# SegWeb: Sistema centralizado de análise de vulnerabilidades em aplicações Web

**Augusto Lazzarotto de Lima[1], Vinicius Bisognin Immich[1], Roberto Franciscatto[1]**

[1]Colégio Agrícola de Frederico Westphalen (CAFW)
Universidade Federal de Santa Maria (UFSM)
98400-000 – Frederico Westphalen – RS – Brasil

{gumarotto,vinibiso}@gmail.com, roberto@cafw.ufsm.br

***Abstract.*** *One of the major problems encountered today on web applications is the large number of vulnerabilities to which these applications are exposed. Vulnerabilities both in the application itself and in the settings of the servers that host it. There are currently several tools to analyze and categorize the vulnerabilities in these applications, but in a decentralized manner. This paper presents the construction of a web-based tool, containing a centralized system for classifying these vulnerabilities based on the major vulnerability assessment projects on the market..*

***Resumo.*** *Um dos grandes problemas encontrados hoje quanto as aplicações web é o grande número de vulnerabilidades a que estas aplicações estão expostas. Vulnerabilidades estas tanto na aplicação propriamente dita quanto nas configurações dos servidores que a hospedam. Existem atualmente várias ferramentas para analisar e catalogar as vulnerabilidades nessas aplicações, porém de forma descentralizada. O presente artigo apresenta a construção de uma ferramenta web, contendo um sistema centralizado de classificação dessas vulnerabilidades, baseado nos principais projetos de análise de vulnerabilidades existentes no mercado.*

## 1. Introdução

A segurança da informação e em particular em aplicações web possui um caráter fundamental nos dias atuais. A quantidade de vulnerabilidades tanto em aplicações, quanto em serviços web sem considerar o próprio fator humano, são preocupações constantes quando uma aplicação web entra em funcionamento. Encontrar formas de identificar o maior número de possíveis problemas e tratá-los de forma adequada tem sido um desafio a profissionais de segurança da informação (CERT, 2013).

A evolução constante e rápida de novas tecnologias no âmbito da informática acarretou em novas formas de desenvolver aplicações cada vez mais complexas. Em contrapartida essa evolução criou novos meios de explorar maliciosamente falhas em aplicações web, necessitando de um monitoramento constante e formas de antecipar vulnerabilidades já conhecidas e catalogadas (CSI, 2013).

O presente trabalho descrito neste artigo tem como objetivo catalogar de forma automática e/ou manual, informações de vulnerabilidades através de uma aplicação web centralizada de registros. Para isto são utilizadas ferramentas conhecidas no mercado para análise automática de vulnerabilidades em aplicações web como, por exemplo, as ferramentas: Acunetix, NetSparker e N-Stalker, para que os responsáveis pela aplicação web consigam interpretar de forma simples, clara e personalizada, possíveis falhas em

suas aplicações. Este trabalho está organizado da seguinte forma: na Seção 2, é demonstrada uma visão geral sobre segurança da informação; na Seção 3, é apresentada a forma como a ferramenta foi desenvolvida, tecnologias utilizadas e ferramentas de suporte. Na Seção 4, são explicados os resultados esperados com o uso da ferramenta e na Seção 5 as conclusões finais.

## 2. Visão Geral da Segurança da Informação

A segurança em aplicações web tem seu foco, de modo geral, em cinco objetivos principais, sendo eles: integridade, confidencialidade, disponibilidade, não repudio e autenticação. Estes pontos cruciais da segurança somam-se a outros pontos secundários formando o elo principal das características que envolvem a segurança da informação. Na tabela 1, abaixo é possível compreender um pouco melhor cada uma delas (LAUREANO, 2012).

**Tabela 1. Objetivos da Segurança na Web.**

| **Objetivo** | **Descrição** |
|---|---|
| Integridade | Garantir se os dados não foram modificados durante o transporte do mesmo, de forma acidental ou intencional. |
| Confidencialidade | Garantir que a informação só seja possível de ser visualizada pelas duas pontas que estão se comunicando. |
| Disponibilidade | Garantia de acesso ou serviço. |
| Não repudio | Garantir que nenhum dos envolvidos negue a comunicação. |
| Autenticação | Garantia de que a identidade de ambos os utilizadores seja realmente quem dizem ser. |

As aplicações web por estarem em um cenário de disponibilidade integral necessitam de proteções para assegurar os requisitos citados no parágrafo anterior. Sabe-se que em uma aplicação web, um atacante pode explorar diversos tipos de vulnerabilidades conhecidas e catalogadas, conforme (OWASP, 2013): injeção de código (SQL injection), quebra de autenticação e gerenciamento de sessão, cross-site scripting (XSS), referência insegura a objetos, configuração incorreta de segurança, exposição de dados sensíveis, redirecionamentos e encaminhamentos inválidos, entre outros. Portanto, faz-se necessário o uso de ferramentas interativas que ajudem na coleta, administração e tratamento de vulnerabilidades, de forma centralizada.

## 3. Desenvolvimento da Aplicação

A presente ferramenta foi construída com o objetivo de desenvolver uma aplicação centralizada para coleta, armazenamento e análise de vulnerabilidades, oriundas de diferentes fontes. Através de tal ferramenta permite-se ao desenvolver de um site, por exemplo, analisar os dados gerados por ferramentas de detecção de vulnerabilidades web de forma dinâmica, além de poder inserir manualmente qualquer informação de vulnerabilidade encontrada em análises estáticas (como a verificação de código fonte da aplicação).

Para o desenvolvimento da aplicação web denominada de SegWeb, foi utilizada a linguagem de programação PHP (quanto ao back-end) o sistema gerenciador de banco de dados MySQL, para criação do banco de dados e as respectivas tabelas, bem como as linguagens HTML e JavaScript no desenvolvimento da interface da aplicação (front-end). Para construção do layout utilizou-se o Framework Bootstrap (Twitter), além das linguagens de formatação HTML5 e CSS3, com o objetivo de tornar a aplicação acessível em qualquer tipo de dispositivo, permitindo desta forma que um maior número de usuários possa utilizá-la.

Quanto a forma de utilização da ferramenta proposta, existem duas maneiras de se fazer a entrada de dados no SegWeb. A primeira delas é o preenchimento de um formulário manual para qualquer um dos três principais sistemas de detecção de vulnerabilidades encontradas atualmente no mercado (considerando neste artigo a utilização das ferramentas Acunetix, NetSparker e N-Stalker). A aplicação proposta permite também enviar arquivos XML que são gerados pelas ferramentas acima citadas (fazendo desta forma a coleta automática dos resultados gerados). Estes arquivos XML, são "filtrados" pela ferramenta proposta (SegWeb) que faz o tratamento e seleciona apenas as tags XML necessárias para que seja possível fazer a classificação nos padrões do SegWeb (baseados no projeto "Top Ten" da OWASP). Na figura 1, é possível visualizar a interface referente a inserção de dados manuais na aplicação.

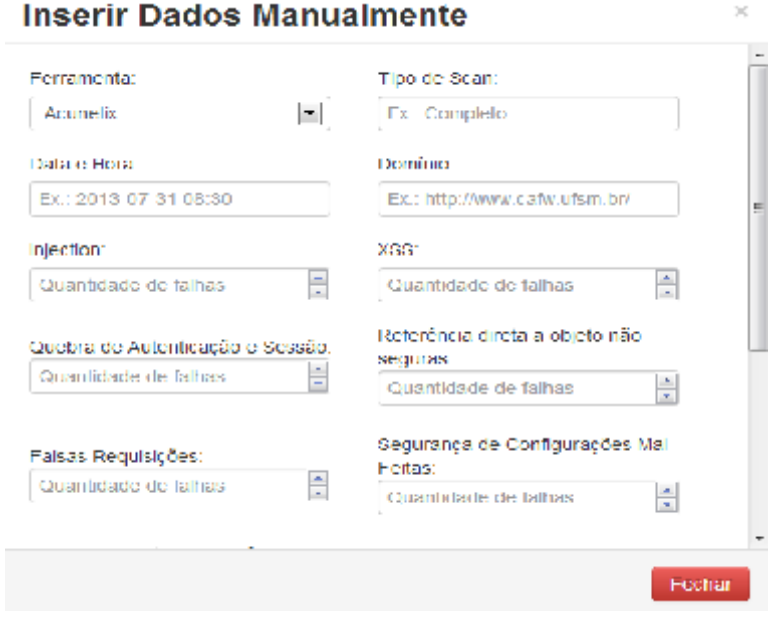


**Figura 1. Formulário de entrada de dados manual**

Como forma de consultar e analisar os resultados catalogados tanto de forma automática (XML) como de forma manual pelo SegWeb, foi desenvolvida uma seção de consultas no protótipo onde é possível ao usuário visualizar todas os dados catalogados. Nesta mesma seção é possível ver um total de todos os escaneamentos (resultados) obtidos, ou então os resultados de uma aplicação específica, ou ainda o resultado segmentado de cada ferramenta de verificação web, conforme Figura 2.


**Figura 2. Seção de consultas da aplicação**

## 4. Resultados Esperados

Como a ferramenta encontra-se em fase final de desenvolvimento, testes e adaptações, tem-se como objetivos quanto ao efetivo uso da ferramenta, que a mesma possa conseguir ler os arquivos XML gerados nas três ferramentas citadas neste trabalho (Acunetix, NetSparker e N-Stalker), de forma completa, bem como, forneça uma base de dados satisfatória a desenvolvedores e administradores de segurança, conforme inserção de dados necessária (seja ela automática ou manual), servindo de base para correção de erros e vulnerabilidades encontradas na aplicação ou servidor.

## 5. Conclusão

Neste trabalho foi possível demonstrar o projeto de uma ferramenta centralizada de coleta de vulnerabilidades denominada de SegWeb. Foi mostrado também como está sendo desenvolvido o SegWeb, uma aplicação que visa agregar e classificar várias informações retiradas de outras plataformas e sistemas de análise de vulnerabilidades. Ainda, reflexões sobre o tema durante o texto, demonstraram a importância em desenvolver ferramentas que contribuam para a verificação de segurança em ambientes web, que estão propícios a intervenções de diferentes tipos, objetivos e ideologias.

## Referências

CERT BR, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br/>.
Acesso em: 14 de setembro de 2013.

CSI, *Computer Security Institute (*Instituto de Segurança de Computadores). Disponível em <http://gocsi.com/>.
Acesso em: 13 de setembro de 2013.

LAUREANO, M. Segurança da Informação. ISBN: 978-85-63687-50-0, Páginas: 152. Editora LT – Curitiba, 2012.

OWASP. Project, 2013. Disponível em: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
Acesso em 10 de agosto de 2013.