PROJETO - LabSecurity

Rui Paredes

RELATÓRIO PARA A OBTENÇÃO DO GRAU DE LICENCIADO

EM ENGENHARIA INFORMÁTICA

Jul/2018

## Elementos Identificativos

**Nome:** Rui Miguel Andrês Paredes

Número: 1011670

**Curso:** Licenciatura em Engenharia Informática

Ano Letivo: 2017/2018

**Escola:** Escola Superior de Tecnologia e Gestão – Instituto Politécnico da Guarda

**Orientador:** Professor José Carlos Coelho Martins Fonseca

Projeto realizado entre: maio e julho de 2018

## Agradecimentos

## Resumo

## Abstract

## Índice

## Siglário

# Introdução

Todos os dias novos programadores entram no mercado de trabalho muitas vezes com pouca informação acerca das várias vulnerabilidades existentes e que podem por em risco o conteúdo que os mesmos desenvolvem. Porém, este problema não afeta apenas os programadores, mas também a comunidade em geral que muitas vezes não tem informações suficientes acerca de ciber-segurança e que são vitimas destes ataques por falta de informação.

Por estas razões surgiu a ideia de desenvolver um laboratório de programação e segurança, onde se poderá aprender mais acerca de vulnerabilidades, ataques e defesas ao nível da segurança informática.

Este laboratório de programação e segurança para lá de disponibilizar informações acerca de várias vulnerabilidades, ciber-ataques existentes e como defender dos mesmos, permite ainda realizar quizzes e competições de hacking contra outros utilizadores.

De forma a implementar as funcionalidades anteriores foram realizadas várias análises, numa fase inicial do projeto, de forma a definir os requisitos funcionais da plataforma, sendo estes os seguintes:

* Registar utilizadores
* Registar vulnerabilidades/ataques
* Adicionar competições
* Registar utilizadores nas competições
* Adicionar desafios de forma modular
* Adicionar desafios a competições
* Adicionar perguntas/respostas a quizzes.
* Plataforma online

-FASES DO TRABALHO

-ESTRUTURA DO DOCUMENTO

# Estado da Arte

Após definidos os objetivos propostos para o desenvolvimento do projeto, foi realizada uma pesquisa de forma a saber quais as soluções atualmente existentes.

Desta pesquisa foram encontradas várias aplicações em que alguns dos objetivos são idênticos aos definidos inicialmente para este projeto, e de onde foram retiradas informações acerca do seu funcionamento que poderão servir de apoio para o desenvolvimento da plataforma web do LabSecurity.

Estas aplicações, embora com alguns objetivos idênticos aos propostos, não chegam a completar todos os objetivos propostos ou divergem um pouco dos mesmos. Algumas das aplicações focam -se em jogos CTF entre equipas ou indivíduos, ou apenas no ataque a cada vulnerabilidade sem competição direta com outros jogadores, ou então apenas na divulgação de eventos da área da cibersegurança onde são realizados estes tipos de jogos.

## Aplicações existentes

Das várias aplicações encontradas na fase de pesquisa foram selecionadas para análise aquelas que demonstraram ter um maior reconhecimento na comunidade, sendo estas a Hacking Lab, CTF365, Reversing.kr, RingZer0Team e WebGoat.

Na Tabela 1 são apresentados os objetivos definidos inicialmente para a plataforma web do LabSecurity e se cada aplicação possuí essas características ou não.

Tabela 1- Aplicações existentes e objetivos propostos

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Aplicação** | **Plataforma Online** | **Ranking** | **Uso de Flags** | **Auto- Correção** | **Ataques na Plataforma Web** | **Propostas de Ataques** | **Vulnerabilidades - Lessons** | **Quizzes** |
| Hacking-Lab | Sim | Sim | Não | Não | Não | Não | Não | Não |
| CTF365 | Sim | Sim | Não | Não | Sim | Não | Não | Não |
| Reversing.kr | Sim | Sim | Sim | Sim | Não | Não | Não | Não |
| RingZeroTeam | Sim | Sim | Sim | Sim | Sim | Não | Não | Não |
| WebGoat | Não | Sim | Sim | Sim | Sim | Não | Sim | Não |

### Hacking Lab

O Hacking Lab é um serviço da organização Security Competence, uma subsidiária da Compass Security.

A Compass Security é especialista em testes de bruteforce, resposta a incidentes, análise forense digital e treinos de segurança. É uma organização com algum reconhecimento, tendo já sido convidada para conferências como a Black Hat Las Vegas e a conferência Blue Hat da Microsoft.

O Hacking-Lab consiste num website de hacking ético, rede computacional e plataforma de desafios de segurança, que tem como objetivos encontrar e educar indivíduos com talento na área da cibersegurança e divulgar conhecimento desta mesma área através das várias competições que vão desde criptografia, a engenharia-reversa, hacking ético, entre outras (Figura 1).

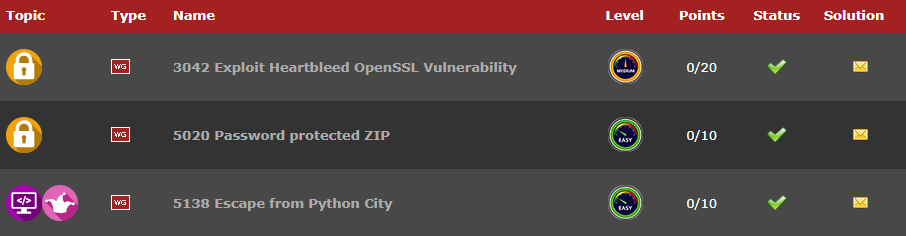
Ao nível dos desafios, o Hacking-Lab apresenta uma variedade de desafios. Algumas destas competições requerem que o utilizador use software adicional para resolver determinados desafios.

O Hacking-Lab dispõe ainda de uma secção de divulgação de conferências de cibersegurança.

De forma a ser possível aos utilizadores resolver os desafios é necessário que estes instalem uma máquina virtual com um sistema fornecido pela plataforma e se conectem através de VPN a esta.

Após resolvido um desafio e submetido, a solução apresentada pelo utilizador é enviada para ser analisada por uma equipa, e caso esta se encontre correta, o mesmo obtém pontos, sendo estes adicionados ao Ranking.

Figura 1- Desafios Hacking- Lab

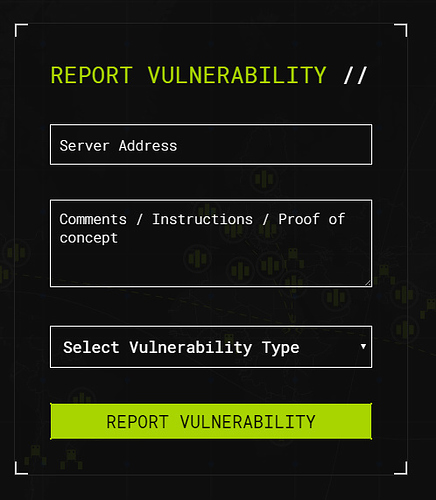


### CTF365

O CTF365 consiste num website com jogos CTF (Capture the Flag), em que são simulados ataques a vulnerabilidades aos serviços que cada equipa possui, e em que o objetivo principal é as equipas tornarem os seus serviços o mais invulneráveis possíveis enquanto atacam os serviços de equipas inimigas. Os serviços de cada equipa encontram -se nos vários “Fortresses” que estas possuem, sendo que um Fortress corresponde a uma máquina virtual criada para a equipa. Na realização de ataques a Fortresses de outras equipas, os jogadores podem usar uma grande variedade de ferramentas, não havendo uma grande quantidade de regras que os jogadores devem respeitar nos seus ataques. A criação de Fortresses é exclusiva a equipas que façam parte de um plano que requer pagamento, porém, qualquer jogador que esteja registado na plataforma, com ou sem equipa ou plano, consegue realizar ataques.

De forma às equipas submeterem as vulnerabilidades encontradas durante os ataques e ganharem pontos é necessário que indicar qual o tipo de vulnerabilidade, a quem pertence o fortress inimigo, e qual o endereço do mesmo, e após esta ser submetida é analisada por uma equipa do CTF365 que verificará se a vulnerabilidade realmente existe ou não no fortress indicado.

Figura 2- CTF365 Submeter Vulnerabilidade



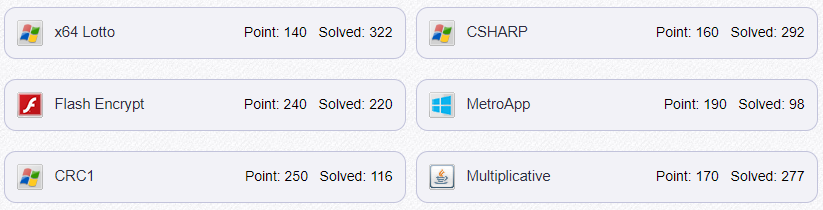
### Reversing.kr

O Reversing.kr é uma plataforma desenvolvida para pôr à prova a capacidade de cracking e de conhecimento de engenharia reversa dos seus utilizadores.

Os desafios que esta plataforma possuí consistem em aplicações para diferentes ambientes (Windows, Linux, Windows Phone, …), Figura 3, em que o ataque é executado nesses mesmos ambientes e após atingir a solução correta, de forma a ganhar pontos na plataforma, a solução encontrada necessita ser inserida numa secção própria na plataforma do Reversing.kr. Após obtenção dos pontos, estes passam a ser visíveis na tabela de Rank da plataforma.

Possuí ainda uma secção onde se encontram plataformas semelhantes a esta.

Figura 3- Reversing.kr - Challenges

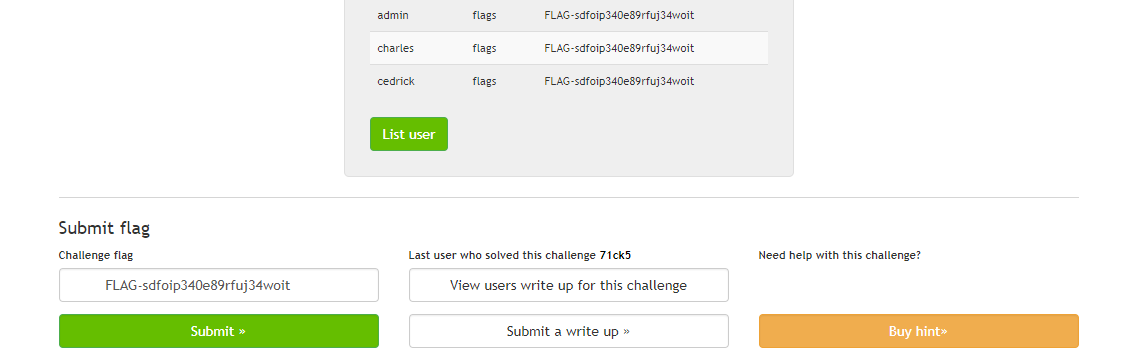


### RingZer0 Team Online CTF

O RingZer0 Team Online CTF consiste numa plataforma onde se encontram disponíveis uma grande variedade de desafios de forma a meter à prova os conhecimentos e capacidades de hacking dos utilizadores através de jogos Capture the Flag.

Estes desafios vão desde desafios de criptografia, análise de malwares, SQL injection, entre outros, onde alguns deles podem ser resolvidos diretamente na plataforma, enquanto que outros a resolução é feita no sistema do utilizador, por exemplo, uma aplicação com vulnerabilidade, ou então através de SSH para uma máquina onde a vulnerabilidade estará presente. Independentemente do tipo de vulnerabilidade, após realizado o ataque com sucesso, é devolvida uma flag que pode ser usada seguidamente na página onde o desafio realizado se encontra, obtendo pontos de acordo com o desafio realizado. A plataforma disponibiliza ainda algumas ferramentas que poderão ser usadas de forma a resolver certos desafios. Possuí ainda um Scoreboard onde são apresentados os 50 utilizadores com mais pontos na plataforma.

Figura 4- RingZer0Team - Desafio SQLi após ataque

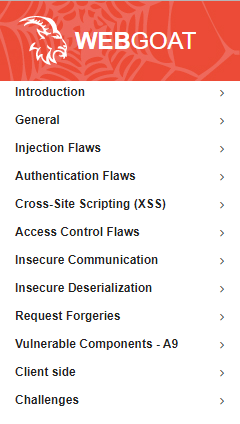


### WebGoat

A WebGoat consiste numa aplicação onde se pode encontrar uma variedade de vulnerabilidades comuns em aplicações desenvolvidas em Java e componentes open source. Esta plataforma, para lá de ter vários desafios sobre diversas vulnerabilidades, que vão desde falhas que podem ser exploradas através de injeção de comandos maliciosos, ataques de SQLi por exemplo, a ataques de CSRF entre outros, tem ainda lições teóricas acerca dos vários ataques que podem ser testados na plataforma. Todos os desafios presentes na WebGoat não necessitam de ferramentas adicionais para a sua resolução, e encontram -se divididas em dois tipos, desafios para testes das vulnerabilidades, nos quais durante a resolução dos mesmos se podem obter dicas de como realizar os ataques sendo que a sua resolução não atribui pontos ao utilizador, e desafios competitivos, nos quais não há qualquer tipo de dicas para chegar à resposta e de onde tem de resultar uma Flag para poder ser usada para obter os pontos pela resolução de determinado desafio.

O servidor para a plataforma WebGoat corre como servidor local, pelo qual se encontra disponível para download na internet.

Figura 5- WebGoat - Menu Principal



## Análise crítica das soluções existentes

Todas as aplicações apresentadas reúnem um conjunto de características que vão ao encontro dos objetivos do LabSecurity.

O Hacking-Lab, tem pontos fortes que devem ser referidos, como uma grande variedade de desafios a explorar e que analisam uma larga área de tipos de vulnerabilidades, que vão desde desafios fáceis a difíceis. Para lá disso, a plataforma online é de fácil uso e possui as informações necessárias à realização de cada desafio. A plataforma apresenta ainda uma secção onde são divulgados eventos de cibersegurança, que apesar de não ir ao encontro dos objetivos especificados para o LabSecurity, não deixa de ser um ponto forte já que esses eventos são uma forma de divulgar informação na área da cibersegurança.

Como pontos fracos o Hacking-Lab apresenta características como a necessidade de ter de instaladar a máquina virtual disponibilizada pela plataforma do Hacking-Lab e o acesso através de VPN à plataforma de forma a ter acesso a grande parte dos desafios. Para lá disso existem ainda características como o uso de ferramentas adicionais e a forma como a solução encontrada para cada desafio é avaliada.

Ao nível do CTF365, esta plataforma tem como principais pontos fortes a ótima apresentação da plataforma, e variedade de vulnerabilidades que podem ser exploradas devido aos ataques serem executados em sandboxes. Tem ainda características positivas como a liberdade na criação dos fortresses de cada equipa e da defesa dos mesmos, bem como a situação de ataque a fortresses de outras equipas. Como pontos fracos apresentam -se características como a falta de informação acerca das várias vulnerabilidades a serem exploradas, a dificuldade que a plataforma apresenta a utilizadores com pouco conhecimento na área da programação e segurança e o método de verificação da vulnerabilidade que exige verificação por parte da gestão da plataforma.

Ao analisar a plataforma Reversing.kr verificou -se características positivas como a variedade de desafios disponíveis, o método de obtenção automática de uma flag após chegar a uma solução correta, e o uso das flags para confirmação que a resposta encontrada está correta e obtenção de pontos. Como características negativas verificou -se que apesar de haver uma boa variedade de desafios disponíveis, todos eles estão relacionados com vulnerabilidades de aplicações, sendo que estas estão ainda limitadas a diversos tipos de sistemas operativos e linguagens de programação o que faz com que seja necessário executar essas aplicações nos sistemas correspondentes. Existe ainda a falta de informação acerca dos vários desafios disponíveis.

O RingZer0 Team Online CTF é uma plataforma que apresenta alguns aspetos positivos como uma vasta variedade de desafios disponíveis, o uso de flags para validação e obtenção de pontos por desafio realizado com sucesso, a disponibilização de ferramentas adicionais que podem ser usadas na resolução de certos desafios e a facilidade de uso da plataforma. Como aspetos negativos verificou -se a falta de informação acerca dos desafios disponíveis e vulnerabilidades a explorar nos mesmos e a necessidade de usar SSH para certas máquinas de forma a poderem ser realizados determinados desafios.

O WebGoat apesar de funcionar como um servidor local, apresenta uma plataforma bastante completa que apresenta características positivas como a variedade de ataques disponíveis, constituídos por informação acerca dos mesmos e desafios de treino e algumas competições. Como ponto positivo existe ainda o uso de flags para a validação e obtenção de pontos para o ranking.

Esta plataforma apresenta ainda como pontos negativos a característica de esta não ser uma plataforma online e de ter muitas poucas competições disponíveis.

No geral, todas as plataformas analisadas têm alguns pontos que a plataforma web a desenvolver tem como objetivos, no entanto nenhuma delas tem um sistema de Quizzes ou de Propostas de ataques feitas pelos utilizadores e sendo que a única que apresenta informação teórica acerca das várias vulnerabilidades a serem exploradas é a plataforma WebGoat que apresenta ser a mais completa de todas as exploradas. Apesar da variedade entre as várias plataformas analisadas, todas elas têm funcionalidades a ter em conta no desenvolvimento da plataforma web LabSecurity.

Seguidamente apresenta -se a metodologia escolhida e que se pretende usar no processo de desenvolvimento da plataforma web.

# Bibliography

Kassem, A., Hamad, M., Moucary, C. E., Nawfal, E., & Aoun, A. (2017). MedBed: Smart Medical bed. *Advances in Biomedical Engineering (ICABME),2017 Fourth International Conference.* Beirut, Lebanon: IEEE.

NodeJs Foundation. (2018, 6 11). *Home*. Retrieved from NodeJs: https://nodejs.org/en/