



OWASP

Open Web Application  
Security Project

# Ciberterrorismo

# 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

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.

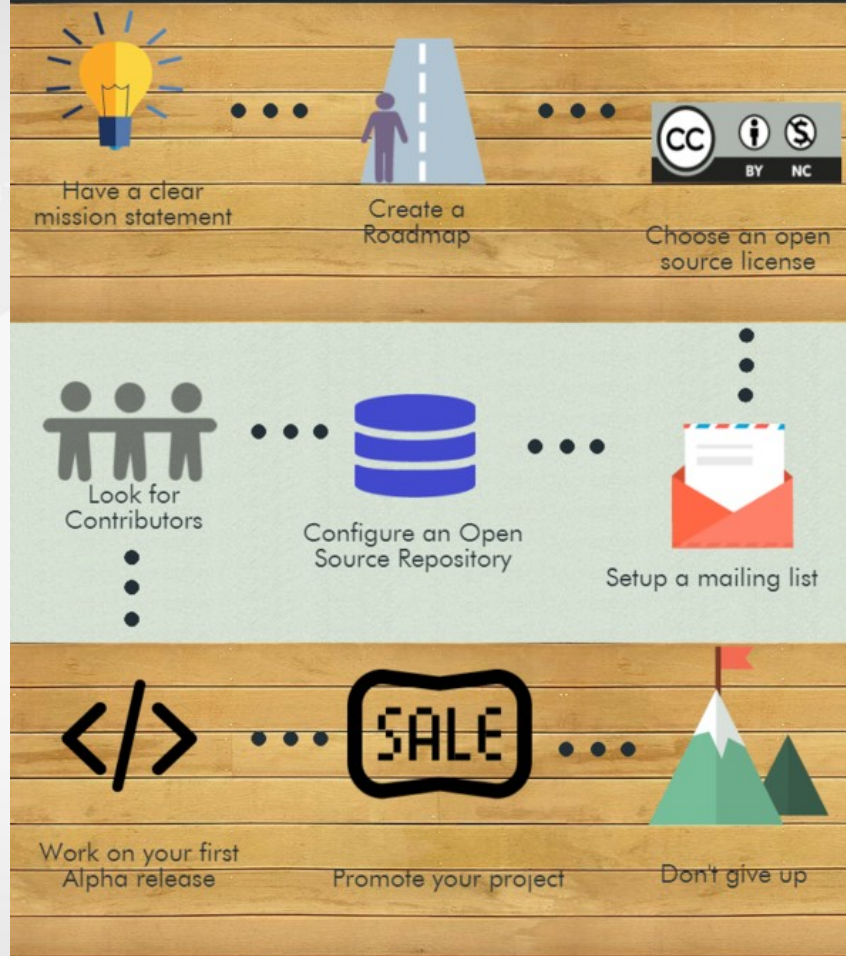
**Projetos de Laboratório:** Os projetos do OWASP Labs representam projetos que produziram uma entrega de valor revisada pelo OWASP.

**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.



# HOW TO START AN OWASP PROJECT

with 9 basic steps for code & tool projects



**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.

Tools 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	Documentation [Health Check January 2017] 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	Contests - Health Check February 2016 OWASP University Challenge OWASP CTF Project  Code 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  
ProjectThumbsup.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  
ProjectThumbsup.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  
ProjectThumbsup.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  
ProjectThumbsup.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)  
ProjectThumbsup.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  
OWASP\_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.

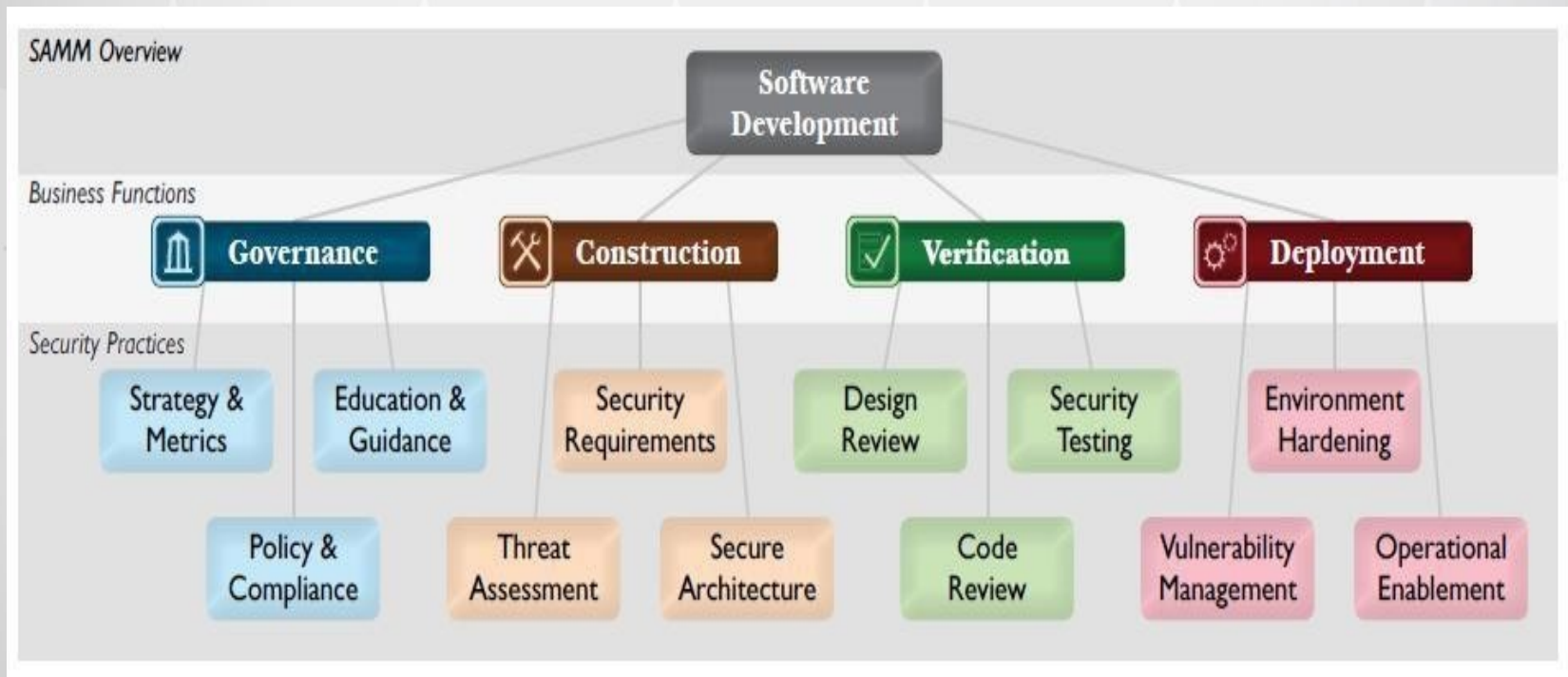
Ele possui recursos que o ajudarão em:

**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 ficará 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 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

## 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	Provisioning and Operating the Application
		Business context	Regulatory context	Technological context	Application specifications repository	Role, responsibilities and qualifications	Application security control library	Life cycle reference model
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.



CONNECT.

LEARN.

GROW.

**Happy Hacking Modafokers! ♥<sup>3</sup> '**



**OWASP**  
Open Web Application  
Security Project

# O que é Cibercrime?

Cibercrime é o nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na rede.

Essas práticas podem envolver invasões de sistema,s computacionais, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros.



# O que é Cibercrime?

O termo "cibercrime" (ou "cybercrime", em inglês) apareceu em uma reunião de um subgrupo do G-8 (grupo composto pelos oito países mais ricos do mundo, mais a Rússia, por sua importância histórica e militar) próximo do final dos anos 90. Essa reunião abordava exatamente as maneiras e os métodos utilizados para combater as práticas ilícitas da internet.



# O que é Cibercrime?

Existem vários tipos de cibercrimes e esse fato deixa as autoridades com ainda mais dificuldades para punir os transgressores devido a falta de tecnologia, recursos e, por falta de leis aplicáveis a determinadas infrações .



# O que é Cibercrime?

Existem vários tipos de cibercrimes e esse fato deixa as autoridades com ainda mais dificuldades para punir os transgressores devido a falta de tecnologia, recursos e, por falta de leis aplicáveis a determinadas infrações .





# O que é Cibercrime?

## **Pornografia Infantil:**

maliciosos utilizam a internet e dispositivos de acesso para criar e distribuir materiais com conteúdo pornográfico de crianças e menores de idade.

POLÍCIA

Quarta-feira, 04 de Setembro de 2019, 08h09 | - A | + A

OPERAÇÃO LUZ NA INFÂNCIA

Twitter Facebook Google+

## Em Cuiabá homem é preso em operação com 70 arquivos pornográficos

Por: O Bom da Notícia

PJC



A Polícia Judiciária Civil de Mato Grosso deu cumprimento a um mandado de busca e apreensão, na manhã desta quarta-feira (04), na operação nacional "Luz na Infância", deflagrada pelas Forças de Segurança Pública de todo Brasil, visando o combate ao crime de pornografia infantil e exploração sexual contra crianças e adolescentes.

Em Mato Grosso, um homem foi preso em posse de cerca de 70 arquivos pornográficos com imagens de crianças e adolescentes. A prisão foi realizada pelos policiais civis da Gerência de Combate a Crimes de Alta Tecnológica (Gerat) e Delegacia Especializada de Defesa dos Direitos da Criança e do Adolescente (Nedra).



# O que é Cibercrime?

**Lavagem de dinheiro:**  
esse tipo de crime é bastante comum. Os criminosos realizam transferências de dinheiro de maneira ilegal com o objetivo de esconder a sua fonte e também o seu destino.



*Laboratório clandestino de bitcoin é encontrado no Rio Grande do Sul. Imagem: Divulgação / Polícia Civil do RS*



# O que é Cibercrime?

**Ciberterrorismo:** esse crime é mais comum em países desenvolvidos e de conflitos políticos, mas também pode ser visto em larga escala em outros lugares do mundo. Consiste em ações premeditadas com motivações políticas cometidas, geralmente, contra governos, partidos e instituições governamentais. Também podem ser cometido amplamente contra civis.



# O que é Cibercrime?

**Ciberativismo:** crime praticado contra organizações que defendem determinadas causas. Esse cibercrime envolve roubo de informações e manipulações nos materiais que são divulgados ao público e à imprensa.

---

## **Lei Geral de Proteção de Dados (Lei 13.709/2019):**

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

(...)

II - realizado para fins exclusivamente:

a) jornalístico e artísticos;

(...)

## **Constituição Federal:**

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

---





# O que é Cibercrime?

**Roubo:** envolve a utilização de computadores ou outros dispositivos para desviar fundos ilegalmente, roubar dados de outros indivíduos, empresas ou instituições, para realizar espionagem, roubo de identidade, fraude, plágio e pirataria.

fonte:

<https://canaltech.com.br/seguranca/O-que-e-cibercrime/>





Name	Date modified	Type	Size
 ctfmon.exe	7/13/2009 10:14 PM	Application	9 KB
 MsCtfMonitor	6/10/2019 11:36 AM	File	11,012 KB
 MsCtfMonitor.dll	6/10/2019 11:49 AM	Application extens...	824 KB
 vjmq.zip	6/12/2019 4:24 AM	WinRAR ZIP archiv	11,308 KB

Figura 1: Componentes de Amavaldo extraídos em uma pasta. Os componentes são: ctfmon.exe (aplicativo legítimo), MsCtfMonitor (trojan bancário criptografado), MsCtfMonitor.dll (injetor).

<https://www.welivesecurity.com/br/2019/08/01/amavaldo-um-trojan-bancario-que-tenta-fazer-vitimas-no-brasil/>



**OWASP**  
Open Web Application  
Security Project

# Comportamentos do Cibercrime

CONNECT.

LEARN.

**Espionagem** - ocorre quando obtém informações sem autorização;

## Stalkerware: tentativas de espionagem no Brasil crescem 228%

Ataques com softwares espiões dispara no Brasil e também cresce no mundo.

Por Filipe Garrett, para o TechTudo

04/10/2019 07h00 · Atualizado há 2 semanas

<https://www.techtudo.com.br/noticias/2019/10/stalkerware-tentativas-de-espionagem-no-brasil-crescem-228percent.ghml>



**OWASP**  
Open Web Application  
Security Project

# Comportamentos do Cibercrime

**Violação de autorização** - quando utiliza a autorização de outra pessoa para finalidades desconhecidas;

## PF combate fraudes contra o INSS

Operação PF - ES

Operação 5X7 investiga saques fraudulentos de Benefícios de Prestação Continuada de Amparo ao Idoso

por

Publicado: 05/06/2019 08h48

Última modificação: 05/06/2019 08h48



Vila Velha/ES – A Polícia Federal deflagrou nesta quarta-feira (5/6) a Operação 5X7, com o objetivo de desbaratar organização criminoso, com atuação no Espírito Santo e Bahia, que pratica fraudes contra o INSS, com a utilização de documentos falsos para criação de pessoas fictícias para saque de Benefícios de Prestação Continuada de Amparo ao Idoso.

<http://www.pf.gov.br/imprensa/noticias/2019/06/pf-combate-fraudes-contr-o-inss>



**OWASP**  
Open Web Application  
Security Project



# Comportamentos do Cibercrime

**Vazamento** - revelação indevida de informação;

## Nº 7 – Facebook

**Número de vítimas:** 87 milhões

**Quem foi alvo:** Usuários do Facebook

**Quais dados foram expostos:** Informações de perfil, crenças políticas, redes de amigos, mensagens privadas

**Período:** Revelado em setembro de 2018

**O que aconteceu:** Esse é o famoso [escândalo da Cambridge Analytica](#), em que a empresa de coleta de dados coletou ilegalmente informações dos usuários sem permissão. A operação secreta foi motivada politicamente, por influência da campanha presidencial americana de 2016. Embora a vazamento tenha ocorrido há alguns anos, apenas esse ano as conclusões da investigação foram divulgadas, oferecendo um panorama mais claro do que aconteceu.

<https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados>



# Comportamentos do Cibercrime

**Sabotagem computacional** - ocorre quando os dados são removidos ou modificados com o intuito de alterar o funcionamento da máquina;

**Recusa de serviço** - não atende à solicitação das requisições legítimas dos usuários;

**Moral** - ocorre quando o servidor on-line (público ou privado)(prestador de serviços, como comunicações, entretenimento, informativo, etc...) expressa diretamente ou indiretamente, atos tais como, racismo, xenofobia, homofobia, humilhação, repreensão, ou outros atos que agridem moralmente o usuário;

**Repúdio** - negação imprópria de uma ação ou transação efetivamente realizada.



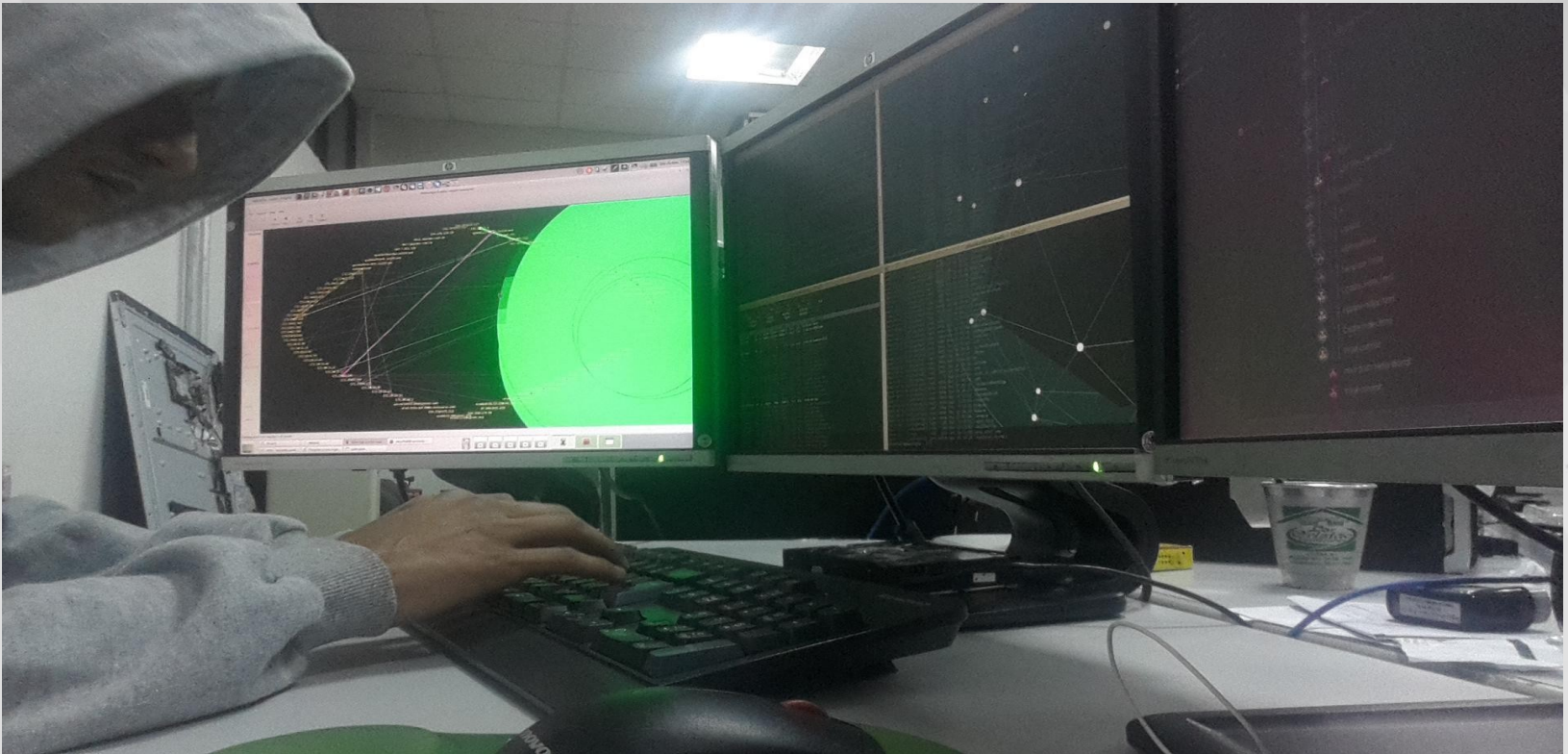
# O que é Ciberterrorismo?

**Ciberterrorismo** é a expressão usada para descrever os ataques terroristas executados pela Internet, com o objetivo de causar danos a sistemas ou equipamentos de comunicação.

Em sua maioria são utilizados de Técnicas de identificação e exploração de alvos para indisponibilizar serviços ou expor os critérios de segurança da informação de uma determinada organização.



# Insecure Network's



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



**OWASP**  
Open Web Application  
Security Project

# Insecure Network's

## Modelo O.S.I.



## Modelo T.C.P./I.P.





# 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

## CAMADA 1 - 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.

Operadora De Internet Tem Cabo De Fibra Ótica Cortado Por Seis Vezes E Suspeita É De Sabotagem Em Coari

dbarreto 15 de outubro de 2019 0 COMMENTS



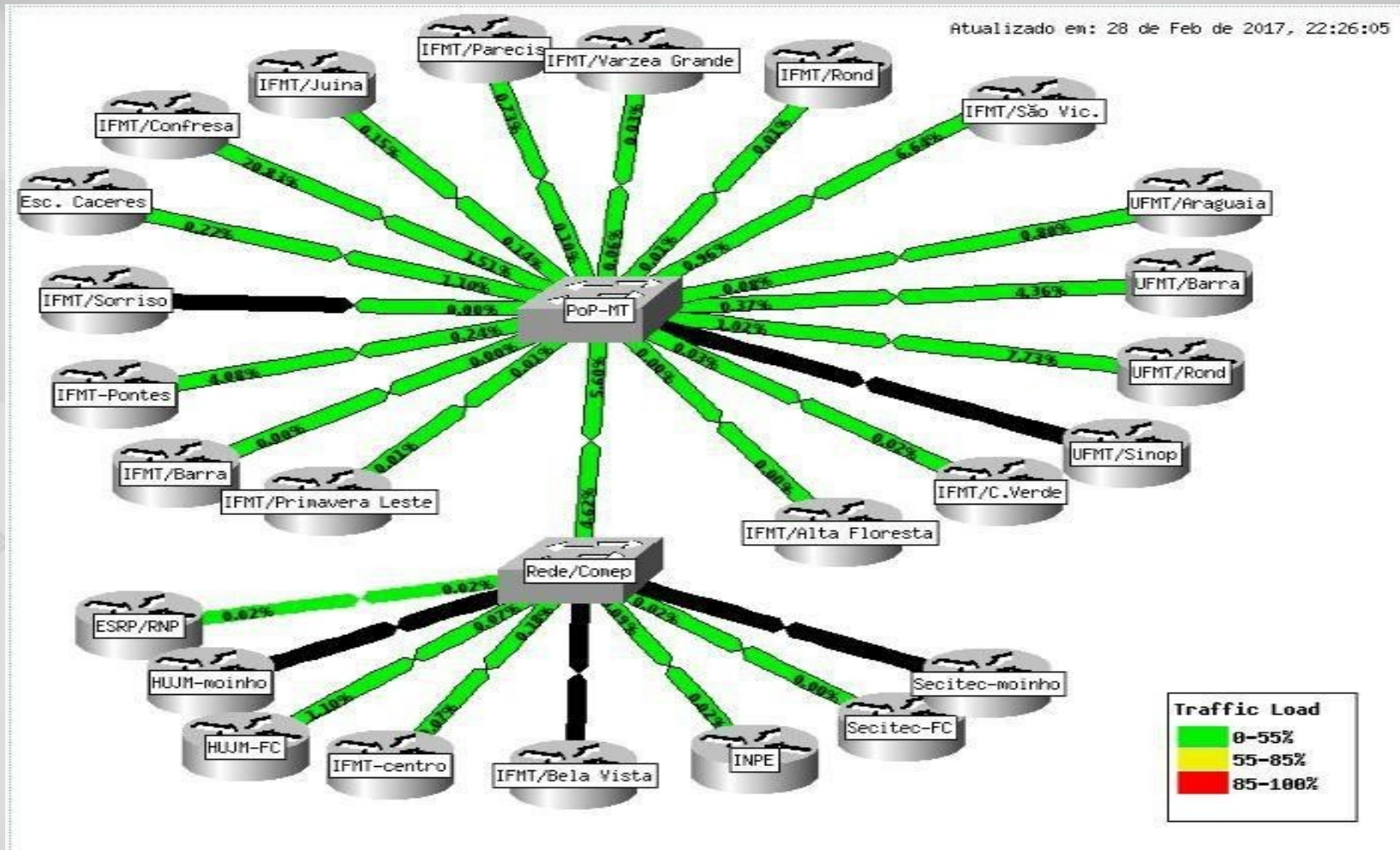
<https://newsam.com.br/operadora-de-internet-tem-cabo-de-fibra-otica-cortado-por-seis-vezes-e-suspeita-e-de-sabotagem-em-coari/>



**OWASP**  
Open Web Application  
Security Project



# Insecure Network's



Fonte: POP- MT - Ponto de Presença Rede Nacional de Pesquisa  
- MTwebsite: [www.pop-mt.rnp.br/site/?page\\_id=44](http://www.pop-mt.rnp.br/site/?page_id=44)

# Insecure Network's

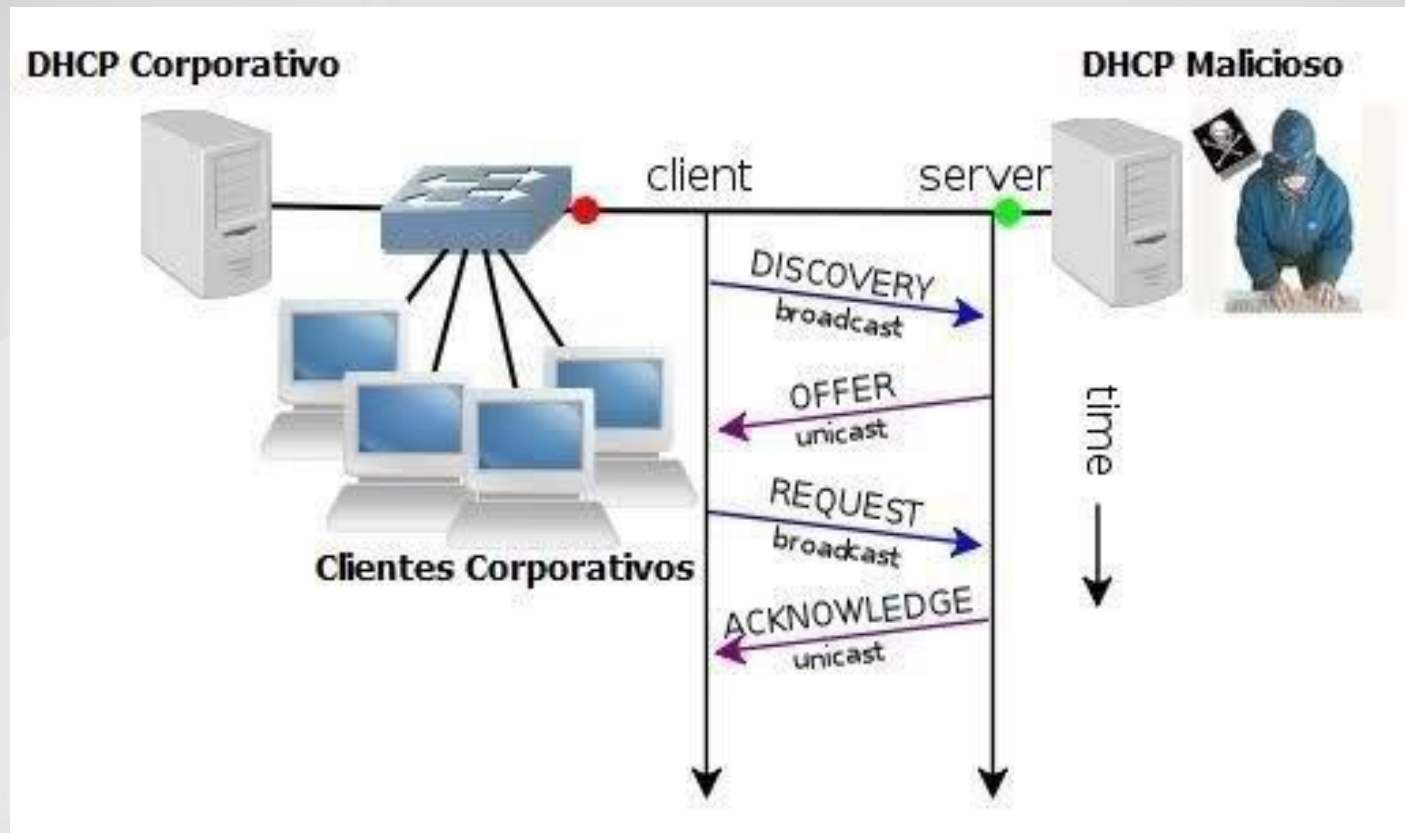
## **CAMADA 2 - Enlace**

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

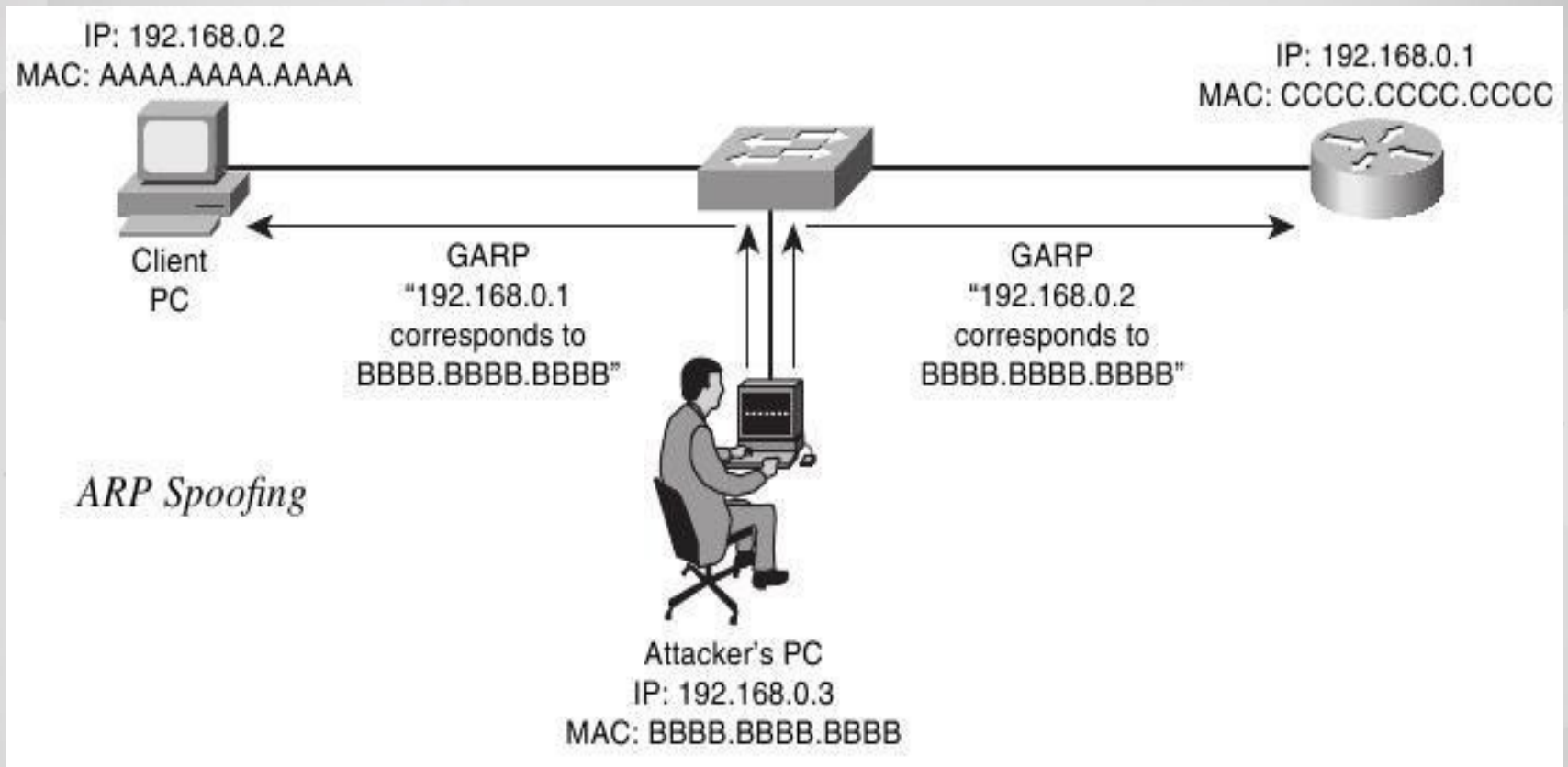


Dhcparpd <http://research.wand.net.nz/software/dhcparpd.php>



**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

Para encontrar alvos na internet atacantes buscam primeiramente pelos segmentos de ip's dos seus próprios provedores, acesse [meuip.com.br](http://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

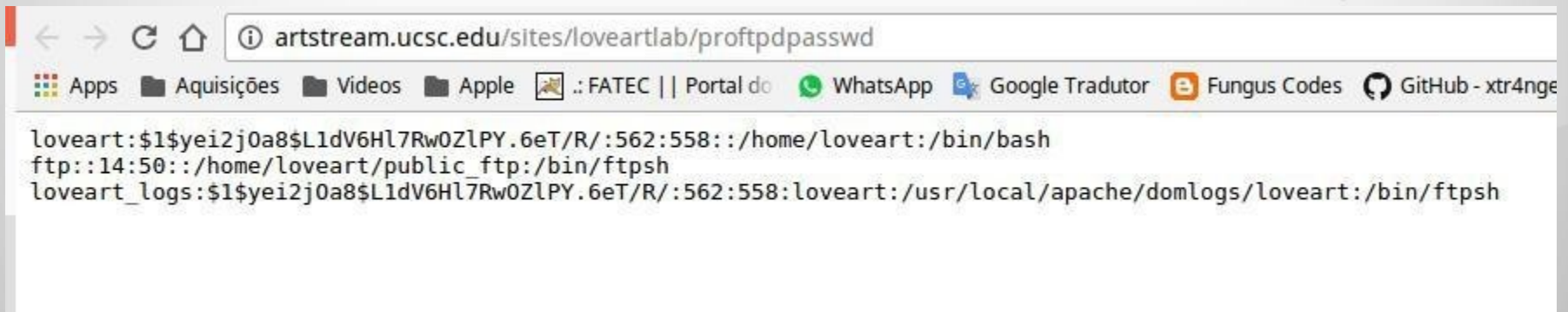
# Insecure Network's

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
```



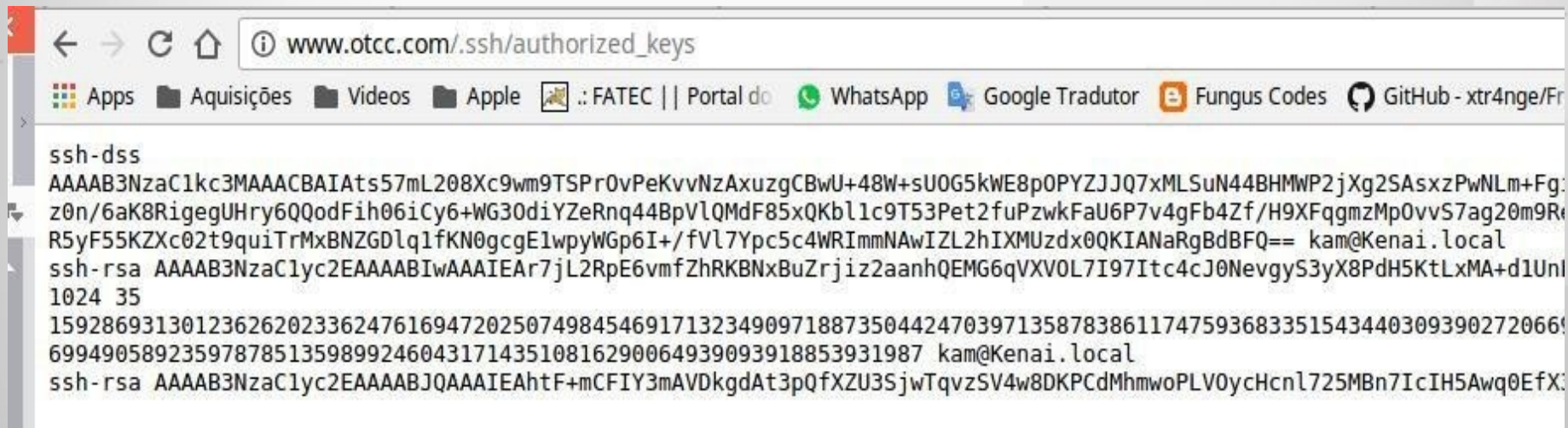
# Insecure Network's

\* Porta 22 Secure Shell (SSH) forwarding

Evasão: **inurl:.ssh intitle:index.of authorized\_keys**

ssh-dss

```
AAAAB3NzaC1kc3MAAACBAIAts57mL208Xc9wm9TSPrOvPeKvvNzAxuzgCBwU+48W+sUOG5kWE8pOPYZJJQ7xMLSuN44BHMWP2jXg2SAsxzPwNLm+FgiX83f4qW/vhE6III/y5VjV/Jcpd2n/w08cX1jRZnqraip2Ujxx56DT86GJezmvdvBG9hmluJcmftLBAAAAFQDLUavNK5zu+tIRi9xYkwokcA3uQAAAIb5Sdzkr2nWbzlz0n/6aK8RigegUHry6QQodFih06iCy6+WG30diYZeRnq44BpVIQMdF85xQKbl1c9T53Pet2fuPzwkFaU6P7v4gFb4Zf/H9XFqgmzMpOvvS7ag20m9RevyzobStv2hh9gjif1wS8oMW9Mtl7YtEwjfp7pnN1BcjwAAAIAbKyqmNpqzHSMfO/+fl/r7T Dp2Bc mzDNZmvqpab8gl++HYk6SVWK7P2yDmOOEW7dJHZrzWDDIHlq1L2sR5yF55KZXc02t9quiTrMxBNZGDlq1fKN0gcgE1wpyWGp6I+/f VI7Yp5c4WRImmNAwIZL2hIXMUzdx0QKIANaRgBdBFQ== kam@Kenai.local
```



[https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/FORTINET\\_BACKDOOR](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 angryip 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	Titanila Telecom	Titanila 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



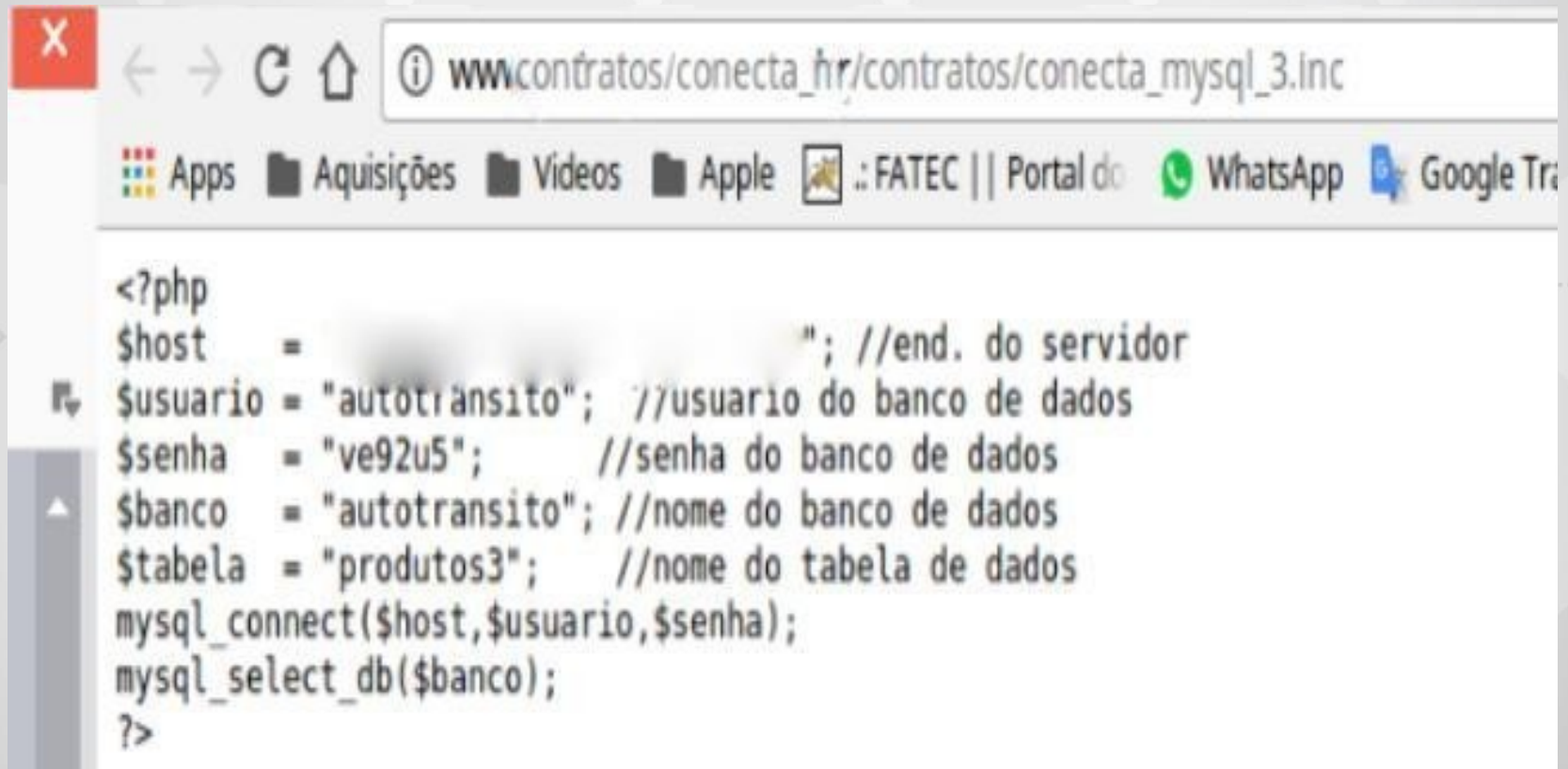


# Insecure Network's

Porta 3306 Mysql SGDB

Evasão: **filetype:inc mysql\_connect OR mysql\_pconnect**

[http://www.xxx.com.br/contratos/conecta\\_mysql\\_3.inc](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](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](https://github.com/DamonMohammadbagher/NativePayload_DNS)



**OWASP**  
Open Web Application  
Security Project

# Evidências de Ciberterrorismo

## Operação Shady RAT

Em 2006, aconteceram uma série de ataques cibernéticos em pelo menos 72 corporações, de acordo com um relatório divulgado pela empresa de segurança McAfee. Os dados de todas essas instituições foram roubados por um grupo de hackers que usou um método de ataque único, que ficou conhecido como Operação Shady RAT. Dentre as organizações atacadas, estavam a Nações Unidas, agências de governo e empresas de segurança de diversos países. A McAfee acredita que os hackers podem ter capturados cerca de 1000 terabytes de informação.

## Shady Rat ataca 70 organizações em 14 países

Editorial IT Forum 365

03/08/2011 às 12h03

Foto:

 <https://www.itforum365.com.br/sha>



Um ataque do tipo ameaça persistente avançada (APT) está ativo há cinco anos e já roubou dados de 70 agências governamentais, corporações internacionais e organizações sem fins lucrativos em 14 países, segundo um novo relatório publicado na revista *Vanity Fair*.



**OWASP**  
Open Web Application  
Security Project



# Evidências de Ciberterrorismo

## Sony Pictures

A Sony Pictures foi invadida em novembro de 2014 e teve seus sistemas destruídos e informações roubadas. Os ataques foram atribuídos à Coreia do Norte, mas até o momento esta alegação não foi comprovada. Acredita-se que o ato tenha sido uma represália ao filme A Entrevista, que relata a história de um complô para assassinar o líder norte-coreano Kim Jong Un. Os especialistas utilizaram os termos “ato de guerra” e “ciberterrorismo” para definir este tipo de ataque.

## Entenda o caso da invasão hacker à Sony Pictures

BRUNO ROMANI  
COLABORAÇÃO PARA A FOLHA

16/12/2014 @ 02h00



Compartilhar



< 0



OUVIR O TEXTO



Mais opções

"Esse foi um ataque sem precedentes", dizia no último dia 7 de dezembro o primeiro comunicado da Sony sobre o bombardeio hacker que eviscerou na internet os computadores da empresa.

O que no último dia 24 de novembro começou como apenas mais um ataque a uma companhia com complicado histórico de cibersegurança, ganhou 13 dias depois, nas palavras da própria Sony, contornos dramáticos.

PUBLICIDADE



**OWASP**  
Open Web Application  
Security Project

# Evidências de Ciberterrorismo

Sistemas militares americanos  
Entre 2001 e 2002, os EUA sofreram o maior ataque de todos os tempos a um computador militar. Cerca de 53 computadores do exército americano, da aeronáutica, do Pentágono e da Agência Espacial Americana (Nasa) foram danificados. O hacker alegou que tinha o objetivo de comprovar a existência de objetos voadores não identificados e comprovar a falta de segurança do sistema americano.

30/07/08 - 10h16 - Atualizado em 30/07/08 - 10h30



## 'Hacker' que invadiu defesa dos EUA pode ser extraditado

Britânico é acusado de invadir computadores da Nasa, Exército e Marinha americana.

Da BBC

Tamanho da letra

A-

A+

Um britânico acusado de entrar em redes de computadores da Nasa e na rede do Departamento de Defesa americano teve o recurso rejeitado e pode ser extraditado para os Estados Unidos para julgamento.



**OWASP**  
Open Web Application  
Security Project



# Evidências de Ciberterrorismo

## Hackers invadem Domino's Pizza e exigem resgate equivalente a US\$ 40 mil

Invasores alegam ter obtido registros de mais de 600 mil clientes na França e na Bélgica

O Globo, com sites

16/06/2014 - 08:59 / Atualizado em 16/06/2014 - 09:47



Loja da rede Domino's Pizza na Rua St. Dominique, em Paris, França Foto: Divulgação



**OWASP**  
Open Web Application  
Security Project

## Hackers furtam cartões de crédito de 40 milhões de pessoas

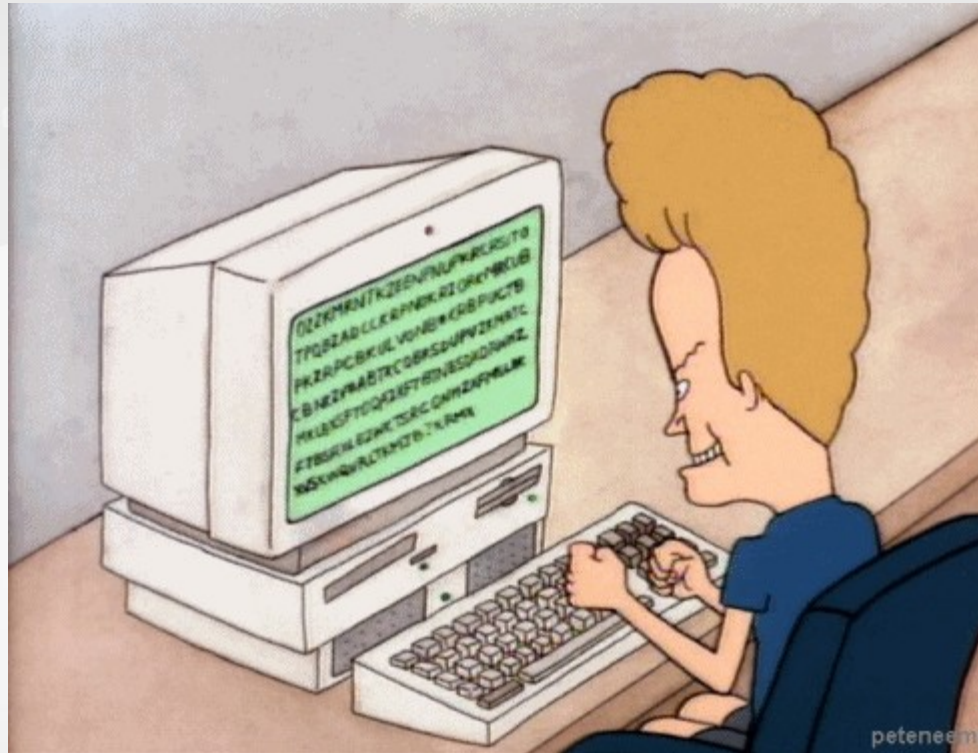
Um ataque ao sistema de pagamento das lojas Target, nos Estados Unidos, resultou no furto de dados de cartões de 40 milhões de pessoas

Por **Maurício Grego**  
🕒 19 dez 2013, 11h12



# [S]ecure Network's

## Ignorando Attack's

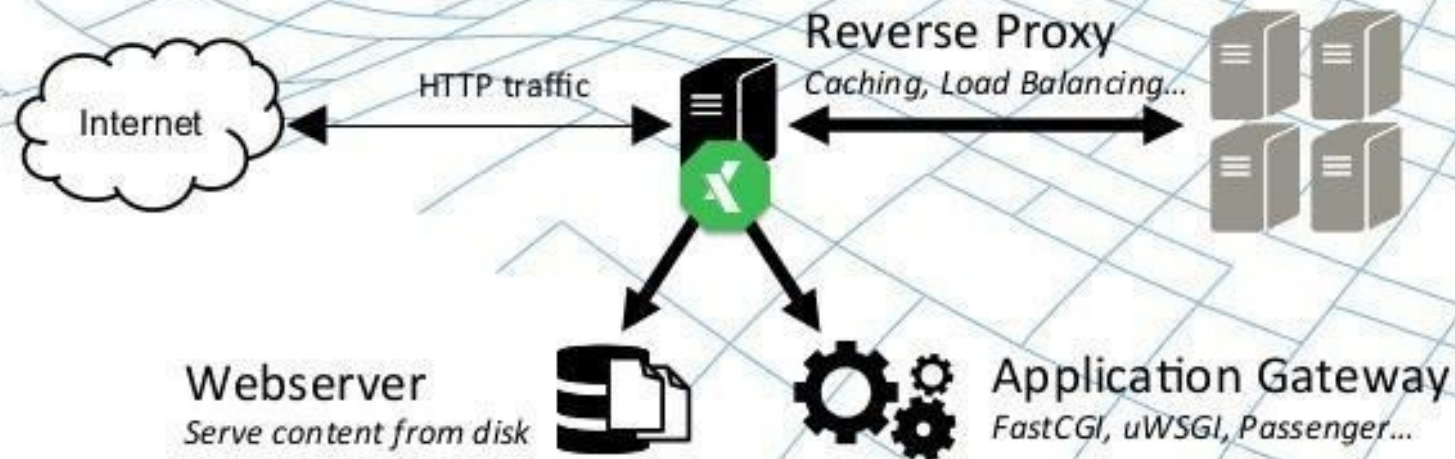




# Insecure Network's

## 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

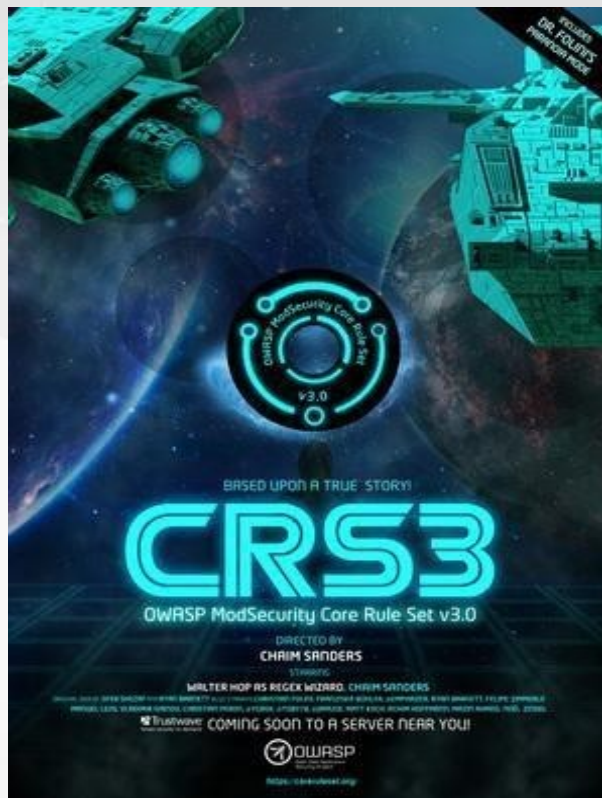
[https://www.owasp.org/index.php/SCG\\_WS\\_nginx](https://www.owasp.org/index.php/SCG_WS_nginx)



**OWASP**  
Open Web Application  
Security Project

# [S]ecure Network's

## OWASP ModSecurity Core Rule Set (CRS)



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

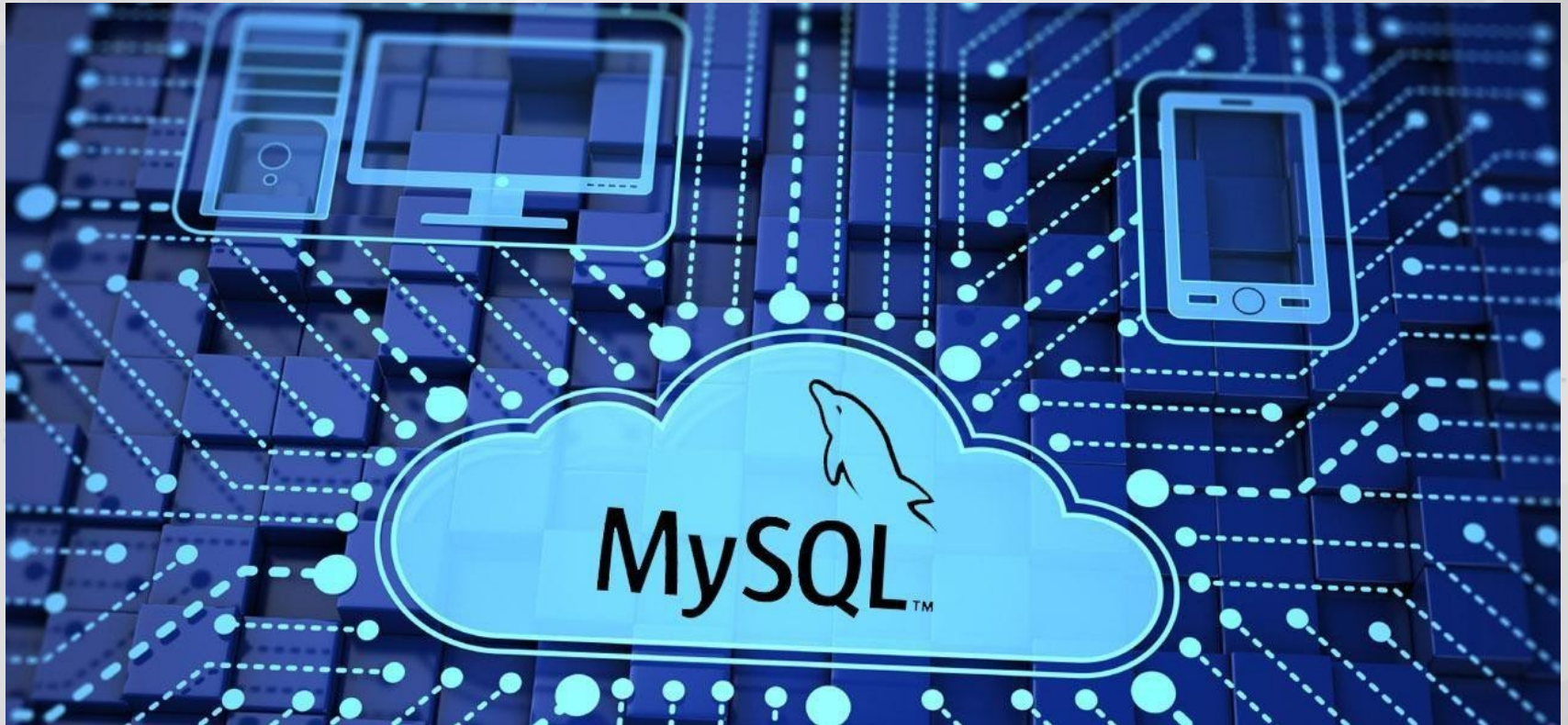
Category:OWASP\_ModSecurity\_Core\_Rule\_Set\_Project



**OWASP**  
Open Web Application  
Security Project

# [S]ecure Network's

## OWASP Backend Security Project MySQL Hardening



[https://](https://www.owasp.org/index.php/OWASP_Backend_Security_Project_MySQL_Hardening)

[www.owasp.org/index.php/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!*