Sumário

Histórico					
Versão	Elaborado por	Data	Revisado por	Data	Principais Alterações
1.0	Edenilton Soares - ejsoares	13.05.2021	Maria das Graças - mgsmfernandes		

Objetivo

Prover aos membros da equipe de infraestrutura um framework para avaliar o nível de requerimentos de segurança que deve ser utilizado e guiar a equipe de Segurança Operacional na seleção destes requisitos para sua implementação, garantindo assim uma maior segurança.

Introdução

A implementação de uma metodologia que possa auxiliar no desenvolvimento seguro é um dos principais pontos dentro de um processo de segurança. Os requisitos apresentados neste documento foram definidos com base nas especificações propostas pelo Open Web Application Security Project® (OWASP) e Center For Internet Security (CIS).

Níveis de Implementação

O documento apresenta três níveis de verificação que devem ser observados durante o processo de configuração do serviço. Cada um dos níveis aqui apresentados tem sua particularidade e profundidade.

Nível 1 - Segurança Mínima Necessária	Nível 2 - Padrão para web	Nível 3 - Alto Valor, Garantia, Segurança e Resiliência
Para níveis baixos de garantia de segurança. Apresenta o nível mínimo de segurança esperado para qualquer aplicação web.	Para aplicações que contêm dados sensíveis. É o nível recomendado para a maioria das aplicações.	Para as aplicações mais críticas, que requerem o mais alto nível de confiança.

Nível 1 - Segurança mínima

Para se adequar a este nível, a aplicação não deve possuir vulnerabilidades de fácil descoberta e exploração, bem como as listadas no TOP 10 da OWASP ou mesmo em outras listas de vulnerabilidades similares classificadas como críticos e altos.

O nível 1 é considerado o mínimo de segurança para qualquer aplicação, no entanto, se os dados que devem ser protegidos por sua aplicação são críticos, raramente somente o Nível 1 trará o nível de proteção recomendado de segurança.

Nível 2 – Segurança Recomendada

Um serviço atinge o nível 2 se tiver resiliência suficiente contra a maioria dos riscos associados a ataques através de recursos externos. Portanto, deve ser utilizado como o nível padrão de segurança. Este nível, que é apropriado para aplicações que tratam dados sensíveis, garante que os controles de segurança existem, funcionam e são utilizados dentro da aplicação.

Ameaças a aplicações neste nível serão tipicamente feitas por atacantes habilidosos e motivados, focando em alvos específicos, utilizando ferramentas e técnicas efetivas para o descobrimento e exploração de fraquezas dentro de aplicações.

Características da Aplicação
Armazena, transmite ou processa dados pessoais, confidenciais ou sensíveis de funcionários, parceiros de negócio, terceiros ou prestadores de serviço
Aplicações cuja integridade é crítica.

Nível 3 – Segurança Alto valor, garantia e resiliência

Este nível é o mais alto e é normalmente reservado para serviços que requerem níveis significativos de verificações de segurança, como em situações de infraestrutura crítica, quando realizam processos críticos para o negócio ou funções sensíveis, quando é necessária a garantia da sua integridade para o funcionamento do negócio, ou seja, nível de segurança 3 é exigido em cenários onde uma falha pode provocar um impacto significativo nas operações da organização.

Características da Aplicação
Aplicações que executam funções críticas, onde a falha pode afetar significativamente as operações. Ex: uma aplicação interna que seja utilizada por várias outras, Sefaz Identity, Portal de Assinaturas, etc Aplicações que manipulam informações sigilosas ou que realizam processos críticos para o negócio ou funções sensíveis. Ex.: manipulação de informações sujeitas ao sigilo fiscal.

Seleção dos Requisitos de Segurança

Para o processo de seleção dos requisitos de segurança ser eficiente, deve-se aplicar uma avaliação mista, levando em consideração os ativos que devem ser protegidos e os riscos mapeados.

O anexo 1 apresenta uma lista de requisitos de segurança propostos, divididos nos três níveis de segurança. Além disso, os requisitos propostos nos anexos, não deverão ser tratados como únicos. Caso seja notada a necessidade de adição de um requisito, o mesmo pode e deve ser adicionado à sua respectiva tabela dentro do respectivo anexo.

A partir destes anexos, o PO irá gerar a Lista de Requisitos de Segurança, que será passada para a fase de sprint de desenvolvimento. Para gerar esta Lista de Requisitos de Segurança do Projeto, considere utilizar ferramentas, Kanban boards, Scrum ou tabelas que facilitarão na seleção e acompanhamento da implementação dos requisitos.

Anexo 1 – Requisitos de Segurança para Aplicações Web

Este anexo apresenta os controles que devem ser avaliados, e caso atendam às necessidades de segurança da solução, devem ser aplicados. Esta lista de requisitos foi baseada primordialmente no CIS (Center For Internet Security) que apresenta uma lista das técnicas de boas práticas que deveriam ser incluídas em toda configuração inicial de recursos com finalidade de desenvolvimento de software.

1. Requisitos de Configuração Tomcat

1.1. Remoção Recursos Externos

#	Descrição	1	2	3
1.1.1.	Recomenda-se a remoção de arquivos e diretórios desnecessários publicados por padrão após a instalação. Remover recursos desnecessários publicados para internet é uma medida de defesa em profundidade que reduz vetores de risco. CIS: Apache Tomcat – Pag 09.	✓		
1.1.2.	Recomenda-se a modificação do arquivo de string **Server.info** que contém informações sobre o serviço utilizado, este valor é apresentado aos clientes quando conectam ao servidor TOMCAT. A alteração desse atributo irá contribuir para o aumento da complexidade para os invasores identificarem vulnerabilidades com ferramentas padrões. CIS: Apache Tomcat – Pag 13.	✓		
1.1.3.	Quando instalamos o Apache Tomcat por padrão vêm aplicações que não são utilizadas e deixam brechas de segurança, portanto remova antes da instalação da aplicação solicitada pelo desenvolvimento. Exemplo: docs, host-manager, manager, root.	✓		
1.1.4.	Recomenda-se a remoção de métodos desnecessários (PUT, DELET e TRACE). As informações de diagnóstico, como as encontradas na resposta a uma solicitação TRACE, geralmente contêm informações confidenciais que podem ser úteis para um invasor. Ao impedir que o Tomcat forneça essas informações, o risco de vazar informações confidenciais para um invasor em potencial é reduzido CIS: Apache Tomcat – Pag: 23	✓		
1.1.5.	Remover Server Banner Recomenda-se alterar a informação do banner de serviço, o atributo server.info contém o nome do serviço de aplicativo. Este valor é apresentado aos clientes Tomcat quando os clientes se conectam ao servidor Tomcat. CIS: Apache Tomcat – Pag: 13	✓		

1.1.6.	Recomenda-se que seja aplicado o HTTPOnly para configuração de cookie seguro no arquivo web.xml:	✓		

1.2. Limitar Exposição de Informação

1.2.1.	Recomenda-se a modificação do arquivo de string Server.info que contém informações sobre o serviço utilizado, este valor é apresentado aos clientes quando conectam ao servidor TOMCAT. A alteração de atributo irá contribuir para o aumento da complexidade para os invasores identificarem vulnerabilidades com ferramentas padrões. CIS: Apache Tomcat – Pag 13.	✓		
1.2.2.	Recomenda-se a alteração do atributo server.number que expõe informações sobre a versão do webserver que está em execução. Essa informação contribui para criação de scripts automatizados para exploração do webserver. CIS: Apache Tomcat – Pag 15.	✓		
1.2.3.	Recomenda-se a modificação para FALSE do cabeçalho HTTP X-Powered-By. Isso ajudará a impedir que o webserver anuncie sua presença, aumentando a complexidade para os invasores determinarem quais vulnerabilidades afetam a plataforma do serviço utilizado pelo servidor. CIS: Apache Tomcat – Pag 19.	✓		
1.2.4.	Recomenda-se a desativação do cliente voltado para **Stack Traces**, devido a depuração conter informações que poderiam ser uteis durante uma tentativa de exploração. Quando ocorre erro de funcionalidade durante o processamento de uma solicitação o webserver acaba exibindo informação de depuração ao cliente solicitante. CIS: Apache Tomcat – Pag 21.	✓		

1.2.5.	Recomenda-se a desativação dos métodos “HTTP TRACE, PUT e DELETE” devido fornecerem informações de depuração e diagnóstico para uma determinada solicitação. As informações de diagnóstico, como as encontradas na resposta de uma solicitação TRACE, geralmente contêm informações confidenciais que podem ser úteis para um invasor. Ao impedir que o Tomcat forneça essas informações, o risco de vazar informações confidenciais para um invasor em potencial é reduzido. CIS: Apache Tomcat – Pag: 23	✓		

1.3. Proteger as configurações do Tomcat

1.3.1.	Recomenda-se que a propriedade do $CATALINA_HOME seja tomcat_admin:tomcat, também é recomendado que a permissão no bloco $CATALINA_HOME bloqueie leitura, escrita e execução (o-rwx) e bloqueie o acesso de escrita ao grupo (g-w) CIS: Apache Tomcat – Pag: 31	✓		
1.3.2.	Recomenda-se que a propriedade do $CATALINA_BASE seja tomcat_admin:tomcat, também é recomendado que a permissão no bloco $CATALINA_BASE bloqueie leitura, escrita e execução (o-rwx) e bloqueie o acesso de escrita ao grupo (g-w) CIS: Apache Tomcat – Pag: 34	✓		
1.3.3.	Recomenda-se que a propriedade do $CATALINA_HOME/conf que contém arquivos de configuração seja tomcat_admin:tomcat, também é recomendado que as permissões neste diretório **neguem** leitura, gravação e execução (o-rwx) e **neguem** acesso de gravação ao grupo (g-w) CIS: Apache Tomcat – Pag: 35	✓		
1.3.4.	Recomenda-se que a propriedade do **$CATALINA_HOME/logs** que contém arquivos de logs seja tomcat_admin:tomcat, também é recomendado que as permissões neste diretório **neguem** leitura, gravação e execução (o-rwx). CIS: Apache Tomcat – Pag: 37	✓		
1.3.5.	Recomenda-se que seja definida como tomcat_admin:tomcat a propriedade do **$CATALINA_HOME/Temp** que e usado pelo tomcat para manter informações temporárias, também é recomendado que as permissões neste diretório **neguem** leitura, gravação e execução (o-rwx). CIS: Apache Tomcat – Pag: 39	✓		

1.3.6.	Recomenda-se que seja definida como tomcat_admin:tomcat a propriedade do **$CATALINA_HOME/bin** que fazem parte do tempo de execução do tomcat, também é recomendado que as permissões neste diretório **neguem** leitura, gravação e execução (o-rwx). CIS: Apache Tomcat – Pag: 41	✓		
1.3.7.	Recomenda-se que seja definida como tomcat_admin:tomcat a propriedade do **$CATALINA_HOME/webapps** que contém aplicativos da web que são implementados por meio do tomcat, também é recomendado que as permissões neste diretório **seja** leitura, gravação e execução (o-rwx) e **negue** o acesso de gravação do grupo (g-w). CIS: Apache Tomcat – Pag: 43	✓		
1.3.8.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **catalina.policy**, devido ser um arquivo usado para configuração de políticas de segurança ao tomcat. CIS: Apache Tomcat – Pag: 47	✓		
1.3.9.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **catalina.properties**, devido ser um arquivo de propriedades java que possuí configurações para tomcat incluindo informações de classes, listas de pacotes de segurança e propriedades de desempenho. CIS: Apache Tomcat – Pag: 45	✓		
1.3.10.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **context.xml** do Tomcat para que não seja feita nenhuma alteração não autorizada, o arquivo é carregado por todos os aplicativos da web. CIS: Apache Tomcat – Pag: 49	✓		
1.3.11.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **logging.properties** do Tomcat para que não seja feita nenhuma alteração não autorizada. Restringir o acesso a esse arquivo impedirá que os usuários locais alterem de forma maliciosa ou inadvertida a política de segurança do Tomcat. CIS: Apache Tomcat – Pag: 51	✓		

1.3.12.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **server.xml** do Tomcat para que não seja feita nenhuma alteração não autorizada, o arquivo contém definições e configurações de server Tomcat. Restringir o acesso a esse arquivo impedirá que os usuários locais alterem de forma maliciosa ou inadvertida. CIS: Apache Tomcat – Pag: 53	✓		
1.3.13.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **tomcat-users.xml** do Tomcat para que não seja feita nenhuma alteração não autorizada, o arquivo contém informações de autenticação para aplicativos do tomcat. Restringir o acesso a esse arquivo impedirá que os usuários locais alterem de forma maliciosa ou inadvertida. CIS: Apache Tomcat – Pag: 55	✓		
1.3.14.	Recomenda-se que seja devidamente controlado os acessos ao arquivo **web.xml** do Tomcat para que não seja feita nenhuma alteração não autorizada, o arquivo armazena configurações de aplicativos. Restringir o acesso a esse arquivo impedirá que os usuários locais alterem de forma maliciosa ou inadvertida. CIS: Apache Tomcat – Pag: 57	✓		

1.4. Segurança do Conector

1.4.1.	Recomenda-se que o método de autenticação seja através de certificado que é considerado mais seguro do que a utilização de senha. Autenticação de certificado de cliente requer que cada cliente se conecta ao servidor tenha um certificado para autenticação tornando assim o método de autenticação mais forte. CIS: Apache Tomcat – Pag: 64	✓		
1.4.2.	Recomenda-se que TLS/SSL seja utilizado para qualquer conector que envie ou receba informações confidenciais, como credenciais de autenticação ou informações pessoais. A configuração SSL-Enable garante que o SSL esteja ativo, garantindo a confidencialidade e integridade das informações confidenciais. CIS: Apache Tomcat – Pag: 66	✓		

1.4.3.	Recomenda-se que seja definido como **true** o atributo "**Secure**", usado para transmitir o status de segurança do conector para aplicativos que operam no conector através da request.isSecure(). Relatar com precisão o estado de segurança do conector ajudará a garantir que os aplicativos construídos no tomcat. CIS: Apache Tomcat – Pag: 68	✓		
1.4.4.	Recomenda-se que os protocolos anteriores a TLSv1.2 sejam desativados, garantindo que apenas os protocolos TSL1.2 e 1.3 estejam habilitados. CIS: Apache Tomcat – Pag: 70	✓		

1.5. Projeta as Informações de Logging

1.5.1.	Recomenda-se que seja estabelecido perfis de registros por aplicativos e que todos os eventos de aplicação sejam armazenados. Por padrão, java.util.logging não fornece os recursos para definir as configurações de aplicativo da web, apenas por VM. Para superar essa limitação, o Tomcat implementa como um wrapper para java.util.logging. CIS: Apache Tomcat – Pag: 72	✓		
1.5.2.	Recomenda-se que os eventos sejam encaminhados através dos manipuladores para fontes de armazenamento além das informações salvas em disco. Garantindo que os eventos não sejam perdidos em casos de falhas ou tentativas de exclusões acidentais e maliciosas. CIS: Apache Tomcat – Pag: 74	✓		
1.5.3.	Recomenda-se que o atributo className esteja definido como AccessLogValve. O atributo className determina o registro de acesso a ser usado. Algumas válvulas de registro não são adequadas para produção e não devem ser usadas. Apache recomenda org.apache.catalina.valves.AccessLogValve. CIS: Apache Tomcat – Pag: 76			
1.5.4.	Recomenda-se que o local de armazenamento dos logs seja protegido contra tentativas maliciosas. Proteger a localização do log ajudará a garantir a integridade e confidencialidade do aplicativo da web. CIS: Apache Tomcat – Pag: 78 e 82	✓		

1.6. Configuração Policies Catalina

1.6.1.	Recomenda-se a restrição do acesso ao tempo de execução a pacotes sensíveis. O **package.access** concede ou revoga o acesso aos pacotes listados durante o tempo de execução. CIS: Apache Tomcat – Pag: 84			

1.7. Application Deployment

1.7.1.	Recomenda-se que os aplicativos sejam executados em uma sendbox usando o **security manager.** O security Manager restringe quais classes o tomcat pode acessar, protegendo o servidor contra erros, vírus e malware. CIS: Apache Tomcat – Pag: 86	✓		
1.7.2.	O Tomcat permite a implantação automática de aplicativos enquanto o Tomcat está em execução. Recomenda-se que esse recurso seja desativado. Isso pode permitir que aplicativos mal-intencionados ou não testados sejam implantados e deve ser desativado. CIS: Apache Tomcat – Pag: 88 e 89			

1.8. Configurações Diversas

1.8.1.	Recomenda-se que o conteúdo da web seja armazenado em uma partição separada dos arquivos de configuração do **tomcat.** CIS: Apache Tomcat – Pag: 90	✓		
1.8.2.	Recomenda-se que seja aplicado o controle de menor privilégio ao acesso as configurações de administração da aplicação. CIS: Apache Tomcat – Pag: 92 e 94	✓		
1.8.3.	Recomenda-se que seja aplicada a segurança de TLS/SSL na configuração do web.xml, por padrão ao acessar o aplicativo de gerenciamento, informações de login são enviadas pela rede em texto claro. CIS: Apache Tomcat – Pag: 96	✓		
1.8.4.	Recomenda-se que o aplicativo de gerenciamento do tomcat deve ser renomeado para dificultar a localização por invasores ou scripts automatizados. CIS: Apache Tomcat – Pag: 98	✓		

1.8.5.	Recomenda-se desativar a sessão Recycle_Facades. Quando o Recycle_Facades é definido como falso, o tomcat irá reciclar a sessão entre as solicitações, o que pode resultar em vazamento de informação. CIS: Apache Tomcat – Pag: 102	✓		
1.8.6.	Recomenda-se configurar o connectionTimeout que permite que os soquetes ociosos após um período especifico de tempo sejam encerrados para economizar recursos do sistema. Fechar soquetes ociosos reduz o uso de recursos do sistema, o que pode fornecer melhor desempenho e ajudar a proteger contra ataques de DDOS. CIS: Apache Tomcat – Pag: 104	✓		
1.8.7.	Recomenda-se limitar o tamanho da solicitação de cabeçalho pode ajudar a proteger contra solicitações de negação de serviço. O **maxHttpHeaderSize** limita o tamanho dos cabeçalhos de solicitação e resposta definidos em bytes. CIS: Apache Tomcat – Pag: 106	✓		
1.8.8.	Recomenda-se que não seja permitido a utilização de **link simbólico.** Permitir links simbólicos torna o Tomcat suscetível à vulnerabilidade de travessia de diretório. Além disso, existe a possibilidade de um aplicativo estar vinculado a outro aplicativo ao qual não deveria estar vinculado. CIS: Apache Tomcat – Pag: 108			
1.8.9.	Não executar aplicação com elevação de privilégios. Em todo context.xml, defina o atributo privilegiado como false, a menos que seja necessário, como o aplicativo gerenciador: Executar um aplicativo em modo privilegiado permite que um aplicativo carregue o gerenciador de bibliotecas. CIS: Apache Tomcat – Pag: 111	✓		
1.8.10.	Recomenda-se não permitir solicitações de contexto cruzado. Permitir crossContext cria a possibilidade de um aplicativo malicioso fazer solicitações a um aplicativo restrito. CIS: Apache Tomcat – Pag: 112			

1.8.11.	Não resolva hosts em logging valves, definir enableLookups como true no conector resultará em pesquisas de DNS para obter o nome do host do cliente remoto antes de registrar qualquer informação. Nos elementos Connector, defina o atributo enableLookups como false ou remova-o. CIS: Apache Tomcat – Pag: 113	✓		
1.8.12.	Recomenda-se habilitar o JRE Memory Leak Prevention Listener para fornecimento de soluções para prevenir a memória. CIS: Apache Tomcat – Pag: 115	✓		
1.8.13.	Recomenda-se que seja criptografado o armazenamento de senhas em texto simples pode permitir que os usuários com acesso para ler o arquivo tomcat-users.xml para obter as credenciais do usuário que recebeu funções atribuídas para o aplicativo gerenciador. o Apache Tomcat vem com um aplicativo gerenciador que requer usuários com uma função de manager-gui, manager-status, manager-script e / ou manager-jmx para autenticar. Os nomes de usuário e senhas para fazer logon no aplicativo gerenciador são armazenados no tomcatusers.xml em texto simples por padrão. CIS: Apache Tomcat – Pag: 121	✓		