



OWASP

Open Web Application
Security Project

(IN)segurança  **3'**

Kembolle Amilkar de Oliveira

- * Cyber Security Evangelist :D
- * Leader Owasp Chapter Cuiabá - MT
- * Member FreeBSD Community
- * Member B.U. - Brazil Underground Community
- * CEO DarkPacket - Security Information Network's.

Skills

- Firewalls
- Reverse Engineering
- Ethical Hacking
- Intrusion Detection (HIDS / NIDS)
- Packet Analysis
- Penetration Tests
- Log Analysis
- Hardening Linux/Unix Systems
- Web Application Firewall
- Web Security
- Incident Response Security.



OWASP
Open Web Application
Security Project

Analista de Segurança da Informação

O que é um Analista de Segurança da Informação

O analista de segurança de informação - dentro do escopo profissional em Tecnologia da Informação (TI) - é o profissional responsável por analisar os **riscos corporativos relacionados à informação gerenciada por sistemas e infraestrutura de TI** e tomar medidas para proteger esta informação em critérios de confidencialidade, integridade e disponibilidade.



Principais Atividades do Analista de Segurança da Informação

- * Detecção de ameaças e vulnerabilidades em serviços de TI que comprometam a informação corporativa
- * Identificar e definir os objetivos de proteção à informação
- * Definição de políticas de segurança da informação (junto com as partes interessadas adequadas, tais como alta direção da empresa)
- * Implementação de normas e procedimentos aderentes à(s) política(s) de segurança
- * Auditoria e controle de processos para identificar se estão adequados às medidas e políticas de segurança da informação
- * Alinhamento das políticas de segurança para TI às políticas empresariais
- * Garantir a implementação de medidas que protejam a informação, minimizando os riscos de segurança a um nível aceitável
- * Definição, monitoramento e reporte de métricas de segurança da informação
- * Realizar testes de invasão.



CONNECT.

LEARN.

GROW.

CARGOS

Segurança da Informação



OWASP
Open Web Application
Security Project

Engenheiro-chefe de softwares de segurança

Desempenhar essa função exige fazer um pouco de tudo, desde a manutenção e implementação de programas de treinamento de funcionários até o desenvolvimento de aspectos relacionados à segurança de aplicativos.

Engenheiros-chefe de softwares de segurança devem possuir no mínimo um diploma em ciência da computação ou área similar, somado a especializações em segurança. Outros requisitos importantes são boa comunicação e trabalho em equipe.



Chief Security Officer

Entre suas atribuições, um CSO deve ser capaz de preparar contra-ataques para ameaças existentes e futuras, além de ser responsável por estabelecer e informar os funcionários a respeito de práticas melhores para a manutenção da segurança de uma organização. Fora isso, zela pelo monitoramento da eficiência das operações de segurança. Além da graduação em ciência da computação ou área similar, o cargo costuma exigir certificações adicionais.



Diretor de Segurança de Informações globais

O posto demanda a manutenção e execução de projetos de segurança de informação e a coordenação da resposta em caso de ataque. Também pode ser exigido do profissional um conhecimento prático das regras específicas do setor (como HIPAA em Saúde ou FISMA na indústria financeira) – além da formação em ciência da computação e especialização em segurança.



Consultor de Segurança

Este profissional trabalha com os clientes no desenvolvimento de estratégias para uma cibersegurança mais efetiva em toda a empresa.

Além de ter conhecimento de práticas e procedimentos recomendados, ele também deve possuir habilidades em comunicação, negociação e gerenciamento de projetos.

As empresas buscam consultores com muitos anos de experiência, fora o conhecimento prático das regras da indústria e de fornecedores e produtos de segurança.



Chief Information Security Officer

O papel do CISO é semelhante ao do CSO, mas foca com maior intensidade na proteção de dados e propriedade intelectual de uma empresa – os chamados “ativos de informação”.

Outras responsabilidades comuns são a manutenção de práticas apropriadas e a projeção de políticas efetivas para lidar com violações e outros desastres.



Chefe de Cibersegurança

O cargo é especialmente exigente, enfrentando grande pressão: é responsável por analisar a companhia em busca de possíveis vulnerabilidades, detectando ataques futuros e informando a gerência.



Engenheiro-Chefe de Segurança

Suas responsabilidades dependem da empresa, mas costumam envolver a proteção de ambientes operativos, sistemas de telefonia e vídeo, além de software, hardware e informação (armazenados em trânsito).

Outro dever comum é a revisão de códigos e procedimentos para detectar vulnerabilidades, conscientizando os funcionários e implementando ferramentas de segurança para proteger a empresa.



Engenheiro de Cibersegurança

Costuma ter experiência em testes de penetração e outras ferramentas de cibersegurança, usando-as para manter a empresa segura contra ameaças internas e externas.

Além de formação em ciência da computação, especialização em segurança e experiência prática na área são exigidas.



Gerente de Segurança de Aplicações

É responsável por garantir que todas as aplicações produzidas ou usadas pela empresa respondem a um padrão mínimo de segurança e privacidade.

O cargo costuma responder diretamente ao diretor de segurança ou posição equivalente.



CONNECT.

LEARN.

GROW.

Melhores praticas em Segurança da Informação.



OWASP
Open Web Application
Security Project



OWASP

The Open Web Application Security Project

A Open Web Application Security Project (OWASP) é uma entidade sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança de softwares aplicativos reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da internet.

Os estudos e documentos da OWASP são disponibilizadas para toda a comunidade internacional, e adotados como referência por entidades como U.S. Defense Information Systems Agency (DISA), U.S. Federal Trade Commission, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo PCI Council.



OWASP
Open Web Application
Security Project

OWASP TOP 10

O OWASP Top 10 é um poderoso documento de conscientização para a segurança das aplicações web. O OWASP Top 10 representa um amplo consenso sobre o que são as falhas de segurança de aplicativos web mais importantes.

Os membros do projeto incluem uma variedade de especialistas em segurança de todo o mundo que compartilharam seus conhecimentos para produzir essa lista.

Incentivamos todas as empresas a adotar este documento de conscientização dentro de sua organização e iniciar o processo para garantir que suas aplicações web não contenham essas falhas.

Adotar o OWASP Top 10 é talvez o primeiro passo mais eficaz para mudar a cultura de desenvolvimento de software dentro de sua organização produzindo um código seguro.

FAILED OWASP TOP 10

How many apps fail the OWASP Top 10 upon initial risk assessment?



The data represents 208,670 application assessments submitted for analysis during the 18-month period from October 1, 2013 through March 31, 2015 by large and small companies, commercial software suppliers, open source projects and software outsourcers.

VERACODE

Fonte: <https://www.veracode.com/directory/owasp-top-10>



OWASP
Open Web Application
Security Project

OWASP Top 10

As 10 principais vulnerabilidades do OWASP são:

- 1- Injeção
- 2- Autenticação Quebrada
- 3- Exposição a dados sensíveis
- 4- XML External Entities (XXE)
- 5- Controle de acesso quebrado
- 6- Erros de segurança
- 7- Cross Site Scripting (XSS)
- 8- Desserialização Insegura
- 9- Usando componentes com vulnerabilidades conhecidas
- 10- Registro e monitoramento insuficientes



OWASP Project

OWASP Project Inventory

Todas as ferramentas OWASP, documentos e projetos de biblioteca de códigos são organizados nas seguintes categorias:

Projetos Flagship: A designação de OWASP Flagship é dada a projetos que demonstraram valor estratégico para o OWASP e a segurança de aplicativos como um todo.

Projetos de Laboratório: Os projetos do OWASP Labs representam projetos que produziram uma entrega de valor revisada pelo OWASP.

Projetos da Incubadora: Os projetos da OWASP Incubadora representam o playground experimental onde os projetos ainda estão sendo desenvolvidos, as ideias ainda estão sendo provadas e o desenvolvimento ainda está em andamento.



OWASP
Open Web Application
Security Project

HOW TO START AN OWASP PROJECT

with 9 basic steps for code & tool projects



Have a clear mission statement



Create a Roadmap



Choose an open source license



Look for Contributors



Configure an Open Source Repository



Setup a mailing list



Work on your first Alpha release



Promote your project



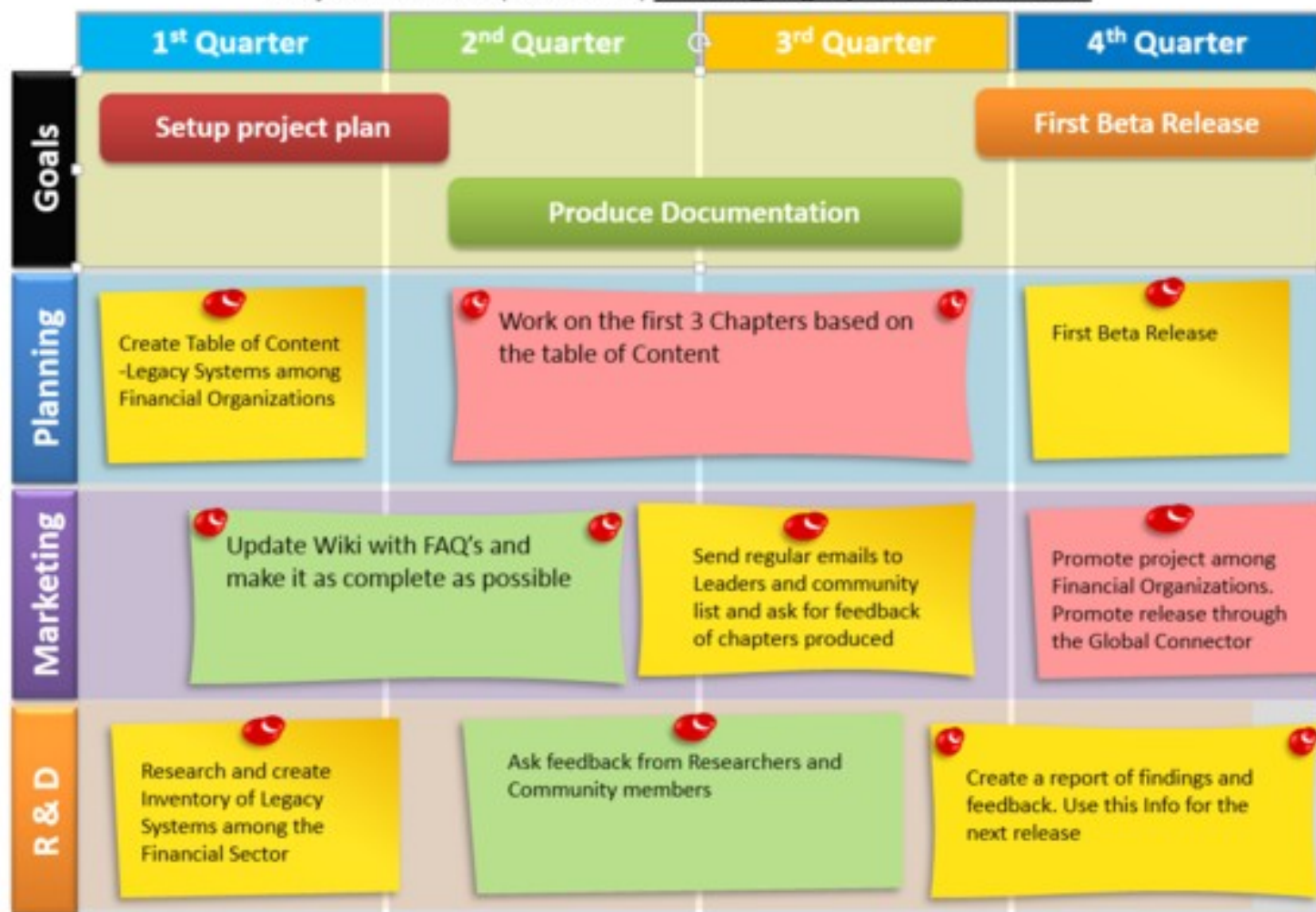
Don't give up



OWASP
Open Web Application
Security Project

Agile Roadmap

Project Incubator (Document) Securing Legacy Web applications



OWASP
Open Web Application
Security Project

OWASP

FLAGSHIP

mature projects

A designação OWASP Flagship é dada a projetos que demonstraram valor estratégico ao OWASP e à segurança de aplicativos como um todo.

Tools

OWASP Zed Attack Proxy
OWASP Web Testing Environment Project
OWASP OWTF
OWASP Dependency Check
OWASP Security Shepherd
OWASP DefectDojo Project
OWASP Juice Shop Project
OWASP Security Knowledge Framework
OWASP Dependency Track Project

Code [Health Check January 2017]

OWASP ModSecurity Core Rule Set Project
OWASP CSRFGuard Project

Documentation

OWASP Application Security Verification Standard Project
OWASP Software Assurance Maturity Model (SAMM)
OWASP AppSensor Project
OWASP Top Ten Project
OWASP Testing Project
OWASP Cheat Sheet Series
OWASP Mobile Security Testing Guide



OWASP
Open Web Application
Security Project



Os projetos do OWASP Labs representam projetos que produziram uma entrega de valor. Embora esses projetos normalmente não estejam prontos para produção, a comunidade OWASP espera que um líder de projeto do OWASP Labs esteja produzindo lançamentos que estejam pelo menos prontos para o uso principal.

<p>Tools</p> <ul style="list-style-type: none"> O-Saft OWASP EnDe Project OWASP Mobile Security Project OWASP O2 Platform OWASP Passfault OWASP WebGoat Project OWASP Xenotix XSS Exploit Framework OWASP Code Pulse Project OWASP SeraphimDroid Project OWASP Glue Tool Project OWASP Amass Project 	<p>Documentation [Health Check January 2017]</p> <ul style="list-style-type: none"> OWASP Code Review Guide Project OWASP Cornucopia OWASP Podcast Project OWASP Proactive Controls OWASP Internet of Things Top Ten Project OWASP Top 10 Privacy Risks Project OWASP Snakes and Ladders Project OWASP Automated Threats to Web Applications 	<p>Contests - Health Check February 2016</p> <ul style="list-style-type: none"> OWASP University Challenge OWASP CTF Project <p>Code</p> <ul style="list-style-type: none"> OWASP Enterprise Security APIT OWASP Security Logging Project OWASP Benchmark
---	--	--



A etiqueta "Incubadora OWASP" permite que os consumidores OWASP identifiquem prontamente a maturidade de um projeto. O rótulo também permite que os líderes de projeto aproveitem o nome OWASP enquanto seu projeto ainda está amadurecendo.

Code
OWASP Java Encoder Project
Thumbsup.png
OWASP Java HTML Sanitizer
Project Thumbsup.png
OWASP Node.js Goat Project
Thumbsup.png
OWASP Mth3l3m3nt Framework
ProjectThumbsup.png
OWASP CSRFProtector Project
OWASP WebGoat PHP
ProjectThumbsup.png
OWASP Secure Headers Project
OWASP Vicnum
ProjctThumbsup.png
OWASP DeepViolet
TLS/SSL_ScannerThumbsup.png
OWASP Off the record 4 Java
ProjectThumbsup.png
OWASP Learning Gateway Project
OWASP SonarQube Project
OWASP Zenzengorri Code Project
OWASP Find Security Bugs
OWASP Vulnerable Web
Application
OWASP Samurai WTF

Code
OWASP Java Encoder Project
Thumbsup.png
OWASP Java HTML Sanitizer
Project Thumbsup.png
OWASP Node.js Goat Project
Thumbsup.png
OWASP Mth3l3m3nt Framework
ProjectThumbsup.png
OWASP CSRFProtector Project
OWASP WebGoat PHP
ProjectThumbsup.png
OWASP Secure Headers Project
OWASP Vicnum
ProjctThumbsup.png
OWASP DeepViolet
TLS/SSL_ScannerThumbsup.png
OWASP Off the record 4 Java
ProjectThumbsup.png
OWASP Learning Gateway Project
OWASP SonarQube Project
OWASP Zenzengorri Code Project
OWASP Find Security Bugs
OWASP Vulnerable Web
Application
OWASP Samurai WTF

Research
Tools
OWASP Threat
DragonThumbsup.png
OWASP Mutillidae 2 Project
OWASP Pyttacker
ProjectThumbsup.png
OWASP ZSC Tool Project
Thumbsup.png
OWASP Basic Expression Lexicon
Variation Algorithms (Belva)
Project]Thumbsup.png
OWASP VBScanThumbsup.png
OWASP Appsec
PipelineThumbsup.png
OWASP Bug Logging
ToolThumbsup.png
OWASP iGoat Tool Project
OWASP Risk Rating Management
OWASP DevSlop Project
OWASP SecurityRAT Project
OWASP SecureTea Project

Documentation
OWASP Vulnerable Web
Applications Directory
ProjectThumbsup.png
OWASP .NET Project
OWASP Incident Response
Project
OWSP_Application_Security_Program_Quick_Start_Guide_Project
OWASP SecLists Project
OWASP Knowledge Based
Authentication Performance
Metrics ProjectThumbsup.png
OWASP RFP Criteria
OWASP Web Mapper

CONNECT.

LEARN.

GROW.

Principais Projetos OWASP



OWASP
Open Web Application
Security Project

Top 10 Controles Preventivos

O **OWASP Top 10 Controles Preventivos** é uma lista de técnicas de segurança que devem ser incluídos em cada projeto de desenvolvimento de software.

Eles são ordenados por ordem de importância, sendo o primeiro o mais importante.

- 1- Verificar a segurança cedo e frequentemente;
- 2- Parametrizar consultas;
- 3- Codificar dados;
- 4- Validar todas as entradas;
- 5- Implementar controles de identidade e autenticação;
- 6- Implementar controles de acesso;
- 7- Proteger os dados;
- 8- Implementar LOG e detecção de intrusão;
- 9- Aproveitar as estruturas de segurança e bibliotecas;
- 10- Erros e Manipulação de exceções.



Modelagem Segura de Software



OWASP Secure Coding Practices

Práticas de Programação Segura no Desenvolvimento de Softwares

CONNECT

LEARN

GROW

O objetivo da segurança em aplicações é manter a confidencialidade, integridade e disponibilidade dos recursos de informação a fim de permitir que as operações de negócios sejam bem sucedidas e esse objetivo é alcançado através da implementação de controles de segurança.

Este guia concentra-se nos controles técnicos, específicos para mitigar as ocorrências das vulnerabilidades mais comuns no software e como o foco principal são as aplicações Web e a infraestrutura de apoio, boa parte desse documento pode ser usada para qualquer plataforma de desenvolvimento de software.



OWASP
Open Web Application
Security Project

Software Assurance Maturity Model

O SAMM é um framework aberto para ajudar as organizações a formular e implementar uma estratégia para a segurança de software.

O Open SAMM foi projetado para ser bem flexível assim podendo ser utilizado em pequenas, médias e grandes empresas e utilizando qualquer estilo de desenvolvimento, podendo ser aplicado para projetos individuais ou para toda uma organização.

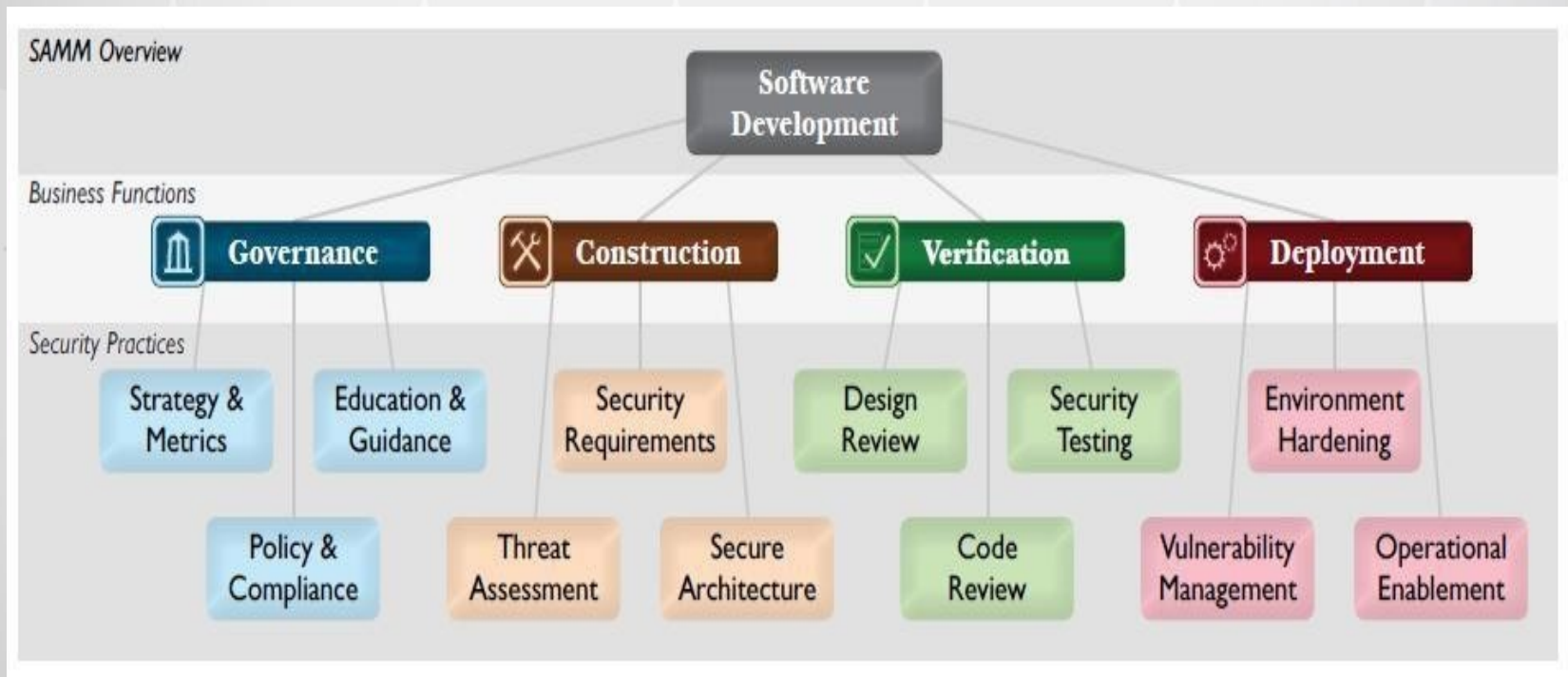
Ele possui recursos que o ajudarão em:

Avaliar as práticas de segurança da organização
Elaborar um programa de segurança de software balanceado
Definir e medir atividades relacionadas a segurança na organização



Software Assurance Maturity Model

O Open SAMM especifica quatro funções de negócios críticos, cada um com três práticas de segurança, são elas:



Software Assurance Maturity Model

Governança

São as atividades da gerência, que seria examinar os grupos de desenvolvimento e também gerenciar os níveis dos negócios estabelecidos pela empresa.

Estratégia e Métricas: Definição da estratégia que será utilizada para a garantia de software ou seja criar definições de metas de segurança e também estudar os riscos da empresa.

Políticas e Conformidade: Entender as diretrizes/políticas e regulamentá-las nos padrões de segurança, também fazer auditorias para descobrir se algum projeto não está dentro das expectativas.

Orientação e Educação: Ensinar as pessoas que estão envolvidas no desenvolvimento do software como desenvolver e implementar um software mais seguro, o OpenSAMM também indica que uma boa alternativa para melhorar o desempenho é através de objetivos para cada funcionário.



Software Assurance Maturity Model

Construção

Definir metas e criar os software dentro dos padrões. Isso inclui o gerenciamento do produto, a especificação do nível da arquitetura, design e implementação.

Modelagem de Ameaças: Identificar e entender os níveis de risco na funcionalidade do software no ambiente em que ele será executado, a partir dos detalhes conseguidos ficara mais fácil tomar decisões.

Requisitos de Segurança: Definir qual será o comportamento esperado a respeito da segurança do software, definindo cada processo por níveis e fazer auditorias para garantir que todas as especificações de segurança estão sendo utilizadas.

Arquitetura Segura: Projetar softwares seguros por padrões, reutilizando os componentes assim os riscos de segurança do software serão drasticamente reduzidos.



Software Assurance Maturity Model

Verificação

Verificações e testes nos produtos durante o desenvolvimento do software, garantindo uma boa qualidade do software.

Revisão de Arquitetura: Avaliar a segurança da arquitetura do software, permitindo assim detectar problemas logo no início. Quando se resolve o problema no início se reduz também o tempo e dinheiro que seria gasto a procura desse problema.

Revisão de Código: Inspeccionar os códigos fontes a fim de encontrar potenciais falhas no software que ocorreu no desenvolvimento. O Code Review seria uma revisão mais profunda já que na hora do desenvolvimento também acontece algumas revisões, outra função é estabelecer uma base para uma codificação mais segura.

Testes de Segurança: Testar o software a procura de vulnerabilidades, para garantir que os resultados serão os esperados quando estiver em execução, basicamente seria a fase de teste a procura de qualquer tipo de erro.



Software Assurance Maturity Model Implantação

São as atividades da gerência, que seria examinar os grupos de desenvolvimento e também gerenciar os níveis dos negócios estabelecidos pela empresa.

· **Estratégia e Métricas:** Definição da estratégia que será utilizada para a garantia de software ou seja criar definições de metas de segurança e também estudar os riscos da empresa.

→ **Políticas e Conformidade:** Entender as diretrizes/políticas e regulamentá-las nos padrões de seguranças, também fazer auditorias para descobrir se algum projeto não está dentro das expectativas.

Orientação e Educação: Ensinar as pessoas que estão envolvidas no desenvolvimento do software como desenvolver e implementar um software mais seguro, o OpenSAMM também indica que uma boa alternativa para melhorar o desempenho é através de objetivos para cada funcionário.



Software Assurance Maturity Model

Comparação entre SAMM e a ISO / IEC 27034

A ISO/IEC 27034[2] é um padrão internacional para ajudar as organizações a implementar mecanismos de segurança durante todo o ciclo de vida do seu desenvolvimento.

A tabela mostra o relacionamento dos recursos do SDL (Secure Development Lifecycle) com as 12 práticas de segurança do OpenSAMM.

O losango grande indica um forte relacionamento com um tópico da ISO/IEC 27034 enquanto o losango pequeno indica um fraco relacionamento:

		ISO/IEC 27034						
		Normative Framework					Application Security Risk Assessment	Application Security Audit
		Business context	Regulatory context	Technological context	Application specifications repository	Application security control library	Life cycle reference model	Provisioning and Operating the Application
Open Software Assurance Maturity Model								
Function	Security Practice							
Governance	Strategy & Metrics	♦					♦	♦
	Policy & Compliance	♦	♦			♦		♦
	Education & Guidance			♦	♦	♦		
Construction	Threat Assessment				♦	♦	♦	
	Security Requirements				♦	♦		♦
	Secure Architecture			♦	♦	♦		♦
Verification	Design Review					♦		♦
	Code Review					♦		♦
	Security Testing					♦		♦
Deployment	Vulnerability Management			♦		♦		♦
	Environment Hardening					♦		♦
	Operational Enablement				♦	♦		♦



Conheça outros projetos top 10 em Infosec da OWASP

- 1- OWASP Internet of Things Top Ten Project
- 2- OWASP Top 10 Privacy Risks Project
- 3- OWASP Top 10 Machine Learning Risks
- 4- OWASP Serverless Top 10 Project
- 5- OWASP Cloud-Native Application Security Top 10
- 6- OWASP Docker Top 10
- 7- OWASP Top 10 Card Game
- 8- OWASP Top 10 Mobile Risks

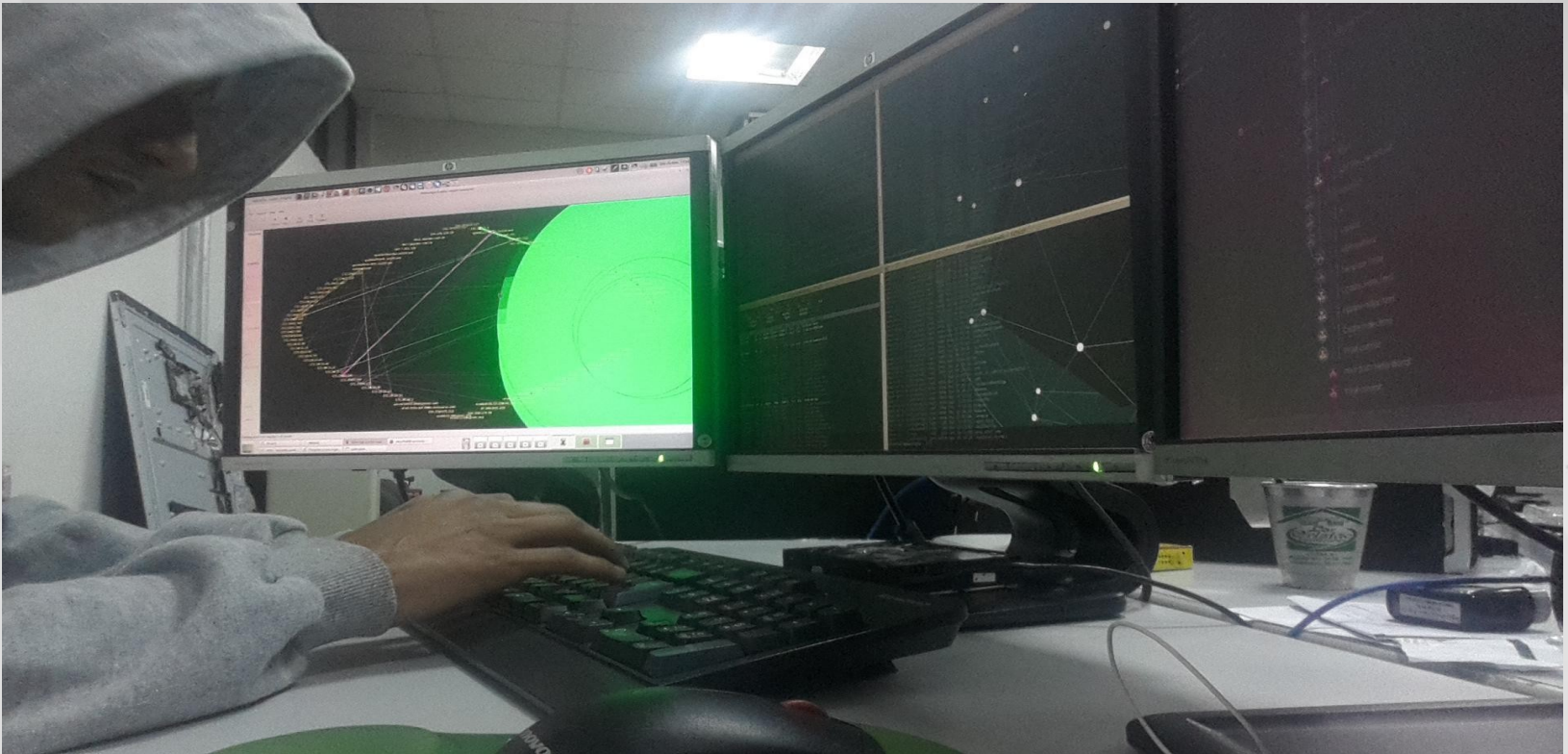
.... e vários outros.

Happy Hacking Modafokers! ♥³ '



OWASP
Open Web Application
Security Project

Insecure Network's



" A atitude é nobre, mas o chapéu sempre será NEGRO" - ♥³ '



OWASP
Open Web Application
Security Project

Insecure Network's

O que é modelo O.S.I. ?

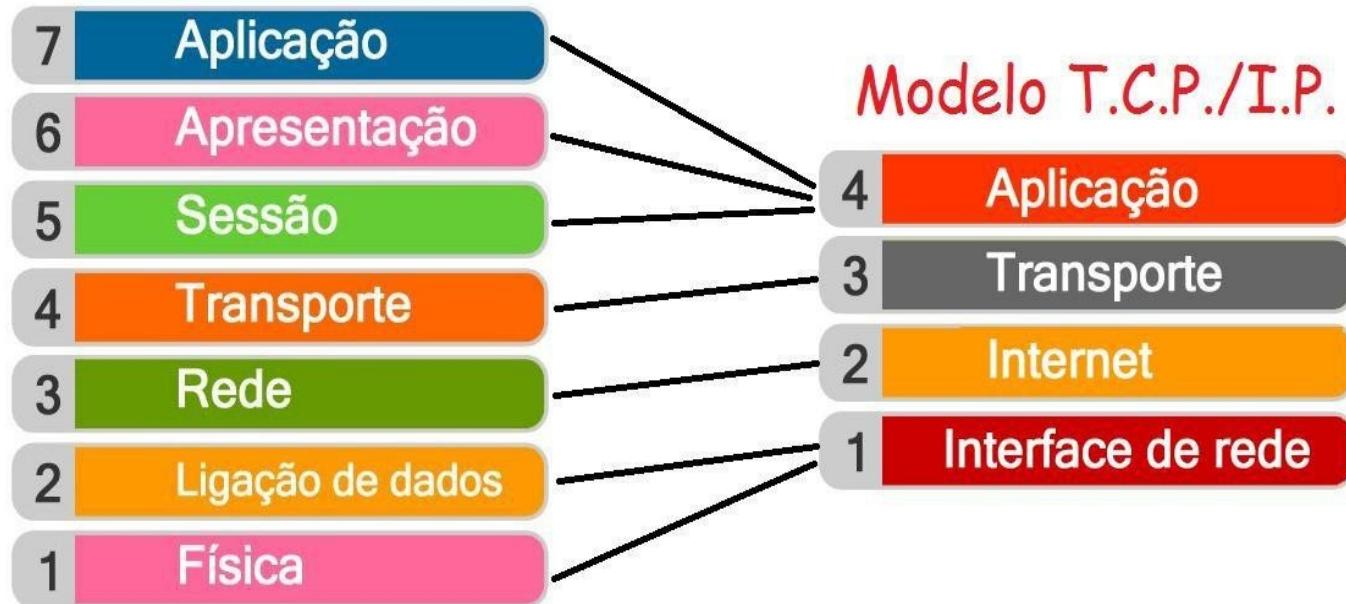
Modelo de referência da ISO, tem como principal objetivo ser um modelo padrão para protocolos de comunicação entre diversos tipos de sistema, garantindo a comunicação end-to-end, o Modelo OSI (em inglês Open Systems Interconnection) foi lançado em 1984 pela Organização Internacional para a Normalização (em inglês International Organization for Standardization).



Insecure Network's

Exploração Camada OSI

Modelo O.S.I.



Insecure Network's

7-Aplicação

Interfaces com aplicativos

6-Apresentação

Formatos / Criptografia

5-Sessão

Controle de Sessões entre Aplicativos

4-Transporte

Conexão entre hosts / Portas

3-Rede

Endereço lógico / Roteadores

2-Enlace de Dados

Endereço físico / Pontes e Switches

1-Física

Hardware / Sinal elétrico / bits



Insecure Network's

Byte = 8 bits

Faixa de valores em diferentes representações:

- Binário: 00000000_2 - 11111111_2
- Decimal: 0_{10} - 255_{10}
- Hexadecimal 00_{16} - FF_{16}

- Representação na base 16
- Dígitos são '0' - '9' e 'A' - 'F'
- Escreva $FA1D37B_{16}$ em C como $0xFA1D37B$ ou $0xfa1d37b$

Hex	Decimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

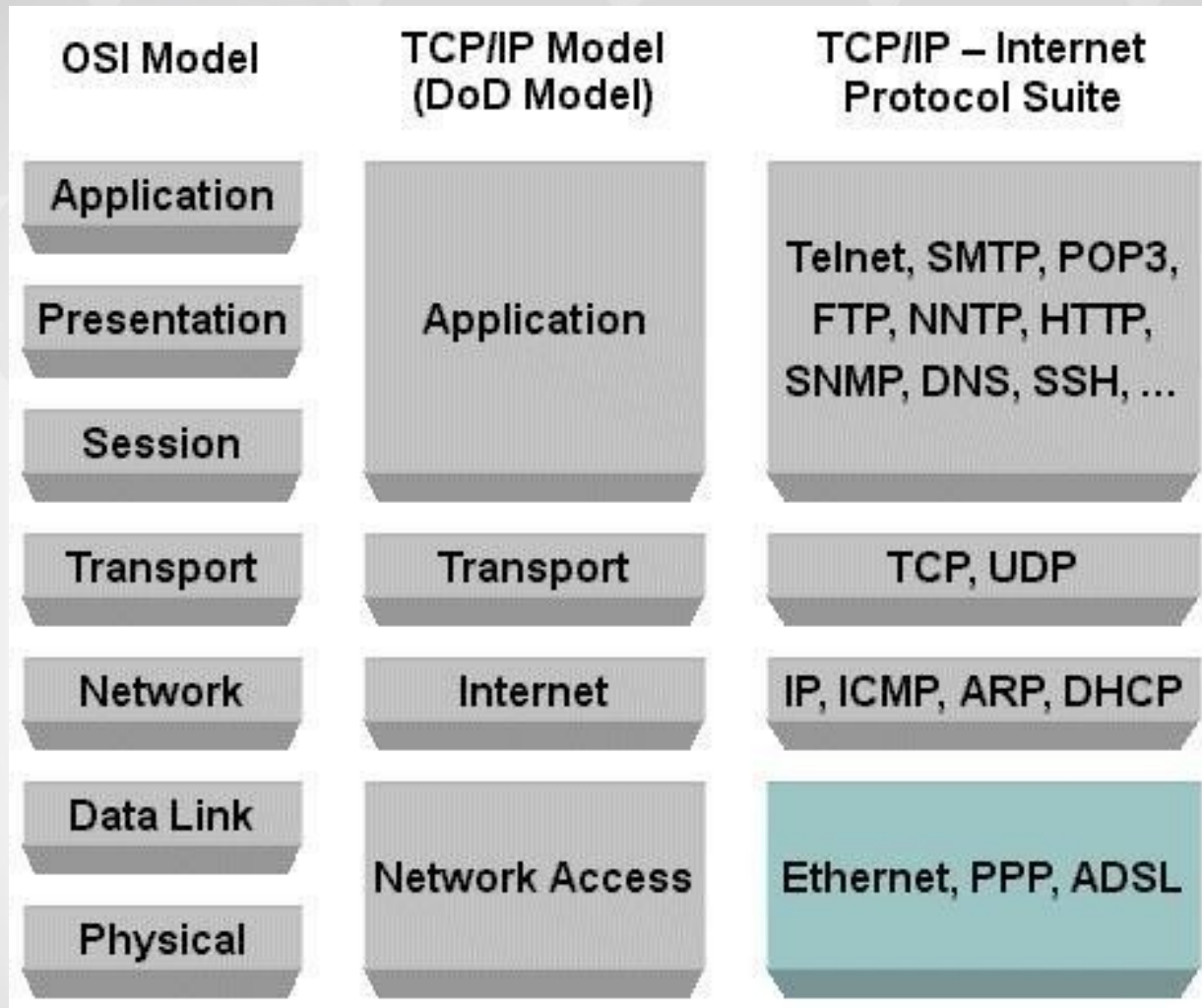


Insecure Network's

Símbolo	Tamanho	Comentários
Bit (b)	1	$2^0 = 1$. Menor unidade de informação: vale 0 ou 1.
Byte (B)	8 bits	$2^3 = 8$. Por convenção, e por ser potência de 2
Kilo (K)	1024 Bytes	$2^{10} = 1.024$
Mega (M)	1024 Kilo	$2^{20} = 1.048.576$
Giga (G)	1024 Mega	$2^{30} = 1.073.741.824$. Unidade dos HDs atuais
Tera (T)	1024 Giga	$2^{40} = 1.099.511.627.776$
Peta (P)	1024 Tera	$2^{50} = 1.125.899.906.842.624$
Exa (E)	1024 Peta	2^{60} . Talvez seja para os seus netos ☺
Zetta (Z)	1024 Exa	2^{70} . O que? Como ?
Yotta (Y)	1024 Zetta	2^{80} . Tu tá de brincadeira, né?



Insecure Network's



Insecure Network's

CAMADA 1 - Física

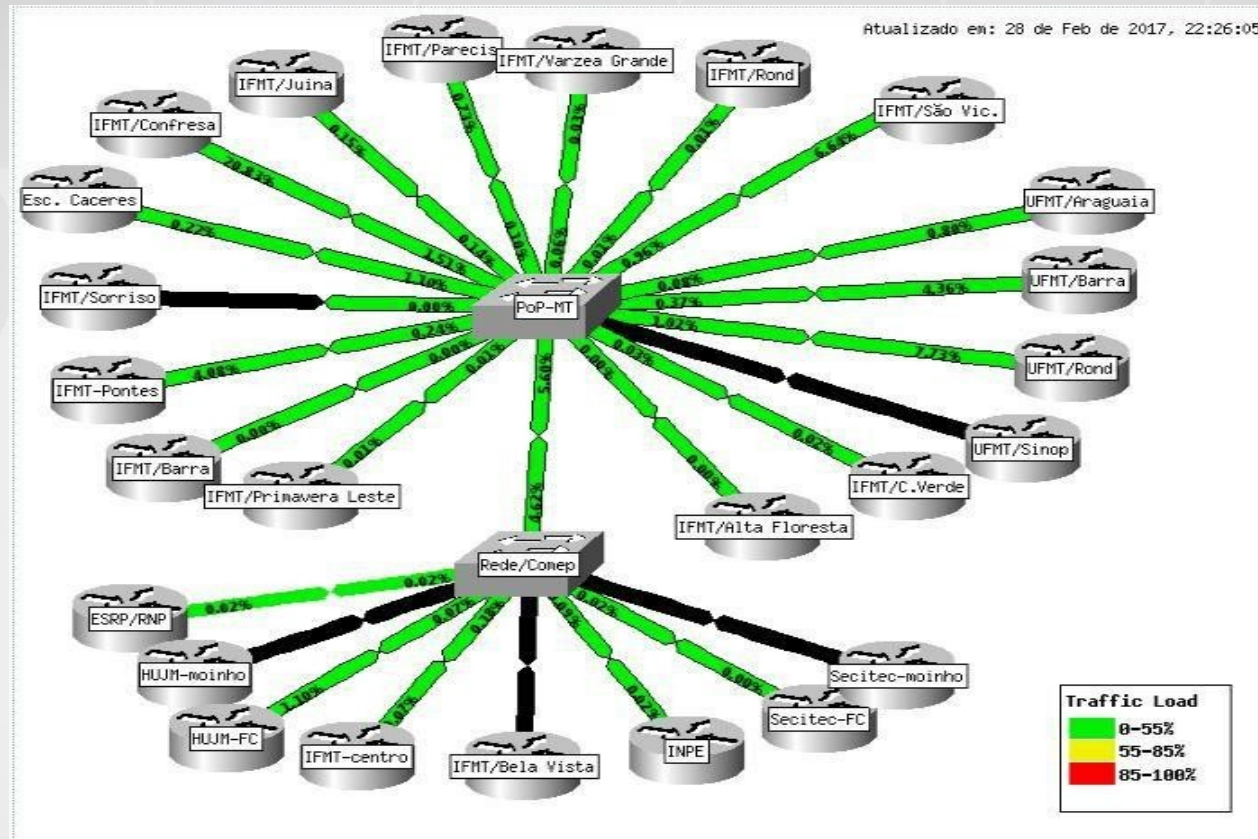
É extremamente importante que os administradores de rede conheçam como estão organizadas as ligações elétricas, para estabelecer uma estratégia que possa minimizar os efeitos de um possível ataque de camada física. Os principais tipos de ataques nessa camada são:

- * **Cortes de cabos e fibras;**
- * Fontes eletromagnéticas próximo de cabos de cobre;
- * Alta tensão aplicada em redes elétricas;
- * Interferências em redes sem fio.



Insecure Network's

Cortes de cabos e fibras



Fonte: POP- MT - Ponto de Presença Rede Nacional de Pesquisa
- MTwebsite: www.pop-mt.rnp.br/site/?page_id=44

Insecure Network's

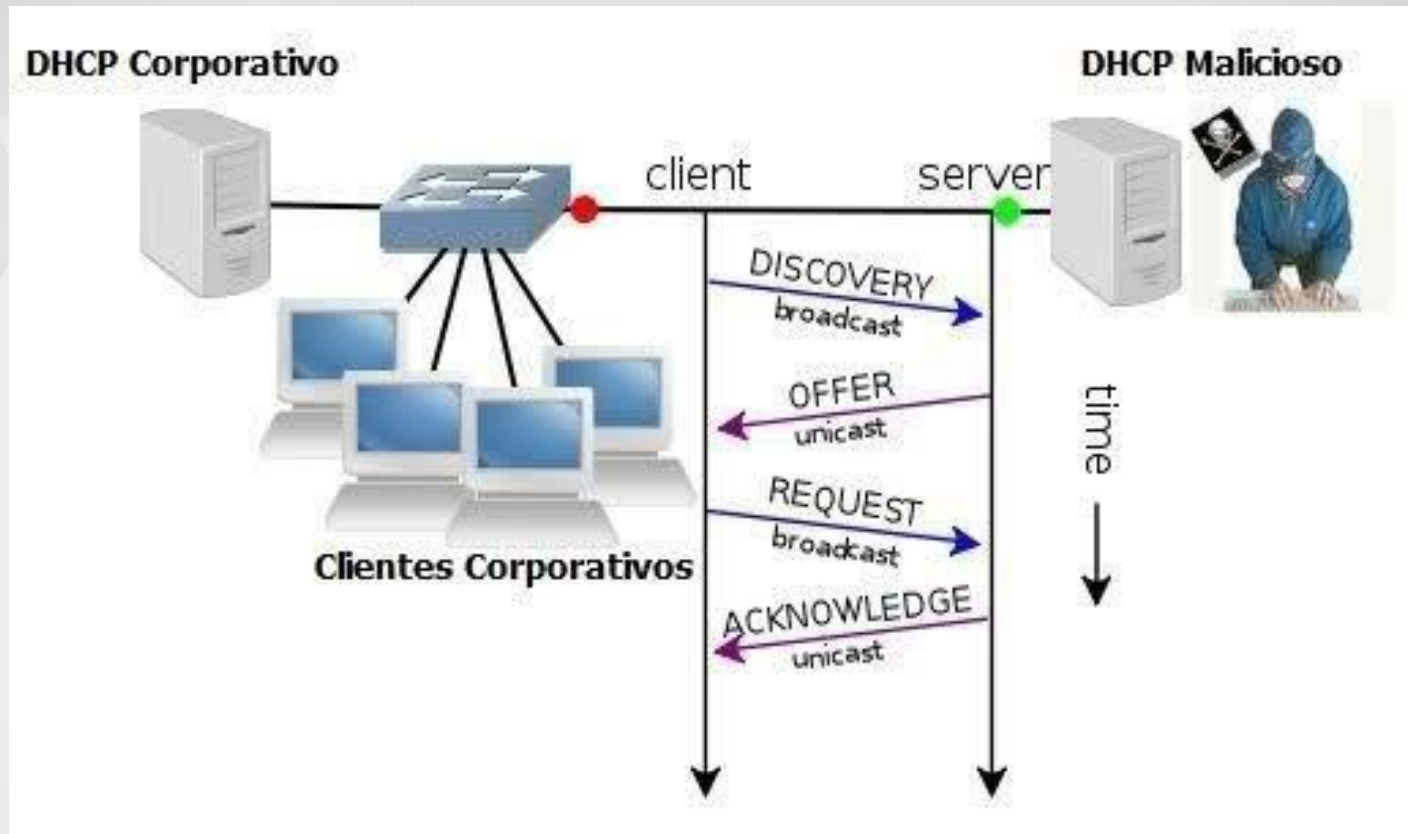
CAMADA 2 - Enlace

É na camada de enlace que são definidos os links de dados, e é onde encontramos protocolos e tecnologias como o ATM, Frame Relay, PPP, Ethernet, Wirelles LAN (802.11a/b/g), entre outros.

- * Ataques MAC
- * **Ataques DHCP**
- * **Ataques ARP**
- * Ataques STP e VLANs



Insecure Network's



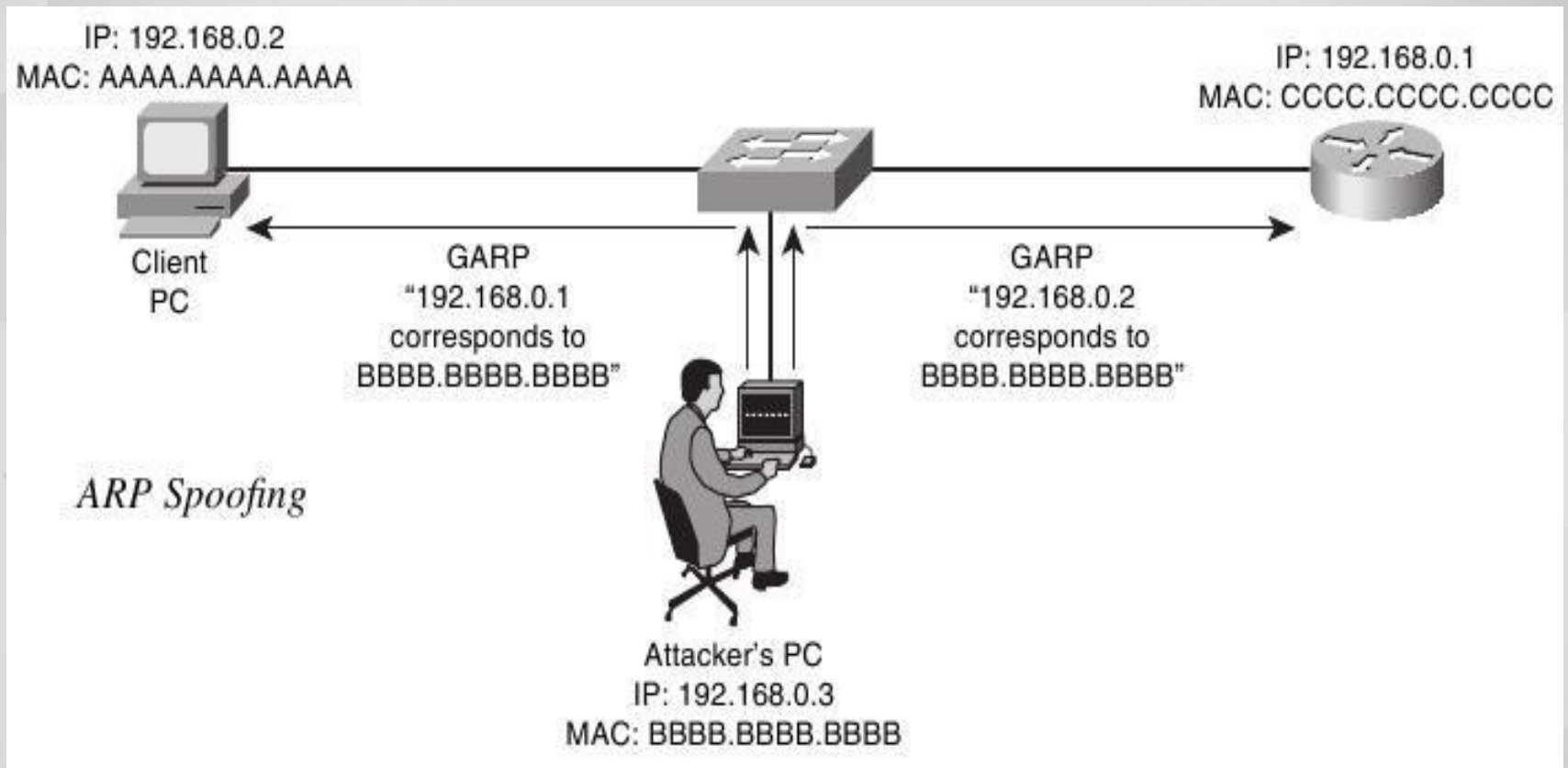
Dhcparpd

<http://research.wand.net.nz/software/dhcparpd.php>



OWASP
Open Web Application
Security Project

Insecure Network's



Ettercap: <https://ettercap.github.io/ettercap/>



OWASP
Open Web Application
Security Project

Insecure Network's

CAMADA 3 - Rede

Nesta camada encontramos o Internet Protocol (IP) com o ICMP sendo uma parte do IP. O IP é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento de dados, e oferece um serviço de datagramas não confiável (também chamado de melhor esforço), ou seja, o pacote vem quase sem garantias podendo chegar desordenado ou duplicado, ou simplesmente perdido por inteiro.

*** Sniffing de pacotes**

* IP Spoofing

* Ataques ICMP



Insecure Network's Sniffing de Pacotes



wireshark <https://www.wireshark.org>



OWASP
Open Web Application
Security Project

Insecure Network's

CAMADA 4 - Transporte

A camada de transporte é onde podemos encontrar os protocolos TCP e UDP. O protocolo TCP é o mais complexo por ser dotado de um mecanismo de controle de fluxo e ser orientado a conexão, enquanto o UDP é simples por não conter o controle de fluxo e não necessitar de conexão. Como em outras camadas, existe uma série de ataques envolvendo a manipulação das vulnerabilidades desses protocolos, os quais serão abordados adiante.

- * Ataques TCP
- * Ataques UDP
- * **Ataques de TCP e UDP Port Scan**



Insecure Network's

Ataques de TCP e UDP Port Scan



Network Mapper: <https://nmap.org>



OWASP
Open Web Application
Security Project

Insecure Network's

CAMADA 5,6,7 - Aplicação

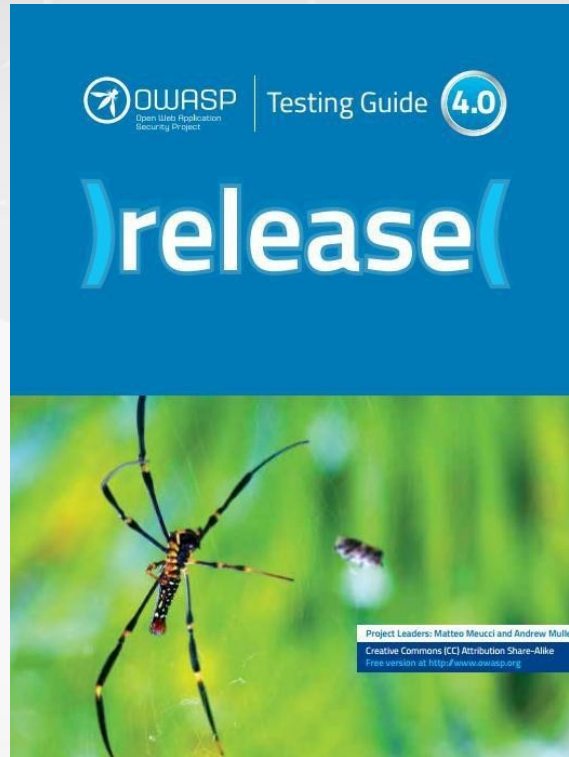
Camada de aplicação da arquitetura TCP/IP, nela é possível encontrar uma série de falhas, das quais serão apresentadas as principais. Seguem abaixo algumas delas.

- * Ataques ao Domain Name System (DNS);
- * **Ataques ao Web Server;**
- * Ataques aos Sistemas de Controle de Versão;
- * Ataques ao Mail Transport Agents (MTA);
- * Ataques ao Simple Network Management Protocol (SNMP);
- * Ataques ao Open Secure Sockets Layer (OpenSSL);



Insecure Network's

Ataques ao Web Server e Aplicações Web (Ensaios de Intrusão)



OWASP Testing Guide v4

www.owasp.org/images/1/19/OTGv4.pdf



OWASP
Open Web Application
Security Project

Insecure Network's

Para encontrar alvos na internet atacantes buscam primeiramente pelos segmentos de ip's dos seus próprios provedores, acesse meuip.com.br e teremos o seguinte:
191.250.xx.xx.dynamic.adsl.gvt.net.br mas e as portas?



OWASP
Open Web Application
Security Project

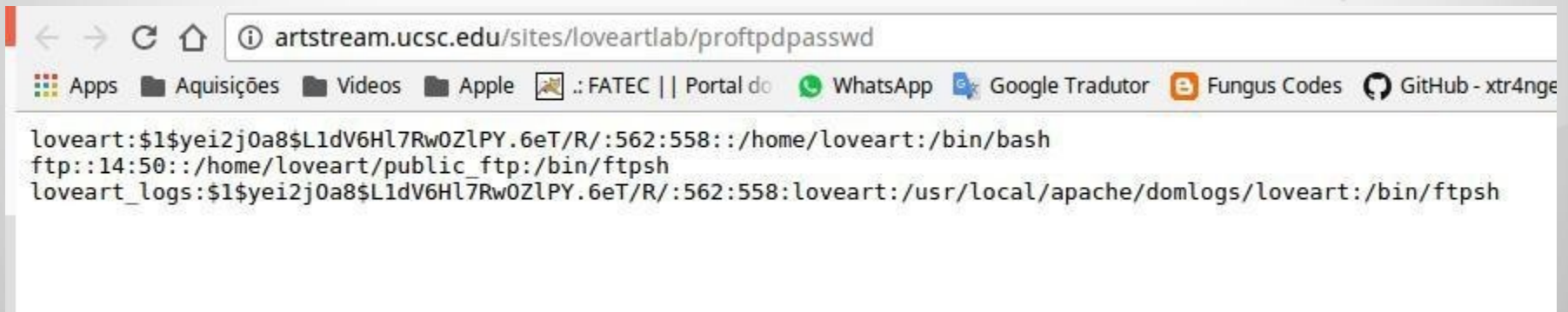
Insecure Network's

OK..

**portas mais exploradas no mundo, metodo
"noob" Google Dork.**

*Porta 21 FTP - Transferencia de arquivos.
Evasão: **inurl:proftpdpasswd**

```
loveart:$1$yei2jOa8$L1dV6Hl7RwOZIPY.6eT/R/:562:558::/home/loveart:/bin/b ash ftp::14:50::/home/loveart/public_ftp:/bin/ftpsh loveart_logs:$1$yei2jOa8$L1dV6Hl7RwOZIPY.6eT/R/:562:558:loveart:/usr/local/apache/domlogs/loveart:/bin/ftpsh
```

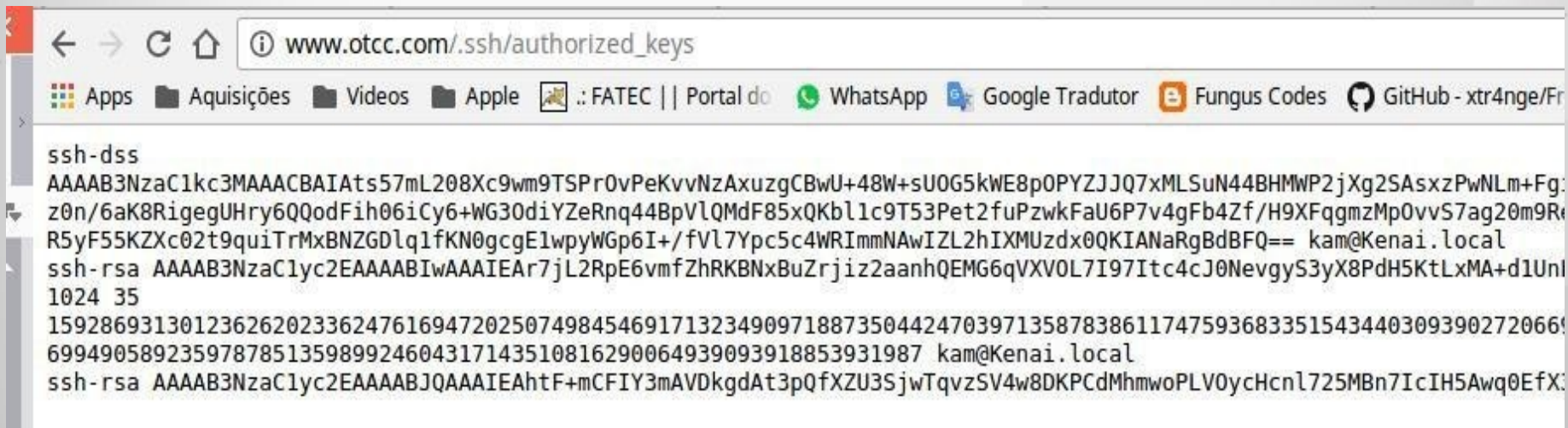


Insecure Network's

* Porta 22 Secure Shell (SSH) forwarding

Evasão: **inurl:.ssh intitle:index.of authorized_keys**

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAIAts57mL208Xc9wm9TSPrOvPeKvvNzAxuzgCBwU+48W+sUOG5kWE8pOPYZJJQ7xMLSuN44BHMWP2j
X
g 2SAsxzPwNLm+FgiX83f4qW/vhE6III/y5VjV/Jcpd2n/w08cX1jRZnqraip2Ujxx56DT86GJezmvdrBG9hmluJcmftLBAAAFQDLUavNK5zu
+tIRi9
xYkwokcA3uQAAAIb5Sdzkr2nWbzIz0n/6aK8RigegUHry6QQodFih06iCy6+WG3OdiYZeRnq44BpVIQMdF85xQKbl1c9T53Pet2fuPzwk
F aU 6P7v4gFb4Zf/H9XFqgmzMpOvvS7ag20m9RevyzobStv2hh9gjif1wS8oMW9Mtl7YtEwjfp7pnN1BcjwAAAIAbKyqmNpqzHSMfO/
+fl/r7T Dp2Bc mzDNZmvqpab8gl+
+HYk6SVWK7P2yDmOOEW7dJHZrzWDDIHlq1L2sR5yF55KZXc02t9quiTrMxBNZGDIq1fKN0gcgE1wpyWGp6I+/f VI7Yp
c5c4WRImmNAwIZL2hIXMUzdx0QKIANaRgBdBFQ== kam@Kenai.local
```



https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/FORTINET_BACKDOOR



OWASP
Open Web Application
Security Project

Insecure Network's

* Porta 23 Telnet

Evasão: Bruteforce em painel com medusa (Private Server)



Insecure Network's

* Porta 3389 Terminal service

Evasão: Provedores e serviços angryp Scanner através de range de IPs por
localidade. (: <http://tools.tracemyip.org/search--city/cuiab%C3%A1-mato+grosso>

ID ↕	IP Address ↕	ISP ↕	Organization ↕	Country↕	Timezone ↕	Browser ↕	Operating System ↕	Bot/spider ↕
1	201.7.19.79	Oi Internet	Oi Internet	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 5.1.1	No
2	191.33.161.196	Vivo	Vivo	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
3	177.13.255.44	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 5.0.2	No
4	177.221.98.34	Bi-Link Telecom	Bi-Link Telecom	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
5	177.13.248.16	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0	No
6	179.216.222.68	NET Virtua	NET Virtua	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
7	2804:d59:a08:8e00:cf8:6a7:9ae8:136f	Oi Internet	Oi Internet	Brazil	America/Cuiaba	Chrome 55.0.2883.91	Android, 5.1.1	No
8	177.13.249.63	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 30.0.0.0	Android, 4.4.2	No
9	201.7.19.159	Oi Internet	Oi Internet	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 5.1.1	No
10	201.71.162.134	Titania Telecom	Titania Telecom	Brazil	America/Cuiaba	Safari 4.0	Android, 4.3	No
11	177.13.248.93	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0	No
12	177.13.254.77	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0	No
13	177.13.81.57	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0	No
14	177.13.251.13	Acom Comunicacoes S.A.	Acom Comunicacoes S.A.	Brazil	America/Cuiaba	Safari 4.0	Android, 4.1.2	No
15	177.41.81.25	Global Village Telecom	Global Village Telecom	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
16	179.216.222.203	NET Virtua	NET Virtua	Brazil	America/Cuiaba	Chrome 43.0.2357.121	Android, 5.0.1	No
17	177.221.107.53	Bi-Link Telecom	Bi-Link Telecom	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
18	177.221.105.54	Bi-Link Telecom	Bi-Link Telecom	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 6.0.1	No
19	2804:7f3:6980:c5bd:1084:fdac:621:489f	Vivo	Vivo	Brazil	America/Cuiaba	Chrome 56.0.2924.87	Android, 5.1.1	No
20	200.163.108.111	Oi Internet	Oi Internet	Brazil	America/Cuiaba	Chrome 55.0.2883.91	Android, 5.1.1	No
21	179.179.91.84	Vivo	Vivo	Brazil	America/Cuiaba	Chrome 55.0.2883.91	Android, 6.0	No

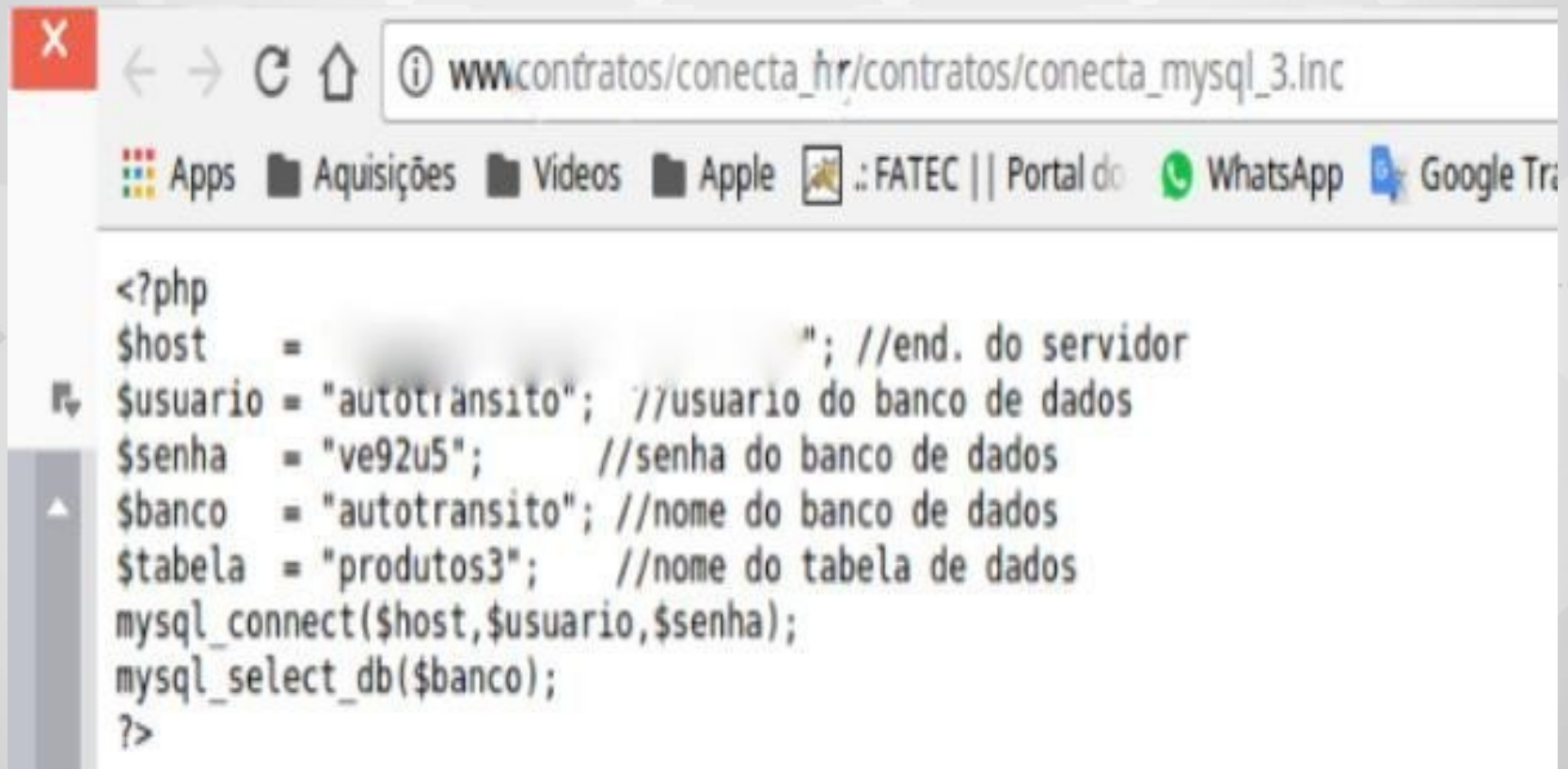


Insecure Network's

Porta 3306 Mysql SGDB

Evasão: **filetype:inc mysql_connect OR mysql_pconnect**

http://www.xxx.com.br/contratos/conecta_mysql_3.inc



```
<?php
$host      = "192.168.1.100"; //end. do servidor
$usuario   = "autotransito"; //usuario do banco de dados
$senha     = "ve92u5";       //senha do banco de dados
$banco     = "autotransito"; //nome do banco de dados
$tabela    = "produtos3";    //nome do tabela de dados
mysql_connect($host,$usuario,$senha);
mysql_select_db($banco);
?>
```

Insecure Network's

Http attack bypassing WAF's

Technology/Environment	Parameter Interpretation	Example
ASP.NET/IIS	Concatenation by comma	par1=val1,val2
ASP/IIS	Concatenation by comma	par1=val1,val2
PHP/APACHE	The last parameter is resulting	par1=val2
PHP/Zeus	The last parameter is resulting	par1=val2
JSP, Servlet/Apache Tomcat	The first parameter is resulting	par1=val1
JSP, Servlet/Oracle Application Server 10g	The first parameter is resulting	par1=val1
JSP, Servlet/Jetty	The first parameter is resulting	par1=val1
IBM Lotus Domino	The first parameter is resulting	par1=val1
IBM HTTP Server	The last parameter is resulting	par1=val2
mod_perl/libapeq2/Apache	The first parameter is resulting	par1=val1
Perl CGI/Apache	The first parameter is resulting	par1=val1
mod_perl/lib??*/Apache	The first parameter is resulting	par1=val1
mod_wsgi (Python)/Apache	An array is returned	ARRAY(0x8b9058c)
Pythin/Zope	The first parameter is resulting	par1=val1
IceWarp	An array is returned	['val1','val2']
AXIS 2400	The last parameter is resulting	par1=val2
Linksys Wireless-G PTZ Internet Camera	Concatenation by comma	par1=val1,val2
Ricoh Aficio 1022 Printer	The last parameter is resulting	par1=val2
webcamXP Pro	The first parameter is resulting	par1=val1
DBMan	Concatenation by two tildes	par1=val1~~val2

https://www.owasp.org/index.php/SQL_Injection_Bypassing_WAF



OWASP
Open Web Application
Security Project

Insecure Network's

NativePayload_DNS : (Backdoor Payloads transfer by IPv4 Address (A and PTR) records and DNS Traffic also Bypassing Anti-viruses)

Host	record type	value	Meterpreter Payload line one {Payload}.1.com
1.1.1.0	PTR	0x990xa50x330xd40xc90x310xbb0x750x000x000xff.1.com	
1.1.1.1	PTR	0xe90xa50x310xd40xcb0x010xbb0x750xcc0x010xef.1.com	
1.1.1.253	PTR	10min5delay.1.com	
1.1.1.254	PTR	0min0delay.1.com	
TimeforReconnect.1.com	A	1.1.10.5	
1.0.1.0	PTR	0x990xa5.1.com	
1.0.1.1	PTR	0x330xd4.1.com	
1.0.1.2	PTR	0xc90x31.1.com	
1.0.1.3	PTR	0xbb0x75.1.com	
1.0.1.4	PTR	0x000x000xff.1.com	

time for backdoor core code to Reconnect to attacker every 10 minute and establish connection for 5 minute
1.1.{10},{5}

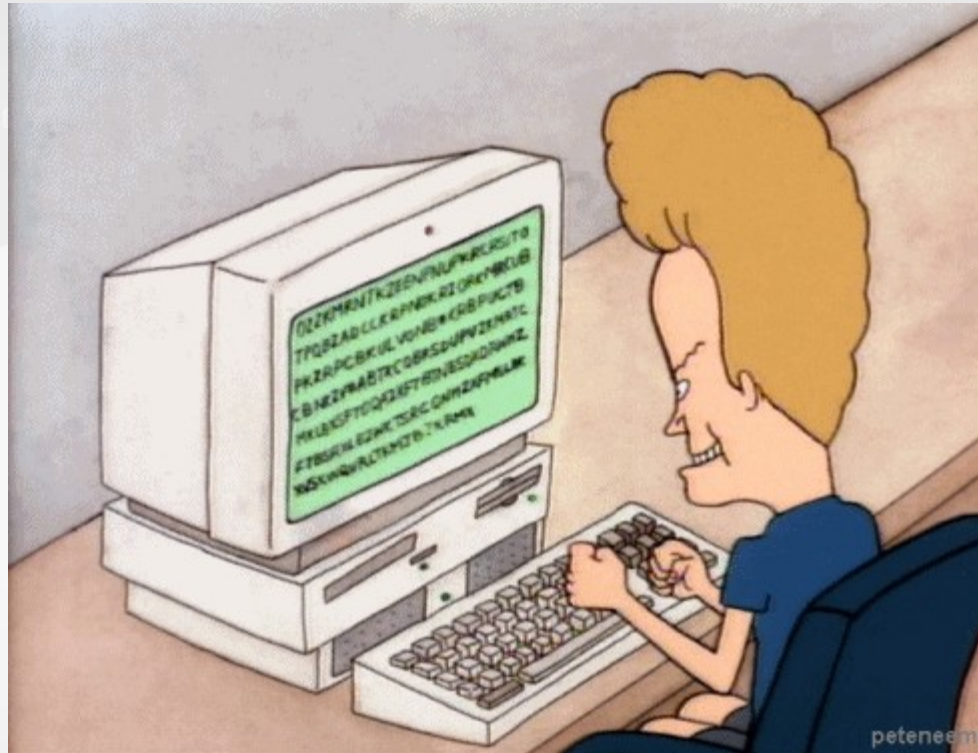
Good way for Bypassing Payload Detection over Network DNS Traffic by signatures for example with Snort (maybe ;-), split 1 record to 5 records and you can Resolve these records by NSLOOKUP with delay time for example (every 2 minute: get 1 record)

https://github.com/DamonMohammadbagher/NativePayload_DNS



OWASP
Open Web Application
Security Project

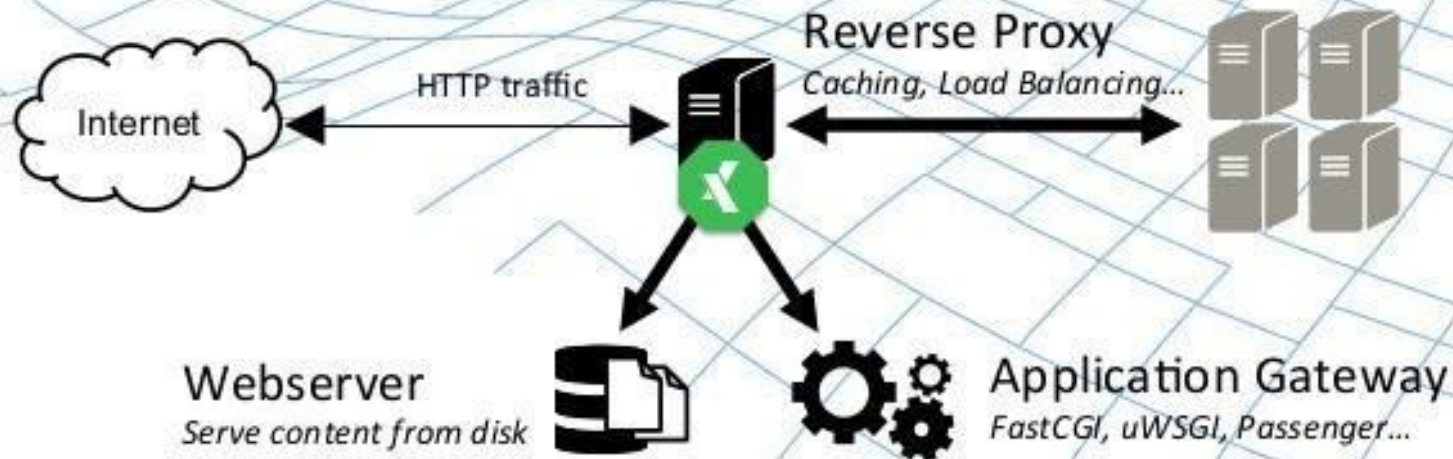
[S]ecure Network's Ignorando Attack's



Insecure Network's

SCG WS Nginx

What is NGINX?



NGINX features:

- ✓ Application Acceleration
- ✓ Content Caching
- ✓ SSL and SPDY termination
- ✓ Bandwidth Management

- ✓ Content-Based Routing
- ✓ Request Manipulation
- ✓ Response Rewriting
- ✓ Authentication

- ✓ Geo-IP
- ✓ Streaming Media
- ✓ Monitoring
- ✓ Configuration

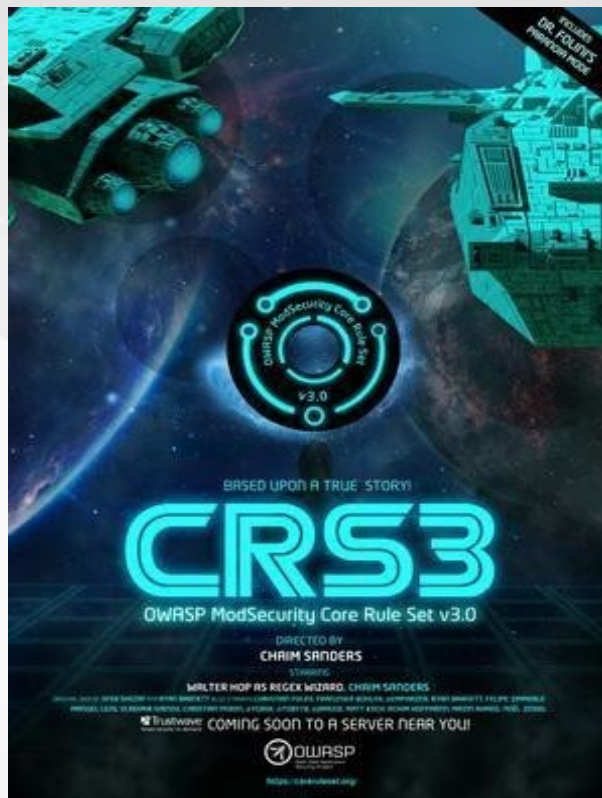
https://www.owasp.org/index.php/SCG_WS_nginx



OWASP
Open Web Application
Security Project

[S]ecure Network's

OWASP ModSecurity Core Rule Set (CRS)



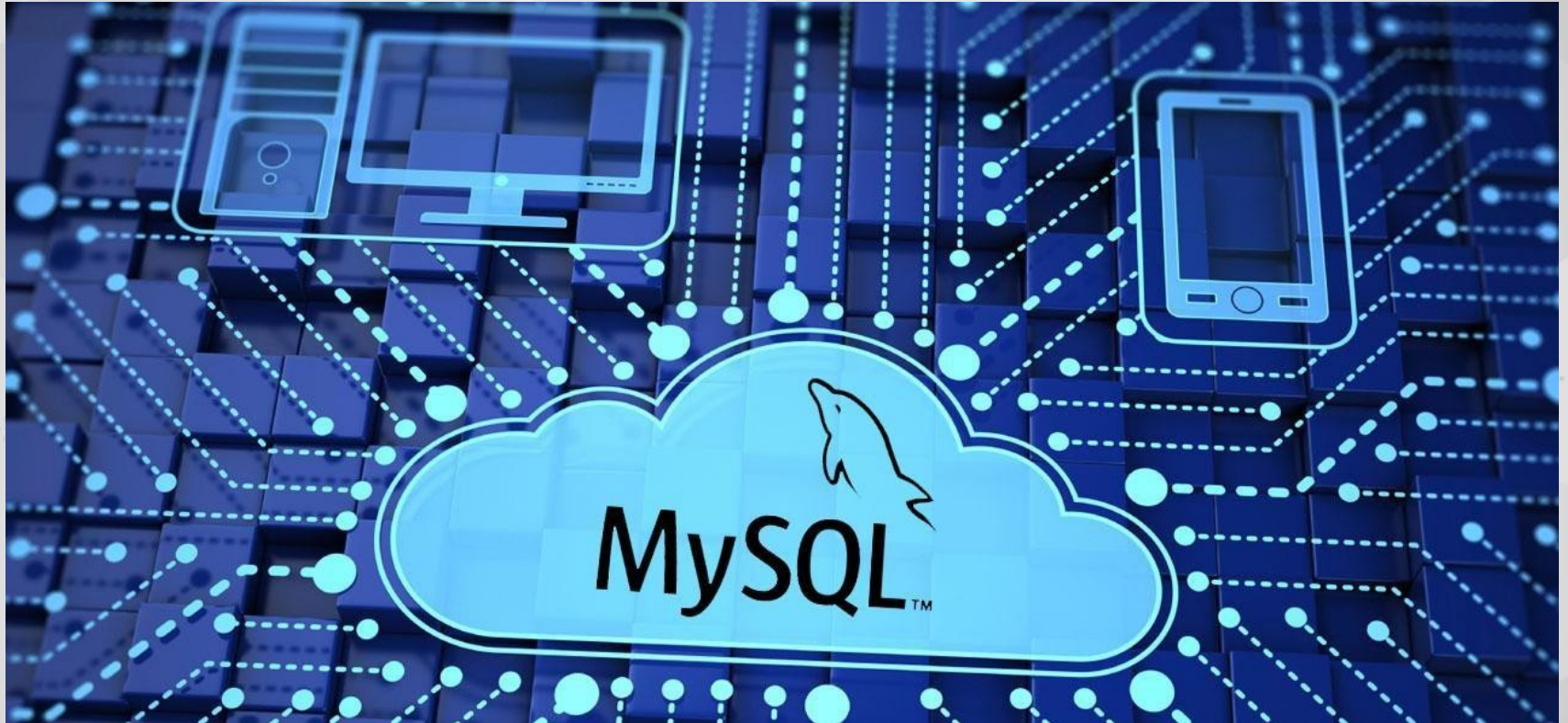
<https://www.owasp.org/index.php/>
Category:OWASP_ModSecurity_Core_Rule_Set_Project



OWASP
Open Web Application
Security Project

[S]ecure Network's

OWASP Backend Security Project MySQL Hardening



<https://>

www.owasp.org/index.php/OWASP_Backend_Security_Project_MySQL_Hardening

[S]ecure Network's

Security + DevOps

Automatic Server Hardening

dev-sec.io



OWASP
Open Web Application
Security Project



That's all Folks!