



Segurança em Aplicações WEB

Professor: Samuel Gonçalves Pereira


**“Somos o que repetidamente
fazemos. Portanto, a excelência
não é um feito, é um hábito”.**

Aristóteles



Porque estudar Segurança de Aplicações WEB?

- As vulnerabilidades mais exploradas são conhecidas e possuem soluções documentadas, porém não são implementadas corretamente nas aplicações.
- O número de aplicações na WEB está em constante crescimento, com a popularização da internet e de dispositivos móveis sempre haverá aumento destas ferramentas.
- As soluções para os problemas relacionados a segurança são simples, só dependem de conhecimentos sólidos.



Home » Segurança

Ataques hackers contra empresas cresceram 148% em março

Por Felipe Demartini | 24 de Abril de 2020 às 07h35

 Cult of Mac

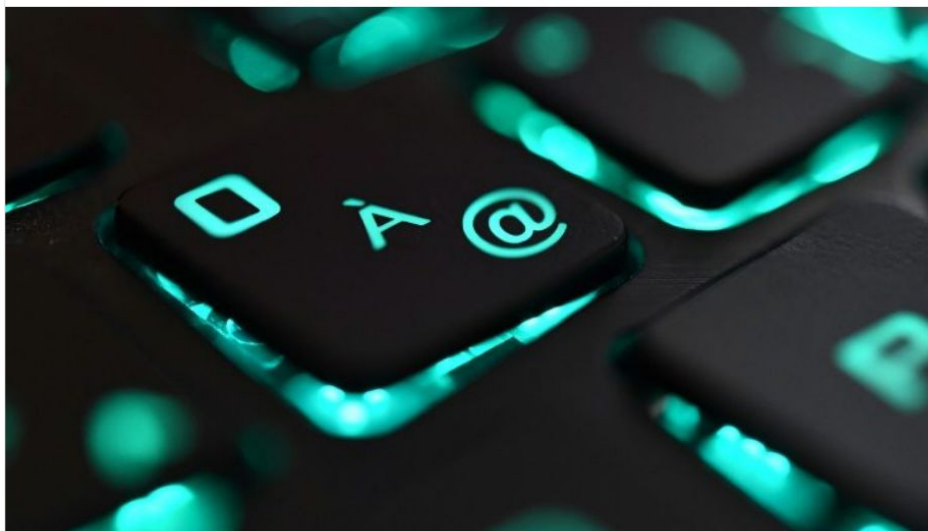
A adoção repentina de regimes de home office e a dificuldade maior de aplicar medidas de segurança para funcionários que trabalham de casa levou a um aumento de 148% no número de ataques hackers contra empresas em março. Os números mostram que os bandidos estão aproveitando o período de pandemia do novo coronavírus para aplicar golpes, apostando na ideia de que, remotamente, os sistemas dificilmente contam com a mesma proteção do que dentro das estruturas internas.

Isso se tornou verdade, principalmente, para quadrilhas que trabalham com **ransomware**, que já vinha crescendo em popularidade e se tornou, no último mês, o tipo de malware que mais atingiu as corporações de todo o mundo. Os dados são da VMware Carbon Clack, uma empresa especializada em cibersegurança e virtualização, que viu o número de ataques mais do que dobrar em relação ao que foi registrado em fevereiro de 2020.

Fonte: <https://canaltech.com.br/seguranca/ataques-hackers-contras-empresas-cresceram-148-em-marco-163768/>

CIENCIA

Google alerta para ataques de hackers usando a COVID-19 como isca



Google alerta para ataques de hackers usando a pandemia do novo coronavírus como isca para enganar os usuários - AFP/Arquivos

AFP

22/04/20 - 19h40 - Atualizado em 23/04/20 - 12h10

Spam, 'phishing' e malware: a crise sanitária global, provocada pela pandemia do novo coronavírus é vista como uma oportunidade para grupos de hackers apoiados por países, alertou a Google nesta quarta-feira

(22). Fonte: <https://www.istoedinheiro.com.br/google-alerta-para-ataques-de-hackers-usando-a-covid-19-como-isca/>

Após análise, Nintendo confirma que 160 mil contas foram invadidas por hackers

No início da semana a Nintendo informou que estava fazendo análises sobre a invasão de contas. Agora a empresa afirmou que cerca de 160 mil contas foram invadidas. Confira os detalhes e saiba como se proteger.

Em 24/04/2020 11:30 em [GAMES](#)



Imagem ilustrativa de Invasão de contas Nintendo. Fonte: dallystar



Desde o mês de março, diversos usuários começaram a relatar o recebimento de alertas de acessos não autorizados em suas contas

Fonte: <https://www.oficinadanet.com.br/games/30742-apos-analise-nintendo-confirma-que-160-mil-contas-foram-invadidas-por-hackers>

Microsoft envia alerta 'inédito' para hospitais vulneráveis a ataques de hackers

Empresa diz que instituições precisam ser protegidas e que hackers adaptaram técnicas para aplicar novos golpes durante a pandemia do coronavírus.

Por Altieres Rohr

03/04/2020 12h25 · Atualizado há 3 semanas



Hacker rouba R\$ 132 milhões em criptomoedas, deixa IP exposto e devolve tudo

"Hacker" deixou IP exposto e resolveu devolver os fundos

Por: **Livecoins** - 21/04/2020 12:04



Hackers conseguiram drenar US \$ 25 milhões de duas carteiras de criptomoedas (bitcoin e ethereum) no último final de semana. Utilizando **ataque de reentrada em contratos inteligentes** eles conseguiram roubar criptomoedas de forma contínua sem nenhuma dificuldade até que o status inicial da transação fosse alterado.
fevereiro de 2020.

Fonte: <https://livecoins.com.br/hacker-rouba-r-132-milhoes-em-criptomoedas-deixa-ip-exposto-e-devolve-tudo/>



Quem sou eu

Samuel Gonçalves Pereira

- Graduado em Sistemas de Informação pela Universidade Estadual de Goiás
- MBA em Data Science e Internet das Coisas pela Faculdade SENAI FATESG
- Profissional certificado:
 - LPIC-1
 - UEWA
 - MTCTCE
 - MTCNA
 - MTCRE
- Network Manager de empresa alimentícia com faturamento diário superior a 10 Mi
- Mais de 8 anos em experiência
- Professor de Segurança em Pós Graduação



O que você aprenderá neste curso?



Infográfico - OWASP Top 10

Veja nos recursos desta aula o infográfico que criei sintetizando as 10 principais vulnerabilidades em aplicações WEB segundo a OWASP(Open Web Application Security Project). Sendo elas:

1. Injeção
2. Autenticação
3. Exposição
4. Referências a XML
5. Acesso ao Sistema
6. Configurações Incorretas
7. XSS Scripts
8. Desserialização
9. Componentes Vulneráveis
10. Registro e Monitoramento insuficientes



Agenda do Curso

- Apresentação do curso "Segurança em Aplicações WEB"
- Criação do Laboratório de Estudos
- Princípios da Segurança da Informação e Proteção de Dados
- Tipos de Testes de Invasão
- OWASP
- Testes realizados em Ambientes WEB
- Injeção SQL
- Local/Remote File Inclusion
- Code Injection
- Command Injection
- XSS / Cross Site Scripting
- Mecanismos de Recuperação de senhas vulneráveis



Apresentação do Curso

- Curso prático com laboratório de testes
- Voltado para profissionais de Segurança e Desenvolvedores
- Exercícios práticos em cada módulo
- Aplicação em ambientes reais
- Possibilidade de renda extra com aplicação do conhecimento do curso



Como estudar neste curso?

- Aulas práticas!
- Assista as aulas e faça os exercícios durante as aulas, para melhor fixação dos conteúdos
- Pergunte sempre que tiver dúvidas!
- Execute todos os exercícios disponíveis no curso
- Utilize a função Split do Mozilla Firefox
- Utilize a plataforma Udemy a seu favor neste curso!



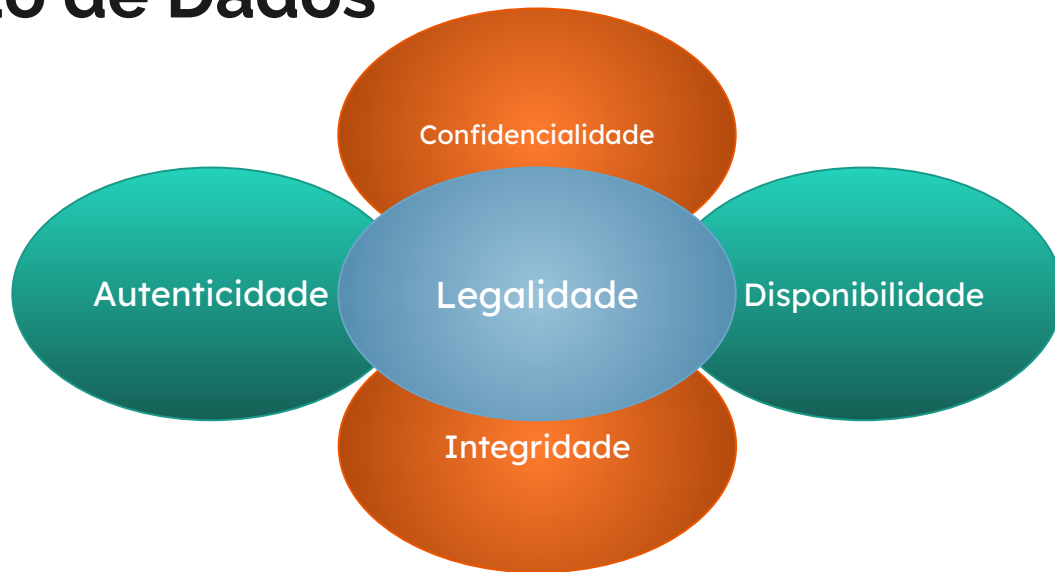
Configuração do Laboratório de Estudos

- Utilizaremos um laboratório virtualizado com Virtual Box
- Faça o download e a instalação do Virtual Box, os arquivos necessários estão disponíveis no link:
 - <https://www.virtualbox.org/wiki/Downloads>
- Faça o download dos arquivos “.ova” necessários, nos links:
 - Kali Linux:
<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b>
 - OWASP BWA
[https://sourceforge.net/projects/owaspbwa/files/1.2/OWASP Broken Web Apps VM 1.2.ova/download](https://sourceforge.net/projects/owaspbwa/files/1.2/OWASP%20Broken%20Web%20Apps%20VM%201.2.ova/download)
- Configure conforme vou lhe mostrar na aula

Módulo 1

Princípios da Segurança, Testes de Vulnerabilidades, Ferramentas e Documentação

Princípios de segurança da Informação e Proteção de Dados





Análise de Vulnerabilidades

- A Análise de Vulnerabilidades é similar ao pentest, pois se trata de uma auditoria completa buscando encontrar possíveis falhas de segurança.
- Em uma análise de vulnerabilidades busca-se sempre manter a integridade do sistema auditado, logo, sua intenção é a correção das vulnerabilidades encontradas.
- Toda aplicação possui vulnerabilidades, cabe a nós encontrá-las e corrigi-las.



Tipos de Análises de Vulnerabilidades

- Black box
 - Sem conhecimento da estrutura
- White box
 - Com conhecimento da estrutura
- Gray box
 - Conhecimento parcial



Análise de Vulnerabilidades - Planejamento

- Informações gerais
- Contrato de acordo
- Objetivo da Análise
- Limitações
- Linha do tempo (Relatórios)



Fases da Análise de Vulnerabilidades

- Reconhecimento (Footprint)
- Varredura (Scanning)
- Exploração (Gaining Access)
- Escalação de Privilégios (Maintaining Access)

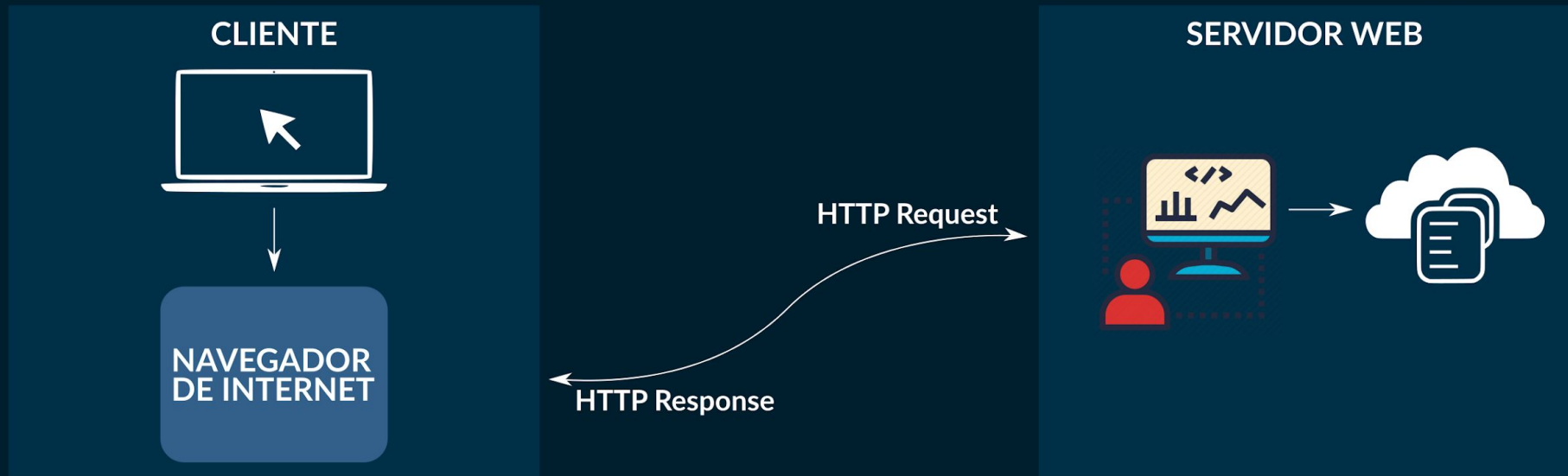


Metodologia para Análise de Vulnerabilidade

Existem vários tipos de metodologias que podem ser aplicadas na Análise de Vulnerabilidades. Cada uma atende à necessidades específicas, algumas destas são:

- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- WASC-TC (Web Application Security Consortium Threat Classification)
- OWASP (Open Web Application Security Project)

ARQUITETURA BÁSICA DE UMA APLICAÇÃO WEB





OWASP

Open Web Application
Security Project



OWASP

Esta metodologia é direcionada para testes em servidores e aplicações WEB. A OWASP mantém uma lista das principais vulnerabilidades para web. Seguem alguns testes realizados em ambientes WEB:

- Injeção: SQL, Local File Inclusion, Remote File Inclusion, Code Injection, Command Injection, XSS
- Quebra do sistema de Autenticação
- Directory Traversal
- File Upload
- Configurações Falhas
- CSRF
- Negação de Serviço

Referências e documentação: https://www.owasp.org/index.php/Main_Page



OWASP BWA

O projeto BWA Broken Web Applications (Aplicações Web Quebradas) se trata de uma máquina virtual executando várias aplicações com vulnerabilidades conhecidas, visando apresentar maneiras simples de testar e aprender sobre:

- segurança de aplicações web
- técnicas de enumeração manual
- ferramentas automatizadas para enumeração
- ferramentas de análise de código fonte vulnerável
- ataques na web
- WAFs e tecnologias de código similares

Documentação: [https://www.owasp.org/index.php/OWASP Broken Web Applications Project](https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)



OWASP ZAP

O OWASP Zed Attack Proxy (ZAP) é uma das ferramentas de segurança gratuitas mais populares do mundo e é mantido ativamente por centenas de voluntários internacionais.

Trata-se de um proxy, que facilita a realização de testes de intrusão em aplicações Web, pois possui scanners automatizados em sua toolbox, dentre outras funcionalidades para o mesmo fim, podendo encontrar automaticamente vulnerabilidades de segurança em seus aplicativos da web enquanto estiver desenvolvendo e testando seus aplicativos, bem como pentesters.

Documentação: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Módulo 2

Testes de Vulnerabilidade e Injeções diversas



SQL Injection

- O SQLi (que significa Injeção de Linguagem de Consulta Estruturada) é um método utilizado para extrair ou modificar dados em um banco de dados disponível em um sistema, geralmente web
- A linguagem SQL foi projetada para gerenciar dados mantidos em um sistema de gerenciamento de banco de dados de relacionamento
- Qualquer site que esteja armazenando dados normalmente o faz com um banco de dados, esses ataques SQL são uma questão importante, mas são fáceis de evitar



Cross Site Scripting

- É uma vulnerabilidade presente em aplicações web que permite que o cibercriminoso insira códigos Java Script para obter certos tipos de vantagem sobre as vítimas.
- O Cross-Site Scripting (XSS) é normalmente aplicado em páginas que sejam comuns a todos os usuários, como por exemplo a página inicial de um site ou até mesmo páginas onde usuários podem deixar seus depoimentos. Para que o ataque possa ocorrer é necessário um formulário que permita a interação do atacante, como por exemplo em campos de busca ou inserção de comentários.



Cross Site Scripting

- Por um lado, o servidor “A” que pertence ao “mibanco.com”, o qual é vulnerável a XSS.
- Por outro lado, um atacante que consegue injetar um código malicioso no “meubanco.com” por meio da exploração da XSS. O código que injeta faz com que, depois que o usuário acesse a página, seja redirecionado para outro site exatamente igual ao “meubanco.com”.
- O usuário vítima acessa por meio do navegador ao “meubanco.com”; no entanto, ao executar o código malicioso injetado pelo atacante (sem saber), estará registrando os seus dados no site clonado. Obviamente, isso compromete completamente as suas informações financeiras.



Command Injection

- Se esta vulnerabilidade existir, é possível executar comandos diretamente da aplicação, conseguindo acesso não autorizado ao sistema.



Local/Remote File Inclusion

- Local File Inclusion (LFI) é o processo de inclusão de arquivos, que já estão presentes localmente no servidor em questão. Esta falha ocorre, por exemplo, quando uma página recebe como entrada, o caminho para o arquivo que será incluído, e esta entrada não é validada de forma correta pela aplicação web, possibilitando assim que caracteres de Directory Traversal - [Passagem de Diretório (../..)] sejam injetados.
- Remote File Inclusion (RFI) é o processo de inclusão de um arquivo externo ao servidor, dentro do mesmo.
- Através da estrutura do site e por uma falha na programação do mesmo, atacantes podem puxar informações vitais de um servidor, injetando códigos através da barra de endereço do navegador.



Denial of Service

Trata-se de um ataque de negação de serviço, onde o objetivo é indisponibilizar o servidor alvo.

Módulo 3

Transporte inseguro e mecanismos de recuperação de senhas vulneráveis



Transporte de credenciais por canais inseguros

- Citada na OWASP como uma vulnerabilidade importante, grande parte das informações trafegadas na WEB não é criptografada.
- Conseguimos interceptar os dados, e capturar informações. Vamos testar!



Captura de pacotes por meio de Sniffers

- Sniffers são uma categoria ampla de aplicações que englobam qualquer utilitário que tenha a capacidade de executar uma função de captura de pacotes
- O sniffing passivo é considerado ser todo o tipo de sniffing onde o tráfego é olhado mas não alterado em nenhuma maneira
- No sniffing ativo, não só o tráfego é monitorado, mas também pode ser alterado de alguma forma, como determinado pelo atacante



Prova de Conceito - Sniffing Passivo

Vamos monitorar o tráfego ao logar em nossas aplicações OWASP BWA com as ferramentas:

- tcpdump
- Wireshark



Brute Force

- O brute force é aplicado para conseguir acesso a contas em determinado site, serviço, desktop ou servidor por meio de tentativas de login e senha, até que se escale os privilégios. A força bruta pode ser aplicada tanto manualmente quanto automaticamente, por meio de softwares.
- Vamos testar usando as ferramentas:
 - Hydra
 - xHydra
 - Cewl
 - Owasp ZAP

Módulo 4

Métodos de descubierta automática de vulnerabilidades



Ferramentas para descoberta automática de Vulnerabilidades

- OWASP ZAP
- Nikto
- WpScan
- Nessus
- Wapiti
- Parsero
- Dradis

Módulo 5

Métodos para proteção



OWASP e a Prevenção de Ataques

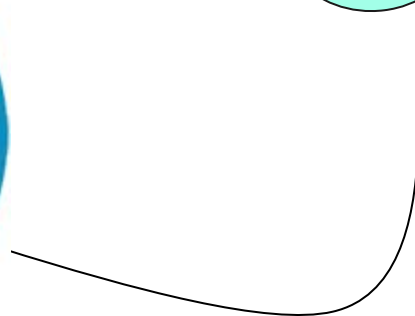
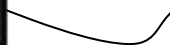
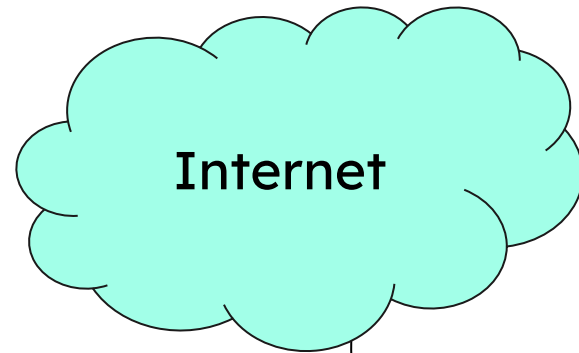
- Até aqui vimos vários ataques, sendo eles:
 - Injeção: SQL, Local File Inclusion, Remote File Inclusion, Command Injection, XSS
 - Quebra do sistema de Autenticação
 - Referência direta a objetos
 - Directory Traversal
 - File Upload
 - Configurações Falhas
 - Exposição de Dados Sensíveis
 - CSRF
 - Controle de Acesso quanto à função
 - Utilização de componentes vulneráveis
 - Manutenção do acesso
 - Negação de Serviço



OWASP e a Prevenção de Ataques

- Aprender a atacar é importante para entender como se defender!
- A OWASP apresenta várias dicas de defesa, todas disponíveis no site owasp.org
- Vejamos algumas soluções propostas para as vulnerabilidades que trabalhamos.

Proxy de Aplicação





Proxy de Aplicação

- Considere um Proxy de aplicação como uma elaborada versão de filtragem de pacotes.
- Muitas vezes é chamado de Proxy Reverso
- O Proxy de aplicação analisa todos os dados de aplicação de um pacote
- A filtragem de pacotes passa um pacote que foi permitido. O mesmo pacote viaja entre a internet e o computador da rede interna. Um proxy de aplicação gera novamente um pacote através de um pacote que foi permitido. Ele constrói um novo pacote e envia do firewall pro servidor da internet (ou pro computador remoto, dependendo do sentido).



Proxy de Aplicação

- As ferramentas mais populares são o Apache e Nginx
- Focaremos no Apache neste curso





Proxy de Aplicação

- O Modsecurity é um Firewall de Aplicação WEB (WAF, do inglês Web-based Firewall Application), que é considerado um kit de ferramentas para monitoramento, registro e controle de acesso de aplicações Web em tempo real.
- É open source e cross platform, podendo rodar em servidores APache, Nginx, IIS e outros...
Independente do Sistema Operacional
- É suportado pela equipe da SpiderLabs e da Trustwave, uma gigante do setor de cibersegurança no mundo.
- Por meio de regras este WAF consegue proteger as aplicações WEB de várias ameaças que estudamos.



Proxy de Aplicação

Contudo ele opera seguindo 4 princípios de orientação, que são:

- **Flexibilidade:** entregue pela poderosa linguagem baseada em regras do Modsecurity;
- **Passividade:** o Modsecurity não toma decisões por você, pois faz apenas o que você determina;
- **Previsibilidade:** o Modsecurity é previsível e te permite entender a ferramenta por completo, inclusive seus pontos fracos para que você possa contorná-los;
- **Qualidade acima de quantidade:** O Modsecurity possui uma quantidade de recursos limitada, mas que são frequentemente trabalhados e melhorados para funcionar da melhor maneira possível



Proxy de Aplicação

O Modsecurity protege as aplicações web através da sua poderosa linguagem baseada em regras. Estas podem ser adquiridas **gratuitamente no site da OWASP** ou de forma paga, com a SpiderLabs. Além disso o usuário também pode criar suas próprias regras, para suprir necessidades específicas.



Proxy de Aplicação - Instalação

Para fazer a instalação a partir do repositório git, basta utilizar os comandos:

```
$ git clone git://github.com/SpiderLabs/ModSecurity.git
$ cd ModSecurity
$ ./autogen.sh
$ ./configure
$ make
$ sudo make install
$ cp /usr/local/modsecurity/lib/mod_security2.so /usr/local/apache/modules/
```

Porém, não precisamos instalar, nosso servidor Web OWASP já possui o Mod Security instalado. Basta habilitarmos. Assim sendo, mãos a obra!



HTTPS

HTTPS é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

Vamos utilizar o WireShark e analisar um tráfego criptografado.



O que é um certificado SSL?

SSL significa Secure Sockets Layer, uma tecnologia global de segurança padrão que permite a comunicação criptografada entre um navegador da Internet e um servidor da web. É utilizado por milhões¹ de empresas on-line e indivíduos para reduzir o risco de roubo ou adulteração das informações confidenciais (ex.: números de cartões de crédito, nomes de usuário, senhas, e-mails, etc.) por hackers e ladrões de identidade. Na essência, o SSL permite uma "conversa" privada entre duas partes interessadas



Tipos de certificado SSL

- **Único:** protege um nome de domínio ou subdomínio totalmente qualificado
- **Curinga:** cobre um nome de domínio e um número ilimitado de subdomínios
- **Multidomínio:** protege vários nomes de domínio



Tipos de validação

- **Validação de domínio** – este nível é o menos caro e cobre criptografia básica e verificação da propriedade do registro de nome de domínio. Normalmente, é necessário esperar de alguns minutos até várias horas para receber esse tipo de certificado.
- **Validação da organização** – além da criptografia básica e da verificação da propriedade do registro de nome de domínio, alguns detalhes do proprietário (ex.: nome e endereço) são autenticados. Normalmente, é necessário esperar de algumas horas até vários dias para receber esse tipo de certificado.
- **Validação estendida (VE)** – este certificado oferece o maior nível de segurança devido à análise completa que é realizada antes de sua emissão (conforme especificado nas diretrizes estabelecidas pelo consórcio regulamentador do setor de certificados SSL). Além da propriedade do registro de nome de domínio e da autenticação da entidade, também são verificadas a existência jurídica, física e operacional da entidade. Normalmente, é necessário esperar de alguns dias até várias semanas para receber esse tipo de certificado.

Revisão - Comunicação TCP

TCP 3 way handshake (SYN, SYN ACK, ACK)

Client: HELLO

Server: ACK -- Server: Hello

Client: ACK

Server: x509 Certificate

Client: ACK

Shared Key Exchange - Encrypted Handshake

Application Data





Como configurar certificado SSL?

- Vamos configurar um certificado Auto Assinado.



Fontes importantes

- Existem alguns sites importantes na descoberta de vulnerabilidades, dentre eles:
 - <https://vulners.com/>
 - <https://www.zero-day.cz/database/>
 - <https://www.zerodayinitiative.com/advisories/published/>
 - <https://www.exploit-db.com/>



Defendendo-se no código

- Existem vários sites que ensinam boas práticas de desenvolvimento visando evitar invasões.
Dentre eles:
 - <https://developers.google.com>
 - <https://developer.mozilla.org>
 - <https://owasp.org>

Thanks!





Vamos manter contato!

Samuel Gonçalves Pereira



pereira.gsamuel@gmail.com



<https://www.linkedin.com/in/samuelgoncalvespereira/>



https://t.me/Samuel_gp