ESCOLA TÉCNICA PROFESSOR MASSUYUKI KAWANO

Técnico em Informática

Lucas Palomo Rosa

Matheus Gonçalves dos Santos

Matheus Sena dos Santos

Rayssa Thainá Kataoka de Carvalho Silva

PENTEST-Verificação de Segurança em Web Sites

Tupã - SP
2017

Lucas Palomo Rosa

Matheus Gonçalves dos Santos

Matheus Sena dos Santos

Rayssa Thainá Kataoka de Carvalho Silva

PENTEST-Verificação de Segurança em Web Sites

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em informática da Etec Professor Massuyuki Kawano, orientado pelo Prof. Anderson Tukiyama Berengue e Wesley Pinho e Silva Carçado como requisito parcial para obtenção do título de técnico em Informática.

Tupã - SP
2017

É de inteira responsabilidade o conteúdo do trabalho apresentado pelo aluno. O Professor, a Banca de Validação e a instituição não são responsáveis e nem endossam as ideias e o conteúdo do mesmo.

Dedicatória

Dedicamos este trabalho primeiramente a Deus, aos nossos pais e a todos os amigos, a toda a equipe de professores competentes, por esse novo desafio que será mais uma conquista em nossas vidas!

Agradecimento

Agradecemos a Deus pela força que nos tem dado até a conclusão do curso.
Agradecemos em especial aos professores Rodrigo Riquena e Guilherme Henrique e aos demais Docentes do Curso Técnico de Informática pela dedicação, sempre incentivando-nos e nos ensinando a desenvolver sempre o melhor para adquirirmos competências e habilidades; pela generosidade e confiança depositada em nós diante de todos os momentos difíceis e por compartilhar de seus conhecimentos profissionais e humanos.

RESUMO

Com a expansão da informatização em diversas áreas, a manipulação e a segurança das informações tendem a evoluir no setor de TI, isto gera um grande mercado carente para profissionais em segurança digital, é um fato triste saber que grande parte do mercado que utiliza de tecnologia para sobreviver não investe na segurança digital. Podemos dizer que o pentest é uma área que cresce no ramo de segurança digital, os profissionais pentesters são especialistas em realizar testes de intrusão em redes, estes testes simulam ataques de uma verdadeira invasão no sistema a procura de falhas que podem ser exploradas pelo invasor. Este trabalho tem como foco ajudar a área de segurança digital desenvolvendo uma ferramenta que possa ser usada por qualquer usuário com o intuito de proteger as informações contidas em um web site.

Palavras-Chave: Pentest, Ferramenta, Invasão, Segurança , Proteger.

Lista de ilustrações

Sumário

1.Introdução

Com a expansão da informatização, a segurança das informações ficam cada vez mais importante, muitas empresas acabam deixando isto em segundo plano por variados motivos que incluem, custo para uma equipe de segurança em tecnologia, achar que não vai sofrer algum tipo de ataque, outra possibilidade também para deixar a segurança defasada é confiarem completamente que os softwares fornecidos para a empresa são totalmente seguros, o que acaba facilitando o acesso de dados sigilosos a pessoas mal intencionadas.
O pentest é um meio de fortalecer a segurança da empresa através de uma realização de testes de vulnerabilidades, onde é possível detectar a vulnerabilidade e a gravidade do mesmo, o pentest é dividido em três etapas as quais são o reconhecimento, penetração e obtenção de dados, qualquer pessoa pode realizar um pentest porém é recomendável contratar um profissional qualificado para este tipo de teste, a empresa Eccouncil[1] fornece a certificação necessária para se tornar um Hacker Ético.

O programa visa á agilidade e a praticidade em realizar estes testes poupando tempo, ele realiza o pentest em servidores e desktop: Linux e Windows e depois traz um relatório exibindo a gravidade e a vulnerabilidade encontrada, o software é desenvolvido na linguagem de programação Java, sendo assim, executável em qualquer sistema operacional.

O Pentest é uma série de testes para checar vulnerabilidades em servidores, sites e sistemas que podem ser exploradas por pessoas de má-fé do qual também será possível identificar a gravidade do perigo que este alvo possui.

O programa identificar falhas cruciais que podem comprometer os dados e segurança da empresa. O programa é dividido por módulos cada um com seus tipos de teste que no final retorna um relatório com o nível da falha, baseado nas vulnerabilidades encontradas, como por exemplo:

Digamos que uma empresa “X”, trabalha com dados privados de pessoas físicas e pessoas jurídicas, estes dados são armazenados em um servidor e esta empresa nunca adquiriu conhecimento sobre a segurança desse servidor, certo dia um pessoa mal intencionada realiza um vazamento desses dados através de acesso a esse servidor. No entanto, se essa empresa tivesse realizado um Pentest, possivelmente, teria evitado o vazamento dessas informações, pois teria providenciado as possíveis correções conforme as falhas encontradas.

O Software visa combater esse tipo de falhas existente no mundo digital, onde muitas empresas não se importam com os dados cadastrados de seus clientes e quem tem um alto valor de comércio nos dias atuais. Há maioria das empresas só buscam essa prevenção logo após sofre um tipo de ataque devastador.

.

[1] Eccouncil: Empresa focalizada em segurança da informação , seu foco é certificar “hackers éticos”. CertifiedEthical Hacker (“ certificado de hacker ético”), o certificado CEH é válido mundialmente e possui um grande valor no mercado de trabalho.

1.1 Definição de Hacker:

Hacker ético : na maioria dos casos contém uma certificação sobre segurança digital, seus ideais são achar as vulnerabilidades de um site ou sistema operacional (SO) e reportando ao administrador.

Hacker antiético (Crack): usa seu conhecimento sobre sistemas para achar falhas em sites e S.O. , a conduta de um hacker antiético é penetrar em sites ou S.O. e alcançar níveis privilegiados e obstruir esta informação, o que é algo nada ético: extraviar informações para aproveitamento de forma ilícita.

Níveis de um pentest:

Reconhecimento: onde é necessário reconhecer o alvo, o reconhecimento pode ser dividido em duas categorias:

- White Box: Possui conhecimento sobre o alvo é focado em reconhecer vulnerabilidades que não estaria no foco de um invasor.

- Gray Box: Possui conhecimento parcial do alvo, é focado em reconhecer vulnerabilidades que esteja acessível a um invasor.

- Black Box: Nenhum conhecimento sobre o alvo, é focado em simular um invasor externo, checando as vulnerabilidades que poderiam ser exploradas facilmente.

Penetração: é o momento em que as vulnerabilidades começam a ser exploradas com o foco de “penetrar” entrar no sistema operacional.

Obtenção de dados: obtenção de dados através da vulnerabilidade encontrada no Pentest.

[2] S.O.: (Sistemas Operacionais)É o conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. O Sistema Operacional cria uma plataforma comum a todos os programas utilizados. Exemplos: Dos, Unix, Linux, Mac OS, OS-2, Windows NT.

2. Metodologia

O tema tem como foco identificar falhas de segurança em servidores partindo dos princípios de uma simulação de ataques externos usando teste como SQL Injection .Que serão representados em texto, para que isso seja possível foi necessário realizar pesquisas sobre intrusão de rede ,aprendendo técnicas como o SQL Injection entre outros ,também foi necessário aprofundar-se em técnicas de programação para web e desktop, utilizando também um breve aprofundamento em técnicas de programação com a linguagem Java e MySQL.

2.1 Objetivos

Este software tem como utilidade melhorar o desempenho economizando tempo e garantindo uma produtividade bem maior a equipe ou usuário final, o programa tem como objetivo mostrar a vulnerabilidade em portas e em sites, ele executa testes com o SQL Injection e o escaneamento de portas retornando um relatório contendo as falhas ;

2.2 Desenvolvimento do Software

2.2.1 Diagrama de Fluxo de Dados

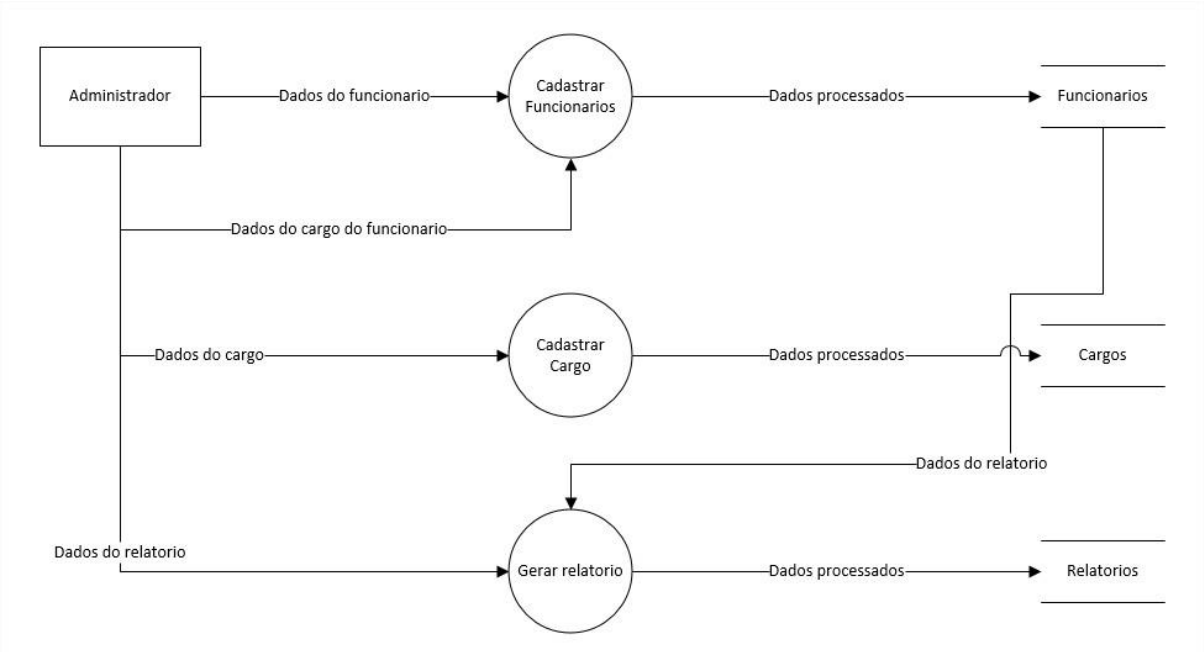

Figura 1:DFD 1

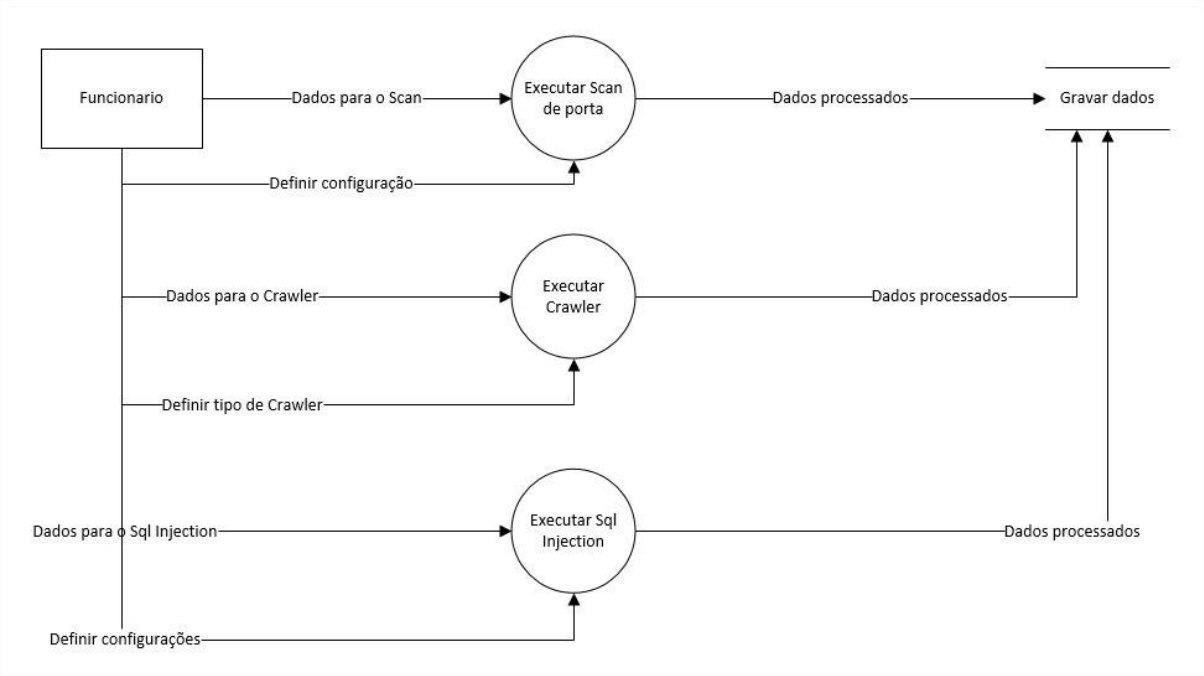

Figura 2:DFD 2

2.2.2 MER

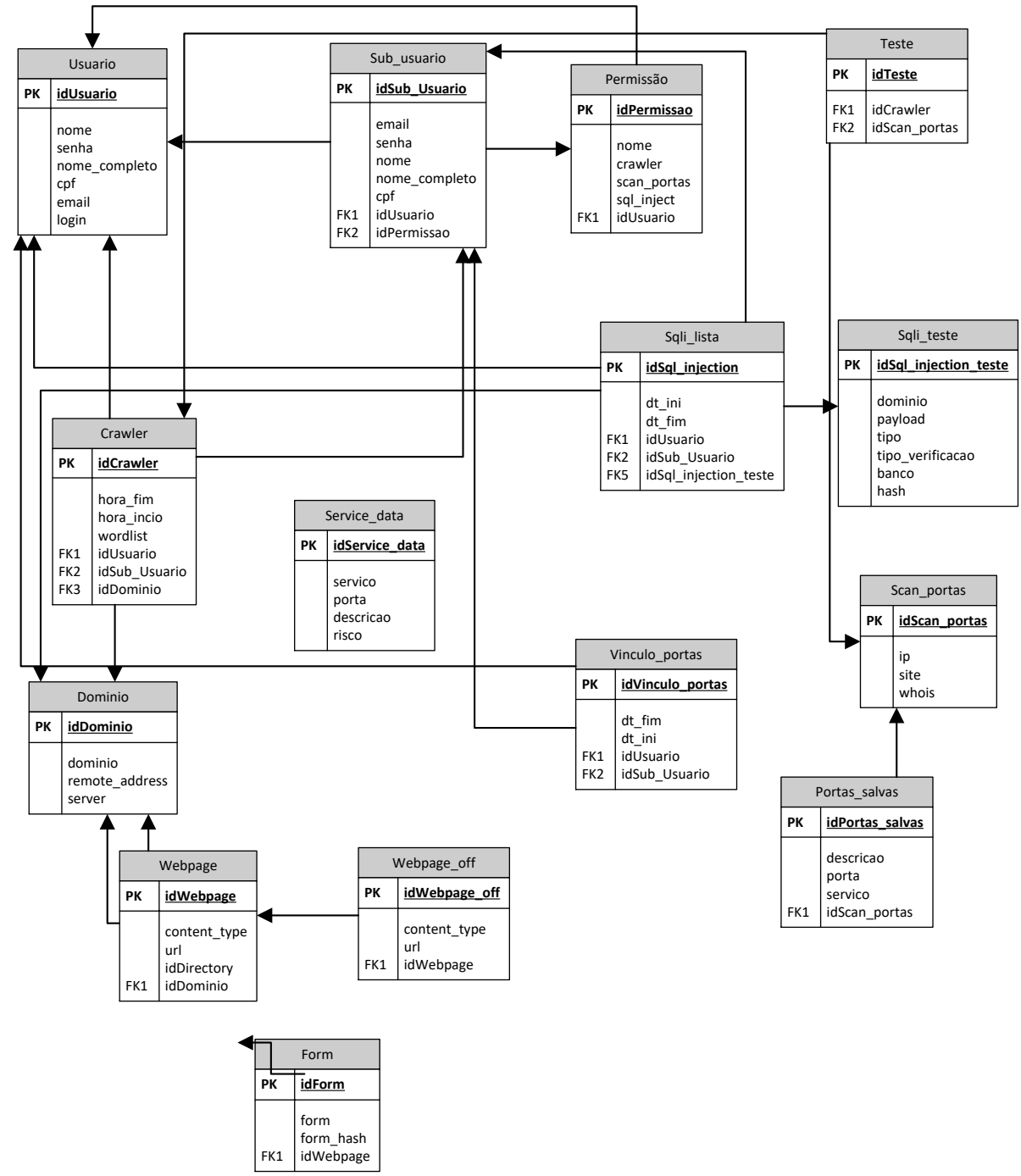

Figura 3:MER

2.2.3 Dicionário de Dados

crawler

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
hora_fim	datetime	Sim	*NULL*	
hora_inicio	datetime	Sim	*NULL*	
wordlist	varchar(255)	Sim	*NULL*	
id_dominio	bigint(20)	Sim	*NULL*	
id_sub_usuario	int(11)	Sim	*NULL*	
id_usuario	int(11)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	8	A	Não	
FK_crawler_id_sub_usuario	BTREE	Não	Não	id_sub_usuario	4	A	Sim	
FK_crawler_id_dominio	BTREE	Não	Não	id_dominio	8	A	Sim	
FK_crawler_id_usuario	BTREE	Não	Não	id_usuario	2	A	Sim	

dominio

Coluna	Tipo	Nulo	Predefinido	Comentários
ID	bigint(20)	Não		
DOMINIO	varchar(255)	Sim	*NULL*	
REMOTE_ADDRESS	varchar(255)	Sim	*NULL*	
SERVER	varchar(255)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	ID	22	A	Não	

Figura 4:Dicionário de Dados 1

form

Coluna	Tipo	Nulo	Predefinido	Comentários
ID	bigint(20)	Não		
FORM	varchar(20000)	Sim	*NULL*	
FORM_HASH	varchar(255)	Sim	*NULL*	
WEBPAGE_ID	bigint(20)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	ID	386	A	Não	
FK_form_WEBPAGE_ID	BTREE	Não	Não	WEBPAGE_ID	386	A	Sim	

permissao

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
Nome	varchar(255)	Sim	*NULL*	
id_usuario	int(11)	Sim	*NULL*	
crawler	tinyint(1)	Não		
scan_portas	tinyint(1)	Não		
sql_inject	tinyint(1)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	14	A	Não	
id_usuario	BTREE	Não	Não	id_usuario	14	A	Sim	

Figura 5:Dicionário de Dados 2

portas_salvas

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
descricao	varchar(255)	Sim	*NULL*	
porta	varchar(255)	Sim	*NULL*	
servico	varchar(255)	Sim	*NULL*	
id_scan_portas	int(11)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	969	A	Não	
FK_portas_salvas_id_scan_portas	BTREE	Não	Não	id_scan_portas	161	A	Sim	

scan_portas

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
ip	varchar(255)	Sim	*NULL*	
site	varchar(255)	Sim	*NULL*	
whois	varchar(5000)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	84	A	Não	

Figura 6:Dicionário de Dados 3

service_data

Coluna	Tipo	Nulo	Predefinido	Comentários
Servico	varchar(36)	Sim	*NULL*	
Porta	int(11)	Sim	*NULL*	
Descricao	varchar(206)	Sim	*NULL*	
Risco	varchar(255)	Sim	Indeterminado	
id	int(11)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	65274	A	Não	

sql_injection

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
dt_ini	datetime	Não		
dt_fim	datetime	Não		
id_user	int(11)	Não		
id_sub	int(11)	Sim	*NULL*	
id_teste	int(11)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	13	A	Não	
fk_sql_injection_sub_usuario1_idx	BTREE	Não	Não	id_sub	2	A	Sim	
fk_sql_injection_usuario1_idx	BTREE	Não	Não	id_user	6	A	Não	
fk_sql_injection_sql_injection_teste1_idx	BTREE	Não	Não	id_teste	13	A	Não	
id_teste	BTREE	Não	Não	id_teste	13	A	Não	

Figura 7:Dicionário de Dados 4

sql_injection_teste

Coluna	Tipo	Nulo	Predefinido	Comentários
idSqlInjection	int(11)	Não		
Dominio	varchar(1000)	Não		
Payload	varchar(1000)	Não		
Tipo	varchar(20)	Não		
TipoVerificacao	varchar(20)	Não		
Banco	varchar(20)	Não		
hash	varchar(40)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	idSqlInjection	24	A	Não	

sqli_lista

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
id_usuario	int(11)	Não		
id_sub_usuario	int(11)	Sim	*NULL*	
hora_inicio	datetime	Não		
hora_fim	datetime	Não		
tipo_verificacao	varchar(20)	Não		
banco	varchar(20)	Não		
id_dominio	bigint(20)	Sim	*NULL*	

Figura 8:Dicionário de Dados 5

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	0	A	Não	
id_usuario	BTREE	Não	Não	id_usuario	0	A	Não	
id_sub_usuario	BTREE	Não	Não	id_sub_usuario	0	A	Sim	
id_dominio	BTREE	Não	Não	id_dominio	0	A	Sim	

sub_usuario

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
senha	varchar(255)	Sim	*NULL*	
Nome	varchar(255)	Sim	*NULL*	
id_permissao	int(11)	Sim	*NULL*	
id_usuario	int(11)	Sim	*NULL*	
cpf	varchar(14)	Não		
nome_completo	varchar(250)	Não		
email	varchar(250)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	32	A	Não	
FK_sub_usuario_id_permissao	BTREE	Não	Não	id_permissao	32	A	Sim	
id_usuario	BTREE	Não	Não	id_usuario	16	A	Sim	

teste

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
id_scan_portas	int(11)	Sim	*NULL*	
id_sql_inject	int(11)	Sim	*NULL*	
id_crawler	int(11)	Sim	*NULL*	

Figura 9:Dicionário de Dados 6

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	5	A	Não	
FK_teste_id_crawler	BTREE	Não	Não	id_crawler	5	A	Sim	
id_scan_portas	BTREE	Não	Não	id_scan_portas	2	A	Sim	

usuario

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
Nome	varchar(255)	Sim	*NULL*	
Senha	varchar(255)	Sim	*NULL*	
nome_completo	varchar(250)	Não		
cpf	varchar(14)	Não		
email	varchar(250)	Não		
login	varchar(250)	Não		

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	11	A	Não	

vinculo_portas

Coluna	Tipo	Nulo	Predefinido	Comentários
id	int(11)	Não		
dt_fim	datetime	Sim	*NULL*	
dt_ini	datetime	Sim	*NULL*	
id_user	int(11)	Sim	*NULL*	
id_sub	int(11)	Sim	*NULL*	
id_teste	int(11)	Sim	*NULL*	

Figura 10:Dicionário de Dados 7

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	32	A	Não	
FK_vinculo_portas_id_teste	BTREE	Não	Não	id_teste	32	A	Sim	
id_user	BTREE	Não	Não	id_user	10	A	Sim	
id_user_2	BTREE	Não	Não	id_user	10	A	Sim	
id_sub	BTREE	Não	Não	id_sub	10	A	Sim	

webpage

Coluna	Tipo	Nulo	Predefinido	Comentários
ID	bigint(20)	Não		
CONTENT_TYPE	varchar(255)	Sim	*NULL*	
URL	varchar(255)	Sim	*NULL*	
DOMINIO_ID	bigint(20)	Sim	*NULL*	
isDirectory	tinyint(1)	Sim	*NULL*	

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	ID	386	A	Não	
FK_webpage_DOMINIO_ID	BTREE	Não	Não	DOMINIO_ID	38	A	Sim	

webpage_off

Coluna	Tipo	Nulo	Predefinido	Comentários
id	bigint(20)	Não		
content_type	varchar(255)	Sim	*NULL*	
url	varchar(255)	Sim	*NULL*	
id_webpage	bigint(20)	Sim	*NULL*	

Figura 11:Dicionário de Dados 8

Índices

Nome da chave	Tipo	Único	Pacote	Coluna	Quantidade	Agrupamento (Collation)	Nulo	Comentário
PRIMARY	BTREE	Sim	Não	id	1145	A	Não	
FK_webpage_off_id_webpage	BTREE	Não	Não	id_webpage	1145	A	Sim	

Figura 12:Dicionário de Dados 9

2.2.4 Tela de Login

A tela de login foi projetada para dois tipos de usuários, o programa segue o conceito de hierarquia simples composta por sub usuários com privilégios limitados e previamente atribuídos por um administrador, ao preencher o login reservado ao administrador (o mesmo será usado pelo sub usuário), ao preencher o campo senha o usuário será redirecionado ao seu ambiente de trabalho com suas atribuídas permissões. A detecção do tipo de utilizador ocorre na verificação das senhas digitadas, o administrador possui uma senha única personalizável que é definida na realização do cadastro, o sub- usuário contém uma senha

única porem esta não pode ser configurada por ele, pois esta já vem previamente configurada com números e letras aleatórios compondo uma senha de seis caracteres.

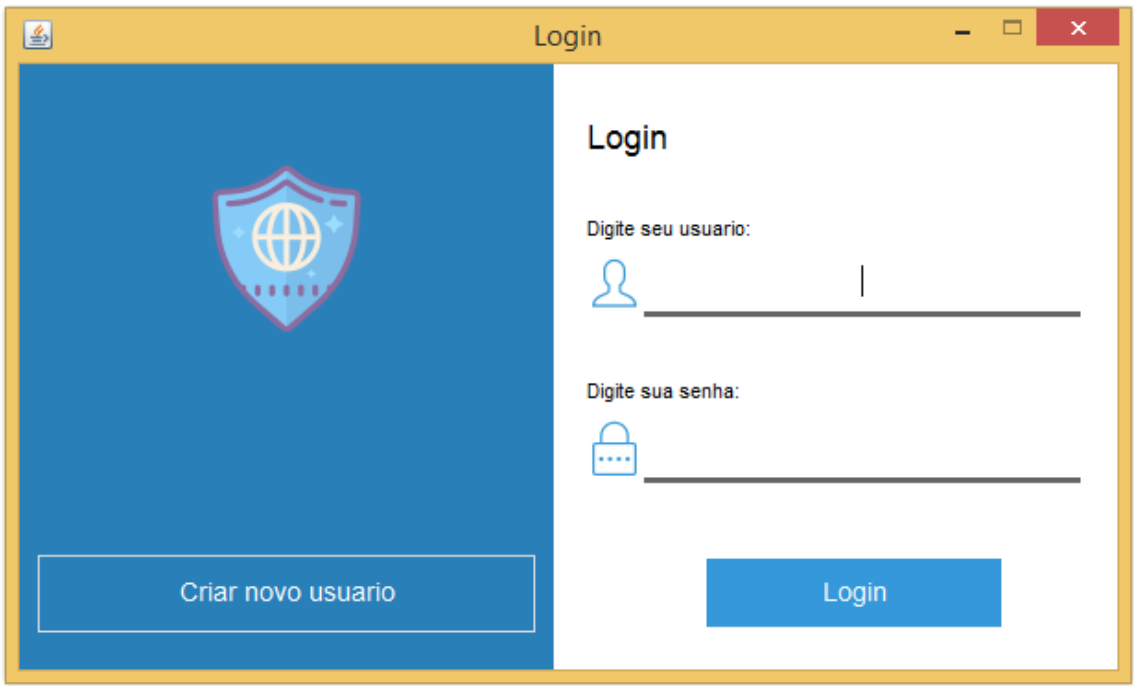

Figura 13:Tela Login

A tela de cadastro de usuários pede ao usuário algumas informações, os campos contem validações para evitar que o usuário digite alguma informação falsa. O botão salvar ira enviar as informações digitas ao banco de dados, Cancelar vai cancelar o cadastro e retornar a tela de login.

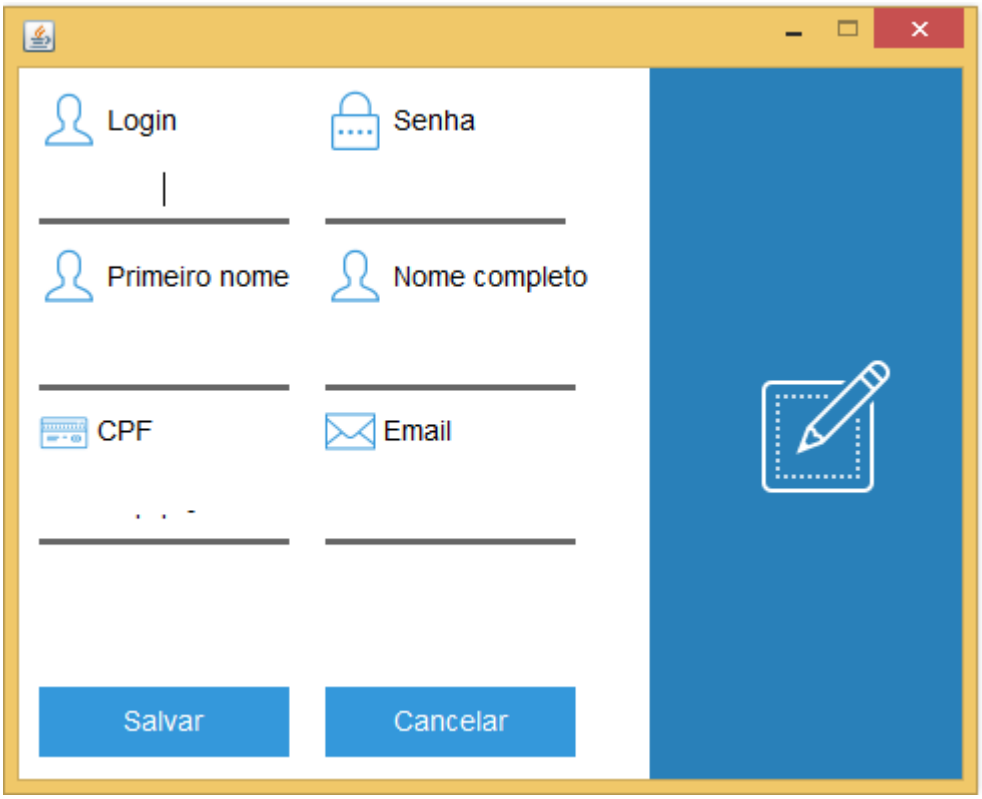

Figura 14:Tela Cadastro

2.2.5 Tela de permissões

A tela de permissões somente o usuário administrador tem acesso, ela permite que o administrador configure uma permissão especifica para um usuário ou um grupo de usuários.
O botão novo cria um nova permissão podendo escolher todas as opções de testes existentes no programa.
O botão excluir remove a permissão selecionada.
O botão editar permite ao administrador reconfigurar a permissão selecionada.
O botão salvar envia todas as informações sobre a permissão para o banco de dados.
O botão cancelar cancela a criação ou edição da permissão atual.

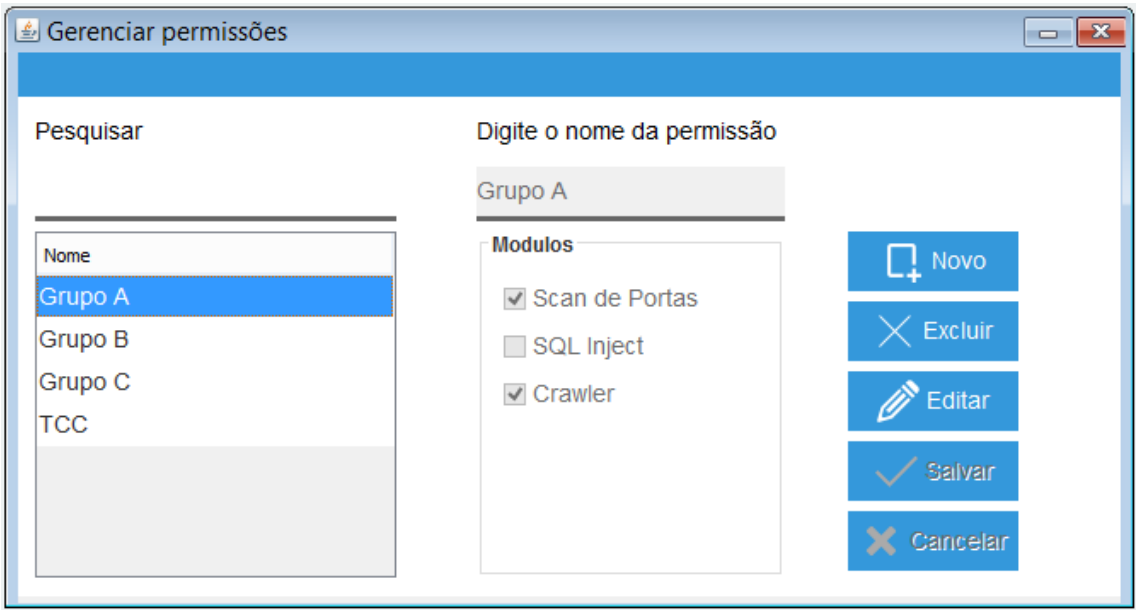

Figura 15:Tela Permissões

2.2.6 Menus

Figura 16:Menus

Sub usuário: abre um sub menu

WEB : abre um sub menu

Sair : Sair da Conta

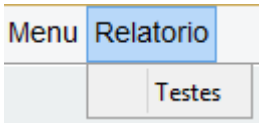

Figura 17:Menu Relatório

Testes : abre a janela com a lista de testes executados

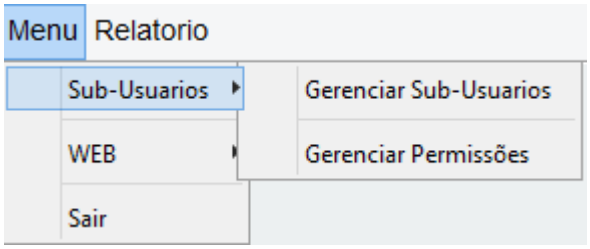

Figura 18:Menu Sub Usuários

Gerenciar sub usuários : abre uma janela de cadastro que permite fazer o gerenciamento de todos os sub usuários cadastrados

Gerenciar permissões : abre uma janela de cadastro que permite fazer o gerenciamento de todos as permissões

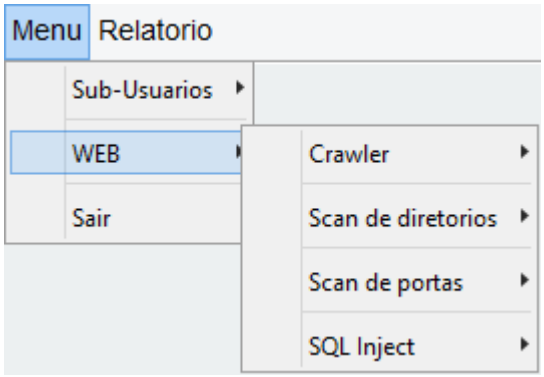

Figura 19:Menu Testes

Crawler : abre um sub menu

Scan de diretórios : abre um sub menu

Scan de portas : abre um sub menu

SQL Inject : abre um sub menu

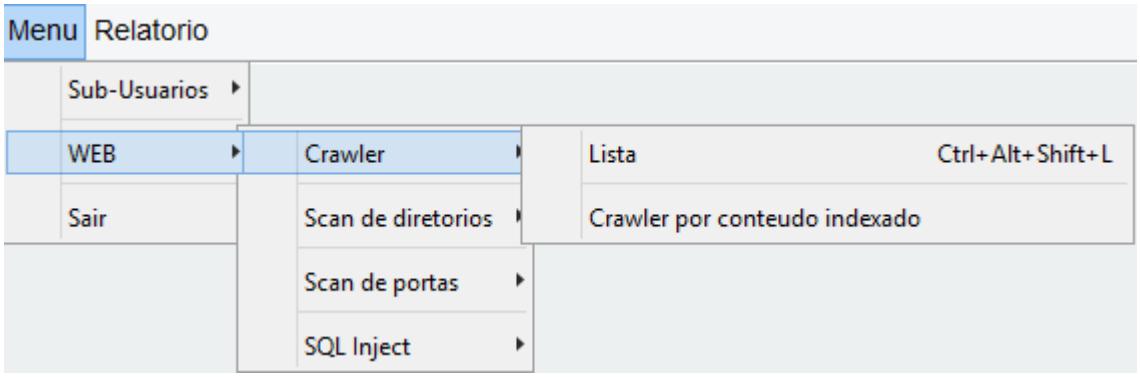

Figura 20:Menu Crawler

Lista : lista os crawler executados

Crawler por conteúdo indexado : abre a janela do crawler

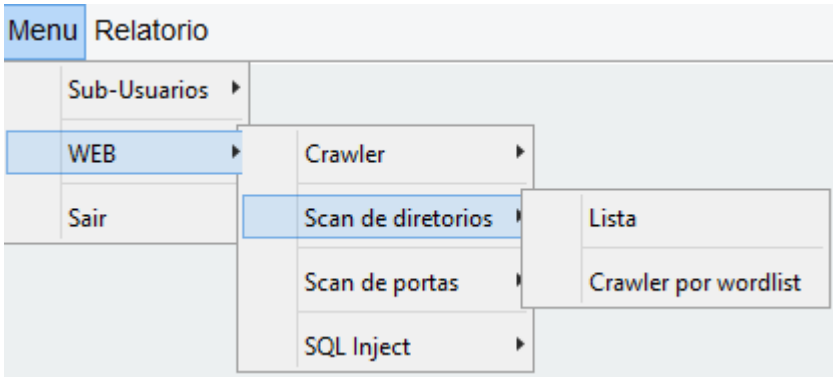

Figura 21:Menu Scan de diretórios

Lista : lista os scanner de diretórios executados.

Crawler por wordlist : abre a janela do crawler por força bruta(wordlist).

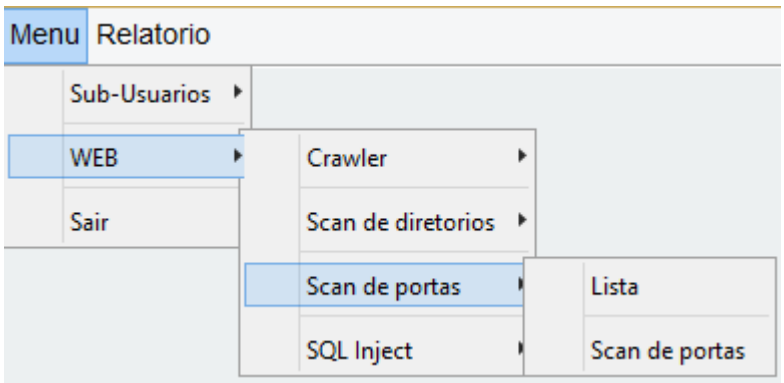

Figura 22:Menu Scan de Portas

Lista : lista os scanner de portas abertas executados.

Scan de portas : abre a janela do scanner de portas abertas.

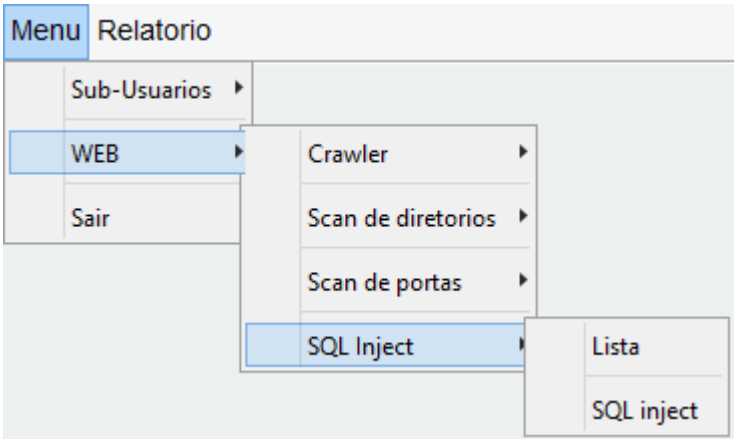

Figura 23:Menu SQL Injection

Lista : lista os scanner de diretórios executados.

SQL inject : abre a janela do teste de SQLInject.

2.2.7 Sub Usuários

A tela de sub usuários somente o usuário administrador tem acesso, ela permite que o administrador gerencie os sub usuários.
O botão novo cria um novo sub usuário podendo configurar as permissões ele terá.
O botão excluir remove o sub usuário selecionado.
O botão editar permite ao administrador modificar as informações do sub usuário selecionado.
O botão salvar envia todas as informações sobre o sub usuário para o banco de dados.
O botão cancelar cancela a criação ou edição atual.
A senha do sub usuário é uma chave que é gerada quando o sub usuário é criado.

Figura 24:Tela Sub Usuários

2.2.8 Scan de portas

O Scan de Porta (Port Scanner) é uma técnica de coleta de informação, onde o principal objetivo é descobrir as portas abertas e suas principais funções, juntamente com o risco.

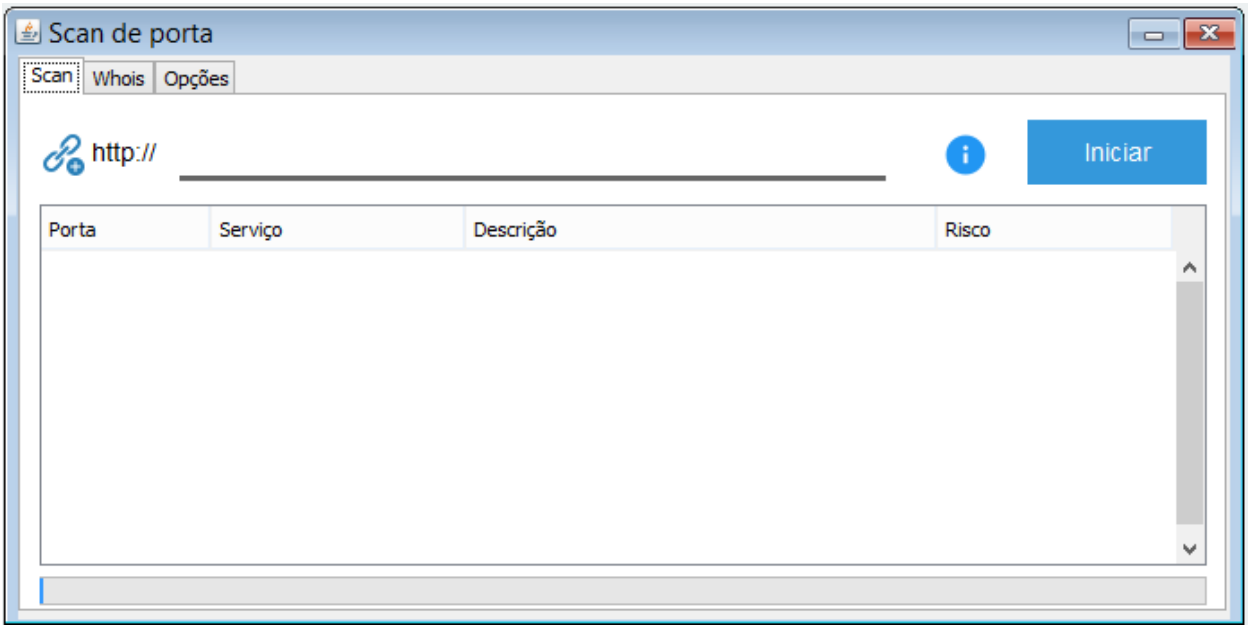

Figura 25:Tela Scan de Porta Principal

Scan:

Nessa janela o usuário poderá escolher o endereço do site, o qual será verificado por um técnica de requisição TCP/IP, esta técnica envia um solicitação para acessar a porta se a conexão for aceita o protocolo TCP envia um confirmação ao solicitante dizendo que a conexão foi bem sucedida. Após testar todas as portas, o programa acessa o banco de dados e através de um índice de portas ele detecta o serviço padrão existente naquela porta e conseqüentemente o risco.

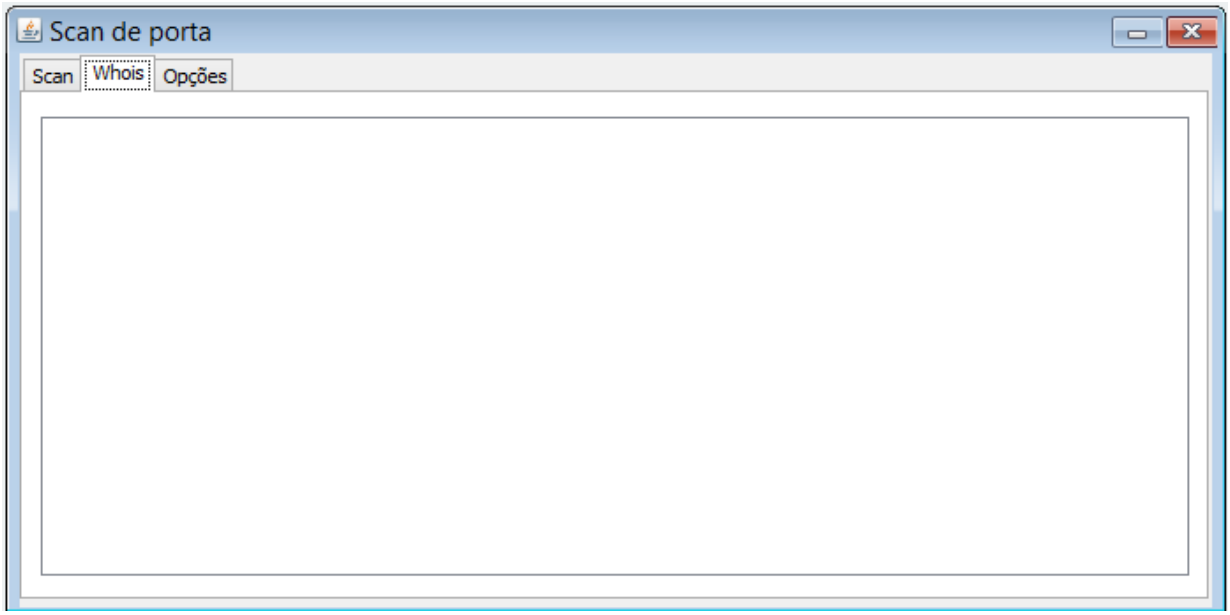

Figura 26:Tela Interface Whois

Whois:

Nessa janela o usuário verifica as informações retornadas pelo whois, este é uma técnica onde os dados do web site, como a data de criação, e-mail do responsável, CNPJ da instituição caso exista. A técnica whois funciona somente para domínios brasileiros e todas as informações coletadas estão disponíveis no órgão Registro BR.

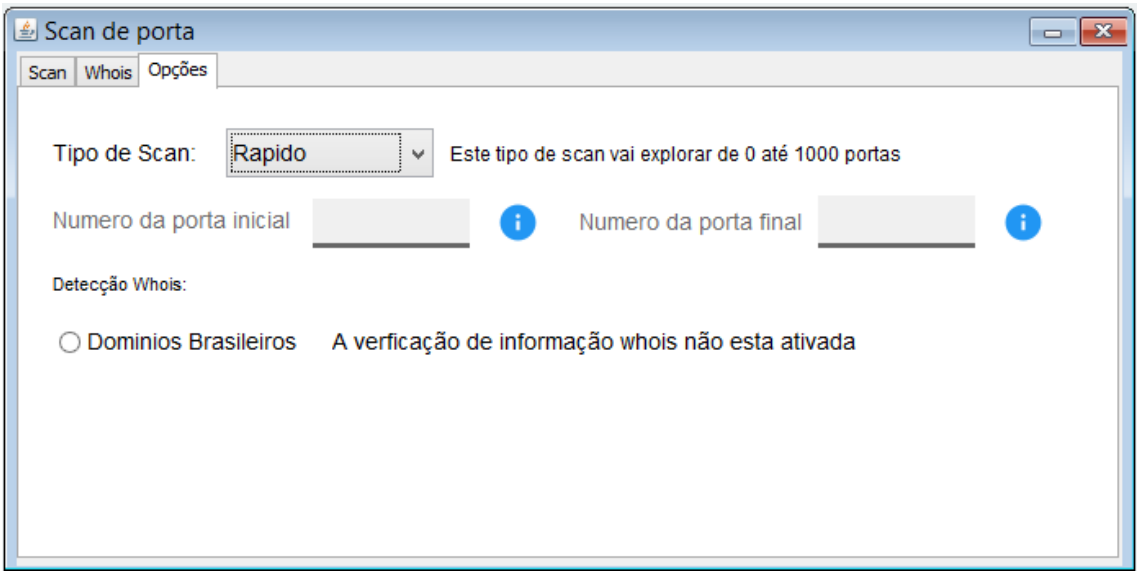

Figura 27:Tela Interface Opções

Opções:

Nessa janela o usuário poderá configurar o scan de acordo com suas necessidades, esta tela conta com a opção de habilitar a verificação whois como descrito no parágrafo anterior e também com tipo de scan. (Ver figura 4).

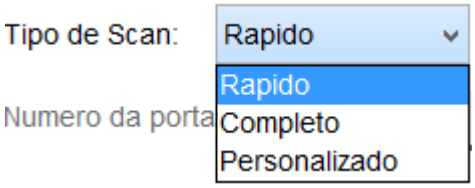

Figura 28:Tipos de Scan

O rápido executa a verificação entre as portas 0 até a porta 1000.

O completo executa a verificação em todas as 65535 portas.

O personalizado executa a verificação entras portas escolhidas pelo usuário.

2.2.9 Crawler

O crawler chamado também de spider ou bot, é o responsável pela execução de um processo conhecido como web crawling ou spidering que tem como principal objetivo mapear um site e fazer a coleta de informações como tags de formulários e links foras do ar. Um exemplo de uso desse processo é em motores de busca como o Google ou o DuckDuckGo.

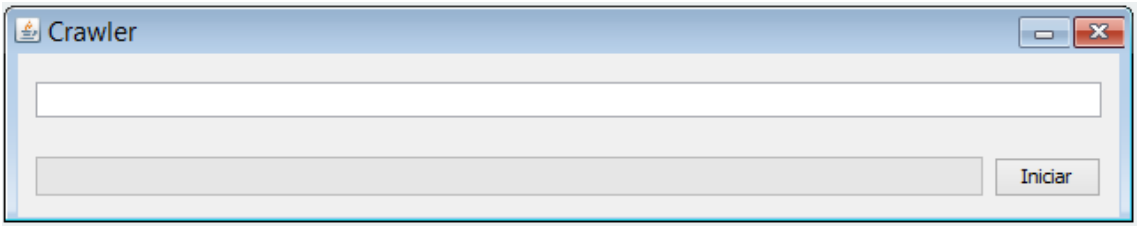

Figura 29:Interface Principal Crawler

No campo de texto o usuário ira digitar a URL do site que deseja executar o processo(exemplo :http://www.etectupa.com.br), ao pressionar o botar de iniciar o crawler ira coletar todas as informações e salvar no banco de dados.

2.2.10 Sql Injection

O SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicações e banco de dados, é uma falha onde permite ao usuário enviar comandos nocivos do SQL ao banco de dados por meio da aplicação seja ela web ou desktop.

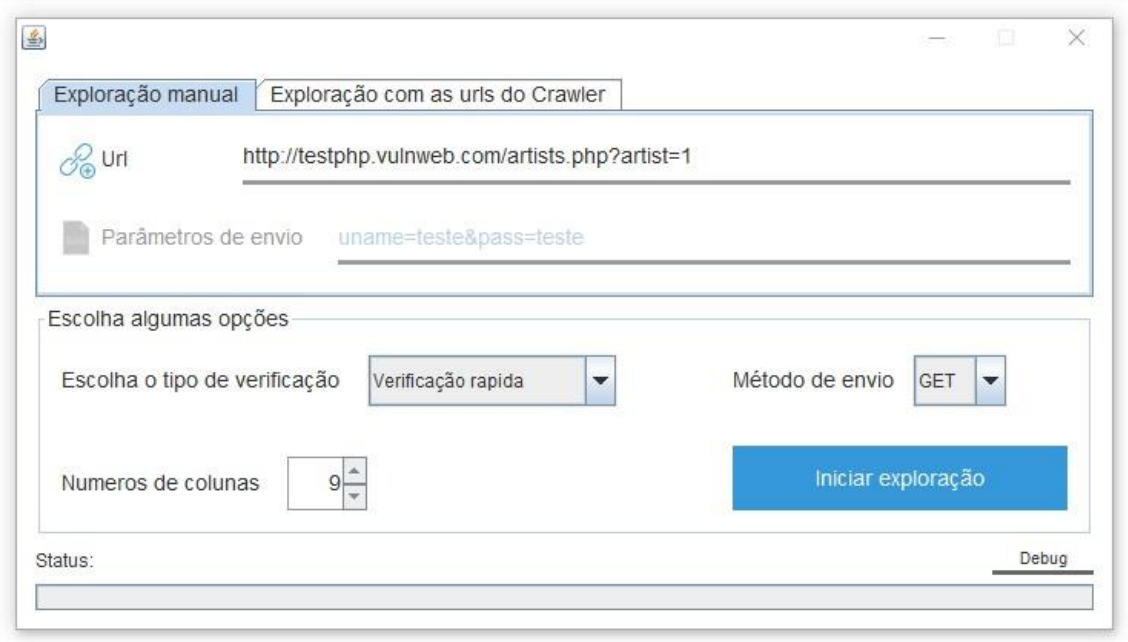

Figura 30:Interface Principal SQL Injection

Exploração manual:
Nessa janela é onde o usuário pode executar o teste contra um site especifico, duas informações devem ser inseridas a primeira é a URL do site, a segunda se for necessária os parâmetros de envio.

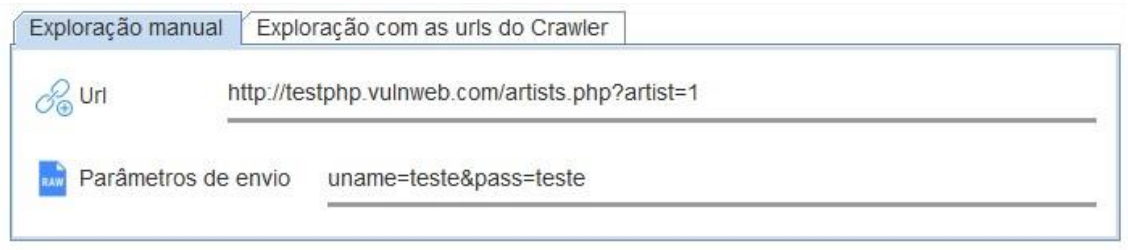

Figura 31: Exploração Manual

Exploração com as urls do Crawler:
Nessa janela o usuário pode escolher um site que foi mapeado pelo o Crawler, nesse teste todos os formulários encontrados serão explorados.

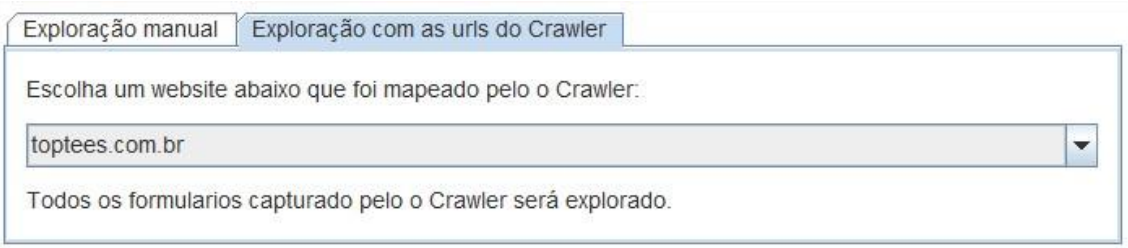

Figura 32:Exploração Automatizada com Crawler

Janela de opções:
Tipo de verificação:
Existem dois tipos de verificações, sendo que o primeiro relata informações de erros comuns, tais eles como: Erro de sintaxes no banco de dados [...].

A segunda trata-se de uma verificação profunda, com esta opção acionada, o site selecionado será explorado com total intensidade utilizando comandos SQL (Injection[...]) pré-configurados/configurados/preparados especificamente para encontrar falhas em qualquer parâmetro vulnerável.

Método de envio:
GET : Este método é utilizado quando se quer passar poucas informações para realizar alguma ação ou passar uma informação para outra pagina através da URL.

POST : Este método utiliza a URI (UniformResourceIdentifier) para envio de informações ao servidor.Ou seja as informações vai por baixo do navegador em vez da url.

Figura 33:Definição de Opções

Por fim temos o botão de Iniciar ele inicia toda a verificação enquanto ele estiver verificando uma barra de progresso está em movimento até que a exploração termine.

2.2.11 Relatório

A tela de relatório somente o usuário administrador tem acesso, ela permite que o administrador gerencie os relatorios dos sub usuarios podendo escolher qual o tipo de teste. Ao escolher um sub usuario será mostrado em uma tabela todos os teste que o sub usuario executou clicando sobre o teste será gerado o relatorio.
A opção Eu mesmo mostra todos os testes executados pelo o proprio administrador.

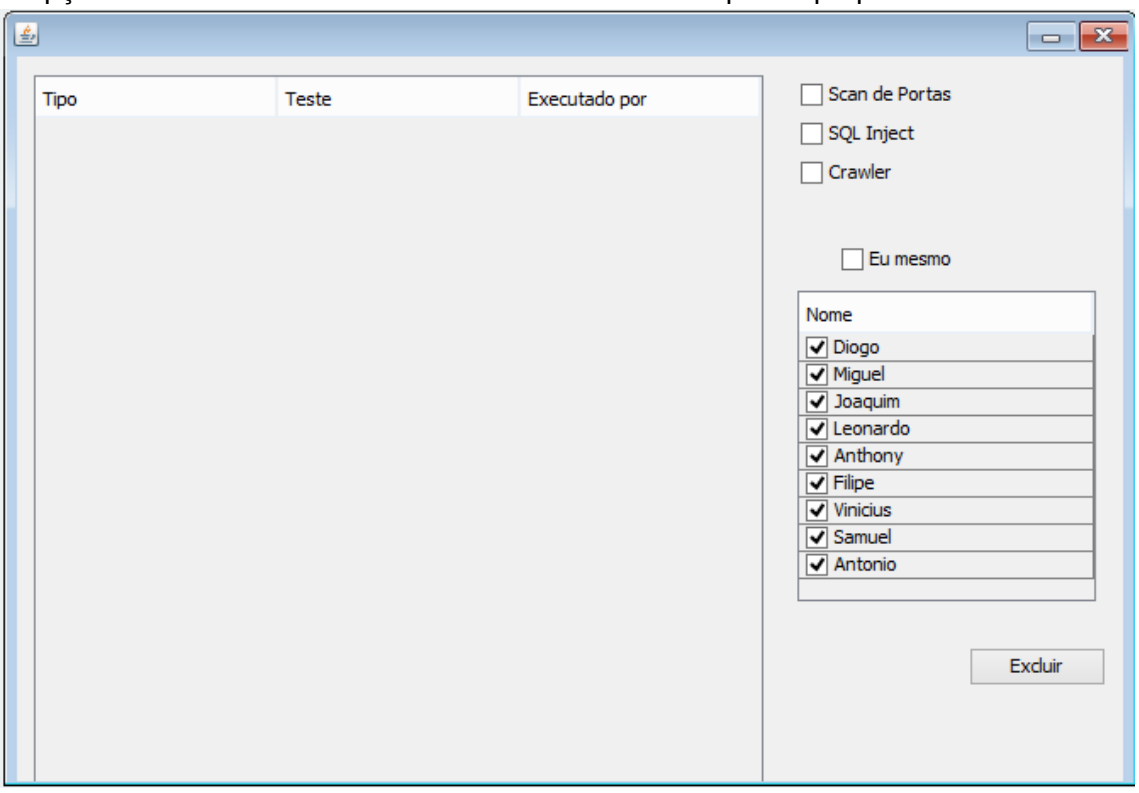

Figura 34:Relatório

Considerações Finais

Considerando o que foi aprendido podemos dizer que o programa possui um suporte a qualquer tipo de Sistema Operacional seja ele Windows, Linux, Mac entre outros, possibilitando sua execução por um único usuário ou uma equipe seu sistema de login garante este tipo de suporte, este modelo de software pode ser executado para atender uma demanda de grandes clientes possibilitando todos os dados serem salvos em tempo real, assim podendo gerar um relatório com todas as informações necessárias para que o usuário possa analisar mais afundo as vulnerabilidades encontradas, com isso é possível que o destinatário final tenha um maior desemprenho .

Referências

Júlio, JV. (2016) O que é Pentest. http://blog.onedaytesting.com.br/o-que-e-pentest-e-para-que-serve/ . Acesso em: 10 abr. 2017.

C.E.H.https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ Acesso em: 17 abr. 2017.

Paulo.PT.(2011) Pentest.http://www.mundodoshackers.com.br/tag/o-que-e-pentest Acesso em: 25 abr. 2017.

Felipe.Payão.https://www.tecmundo.com.br/tecmundo-explica/113195-sql-injection-saiba-tudo-ataque-simples-devastador.htm Acesso em: 29 mai. 2017.

GUJ. http://www.guj.com.br/c/programacao/java Acesso em: 2 jun. 2017.

StackOverflow. https://pt.stackoverflow.com/ Acesso em: 5 jun. 2017.

Caelum. https://www.caelum.com.br/ Acesso em: 10 jun. 2017.

DevMedia. https://www.devmedia.com.br/ Acesso em: 12 jun. 2017.

GITHUB. https://github.com/nmap/nmapAcesso em: 20 jun.2017.

Gustavo.Lima.http://blog.corujadeti.com.br/aonde-estao-os-melhores-hackers-mundo/ Acesso em: 25 out. 2017.

WeSchools.https://www.w3schools.com/sql/sql_injection.asp Acesso em: 29 out. 2017.

Java Documentation.https://docs.oracle.com/en/java/ Acesso em: 30 out. 2017.

CÉSAR, Silvio ; RAIMUNDO, Gerson.Backtrack Linux: Auditoria e Teste de Invasão em Redes de Computadores.1ª.e.d. Ciência Moderna Edit, 2013. 248pág.

MORENO,Daniel. Introdução ao Pentest.1ª.e.d. Novatec,2015.296pág.

BROAD, James; BINDNER, Andrew. Hacking Com Kali Linux: Técnicas Práticas para Testes de Invasão.1ª.e.d. Novatec,2013.288 pág.

ENGEBRETSON, Patrick . Introdução ao Hacking e aos Testes de Invasão: Facilitando o Hacking Ético e os Testes de Invasão.1ª.e.d. Novatec,2013.304 pág.

DEITEL, Paul; DEITEL, Harvey. Java como programar. 10ª.ed. Pearson, 2016. 968 pág.

CORDEIRO, Gilliard. Aplicações Java para web com JSF e JPA. Casa do código, 2012. 329 pág.

TURINI, Rodrigo. Desbravando Java e Orientação a Objetos. Casa do código, 2014. 222 pág.