The OWASP Foundation
http://www.owasp.org

OWASP

Open Web Application Security Project

Experimento 04 - Teoria

OWASP :: Open Web Application Security Project

- Projeto aberto de Segurança em Aplicações Web;
- Comunidade aberta que promove a aplicação de princípios de segurança na construção de aplicações.
- Libera diversos artigos, metodologias, ferramentas da testes tratando de:
  - Metodologias (***OSSTMM - Open Source Security Testing Methodology Manual***)
  - Treinamentos (**SANS - *Information Security Training***)
  - Guias de “Boas Práticas”
  - Modelos defensivos e ferramentas de testes ofensivas controlados
  - Avaliação periódica dos **Top 10 OWASP**

OWASP :: Referências

Em português:

- https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf

Em inglês:

- https://www.owasp.org
- https://www.sans.org/
- http://www.isecom.org/mirror/OSSTMM.3.pdf
- http://onlinepresent.org/proceedings/vol87_2015/8.pdf

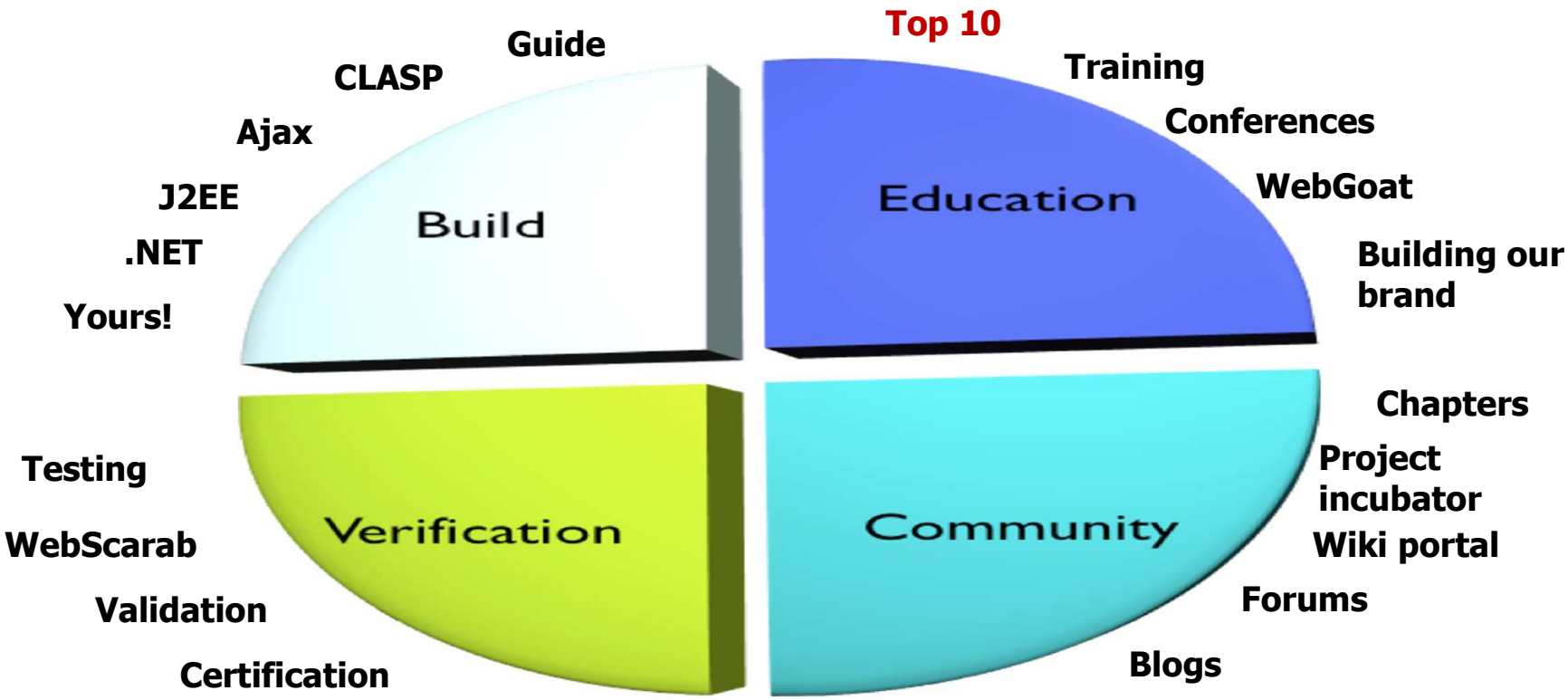
OWASP :: Organização

- *Board* Central / Global
- Comitês Globais
  - Educação
  - Capítulos
  - Conferências
  - Indústria
  - Projetos
  - Ferramentas
  - Filiação
- Funcionários e Voluntários

OWASP :: Código de Ética

- Desempenhar todas as atividades e deveres profissionais de acordo com todas as leis aplicáveis e os mais altos princípios éticos
- Promover a implementação e promover a conformidade com padrões, procedimentos, controles para segurança de aplicativos
- Manter a confidencialidade adequada de informações confidenciais ou de outra natureza sensíveis encontradas no decorrer de atividades profissionais
- Cumpra as responsabilidades profissionais com diligência e honestidade
- Abster-se de quaisquer atividades que possam constituir um conflito de interesses ou de outra forma prejudicar a reputação dos empregadores, da profissão de segurança da informação ou da Associação.
- Não intencionalmente prejudicar ou impugnar a reputação profissional da prática de colegas, clientes ou empregadores

OWASP :: Principais Iniciativas



OWASP :: Big 4


Building Guide
Code Review Guide
Testing Guide
Application Security Desk Reference (ASDR)

OWASP :: Top 10

- As 10 principais vulnerabilidades de segurança de aplicativos da Web.
- Uma lista dos 10 problemas de segurança mais graves
- Atualizado recentemente (2017)
- Resolver problemas com aplicativos
- Crescente aceitação da indústria
  - Comissão Federal de Comércio (Gov dos EUA)
  - Agência de Sistemas de Informação de Defesa dos EUA
  - VISA (Programa de Segurança da Informação do Titular do Cartão)
  - Referenciado pelo padrão PCI-DSS
  - Tendência forte para formar padrões

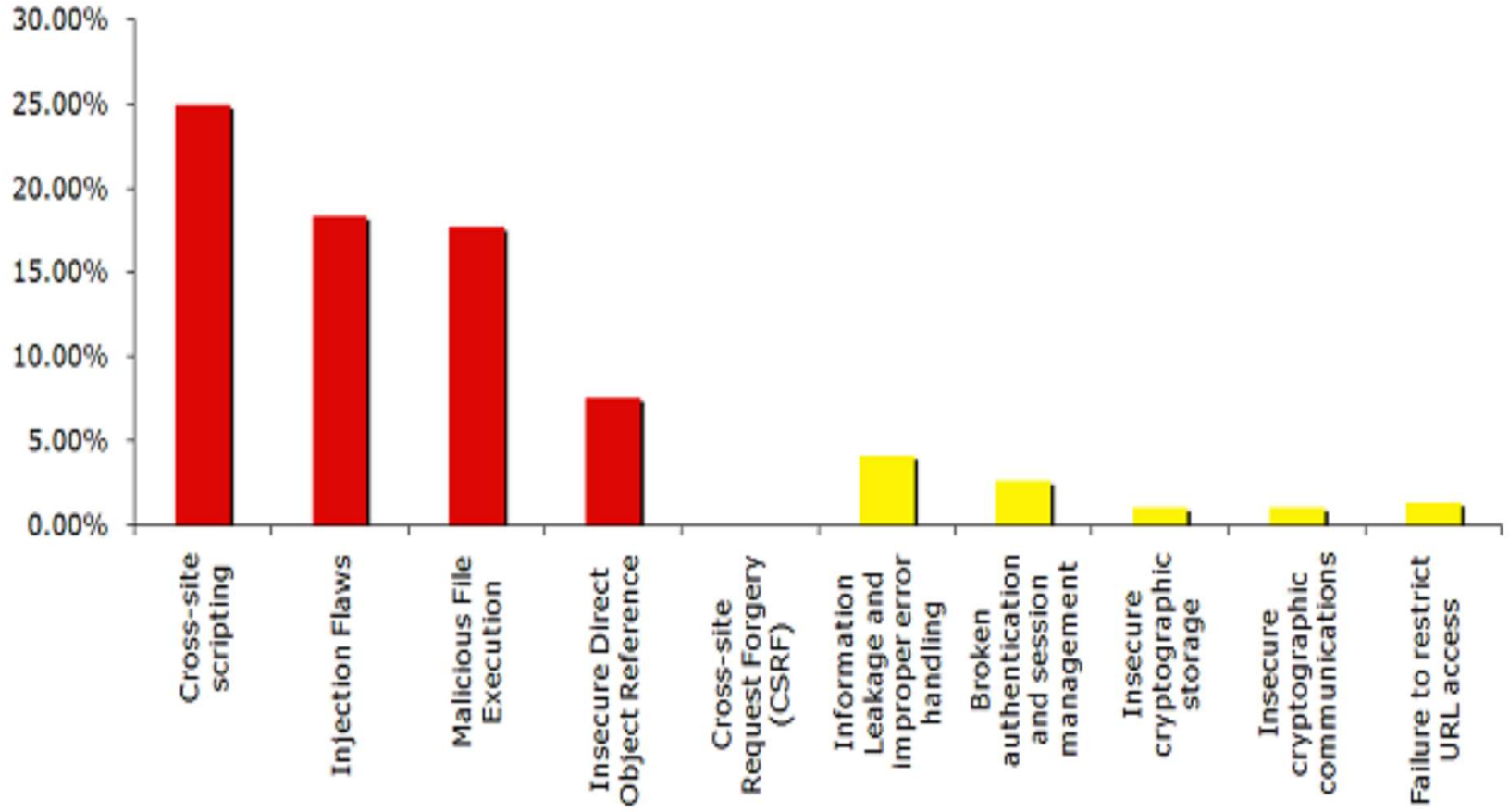
OWASP :: Top Ten 2007

A1 - Cross Site Scripting (XSS)’’	Os furos XSS ocorrem sempre que uma aplicação obtém as informações fornecidas pelo usuário e as envia de volta ao navegador sem realizar validação ou codificação daquele conteúdo. O XSS permite aos atacantes executarem scripts no navegador da vítima, o qual pode roubar sessões de usuário, pichar sites Web, introduzir *worms*, etc.
A2 - Falhas de Injeção	As falhas de injeção, em especial SQL Injection, são comuns em aplicações Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados a um interpretador com parte do comando ou consulta. A informação maliciosa fornecida pelo atacante engana o interpretador que irá executar comandos mal intencionados ou manipular informações.
A3 - Execução maliciosa de arquivos	Os códigos vulneráveis à inclusão remota de arquivos (RFI) permite ao atacante incluir código e dados maliciosos, resultando em ataques devastadores, como o comprometimento total do servidor. Os ataques de execução de arquivos maliciosos afeta PHP, XML e todos os frameworks que aceitem nomes de arquivo ou arquivos dos usuários.
A4 - Referência Insegura Direta à Objetos	Uma referência direta à objeto ocorre quando um desenvolvedor expõe a referência a um objeto implementado internamente, como é o caso de arquivos, diretórios, registros da base de dados ou chaves, na forma de uma URL ou parâmetro de formulário. Os atacantes podem manipular estas referências para acessar outros objetos sem autorização.
A5 - Cross Site Request Forgery (CSRF)	Um ataque CSRF força o navegador da vítima, que esteja autenticado em uma aplicação, a enviar uma requisição pré-autenticada à um servidor Web vulnerável, que por sua vez força o navegador da vítima a executar uma ação maliciosa em prol do atacante. O CSRF pode ser tão poderoso quanto a aplicação Web que ele ataca.

OWASP :: Top Ten 2007

A6 - Vazamento de Informações e Tratamento de Erros Inapropriado	As aplicações podem divulgar informações sobre suas configurações, processos internos ou violar a privacidade por meio de uma série de problemas na aplicação, sem haver qualquer intenção. Os atacantes podem usar esta fragilidade para roubar informações consideradas sensíveis ou conduzir ataques mais estruturados.
A7 - Autenticação falha e Gerenciamento de Sessão	As credenciais de acesso e token de sessão não são protegidos apropriadamente com bastante frequência. Atacantes comprometem senhas, chaves ou tokens de autenticação de forma a assumir a identidade de outros usuários.
A8 - Armazenamento Criptográfico Inseguro	As aplicações Web raramente utilizam funções criptográficas de forma adequada para proteção de informações e credenciais. Os atacantes se aproveitam de informações mal protegidas para realizar roubo de identidade e outros crimes, como fraudes de cartões de crédito.
A9 - Comunicações inseguras	As aplicações frequentemente falham em criptografar tráfego de rede quando se faz necessário proteger comunicações críticas/confidenciais.
A10 - Falha de Restrição de Acesso à URL	Frequentemente, uma aplicação protege suas funcionalidades críticas somente pela supressão de informações como links ou URLs para usuários não autorizados. Os atacantes podem fazer uso desta fragilidade para acessar e realizar operações não autorizadas por meio do acesso direto às URLs.

OWASP :: Top Ten 2007



OWASP :: Top Ten 2017

A1 - Injeção de Código (INJECTION): Permitir que dados não confiáveis sejam enviados como parte de um comando ou consulta

O QUE É ISSO?

Websites e aplicativos ocasionalmente precisam executar comandos no banco de dados ou sistema operacional para adicionar ou excluir dados, executar um script ou iniciar outros aplicativos. Se as entradas não forem verificadas podem ser adicionadas uma “cadeia de comandos” ou um “comando completo de” banco de dados, e assim os atacantes podem lançar comandos à vontade para assumir o controle de um servidor, dispositivo ou dados.

COMO FUNCIONA?

Se um site, aplicativo ou dispositivo incorporar a entrada do usuário em um comando, o invasor pode inserir um comando “completo" diretamente na entrada mencionada. Se essa entrada não é verificado, um invasor "injeta" e executa seus próprios comandos.

POR QUE É RUIM?

Depois que os invasores puderem fazer comandos, eles poderão controlar seu website, aplicativos, e dados.

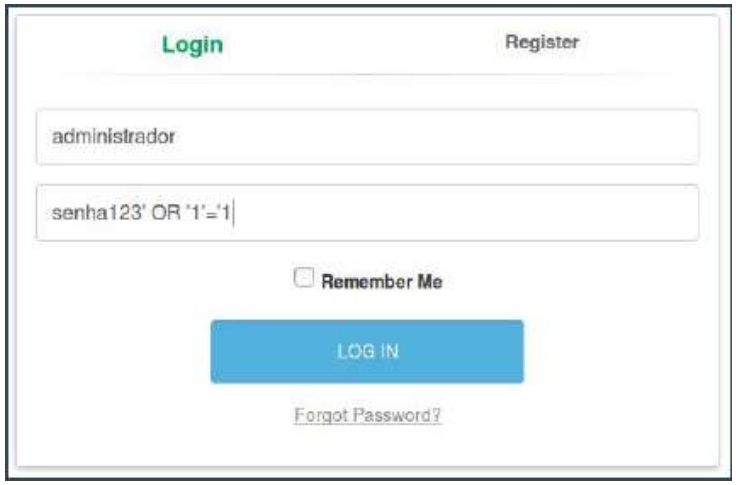
FATOS OCORRIDOS

A injeção de SQL foi aproveitada no infame hack da Sony Pictures em 2014, quando suspeitos operários norte-coreanos obtiveram acesso a dados confidenciais. De acordo com a US-CERT, os invasores usaram uma ferramenta Worm de bloqueio de mensagem de servidor para instalar vários componentes maliciosos, incluindo um *backdoor* e outras ferramentas destrutivas.

OWASP :: Top Ten 2017

- Injeção de códigos, seja de Sistema Operacional, de SQL, de LDAP ou de linguagem interpretada (PHP/ASP).
- Impacto:
  - Executar códigos diretamente no Servidor;
  - Acesso e modificação de Informações Internas;
  - Comprometimento do Sistema.

```
SELECT * FROM USUARIOS
WHERE USERNAME = 'administrator' AND
PASSWORD = 'senha123' OR '1'=1;
```




```
SELECT * FROM PESSOAS WHERE NOME LIKE '%%%'
```

OWASP :: Top Ten 2017

A2 - Quebra de Autenticação e gerenciamento de sessão (BROKEN AUTHENTICATION): Funções de autenticação (quebra de autenticação) e gerenciamento de sessão implementadas incorretamente.

O QUE É ISSO?

Autenticação é o processo para garantir que você realmente esteja acessando contas e dados. Geralmente, é facilitado por um nome de usuário e senha combinação, mas a complexidade é adicionada quando as pessoas esquecem ou mudam senhas ou deseja atualizar seus endereços de e-mail. Fica ainda mais complexo como um site, aplicativo ou dispositivo em si torna-se maior, mais amplo e mais conectado com outros sites, aplicativos ou dispositivos.

COMO FUNCIONA?

Nos ataques mais simples, as senhas podem ser adivinhadas ou roubadas se deixadas desprotegidas. À medida que as complexidades são adicionadas, os invasores podem encontrar outras áreas nas quais as credenciais do usuário ou as sessões têm proteções inadequadas e, em seguida, sequestram o acesso de um usuário e eventualmente, seus dados.

POR QUE É RUIM?

Se os invasores puderem sequestrar a sessão de um usuário ou administrador, eles terão acesso a tudo disponível nessa conta, desde dados até o controle da conta

FATOS OCORRIDOS

Os exemplos mais simples dessa vulnerabilidade são armazenar credenciais de usuário sem criptografia ou permitir que sejam facilmente adivinhadas. Outros exemplos incluem o uso de IDs de sessão na URL e a ativação de tempos limites de sessões excessivamente longos.

OWASP :: Top Ten 2017

- Sessões de usuários que não expiram, *tokens* transmitidos na URL, credenciais armazenadas de modo inseguro.
- Impacto:
  - Acesso a informações de outros usuários;
  - Escalonamento de Privilégios.

http://minh1a5loja.com.br/meucarrinho?sessionid=A2017031223110001

OWASP :: Top Ten 2017

A3 - Exposição de Dados Sensíveis (SENSITIVE DATA EXPOSURE): Muitas tecnologias da Web não foram projetadas para lidar com transferências de dados pessoais ou financeiros.

O QUE É ISSO?

Dados confidenciais, como números de cartão de crédito, dados de integridade ou senhas, tem proteção extra, dado o potencial de danos se cair no erro mãos. Existem até regulamentações e padrões projetados para proteger dados. Mas, se dados sensíveis forem armazenados, transmitidos ou protegidos por métodos, pode ser exposto a invasores.

COMO FUNCIONA?

Se os dados forem armazenados ou transferidos como texto simples, se a criptografia mais antiga / mais fraca usado, ou se os dados forem descriptografados de maneira descuidada, os invasores podem obter acesso e explorar os dados.

POR QUE É RUIM?

Uma vez que um atacante tem senhas e números de cartão de crédito, eles podem fazer dano real

FATOS OCORRIDOS

Os roteadores sem fio oferecem proteções de dados notoriamente fracas. Pesquisadores descobriram que a criptografia que protege o WPA2, o padrão da indústria, expõe os dados e permite que sejam lidos ou manipulados à medida que são transferidos sem fio.

OWASP :: Top Ten 2017

- Exposição de dados e informações da aplicação, como arquivos de backup, de configuração e de senhas.
- Impacto:
  - Acesso a informações e arquivos internos;
  - Listagem de informações.

inurl:sitevulneravel.com intext:"index of"

OWASP :: Top Ten 2017

A4 - XML ETERNAL ENTITIES: “Entidades” XML podem ser usadas para solicitar dados ou arquivos locais.

O QUE É ISSO?

XML é um formato de dados usado para descrever diferentes elementos de dados. XML também é usado em “Entidades” para ajudar a definir dados relacionados, mas para que as entidades podem acessar conteúdo, tão inofensivo quanto puxar o preço atual das ações de um site de terceiros. As entidades podem, no entanto, ser usadas para solicitar dados ou arquivos locais, que ser devolvido - mesmo que esses dados nunca tenham sido destinados ao acesso externo.

COMO FUNCIONA?

Um invasor envia valores de pesquisa de dados maliciosos solicitando o site, o dispositivo ou o aplicativo para solicitar e exibir dados de um arquivo local. Se um desenvolvedor usa um nome de arquivo padrão em um local comum, o trabalho de um invasor é fácil.

POR QUE É RUIM?

Os invasores podem obter acesso a todos os dados armazenados localmente ou podem atacar outros sistemas internos.

FATOS OCORRIDOS

O clássico ataque de “*Billion L’aughs*” explora o XXE definindo 10 elementos que se referem uns aos outros, excedendo rapidamente qualquer memória disponível e interrompendo serviços inteiros.

OWASP :: Top Ten 2017

A5 - Falta de Função para Controle de Nível de Acesso (BROKEN ACCESS CONTROL): Regras indevidas do que os usuários autenticados “podem fazer”.

O QUE É ISSO?

O controle de acesso, ou autorização, é como os aplicativos da web permitem que usuários diferentes acessem diferentes conteúdos, dados ou funções. É como o Netflix limita as pessoas ao seu plano "padrão" para conteúdo em HD, enquanto os usuários "premium" podem assistir a 4K. Quando está quebrado, você pode acessar mais do que deveria.

COMO FUNCIONA?

Às vezes, obter acesso não autorizado é tão simples quanto inserir manualmente um URL não vinculado em um navegador, como http://example.com/admin.

POR QUE É RUIM?

Assim como outras vulnerabilidades, os invasores podem acessar (e modificar) dados, contas e funções que não deveriam.

FATOS OCORRIDOS

Uma plataforma de reunião na Web, o Fuze, possibilitou o acesso à reunião por meio de um URL simples que termina com um número incremental de sete dígitos. O uso de qualquer número forneceu acesso a replays da reunião correspondente. Como os URL’s estavam desprotegidos, o conteúdo era indexado por - e pesquisável pelos - mecanismos de pesquisa populares.

OWASP :: Top Ten 2017

- A aplicação não valida se o usuário esta logado para enviar as informações para ele.
- Impacto:
  - Exposição de dados para usuários sem permissões;
  - Quebra da Confidencialidade da Informação.

http://site1v5ulneravel.com/intranet/tmp/procedimento_interno.jpg

OWASP :: Top Ten 2017

A6 - Configuração Incorreta de Segurança (SECURITY MISCONFIGURATION)

Configurações manual, ad hoc, insegura ou falta de segurança que permitem acesso não autorizado

O QUE É ISSO?

Exatamente o que o nome indica, a configuração incorreta da segurança é quando você ignorou algumas vulnerabilidades. Isso inclui o uso de credenciais padrão, deixando os arquivos desprotegidos em servidores públicos, com falhas conhecidas, mas sem correção, e mais, e em qualquer camada da pilha de software. Em outras palavras, a culpa é sua.

COMO FUNCIONA?

As pessoas ficam ocupadas, as coisas são perdidas, as decisões de priorização são tomadas ... e as vulnerabilidades são deixadas sem controle.

POR QUE É RUIM?

Facilita que até mesmo invasores iniciantes encontrem e acessem seus valiosos sistemas e dados. Felizmente, a maioria desses tipos de vulnerabilidades também é fácil de encontrar e corrigir.

FATOS OCORRIDOS

O botnet Mirai de 2016 contava com credenciais padrão inalteradas (como um login de "admin" e uma senha de "1234") de pouco mais de 60 dispositivos IoT específicos. Quando explorada, eventualmente infectou quase 400.000 unidades de apenas 60 dispositivos desprotegidos.

OWASP :: Top Ten 2017

- Configurações incorretas que expõem informações da aplicação, como versão do Servidor ou Sistema Operacional, “Index of” aberto, SSL utilizando cifras consideradas fracas.
- Impacto:
  - Conhecimento das aplicações;
  - Possibilidade de efetuar ataques direcionados;
  - Exposição de Informações Sensíveis.

```
HTTP/1.1 200 OK
Connection: close
Date: Sun, 19 Mar 2017 23:09:06 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Set-Cookie: PHPSESSID=02i7lr56hkbrfk62eodjbill51
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Set-Cookie: PHPSESSID=kvkvd2hj9emr0ku6dgm5e80bc6
Content-Type: text/html
Content-Length: 0
```

$ curl -IsL sitevulneravel.com.br

OWASP :: Top Ten 2017

A7 - CROSS-SITE SCRIPTING (XSS): Um aplicativo da web inclui dados não confiáveis em uma nova página da web sem a devida validação

O QUE É ISSO?

O XSS permite que códigos mal-intencionados sejam adicionados a uma página da Web ou aplicativo, por meio de comentários de usuários ou envios de formulários usados ??para definir a ação subsequente. Como o HTML mistura instruções de controle, formatação e o conteúdo solicitado no código-fonte da página da Web, permite que uma oportunidade de código não-anulado seja usada na página resultante.

COMO FUNCIONA?

Quando uma página da Web ou aplicativo utiliza conteúdo inserido pelo usuário como parte de uma página resultante sem verificar coisas ruins, um usuário mal-intencionado pode inserir conteúdo que inclua entidades HTML.

POR QUE É RUIM?

Os invasores podem alterar o comportamento de um aplicativo, direcionar dados para seus próprios sistemas ou corromper ou substituir dados existentes.

FATOS OCORRIDOS

As explorações de XSS foram relatadas por mais de 20 anos e afetaram o Twitter, o Facebook, o YouTube e muitas, muitas outras. Estas vulnerabilidades são um “assunto sem fim”, mas alguns “vitórias” já forma atingidas, tal como a Adobe e o WordPress corrigiram diversas vulnerabilidades de XSS recentemente, em novembro de 2017.

OWASP :: Top Ten 2017

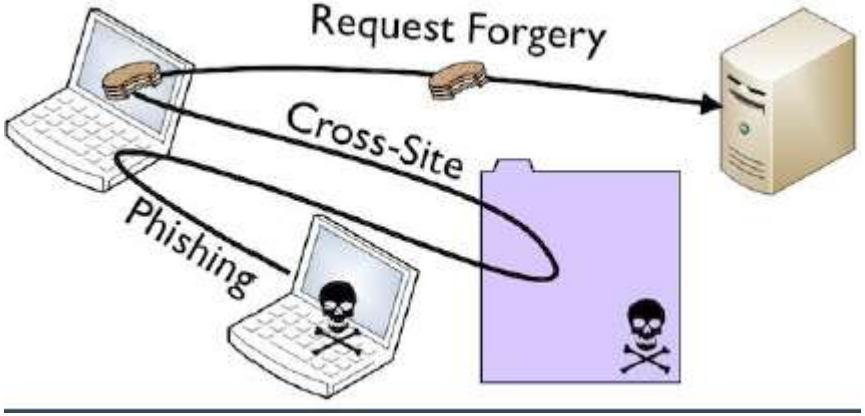
- Execução de ataques diretamente no usuário final.
- Impacto:
  - *Phishing;*
  - Redirecionamento para páginas maliciosas;
  - Roubo de credenciais e sessão;
  - Print-screen da tela;
  - *Pastejacking.*

http://minhaloja.com.br/busca?=<script>prompt("Digite sua senha abaixo para continuar navegando")</script>

OWASP :: Top Ten 2017

Cross-Site Request Forgery (CSRF)

- O usuário clica em um link malicioso, enquanto estava logado na aplicação. O link malicioso efetua uma ação na aplicação sem o consentimento do usuário.
- Impacto:
  - Requisições sem o conhecimento do usuário
  - Modificação de informações da aplicação através de *Phishing*



http://sitevulneravel.com/intranet/new_user.php

OWASP :: Top Ten 2017

Redirecionamentos e Encaminhamentos Inválidos

- Redirecionamento para páginas maliciosas sem o consentimento do usuário
- Impacto:
  - Ataques ao usuários utilizando técnicas de *Phishing*

http://aplicacaovulneravel.com/redirect.php?url=http://atacante.com

OWASP :: Top Ten 2017

A8 – DESERIALIZAÇÃO INSEGURA (INSECURE DESERIALIZATION) / Referencia Insegura e Direta a Objeto: Recebimento de objetos serializados hostis resultando em execução remota de código

O QUE É ISSO?

Antes que os dados sejam armazenados ou transmitidos, os bits geralmente são serializados para que possam ser restaurados posteriormente à estrutura original dos dados. A remontagem de uma série de bits em um arquivo ou objeto é chamada desserialização.

COMO FUNCIONA?

Os dados desserializados podem ser modificados para incluir códigos maliciosos, o que provavelmente causará problemas se o aplicativo não verificar a origem ou o conteúdo dos dados antes da desserialização.

POR QUE É RUIM?

Os invasores podem criar objetos ilegítimos que executam comandos em um aplicativo infectado.

FATOS OCORRIDOS

Durante 2015 e 2016, a desserialização insegura foi encontrada em tantas aplicações Java, incluindo uma no PayPal, que essa "onda de vulnerabilidade" foi apelidada de "*Deserialization Apocalypse Java*".

OWASP :: Top Ten 2017

- Arquivos utilizando numerações sequenciais, id de usuários sequenciais, “ocultação” incorreta de dados.
- Impacto:
  - Acesso a dados confidenciais;
  - Escalonamento de privilégios.

http://minhaloja.com.br/boletos/boleto386.pdf

OWASP :: Top Ten 2017

A9 - Utilização de Componentes Vulneráveis Conhecidos (USING COMPONENTS WITH KNOWN VULNERABILITIES): Encontrar e explorar vulnerabilidades já conhecidas antes de serem corrigidas

O QUE É ISSO?

Quando as vulnerabilidades se tornam conhecidas, os fornecedores geralmente as corrigem com um patch ou atualizar. O processo de atualização do software elimina ou mitiga vulnerabilidade.

COMO FUNCIONA?

Às vezes, as organizações não conseguem manter o software atualizado, especialmente se pilhas são grandes ou complexas, ou se exigiria um compromisso significativo para validar seus sistemas ou produtos após uma atualização. Quando uma façanha é feita público ou um patch é lançado, os atacantes sabem que algumas organizações não agirão imediatamente. Os atacantes agora têm uma janela, de dias a anos, para procurar sistemas ou aplicativos em que a vulnerabilidade conhecida ainda está em vigor.

POR QUE É RUIM?

Como são informações públicas, os invasores têm um caminho recomendado para explorar e as organizações têm pouca desculpa para deixar o caminho aberto.

FATOS OCORRIDOS

O ex-CEO da Equifax, ao testemunhar perante o Congresso sobre sua infame violação de 2017, culpou alguém da TI, afirmando que "o erro humano era que o indivíduo responsável pela comunicação para a organização que deveria ter sido aplicado o *patch*, e ele não o fez".

OWASP :: Top Ten 2017

- Utilização de aplicações, bibliotecas e ferramentas desatualizadas.
- Impacto:
  - Possibilidade de existir uma vulnerabilidade conhecida publicamente e explorável

https://wpvu1ln5db.com/

OWASP :: Top Ten 2017

As 10 vulnerabilidades de segurança mais críticas em aplicações WEB

A10 - "Traços de Auditoria" e monitoramento insuficiente (INSUFFICIENT LOGGING AND MONITORING): Um monitoramento insuficiente permite que os invasores trabalhem sem serem notados.

O QUE É ISSO?

Se você não está procurando invasores ou atividades suspeitas, não os encontrará.

COMO FUNCIONA?

Softwares e sistemas têm habilidades de monitoramento para que as organizações possam ver logins, transações, tráfego e muito mais. Ao monitorar atividades suspeitas, como logins com falha, as organizações podem ver e interromper atividades suspeitas.

POR QUE É RUIM?

Os invasores contam com a falta de monitoramento para explorar as vulnerabilidades antes que elas sejam detectadas. Sem o monitoramento e o registro para verificar o que aconteceu, os invasores podem causar danos agora e no futuro.

FATOS OCORRIDOS

O registro não é importante apenas para identificar ataques em andamento; Ele pode ajudar com a análise forense após um ataque ter sido bem sucedido.

Ferramentas :: OWASP Zed Attack Proxy Project

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

- O ZAP pode ajudá-lo a encontrar automaticamente vulnerabilidades de segurança em seus aplicativos da Web enquanto você desenvolve e testa seus aplicativos. É também uma ótima ferramenta para os pentesters experientes usarem para testes de segurança manuais.

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

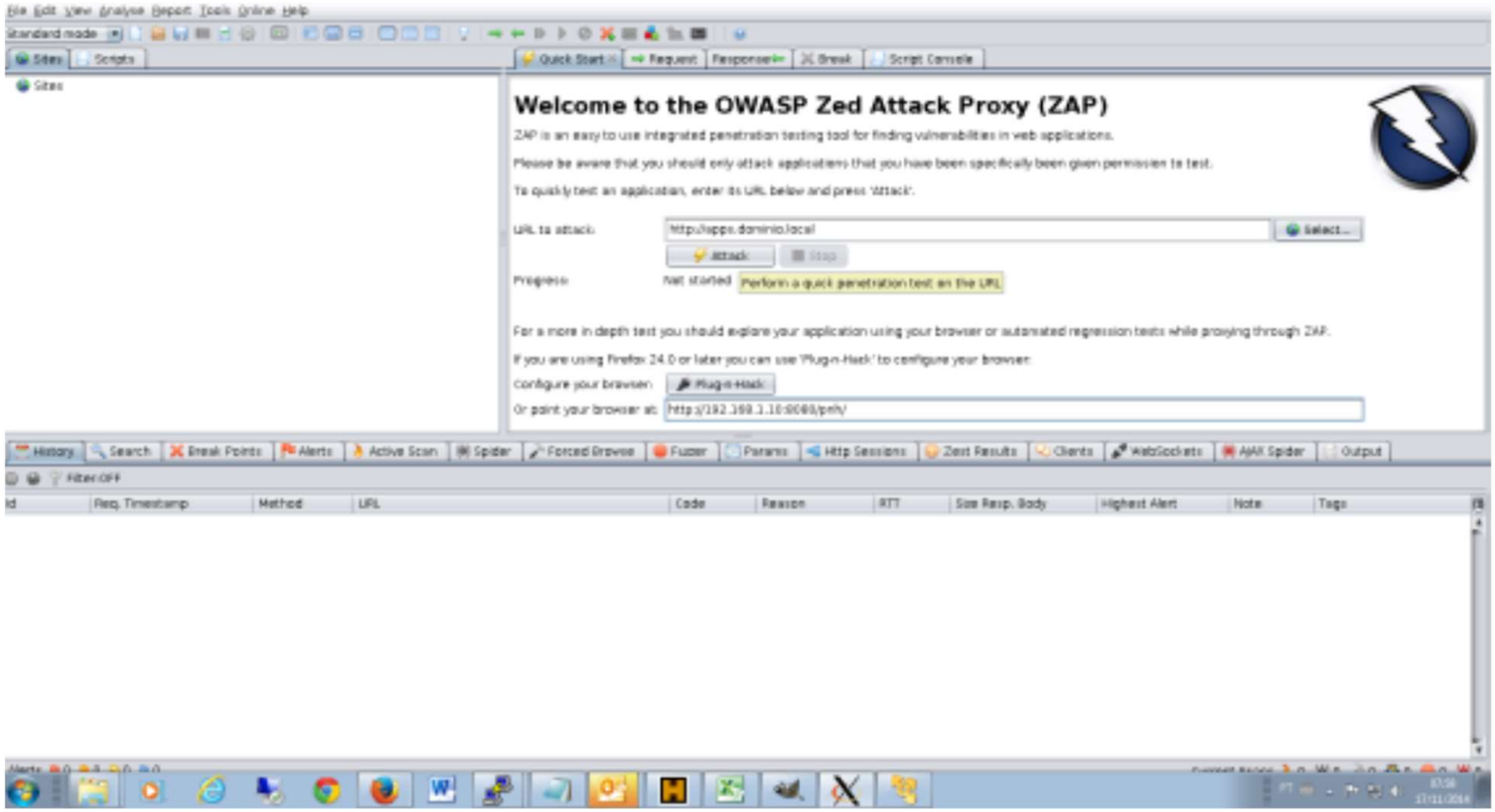
https://github.com/zaproxy/zaproxy/releases/download/2.6.0/ZAPGettingStartedGuide-2.6.pdf

Ferramentas :: OWASP ZAP

- Opensource multiplataforma, com versão em português
- Iniciativa apoiada por grandes empresas (Microsoft, Google, Mozilla, Ernst & Young, dentre outras)
- Possui scanners automatizados
- Conjunto de ferramentas para encontrar vulnerabilidades manualmente.
- Perfis pré-definidos que trazem alguns plug-ins selecionados de acordo com a finalidade do perfil
  - Trabalha sobre o OWASP_TOP10
  - audit_high_risk
  - bruteforce
  - fast_scan
  - full_audit

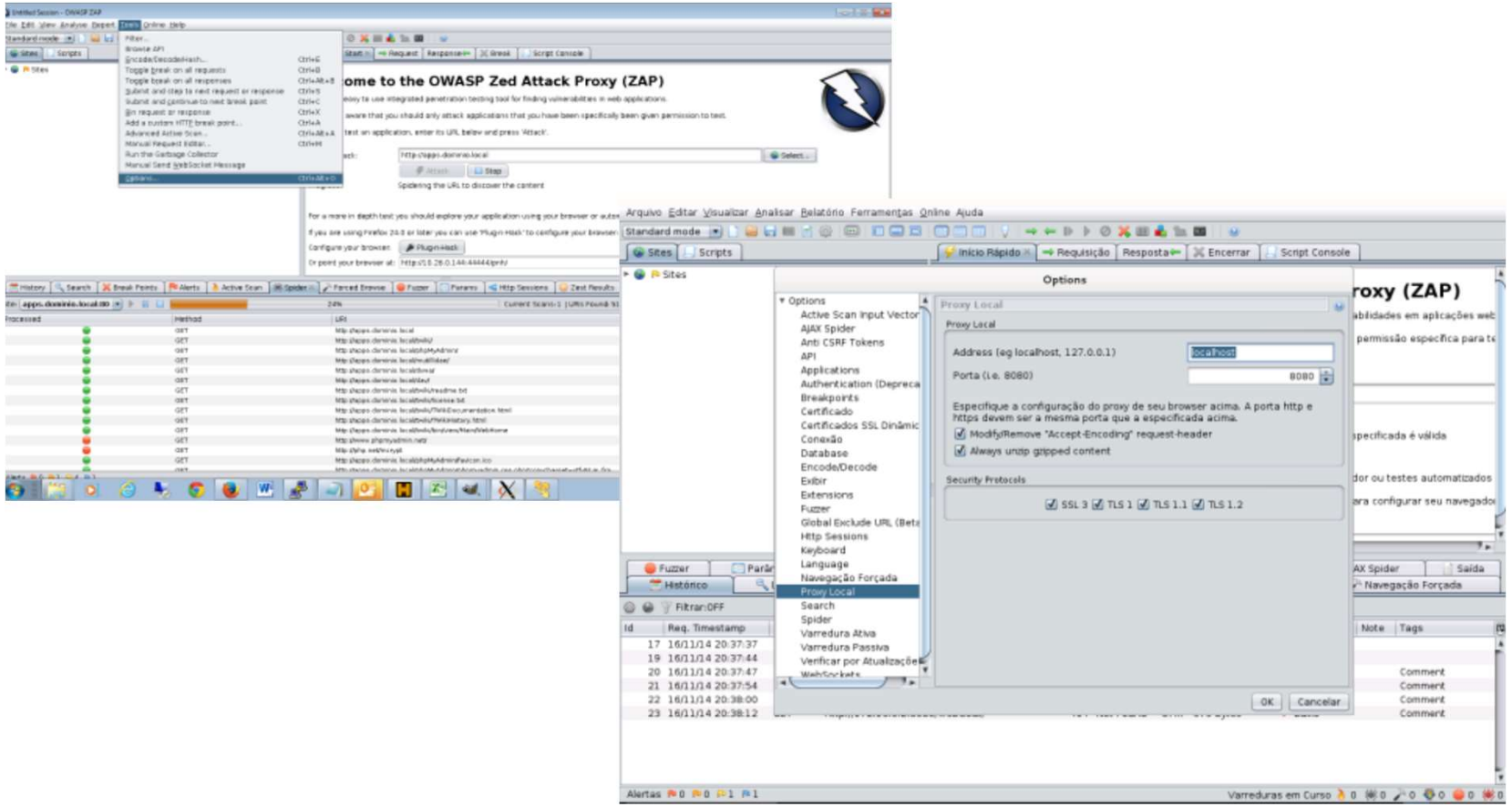
Ferramentas :: OWASP ZAP

Tela Inicial



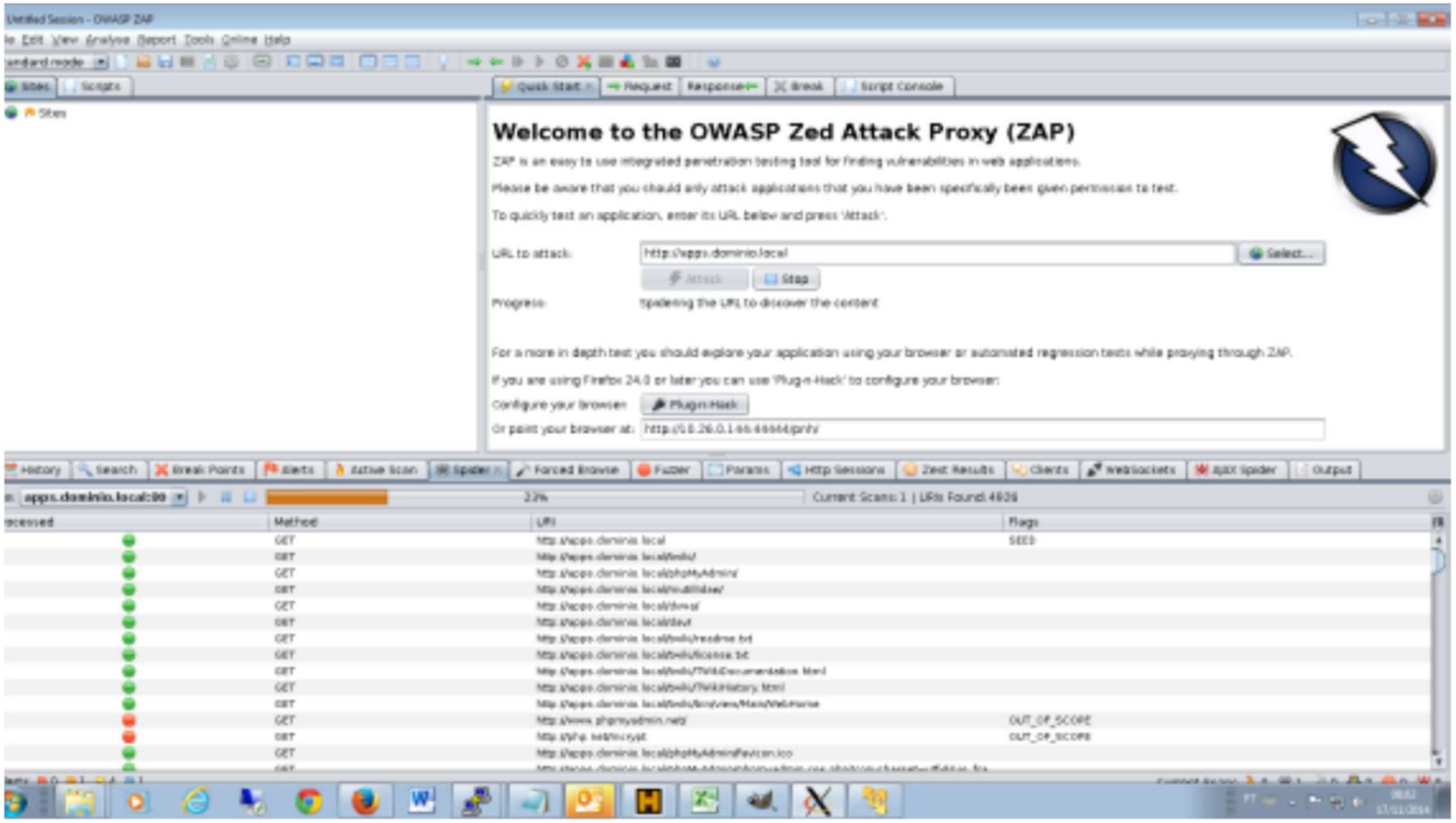
Ferramentas :: OWASP ZAP

Configurações de Proxy



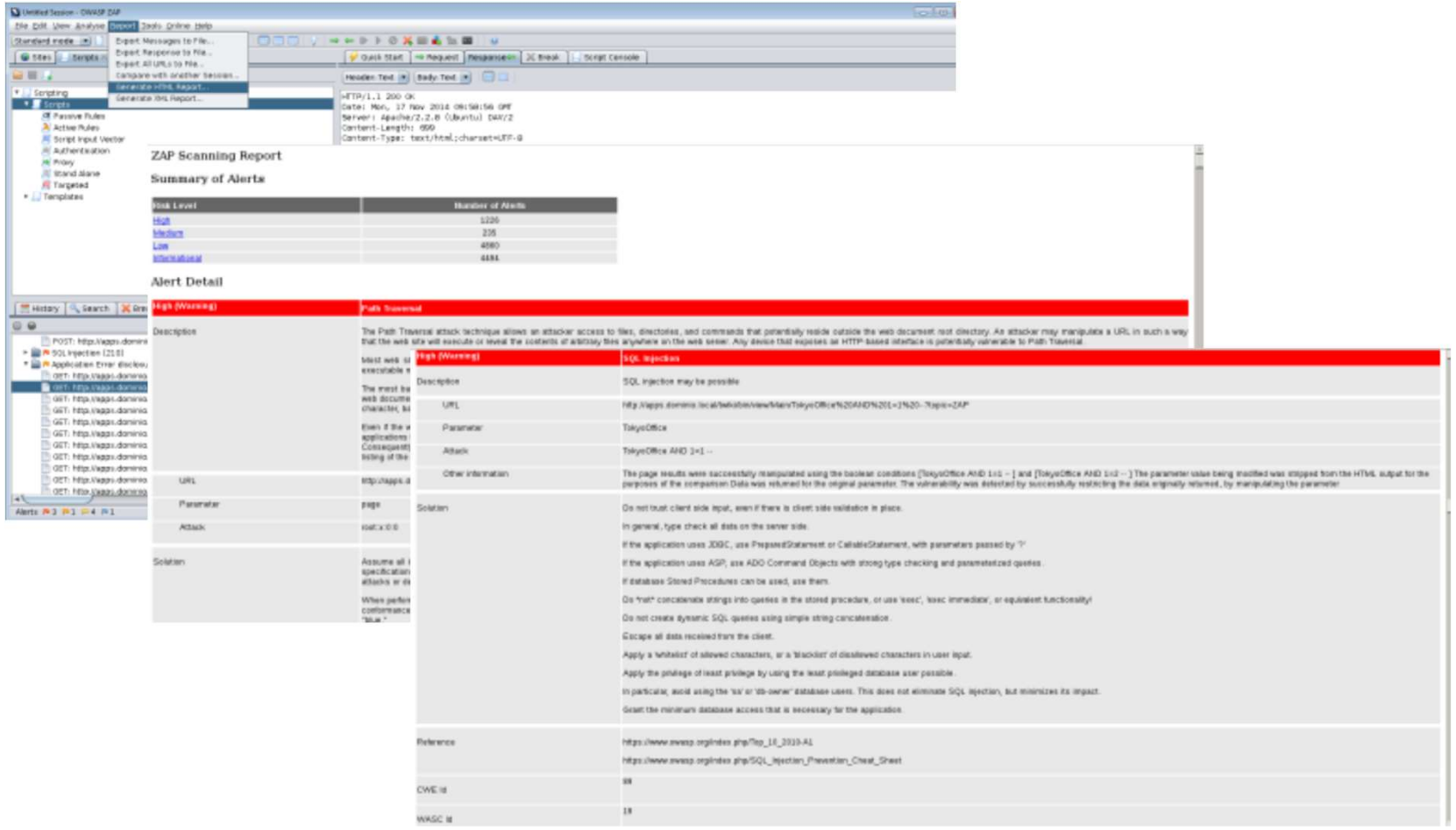
Ferramentas :: OWASP ZAP

Execução do Scan



Ferramentas :: OWASP ZAP

Geração do Relatório



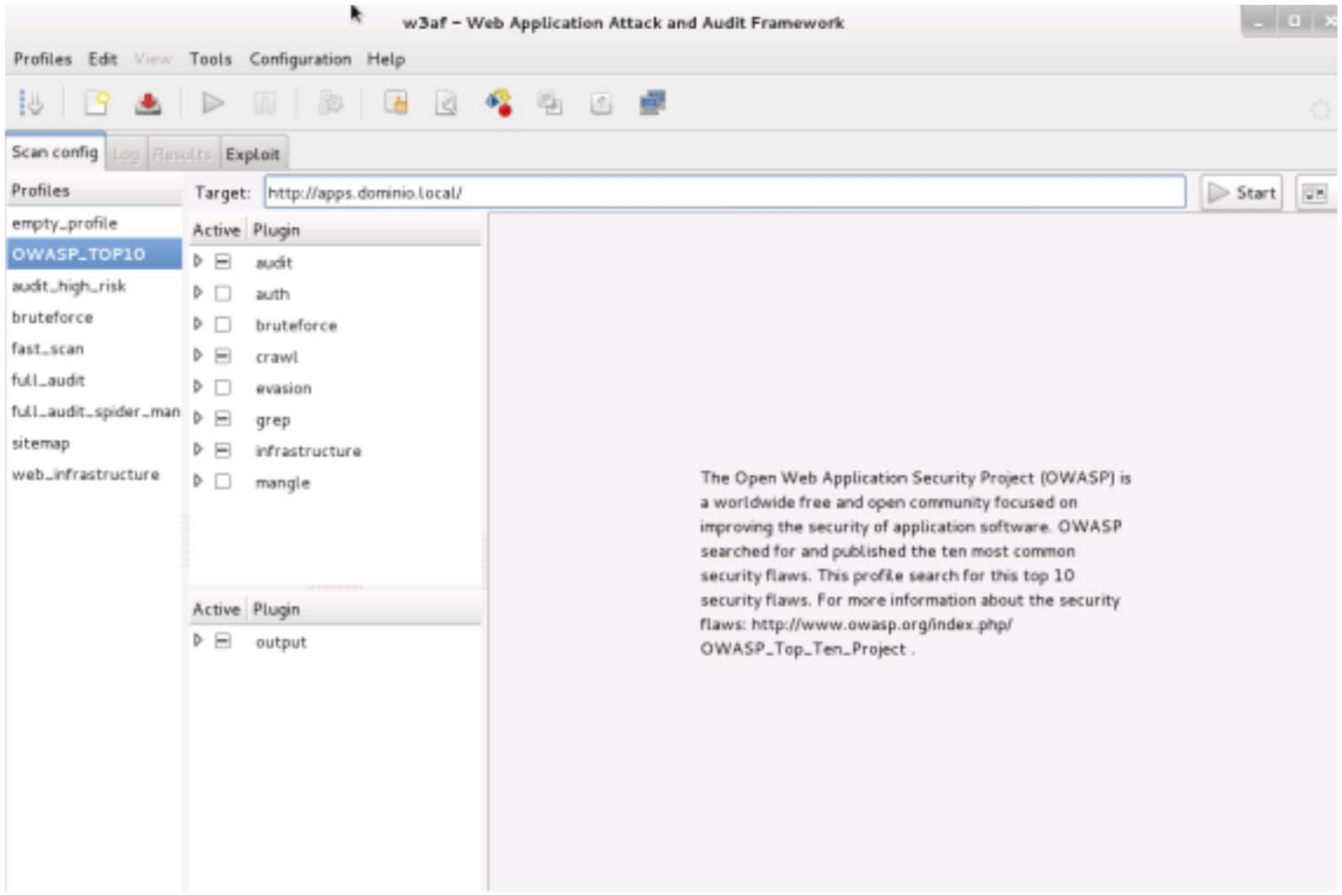
Ferramentas :: Web Application Attack and Audit Framework (W3AF)

- Desenvolvido em Python
- Interface gráfica e linha de comando
- Multiplataforma (Windows, Linux, Mac, FreeBSD e OpenBSD)
- Arquitetura
  - Core
  - Interface de usuário
  - Plugins

http://w3af.org/

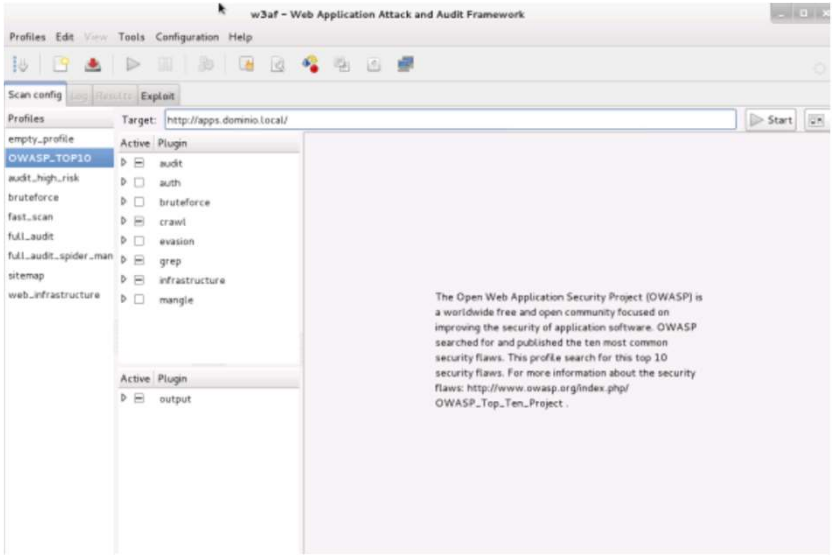
Ferramentas :: OWASP Zed Attack Proxy Project

Interface Gráfica: Executável w3af_gui



Ferramentas :: OWASP Zed Attack Proxy Project

Interface Gráfica



Perfil	Descrição
empty_profile	É um perfil vazio, sem nenhum plug-in selecionado. Pode ser usado como ponto de partida para a definição de um novo perfil.
OWASP_TOP10	Estão habilitados os plug-ins que detectam as vulnerabilidades contidas no relatório anual TOP10 da OWASP
audit_high_risk	Estão habilitados os plug-ins que detectam vulnerabilidades de maior risco, tais como SQL Injection, upload inseguro de arquivos etc.
bruteforce	Estão habilitados os plug-ins que executam ataques de força bruta, usando credenciais padrões
fast_scan	Estão habilitados alguns plug-ins de descoberta e os plug-ins de auditoria mais rápidos
full_audit	Permite executar uma auditoria completa. A descoberta de novas URLs é feita pelo plug-in web_spider
full_audit_spider_man	Permite executar uma auditoria completa. A descoberta de novas URLs é feita pelo plug-in spider_man(proxy)
sitemap	Estão habilitados apenas os plug-ins que permitem a criação de um mapa do sistema alvo
web_infraestructure	Estão habilitados os plug-ins relacionados à descoberta de informações da infraestrutura do sistema alvo. Exemplos: descoberta de virtual hosts, versão do sistema operacional, detecção de proxy reverso etc.