OWASP

The Open Web Application Security Project

06/09

OWASP Application Security Verification Standard 2009

– Web Application Standard

Versão em Português (Brasil) - PT-BR

release

Prefácio

Este documento define quatro níveis de verificação de segurança em aplicações Web. A segurança no nível da aplicação concentra-se na análise dos componentes que integram a camada de aplicação do modelo de referência OSI (Open Systems Interconnection Reference Model), ao invés de focar, por exemplo, nos níveis mais baixos do sistema operacional ou da rede. Cada nível descrito neste documento inclui um conjunto de requisitos para verificação da eficácia dos controles de segurança que protegem as aplicações Web.

Os requisitos foram desenvolvidos com os seguintes objetivos em mente:

- *Usar como uma métrica* – Fornecer aos desenvolvedores e proprietários de aplicações um ponto de referência que permita avaliar o grau de confiança que pode ser colocado em suas aplicações Web,
- *Usar como orientação* – Orientar os desenvolvedores de controles de segurança sobre o que construir a fim de satisfazer os requisitos de segurança de aplicações[1], e,
- *Usar durante a aquisição* – Fornecer uma base para a especificação dos requisitos de verificação de segurança de aplicações em contratos[2].

Os requisitos foram definidos para atender os objetivos acima assegurando a validação de como os controles de segurança são projetados, implementados e usados por uma aplicação. Os requisitos garantem que os controles de segurança usados por uma aplicação funcionam com uma estratégia de negar por padrão, são centralizados, estão localizados no lado do servidor, e são todos utilizados sempre que necessário.

Copyright e Licença

[1] Para mais informações sobre a criação e utilização de controles de segurança que atendam aos requisitos ASVS, veja Enterprise Security API (ESAPI) (OWASP, 2009).

[2] Para mais informações sobre a utilização do ASVS em contratos, veja Contract Annex (OWASP, 2009).

Sumário

Introdução v

Abordagem v

Agradecimentos vii

Níveis de verificação de segurança da aplicação viii

- Nível 1 – Verificação Automática viii
- Nível 1A – Análise Dinâmica (Verificação Automática Parcial) x
- Nível 1B – Análise de Código Fonte (Verificação Automática Parcial) xi
- Nível 2 – Verificação Manual xi
- Nível 2A – Teste de Penetração (Verificação Manual Parcial) xiv
- Nível 2B – Revisão de Código (Verificação Manual Parcial) xiv
- Nível 3 – Verificação do *Design* xiv
- Nível 4 – Verificação Interna xvii
- Interpretações dos Requisitos e Direcionamentos xix

Detalhamento dos Requisitos de Verificação xx

- V1 – Requisitos de Documentação da Arquitetura de Segurança xxi
- V2 – Requisitos de Verificação da Autenticação xxii
- V3 – Requisitos de Verificação do Gerenciamento de Sessões xxiii
- V4 – Requisitos de Verificação do Controle de Acesso xxiv
- V5 – Requisitos de Verificação da Validação de Entradas xxvi
- V6 – Requisitos de Verificação da Codificação/Escape de Saídas xxvi
- V7 – Requisitos de Verificação da Criptografia xxvii
- V8 – Requisitos de Verificação do Tratamento de Erros e Logs xxviii
- V9 – Requisitos de Verificação da Proteção de Dados xxx
- V10 – Requisitos de Verificação da Segurança da Comunicação xxxi
- V11 – Requisitos de Verificação da Segurança do HTTP xxxii
- V12 – Requisitos de Verificação da Configuração da Segurança xxxiii
- V13 – Requisitos de Verificação da Investigação de Códigos Maliciosos xxxiii
- V14 – Requisitos de Verificação da Segurança Interna xxxiv

Requisitos para o Relatório de Verificação xxxvi

- R1 – Introdução do Relatório xxxvi
- R2 – Descrição da Aplicação xxxvi
- R3 – Arquitetura de Segurança da Aplicação xxxvi
- R4 – Resultados da Verificação xxxvii

Glossário xxxviii

Onde ir a partir de agora xl

Figuras

Figura 1 – Níveis do OWASP ASVS vi

Figura 2 – Uma forma de introduzir verificação como uma atividade em seu SDLC vi

Figura 3 – Níveis 1, 1A e 1B do OWASP ASVS ix

Figura 4 – Exemplo de Arquitetura de Segurança Nível 1 do OWASP ASVS x

Figura 5 – Níveis 2, 2A e 2B do OWASP ASVS xi

Figura 6 – Exemplo de Arquitetura de Segurança Nível 2 do OWASP ASVS xiii

Figura 7 – Nível 3 do OWASP ASVS xv

Figura 8 – Exemplo de Arquitetura de Segurança Nível 3 do OWASP ASVS xvi

Figura 9 – Nível 4 do OWASP ASVS xvii
Figura 10 – Exemplo de código não examinado do OWASP ASVS Nível 4 xix
Figura 11 – Conteúdo do Relatório xxxvi

Tabelas

Tabela 1 – OWASP ASVS Requisitos da Arquitetura de Segurança (V1) xxi
Tabela 2 – OWASP ASVS Requisitos de Autenticação (V2) xxii
Tabela 3 – OWASP ASVS Requisitos de Gerenciamento de Sessões (V3) xxiii
Tabela 4 – OWASP ASVS Requisitos de Controle de Acesso (V4) xxv
Tabela 5 – OWASP ASVS Requisitos de Validação de Entradas (V5) xxvi
Tabela 6 – OWASP ASVS Requisitos de Codificação/Escape de Saídas (V6) xxvii
Tabela 7 – OWASP ASVS Requisitos de Criptografia (V7) xxviii
Tabela 8 – OWASP ASVS Requisitos de Tratamento de Erros e Logs (V8) xxix
Tabela 9 – OWASP ASVS Requisitos de Proteção de Dados (V9) xxx
Tabela 10 – OWASP ASVS Requisitos de Segurança da Comunicação (V10) xxxi
Tabela 11 – OWASP ASVS Requisitos de Segurança do HTTP (V11) xxxii
Tabela 12 – OWASP ASVS Requisitos de Configuração da Segurança (V12) xxxiii
Tabela 13 – OWASP ASVS Requisitos de Investigação de Códigos Maliciosos (V13) xxxiv
Tabela 14 – OWASP ASVS Requisitos de Segurança Interna (V14) xxxv
Tabela 15 – OWASP ASVS Verificação do Relatório de Conteúdos dos Resultados xxxvii

Introdução

Open Web Application Security Project (OWASP) é uma comunidade aberta dedicada a habilitar as organizações a desenvolver, adquirir e manter aplicações que possam ser confiáveis. Todas as ferramentas da OWASP, documentos, fóruns e capítulos são gratuitos e abertos a qualquer pessoa interessada em melhorar a segurança das aplicações. Nós defendemos a abordagem da segurança das aplicações como um problema relacionado com pessoas, processos e tecnologia, porque as abordagens mais eficazes para segurança de aplicações incluem melhorias em todas estas áreas. Nós podemos ser encontrados em www.owasp.org.

OWASP é um novo tipo de organização. Nossa liberdade de pressões comerciais nos permite oferecer informações imparciais, práticas e de ótimo custo-benefício sobre segurança de aplicações. OWASP não é afiliado com qualquer empresa de tecnologia, apesar de apoiar o uso claro de tecnologia comercial de segurança. Semelhante a muitos projetos de software livre, OWASP produz vários tipos de materiais de forma colaborativa e aberta. A Fundação OWASP é uma entidade sem fins lucrativos que garante o sucesso do projeto a longo prazo.

O objetivo principal do Projeto OWASP Padrão de Verificação de Segurança da Aplicação (em inglês, ASVS) é normalizar o intervalo na cobertura e nível de rigor disponíveis no mercado quando se trata de realizar verificação de segurança de aplicações Web utilizando um padrão aberto comercialmente funcional. O padrão fornece uma base para testar os controles técnicos de segurança da aplicação, bem como do ambiente, que são invocados para proteger contra vulnerabilidades, como Cross-Site Scripting (XSS) e SQL injection.[3] Este padrão pode ser usado para estabelecer um nível de confiança na segurança de aplicações web.

Abordagem

O Padrão de Verificação de Segurança da Aplicação (em inglês, ASVS) define requisitos de verificação e documentação que são agrupados com base na cobertura relacionada e nível de rigor. O padrão define quatro níveis hierárquicos (por exemplo, o Nível 2 requer maior cobertura e rigor do que o Nível 1), como representado na figura abaixo:

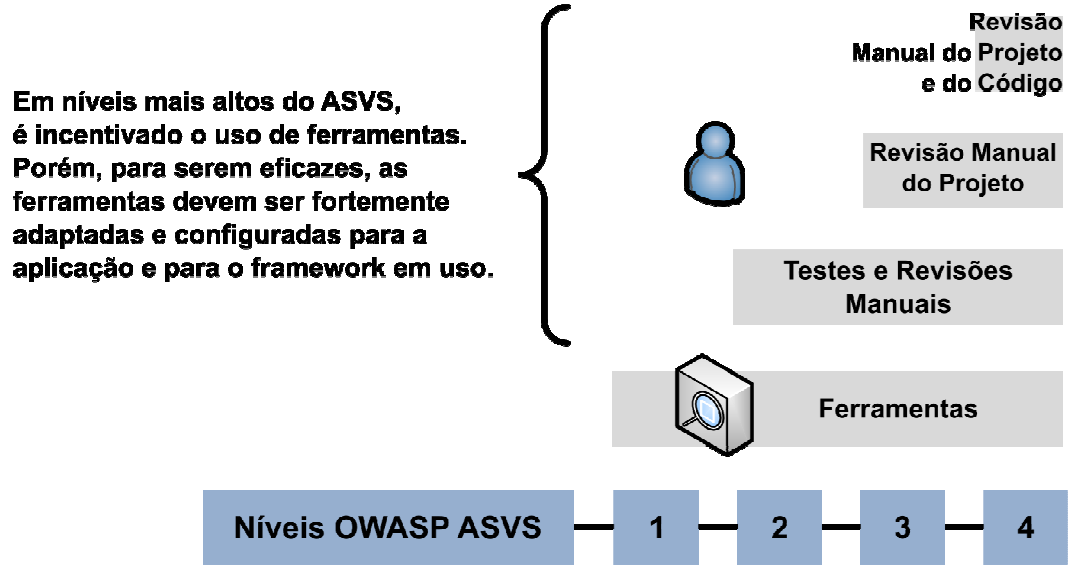

Figura 1 - Níveis do OWASP ASVS

[3] Para mais informações sobre vulnerabilidades comuns de aplicações Web, consulte o *OWASP* Top Ten (OWASP, 2007).

A verificação de segurança em aplicações web é realizada sob um ponto de vista lógico seguindo (ou tentando seguir) caminhos dentro e fora da aplicação (chamada de Alvo de Verificação, em inglês *Target of Verification* ou TOV) e executando análises ao longo desses caminhos. Aplicações mais complexas normalmente levam mais tempo para analisar, resultando em verificações longas e mais caras. Linhas de código não são os únicos fatores que determinam a complexidade de uma aplicação – diferentes tecnologias normalmente exigirão quantidades diferentes de análise. Aplicações simples podem incluir, por exemplo, bibliotecas e frameworks. Aplicações de complexidade moderada podem incluir aplicativos Web 1.0 simples. Aplicações complexas podem incluir aplicações Web 2.0 e tecnologias Web novas/únicas.

O padrão ASVS define elementos componentes para os Níveis 1 e 2 (por exemplo, verificação no Nível 1 exige atingir os requisitos dos Níveis 1A e 1B). Por exemplo, aplicações podem reivindicar conformidade aos níveis 1A ou 1B ao invés do Nível 1, mas tais reivindicações são mais fracas do que a conformidade com o Nível 1. Verificação e requisitos de documentação são definidos neste Padrão usando três tipos de requisitos: de Alto-nível, Detalhados e de Relatório. Requisitos de Alto-nível definem em alto nível os requisitos de implementação de aplicações e requisitos de verificação. Os requisitos Detalhados definem os mesmos em baixo nível (por exemplo, itens específicos para verificar). Os requisitos de Relatório definem como devem ser documentados os resultados da verificação da aplicação web de acordo com o OWASP ASVS.

OWASP fornece numerosos recursos, incluindo o padrão ASVS, para ajudar a organização a desenvolver e manter aplicações seguras. O OWASP ASVS, OWASP Anexo Contrato[4] e OWASP ESAPI[5] podem ser usados para apoiar seu Ciclo de Vida de Desenvolvimento de Software (em inglês, Software Development Life Cycle - SDLC) como representado na figura abaixo.

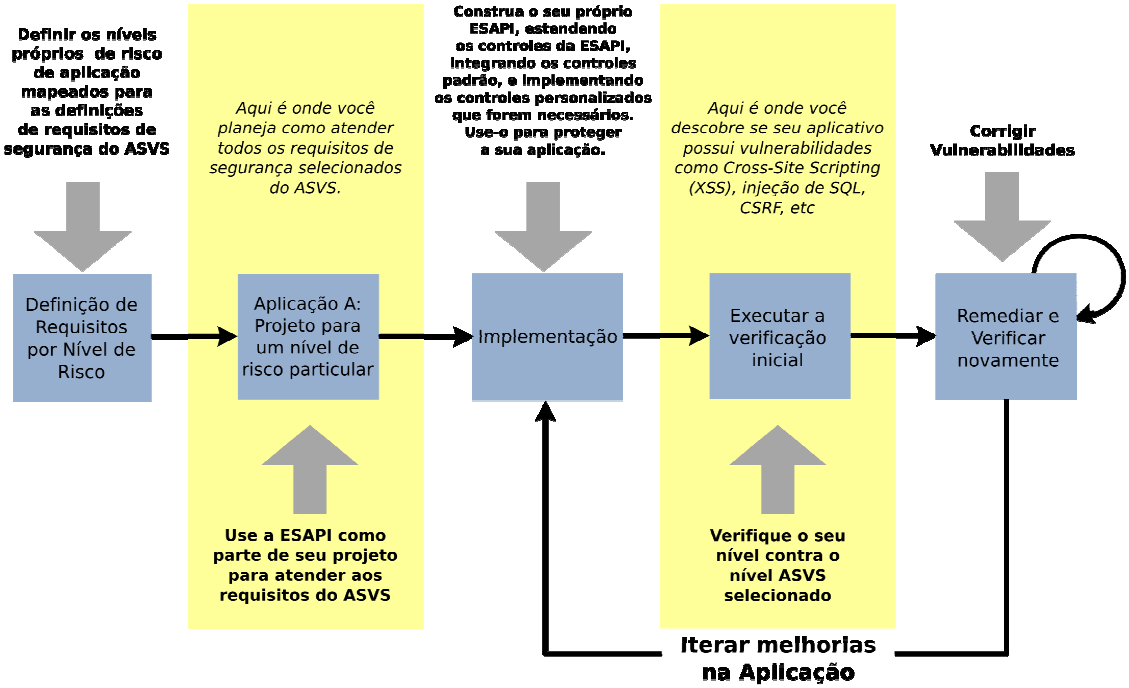

Figura 2 - Uma forma de introduzir verificação como uma atividade em seu SDLC[6]

[4] Para informações sobre como especificar um nível ASVS em um contrato, consulte o *OWASP* Anexo Contrato.

[5] Para mais informações sobre como habilitar o ESAPI em sua aplicação, consulte o projeto OWASP ESAPI (OWASP 2009).

[6] Para mais informações sobre a introdução de atividades relacionadas à segurança no seu SDLC existente, consulte o *OWASP CLASP* (OWASP 2008) ou *OWASP SAMM* Projects (OWASP 2009).

Agradecimentos

Nós agradecemos a OWASP Foundation por patrocinar o OWASP Application Security Verification Standard Project durante o OWASP Summer of Code 2008.

Líder de Projeto: [7] Mike Boberski (Booz Allen Hamilton)

Autores: [8] Mike Boberski (Booz Allen Hamilton), Jeff Williams (Aspect Security), Dave Wichers (Aspect Security)

Patrocinadores:

Booz | Allen | Hamilton

Reconhecimento é dado para as contribuições de: Pierre Parrend, que atuou como Revisor no OWASP Summer of Code 2008; Andrew van der Stock (Aspect Security); Nam Nguyen (Blue Moon Consulting); John Martin (Boeing); Gaurang Shah (Booz Allen Hamilton); Theodore Winograd (Booz Allen Hamilton); Stan Wisseman (Booz Allen Hamilton); Barry Boyd (CGI Federal); Steve Coyle (CGI Federal); Paul Douthit (CGI Federal); Ken Huang (CGI Federal); Dave Hausladen (CGI Federal); Mandeep Khera (Cenzic); Scott Matsumoto (Cigital); John Steven (Cigital); Stephen de Vries (Corsaire); Dan Cornell (Denim Group); Shouvik Bardhan (Electrosoft), Dr. Sarbari Gupta (Electrosoft); Eoin Keary (Ernst & Young); Richard Campbell (Federal Deposit Insurance Corporation); Matt Presson (FedEx); Jeff LoSapio (Fortify Software); Liz Fong (National Institute of Standards and Technology); George Lawless (Noblis); Dave van Stein (ps_testware); Terrie Diaz (SAIC); Ketan Dilipkumar Vyas (Tata Consultancy Services); Bedirhan Urgun (TURKCELL); Dr. Thomas Braun (United Nations); Colin Watson (Watson Hall); Jeremiah Grossman (WhiteHat Security); e finalmente, agradecemos a comunidade de verificação de segurança em aplicações e outros interessados em computação Web confiável por sua assistência e orientação entusiásticas ao longo deste esforço.

[7] Email: mike.boberski@owasp.org
[8] Email: jeff.williams@owasp.org, dave.wichers@owasp.org

Níveis de Verificação de Segurança da Aplicação

O Padrão de Verificação de Segurança da Aplicação (ASVS) do OWASP define quatro níveis de verificação que crescem tanto em amplitude como em profundidade à medida que os níveis aumentam. A amplitude é definida em cada nível pelo conjunto de requisitos de segurança que devem ser tratados. A profundidade da verificação é definida pela abordagem e pelo nível de rigor exigido na verificação de cada requisito de segurança. As ferramentas são uma parte importante de cada nível ASVS. Em níveis mais altos do ASVS, o uso de ferramentas é incentivado. Mas, para serem eficazes, as ferramentas devem ser fortemente adaptadas e configuradas para a aplicação e para o framework em uso. E, em todos os níveis, os resultados das ferramentas devem ser manualmente verificados.

É de responsabilidade do verificador determinar se uma aplicação atinge todos os requisitos de um nível que são alvos de uma revisão. Se a aplicação atingir todos os requisitos para aquele nível, então ela pode ser considerada uma aplicação OWASP ASVS Nível N, onde N é o nível de verificação que aquela aplicação atingiu. Se a aplicação não atinge todos os requisitos de um nível em particular, mas atinge todos de um nível mais baixo, então ela é considerada deste último nível. Esse padrão utiliza o termo 'verificador' para indicar a pessoa ou o time que está revisando a aplicação contra estes requisitos.

A especificação para uma aplicação pode exigir OWASP ASVS Nível N, mas pode também incluir outros requisitos detalhados adicionais de um nível ASVS superior. Por exemplo, uma organização financeira pode ter uma aplicação de baixo risco verificada para OWASP ASVS Nível 2, mas também pode querer que a verificação de código malicioso (consulte V13, Nível 4 apenas) seja incluída. Outros requisitos de negócio ou da organização podem se aplicar, como a conformidade com políticas de segurança da informação ou regulamentações específicas.

Não existe Nível 0 de verificação. Além disso, para ganhar um nível, as vulnerabilidades devem ser remediadas (ou mitigadas), e a aplicação re-verificada.

Nível 1 – Verificação Automática

Nível 1 ("Verificação Automática") é tipicamente apropriado para aplicações onde alguma confiança é exigida no uso correto dos controles de segurança. Ameaças à segurança[9] serão tipicamente vírus e worms (os alvos são escolhidos indiscriminadamente através de varreduras amplas e que impactem os mais vulneráveis). O escopo de verificação inclui o código que foi desenvolvido ou modificado a fim de criar a aplicação.

No Nível 1, a verificação envolve o uso de ferramentas automáticas acrescidas de verificação manual. Esse nível somente fornece cobertura parcial de verificação de segurança da aplicação web. A verificação manual não tem a intenção de fazer com que a verificação de segurança da aplicação realizada neste nível seja completa, mas somente verificar que cada evidência encontrada pela ferramenta automática não é um falso positivo.

Existem dois elementos componentes para o Nível 1. Nível 1A é para o uso de ferramentas automáticas de análise de vulnerabilidades (análise dinâmica), e o Nível 1B é para o uso de ferramentas automáticas de análise de código fonte (análise estática). Esforços de verificação podem usar quaisquer desses componentes individualmente, ou podem realizar uma combinação dessas abordagens para atingir a avaliação de Nível 1 completa. A estrutura desses níveis é descrita pela seguinte figura:

[9] Para mais informações sobre identificação e estimativa de riscos associados com vulnerabilidades, consulte o Guia de Testes OWASP (OWASP, 2008).

Enquanto se pode determinar que uma aplicação atinja o Nível 1A ou o Nível 1B, nenhum desses níveis sozinhos fornecem o mesmo nível de rigor ou cobertura que uma aplicação que atinge o Nível 1. Uma aplicação que atinge o Nível 1 deve atender tanto os requisitos do Nível 1A como os do Nível 1B.

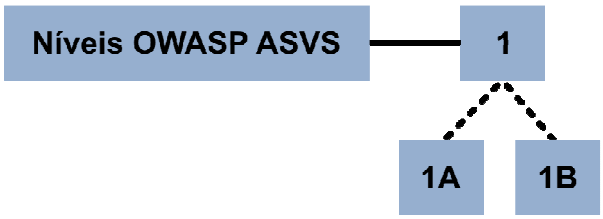

Figura 3 - Níveis 1, 1A e 1B do OWASP ASVS

A seguir estão os requisitos de alto nível mínimos para aplicações Nível 1, 1A ou 1B:

Escopo de Verificação

L1.1	O escopo de verificação inclui todo o código que foi desenvolvido ou modificado a fim de criar a aplicação.

Requisitos de Comportamento dos Controles de Segurança

Nenhum	Não existem requisitos de como os controles de segurança da aplicação tomam decisões no Nível 1.

Requisitos de Uso dos Controles de Segurança

Nenhum	Não existem requisitos de onde os controles de segurança da aplicação são usados na aplicação no Nível 1.

Requisitos de Implementação dos Controles de Segurança

Nenhum	Não existem requisitos de como os controles de segurança da aplicação são construídos no Nível 1.

Requisitos de Verificação dos Controles de Segurança

L1.2	Analisar dinamicamente a aplicação de acordo com os requisitos do Nível 1A da seção “Detalhamento dos Requisitos de Verificação”.
L1.3	Realizar análise de código fonte na aplicação de acordo com os requisitos do Nível 1B da seção “Detalhamento dos Requisitos de Verificação”.

Requisitos do Nível 1 que permitem o uso de uma ou outra técnica de verificação não precisam ser avaliados com ambas. Esses requisitos de verificação podem ser avaliados com uma das técnicas no Nível 1. Além disso, se o conjunto de ferramentas selecionadas pelo verificador não tem a capacidade de verificar um requisito especificado, o verificador pode executar uma verificação manual para preencher esta lacuna.[10] [11]

[10] Para mais informações sobre a execução de verificação manual através de técnicas de penetration testing, consulte o Guia de Testes OWASP (OWASP, 2008).

[11] Para mais informações sobre a execução de verificação manual através de revisão de código, consulte o Guia de Revisão de Código OWASP (OWASP, 2008).

Requisitos de Documentação

L1.4	Criar um relatório de verificação que detalhe a arquitetura de segurança da aplicação, listando seus componentes , e incluir os resultados da verificação de acordo com os requisitos da seção "Requisitos para o Relatório de Verificação".

No Nível 1, os componentes da aplicação podem ser definidos tanto em termos individuais como em grupos de arquivos fonte, bibliotecas e/ou executáveis, como representado na figura abaixo. No Nível 1, a lista não precisa ser ordenada ou organizada mas sim apenas identificar quais componentes são parte da aplicação, e quais são parte do ambiente de TI. A aplicação pode então ser tratada como grupos de componentes dentro de uma única entidade monolítica. O caminho ou os caminhos que uma requisição de um determinado usuário final pode tomar dentro da aplicação não precisam ser identificados e documentados.

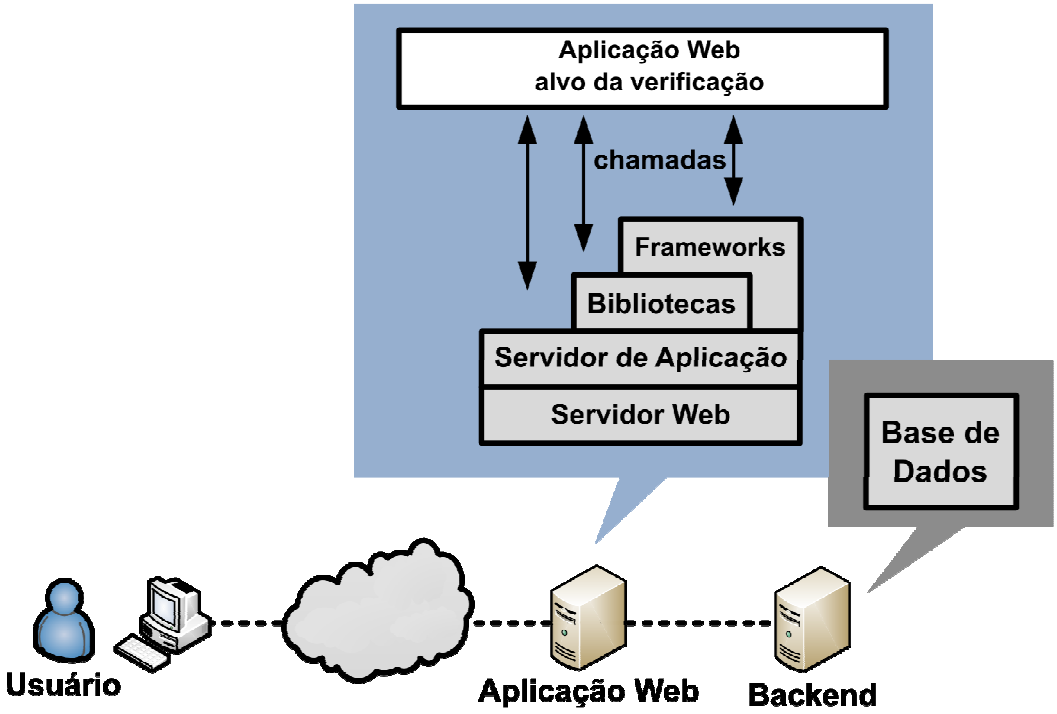

Figura 4 - Exemplo de Arquitetura de Segurança Nível 1 do OWASP ASVS

Nível 1A - Análise Dinâmica (Verificação Automática Parcial)

Requisitos de Verificação dos Controles de Segurança de Análise Dinâmica

Análise dinâmica (conhecida também como "análise de vulnerabilidades") consiste em usar ferramentas automatizadas para acessar interfaces de aplicações, enquanto a mesma está rodando, com o objetivo de detectar vulnerabilidades nos controles de segurança da aplicação. Note que isto não é o suficiente para verificar se o *design*, a implementação e o uso de controles de segurança estão corretos, mas é uma verificação aceitável no Nível 1. O escopo de verificação é definido pelos requisitos de arquitetura de segurança desse Nível.

L1A.1	Analisar dinamicamente a aplicação de acordo com os requisitos do Nível 1A especificados na seção "Detalhamento dos Requisitos de Verificação".

L1A.2	Verificar todos os resultados da análise dinâmica usando um teste de penetração manual ou uma revisão de código. Resultados automáticos não verificados não são considerados para fornecer qualquer garantia e não são suficientes para qualificar para o Nível 1.

Múltiplas instâncias de um tipo particular de vulnerabilidade que podem ser rastreadas para uma única causa raiz devem ser combinadas em uma única descoberta se a ferramenta de análise já não o fez.

Nível 1B - Análise de Código Fonte (Verificação Automática Parcial)

Requisitos de Verificação dos Controles de Segurança de Análise de Código Fonte

Análise de código fonte (conhecida também como "análise estática") consiste em usar ferramentas automatizadas para pesquisar o código fonte da aplicação à procura de padrões que representem vulnerabilidades. Note que isto não é o suficiente para verificar se o *design*, a implementação e o uso de controles de segurança estão corretos, mas é uma verificação aceitável no Nível 1. O escopo de verificação é definido pelos requisitos de arquitetura de segurança desse Nível.

L1B.1	Realizar análise de código fonte na aplicação de acordo com os requisitos da seção "Detalhamento dos Requisitos de Verificação".
L1B.2	Verificar todos os resultados da análise de código fonte usando um teste de penetração manual ou uma revisão de código. Resultados automáticos não verificados não são considerados para fornecer qualquer garantia e não são suficientes para qualificar para o Nível 1.

Múltiplas instâncias de um tipo particular de vulnerabilidade que podem ser rastreadas para uma única causa raiz devem ser combinadas em uma única descoberta se a ferramenta de análise de código já não o fez.

Nível 2 - Verificação Manual

Nível 2 ("Verificação Manual") é tipicamente apropriado para aplicações que lidam com transações pessoais, transações B2B, que processam informações de cartão de crédito ou processam informações de identificação pessoal. Nível 2 fornece alguma confiança no uso correto de controles de segurança e confiança de que os controles de segurança em si estão funcionando corretamente. Ameaças à segurança serão tipicamente vírus, worms e oportunistas pouco sofisticados, como os atacantes com ferramentas de ataque profissionais ou de código aberto. O escopo de verificação inclui todo o código desenvolvido ou modificado para o aplicação, bem como examinar a segurança de todos os componentes de terceiros que fornecem funcionalidades de segurança para a aplicação. Existem dois elementos componentes para o Nível 2, conforme representado na figura abaixo.

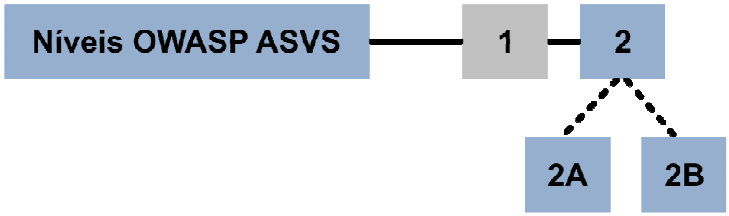

Figura 5 - Níveis 2, 2A e 2B do OWASP ASVS

Enquanto se pode determinar que uma aplicação atinge o Nível 2A ou o Nível 2B, nenhum desses níveis sozinhos fornecem o mesmo nível de rigor ou cobertura que uma aplicação que atinge o Nível 2. Além disso, enquanto o Nível 2 é um superconjunto do Nível 1, não existe nenhum requisito para rodar uma ferramenta automatizada para atender os requisitos do Nível 2. Ao invés disto, o verificador tem a opção de usar somente técnicas manuais para todos os requisitos. Se estiverem

disponíveis resultados de ferramentas automatizadas, o verificador pode utilizá-los para apoiar a análise. Entretanto, um requisito que passe no Nível 1 não indica que automaticamente passe o mesmo requisito no Nível 2. Isto porque ferramentas automatizadas não fornecem evidências suficientes de que o requisito positivo foi atingido.

Técnicas manuais continuam a presumir o emprego de ferramentas. Isto pode incluir o uso de qualquer tipo de ferramenta de análise de segurança ou teste, incluindo as ferramentas automatizadas que são usadas nas verificações do Nível 1. Entretanto, tais ferramentas são simples auxílios para o analista achar e avaliar os controles de segurança que estão sendo verificados. Tais ferramentas podem ou não conter lógica para detectar vulnerabilidades da aplicação automaticamente.

A seguir estão os requisitos de alto-nível mínimos para aplicações Nível 2, 2A ou 2B:

Escopo de Verificação

L2.1	O escopo de verificação inclui todo o código que foi desenvolvido ou modificado a fim de criar a aplicação. Esse requisito foi introduzido no Nível 1.
L2.2	O escopo de verificação inclui o código de todos os sistemas de terceiros, biblioteca, e funcionalidade de segurança do serviço que é invocado por ou apóia a segurança da aplicação. Esse é um novo requisito no Nível 2.

Requisitos de Comportamento dos Controles de Segurança

L2.3	Verificar se todos os controles técnicos de segurança tomam decisões usando uma abordagem de lista-branca. Esse é um novo requisito no Nível 2.
L2.4	Verificar se todos os controles de segurança que realizam as verificações de segurança e controles que resultam em efeitos de segurança não sejam ignorados de acordo com o Nível 2A e os requisitos do Nível 2B especificados na seção “Detalhamento dos Requisitos de Verificação”. Esse é um novo requisito no Nível 2.

Requisitos de Uso dos Controles de Segurança

L2.5	Verificar se todos os controles de segurança são usados em todos os lugares dentro da aplicação nos quais eles precisam estar, no lado do servidor, de acordo com os requisitos de Nível 2 especificados na seção “Detalhamento dos Requisitos de Verificação”. Esse é um novo requisito no Nível 2.

Requisitos de Implementação dos Controles de Segurança

Nenhum	Não existem requisitos para a forma como os controles de segurança de aplicações são construídos no Nível 2.

Requisitos de Verificação dos Controles de Segurança

L2.6	Realizar um teste de penetração manual na aplicação de acordo com os requisitos especificados no Nível 2A da seção “Detalhamento dos Requisitos de Verificação”. Esse é um novo requisito no Nível 2.
L2.7	Realizar a revisão manual do código fonte na aplicação de acordo com os requisitos especificados no Nível 2B da seção “Detalhamento dos Requisitos de Verificação”. Esse é um novo requisito no Nível 2.

Requisitos do Nível 2 que permitam a utilização de qualquer técnica de verificação devem ser verificados com apenas uma técnica.

O verificador pode incluir verificação automática ou análise de código como parte de seu esforço de verificação no nível 2, mas a verificação automática não pode ser usada no lugar da revisão manual necessária para cada requisito de Nível 2. Se os resultados da análise ajudarem o verificador a executar o seu trabalho de forma mais rápida ou aumentarem os resultados da porção manual da revisão, elas podem, certamente, ser utilizadas para auxiliar a realização de uma verificação Nível 2.

Requisitos de Documentação

L2.8	Criar um relatório de verificação que descreva a arquitetura de segurança da aplicação agrupando seus componentes em uma arquitetura de alto nível, e incluir os resultados da verificação de acordo com os requisitos da seção "Requisitos para o Relatório de Verificação". Isto aumenta o requisito de documentação introduzido no Nível 1.

No Nível 2, os componentes da aplicação podem ser definidos tanto em termos individuais como em grupos de arquivos fonte, bibliotecas e/ou executáveis que são organizados em uma arquitetura de alto-nível (por exemplo, os componentes do MVC - *Model-View-Controller*, componentes de funções do negócio e componentes da camada de dados). Por exemplo, o diagrama a seguir descreve uma aplicação que consiste em um servidor web, um servidor de aplicação, código personalizado, bibliotecas e uma aplicação de banco de dados que são agrupados de acordo com uma arquitetura MVC. No Nível 2, o caminho ou os caminhos que uma requisição de um usuário final pode tomar dentro da aplicação devem ser documentados, conforme ilustrado na figura abaixo. Entretanto, nem todos os caminhos devem ser examinados.

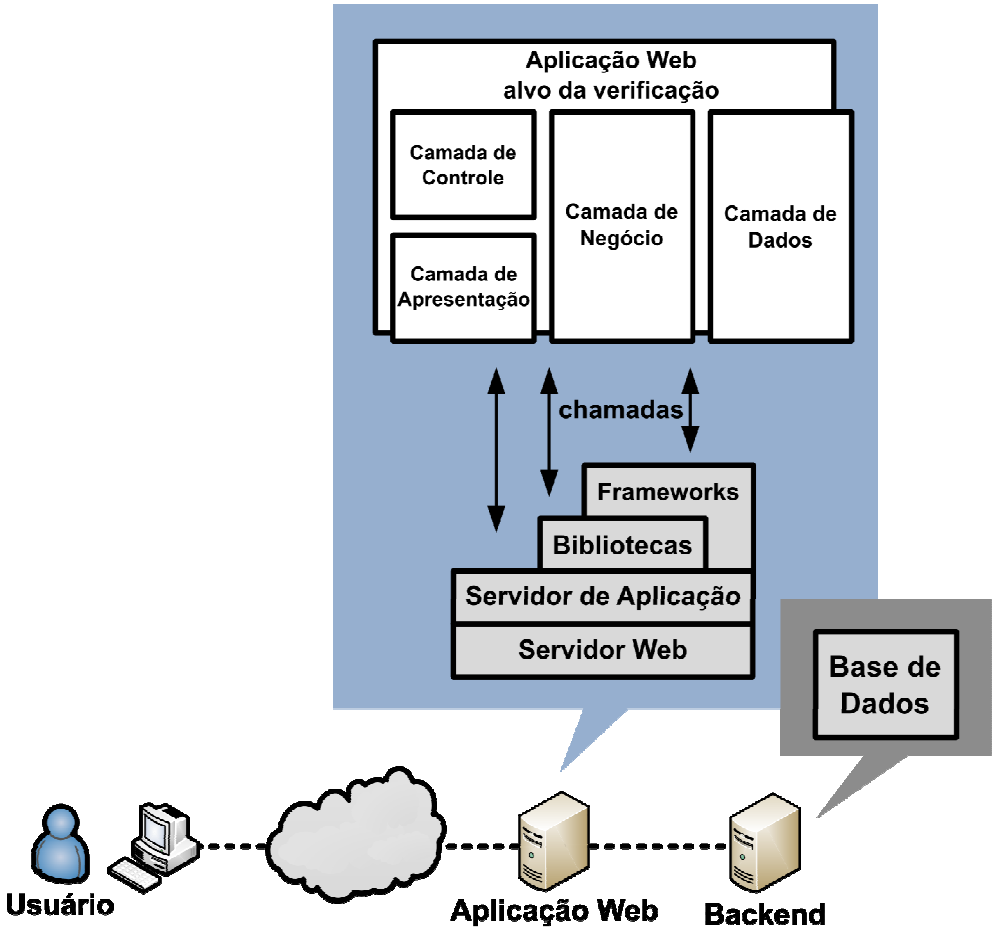

Figura 6 - Exemplo de Arquitetura de Segurança Nível 2 do OWASP ASVS

Nível 2A – Teste de Penetração (Verificação Manual Parcial)

Requisitos de Verificação dos Controles de Segurança de Teste de Penetração

Teste de penetração manual da aplicação consiste em criar testes dinâmicos para verificar o *design*, a implementação e o uso de controles de segurança apropriados na aplicação. O escopo de verificação é definido pelos requisitos da arquitetura de segurança desse Nível.

L2A.1	Realizar teste manual de penetração na aplicação de acordo com os requisitos do Nível 2A especificados na seção "Detalhamento dos Requisitos de Verificação". Esse é um novo requisito no Nível 2.

Onde for apropriado, o verificador pode usar amostras para estabelecer o uso efetivo de um controle de segurança. O verificador pode escolher documentar um padrão de vulnerabilidade que permitirá aos desenvolvedores confidencialmente localizar e corrigir todas as instâncias do padrão na *baseline* do software. Múltiplas instâncias de um padrão de vulnerabilidade que podem ser rastreadas para uma única causa raiz devem ser combinadas em uma única descoberta.

Nível 2B – Revisão de Código (Verificação Manual Parcial)

Requisitos de Verificação dos Controles de Segurança de Revisão Manual de Código

A revisão manual de código consiste em uma pessoa buscar e analisar o código fonte da aplicação para verificar seu *design*, implementação e uso adequado de controles de segurança. Espera-se que tal análise seja auxiliada por ferramentas, mas poderia simplesmente envolver ferramentas comumente disponíveis tais como um editor de código fonte ou um Ambiente de Desenvolvimento Integrado (do inglês, *IDE - Integrated Development Environment*). O escopo de verificação é definido pelos requisitos da arquitetura de segurança desse Nível.

L2B.1	Realizar revisão manual de código na aplicação de acordo com os requisitos do Nível 2B da seção "Detalhamento dos Requisitos de Verificação". Esse é um novo requisito no Nível 2.

Onde for apropriado, o verificador pode usar amostras para estabelecer o uso efetivo de um controle de segurança. O verificador pode escolher documentar um padrão de vulnerabilidade que permitirá aos desenvolvedores confidencialmente localizar e corrigir todas as instâncias do padrão na *baseline* do software. Múltiplas instâncias de um padrão de vulnerabilidade que podem ser rastreadas para uma única causa raiz devem ser combinadas em uma única descoberta.

Nível 3 – Verificação do Design

Nível 3 ("Verificação do Design") é tipicamente apropriado para aplicações que lidam com transações B2B significativas, incluindo aquelas que processam informações de saúde pública, implementam funções de negócio críticas ou sensíveis, ou processam outros ativos sensíveis. Ameaças à segurança serão tipicamente vírus, worms, oportunistas, e possivelmente atacantes determinados (atacantes qualificados e motivados com foco em alvos específicas, utilizando ferramentas incluindo algumas construídas com propósitos definidos). O escopo de verificação inclui todo o código desenvolvido ou modificado para o aplicação, bem como examinar a segurança de todos os componentes de terceiros que fornecem funcionalidades de segurança para a aplicação. O Nível 3 certifica que os controles de segurança em si estão funcionando corretamente e que os controles de segurança são usados em todos os locais da aplicação onde eles precisam estar para assegurar as políticas específicas da aplicação. O Nível 3 não é quebrado em múltiplos componentes, conforme representado na figura abaixo.

Figura 7 - Nível 3 do OWASP ASVS

A seguir estão os requisitos mínimos de alto-nível para aplicações Nível 3:

Escopo de Verificação

L3.1	O escopo de verificação inclui todo o código que foi desenvolvido ou modificado a fim de criar a aplicação. Esse requisito foi introduzido no Nível 1.
L3.2	O escopo de verificação inclui o código de todos os sistemas de terceiros, biblioteca, e funcionalidade de segurança do serviço que é invocado por ou apóia a segurança da aplicação. Esse requisito foi introduzido no Nível 2.
L3.3	O escopo de verificação inclui o código de todos os sistemas de terceiros, biblioteca, e serviços associados à aplicação. Esse é um novo requisito no Nível 3.

Requisitos de Comportamento dos Controles de Segurança

L3.4	Verificar se todos os controles de segurança tomam decisões usando uma abordagem de lista-branca. Esse requisito foi introduzido no Nível 2.
L3.5	Verificar se todos os controles de segurança que realizam as verificações de segurança e controles que resultam em efeitos de segurança não sejam ignorados de acordo com os requisitos do Nível 3 especificados na seção “Detalhamento dos Requisitos de Verificação”. Esse requisito foi introduzido no Nível 2.

Requisitos de Uso dos Controles de Segurança

L3.6	Verificar se todos os controles de segurança são usados em todos os lugares dentro da aplicação nos quais eles precisam estar, e as implementações são centralizadas na aplicação, no lado do servidor, de acordo com os requisitos de Nível 3 especificados na seção “Detalhamento dos Requisitos de Verificação”. Esse requisito foi introduzido no Nível 2.

Requisitos de Implementação dos Controles de Segurança

Nenhum	Não existem requisitos para a forma como os controles de segurança de aplicações são construídos no Nível 3.

Requisitos de Verificação dos Controles de Segurança

L3.7	Realizar verificação manual da aplicação de acordo com os requisitos especificados no Nível 3 da seção “Detalhamento dos Requisitos de Verificação”. Isto aumenta os requisitos de verificação manual introduzidos no Nível 2.
L3.8	Documentar uma arquitetura de segurança e usá-la para verificar o design apropriado e usar todos os controles de segurança por meio de uma modelagem de ameaças. Esse é um novo requisito no Nível 3.

Requisitos de Documentação

L3.9	Criar um relatório de verificação que descreva a arquitetura de segurança da aplicação agrupando seus componentes em uma arquitetura de alto nível que inclua informações sobre modelagem de ameaças, e incluir os resultados da verificação de acordo com os requisitos da seção "Requisitos para o Relatório de Verificação". Isto aumenta o requisito de documentação introduzido no Nível 2.

No Nível 3, os componentes da aplicação podem ser definidos tanto em termos individuais como em grupos de arquivos fonte, bibliotecas e/ou executáveis que são organizados em uma arquitetura de alto-nível (por exemplo, os componentes do MVC - Model-View-Controller, componentes de funções do negócio e componentes da camada de dados). No Nível 3, informações de apoio da modelagem de ameaças sobre agentes e ativos devem, adicionalmente, ser fornecidas. O caminho ou os caminhos que uma requisição de um usuário final pode tomar dentro de uma visão de alto-nível da aplicação devem ser documentados, conforme ilustrado na figura abaixo. No Nível 3, *todos* os caminhos potenciais dentro de uma visão de alto-nível da aplicação devem ser examinados.

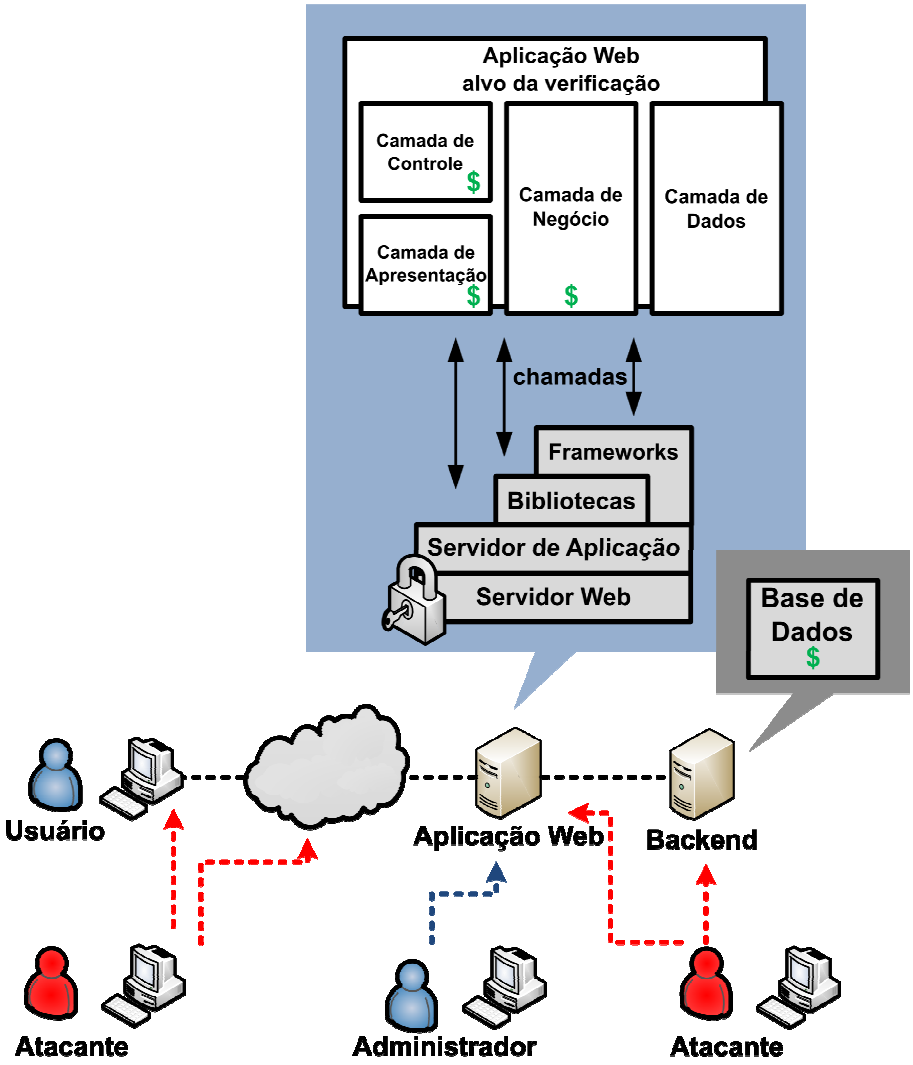

Figura 8 - Exemplo de Arquitetura de Segurança Nível 3 do OWASP ASVS[12]

[12] O símbolo de cifrão indica os ativos no diagrama.

Nível 4 - Verificação Interna

Nível 4 ("Verificação Interna") é tipicamente apropriado para aplicações críticas que protegem a vida e a segurança, infraestrutura crítica ou funções relacionadas à defesa. O Nível 4 também pode ser apropriado para aplicações que processam ativos sensíveis. Nível 4 certifica que os controles de segurança em si estão funcionando corretamente, que os controles de segurança são usados em todos os locais da aplicação que eles precisam estar para assegurar as políticas específicas da aplicação e que as práticas de codificação segura foram seguidas. Ameaças à segurança partirão de atacantes determinados (atacantes qualificados e motivados com foco em alvos específicas, utilizando ferramentas incluindo algumas construídas com propósitos definidos). O escopo de verificação se expande além do escopo do Nível 3 e inclui todo o código usado pela aplicação. O Nível 4 não é quebrado em elementos componentes, conforme representado na figura abaixo.

Figura 9 - Nível 4 do OWASP ASVS

A seguir estão os requisitos mínimos de alto-nível para aplicações Nível 4:

Escopo de Verificação

L4.1	O escopo de verificação inclui todo o código que foi desenvolvido ou modificado a fim de criar a aplicação. Esse requisito foi introduzido no Nível 1.
L4.2	O escopo de verificação inclui o código de todos os sistemas de terceiros, biblioteca, e funcionalidade de segurança do serviço que é invocado por ou apóia a segurança da aplicação. Esse requisito foi introduzido no Nível 2.
L4.3	O escopo de verificação inclui o código de todos os sistemas de terceiros, biblioteca, e serviços associados à aplicação. Esse requisito foi introduzido no Nível 3.
L4.4	O escopo de verificação inclui todo o código remanescente associado à aplicação, incluindo frameworks, bibliotecas, ambientes de execução, ferramentas de desenvolvimento, construção e implantação. O escopo não inclui o código para o software de plataforma, como um servidor de aplicativos, servidor de banco de dados, máquina virtual, ou sistema operacional, que tenha recebido uma quantidade substancial de escrutínio público. Esse é um novo requisito no Nível 4.

Requisitos de Comportamento dos Controles de Segurança

L4.5	Verificar se todos os controles de segurança tomam decisões usando uma abordagem de lista-branca ("positiva"). Esse requisito foi introduzido no Nível 2.
L4.6	Verificar se todos os controles de segurança que realizam as verificações de segurança e controles que resultam em efeitos de segurança não sejam ignorados de acordo com os requisitos do Nível 4 especificados na seção "Detalhamento dos Requisitos de Verificação". Esse requisito foi introduzido no Nível 2.

Requisitos de Uso dos Controles de Segurança

L4.7	Verificar se todos os controles de segurança são usados em todos os lugares dentro da aplicação nos quais eles precisam estar, e as implementações são centralizadas na aplicação, no lado do servidor, de acordo com os requisitos de Nível 4 especificados na seção "Detalhamento dos Requisitos de Verificação". Esse requisito foi introduzido no Nível 3.

Requisitos de Implementação dos Controles de Segurança

L4.8	Verificar se a aplicação não contém qualquer código malicioso de acordo com os requisitos de Nível 4 especificados na seção "Detalhamento dos Requisitos de Verificação". Esse é um novo requisito no Nível 4.

Requisitos de Verificação dos Controles de Segurança

L4.9	Realizar verificação manual da aplicação de acordo com os requisitos especificados no Nível 4 da seção "Detalhamento dos Requisitos de Verificação". Isto aumenta os requisitos do Nível 3.
L4.10	Documentar uma arquitetura de segurança e usá-la para verificar o design apropriado e usar todos os controles de segurança por meio de uma modelagem de ameaças. Esse requisito foi introduzido no Nível 3.
L4.11	Revisar manualmente todo o código desenvolvido ou modificado para esta aplicação a procura de código malicioso[13] de acordo com os requisitos de Nível 4 especificados na seção "Detalhamento dos Requisitos de Verificação". Esse é um novo requisito no Nível 4.

Requisitos de Documentação

L4.12	Criar um relatório de verificação que descreva a arquitetura de segurança da aplicação de acordo com os requisitos do Nível 3, que abrange todo o código da aplicação, e incluir os resultados da verificação de acordo com os requisitos da seção "Requisitos para o Relatório de Verificação". Isto aumenta o requisito de documentação do Nível 3.

No Nível 4, a arquitetura da aplicação deve ser capturada conforme exigido no Nível 3. Além disso, o Nível 4 exige que todo o código da aplicação, incluindo código não explicitamente examinado, seja identificado como parte da definição da aplicação, conforme ilustrado na figura abaixo. Este código deve incluir todas as bibliotecas, frameworks, e códigos de apoio que a aplicação confia. Verificações anteriores desses componentes podem ser reutilizadas como parte de outro esforço de verificação. Códigos de plataforma como os de sistema operacional, máquina virtual ou bibliotecas núcleo emitidos com um ambiente de máquina virtual, servidor web ou servidor de aplicação, não são incluídos no Nível 4. Por exemplo, bibliotecas associadas com o ambiente de execução Java não precisariam ser avaliadas no Nível 4.

[13] Código malicioso não é o mesmo que *malware*. Consulte no glossário a definição de código malicioso.

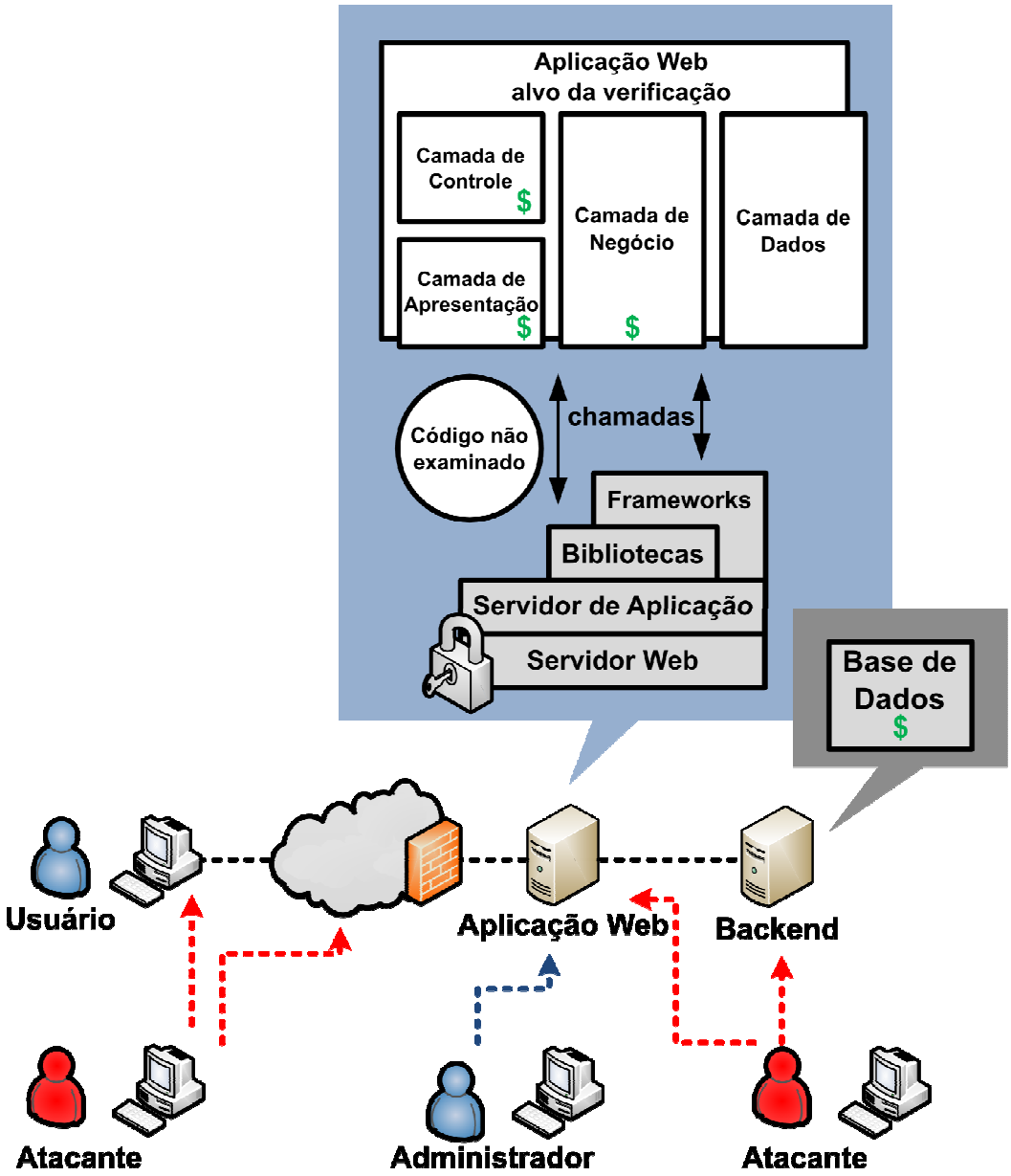

Figura 10 - Exemplo de código não examinado do OWASP ASVS Nível 4

Interpretações dos Requisitos e Direcionamentos

O OWASP ASVS é um documento bastante dinâmico. Se você está realizando uma verificação de segurança de aplicação de acordo com este padrão, então você deve sempre rever os artigos que podem ser encontrados na página do projeto OWASP ASVS no seguinte local: http://www.owasp.org/index.php/ASVS#Articles_Below_-_More_About_ASVS_and_Using_It . Os artigos na página do projeto OWASP ASVS fornecem esclarecimentos e direcionamentos de veredito sobre os requisitos, além de dicas úteis.

Detalhamento dos Requisitos de Verificação

Esta seção do Padrão de Verificação de Segurança da Aplicação (em inglês, ASVS) define requisitos detalhados de verificação que foram derivados a partir dos requisitos de alto nível para cada um dos níveis de verificação definidos nesse padrão. Cada seção abaixo define um conjunto de requisitos detalhados de verificação agrupados em áreas relacionadas.

O ASVS define as seguintes áreas dos requisitos de verificação:

V1. Arquitetura de Segurança
V2. Autenticação
V3. Gerenciamento de Sessões
V4. Controle de Acesso
V5. Validação de Entradas
V6. Codificação/Escape de Saídas
V7. Criptografia
V8. Tratamento de Erros e Logs
V9. Proteção de Dados
V10. Segurança da Comunicação
V11. Segurança do HTTP
V12. Configuração da Segurança
V13. Investigação de Códigos Maliciosos
V14. Segurança Interna

Para cada uma dessas áreas, serão especificados os requisitos que devem ser atendidos em cada nível de verificação listado abaixo:

Nível 1: Verificação Automática
- Nível 1A – Análise Dinâmica (Verificação Automática Parcial)
- Nível 1B – Análise de Código Fonte (Verificação Automática Parcial)

Nível 2: Verificação Manual
- Nível 2A – Teste de Penetração (Verificação Manual Parcial)
- Nível 2B – Revisão de Código (Verificação Manual Parcial)

Nível 3: Verificação do *Design*

Nível 4: Verificação Interna

V1 – Requisitos de Documentação da Arquitetura de Segurança

Para todos os níveis do padrão ASVS, documentar alguma informação básica da arquitetura de segurança é necessário para assegurar tanto a completude como a exatidão (e repetição quando a correção é exigida) da verificação de segurança da aplicação que é executada. Análises podem ser direcionadas e resultados podem ser rastreados para uma arquitetura de segurança de alto nível da aplicação. Estes requisitos começam com um nível básico de detalhe da arquitetura de segurança que deve ser capturada e este nível de detalhe aumenta a cada nível. A tabela abaixo define os requisitos de documentação da arquitetura de segurança correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 1 - OWASP ASVS Requisitos da Arquitetura de Segurança (V1)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V1.1	Verificar se todos os componentes da aplicação (tanto individuais como grupos de código-fonte, bibliotecas e/ou executáveis) que estão presentes estão identificados.						
V1.2	Verificar se todos os componentes que não são parte da aplicação, mas que a aplicação depende para operar, estão identificados.						
V1.3	Verificar se uma arquitetura de alto nível para a aplicação foi definida.[14]						
V1.4	Verificar se todos os componentes da aplicação estão definidos em termos das funções de negócio e/ou funções de segurança que eles proveem.						
V1.5	Verificar se todos os componentes que não são parte da aplicação, mas que a aplicação depende para operar, estão definidos em termos das funções de negócio e/ou funções de segurança que eles proveem.						
V1.6	Verificar se as informações de modelagem de ameaças foram fornecidas.						

[14] O verificador pode criar ou documentar um projeto de alto nível se o desenvolvedor da aplicação não fornecê-lo.

V2 - Requisitos de Verificação da Autenticação

Os Requisitos de Verificação da Autenticação definem um conjunto de requisitos para gerar e tratar de forma segura as credenciais de contas. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 2 - OWASP ASVS Requisitos de Autenticação (V2)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V2.1	Verificar se todas as páginas e recursos requerem autenticação exceto aquelas que especificamente devem ser públicas.						
V2.2	Verificar se todos os campos de senha não retornam a senha do usuário quando ela é submetida, e se os campos de senha (ou os formulários que os contêm) estão com o recurso de autocompletar desabilitado.						
V2.3	Verificar se um número máximo de tentativas de autenticação for excedido, a conta é bloqueada por um período de tempo suficiente para deter os ataques de força bruta.						
V2.4	Verificar se todos os controles de autenticação são executados no lado do servidor.						
V2.5	Verificar se todos os controles de autenticação (incluindo bibliotecas que chamam serviços de autenticação externa) tem uma implementação centralizada.						
V2.6	Verificar se todos os controles de autenticação falham de forma segura (princípio do *fail safe*).						
V2.7	Verificar se a força de quaisquer credenciais de autenticação é suficiente para resistir aos ataques que são típicos das ameaças no ambiente implantado.						
V2.8	Verificar se todas as funções de gerenciamento de contas são no mínimo tão resistentes a ataques quanto o mecanismo primário de autenticação.						

V2.9	Verificar se os usuários podem mudar suas credenciais com segurança usando um mecanismo que seja no mínimo tão resistente a ataques quanto o mecanismo primário de autenticação.						
V2.10	Verificar se a re-autenticação é exigida antes que quaisquer operações sensíveis da aplicação sejam permitidas.						
V2.11	Verificar se após um período administrativamente configurável de tempo, as credenciais de autenticação expiram.						
V2.12	Verificar se todas as decisões de autenticação são registradas (*logs*).						
V2.13	Verificar se as senhas de contas utilizam um valor aleatório (*salt*) que seja única para esta conta (por exemplo, ID interno do usuário, criação da conta) e são codificadas em *hash* antes do armazenamento.						
V2.14	Verificar se todas as credenciais de autenticação para acesso a serviços externos à aplicação são cifradas e armazenadas em um local protegido (não dentro do código-fonte).						
V2.15	Verificar se todos os códigos que implementam ou usam controles de autenticação não são afetados por qualquer código malicioso.						

V3 - Requisitos de Verificação do Gerenciamento de Sessões

Os Requisitos de Verificação do Gerenciamento de Sessões definem um conjunto de requisitos para usar de forma segura requisições e respostas HTTP, sessões, *cookies*, cabeçalhos e logs para gerenciar apropriadamente as sessões. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 3 - OWASP ASVS Requisitos de Gerenciamento de Sessões (V3)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V3.1	Verificar se a implementação padrão do gerenciamento de sessões do *framework* é utilizada pela aplicação.						
V3.2	Verificar se as sessões são invalidadas quando o usuário sai da aplicação.						

V3.3	Verificar se as sessões expiram (*timeout*) após um período especificado de inatividade.						
V3.4	Verificar se as sessões expiram (*timeout*) após um período máximo de tempo administrativamente configurável, independentemente da atividade (um *timeout* absoluto).						
V3.5	Verificar se todas as páginas autenticadas têm *links* de *logout*.						
V3.6	Verificar se a identificação da sessão nunca é divulgada, a não ser nos cabeçalhos dos *cookies*; particularmente em URLs, mensagens de erro ou logs. Isto inclui verificar se a aplicação não suporta reescrita de URLs dos *cookies* de sessão.						
V3.7	Verificar se a identificação da sessão é alterada no login.						
V3.8	Verificar se a identificação da sessão é alterada na re-autenticação.						
V3.9	Verificar se a identificação da sessão é alterada ou cancelada no logout.						
V3.10	Verificar se somente identificadores de sessão gerados pelo *framework* da aplicação são reconhecidos como válidos.						
V3.11	Verificar se os tokens de sessões autenticadas são suficientemente longos e randômicos para resistir aos ataques que são típicos das ameaças no ambiente implantado.						
V3.12	Verificar se os cookies que contêm os tokens/identificadores de sessões autenticadas têm seu domínio e caminho definidos para um valor adequadamente restritivo para o site.						
V3.13	Verificar se todos os códigos que implementam ou usam controles de gerenciamento de sessões não são afetados por qualquer código malicioso.						

V4 - Requisitos de Verificação do Controle de Acesso

Os Requisitos de Verificação do Controle de Acesso definem como uma aplicação pode executar o controle de acesso com segurança. Na maioria das aplicações, o controle de acesso deve ser realizado em diferentes locais através de várias camadas da aplicação. Esses requisitos de verificação definem requisitos de controles de acesso para URLs, funções do negócio, dados,

serviços e arquivos. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 4 - OWASP ASVS Requisitos de Controle de Acesso (V4)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V4.1	Verificar se os usuários podem acessar somente funções protegidas para as quais eles possuem autorização específica.						
V4.2	Verificar se os usuários podem acessar somente URLs para as quais eles possuem autorização específica.						
V4.3	Verificar se os usuários podem acessar somente arquivos para os quais eles possuem autorização específica.						
V4.4	Verificar se referências diretas a objetos são protegidas, de tal forma que somente objetos autorizados sejam acessíveis para cada usuário.						
V4.5	Verificar se a navegação pelos diretórios está desabilitada a menos que explicitamente desejada.						
V4.6	Verificar se os usuários podem acessar somente serviços para os quais eles possuem autorização específica.						
V4.7	Verificar se os usuários podem acessar somente os dados para os quais eles possuem autorização específica.						
V4.8	Verificar se os controles de acesso falham de forma segura (princípio do fail safe).						
V4.9	Verificar se as mesmas regras de controle de acesso aplicadas pela camada de apresentação são executadas no lado servidor.						
V4.10	Verificar se todos os atributos de dados e usuários e informações de política usados pelos controles de acesso não podem ser manipulados pelos usuários finais a menos que especificamente autorizado.						
V4.11	Verificar se todos os controles de acesso são executados no lado servidor.						

V4.12	Verificar se há um mecanismo centralizado (incluindo bibliotecas que chamam serviços de autorização externa) para proteger o acesso a cada tipo de recurso protegido.						
V4.13	Verificar se as limitações de entrada e de acesso impostas pelo negócio na aplicação (tais como limites de transações diárias ou sequenciamento de tarefas) não podem ser burladas						
V4.14	Verificar se todas as decisões de controle de acesso são registradas (logs), inclusive as decisões de falha de acesso.						
V4.15	Verificar se todos os códigos que implementam ou usam controles de acesso não são afetados por qualquer código malicioso						

V5 - Requisitos de Verificação da Validação de Entradas

Os Requisitos de Verificação da Validação de Entradas definem um conjunto de requisitos para validar entradas de tal forma que elas sejam usadas de forma segura dentro da aplicação. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 5 - OWASP ASVS Requisitos de Validação de Entradas (V5)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V5.1	Verificar se o ambiente não é suscetível a *buffer overflows*, ou se os controles de segurança previnem *buffer overflows*.						
V5.2	Verificar se um padrão de validação positiva é definido e aplicado para todas as entradas.						
V5.3	Verificar se todas as falhas na validação de entradas resultam na rejeição ou sanitização da entrada.						
V5.4	Verificar se uma codificação de caracteres, por exemplo UTF-8, é especificada para todas as fontes de entrada.						
V5.5	Verificar se todas as validações de entrada são realizadas no lado do servidor.						

V5.6	Verificar se um único controle de validação de entrada é usado pela aplicação para cada tipo de dado que é aceito.						
V5.7	Verificar se todas as falhas na validação de entradas são registradas (logs).						
V5.8	Verificar se todos os dados de entrada são canonizados por todos os decodificadores ou interpretadores antes da validação.						
V5.9	Verificar se todos os controles de validação de entrada não são afetados por qualquer código malicioso.						

V6 - Requisitos de Verificação da Codificação/Escape de Saídas

Os Requisitos de Verificação da Codificação/Escape de Saídas definem um conjunto de requisitos para verificar se as saídas são apropriadamente codificadas de forma que sejam seguras para aplicações externas. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 6 - OWASP ASVS Requisitos de Codificação/Escape de Saídas (V6)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V6.1	Verificar se todos os dados não confiáveis que são saídas para HTML (incluindo elementos HTML, valores de dados *javascript*, blocos CSS, atributos URI) realizam o escape apropriado para o contexto da aplicação.						
V6.2	Verificar se todos os controles de codificação/escape de saídas são implementados no lado servidor.						
V6.3	Verificar se os controles de codificação/escape de saídas codificam todos os caracteres desconhecidos para garantir segurança ao interpretador.						
V6.4	Verificar se todos os dados não confiáveis que são saídas para interpretadores SQL, usam interfaces parametrizadas, instruções preparadas ou realizam o escape apropriado.						

V6.5	Verificar se todos os dados não confiáveis que são saídas para XML usam interfaces parametrizadas ou realizam o escape apropriadamente.						
V6.6	Verificar se todos os dados não confiáveis usados em consultas LDAP realizam o escape apropriado.						
V6.7	Verificar se todos os dados não confiáveis que são incluídos em parâmetros de comandos do sistema operacional realizam o escape apropriado.						
V6.8	Verificar se todos os dados não confiáveis que são saídas para quaisquer interpretadores não listados especificamente acima realizam o escape apropriado.						
V6.9	Verificar se para cada tipo de codificação/escape realizado pela aplicação, exista um único controle de segurança para este tipo de saída para o destino pretendido.						
V6.10	Verificar se todos os códigos que implementam ou usam validação de saídas não são afetados por qualquer código malicioso.						

V7 - Requisitos de Verificação da Criptografia

Os Requisitos de Verificação da Criptografia definem um conjunto de requisitos que podem ser usados para validar a encriptação da aplicação, o gerenciamento de chaves, números aleatórios e operações *hashes*. Aplicações devem usar sempre módulos de criptografia FIPS 140-2 validados ou módulos de criptografia validados de acordo com um padrão equivalente (por exemplo, um padrão de fora dos EUA). A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 7 - OWASP ASVS Requisitos de Criptografia (V7)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V7.1	Verificar se todas as funções criptográficas usadas para proteger segredos do usuário da aplicação são implementadas no lado servidor.						
V7.2	Verificar se todos os módulos criptográficos falham de forma segura (princípio do *fail safe*).						

V7.3	Verificar se o acesso a qualquer segredo master é protegido de acesso não autorizado (Um segredo master é uma credencial da aplicação armazenada em texto claro no disco que é usada para proteger o acesso às informações de configuração de segurança).						
V7.4	Verificar se os hashes das senhas utilizam um *salt* quando são criados.						
V7.5	Verificar se as falhas nos módulos criptográficos são registradas (logs).						
V7.6	Verificar se todos os números, nomes de arquivo, GUIDs e strings randômicos são gerados por um mecanismo aprovado de forma a evitar que possam ser adivinhados por um atacante.						
V7.7	Verificar se os módulos criptográficos usados pela aplicação foram validados pelo padrão FIPS 140-2 ou algum equivalente (Veja http://csrc.nist.gov/groups/STM/cmvp/validation.html).						
V7.8	Verificar se os módulos criptográficos operam em seus modos aprovados de acordo com suas políticas de segurança publicadas (Veja http://csrc.nist.gov/groups/STM/cmvp/validation.html).						
V7.9	Verificar se há uma política explícita de como as chaves criptográficas são gerenciados (por exemplo, gerada, distribuída, revogada, expirada). Verificar se esta política é apropriadamente aplicada.						
V7.10	Verificar se todos os códigos que suportam ou usam um módulo criptográfico não são afetados por qualquer código malicioso.						

V8 – Requisitos de Verificação do Tratamento de Erros e Logs

Os Requisitos de Verificação do Tratamento de Erros e Logs definem um conjunto de requisitos que podem ser usados para analisar o rastreamento de eventos de segurança relevantes e identificar o comportamento de um ataque. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 8 - OWASP ASVS Requisitos de Tratamento de Erros e Logs (V8)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V8.1	Verificar se a aplicação não exibe mensagens de erro ou vestígios de pilhas contendo informações sensíveis que poderiam ajudar um atacante, incluindo identificadores de sessão ou informações pessoais.						

V8.2	Verificar se todos os erros do lado do servidor são processados no servidor.						
V8.3	Verificar se todos os controles de logs são implementados no lado servidor.						
V8.4	Verificar se lógica de tratamento de erros nos controles de segurança nega o acesso por padrão.						
V8.5	Verificar se os controles de logs de segurança registram tanto eventos de falhas como os de sucesso identificados como relevantes para a segurança.						
V8.6	Verificar se cada evento de log inclui: 1. um carimbo de tempo de fonte confiável, 2. nível de segurança do evento, 3. um indicador que o evento é relevante para a segurança (se misturado com outros registros), 4. a identidade do usuário que causou o evento (se há um usuário associado ao evento), 5. o endereço IP de origem da requisição associada ao evento, 6. se o evento teve sucesso ou falha, e 7. uma descrição do evento.						
V8.7	Verificar se todos os eventos que incluem dados não confiáveis não serão executados como código no software destinado à visualização de log.						
V8.8	Verificar se os logs de segurança são protegidos contra acessos não autorizados e modificação.						
V8.9	Verificar se existe uma única implementação de registro de logs usada pela aplicação.						
V8.10	Verificar se a aplicação não registra dados sensíveis específicos da aplicação que poderiam ajudar um atacante, incluindo identificadores de sessão do usuário e informações pessoais ou sensíveis.						
V8.11	Verificar se está disponível uma ferramenta de análise de logs que permite procurar por eventos de acordo com combinações de critérios de busca, através de todos os campos no formato de registro de logs suportado por este sistema.						

V8.12	Verificar se todos os códigos que implementam ou usam tratamento de erros e controles de logs não são afetados por qualquer código malicioso.						

V9 - Requisitos de Verificação da Proteção de Dados

Os Requisitos de Verificação da Proteção de Dados definem um conjunto de requisitos que podem ser usados para avaliar a proteção de informações sensíveis (por exemplo, número do cartão de crédito, passaporte, identidade, dados privados). A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 9 - OWASP ASVS Requisitos de Proteção de Dados (V9)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V9.1	Verificar se todos os formulários que contenham informações sensíveis têm desabilitado o cache do lado do cliente, incluindo recursos de auto completar.						
V9.2	Verificar se a lista de dados sensíveis processados pela aplicação é identificada, e que existe uma política explícita de como o acesso a esses dados deve ser controlado e quando estes dados devem ser cifrados (tanto em repouso quanto em trânsito). Verificar se esta política é devidamente aplicada.						
V9.3	Verificar se todos os dados sensíveis são enviados para o servidor no corpo da mensagem HTTP (parâmetros URL nunca são usados para enviar dados sensíveis).						
V9.4	Verificar se todas as informações sensíveis em cache ou as cópias temporárias enviadas ao cliente são protegidas contra acesso não autorizado, ou se elas são removidas /invalidadas após serem acessadas por um usuário autorizado (por exemplo, os cabeçalhos *no-cache* e *no-store Cache-Control* são definidos).						

V9.5	Verificar se todas as informações sensíveis em cache ou as cópias temporárias armazenadas no servidor são protegidas contra acesso não autorizado, ou removidas/ invalidadas após serem acessadas por um usuário autorizado.						
V9.6	Verificar se há um método para remover cada tipo de dados sensíveis da aplicação no final do seu período exigido de retenção.						

V10 – Requisitos de Verificação da Segurança da Comunicação

Os Requisitos de Verificação da Segurança da Comunicação definem um conjunto de requisitos que podem ser usados para certificar que todas as comunicações com a aplicação são devidamente seguras. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 10 - OWASP ASVS Requisitos de Segurança da Comunicação (V10)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V10.1	Verificar se um caminho pode ser construído a partir de uma CA confiável para cada certificado de servidor Transport Layer Security (TLS), e se cada certificado de servidor é válido.						
V10.2	Verificar se falhas de conexões TLS não recaem em uma conexão insegura.						
V10.3	Verificar se o TLS é usado para todas as conexões (incluindo tanto conexões externas como de *backend*) que são autenticadas ou que envolvem funções ou dados sensíveis.						
V10.4	Verificar se as falhas nas conexões TLS *backend* são registradas.						
V10.5	Verificar se caminhos certificados são construídos e verificados para todos os certificados clientes usando âncoras confiáveis configuradas e informações de revogação.						
V10.6	Verificar se todas as conexões com sistemas externos que envolvem informações ou funções sensíveis são autenticadas.						

V10.7	Verificar se todas as conexões com sistemas externos que envolvem informações ou funções sensíveis usam uma conta com os privilégios mínimos necessários para a aplicação funcionar adequadamente.						
V10.8	Verificar se existe um padrão único de implementação do TLS, usado pela aplicação, que é configurado para operar de maneira aprovada*. Veja http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf).						
V10.9	Verificar se codificações de caracteres específicas (por exemplo, UTF-8) são definidas para todas as conexões.						

V11 – Requisitos de Verificação da Segurança do HTTP

Os Requisitos de Verificação da Segurança do HTTP definem um conjunto de requisitos que podem ser usados para avaliar a segurança relacionada às requisições e respostas HTTP, sessões, cookies, cabeçalhos e logs. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 11 - OWASP ASVS Requisitos de Segurança do HTTP (V11)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V11.1	Verificar se redirecionamentos não incluem dados que não foram validados.						
V11.2	Verificar se a aplicação aceita somente um conjunto definido de métodos de requisição HTTP, tais como GET e POST.						
V11.3	Verificar se toda resposta HTTP contém um cabeçalho do tipo de conteúdo (*content type header*) especificando um conjunto seguro de caracteres (por exemplo, UTF-8).						
V11.4	Verificar se a *flag* HTTPOnly é usada em todos os cookies que não requerem, especificamente, acesso do JavaScript.						
V11.5	Verificar se a *flag* de segurança é usada em todos os cookies que contêm informações sensíveis, inclusive o cookie de sessão.						

V11.6	Verificar se cabeçalhos HTTP tanto nas requisições como nas respostas contêm somente caracteres ASCII imprimíveis.						
V11.7	Verificar se a aplicação gera um token aleatório como parte de todos os links e formulários associados com transações ou no acesso a informações sensíveis, e se a aplicação verifica a presença desse token com o valor adequado para o usuário atual no processamento dessas requisições.[15]						

V12 – Requisitos de Verificação da Configuração da Segurança

Os Requisitos de Verificação da Configuração da Segurança definem um conjunto de requisitos que podem ser usados para certificar o armazenamento seguro de todas as informações de configuração que direcionam os comportamentos relacionados à segurança da aplicação. A proteção dessas informações de configuração é crítica para o funcionamento seguro da aplicação. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 12 - OWASP ASVS Requisitos de Configuração da Segurança (V12)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V12.1	Verificar se toda informação de configuração relevante à segurança é armazenada em locais protegidos contra acesso não autorizado.						
V12.2	Verificar se todo o acesso à aplicação é negado caso a aplicação não possa acessar sua informação de configuração de segurança.						
V12.3	Verificar se todas as mudanças nos parâmetros de configuração de segurança, gerenciados pela aplicação, são registradas nos logs de eventos de segurança.						
V12.4	Verificar se a configuração armazenada pode ser exibida em um formato legível para facilitar a auditoria.						

[15] Esse requisito descreve o mecanismo exigido para defender-se de ataques CSRF (Cross Site Request Forgery).

V13 – Requisitos de Verificação da Investigação de Códigos Maliciosos

Para o Nível 4, é exigido procurar por códigos maliciosos em qualquer código que ainda não foi examinado após realizar uma verificação de Nível 3 na aplicação. A tabela abaixo define os requisitos de verificação da Investigação de Códigos Maliciosos que são introduzidos no Nível 4.

Tabela 13 - OWASP ASVS Requisitos de Investigação de Códigos Maliciosos (V13)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V13.1	Verificar se existe código malicioso em qualquer código que tenha sido desenvolvido ou modificado a fim de criar a aplicação.[16]						
V13.2	Verificar se a integridade do código interpretado, bibliotecas, arquivos executáveis e de configuração, é verificada através de *checksums* ou *hashes*.						

V14 – Requisitos de Verificação da Segurança Interna

Os Requisitos de Verificação da Segurança Interna definem um conjunto de requisitos que podem ser usados para certificar se a aplicação se protege em um grau adicional contra falhas da execução. A tabela abaixo define os requisitos de verificação correspondentes que se aplicam a cada um dos quatro níveis de verificação.

Tabela 14 - OWASP ASVS Requisitos de Segurança Interna (V14)

Requisito de Verificação		Nível 1A	Nível 1B	Nível 2A	Nível 2B	Nível 3	Nível 4
V14.1	Verificar se a aplicação protege de acesso não autorizado ou modificação os atributos do usuário e dos dados e a informação da política usada por controles de acesso.						
V14.2	Verificar se as interfaces do controle de segurança são simples o suficiente para que os desenvolvedores as utilizem corretamente.						
V14.3	Verificar se a aplicação protege adequadamente as variáveis e recursos compartilhados contra acesso concorrente inapropriado.						

[16] Por exemplo, procurar por bombas de tempo (*time bombs*) em chamadas ao relógio do sistema, *back doors* em funções não relacionadas aos requisitos do negócio, Easter eggs em caminhos de execução, ataques do tipo salami em transações financeiras com lógica incorreta, outros tipos de código malicioso.

Requisitos para o Relatório de Verificação

Um Relatório ASVS do OWASP contém a descrição da aplicação que foi analisada em relação aos requisitos do ASVS para um determinado nível. O Relatório também documenta os resultados da análise, incluindo quaisquer correções de vulnerabilidades que sejam necessárias.

Os requisitos do relatório ASVS definem o tipo de informação que deve estar presente no relatório. Os requisitos não definem a estrutura, a organização, ou o formato do relatório, mas não impedem que essas informações adicionais sejam incluídas no relatório.

O tipo de informação que é exigido por cada conjunto de requisitos do relatório pode ser nomeado, formatado e organizado de acordo com os requisitos de um verificador. Os requisitos são satisfeitos desde que a informação requerida esteja presente. Um Relatório deve incluir todo o material necessário para que um leitor entenda a análise que foi realizada e os seus resultados, incluindo informação de configuração e fragmentos de códigos, como representado na figura adjacente, que pode ser utilizada para construir a estrutura do Relatório.

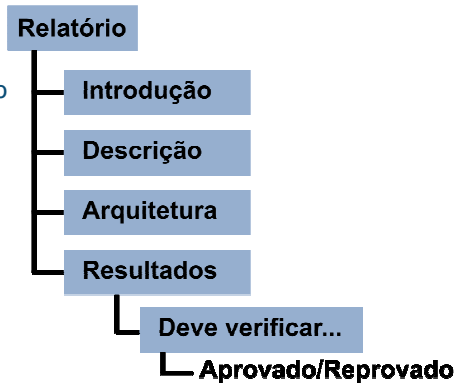

Figura 11 - Conteúdo do Relatório

R1 - Introdução do Relatório

R1.1	Deve fornecer informação suficiente para identificar tanto o relatório como a aplicação que é objeto do relatório.
R1.2	Deve resumir a confiança geral na segurança da aplicação.
R1.3	Deve identificar os principais riscos do negócio associados com a operação da aplicação.
R1.4	Deve identificar as regras de engajamento associadas com a realização da verificação ou que esta pode estar restrita ao escopo da verificação.

R2 - Descrição da Aplicação

R2.1	Deve fornecer uma descrição da aplicação suficiente para ajudar o entendimento de sua operação e do ambiente no qual ela opera.

R3 - Arquitetura de Segurança da Aplicação

R3.1	Deve fornecer detalhes adicionais descrevendo a aplicação, servindo como primeiro passo para garantir ao leitor do relatório que a análise realizada foi completa e exata. Esta parte do relatório fornece o contexto da análise. A informação apresentada nesta sessão será usada no andamento da análise para identificar inconsistências. Esta parte do relatório deve fornecer diferentes níveis de detalhe, dependendo do Nível do ASVS em que a análise foi realizada. Detalhes irão variar de acordo com o Nível.

R4 – Resultados da Verificação

R4.1	Deve apresentar os resultados da análise que foi realizada de acordo com a sessão "Requisitos de Verificação" deste Padrão, incluindo a descrição de quaisquer correções de vulnerabilidades que sejam necessárias, conforme a seguir:

Tabela 15 - OWASP ASVS Verificação do Relatório de Conteúdos dos Resultados

Nível	Aprovado	Reprovado
Resultados do Nível 1	• Veredicto • Configuração da ferramenta (se a ferramenta pode executar a verificação) ou justificativa do veredicto (um argumento para a completude e exatidão, fornecendo evidência específica) • Um mapeamento das capacidades de ferramentas automatizadas para requisitos aplicáveis de verificação detalhada • Uma descrição da configuração da ferramenta e um mapeamento das capacidades da mesma só devem ser fornecidos uma vez como parte do relatório.	• Veredicto • Localização (URL com parâmetros e/ou caminho do arquivo fonte, nome e número(s) de linha) • Descrição (incluindo informações de configuração conforme apropriado) • Classificação de riscos[17] • Justificativa dos riscos
	Uma descrição da configuração da ferramenta e um mapeamento de capacidades da mesma também deve ser fornecido como parte do relatório.	
Resultados dos Níveis 2 – 4	• Veredicto • Justificativa do veredicto (um argumento para completude e exatidão, fornecendo evidência específica)	• Veredicto • Localização (URL com parâmetros e/ou caminho do arquivo fonte, nome e número(s) de linha) • Descrição (incluindo caminhos através dos componentes da aplicação e passos para reprodução) • Classificação de riscos (veja a metodologia OWASP para Avaliação de Riscos) • Justificativa dos riscos

[17] Para maiores informações sobre identificação e estimativa dos riscos associados com vulnerabilidades, consulte o Testing Guide (OWASP, 2008).

Glossário

Alvo de Verificação (TOV - Target of Verification) - Se você estiver realizando uma verificação de segurança de aplicação de acordo com os requisitos do OWASP ASVS, a verificação será de uma aplicação específica. Esta aplicação é chamada de "Alvo de Verificação", ou simplesmente TOV.

Arquitetura de Segurança – Uma abstração de projeto de uma aplicação que identifica e descreve onde e como os controles de segurança são usados, bem como a localização e sensibilidade do usuário e dos dados da aplicação.

Ataques de Negação de Serviço (DOS - Denial of Service) – A inundação de uma aplicação com mais solicitações do que pode suportar.

Ataque Salami - Um tipo de código malicioso que é usado para redirecionar pequenas quantias de dinheiro, sem ser detectado, em operações financeiras.

Autenticação – A verificação da identidade alegada de um usuário da aplicação.

Back Doors (portas dos fundos) – Um tipo de código malicioso que permite o acesso não autorizado a uma aplicação.

Bomba Relógio (Time Bomb) – Um tipo de código malicioso que não é executado até que um tempo pré-configurado ou data tenha decorrido.

Código Malicioso – Código introduzido em uma aplicação durante o seu desenvolvimento sem o conhecimento do proprietário e que burla a política desejada de segurança da aplicação. Não é o mesmo que malware, como um vírus ou worm!

Common Criteria (CC) – Um padrão de várias partes que pode ser usado como a base para a verificação do projeto e implementação de controles de segurança em produtos de TI.

Componente da aplicação – Uma unidade ou grupo de arquivos-fonte, bibliotecas e/ou executáveis, tal como definido pelo verificador para uma determinada.

Configuração de Segurança – A configuração em tempo de execução de uma aplicação que afeta a forma como os controles de segurança são usados.

Controle de Acesso – Um meio de restringir o acesso a arquivos, funções referenciadas, URLs, e dados com base na identidade dos usuários e/ou grupos a que pertencem.

Controle de Segurança – Uma função ou componente que executa uma verificação de segurança (por exemplo, uma verificação de controle de acesso) ou quando chamado resulta num efeito de segurança (por exemplo, gerando um registo de auditoria).

FIPS 140-2 – Um padrão que pode ser usado como a base para a verificação do projeto e implementação de módulos criptográficos.

Malware – Código executável que é introduzido em uma aplicação durante a execução sem o conhecimento do usuário ou do administrador.

Modelagem de Ameaças - Uma técnica que consiste no desenvolvimento de arquiteturas de segurança cada vez mais refinados para identificar agentes de ameaça, zonas de segurança, controles de segurança e importantes ativos técnicos e de negócios.

Módulo Criptográfico – Hardware, software, e/ou firmware que implementa algoritmos criptográficos e/ou gera chaves criptográficas.

Lista Branca – Uma lista de dados ou operações permitidas, por exemplo, uma lista de caracteres permitidos para realizar a validação de entradas.

Lista Negra (em inglês, Blacklist) – Uma lista de dados ou operações que não são permitidos, por exemplo, uma lista de caracteres que não são permitidos como entrada.

Ovos de Páscoa (*Easter Eggs)* – Um tipo de código malicioso que não é executado até que ocorra um evento específico de entrada de um usuário.

Open Web Application Security Project (OWASP) – é uma comunidade mundial livre e aberta com foco em melhorar a segurança de softwares de aplicação. Nossa missão é tornar a segurança de aplicações "visível", para que pessoas e organizações possam tomar decisões informadas sobre os riscos de segurança das aplicações. Consulte: http://www.owasp.org/

OWASP API de Segurança Corporativa (Enterprise Security API - ESAPI) – Uma coleção livre e aberta de todos os métodos de segurança que os desenvolvedores precisam para criar aplicações Web seguras. Consulte: http://www.owasp.org/index.php/ESAPI

OWASP Guia de Testes – Um documento concebido para ajudar as organizações a entender o que compreende um programa de testes, e para ajudá-los a identificar os passos necessários para construir e operar o programa de testes. Consulte: http://www.owasp.org/index.php/Category:OWASP_Testing_Project

OWASP Metodologia de Avaliação de Riscos – Uma metodologia de classificação de riscos que foi personalizada para segurança de aplicações. Consulte: http://www.owasp.org/index.php/How_to_value_the_real_risk

OWASP Top Ten – Um documento que representa um amplo consenso sobre quais são as falhas de segurança de aplicação Web mais críticas. Consulte: http://www.owasp.org/index.php/Top10

Padrão de Verificação de Segurança da Aplicação (em inglês, ASVS) – Um padrão do OWASP que define quatro níveis de verificação de segurança das aplicações.

Positivo – Veja Lista Branca.

Relatório de Verificação de Segurança da Aplicação – Um relatório que documenta todos os resultados e a devida análise produzida pelo verificador para uma aplicação particular.

Segurança da Aplicação – Segurança em nível de aplicação centra-se na análise dos componentes da camada de aplicação do Modelo OSI (*Open Systems Interconnection*), ao invés de focar, por exemplo, no sistema operacional ou redes conectadas.

Segurança da Comunicação – A proteção dos dados da aplicação quando são transmitidos entre seus componentes, entre clientes e servidores, e entre os sistemas externos e a aplicação.

Sistemas Externos – Uma aplicação do lado do servidor ou serviço que não é parte da aplicação.

Validação de Entrada – A canonização e validação de entradas de usuário não confiáveis.

Validação de Saída – A canonização e validação de saídas da aplicação para os navegadores da Web e sistemas externos.

Verificação Automatizada – O uso de ferramentas automatizadas (tanto as ferramentas de análise dinâmica, estática ou ambas) que usam assinaturas de vulnerabilidades para encontrar problemas.

Verificação Dinâmica – O uso de ferramentas automatizadas que utilizam assinaturas de vulnerabilidades para encontrar problemas durante a execução de uma aplicação.

Verificação de Segurança da Aplicação – A avaliação técnica de uma aplicação de acordo com o OWASP ASVS.

Verificação do Projeto – A avaliação técnica da arquitetura de segurança de uma aplicação.

Verificação Estática – O uso de ferramentas automatizadas que utilizam assinaturas de vulnerabilidades para encontrar problemas no código-fonte da aplicação.

Verificação Interna – A avaliação técnica dos aspectos específicos da arquitetura de segurança de uma aplicação, tal como definido no padrão OWASP ASVS.

Verificador - Uma pessoa ou equipe que está analisando uma aplicação de acordo com as exigências do OWASP ASVS.

Aonde ir a partir de agora

OWASP é o melhor local para segurança de aplicações Web. O site OWASP hospeda muitos projetos, fóruns, blogs, apresentações, ferramentas e artigos. Além disso, o OWASP organiza duas grandes conferências de segurança de aplicações Web por ano, e tem mais de 80 capítulos locais. A página do projeto OWASP pode ser acessada em http://www.owasp.org/index.php/ASVS.

Os projetos do OWASP listados a seguir podem ser úteis para usuários/adotantes deste padrão:

- *Projeto OWASP Top Ten* - http://www.owasp.org/index.php/Top_10
- *Guia OWASP de Revisão de Código* - http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- *Guia OWASP de Testes* - http://www.owasp.org/index.php/Testing_Guide
- *Projeto API Segurança Corporativa OWASP* - http://www.owasp.org/index.php/ESAPI
- *Projeto Legal OWASP* - http://www.owasp.org/index.php/Category:OWASP_Legal_Project

De forma similar, os seguintes sites também podem ser úteis para usuários/adotantes deste padrão:

- *OWASP* - http://www.owasp.org
- *MITRE* - Common Weakness Enumeration – Vulnerability Trends, http://cwe.mitre.org/documents/vuln-trends.html
- *PCI Security Standards Council* - editores das normas PCI, relevantes para todas as organizações de processamento ou armazenamento de dados de cartão de crédito, https://www.pcisecuritystandards.org
- *PCI Data Security Standard (DSS) v1.1* - https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

THE BELOW ICONS REPRESENT WHAT OTHER VERSIONS ARE AVAILABLE IN PRINT FOR THIS TITLE BOOK.

ALPHA: "Alpha Quality" book content is a working draft. Content is very rough and in development until the next level of publication.

BETA: "Beta Quality" book content is the next highest level. Content is still in development until the next publishing.

RELEASE: "Release Quality" book content is the highest level of quality in a books title's lifecycle, and is a final product.

ALPHA
PUBLISHED

BETA
PUBLISHED

RELEASE
PUBLISHED

YOU ARE FREE:

to share - to copy, distribute and transmit the work

to Remix - to adapt the work

UNDER THE FOLLOWING CONDITIONS:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike. - If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

OWASP
The Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

On the cover: Braconid wasps are beneficial parasites. Braconids parasitize a broad range of hosts: caterpillars, flies, wasps, beetles, and aphids. After a female injects an egg into a host, the larva feeds slowly on that single host. By the time the host dies, the larva is fully grown. It pupates inside or near the dead host, sometimes in a silken cocoon, to emerge later as an adult wasp.