FACULDADES INTEGRADAS PROMOVE DE BRASÍLIA
PROJETO DE INICIAÇÃO CIENTÍFICA

SOLUÇÃO SISTÊMICA BASEADA EM CÓDIGO ABERTO PARA DEFESA E MITIGAÇÃO DE ATAQUES À APLICAÇÕES WEB.

DANIEL ALMEIDA DE PAULA

BRASÍLIA
2013

DANIEL ALMEIDA DE PAULA

SOLUÇÃO SISTÊMICA BASEADA EM CÓDIGO ABERTO PARA DEFESA E MITIGAÇÃO DE ATAQUES À APLICAÇÕES WEB.

Projeto de Iniciação Científica apresentado ao PIBC (Programa Institucional de Bolsas de Iniciação Científica) das Faculdades Integradas ICESP/Promove de Brasília.

Orientador: Professor Dirceu Silva da Silva Junior

BRASÍLIA
2013

DANIEL ALMEIDA DE PAULA

SOLUÇÃO SISTÊMICA BASEADA EM CÓDIGO ABERTO PARA DEFESA E MITIGAÇÃO DE ATAQUES À APLICAÇÕES WEB.

Projeto de Iniciação Científica apresentado ao PIBC (Programa Institucional de Bolsas de Iniciação Científica) das Faculdades Integradas ICESP/Promove de Brasília.

APROVADO EM:_____DE_____DE_____:

_____

Orientador (a) Profº. DIRCEU SILVA DA SILVA JUNIOR

Instituto Científico de Ensino Superior e Pesquisa – ICESP/Promove de Brasília

_____

Avaliador (a) Profº.

Instituto Científico de Ensino Superior e Pesquisa – ICESP/Promove de Brasília

_____

Avaliador (a) Profº.

Instituto Científico de Ensino Superior e Pesquisa – ICESP/Promove de Brasília

BRASÍLIA – DF
2013

SUMÁRIO

1 – APRESENTAÇÃO

Este projeto propõem apresentar solução sistêmica para realizar a defesa de perímetro e, consequentemente, a mitigação de ataques realizados em aplicações web. Para isto, inicialmente realizar-se-á pesquisa documental e bibliográfica para listar os principais ataques que ameaçam as aplicações deste tipo atualmente e, posteriormente, utilizar-se-á componentes de código aberto, melhores práticas vigentes em segurança da informação e desenvolvimento de software para apresentar modelo de protótipo que contribua de maneira positiva para a segurança de aplicações web vulneráveis.

1.1 – INTRODUÇÃO

Em paralelo ao crescimento da rede mundial de computadores (Internet), surgiu a necessidade da prestação de serviços instantâneos visando suprir necessidades de diversos setores e atividades, como: mundo financeiro, comércio eletrônico, pesquisas acadêmicas e, até mesmo, relacionamentos interpessoais.

Com a facilidade de acesso a informação, e o crescimento da demanda pelos serviços envolvidos, aplicações web começaram a ser desenvolvidas de forma acelerada e indiscriminada. Este tipo de aplicação, atualmente, é alvo de diversos tipos de ataques e estão suscetíveis a uma gama de ameaças.

Dentro os muitos tipos de ataques existentes, exemplo são os ataques de injeção de códigos (*injection*) que de acordo com a OWASP (*Open Web Application Security*) lideram o topo do ranking de ataques praticados diretamente a aplicações web. Para este tipo de ataque, diversos tipos de tecnologias são utilizadas, como: SQL, LDAP, etc. O ataque consiste em inserir códigos afim de enganar o interpretador, com a finalidade executar comandos ou acessar dados indevidamente. Os agentes desta forma de ataque, podem ser usuários locais (internos) ou remotos (externos).

Bancos de dados também são alvos e vítimas da insegurança de aplicações web. A injeção de código malicioso em formulários de aplicações web (Exemplo: *MySQL Injection*) está entre as técnicas mais apuradas e realizadas nos últimos anos. A empresa de segurança web Imperva, afirma que ataques nesta modalidade

comprometeram a segurança de sites famosos com Yahoo, com o roubo de 453 mil senhas no ano de 2012. Para o levantamento destes estudos, a Impeva monitorou cerca de 50 aplicativos web, e alguns destes, foram atacados a cada 3 dias.

Outra modalidade de ataque muito utilizada contra aplicações web, é o ataque de Negação de Serviço, o famoso DDoS – o qual tem a finalidade de deixar um determinado serviço indisponível, utilizando para isto muitas requisições simultâneas. De acordo com o site Atlas Arbor, que faz o monitoramento do trafego internacional de dados na internet, o Brasil esta na sétima posição de países que mais realizam ou estão envolvidos nesta modalidade de ataque. O grupo ativista, mundialmente conhecido com *Anonymous*, especializado a atacar sites governamentais, divulgou uma nota em seu site oficial relatando que estão juntando assinaturas com o intuito de tornar essa modalidade de ataque em uma espécie de protesto.

A nova economia está intrinsecamente ligada ao desenvolvimento e disponibilização de aplicações web. Estas, por sua vez, necessitam ser protegidas.

1.2 – JUSTIFICATIVA

A grande maioria das aplicações são desenvolvidas com prazos curtos e determinados – o que também contribui para sua insegurança. A presente proposta de trabalho visa apresentar solução sistêmica com o intuito de fortalecer a segurança de aplicações web, bem como mitigar os ataques mais utilizados na atualidade. O projeto de pesquisa justifica-se no momento que considera-se a importância das aplicações web para a nova economia, as ameaças e ataques atuais que existem neste tipo de arquitetura computacional e as más praticas de programação.

1.3 – OBJETIVOS

1.3.1 – Geral

Pesquisar e analisar as principais formas de ataques realizados contra aplicações web e identificar os mecanismos necessários para aperfeiçoar a defesa de determinada aplicação web insegura.

1.3.2 – Específicos

Os objetivos específicos são:

- Identificar e apresentar os principais ataques realizados em aplicações web;
- Projetar ambiente para simular aplicação web vulnerável que permita a simulação e testes dos principais tipos de ataques;
- Em ambiente controlado e de testes, efetuar os principais tipos de ataques com o intuito de mensurar a utilização dos canais de ataques e estabelecer critérios mínimos de identificação; e
- Projetar solução sistêmica baseada em objetos de código aberto para proteção de aplicação web.

2 – MATERIAIS E MÉTODOS

Primeiro será realizada uma revisão teórica abordando os seguintes temas: arquitetura cliente servidor, camadas de aplicação web, camadas de comunicação, ataques, ameaças, riscos, entre outros.

Posteriormente, realizar-se-á desenvolvimento de soluções que simule tanto exemplos de vulnerabilidades de aplicações web quanto exemplos de ataques. Neste momento, será projeto e implantado ambiente controlado e simulado para os testes.

Por fim, será projetada, implementada, implantada e testada solução sistêmica para defesa e mitigação de ataques para ambientes que fornecem aplicações web.

Quando necessário o desenvolvimento dos novos objetos de software, será utilizado o modelo de engenharia de software conhecido como Programação Extrema (XP, do inglês *eXtreming Programming*). *XP* é uma metodologia americana que surgiu no final da década de 90, focada num pequeno conjunto de valores, princípios e práticas, que diferem da forma tradicional de se desenvolver.

Toda os recursos de hardware e software serão fornecidos pelo pesquisador/orientador.

3 – CRONOGRAMA

ATIVIDADES	PERÍODO
Realizar levantamento dos principais tipos de ataques que ameaçam de aplicações web.	Mês 1
Verificar quais os métodos e vetores utilizados pelos principais tipos de ataques que ameaçam as aplicações web	Mês 2
Levantar os requisitos funcionais e não funcionais para proteger as aplicações web dos principais tipos de ataques. Listar quais tipos de ataques serão objetos de estudo/mitigação.	Mês 3
Projetar ambiente para simular aplicação web vulnerável aos principais tipos de ataques (ataques selecionados).	Mês 4
Implantar ambiente de testes. Incluindo aplicação web insegura e implementação de simulações dos principais tipos de ataques.	Mês 5
Realizar os principais tipos de ataques no ambiente de testes. Realizar análise dos ataques. Mensurar canais de ataques e critérios de identificação/proteção dos mesmos.	Mês 6
Projetar solução. Apresentar modelos.	Mês 7
Implantar ambiente de desenvolvimento e homologação. Iniciar implementação da solução.	Mês 8
Escolher e implantar principais objetos de back-end.	Mês 9
Implementação dos objetos necessários.	Mês 10
Implementação dos objetos necessários	Mês 11
Realizar deploy de protótipo	Mês 12

4 – REFERÊNCIAS

OWASP, Open Web Application Security Project - Disponível em: <https://www.owasp.org/index.php/Top_10_2013-T10> . Acessado em 28 de abril de 2013.

ANONYMOUS BRASIL, Site oficial do grupo ativista Anonymous - Disponível em: <http://www.anonymousbrasil.com/brasil-e-o-4o-pior-do-mundo-em-seguranca-tecnologica/>. Acessado em 28 de abril de 2013.

Blog Kaspersky Brasil, Blog oficial da empresa de segurança e soluções Kaspersky. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/blog-da-kaspersky>. Acessado em 28 de abril de 2013.

ATLAS DASHBOARD - **Active Threat Level Analysis System**, Sistemas de monitoramento da Internet, Disponível em: <http://atlas.arbor.net/>. Acessado em 28 de abril de 2013.

iMPERVA – **Security Network Solutions**, Disponível em: < - http://www.imperva.com/docs/HII_Lessons_Learned_From_the_Yahoo_Hack.pdf> Acessado em 28 de abril de 2013.

Portal Tecmundo - Site oficial sobre notícias relacionado a Tecnologia da Informação - Disponível em: < http://www.tecmundo.com.br/ataque-hacker/35056-anonymous-quer-que-ddos-seja-reconhecido-como-forma-legal-de-protesto.htm> Acessado em 28 de abril de 2013.