+R Notas Sobre Riscos

Isso é sobre riscos, não sobre vulnerabilidades

Embora as versões do OWASP Top 10 de [2007](https://www.owasp.org/index.php/Top_10_2007) e anteriores, fossem focadas em identificar as "vulnerabilidades" mais comuns, o [OWASP Top 10](https://www.owasp.org/index.php/Top10) sempre foi organizado em torno de riscos. Isto tem causado alguma confusão compreensível por parte das pessoas em busca de uma taxonomia estanque de vulnerabilidades. O [OWASP Top 10 de 2010](https://www.owasp.org/index.php/Top_10_2010), esclareceu o foco de risco no Top 10 por ser muito explícito sobre como agentes de ameaça, vetores de ataque, vulnerabilidades, impactos técnicos e no negócio se combinavam para produzir riscos. Esta versão do OWASP Top 10 segue a mesma metodologia.

A metodologia de Classificação de Risco para o Top 10 é baseado no [OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology). Para cada item Top 10, estimou-se o risco típico que cada vulnerabilidade introduz em uma aplicação web típica verificando fatores comuns de probabilidade e fatores de impacto para cada vulnerabilidade comum. Em seguida, classificamos de forma ordenada o Top 10 de acordo com as vulnerabilidades que normalmente apresentam o risco mais significativo para uma aplicação.

A [OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology) define inúmeros fatores para ajudar a calcular o risco de uma vulnerabilidade identificada. No entanto, o Top 10 deve falar sobre generalidades, ao invés de vulnerabilidades específicas em aplicações reais. Consequentemente, não podemos ser tão exatos quanto os proprietários do sistema podem ser quando calculam os riscos para sua aplicação. Você está melhor equipado para julgar a importância de suas aplicações e dados, quais são seus agentes de ameaça, e como o sistema foi desenvolvido e está sendo operado.

Nossa metodologia inclui três fatores de probabilidade para cada vulnerabilidade (prevalência, detecção e facilidade de exploração) e um fator de impacto (impacto técnico). A prevalência de uma vulnerabilidade é um fator que normalmente você não tem que calcular. Para os dados de prevalência, foram fornecidas estatísticas a partir de um certo número de diferentes organizações (como referenciado na seção Agradecimentos na página 4) e temos uma média de seus dados em conjunto para chegar a uma lista Top 10 da probabilidade de existência por prevalência. Estes dados foram então combinados com os dois outros fatores de probabilidade (detecção e facilidade de exploração) para calcular uma classificação de probabilidade para cada vulnerabilidade. Este valor foi então multiplicado pelo nosso impacto técnico médio estimado para cada item para chegar a uma classificação de risco global do Top 10.

Observe que esta abordagem não leva em conta a probabilidade do agente de ameaça. Nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real sobre o seu negócio. Sua organização terá de decidir qual o grau de risco de segurança das aplicações está disposta a aceitar dada a sua cultura, indústria e ambiente regulatório. O objetivo do OWASP Top 10 não é fazer a análise de risco para você.

A figura seguinte ilustra o nosso cálculo do risco para A3: Cross-Site Scripting, como um exemplo. XSS é tão comum que justifica o único "muito difundido", valor 0 de prevalência. Todos os outros riscos variaram de generalizada a rara (valor de 1 a 3).

Agentes de ameaça

Vetores de ataque

Vulnerabilidades de Segurança

Impactos Técnicos

Impactos do Négocio

Específico da Aplicação

Exploração

MÉDIA

Prevalência

MUITO DIFUNDIDA

Detecção

FÁCIL

Impacto

MODERADO

Específico do Negócio/

Aplicação