



FACULDADE IEDUCARE - FIED

RONNEY DAMASCENO FREITAS

**GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA
VULNERABILIDADE TÉCNICA DO PAINEL ADMINISTRATIVO DE UM
WEBSITE**

**TIANGUÁ - CE
2016**

FIED - FACULDADE IEDUCARE

**GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA
VULNERABILIDADE TÉCNICA DO PAINEL ADMINISTRATIVO DE UM
WEBSITE**

Monografia apresentada pelo aluno Roney Damasceno Freitas à coordenação Acadêmica do Ieducare como parte das Exigências para Obtenção do Título de Bacharelado em Sistemas de Informação, outorgado pela Faculdade Ieducare.

ORIENTADOR: Professor Esp. Rhyan Ximenes de Brito

COORIENTADOR(a): Professor(a) Esp. Janaide Nogueira de Sousa Ximenes

FACULDADE IEDUCARE

SISTEMAS DE INFORMAÇÃO

GESTÃO DE SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA VULNERABILIDADE TÉCNICA DO PAINEL ADMINISTRATIVO DE UM WEBSITE

Autor: Roney Damasceno Freitas

Defesa em: ____/____/____

Nota obtida: _____

Banca Examinadora

Prof. (a) ORIENTADOR (A)

1º AVALIADOR(A)

2º AVALIADOR(A)

Dedico este trabalho a Deus, à
minha família, aos meus amigos e
à meu orientador.

AGRADECIMENTO

A conclusão deste trabalho que tem um valor incalculável na minha vida, foi realizado graças a colaboração de algumas pessoas que, de diversas formas, deram sua contribuição em diferentes etapas. Destas, manifesto um agradecimento especial primeiramente a Deus por ter me proporcionado sabedoria e saúde ao longo dessa etapa maravilhosa na minha vida, aos professores por terem colaborado no meu desenvolvimento intelectual em especial ao professor Rhyan Ximenes de Brito por sempre ter me incentivado a escrever artigos científicos e a faculdade IEducare, pelo apoio nos eventos científicos.

Finalmente, minha família pelo incentivo e por sempre terem acreditado no meu potencial, aos meus amigos, pelo incentivo e companheirismo imprescindíveis ao longo de minha trajetória.

EPÍGRAFE

“Tente uma, duas, três vezes e se possível tente a quarta, a quinta e quantas vezes for necessário. Só não desista nas primeiras tentativas, a persistência é amiga da conquista. Se você quer chegar a onde a maioria não chega, faça o que a maioria não faz.”

Bill Gates

RESUMO

A Internet hoje sem duvidas é o maior meio de comunicação no mundo, por ela trafega grandes quantidades de informações, onde muitas dessas informações precisam esta em ambientes seguros e gerenciáveis apenas por pessoas autorizadas, ou seja, pessoas que terão posse de credenciais que permitiram a manipulação das informações de forma correta. O presente trabalho aborda um estudo sobre a segurança e gestão da informação com foco direcionado a aplicações *web*. O objetivo geral desse estudo é realizar testes de invasão utilizando uma máquina virtual juntamente com o sistema operacional *Kali Linux* utilizando diversas ferramentas com finalidade de mostrar quais os tipos de vulnerabilidades que existem no painel administrativo do site eleições 2016, onde os testes abordados nesse trabalho podem ser aplicados em qualquer painel administrativo de aplicações *web*.

Palavras-chave: Segurança da Informação. Teste de Invasão. Vulnerabilidades.

RESUMEN

La Internet hoy sin duda es el mayor medio de comunicación en el mundo, por ella pasa grandes cantidades de informaciones, donde gran parte de estas informaciones necesitan estar en un entorno seguro y administrable por personas autorizadas, o sea, personas que tendrán pose de credenciales donde les permitan hacer la manipulación de las informaciones correctamente. El presente trabajo aborda un estudio sobre la seguridad y gestión de la información con un enfoque dirigido a las aplicaciones *web*. El objetivo general de este estudio es realizar pruebas de penetración utilizando una máquina virtual con el sistema operativo Kali Linux utilizando de diversas herramientas con el propósito de mostrarles cuales son los tipos de vulnerabilidades que hay en el panel administrativo del sitio elecciones 2016, donde las pruebas dirigidas en este trabajo pueden ser aplicadas en cualquier panel de administración de las aplicaciones web.

Palabras claves: Seguridad de la Información. Prueba de Penetración. Vulnerabilidades.

SUMÁRIO

1. INTRODUÇÃO	11
2. HISTÓRICO DA SEGURANÇA DA INFORMAÇÃO	13
3. GESTÃO DA SEGURANÇA DA INFORMAÇÃO	16
3.1. Conceitos Básicos de Segurança da Informação	16
3.1.1 Ameaças	18
3.1.2. Vulnerabilidades	18
3.1.3. Ataques	19
3.1.4. Riscos	21
4. SEGURANÇA DA INFORMAÇÃO	22
4.1. Tipos de Criptografias	23
4.2. Principais Algoritmos de Criptografia	24
4.2.1. DES	24
4.2.2. AES	25
4.2.3. RSA	25
4.2.4. MD5	26
5. CARACTERIZAÇÃO DO SITE ELEIÇÕES 2016	27
5.1. Surgimento da Ideia de Implementação do Site	27
5.2. Linguagens Utilizadas na Implementação	29
5.2.1. <i>Sublime Text 3</i>	29
5.2.2. HTML5	29
5.2.3. CSS3	30
5.2.4. <i>JavaScript</i>	30
5.2.5. PHP	31
5.2.6. <i>Bootstrap</i>	31
5.3. Sistemas de Banco de Dados Utilizado	32
5.4. Funcionalidades Implementadas no Painel de Controle	32
5.5. Como Funciona a Interação Entre o Site e o App Eleições	33
6. MECANISMOS DE SEGURANÇA IMPLEMENTADOS NO PAINEL DE CONTROLE	34
6.1. Algoritmo de Criptografia	34
6.2. Forma de Autenticação	34
6.3. Controle de Usuário	35

6.4. Simulações, Testes e Resultado de Ataques ao Painel do Site	36
7. CONSIDERAÇÕES FINAIS	46
8. REFERÊNCIAS BIBLIOGRÁFICAS	47

LISTA DE FIGURAS

Figura 1 - Cifra de CésarFonte: Stallings, 2008.	14
Figura 2 - Página Index do Site Eleições 2016	28
Figura 3 - Design responsivo	32
Figura 4 - Menus do Painel Administrativo.....	33
Figura 5 - Tela de Login	34
Figura 6 - Implementação das variáveis de login e senha	35
Figura 7 - Níveis de usuários	36
Figura 8 - Execução do Kali Linux na VM	36
Figura 9 - Histórico de vulnerabilidades encontradas pelo Nessus no Site Eleições 2016	38
Figura 10 - Resultados obtidos pela ferramenta Nmap.....	39
Figura 11 - Resultados obtidos pela ferramenta Nikto	40
Figura 12 - Execução da ferramenta Uniscan.....	41
Figura 13 - Alguns resultados da ferramenta Uniscan	41
Figura 14 -Interface do Burp Suite	42
Figura 15 - Criando word list com Cewl	43
Figura 16 - Criando word list com Crunch.....	44
Figura 17 - Resultado do ataque força bruta com Burp Suite	45

1. INTRODUÇÃO

Este trabalho está direcionado a gestão da segurança da informação voltado ao painel administrativo do site eleições 2016, onde apenas pessoas autorizadas podem ter acesso ao gerenciamento das informações administrativas do site e terá o controle dos dados que serão expostos ao público em geral. A motivação para investigar tal temática, foi a participação como membro da equipe de desenvolvimento do site, tendo a percepção e vivência do quanto se faz necessário a preocupação com a segurança e integridade das informações na *web*, lugar este onde a privacidade está sempre exposta e sujeita a diversos tipos de ataques e ameaças a qualquer momento. Atualmente pode-se perceber o quanto é importante focar na segurança da informação no cotidiano, em uma era em que, para acompanhar o crescimento tecnológico da sociedade, é impossível não estar conectado a Internet, que conseqüentemente estando conectado, passa-se a estar vulnerável e sujeito a vários tipos de ataques e ameaças. As aplicações *web* também sofrem constantemente com esse fator, ataques esses que tem como objetivo adquirir acesso às informações confidenciais, podendo expor ou alterar tais informações.

Devido a toda insegurança no mundo virtual, a sociedade é alvo direto de ameaças, que conseqüentemente apresenta a necessidade em deixar o site eleições 2016 o mais seguro possível, aplicando técnicas e métodos direcionados à segurança da aplicação, podendo assim evitar possíveis transtornos, como perda de dados, alterações, constrangimento, e até mesmo, perda financeira.

Este trabalho propõe mostrar a importância da segurança da informação e a realização de testes de invasão voltados á painéis administrativos na *web* em especial ao painel do site eleições 2016, apresentando diversas ferramentas para tal finalidade, serão também utilizados conceitos oriundos das áreas da informática de diferentes tecnologias, com enfoque principal voltado em segurança da informação e tecnologias *web*, trazendo a mais correta abordagem para o tema proposto acima.

Buscando-se, deste modo, uma clara abordagem na identificação dos elementos, os quais serão indagados para a contribuição do levantamento científico teórico, trazendo de forma clara e concreta a resolução para o problema exposto.

Segundo Dias (2000), a segurança é proteger as informações, sistemas, recursos e serviços contra manipulação não autorizada e desastres visando à redução do impacto e diminuir a probabilidade de incidentes de segurança.

Em uma abordagem de Carneiro (2002), define segurança sendo, um conjunto de medidas e procedimentos, com objetivo de proteger informações, contra destruição indevida, alterações de uma forma não organizada.

Pode-se então, destacar com Ferreira (2003), que a segurança da informação protege a informação dos diversos tipos de ameaças. Pode se concluir que a segurança da informação é de fundamental importância contra acessos indevidos de pessoas não autorizadas com o objetivo de manipular as informações.

2. HISTÓRICO DA SEGURANÇA DA INFORMAÇÃO

A necessidade da segurança da informação para o homem surgiu há muitos anos atrás. Nos primórdios, possuir informações úteis era considerado de grande importância, pois pessoas que detinha informações poderiam se tornar mais poderosas que as outras. Com o passar do tempo e a evolução dos meios tecnológicos, as formas de possuir registros de informações passam a ser alteradas, quando antes a única forma de armazenar informações era apenas na memória humana, passou a ser registrada através de símbolos. Segundo Paula (2008), os dados são símbolos com valores físicos ou não, registros são fatos que composto de relevância se transformam em matéria prima para a geração de informação.

A segurança da informação é algo muito importante para a humanidade, uma questão que sempre se estar discutindo e buscando novos métodos a fim de manter a informação segura. De acordo com Paula (2008), a informação participa do cotidiano das pessoas desde os tempos primórdios, os homens primitivos registraram informações, mudaram os suportes quando surgiu a necessidade de locomover tais registros e disseminaram as informações.

Caruso (2006) entende que o homem busca, desde os primórdios, manter o controle sobre as informações que de alguma forma tenha um grau de importância. A troca de informações, sempre foi algo com que o homem tem se preocupado constantemente, pensando na melhor forma de levar as informações de modo seguro. Ao longo dos anos a sociedade vem buscando métodos de assegurar e manter a confidencialidade e integridade das informações.

Com o surgimento do computador e sua constante evolução, passou a ser o principal meio de armazenamento de informação. Atualmente a sociedade tem a informação como um de seus bens mais preciosos, de forma em que se faz necessário manter os dados importantes seguros. Com a necessidade de que as informações não fossem descobertas motivou o homem a desenvolver métodos e técnicas com a finalidade de assegurar tais informações. Conforme Paula (2008), a sociedade evolui rápido com o passar do tempo, as mudanças aconteceram de acordo com as necessidades do ser humano.

Um das técnicas que revolucionou a segurança da informação foi a cifra de César que foi chamado assim em homenagem ao imperador Romano Júlio César o qual imperava na época. A cifra era simples, onde em um texto era realizada a substituição de cada letra pela letra que seguia em três posições à frente de acordo com o alfabeto. Stallings (2008) complementa que a cifra feita por Júlio César tem o uso mais antigo e o mais simples que conhecemos de uma cifra de substituição, como mostra na figura 1.

Figura 1 - Cifra de César

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Stallings, 2008.

Atualmente é utilizada a denominação de cifra de César em qualquer cifragem, na qual cada letra da mensagem clara é substituída por outra deslocada um número fixo de posições, não necessariamente três.

Para Moraes e Noronha (2014), manter restrito o acesso às informações, sem a perda de suas propriedades significativas de seu conteúdo foi implantada desde o contexto das batalhas há muito tempo. Uma das técnicas desenvolvidas para a troca de informações confidenciais entre transmissores e receptores foi o surgimento da criptografia, que significa mensagem escrita de forma desconhecida. Técnica essa onde as informações são codificadas de forma que apenas o emissor e receptor conseguem decifrar a mensagem. Para Hinz (2000), desde tempos remotos, a criptografia sempre teve papel significativo na transmissão de dados secretos. Pois ela torna, ou tenta tornar, os dados da mensagem irreconhecíveis para qualquer pessoa que não seja remetente ou receptor.

Com o passar dos anos, a rede mundial de computadores cresceu significativamente, de acordo com Nobre (2009), foi na revolução industrial onde as tecnologias tiveram destaque, como forma de agilizar os processos operacionais. Foi nessa época onde a sociedade passou a conviver gradativamente com as tecnologias e principalmente computacionais.

Oliveira (1994) entende que o crescimento de informações, as novas tecnologias de comunicação e de banco de dados são fortes impulsionadores da atual transformação da sociedade. Com esse crescimento, a segurança da informação passou a ser algo primordial dentro de qualquer organização, sendo de fundamental importância possuir suas informações seguras e confiáveis, evitando assim possíveis vazamentos de dados de forma inadequada.

Morais e Noronha (2014) expressam que se durante a antiguidade a única forma de armazenamento era a memória do homem, depois com a elaboração dos primeiros alfabetos proporcionou uma nova forma de registrar as informações. Vários anos depois, veio o surgimento de novas tecnologias para aumentar a gama de armazenamento e organização dos dados: a máquina de escrever e, logo após, veio algo para revolucionar o mundo da tecnologia, que até hoje está presente na sociedade, o computador, que tem se tornado hoje o maior e mais importante repositório de armazenamento e organização dos dados.

Dessa forma fica evidente que, com o avanço tecnológico e disponibilidade de informações no mundo virtual, manter restrito o acesso às informações, mesmo com a implementação de técnicas de proteção não é algo simples, a sociedade vem sofrendo com a insegurança constantemente, onde criminosos virtuais cada vez mais adquirem novos métodos de burlar a segurança. Manter a segurança de dados na Internet tem se tornado algo difícil e complexo, problema esse encontrado facilmente no Brasil e mundo.

3. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Gestão de Segurança da Informação (GSI) tem um objetivo de fornecer modelos, técnicas e metodologias para minimizar os riscos ao acesso indevido às informações em uma organização. De acordo com Santos e Silva (2012), a gestão de segurança tem o propósito de buscar estratégias de melhorias, como estabelecer, implementar, operar, monitorar, rever e manter o controle sobre a segurança das informações com base em uma correta avaliação e gestão de uma organização inerente a riscos. Já para Laudon e Laudon (2001), atribui ao gerente de TI (Tecnologia da Informação) o uso de metodologias adequadas à redução das contingências e dos riscos e ameaças às organizações, combinando medidas manuais e autorizadas que, juntas mantêm as correspondências ao efetivo controle. A partir dessas definições pode-se assegurar que uma organização necessita de um GSI implementado em seu ambiente, para prover e manter baixos níveis de riscos e ameaças sobre suas informações.

De acordo com a definição de Ramos (2008), GSI visa justamente possibilitar que a organização que o implanta atinja seus objetivos referentes à segurança da informação. Pode-se perceber de acordo com os autores mencionados acima, que a GSI tem como objetivo buscar métodos com finalidade de minimizar os acessos indevidos às informações, buscando também procedimentos para aperfeiçoar os mecanismos de segurança.

3.1. Conceitos Básicos de Segurança da Informação

Nas organizações, as quais fazem parte do meio tecnológico, estão constantemente sujeitas a exploração de vulnerabilidades, fazendo-se necessário o uso da gestão de segurança da informação com a finalidade de buscar a proteção das informações. A exploração dessas fraquezas é realizada por meios de ações de origem humana, que quando são exploradas estão sujeitos a identificar fendas, onde a partir desses pontos críticos pode-se produzir ataques, e logo, comprometer as informações, causando a perda de um ou mais pilares básicos da segurança da

informação, podendo citar a confidencialidade, disponibilidade, integridade e autenticidade.

A segurança da informação para Sêmola (2003) é a proteção de diversos tipos de ameaças às informações, preservando seus atributos, como a confidencialidade, integridade, disponibilidade e autenticidade. Pode-se destacar que, ter um conhecimento mais aprofundado sobre os principais pilares da GSI é essencial para entender de forma detalhada o conceito de segurança da informação.

De acordo com Ramos (2008), é definido o atributo de confidencialidade da segurança da informação como o sigilo da informação, então preservar a confidencialidade significa garantir que apenas as pessoas autorizadas poderão ter acesso. Diferentes tipos de informação terão diferentes necessidades em termos de confidencialidade. Conforme Fontes (2000), a confidencialidade tem como princípio o acesso das informações somente pelos usuários com autorização. Campos (2006) menciona que confidencialidade é respeitada quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação, ou seja, a informação no ambiente organizacional requer essa cautela por parte dos gestores da informação em designar as pessoas certas no que diz respeito à guarda das informações para que não haja quebra da confidencialidade. Já no que diz respeito à integridade, fato esse meramente importante para qualquer organização referente ao tratamento das informações, no qual Ramos (2008) destaca que a preservação da integridade envolve proteger as informações contra modificações em seu estado original. Essas modificações podem ser tanto intencionais quanto acidentais. Campos (2006) expressa que o princípio da integridade é obedecida quando a informação acessada está completa, sem alterações, ou seja, quando a informação é modificada ou chegada ao seu destino de forma alterada, isto faz com que se perca a integridade. Quando se diz respeito à disponibilidade, quer dizer que a informação precisa estar disponível a todo o momento. Ramos (2008) aborda que uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que seja necessário. Já para Silva, Carvalho e Torres (2003), disponibilidade é vital ao acesso à informação, de modo que ter a informação necessária, mas não ter disponível no momento desejado, equivale a não possuir qualquer informação. É destacado também o atributo de autenticidade, onde o mesmo pode garantir a identidade de quem está enviando algum tipo de informação. Simão (2009) comenta que a autenticidade associa-se com a confirmação ou comprovação de autoria,

dessa forma pode ter a certeza de que a informação manteve sua originalidade, mesmo sendo manipulada.

A Internet é um dos meios de comunicação onde se utiliza de serviços disponíveis para o tráfego de informações, podendo existir no mesmo ambiente, pessoas maliciosas em busca das informações que neste meio trafegam, com a finalidade de romper a segurança da informação, com isso, se faz necessário tomar medidas cabíveis conseguidas através dos atributos acima citados para garantir a proteção dos dados, seja em uma organização ou não.

Sêmola (2003) expõe o quanto é importante salientar que a segurança da informação não se restringe apenas às informações eletrônicas, sistemas computacionais ou mecanismos de armazenamentos, ela está presente em todos os aspectos de proteção e armazenamento da informação, em qualquer formato, seja ela em papel ou em distintos tipos de arquivos de mídias.

3.1.1 Ameaças

Uma ameaça pode ser considerada física ou virtual, podendo comprometer toda a segurança da informação, esse acontecimento pode ser causado por um fenômeno natural ou por uma simples ação humana. Fenômeno natural podendo ser incêndio, terremoto e entre outros, já por ação humana, pode ser de forma física ou virtual, onde de maneira física pode ser o simples fato de conseguir acesso ao local onde se encontra as informações, já de maneira virtual, pode ser feito através de vírus, que tem como objetivo roubar ou danificar as informações. Ramos (2008) aponta que a ameaça é algo que pode causar dano a informação. Entre as ameaças possíveis, se pode citar criminosos virtuais e vírus. Segundo Dias (2000) uma ameaça é um evento ou atitude indesejável, ou seja, roubo, incêndio ou vírus, que tem um potencial de remover, desabilitar, danificar ou destruir um recurso. Já Santos e Silva (2012) concluem que esse ato pode causar o potencial de um acontecimento indesejado, o que pode ocasionar em danos para um sistema ou entidade.

3.1.2. Vulnerabilidades

Na rede mundial de computadores atualmente existem milhares de aplicações disponibilizando algum tipo de informação e todas as informações consequentemente estão em um ambiente inseguro, onde qualquer tipo de vulnerabilidade na aplicação pode possibilitar explorações por atacantes virtuais, com possibilidades de gerar grandes prejuízos.

Sistemas *web* (online) são os alvos preferidos dos usuários mal intencionados, pois estando diretamente ligado à Internet viabiliza ao criminoso virtual se aproveitar do ambiente de forma camuflada para estar explorando as vulnerabilidades em busca de falhas de segurança. Vulnerabilidade na *web* pode resultar de diversos fatores, onde pode se destacar os mais comuns como:

- a produção de aplicação de péssima qualidade, devido aos curtos prazos de entrega, elevando assim o grau de risco susceptíveis a falhas no desenvolvimento da aplicação, acarretando em sérios problemas de segurança;
- ausência da criptografia, onde muitas aplicações *web* não utilizam desse mecanismo, onde auxiliaria na proteção dos dados contra acesso indevido de usuários mal intencionados, que atualmente é fundamental que qualquer aplicação utilize de tal mecanismo, dificultando assim o acesso indevido das informações.

Elias (2015) fala que uma ameaça é concretizada mediante a existência de uma vulnerabilidade, ou seja, uma deficiência a ser explorada pelo agente da ameaça para concretizá-la. A facilidade de abrir a fechadura de uma porta, por exemplo, é uma vulnerabilidade a ser explorada por um invasor tentando entrar em uma casa de forma não autorizada.

Já de acordo com Sêmola (2003), os negócios, seus processos e ativos físicos, tecnológicos e humanos são a todo instante alvo de ameaças, que buscam identificar um ponto frágil compatível, uma vulnerabilidade capaz de fortalecer sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.

3.1.3. Ataques

Os ataques são resultados de ações realizadas por invasores que utilizam de ferramentas como vírus, com a finalidade de roubar informações das vítimas. Essas ações são realizadas geralmente em ambientes virtuais, devido o rápido

alcance as informações, altos ganhos, e o baixo risco que os criminosos podem estar expostos.

Um ataque pode ser ocasionado por vários fatores, seja ele por motivações financeiras, demonstração de poder, prestígio, entre outros, podendo ser considerado um ato prejudicial às informações. Ele se trata de um acesso não autorizado que pode fazer modificações nas informações. Um ataque corresponde à concretização de uma ameaça, podendo ser bem sucedida ou não, mediante uma ação deliberada e por vezes meticulosamente planejada, Marciano (2009).

Pode se destacar como um dos ataques mais comuns em aplicações *web*:

- XSS (*Cross-site Scripting*) é um ataque do tipo *Injection*, que acontece quando o invasor consegue explorar a área de um site que possui conteúdos dinâmicos e consegue rodar seu código malicioso dentro do site da vítima, causando vários danos, como o roubo de contas de usuários, controle do navegador e muito mais. Weidman (2014) aponta que o XSS talvez seja a vulnerabilidade de segurança de aplicações *web* mais comum e mais questionada e quando está presente possibilita aos invasores injetar *scripts* maliciosos em sites vulneráveis. Segundo Pauli (2014), o XSS é a vulnerabilidade mais disseminada em aplicações *web* atualmente, porém, frequentemente é menosprezada como sendo apenas uma janela que abre no navegador;
- SQL *Injection* ou injeção de SQL, consiste na inserção de comandos SQL através de consultas de entradas de dados, caso a inserção seja bem sucedida o atacante poderá ter acesso a dados sigilosos do banco de dados, podendo manipular o mesmo da forma que melhor lhe convém. Segundo Weidman (2014), a página de login é um lugar natural para procurar por falhas de injeção de SQL e ataques bem-sucedidos de injeção de SQL possibilitam ler dados do banco de dados, modifica-los, desativar ou até mesmo destruir o banco de dados. De acordo com Pauli (2014), a injeção de SQL é uma das vulnerabilidades mais antigas na *web* á muito tempo vem causando prejuízos e continua proporcionando o risco mais grave às aplicações *web*.

3.1.4. Riscos

O risco é a possibilidade de que aconteça alguma ação prejudicial, é a possibilidade de um perigo iminente, onde se materializa a chance de se executar alguma ação perigosa. Para Sêmola (2003) o risco é a probabilidade de que agentes, que são as ameaças, explorem vulnerabilidades, mostrando os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos. Estes impactos são limitados por medidas de segurança, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

4. SEGURANÇA DA INFORMAÇÃO

Na atualidade é de fundamental importância que a sociedade esteja ciente dos riscos que se está exposto no meio virtual, onde se faz necessário empregar metodologias de segurança da informação. Pois é através dela que se consegue reduzir possíveis ataques de criminosos virtuais, como roubo informações, alteração de senhas e até mesmo a realização de determinadas transações, como compras e transferências de dinheiro.

De acordo com Santos e Silva (2012), a segurança da informação consiste em garantir que a informação existente em qualquer formato, esteja protegida contra qualquer tipo acesso não autorizado, está sempre disponível quando necessária, é confiável e autêntica de acordo com os atributos da segurança da informação.

Monteiro (2015) retrata que com a evolução da Internet e com o crescimento do número de aplicações *web*, a segurança é sem dúvida um assunto bastante abordado atualmente. Com a expansão das aplicações e a constante evolução da Internet, consequentemente cresce o número de usuários conectados. Dessa forma não é tarefa fácil manter-se seguro no ambiente virtual ao qual viabiliza a descoberta de vulnerabilidades por atacantes, onde a partir da exploração das vulnerabilidades se dá início ao processo de ferimento aos princípios da segurança da informação, comprometendo a segurança da aplicação.

Segundo De Carvalho (2013), as probabilidades de sucesso de um ataque a uma aplicação *web*, são realmente elevadas devido à fácil exploração das vulnerabilidades, fácil acesso a ferramentas de explorações e a grande quantidade de programadores que não se preocupam com a segurança. Muitos desenvolvedores por sua imaturidade ou desconhecimento sobre segurança da informação, se preocupam apenas em deixar a aplicação funcional menosprezando a segurança, algo indispensável na Internet.

Segundo Freitas (2009), um ataque deriva de uma ameaça inteligente e é uma ação dirigida contra as políticas de segurança da aplicação aproveitando-se de suas vulnerabilidades. A abordagem de técnicas de segurança, sendo tratadas no

processo de desenvolvimento da aplicação, amenizará drasticamente problemas relacionados à segurança da informação.

4.1. Tipos de Criptografias

O termo criptografia vem das palavras *kryptos* (oculto) e *graphein* (escrita), conhecida por ser a ciência que estuda maneiras para codificar as mensagens deixando seu conteúdo de forma secreta. O termo criptografia não é ocultar a existência da mensagem, e sim deixar escondido o seu significado, esse processo é conhecido como encriptação (SINGH, 2008).

Através do método de codificação de informação, torna-se mais seguro o envio de mensagens através da Internet, como *e-mails* ou transações bancárias e comerciais, levando em consideração que os dados trafegam por um ambiente público e vulnerável. A cada dia técnicas criptográficas são aperfeiçoadas, com objetivo de buscar altos níveis de segurança e impedir que informações mesmo que interceptadas por criminosos, não poderão decifrar a informação contida na mensagem.

De acordo com CERT.BR (2012), a criptografia é considerada como a ciência e a arte de escrever mensagens em forma de código ou cifrada, é considerada uma das principais ferramentas de segurança que se pode usar para se proteger dos riscos associados ao uso da Internet.

Pode-se destacar que a criptografia necessita de chaves para que se possa cifrar e decifrar as mensagens. Existem dois métodos para se trabalhar com chaves criptográficas, onde se pode destacar, a criptografia de chave simétrica e criptografia de chave assimétrica.

De acordo com Oliveira (2012), a criptografia de chave simétrica é o modelo mais antigo de criptografia, método conhecido também como criptografia de chave privada, onde o elemento que dá acesso à mensagem entre ambas as partes é igual. A chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem, como pelo destinatário para decodificar a mensagem.

Para que o processo funcione, todas as pessoas envolvidas no processo devem conhecer a chave, pois quando uma mensagem criptografada é enviada, só poderá ter acesso ao conteúdo quem possui a chave, utilizada principalmente para garantir a confidencialidade dos dados.

Conforme Oliveira (2012), a criptografia de chave assimétrica ou criptografia de chave pública é um método que se utiliza duas chaves, uma privada para criptografar, que fica em segredo apenas com o titular da mensagem, e outra pública para decodificar a mesma mensagem, que fica com qualquer pessoa que queira se comunicar de modo seguro.

4.2. Principais Algoritmos de Criptografia

A criptografia é uma ferramenta extremamente importante para a sociedade, ela tem o objetivo de manter as informações confidenciais, proporciona integridade, autenticidade e maior segurança. Atualmente existem vários sistemas criptográficos que são baseados em algoritmos, onde os mesmos são responsáveis em deixar os dados criptografados usando transformações complexas em sua execução, deixando um texto simples em um texto cifrado ou criptografado. Pode-se destacar alguns algoritmos importantes nesse processo criptográfico, como o DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*), RSA (Devido aos seus desenvolvedores *Rivest, Shamir, e Adleman*) e MD5 (*Message-Digest algorithm 5*).

4.2.1. DES

O DES é classificado como um modelo criptográfico simétrico criado na década de 70 e patentado pela empresa IBM (*International Business Machines*), que posteriormente tornou disponível para uso público, descreve (DE LUCCA, 1995). De acordo com Kurose e Ross (2006), o DES codifica texto aberto em proporções de 64 *bits* usando uma chave de 64 *bits*, onde oito desses *bits* da chave são *bits* de paridade ímpar, de modo que a chave DES tem efetivamente 56 *bits* de comprimento, produzindo assim um texto cifrado de 64 *bits*. Para uma eficácia maior é realizado 16 iterações e cada uma delas é utilizado uma porção diferente da chave. O mesmo método utilizado na criptografia é utilizado na decriptografia, sendo que a diferença é a sequência das chaves que são utilizadas na ordem inversa.

Segundo De Lucca (1995), o DES é um algoritmo baseado em funções que consiste em efetuar combinações, substituições e permutações entre o texto a ser codificado e a chave, a nível de *bits*, de blocos de 64 *bits* com chave de 56 *bits*.

Sua estrutura é de tal forma que, se qualquer *bit* de entrada for modificado, todos os *bits* de saída serão afetados.

Antigamente o DES era considerado extremamente seguro, porém com os crescentes avanços computacionais, foram desenvolvidas técnicas por criptoanalistas com a finalidade de quebrar a segurança de algoritmos criptográficos, com isso o DES tornou-se inseguro. Pela insegurança que o algoritmo estava sofrendo, foram desenvolvidas novas formas de deixá-lo mais seguro, surgiu então uma versão bem mais forte, chamada de 3DES (*Triple Data Encryption Standard*). Conforme Kurose e Ross (2006), o 3DES é um padrão proposto pelo governo norte-americano para substituir o DES. Ele passa a usar três chaves de 56 *bits*, onde os dados são encriptados com a primeira chave, decriptado com a segunda e finalmente encriptado novamente com a terceira chave. Isso faz o 3DES oferecer muito mais segurança que o DES.

4.2.2. AES

Segundo Souza e Oliveira (2007), o AES ou Padrão Avançado de Ciframento é um algoritmo, que surgiu a partir de um concurso lançado em 1997 pela NIST (*National Institute of Standards and Technology*), com a necessidade de escolher um algoritmo que fosse mais seguro e eficiente para substituir o DES.

Logo depois, o AES tornou-se um algoritmo padrão reconhecido pela NIST logo após vencer a batalha do concurso em cima de outros algoritmos, se mostrando um algoritmo com qualidades em segurança, rapidez e bom desempenho em software e hardware.

O AES por ser um algoritmo de chave simétrica ele processa dados em blocos de 128 *bits* e pode funcionar com chaves de 128, 192 e 256 *bits* de comprimento. O NIST estima que uma máquina que conseguisse quebrar a criptografia do DES de 56 *bits* em 1 segundo levaria aproximadamente 149 trilhões de anos para conseguir quebrar uma chave AES de 128 *bits*.

4.2.3. RSA

O algoritmo RSA teve seu desenvolvimento no MIT (*Massachusetts Institute of Technology*) em 1978 por Ron Rivest, Adi Shamir e Leonard Adleman, as

siglas fazem referência ao nome de seus criadores. O RSA foi o primeiro algoritmo desenvolvido de chaves públicas, ou seja, baseado no método de criptografia assimétrica (BARBOSA, 2003).

O algoritmo é basicamente o resultado de dois cálculos matemáticos, onde um para cifrar e outro para decifrar. Por ser de método assimétrico, usam-se duas chaves criptográficas, uma chave de domínio pública utilizada para criptografar a mensagem e a outra privada, usada para descriptografar a mensagem.

O RSA é fácil de ser implementado e utilizado para a segurança de informações em atividades comerciais e até mesmo para o envio de mensagens em ambientes inseguros. Segundo Barbosa (2003) o algoritmo RSA é muito utilizado em aplicações comerciais e foi o primeiro algoritmo assimétrico mundialmente adotado como padrão. A segurança deste sistema de criptografia está baseada nos números, pois ele é baseado na dificuldade da fatoração de número muito grande.

4.2.4. MD5

O algoritmo MD5 é uma função criptográfica *hash* que recebe uma mensagem de um determinado valor e retorna um *hash* de 128 *bits* unidirecional, desenvolvida pela empresa RSA Data Security, Inc. O algoritmo MD5 foi elaborado com o objetivo de ser utilizados em aplicações de assinaturas digitais, e é muito utilizado para integridade de arquivos e *logins* (DETOMINI, 2010).

A utilização do MD5 é muito útil quando se deseja arquivar senhas de usuário em bancos de dados, sem que o próprio administrado possa visualizar e decifrar tal senha, o que ele irá ver é apenas o MD5 *hash*.

5. CARACTERIZAÇÃO DO SITE ELEIÇÕES 2016

5.1. Surgimento da Ideia de Implementação do Site

O projeto de implementação surgiu a partir de março de 2016, quando alunos do curso de sistemas de informação da Faculdade IEducare, tiveram a ideia de formar um grupo de desenvolvimento de Software, o grupo foi composto inicialmente por Roney Damasceno Freitas, Lisandro Sousa Lima, Francisco Guilherme Portela de Vasconcelos, Juliana Machado Gomes Magalhães e Francisco Kelpson Gomes Lima, ao grupo foi atribuído o nome de *DevSystems* (Desenvolvimento de Sistemas). A proposta inicial para o primeiro software a ser desenvolvida foi motivada pelo integrante Lisandro, com sua vasta experiência de relacionamento com o setor público, onde a proposta foi de desenvolver um sistema voltado para a educação, no entanto por ser ano eleitoral, apresentou também a ideia para o desenvolvimento de um projeto destinado às eleições 2016. Todos os membros da equipe apoiaram a ideia e deu-se início ao projeto eleições 2016, deixando o projeto educação para o segundo sistema a ser elaborado.

O primeiro escopo foi chamado de Sistemas Eleições 2016, onde o mesmo seria composto por um aplicativo mobile, um site e um painel administrativo para gerenciar os conteúdos do site e do aplicativo, com o intuito de poder aprimorar as divulgações das propagandas eleitorais dos candidatos, já que os meios mais rápidos e eficientes de disseminação de propagandas hoje é através da Internet, através de sites e aplicativo mobile. Ferreira (2010) expõe que a Internet, vem se tornando o meio de interação mais importante utilizado entre as pessoas.

De acordo com Madruga (2012), propaganda eleitoral é aquela que divulgada em época de eleições, que tem como objetivo dar conhecimento ao público de determinada candidatura a cargo eletivo e, conseqüentemente, poder captar o voto do eleitor.

A ideia do site eleições 2016 foi implementar várias opções no menu, como bibliografia com breve descrição do candidato, fotos contendo as fotos dos eventos realizados, projetos mostrando os planos de governo e opção para *download*, vídeos dos eventos ocorridos, músicas da campanha com opção de

download, agendas para divulgar locais de eventos e mensagens onde o eleitor poderá enviar mensagens para o candidato. Todas essas opções estão compostas no site como mostra na figura 2 e no aplicativo, onde cada item apresentado contém informações importantes relacionadas ao candidato. Na página principal mostra na figura 2 além dos menus, fotos recentes dos eventos, foto do candidato, opções para *download* do aplicativo e uma área restrita que leva ao painel administrativo, onde somente pessoas autorizadas com usuário e senha podem acessar e fazer o gerenciamento de conteúdo do site e do aplicativo.

Figura 2 - Página Index do Site Eleições 2016



Fonte: Site Eleições 2016, 2016.

No decorrer da construção do projeto o integrante Francisco Kelson Gomes Lima deixou de fazer parte da equipe, mas o restante dos integrantes seguiram empenhados no desenvolvimento do projeto, onde o mesmo tinha prazo para ser concluído antes das eleições 2016. Nesse período o nome do grupo foi alterado para *NewSystems* (Novos Sistemas), como também, foi agregado um novo participante na equipe chamado de Diego Izidro de Sousa Gomes, com o intuito de ajudar a equipe na elaboração o projeto, pois o tempo para a finalização do mesmo estava muito próximo do previsto. Quando o projeto se encontrava em sua fase final de produção o nome do grupo foi alterado mais uma vez, pois o nome definido anteriormente, não se encontrava mais disponível para reserva de domínio, que sem opção a equipe passou a ter o nome de *BrasilSystems*.

5.2. Linguagens Utilizadas na Implementação

Para o desenvolvimento do site eleições 2016, foram utilizadas de vários recurso tecnológicos como as linguagens, HTML5, CSS3, *JavaScript*, PHP e para a responsividade da aplicação o *framework bootstrap*. Foi utilizado a ferramenta *Sublime Text 3* para a codificação, por ter um ambiente amigável e leve.

5.2.1. Sublime Text 3

De acordo com Combarros (2015), o editor *Sublime Text* é um editor de texto e código fonte, embora sua distribuição seja gratuita é um *software* proprietário. Suporta grande variedade de linguagens de programação e de marcação, dentre algumas de suas características pode-se destacar sua rapidez, adequação a linguagens de programação do lado do cliente e a opção de poder usar vários *plugins* deixando o editor ainda mais completo. Atualmente a versão do *Sublime Text 3* ainda se encontra na versão *beta*.

5.2.2. HTML5

O HTML (*HyperText Markup Language*), que, em português, significa linguagem por marcação de hipertexto, é uma linguagem de conteúdo para *web*

criada por Sir Tim Berners-Lee visando a comunicação de resultados de pesquisas científicas (SILVA 2014). Tim é também diretor e fundador da W3C (*World Wide Web Consortium*).

Após a criação do HTML com o intuito de aprimorar a utilização da linguagem, passou-se a serem criadas várias versões, surgindo então a quinta versão da linguagem, que hoje, é bastante utilizada. Essa nova versão, o HTML5 incorpora várias mudanças importantes com relação às funcionalidades do HTML, como a semântica, ou seja, implica mecanismos para dar significados às palavras publicadas, com finalidade de poder atribuir um sentido aos conteúdos das páginas, de modo que seja explícito tanto pelo o ser humano, como pelo o computador, e a incrementação de uma série de recursos que o tornaram diferenciados de todas as versões anteriores (TONSIG, 2012).

5.2.3. CSS3

O CSS (*Cascading Style Sheets*) é um simples mecanismo para adicionar estilo por exemplo, cores, fontes, espaçamento a documentos *web* (W3C, 2016). O CSS fica responsável em aplicar estilo aos elementos de páginas *web*, onde junto ao HTML deixam as páginas visualmente muito mais agradáveis.

O CSS3 é a nova versão do CSS que vem com inúmeras melhorias e características. Essa nova versão conta com melhorias onde na versão anterior não estava disponível (MIR, 2012). O CSS3 surgiu para trazer mais recursos e assim aprimorar a experiência no desenvolvimento *web*.

5.2.4. JavaScript

O *JavaScript* foi criado com o objetivo de aprimorar a experiência dos usuário com as páginas *web*, deixando as páginas mais dinâmicas. De acordo com Remoaldo (2008), o *JavaScript* é uma linguagem de *scripting* interpretada, sendo necessário a sua utilização em conjunto com outra linguagem, como é o caso de sua utilização com o HTML.

Segundo Morrison (2008), o *JavaScript* é definido como uma linguagem de programação de *scripts* que tem como propósito integrar com o lado do cliente

(*browser*), essa linguagem é muito utilizada para validar informações inseridas em campos de textos e para a realização de cálculos.

5.2.5. PHP

O PHP (é um acrônimo recursivo de PHP: *Hypertext Processor*) é uma linguagem de *scripting*, muito utilizada, e em conjunto de outras linguagens é muito utilizada especialmente no desenvolvimento *web* e pode ser utilizado em diversos sistemas operacionais sem a necessidade da alteração do código fonte (REMOALDO, 2008).

A linguagem é interpretada e muito utilizada na criação de sistemas *web*, tanto pela sua flexibilidade de compatibilidade com uma grande variedade de bancos de dados, com por ser uma linguagem simples que oferece muitos recursos para que um programador profissional possa fazer uso. Silva (2014) explana que o PHP trata-se de uma linguagem imensamente modularizada, o que a torna ideal para o uso em servidores *web* e para instalação.

5.2.6. Bootstrap

O *Bootstrap* é um *framework* de código aberto que facilita aos desenvolvedores na construção de *sites* e aplicações *web*, principalmente em relação a otimização do tempo, pois ele contém uma série de folhas de estilos e *plugins* prontos. De acordo com Minetto (2007), um *framework* de desenvolvimento é uma coleção de códigos-fonte, funções e metodologias que facilitam o desenvolvimento de novos sistemas, sendo também uma base para o desenvolvimento de algo maior ou mais específico.

Outra vantagem do *Bootstrap* e umas das maiores razões para sua utilização no Site Eleições 2016 é por seu (*Responsive Web Design*), que, em português, significa *web design* responsivo, ou seja, ele tem a capacidade de ajustar toda sua estrutura para a visualização em um maior números dispositivos. Conforme Zemel (2015), um site com *web design* responsivo pode ser acessado de um *desktop*, *notebook*, *smartphone*, *tablet*, de qualquer dispositivo com acesso à rede, independente de sua resolução, capacidade de cores ou se é *touch*.

Figura 3 - Design responsivo



Fonte: Página do Dater Tecnologia, 2016.

5.3. Sistemas de Banco de Dados Utilizado

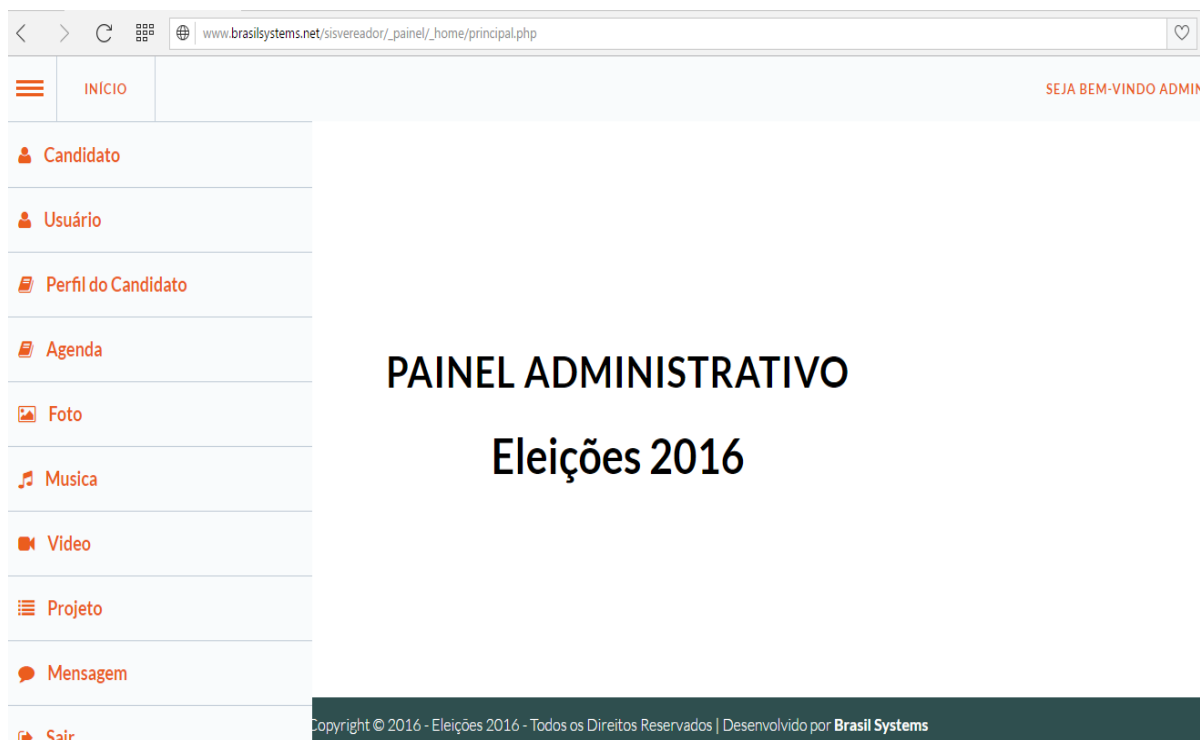
O sistema de gerenciamento de banco de dados utilizado foi o *MySQL*, por ser uma ferramenta gratuita, possui compatibilidade com a linguagem PHP, facilidade no manuseio, excelente desempenho e estabilidade. De acordo com Remoaldo (2008), o *MySQL* é um sistema de gestão de base de dados que utiliza o modelo relacional, ou seja, ele armazena os dados em tabelas compostas por linhas e colunas.

Além do banco de dados ajudar no armazenamento de conteúdos, ele facilita na automatização de obtenção de informações, como alteração, exclusão, atualização e até mesmo na criação.

5.4. Funcionalidades Implementadas no Painel de Controle

O painel de controle foi desenvolvido para facilitar o gerenciamento de conteúdo do *site* Eleições e do Aplicativo Eleições, de forma que o usuário possa disponibilizar as informações de modo rápida e fácil, permitindo também o total controle dos conteúdos que podem, ou não, ser acessados. O usuário com acesso ao painel administrativo tem disponível um menu com uma série de opções necessárias para as atualizações dos conteúdos que serão exibidos no *site* e no aplicativo, como mostra abaixo na figura 4.

Figura 4 - Menus do Painel Administrativo



Fonte: Painel Administrativo Eleições 2016, 2016.

Cada opção de menu inclui a possibilidade para fazer buscas de dados, além de realizar atividades, com edições, alterações e exclusões de dados.

5.5. Como Funciona a Interação Entre o Site e o App Eleições

A interação entre o *site* e o aplicativo é realizado através do banco de dados *MySQL*, onde, as informações são adicionadas ou alteradas através do painel administrativo, e salvas no banco de dados, que através da conexão que ambos tem com o banco de dados, conseguem obter as informações que são carregadas e mostradas aos usuários, tanto no site como no aplicativo.

6. MECANISMOS DE SEGURANÇA IMPLEMENTADOS NO PAINEL DE CONTROLE

6.1. Algoritmo de Criptografia

Pensando na segurança das senhas dos usuários, foi realizado a implementação do algoritmo de função criptografia MD5 *hash*, utilizado para deixar as senhas armazenadas no banco de dados de forma cifrada, onde nem mesmo o próprio administrador ou um possível acesso indevido ao banco de dados, poderão ter acesso ao texto claro da senha e sim um texto cifrado, dificultando qualquer possibilidade de uso indevido com as credenciais dos usuários do sistema.

Um dos sistemas de criptografia e autenticação que apresenta segurança computacional que é utilizado nas mais diversas aplicações é o algoritmo de chave pública MD5 (AZEVEDO, 2006).

6.2. Forma de Autenticação

Método de autenticação utilizada foi baseado em no reconhecimento de *login* e senha como mostra na figura abaixo.

Figura 5 - Tela de Login



A tela de login apresenta o título "ACESSO AO SISTEMA" em letras grandes e negritadas. Abaixo dele, há uma instrução: "Informe nome de Usuário e Senha para acessar." A interface contém dois campos de entrada: "LOGIN DE USUÁRIO" com um ícone de pessoa e o placeholder "Digite o Usuário", e "SENHA DE ACESSO" com um ícone de cadeado e o placeholder "Digite a Senha". No final, há um botão laranja com o texto "✓ ENTRAR".

Fonte: http://www.brasilsystems.net/sisvereador/_painel/index.php

A figura 6 mostra parte do código utilizado na implementação, responsável pela verificação de validação de usuários do sistema, onde é realizado o processo de recebimentos de nome de usuário e senha, para acesso ao painel. No código, a função *empty* tem como finalidade verificar se o usuário está passando dados vazios, caso isso aconteça à função evitará tal ação, a função *addslashes* tem a finalidade de retornar *string* com barras invertidas quando são usados caracteres indevidos que podem ser utilizados em ataques como *SQL Injection*, já a função *md5* tem a finalidade de gerar a criptografia da senha ingressada e será verificada se a mesma corresponde à senha já gravada no banco de dados. Quando o usuário ingresa seu *login* e senha é submetida a uma verificação se os dados correspondem aos dados armazenados no banco de dados, caso essa verificação seja verdadeira o usuário terá acesso ao painel administrativo, caso contrario o acesso é evitado.

Figura 6 - Implementação das variáveis de login e senha

```
1 <?php
2     if(isset($_POST['entrar'])){
3         if(!(empty($_POST['nome'])) && !(empty($_POST['senha']))){
4             $nome =addslashes($_POST['nome']);
5             $senha =md5(addslashes($_POST['senha']));
```

Fonte: Próprio autor

O processo de identificação define para o computador que realmente é o usuário e a senha corresponde a um autenticador, isto é, ela prova ao computador que o usuário é quem realmente ele diz ser (TCU, 2012).

6.3. Controle de Usuário

Os usuários que têm acesso ao painel administrativo são controlados por níveis, onde o nível 1, corresponde aos usuários administradores do sistema, podendo realizar desde criação de usuários até a publicação e aprovação de conteúdos, o nível 2, corresponde aos usuários administradores que poderão apenas gerenciar a publicação e aprovação dos conteúdos a partir do painel.

Figura 7 - Níveis de usuários

login_user	nivel_user
Francisco	2
admin	1
Juliana	1

Fonte: Próprio autor

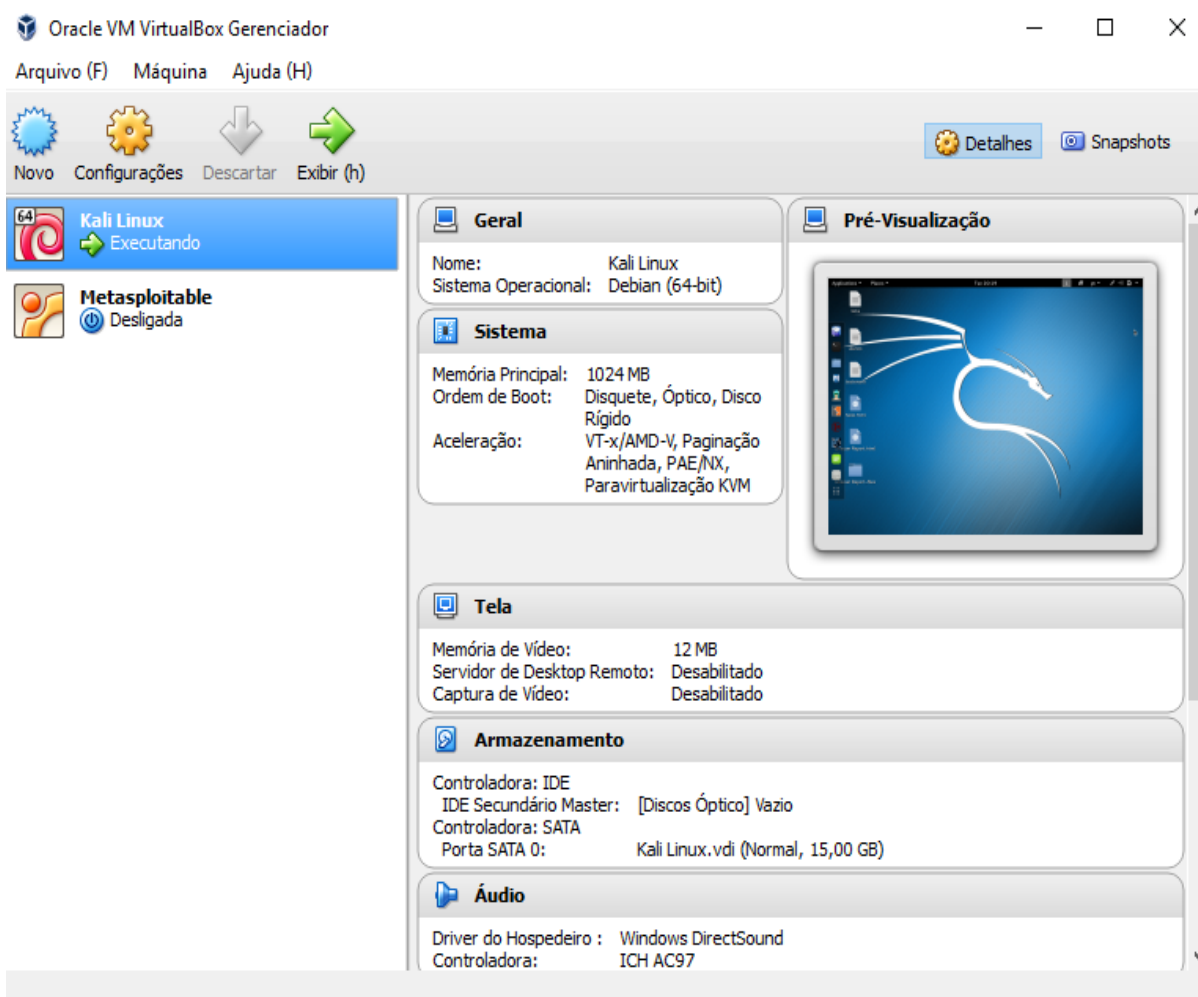
6.4. Simulações, Testes e Resultado de Ataques ao Painel do Site

Com o objetivo de verificar e futuramente corrigir falhas de segurança no painel administrativo do site eleições 2016, foram realizados alguns testes de invasão a fim de ganhar acesso a área administrativa do painel. Foram utilizadas algumas ferramentas para a exploração de vulnerabilidades e ataques onde o sistema operacional utilizado como cenário da realização das análises foi o *Kali Linux* instalado no ambiente virtualizado com o *VirtualBox*.

Segundo VirtualBox (2016), o ambiente é criado com um aplicativo de virtualização onde permite a instalação e execução de vários sistemas operacionais dentro de várias máquinas virtuais ao mesmo tempo, proporciona também o compartilhamento dos mesmo *hardware*. Ele é direcionado para servidores, desktops e uso incorporado.

Como mostra em Kali (2016), o sistema operacional *Kali Linux* é uma distribuição *Linux* baseada em *Debian* destinada a testes de penetração avançados e auditoria de segurança. O sistema contém várias ferramentas destinadas para realizar testes de segurança e adaptado especialmente às necessidades dos profissionais. Na figura 8, mostra a execução do *Kali Linux* na VM (Máquina Virtual).

Figura 8 - Execução do Kali Linux na VM



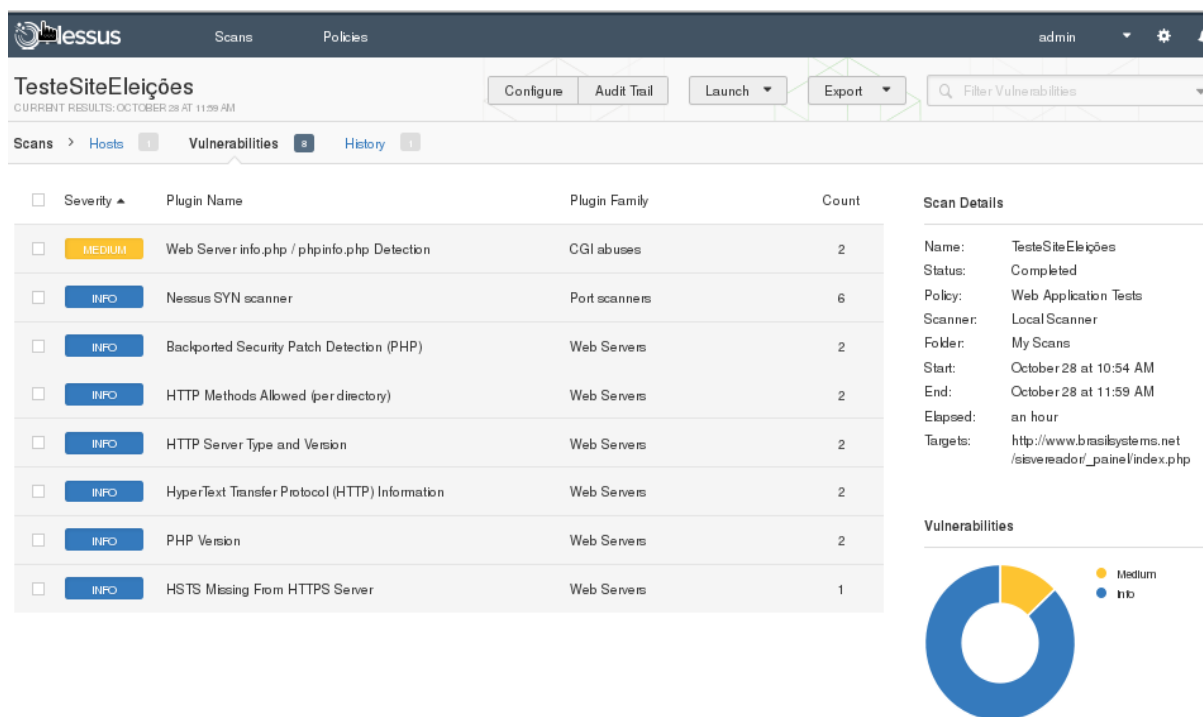
Fonte: Próprio autor

Com a finalidade de obter informações e consequentemente encontrar vulnerabilidades no painel administrativo do sistema eleições 2016, foram utilizadas algumas ferramentas, as quais serão abordadas a seguir.

- **Nessus**

Após a preparação do ambiente, foi utilizado o software Nessus, um dos mais populares para realização de testes de análises de vulnerabilidades, com o objetivo de detectar os pontos considerados fracos em seus serviços de execução. Em Pauli (2014) e Weidman (2014), aponta que o Nessus é um dos *scanners* de vulnerabilidades disponíveis mais populares para realizar o passo de *scanning* de vulnerabilidades onde seu banco de dados inclui vulnerabilidades em plataformas e protocolos, e o seu scanner realiza uma série de verificações para detecção problemas conhecidos. Na figura 9 é mostrado os resultados realizado pelo Nessus no módulo de testes para aplicações *web*.

Figura 9 - Histórico de vulnerabilidades encontradas pelo Nessus no Site Eleições 2016



Fonte: Próprio autor

Como pode ser observadora na figura 9, os resultados da varredura mostra que existem duas vulnerabilidades média e o restante apenas informações, onde os níveis são classificados como, crítico, alto, médio, baixo e informativo.

Em relação às vulnerabilidades de nível médio encontradas o Nessus relata que, caso o arquivo *php.info* seja acessado por um invasor remoto ele pode descobrir uma grande quantidade de informações sobre o servidor *web* remoto, como o nome do usuário que instalou o php e se é usuário SUDO (possui todas as permissões do sistema), endereço do *host*, versão do sistema operacional, versão do servidor *web*, diretório raiz do servidor *web* e configuração sobre instalação remoto do php. O Nessus mostra como solução para eliminar essas vulnerabilidades encontradas efetuar a remoção do arquivo afetado *php.info*.

- Nmap

O Nmap tem como finalidade fazer varreduras no alvo à procura de portas abertas, serviços ativos, versões de sistemas operacionais e vários outros tipos de *scan*. Segundo Weidman (2014), o Nmap é tido como padrão do mercado quando o assunto é scanning de portas. Já para Pauli (2014), o Nmap é o scanner de porta popularmente mais utilizado e continua a ganhar destaque como o melhor scanner

de portas do mundo, com funcionalidades adicionais para exploração de falhas e *scanning* de vulnerabilidades. Na figura 10, mostra os resultados obtidos pela Nmap.

Figura 10 - Resultados obtidos pela ferramenta Nmap

```
root@kali:~# nmap -sV -sS -O 186.202.153.147

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-11-12 15:31 EST
Stats: 0:05:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.56% done; ETC: 15:46 (0:09:24 remaining)
Stats: 0:15:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.76% done; ETC: 16:04 (0:17:50 remaining)
Stats: 0:29:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.77% done; ETC: 16:20 (0:19:57 remaining)
Nmap scan report for hm8208.locaweb.com.br (186.202.153.147)
Host is up (0.078s latency).
Not shown: 865 filtered ports, 133 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1 (protocol 2.0)
443/tcp    open  ssl/http     Apache httpd
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.38 (89%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4573.89 seconds
root@kali:~#
```

Fonte: Próprio autor

Como mostra a figura 10, o comando executado `nmap -sV -sS -O 186.202.153.147` realiza as seguintes ações:

- o `-sV` designa o *scan* como um *scan* de versão, que mostrará como resultado as versões específicas dos serviços em execução.
- o `-sS` inicia um *scan* camuflado, ou seja, ele descobre se uma porta está aberta sem se conectar totalmente com o alvo.
- o `-O` retorna informações referentes ao sistema operacional.
- o IP (Protocolo de Internet) 186.202.153.147 é equivalente ao domínio `http://www.brasilsystems.net/*`.

O resultado mostra duas portas abertas com seus respectivos serviços e versões, revelando também a existência de uma probabilidade de 89% que o sistema operacional é o *Linux 2.6.38*.

- Nikto

O Nikto é uma ferramenta que tem o objetivo de constatar diversos tipos de arquivos, configurações de programas padrões e inseguros nos servidores *web*

que podem ser passivos a algum tipo de ataque. Pauli (2014) relata que o Nikto realiza verificações relativas a 6.400 arquivos e *scripts* potencialmente perigosos, 1200 versões desatualizadas de servidores e cerca de 300 problemas específicos de versões de servidores *web*, é um scanning de vulnerabilidades de código aberto. De acordo com Weidman (2014), o Nikto é um scanner de vulnerabilidades de aplicações *web*, que procura problemas como arquivos perigosos, versões desatualizadas e erros de configuração. Na figura 11, mostra os resultados obtidos pela ferramenta Nikto.

Figura 11 - Resultados obtidos pela ferramenta Nikto

```

root@kali:~# nikto -h http://www.brasilystems.net --mutate-options 1,2,3,4,5
- Nikto v2.1.6
-----
+ Target IP:      186.202.153.147
+ Target Hostname: www.brasilystems.net
+ Target Port:    80
+ Start Time:     2016-10-28 21:17:55 (GMT-4)
-----
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect a
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the cor
e in a different fashion to the MIME type
+ Retrieved via header: 1.1 varnish-v4
+ All CGI directories 'found', use '-C none' to test none
- STATUS: Completed 3590 requests (~52% complete, 9.5 minutes left): currently in plugin 'Nikto
- STATUS: Running average: 100 requests: 0.15254 sec, 10 requests: 0.1571 sec.
- STATUS: Completed 11650 requests: currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.11691 sec, 10 requests: 0.1182 sec.
- STATUS: Completed 12390 requests: currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.11613 sec, 10 requests: 0.1172 sec.
+ 26182 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2016-10-28 22:24:25 (GMT-4) (3990 seconds)
-----
+ 1 host(s) tested
root@kali:~# █

```

Fonte: Próprio autor

Como pode ser observado, o comando realizado na figura 11, foram executadas uma série de consultas simultâneas, com o objetivo principal de verificar todos os diretórios raiz, tentar adivinhar diretórios, enumera nomes de usuários via *apache* realizando força bruta em alguns serviços, lista nomes de usuários via CGI (*Common Gateway Interface*) e testa força bruta em subdomínios.

De acordo com os resultados apresentados, alguns dados como o IP e servidor, apresenta que apenas alguns tipos de cabeçalhos não estão definidos, mas as principais consultas não conseguiram trazer resultados relevantes.

- Uniscan

O Uniscan é uma ferramenta de scanning que faz varreduras buscando vulnerabilidades em aplicações *web*, onde algumas delas pode-se destacar, como *SQL Injection* e *XSS*. Cabello (2016), comenta que o Uniscan está direcionado a segurança da informática, com o objetivo de buscar vulnerabilidades nos sistemas *web*. Na figura 12 mostra a execução da ferramenta.

Figura 12 - Execução da ferramenta Uniscan

```
root@kali:/# uniscan -u http://186.202.153.147/sisvereador/_painel/admin.php -qweds
#####
# Uniscan project                               #
# http://uniscan.sourceforge.net/               #
#####
V. 6.3

Scan date: 28-10-2016 22:30:44
=====
| Domain: http://186.202.153.147/sisvereador/_painel/admin.php/
| Server: Apache
| IP: 186.202.153.147
=====
|
| Directory check:
=====
```

Fonte: Próprio autor

O comando executado na figura 12, `-qweds` tem como objetivo ativar verificação de diretório, verificação de arquivos, verificação de `robots.txt` e `sitemap.xml`, verificações dinâmicas e estáticas. A seguir, na figura 13 pode-se visualizar os resultados obtidos pelo comando.

Figura 13 - Alguns resultados da ferramenta Uniscan

```

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:
=====
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.

Local File Include:

Remote Command Execution:

Remote File Include:
=====
Scan end date: 28-10-2016 22:37:50

HTML report saved in: report/186.202.153.147.html
root@kali:/#

```

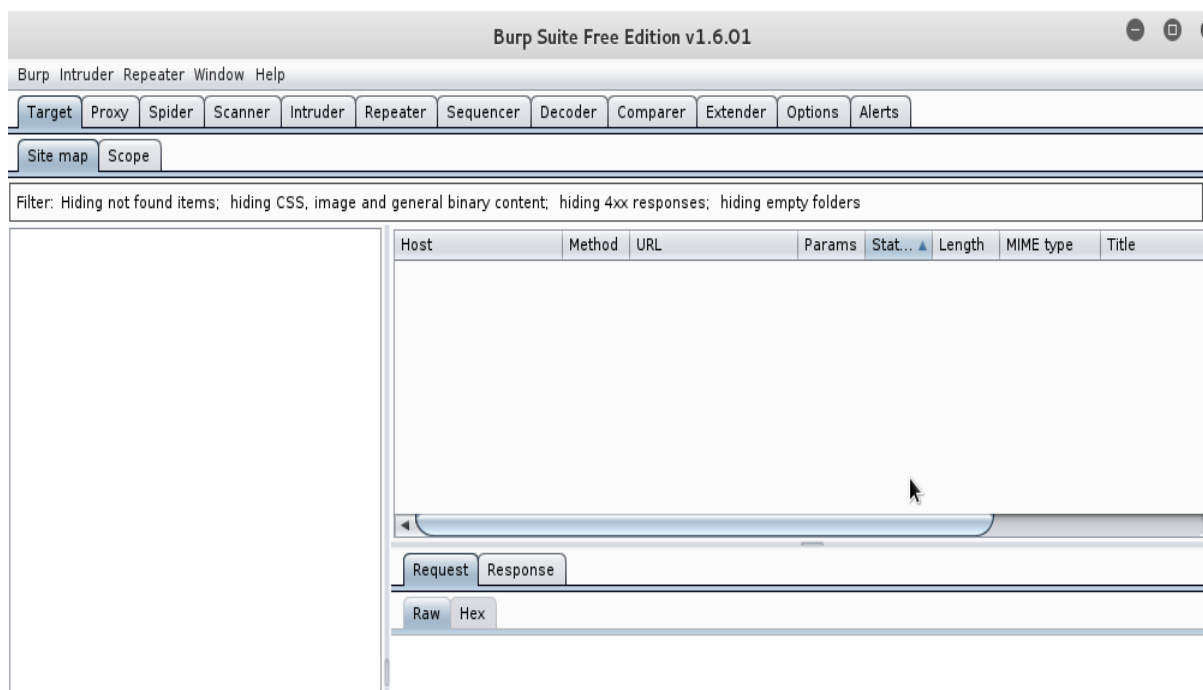
Fonte: Próprio autor

De acordo com as verificações realizadas, foi constatado que, não foram encontrados diretórios, execução de comandos remotos, inclusão de arquivos remotos, falhas de SQL Injection, falhas de XSS dentre outros.

- Burp Suite

O *Burp Suite* é uma aplicação composta por várias ferramentas de testes de penetração. Ele mapeia e analisa aplicações *web* com o objetivo de explorar as fraquezas. Trata-se de uma plataforma integrada para realizar averiguações de segurança nas aplicações *web*, interceptar tráfego HTTP e HTTPS, permite auditar se a aplicação é segura e além de observar o tráfego ele manipula as solicitações (NARVÁEZ, 2015).

Figura 14 -Interface do Burp Suite



Fonte: Próprio autor

O *Burp Suite* foi utilizado para explorar o painel do site através do método de força bruta, sendo que, para a realização do teste foi criado (*word lists*), que, em português, significa lista de palavras, onde foram usadas algumas ferramentas para automatizar no processo de criação das listas de palavras de usuários e senhas como:

- CeWL, uma ferramenta que auxilia na criação de listas de palavras, onde o mesmo analisa todo o site e captura todas as palavras nele contido e ainda auxilia na capturar de palavras do código fonte, que serão utilizados para definir nomes de possíveis usuários e senhas. O CeWL é uma ferramenta do *Kali Linux* que rastreia uma lista de palavras individuais, além de poder fornecer o número de repetições para cada palavra, salvar os resultados em arquivos e muito mais (NÁJERA-GUTIÉRREZ, 2016).

Figura 15 - Criando word list com Cewl

```

root@kali:~# cewl -m 5 http://www.brasilystems.net/sisvereador > nomes_cewl.txt
root@kali:~# ls
ativos.txt  Downloads      Pictures  Templates  wordlistest.txt
Desktop    Music          Public    theHarvester
Documents  nomes_cewl.txt roney     Videos
root@kali:~# cat nomes_cewl.txt
CeWL 5.1 Robin Wood (robin@dig.ninja) (http://dig.ninja)

Votar
desenvolvimento
software
links
widgets
Seguir
document
Prefeito
JavaScript
Brasil
Systems
Candidato
Custom
Fonts
Copyright

```

Fonte: Próprio autor

Na figura 15, o comando `cewl -m 5 http://brasilystems.net/sisvereador > nomes_cewl.txt`, cria uma lista de palavras capturadas do site, definido o mínimo 5 caracteres e salvo no arquivo criado `nomes_cewl.txt`. Após a conclusão da *word list* é realizado o comando `cat nomes_cewl.txt` para mostrar as palavras capturadas.

- Crunch, ferramenta que auxilia na criação de lista de palavras, onde a mesma possibilita a geração de inúmeras formas de combinações possíveis. Crunch é um gerador baseado em um conjunto de caracteres fornecido pelo usuário, onde se é usado esse conjunto para gerar todas as combinações possíveis (NÁJERA-GUTIÉRREZ, 2016).

Figura 16 - Criando word list com Crunch

```

root@kali:~# crunch 5 7 123456abc > senhaCrunch1.txt
Crunch will now generate the following amount of data: 42338133 bytes
40 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 5373459
root@kali:~#

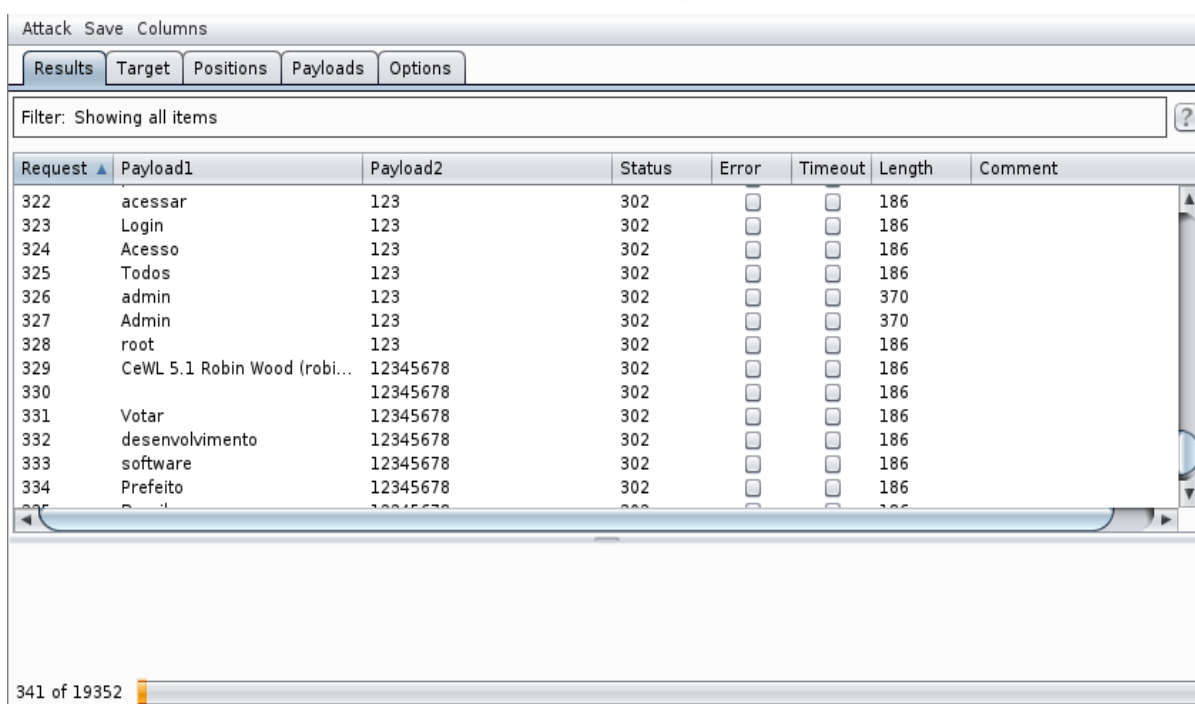
```

Fonte: Próprio autor

Na figura 16, foi realizado o comando `crunch 5 7 123456abc > senhaCrunch.txt`, onde cria uma *word list* entre 5 e 7 caracteres, contendo (1,2,3,4,5,6,a,b e c) e salvo no arquivo criado *senhaCrunch.txt*. Com a configuração especificada no comando, o arquivo foi gerado com 5.373.459 palavras.

Após a criação de usuários e senha através das ferramentas automatizadas acima, foram adicionadas pelo próprio autor alguns possíveis nomes de usuários no arquivo *nomes_cewl.txt* e senhas no arquivo *senhaCrunch.txt*, aumentando ainda mais a probabilidade de êxito no ataque. Na figura 17, mostra os resultados da força bruta.

Figura 17 - Resultado do ataque força bruta com Burp Suite



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
322	acessar	123	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
323	Login	123	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
324	Acesso	123	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
325	Todos	123	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
326	admin	123	302	<input type="checkbox"/>	<input type="checkbox"/>	370	
327	Admin	123	302	<input type="checkbox"/>	<input type="checkbox"/>	370	
328	root	123	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
329	CeWL 5.1 Robin Wood (robi...	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
330		12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
331	Votar	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
332	desenvolvimento	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
333	software	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	
334	Prefeito	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	186	

341 of 19352

Fonte: Próprio autor

De acordo com os resultados mostrados na figura 17, as requisições de número 326 e 327 apresentaram um tamanho diferente das demais requisições, logo os mesmo foram testados como credenciais no painel administrativo e com ambos foram possíveis as tentativas de acesso a área restrita do painel, passando a ter o controle de gerenciamento de conteúdo do site eleições 2016 e do aplicativo Eleições 2016.

7. CONSIDERAÇÕES FINAIS

O presente trabalho apresentou conceitos sobre a segurança da informação dando ênfase ao painel do Site Eleições 2016. Nesse contexto sabe-se que todas as aplicações *web* na Internet, estão susceptíveis a serem alvos fáceis para os criminosos virtuais, onde buscam por vulnerabilidades para a efetivação de seus ataques. Diante de tal fato, fica evidente a necessidade de buscar métodos de segurança que colaborem e contribuam contra a inibição de qualquer tipo de ataques contra aplicações *web*.

A realização de testes em aplicações *web* é de fundamental importância, pois é nesse processo onde se pode mensurar e precaver os riscos, evitando graves problemas de invasões. Durante a elaboração deste trabalho foram utilizadas de várias ferramentas para auxiliar na composição de ataques ao painel administrativo do site, com a finalidade de identificar suas vulnerabilidades.

Diante dos vários métodos abordados nos testes com as ferramentas estudadas, o método aplicado por força bruta utilizando o *Burp Suite* proporcionou um acesso indevido ao painel por meio da captura de usuário e senha através de força bruta, possibilitando ao invasor fazer qualquer tipo de alteração nas informações. Foi constatado que o próprio administrador do sistema, proporcionou tal vulnerabilidade, pelo simples fato de ter criado uma senha considerada muito fraca.

Como sugestão de trabalhos futuros, serão analisados e testados novos métodos de ataques, com a finalidade de focar nos níveis de segurança da aplicação, de maneira a aprimorar mecanismos de autenticação, criação de usuários, senhas, métodos de criptografia, validação de formulários, dentre outros. Buscando sempre proporcionar a segurança da informação na aplicação evitando qualquer tipo de ataques realizados por criminosos virtuais que venham a comprometer as informações.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de Criptografia RSA: Análise entre a segurança e velocidade**. Eventos Pedagógicos, 2012.

AZEVEDO, Manoel Socorro Santos. **Protocolo Híbrido para Autenticação Quântica de Mensagens Clássicas com uso do Gerador de Sequências Pseudo-aleatórias Blum-Blum-Shub**. 2006. Tese de Doutorado. Universidade Federal de Campina Grande.

BARBOSA, Luis Alberto de Moraes et al. **RSA: Criptografia assimétrica e assinatura digital**. 2003. 50 p. Especialização em Redes de Computadores)- Universidade Estadual de Campinas, Campinas, 2003..

CARUSO, Carlos A. A. **Segurança em Informática e de Informações**. 3º ed. rev. e ampl. - São Paulo: Editora Senac São Paulo, 2006.

CAMPOS, André L. N. **Sistema de Segurança da Informação: Controlando os riscos**. Florianópolis: Visual Books, 2006.

CARNEIRO, Alberto. **Introdução à Segurança dos Sistemas de Informação**. 2002.

CERT.BR. **Cartilha de Segurança para Internet**. 2º ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

COMBARROS GÓMEZ, Javier. **Aplicación Web y Móvil Usando Android y AngularJS Contra Spring Web Services**. 2015. Tesis Doctoral. ETSI_Sistemas_Infor.

DA UNIÃO, TCU Tribunal de Contas. **Boas Práticas em Segurança da Informação**. 4º ed Brasília: TCU, 2012.

DE CARVALHO, Fernanda Ramos et al. **Vulnerabilidades em Aplicações Web**. RE3C-Revista Eletrônica Científica de Ciência da Computação, v. 8, n. 1, 2013.

DE LUCCA, José Eduardo. **Arquitetura de Segurança para Redes Aplicada a Sistemas de Gerencia**. 1995. Tese de Doutorado. UNIVERSIDADE FEDERAL DE SANTA CATARINA

DE OLIVEIRA, Gabriella Domingos et al. **Gestão da Segurança da Informação: Perspectivas baseadas na tecnologia da informação (TI)**. Múltiplos Olhares em Ciência da Informação-ISSN 2237-6658, v. 3, n. 2, 2014.

DETOMINI, Renan Corrêa. **Exploração de Paralelismo em Criptografia Utilizando GPUs**. 2010. Tese de Doutorado. Universidade Estadual Paulista “Júlio de Mesquita Filho”.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Axcel Books, 2000.

ELIAS, Wagner. Segurança no Desenvolvimento de Software. **Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados**, p. 121, 2015.

FERREIRA, Fernando Nicolau Freit. **Segurança da Informação**. Rio de Janeiro; Editora Ciência Moderna, 2003.

FERREIRA, Marcio. **Propaganda Eleitoral na Internet**. Curitiba, 2010.

FONTES, Edison Luiz Gonçalves. **Vivendo a Segurança da Informação: Orientações práticas para pessoas e organizações**. São Paulo: Sicurezza: Brasiliano & Associados, 2000.

FREITAS, Eduardo Antônio Mello. **Gestão de Riscos Aplicada a Sistemas de Informação: segurança estratégica da informação**. 2009.

HINZ, Marco Antônio Mielke. **Um Estudo Descritivo de Novos Algoritmos de Criptografia**. 2000. Tese de Doutorado. Universidade Federal de Pelotas.

KALI, **Linux Official Documentation: What is kali linux ?**. Disponível em: <<http://docs.kali.org/introduction/what-is-kali-linux>>. Acesso em: 08 nov. 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LAUDON, K. C; LAUDON, J. P. **Gerenciamento de Sistemas de Informação**. 3. ed. Rio de Janeiro: LTC, 2001.

CABELLO, Tomás et al. **Laboratorio Virtual para el Estudio de Vulnerabilidades en la Nube**. 2016.

LOUREIRO, S. C. **Segurança da Informação: Preservação das Informações Estratégicas com Foco em sua Segurança.[SI]**, 12 2008. 66 p. Monografia de Conclusão de Curso (Especialização)-Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

MADRUGA, Sidney Pessoa. **Propaganda eleitoral. Espécies. Propaganda antecipada. Propaganda na internet. Temas de direito eleitoral no século XXI**. Brasília: Escola Superior do Ministério Público da União, p. 355-396, 2012.

MARCIANO, João Luiz Pereira. **Segurança da Informação: Uma abordagem social**. 2009.

MINETTO, Elton Luís. **Frameworks para Desenvolvimento em PHP**. São Paulo: Novatec, 2007.

MIR, et al. **Estudio de los Futuros Estándares HTML5 y CSS3: Propuesta de actualización del sitio www. mpiua. net**. 2012.

MONTEIRO, Nuno Miguel da Silva. **Estudo de Vulnerabilidades em Aplicações Web e o seu Reflexo em Domínios Portugueses**. 2015. Tese de Doutorado.

MORAIS, F. M. F.; NORONHA, I. C. P. **Uma Abordagem Histórica, Evolutiva e Aplicacional da Criptografia**. 2014.

MORRISON, Michael. **Use a Cabeça: JavaScript**. Alta Books, 2008.

NÁJERA-GUTIÉRREZ, Gilberto. **Kali Linux Web Penetration Testing Cookbook**. Packt Publishing Ltd, 2016.

NOBRE, Anna Cláudia dos Santos. **Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil**. 2009.

OLIVEIRA, José Palazzo M. de. Informação, informática e sociedade. **Revista São Paulo em Perspectiva, Fundação Estadual de Análise de Dados–SEADE, São Paulo**, v. 8, n. 4, 1994.

OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e Assimétrica-os Principais Algoritmos de Cifragem**. Segurança Digital [Revista online], v. 31, p. 11-15, 2012.

OLIVEIRA, Wender F. **Gestão de segurança da Informação**. Disponível em: <http://lms.ead1.com.br/webfolio/Mod4467/gestao_da_seguranca_da_informacao.pdf> Acesso em: 13 set. 2016.

PAULA, Najara Mara Nascimento de. **Segurança da Informação com Ênfase na Segurança Física de Acervos Informacionais**. 2008.

PAULI, Josh. **Introdução ao Web Hacking: Ferramentas e técnicas para invasão de aplicações web**. Novatec Editora, São Paulo, 2014.

PEREIRA, Fábio Dacêncio; MORENO, Edward David. **Otimização em VHDL e Desempenho em FPGAs do Algoritmo de Criptografia DES**. In: Quarto Workshop em Sistemas Computacionais de Alto Desempenho (WSCAD), São Paulo. 2003.

RAMOS, Anderson. **Security Officer–1: Guia oficial para formação de gestores em segurança**. Segunda Edição. Porto Alegre–RS: Editora Zouk, 2008.

REMOALDO, Pedro. **O Guia Prático do Dreamweaver CS3 com PHP, Javascript e Ajax**. Centro Atlântico, 2008.

SANTOS, Diana Luísa Rocha; SILVA, Rita Maria Santos. **Segurança da Informação: A norma ISO/IEC 27000 e ISO/IEC**. 2012.

STALLINGS, William. **Criptografia e Segurança de Redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão executiva**. Ed. Campus, 2003.

SILVA, Luiz Antônio da. **iFrame: Framework para o desenvolvimento de aplicações Web**. 2014.

SILVA, Mauricio Samy. **HTML5–2ª Edição: A linguagem de marcação que revolucionou a web**. Novatec Editora, 2014.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos sistemas de informação: Gestão estratégica da segurança empresarial**. Centro Atlântico, 2003.

SIMIÃO, Reinaldo Silva. **Segurança da Informação e Comunicações: Conceito aplicável em organizações governamentais**. Monografia de Conclusão de Curso (Especialização). Universidade de Brasília, 2009.

SINGH, Simon. O livro dos códigos. **A ciência do Sigilo-do Antigo Egito Criptografia Quântica**. Sétima edição, 2008.

SOUZA, R. A.; OLIVEIRA, F. B. **O Padrão de Criptografia Simétrica AES**. Laboratório nacional de computação científica. Petrópolis, 2007.

TAVARES, Carlos. **Utilização da Virtual Private Network Caso da Universidade Jean Piaget de Cabo Verde**. 2012.

TONSIG, Sérgio Luiz. **Aplicações na Nuvem-Como Construir com Html5, Javascript, Css, Php e Mysql**. Rio de Janeiro, RJ: Editora Ciência Moderna Ltda, 2012.

VIRTUALBOX. **About VirtualBox**: Disponível em: <<https://www.virtualbox.org/wiki/VirtualBox>> Acesso em: 06 de nov. de 2016.

WEIDMAN, Georgia. **Testes de Invasão: Uma introdução prática ao hacking**. Novatec Editora, São Paulo, 2014.

W3C. **Cascading Style Sheets Home Page**. Disponível em: <<https://www.w3.org/Style/CSS/>> Acesso em: 14 Out. 2016.

ZEMEL, Tércio. **Web Design Responsivo: Páginas adaptáveis para todos os dispositivos**. Editora Casa do Código, 2015.