**Faculdade de Tecnologia de Sorocaba Tecnologia em Análise e Desenvolvimento de Sistemas**

**Documentação de Desenvolvimento de Software**

**Título: Atividade 2**

**Segurança na Web**

Matheus Bueno Martins RA: 0030481823008

Sorocaba/SP

08/2020

**Introdução**

A informação é hoje uma verdadeira ferramenta de negócios, capaz de gerar valor e causar impactos nos resultados de qualquer empresa. Com a transformação digital, o sigilo sobre os dados se tornou algo ainda mais importante, já que um vazamento — ou mesmo uma perda de dados — pode causar sérios estragos.

Por isso, a preocupação das empresas com a segurança de navegação web cresce cada vez mais. Mesmo sites seguros e conhecidos estão sujeitos a servir de vetor para vírus e ciberataques.

**O que é segurança na navegação web ?**

Ao mesmo tempo em que a internet provê uma série de benefícios para o uso doméstico e corporativo, ela representa uma porta aberta para operações de diferentes tipos. Assim, separar as trocas de dados seguras das indesejadas se torna um verdadeiro desafio.

A segurança de navegação web é um conceito que ainda não recebe o nível de atenção merecido pelas empresas. Segundo uma pesquisa de 2017 da Forbes, somente 24% das organizações contam com um plano de respostas a incidentes, como ataques malware.

O principal problema é geralmente o desconhecimento dos riscos e o tamanho dos possíveis prejuízos. Os ataques ransomware de 2017 são bons exemplos do estrago que um sequestro de dados pode causar — as perdas chegam na casa dos bilhões de dólares ao ano.

E os meios utilizados para os ataques são variados. Um pen drive ou CD infectado são bons exemplos disso. Entretanto, é na navegação web que estão os maiores riscos de ameaças virtuais.

Com a ampliação dos negócios no ambiente digital, a variedade de plataformas e sites acessados pelos funcionários de qualquer empresa é muito grande. Consequentemente, os riscos também crescem.

Portanto, a segurança de navegação web depende diretamente de uma infraestrutura digital de proteção e do comportamento adequado dos usuários da rede.

**Por que se preocupar com isso ?**

É normal se questionar sobre o tamanho do prejuízo de um ciberataque a qualquer empresa. À primeira vista, muitos gestores e empresários tendem a acreditar que isso não vai acontecer pois as informações na rede não são de interesse alheio. Entretanto, não é preciso ser um banco e movimentar dinheiro em seu servidor para se tornar um alvo.

Mesmo a menor das empresas conta com informações delicadas em cada computador. Uma lista de contatos e dados de clientes e fornecedores salva em uma planilha, por exemplo, deve ser bem protegida. Um vazamento ou a perda desses dados compromete os processos operacionais, gera atrasos e pode até acabar na justiça.

Afinal, se um cibercriminoso rouba dados de sua empresa que expõem a identidade e outras informações de clientes, há o risco de um processo judicial. Imagine então sofrer ataque ransomware como o WannaCry, no qual um computador infectado transmite o vírus para todos os dispositivos conectados à rede da empresa e criptografa seus dados.

Quebrar a criptografia é quase inviável e pagar um resgate a criminosos sem qualquer garantia de retorno é algo pelo qual ninguém quer passar. Por isso, é fundamental estabelecer mecanismos de proteção e contar com uma política de segurança eficiente.

A navegação web deve ser uma ferramenta para gerar valor aos seus negócios — e não para colocá-los em risco.

**Lista das 10 principais vulnerabilidades:**

### ***1. Injection***

Esse tipo de falha é muito conhecida pela técnica *SQL Injection*, onde o invasor realiza consultas indevidas no banco de dados, por meio de um formulário ou URL.

Com isso, o hacker consegue logar em seu sistema com privilégios de administrador, e explorar este acesso como desejar.

### ***2. Broken Authentication***

Essa falha ocorre quando o sistema não utiliza métodos confiáveis de autenticação e armazenamento das informações do usuário, com credenciais de acesso que facilitam ataques de força bruta.

Um dos exemplos mais comuns de *broken authentication* é utilizar senhas muito curtas que facilitam ataques de força bruta. Normalmente, é a primeira forma que um cracker tentará utilizar para invadir seu sistema.

A solução mais imediata para este problema é criar uma política de senhas seguras, com mínimo de caracteres, combinação de letras e números, etc.

### ***3. Sensitive Data Exposure***

As ferramentas de inspecionar elementos em uma página ou aplicação web, como o *Chrome DevTools*, estão entre as ferramentas preferidas dos desenvolvedores, e também dos hackers mal-intencionados.

Muitas APIs não protegem devidamente as informações que são transmitidas através delas, o que permite que invasores tirem proveito dos parâmetros retornados por ela, simplesmente inspecionando a aba ‘network’ do seu sistema.

Quanto a isso, é necessário dedicar uma atenção especial ao definir como estas informações vão trafegar pela interface, e criptografá-las devidamente.

### ***4. XML External Entities (XXE)***

Esta vulnerabilidade é específica de sistemas que trabalham com a linguagem XML, como por exemplo, software emissores de documentos fiscais eletrônicos.

Invasores podem explorar processadores de XML vulneráveis, onde é possível injetar códigos maliciosos e enviar para uma aplicação que fará a leitura desse XML.

### ***5. Broken Access Control***

Essa falha ocorre em aplicações que possuem páginas, rotas com informações que apenas o administrador deveria ter acesso, porém o controle de usuários não funciona.

Neste formato, o hacker consegue autenticar-se como administrador, e a partir daí, acessar, copiar e até excluir seus dados.

Para prevenir problemas de *broken access control*, é necessário que a validação do perfil de acesso venha do seu servidor, e não possa ser alterada externamente.

### ***6. Security Misconfiguration***

Se trata de configurações padrão de fábrica, informações abertas na nuvem, headers http configurados incorretamente, erros verbosos que indicam com precisão o motivo do erro.

A solução desse problema é bem simples: sempre lembre-se de excluir os arquivos e configurações default dos frameworks que utilizar. Alguns frameworks vão te lembrar disso após a instalação. Outros, não.

### ***7. Cross-Site Scripting (XSS)***

Assim como SQL Injection, essa falha é muito conhecida na internet. Através dela, invasores conseguem inserir códigos maliciosos de javascript e tags html na página.

Normalmente, o *cross-site scripting* requer um determinado comportamento do usuário, como acessar um link específico. No entanto, quando bem executada, este tipo de fraude é muito difícil de identificar, principalmente para usuários leigos.

### ***8. Insecure Deserialization***

Falha muito utilizada para execução remota de códigos maliciosos. Mesmo quando essa falha de segurança não resulta em um acesso remoto por parte do hacker, ele podem utilizar a brecha para uma escalação de privilégios, configurando-se como administrador.

### ***9. Using Components with Known Vulnerabilities***

Mesmo que sua aplicação esteja desenvolvida seguindo um padrão seguro, as bibliotecas de terceiros que sua aplicação utiliza podem possuir falhas que são conhecidas na internet. Isso resulta em exploits, softwares prontos para serem utilizados para uma invasão.

Assim, é necessário ficar atento a possíveis vulnerabilidades de todos os componentes, bibliotecas e APIs que você irá consumir em seu software.

### ***10. Insufficient Logging & Monitoring***

Um sistema sem logs, não consegue detectar que em algum lugar de sua API/Sistema alguém está tentando explorar alguma falha.

Muitos desenvolvedores são resistentes a implementar um módulo de logs no seu sistema, principalmente devido ao peso destes dados no banco. Se este for o problema, defina um período de auto-exclusão do log que você pode suportar. Um mês é o mínimo!

Outra solução é o monitoramento em tempo real, que permite a você e sua equipe perceber comportamentos estranhos no seu sistema, como picos ou quedas absurdas de acesso.

Assim, é importante manter painéis de informações ao vivo da sua aplicação, normalmente em monitores ou televisores sempre ligados nesta tela, com alertas sonoros caso julgue necessário.

**Conclusão**

Hoje em dia, a informação está valendo muito dinheiro, em alguns casos valendo mais que o petróleo. Isso acaba atraindo a atenção de criminosos que querem ganhar dinheiro com o roubo delas. Por isso, hoje em dia, é de extrema importância cuidar da segurança do seu sistema, já que você desenvolveu ele para trazer facilidades e não mais problemas.

**Referências**

SERRA, Gabriel. **Segurança em aplicações web: as 10 principais vulnerabilidades**. 2019. Disponível em: https://blog.tecnospeed.com.br/seguranca-em-aplicacoes-web/. Acesso em: 26 ago. 2020.

.BRASIL, Hsc. **Dicas de segurança de navegação web para sua empresa**. 2018. Disponível em: https://www.hscbrasil.com.br/dicas-de-seguranca-de-navegacao-web/. Acesso em: 26 ago. 2020.