

SEGURANÇA WEB



Alunos: Fábio Castro e Natali Lisboa

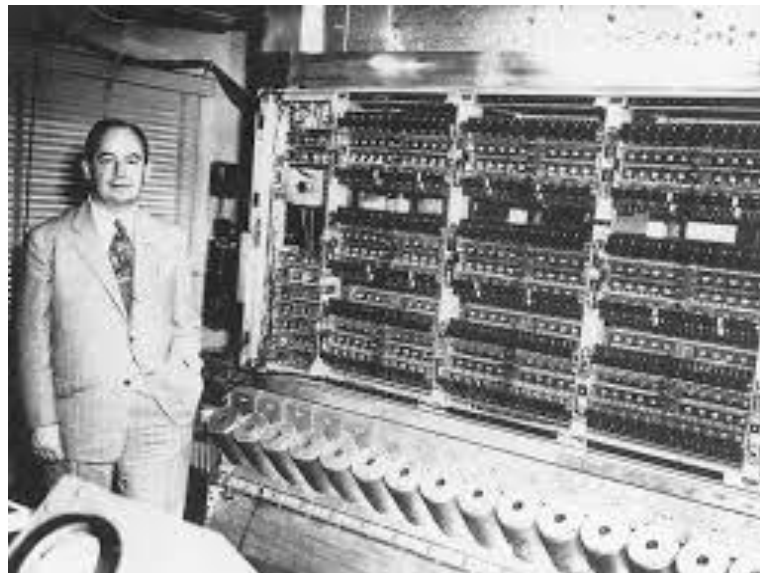
INTRODUÇÃO

Segurança Web é qualquer atividade projetada para proteger a usabilidade e a integridade de sua rede e dados. Inclui tecnologias de hardware e software.



HISTÓRIA

Em 1949, John Von Neuman criou a teoria de auto-reprodutores, que dizia haver possibilidade de se desenvolverem pequenos programas replicáveis, capazes de controlar outros programas com uma estrutura semelhante. Apesar do conceito poder ter milhares de aplicações legítimas na informática, é fácil imaginar as implicações negativas desta teoria defendida por Von Neumann: os vírus informáticos.



HISTÓRIA

Em 1959, nos laboratórios informáticos da Bell, três jovens programadores: Robert Thomas Morris, Douglas McIlroy e Victor Vysotsky, criaram um jogo chamado CoreWar, baseado na teoria de Von Neumann, e em que os programas combatiam entre si, tentando ocupar tanta memória quanto possível, e eliminar os programas opositores. Este jogo é considerado o precursor dos vírus informáticos.

HISTÓRIA

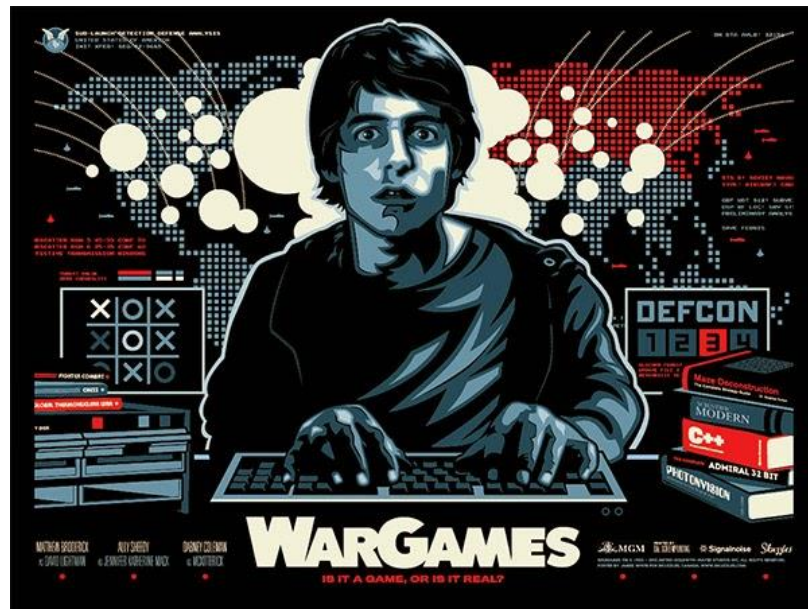
Em 1972, Robert Thomas Morris criou o primeiro vírus digno dessa designação: o Creeper, que infectava máquinas IBM 360 na ARPANET (o predecessor da Internet), mostrando uma mensagem dizendo “**I’m the creeper, catch me if you can**”. Para o eliminar, foi criado um vírus chamado Reaper para o procurar e destruir. Esta é a verdadeira origem dos antivírus atuais.

HISTÓRIA

Ao longo dos anos 80 os computadores se tornaram mais populares, e nessa época começaram a ver os primeiros criadores dedicados de programas maliciosos, e em 1981, Richard Skrenta criou o primeiro vírus de propagação massiva: o Elk Cloner, que mostrava um poema a cada 50 reinicializações dos computadores infectados.

HISTÓRIA


O Jogo de Guerra (WarGames, 1983), conta a história de um adolescente apaixonado pela informática e por jogos de video game. Sua vontade de jogar é tamanha que, durante uma busca por um novo jogo, ele acaba se conectando acidentalmente ao sistema de defesa americano, provocando uma iminente terceira guerra mundial. A princípio, o governo acreditava que o adolescente era um espião soviético, mas depois que bagunça causada na defesa militar é desfeita, percebem que ele não era nada mais que um viciado em jogos virtuais.



INPIRAÇÃO EM WARGAMES

A popularidade do filme inspirou muitas pessoas a começarem a implementar alguns dos métodos que o jovem utilizou para violar sistemas restritos, inclusive o que é conhecido como *war dialing*.

Um discador de guerra é um programa de computador usado para identificar os números de telefone que podem fazer uma conexão com um modem de computador. O programa discava automaticamente um intervalo definido de números de telefone e registros e insere em um banco de dados os números que se conectam com sucesso ao modem. Alguns programas também podem identificar o sistema operacional em execução no computador e também podem realizar testes de penetração automatizados. Nesses casos, o discador de guerra percorre uma lista predeterminada de nomes de usuário e senhas comuns, na tentativa de obter acesso ao sistema.



MALWARE, VÍRUS,
WORMS, TROJANS,
ROOTKITS, SPYWARES,
ADWARE

MALWARES

Malware é a combinação das palavras inglesas *malicious* e *software*, ou seja, programas maliciosos. São programas e comandos feitos para diferentes propósitos: apenas infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços, etc.

Os malwares se dividem em categorias, sendo: vírus, worms, trojans, rootkits, spywares, adwares.

VÍRUS

Os vírus se diferenciam dos outros malwares por sua capacidade de infectar um sistema, fazer cópias de si mesmo e tentar se espalhar para outros computadores, da mesma maneira que um vírus biológico faz.

Vírus são típicos de arquivos anexos de emails, pois quase sempre é necessário que um vírus seja acionado através de uma ação do usuário.



VÍRUS

Um dos vírus mais perigosos já registrados teve origem nas Filipinas. “ILOVEYOU”, uma carta de amor que se espalhou por email, afetou mais de 50 milhões de computadores Windows em 5 de maio de 2000. Seu nome oficial é “LOVE-LETTER-FOR-YOU.txt.vbs” (sendo essa última extensão .vbs escondida por padrão pelo Windows) e sua abreviação é ILOVEYOU. Danificava a máquina local e mandava uma cópia de si mesmo para todos os contatos do usuário no Outlook.



WORMS

Um worm (verme) de computador é um programa malicioso que se utiliza de uma rede para se espalhar por vários computadores sem que nenhum usuário interfira neste processo (aí está a diferença entre vírus e worm).

Os worms são perigosos, pois podem ser disparados, aplicados e espalhados em um processo totalmente automático e não precisam se anexar a nenhum arquivo para isso. Enquanto vírus buscam modificar e corromper arquivos, os worms, costumam consumir banda de uma rede.

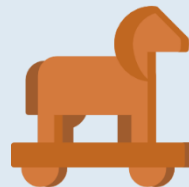


TROJANS

A relação com o cavalo de tróia, recebe-se um conteúdo que acha ser uma coisa, mas ele se desenrola em outras coisas que você não esperava ou não foi alertado.

Trojan é um conjunto de funções desenvolvido para executar ações indesejadas e escondidas.

Nem todo trojan prejudica um computador, pois, em alguns casos, ele apenas instala componentes dos quais não temos conhecimento, forçadamente.



ROOTKITS

Os rootkits miram simplesmente o controle de um sistema operacional sem o consentimento do usuário e sem serem detectados.

O grande mérito do rootkit é sua capacidade de se esconder de quase todos os programas antimalwares através de um avançado código de programação. Mesmo que um arquivo rootkit seja encontrado, em alguns casos ele consegue impedir que você o delete.



ADWARE

Adwares são programas que exibem, executam ou baixam anúncios e propagandas automaticamente e sem que o usuário possa interferir.

Geralmente, ícones indesejados são colocados em sua área de trabalho ou no menu Iniciar para que você acesse o serviço desejado.



XSS

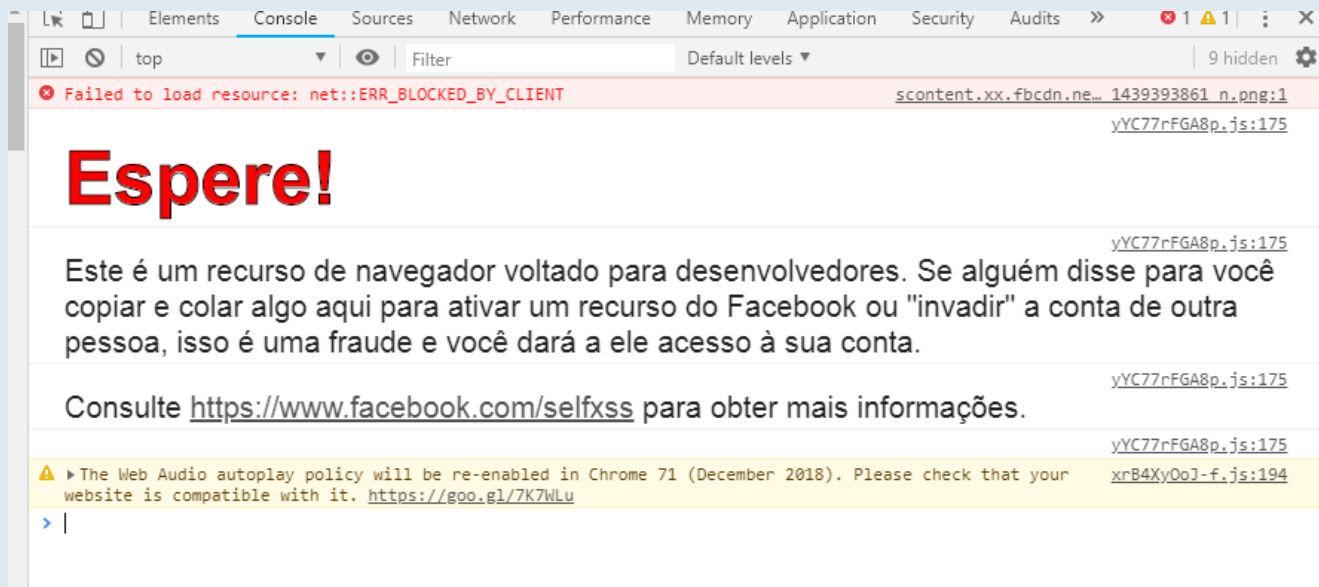
CROSS-SITE SCRIPTING

Os ataques Cross-Site Scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites benignos e confiáveis.

Ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código mal-intencionado, geralmente na forma de um script, para um usuário final diferente.

Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário desavisado. O navegador do usuário final não tem como saber que o script não deve ser confiável e irá executar o script. Como ele acredita que o script veio de uma fonte confiável, o script mal-intencionado pode acessar cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

PREVENÇÃO DO FACEBOOK



SQL INJECTION

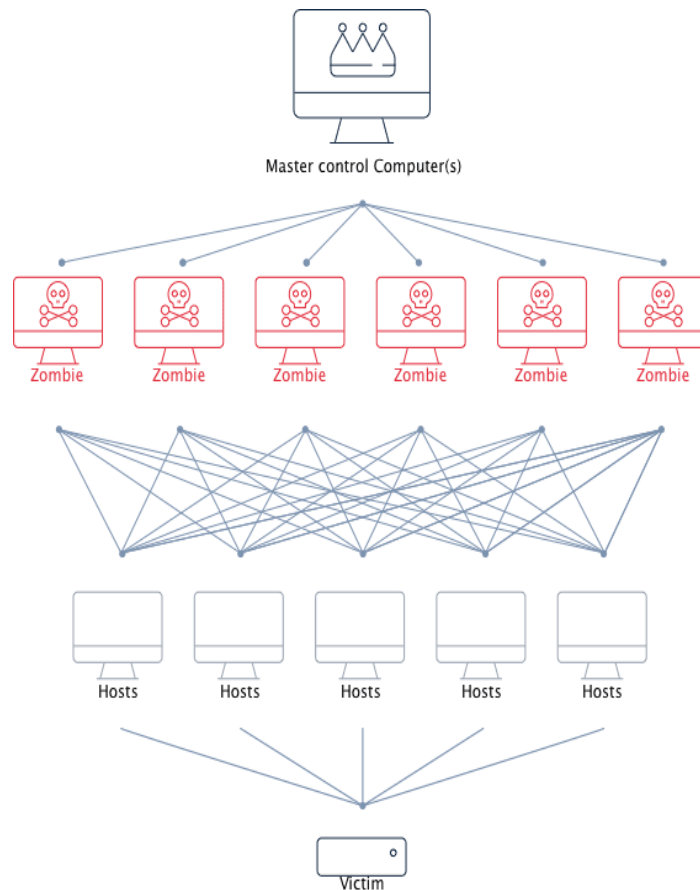
É uma técnica em que usuários maliciosos podem injetar comandos SQL em um procedimento SQL através da entrada de dados em uma página web. Esses comandos SQL injetados alteram um SQL já existente e que deveria processar uma requisição pré-definida. Esse SQL que pode ser injetado compromete severamente a segurança de uma aplicação web.

A alteração direta de comandos SQL pode expor dados escondidos, sobrescrever dados valiosos, ou ainda executar comandos de sistema perigosos no servidor.

ATAQUE DE NEGAÇÃO DE SERVIÇO DOS (DENIAL OF SERVICE)

O criminoso cria um fluxo interminável de solicitações falsas ao computador alvo, de tal maneira que ele fique sobrecarregado e impedido de atender às solicitações dos usuários verdadeiros.

Esse ataque é comumente realizado pelas chamadas redes zumbis, da qual fazem parte computadores infectados com um determinado tipo de praga digital. Os computadores infectados ficam sob o controle do criminoso, que ordena a realização dos acessos falsos que irão sobrecarregar o sistema alvo.



CONTEÚDO MISTO

Quando um usuário visita uma página veiculada por HTTPS, sua conexão com o servidor da Web é criptografada com o TLS e, portanto, protegida da maioria dos sniffers e ataques man-in-the-middle.

Uma página HTTPS que inclui conteúdo buscado usando HTTP de texto não criptografado é chamada de página de conteúdo misto. Páginas como essa são criptografadas apenas parcialmente, deixando o conteúdo não criptografado acessível a sniffers e invasores man-in-the-middle.

CSP

POLÍTICA DE SEGURANÇA DE CONTEÚDO

É um padrão de segurança de computador introduzido para impedir o cross-site scripting (XSS), clickjacking e outros ataques de injeção de código resultantes da execução de conteúdo mal-intencionado no contexto confiável da página da web.

É uma Recomendação do Candidato do grupo de trabalho W3C sobre Segurança de Aplicações Web, amplamente apoiada por navegadores modernos.

POLÍTICA DE MESMA ORIGEM

A política de mesma origem é um mecanismo de segurança crítico que restringe como um documento ou script carregado de uma origem pode interagir com um recurso de outra origem. Ajuda a isolar documentos potencialmente maliciosos, reduzindo possíveis vetores de ataque.

HTTP e HTTPS

É o protocolo padrão para a Web. Através dele, os navegadores requisitam as páginas da Web e as recebem. No entanto, como o HTTP é um protocolo baseado em texto, ou seja, toda a informação transmitida está em texto, os dados do usuário e do servidor podem ser interceptados ou alterados no meio do caminho.

Com o uso do HTTPS, que é o HTTP seguro, adiciona-se alguns princípios de segurança, como confidencialidade, integridade e autenticação.

A maioria das explicações resume o HTTPS como um HTTP com o SSL (*Secure Sockets Layer*). A base do SSL e dos certificados da Internet é a criptografia.

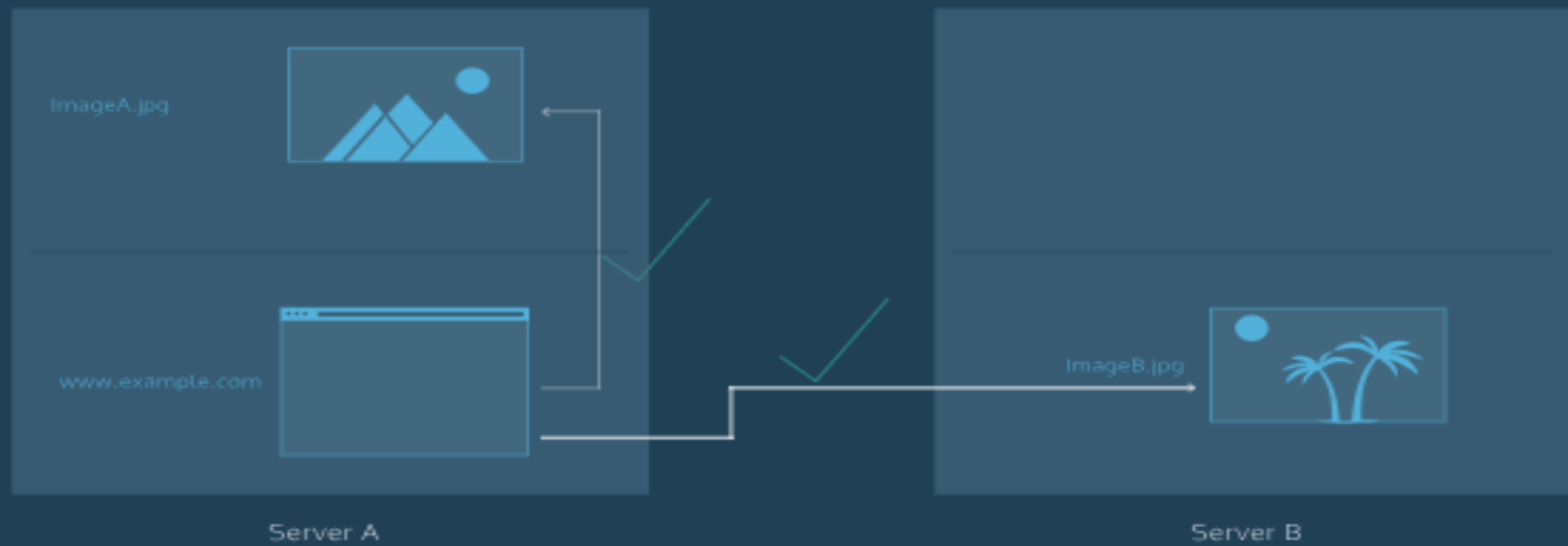
HTTPS é criptografado e HTTP não é.

CORS

COMPARTILHAMENTO DE RECURSOS DE ORIGEM CRUZADA

Uma solicitação de recurso (como uma imagem ou uma fonte) fora da origem é conhecida como solicitação de *origem cruzada*. O CORS (compartilhamento de recursos de origem cruzada) gerencia solicitações de origem cruzada.

O CORS permite que os servidores especifiquem quem (ou seja, quais origens) podem acessar os ativos no servidor, entre muitas outras coisas.



Cross - origin policy

PADRONIZAÇÃO E SEGURANÇA

Empresas de todos os setores dependem de regulamentações e padrões definidos por associações, o que não é diferente no setor de segurança da informação.

Muitas consultorias e fabricantes da área de segurança concordam com o modelo de segurança padrão conhecido como CIA.



CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE

Confidentiality, Integrity, and Availability

CONFIDENCIALIDADE

Refere-se a proteger informações confidenciais de serem acessadas por partes não autorizadas.



INTEGRIDADE

É garantir a autenticidade da informação - essa informação não é alterada e a fonte da informação é genuína.

DISPONIBILIDADE

Significa garantir que a informação possa ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções.



REFERÊNCIAS
