serviço.

Os programas de *bug bounty* oferecem uma alternativa de custo-benefício melhor do que os mais comuns testes de penetração, que são realizados por especialistas de segurança cujo tempo é caro e limitado. Não só isso, como também requer uma preparação exigente, considerando que estes normalmente são executados em um ambiente de teste que requer várias configurações formais e técnicas, em vez de em um ambiente de produção.

Numa plataforma de recompensas de *bugs*, o produto é testado por vários hackers com pensamentos e técnicas diferentes que até competem entre si para encontrar os erros, já que o primeiro a descobrir a falha é quem ganha a recompensa. Todo esse sistema ajuda as empresas a entregarem um produto e/ou serviço mais seguro com gastos menores em segurança, já que as recompensas são pagas apenas quando os hackers realmente acham uma falha de segurança relevante.

1. Metodologia

A plataforma será construída utilizando um modelo de projeto chamado Cascata. Primeiro, será feito um estudo sobre a viabilidade da realização do projeto. Em seguida, será realizada uma análise sobre todos os requisitos que o projeto irá abordar e as tecnologias que serão usadas. Após a etapa de análise, será iniciada a etapa de codificação do projeto baseada nos requisitos e especificações que foram abordados na etapa anterior. Por fim, será executada a etapa de testes, para garantir que o projeto desenvolvido não passe para a etapa de implantação com problemas.

O projeto será desenvolvido para a web utilizando tecnologias responsivas, para que seja possível utilizá-lo através de qualquer dispositivo móvel. Para o desenvolvimento do projeto, será utilizado o .NET Framework da Microsoft voltado para aplicações web. As interfaces do projeto serão desenvolvidas utilizando a tecnologia ASP.NET, uma solução de alto desempenho. A aparência das interfaces será construída utilizando o framework Bootstrap na versão 4.0.0. A persistência dos dados será realizada no SQL Server 2017 em conjunto com o Entity Framework 6. Todo o sistema será desenvolvido utilizando o Microsoft Visual Studio Community 2017, que possui compatibilidade com todas as tecnologias que foram escolhidas para o desenvolvimento do sistema.

1. Resultados

Esta aplicação visa se tornar uma ponte entre profissionais da área de segurança da informação e empresas que oferecem produtos e serviços online. Nessa plataforma, as empresas podem publicar programas de recompensas por falhas, onde os usuários irão testar seus produtos e reportar qualquer falha encontrada. Após uma análise dessa falha e histórico do profissional que a reportou, a empresa irá recompensar o profissional de acordo com a severidade da falha.

A empresa poderá criar programas de recompensas com diferentes direcionamentos. Programas públicos permitem que todos os usuários da plataforma possam testar e reportar falhas. Os programas privados funcionam selecionando apenas um grupo customizado de testadores. Os pesquisadores podem ser selecionados de acordo com sua reputação na plataforma que, por exemplo, depende da quantidade de bugs encontrados, severidade e validação dos mesmos.

A plataforma irá reter uma pequena porcentagem da recompensa como um custo de uso pelo profissional. Além de criar um programa para os produtos já publicados, a empresa poderá criar programas para produtos que ainda vão ser lançados, garantindo que, ainda antes que este chegue ao usuário final, o produto tenha um nível maior de segurança.

* 1. Requisitos Funcionais

Esta seção descreve as funcionalidades presentes no software que será produzido. Os requisitos funcionais descritos abaixo possuem código para auxiliar a sua rastreabilidade. Este código está descrito no título de cada requisito entre colchetes.

Tabela 4.1: Lista de requisitos funcionais e não-funcionais

|  |  |
| --- | --- |
| **Código** | **Descrição** |
| RF001 | Cadastrar Empresas |
| RF002 | Gerenciar Grupos de Usuários |
| RF003 | Gerenciar Funcionários |
| RF004 | Gerenciar Programas de Recompensas |
| RF005 | Cadastrar Usuários |
| RF006 | Enviar Relatórios |
| RF007 | Analisar Relatórios |
| RF008 | Enviar Pagamentos |
| RF009 | Receber Pagamentos |
| RNF001 | Interface do software |
| RNF002 | Linguagem de desenvolvimento do software |
| RNF003 | Sistema de Gerenciamento de Banco de Dados |

* + 1. [RF001] Cadastrar Empresas

O software deve permitir o cadastro gratuito de empresas que estejam interessadas em abrir programas de recompensas por bugs encontrados em suas aplicações.

* + 1. [RF002] Gerenciar Grupos de Usuários

O software deve permitir que a empresa crie, edite e remova grupos de usuários para definir acessos e permissões aos seus funcionários.

Os tipos de permissões básicos são os seguintes:

* Admin: permite gerenciar funcionários, informações de pagamento e definir permissões;
* Rewards: permite dar recompensas aos pesquisadores e postar comentários nos relatórios enviados;
* Report: permite postar comentários, editar título, tipo de vulnerabilidade e estado dos relatórios (enviado, em análise, concluído);
* Program: permite gerenciar programas de recompensas e convidar pesquisadores de segurança.
  + 1. [RF003] Gerenciar Funcionários

O software deve permitir o cadastro, edição e desligamento de funcionários dentro do nas empresas, gerenciando suas permissões e ações em nome da empresa de acordo com os grupos de usuários descritos em [RF002].

* + 1. [RF004] Gerenciar Programas de Recompensas

O software deve permitir o cadastro, edição e exclusão de programas de recompensas públicos e privados. Os programas públicos poderão ser vistos por todos os usuários cadastrados na plataforma. Nos programas privados, a empresa deverá convidar manualmente os usuários que faram parte do mesmo.

Programas que já foram iniciados não poderão ser excluídos, mas poderão ser desligados.

* + 1. [RF005] Cadastrar Usuários

O software deve permitir o cadastro de pesquisadores de segurança, que serão responsáveis por procurar bugs nos programas de recompensas.

* + 1. [RF006] Enviar Relatórios

O software deve permitir que os usuários enviem relatórios para bugs encontrados nos programas de recompensa ativos. Os relatórios incluem título, descrição, tipo de vulnerabilidade, severidade, impacto e outros detalhes.

* + 1. [RF007] Analisar Relatórios

O software deve permitir que os funcionários da empresa com permissão de *Report* (como descrito em [RF002]) possam analisar, responder e aprovar os relatórios enviados pelos usuários. O valor do pagamento é definido na análise do relatório.

* + 1. [RF008] Enviar Pagamentos

O software deve permitir que os funcionários da empresa com permissão de *Rewards* (como descrito em [RF002]) possam efetivamente enviar pagamentos para os usuários. 10% do valor enviado irá para a BugFeed. O pagamento será processado através da Stripe API.

* + 1. [RF009] Receber Pagamentos

O software deve permitir que os usuários recebam gratuitamente os pagamentos das empresas em conta bancária brasileira, através de Transferência Eletrônica Disponível (TED). A transferência é gratuita e possui valor mínimo de R$ 100,00.

* 1. Requisitos Não-Funcionais

Esta seção descreve as restrições e exigências do software. Os requisitos não-funcionais descritos abaixo possuem código para auxiliar a sua rastreabilidade. Este código está descrito no título de cada requisito entre colchetes.

* + 1. [RNF001] Interface do software

O software deverá ser desenvolvido com interface web, com o intuito de facilitar a compatibilidade com a maior quantidade de dispositivos possível.

* + 1. [RNF002] Linguagem de desenvolvimento do software

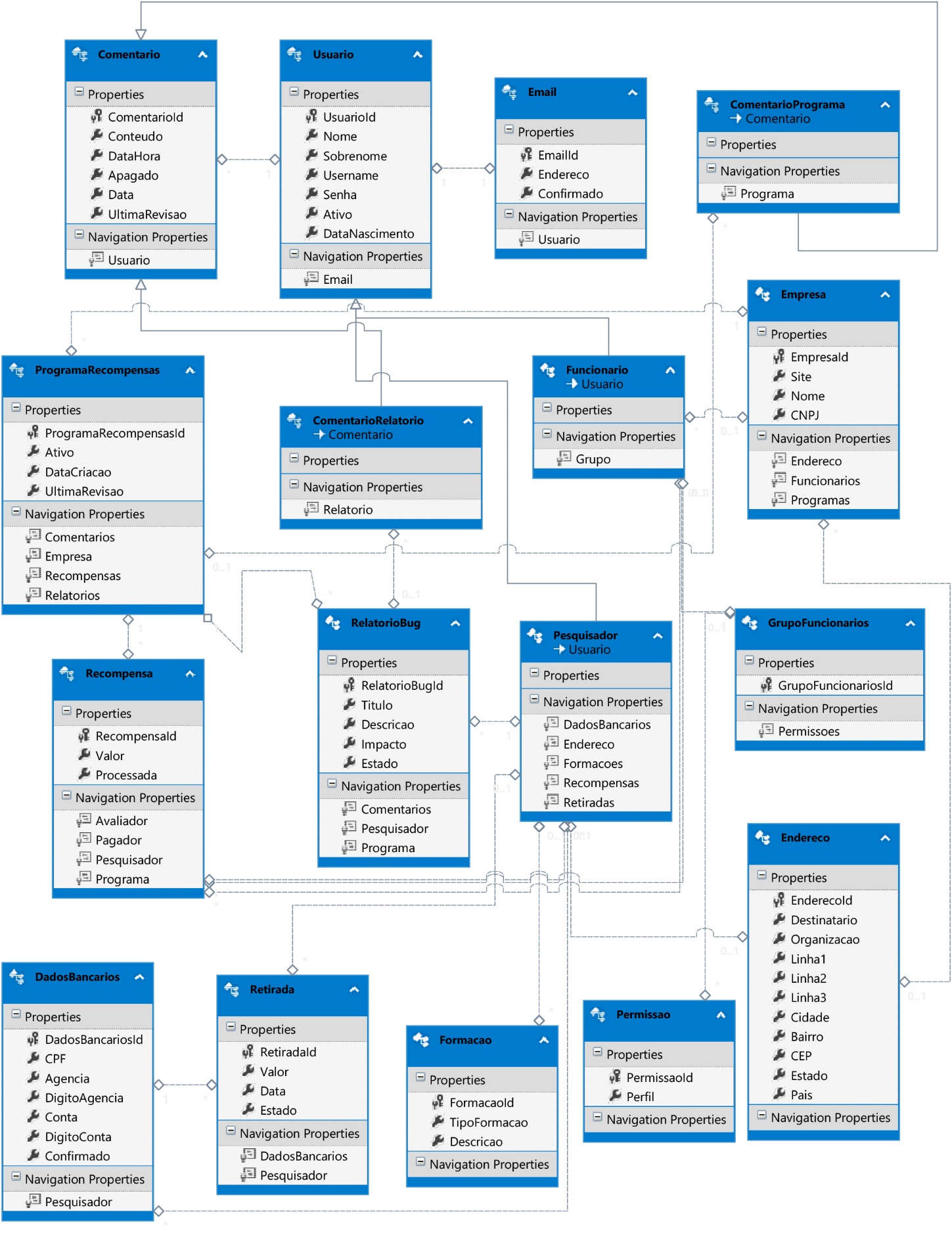
O software deverá ser desenvolvido utilizando ferramentas Microsoft; a linguagem de programação será C# e ASP.NET será o framework utilizado para a aplicação web.

* + 1. [RNF003] Sistema de Gerenciamento de Banco de Dados

O SQL Server 2017 Express foi o SGBD escolhido por possuir grande suporte e integração mais completa com o conjunto de ferramentas de desenvolvimento da Microsoft.

* 1. Diagrama de Entidades e Relacionamento

O diagrama demostra as entidades e os relacionamentos das mesmas que estão presentes na modelagem do banco de dados utilizado para armazenamento. A Figura 4.1 descreve visualmente o diagrame de entidades e relacionamentos, e tem como objetivo o mapeamento dos relacionamentos entre entidades e das próprias entidades. Este modelo de banco de dados foi desenvolvido para atender os requisitos funcionais e não funcionais do sistema deste trabalho, possuindo 13 entidades e 20 relacionamentos.

Figura 4.1: Essa imagem representa o diagrama de entidades e relacionamentos do banco de dados.

1. Referências

KEMP, S.; Digital in 2018: World’s internet users pass the 4 billion mark. 2018. Disponível em: <<https://wearesocial.com/blog/2018/01/global-digital-report-2018>>. Acesso em: 20 abr. 2018.

AKAMAI. The Akamai Intelligent Plataform. Disponível em: <<https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/>>. Acesso em : 28 abr. 2018.

RICHARDS, Dr Reshan; VALENTINE, Stephen J. Blending Leadership: Six Simple Beliefs for Leading Online and Off. 1. ed. [S.l.: s.n.], 2016. 224 p. Disponível em: <<https://books.google.com.br/books?id=HfxUDAAAQBAJ>>. Acesso em: 28 abr. 2018.

Miniwatts Marketing Group. Internet World Stats: The Internet Big Picture. Disponível em: <<https://www.internetworldstats.com/stats.htm>>. Acesso em: 28 abr. 2018.

Statista. Number of mobile app downloads worldwide in 2016, 2017 and 2021 (in billions). Disponível em: < <https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/>>. Acesso em: 28 abr. 2018.

Identity Theft Resource Center. ITRC Data Breach Report. 2017. Disponível em: <<https://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf>>. Acesso em: 28 abr. 2018.

Google. Google Vulnerability Reward Program (VRP) Rules. Disponível em: <<https://www.google.com/about/appsecurity/reward-program/>>. Acesso em: 28 abr. 2018.

Facebook. Bug Bounty Program. Disponível em: <<https://www.facebook.com/whitehat>>. Acesso em: 28 abr. 2018.

Samsung. Rewards Program. Disponível em: < <https://security.samsungmobile.com/rewardsProgram.smsb>>. Acesso em: 15 mar. 2018.

Microsoft. Programas de Recompensa da Microsoft. Disponível em: <<https://technet.microsoft.com/pt-br/library/dn425036.aspx>>. Acesso em: 28 mar. 2018.