

Gerenciamento de segurança on-line

White paper

Dezembro de 2007

Rational software



As doze maiores ameaças do mercado intermediário: evitando ataques maliciosos comuns em nível de aplicativo.

Conteúdo

- 2** *Introdução*
- 3** *Compreendendo ataques maliciosos comuns*
- 3** *Doze ataques maliciosos comuns*
- 6** *Construindo aplicativos mais resistentes a ataques maliciosos*
- 7** *Como a IBM pode ajudar*

Introdução

Conforme as organizações crescem cada vez mais dependentes de software on-line, o risco de ataques maliciosos também tem se tornado mais sério. Tais ataques podem causar uma paralisação dos negócios, custar milhões de dólares à empresa em transações perdidas e potencialmente manchar a imagem da marca.

Embora a maioria das empresas seja capaz de implementar segurança eficiente em nível de rede utilizando firewalls e criptografia, muitas delas inadvertidamente colocam informações sigilosas de clientes e corporações em risco ao falharem na proteção em nível do aplicativo. Consequentemente, pensando como um desenvolvedor e identificando atalhos que ele deveria ter criado, um hacker pode destruir um aplicativo vulnerável e sua infraestrutura adjacente em questão de horas, usando nada mais que um navegador de internet.

Felizmente, organizações bem administradas podem proteger seus aplicativos de web incluindo avaliações de vulnerabilidade e simulações de ataques (ethical hacks) em seu processo de desenvolvimento e entrega de software. Utilizando ferramentas automatizadas para realizar essas verificações em todo o ciclo de vida do aplicativo on-line, auditores, desenvolvedores e profissionais de garantia de qualidade (QA) podem ajudar a anular os hackers e a reduzir a exposição da empresa a potenciais perdas de negócios. Este artigo descreve 12 dos ataques maliciosos mais comuns e oferece as regras básicas que você pode seguir para ajudar a criar aplicativos de web mais resistentes aos ataques.

Destaque

Os peritos do IBM Rational trabalharam com clientes em vários setores regulamentados para identificar vulnerabilidades comuns na segurança de aplicativos da Web.

Ataques comuns incluem envenenamento de cookie, manipulação de campo oculto e violação de parâmetro.

Compreendendo ataques maliciosos comuns

Depois de trabalhar com clientes líderes empresariais em uma ampla gama de setores regulados – inclusive serviços financeiros, governo e indústria farmacêutica – a equipe técnica IBM Rational identificou e estudou os 12 ataques maliciosos mais comuns.

Doze ataques maliciosos comuns

Tipo de ataque	Proposta ilícita	Como acontece
1. Envenenamento de cookie	Roubo de identidade/interceptação de sessão	Muitos aplicativos de Web utilizam cookies para salvar informações como ID de usuário ou registro de data e horário, na máquina do cliente. Mas esses cookies nem sempre são criptograficamente seguros, assim, um hacker pode modificá-los e enganar o aplicativo mudando seus valores – essencialmente “envenenando” o cookie. O hacker pode assim ganhar acesso a contas de outras pessoas e efetuar transações fraudulentas, como compras e transferências de dinheiro.
2. Manipulação de campo oculto	Furto em loja eletrônica	As aplicações de comércio eletrônico frequentemente utilizam campos ocultos para salvar informações sobre a sessão de um cliente, eliminando a necessidade de manter um banco de dados complexo no lado do servidor. Muitos também utilizam tais campos para armazenar preços de mercadorias. Em sites desprotegidos, os hackers podem visualizar códigos fonte, encontrar esses campos ocultos e alterar os preços. As empresas podem não detectar tais mudanças e enviar a mercadoria ao hacker com um preço alterado – e talvez até fazer um desconto.
3. Violação de parâmetro	Fraude	Muitos aplicativos falham em confirmar a exatidão de parâmetros de interface gateway comum (CGI) embutidos em um hyperlink, logo os hackers são capazes de alterar facilmente esses parâmetros. Isso pode permitir que o hacker tenha um cartão de crédito com limite de US\$500.000, ignore uma tela de login ou ganhe acesso a pedidos e informações de outros clientes.

As doze maiores ameaças do mercado intermediário: evitando ataques maliciosos comuns em nível de aplicativo.

Página 4

Destaques	Tipo de ataque	Proposta ilícita	Como acontece
<i>Ao explorar as vulnerabilidades comuns de segurança, os hackers podem atacar aplicativos de web empresariais usando várias abordagens.</i>	4. Estouro de buffer	Negação de Serviço	Ao explorar uma falha em um formulário de Web, os hackers podem sobrecarregar um servidor com excesso de informações, fazendo com que ele trave e feche o web site.
	5. Scripting inter-sites	Interceptação/roubo de identidade	Os hackers podem injetar códigos maliciosos em um web site que os executa como se tivessem sido originados no site alvo. Isso dá aos invasores total acesso ao documento recuperado e podem até conseguir o envio dos dados da página para eles.
	6. Exploração de invasão e opções de depuração	Infração	Os desenvolvedores normalmente incorporam opções de depuração no código para testar o site antes de colocá-lo no ar. Se eles se esquecerem de fechar esses falhas de segurança, os hackers podem acessar livremente informações sigilosas.
	7. Navegação forçada	Violação e invasão	Os hackers podem sabotar o fluxo do aplicativo e acessar informações e componentes que deveriam ser inacessíveis, como arquivos de registros, instalações administrativas e código fonte de aplicativo.
	8. Divisão de respostas HTTP	Phishing, roubo de identidade e e-graffiti	Os hackers podem envenenar um cache de web no mesmo site e em sistemas intermediários, o que permite que eles mudem páginas de web no cache e realizem uma série de ataques contra os usuários. E mais, esta tática dá aos hackers uma habilidade aprimorada de ocultar suas atividades.

As doze maiores ameaças do mercado intermediário: evitando ataques maliciosos comuns em nível de aplicativo.

Página 5

Destaques

Algumas infraestruturas e protocolos integrados que suportam aplicativos baseados em XML podem introduzir vulnerabilidades na infraestrutura, protocolos e conteúdo de um site.

Tipo de ataque	Proposta ilícita	Como acontece
9. Furto/Cavalo de tróia	Dano malicioso	Os hackers podem ocultar comandos perigosos por meio de um cavalo de tróia que libera código malicioso ou não autorizado, danificando o site.
10. Exploração de falha de configuração de terceiro	Dano malicioso	Os hackers normalmente visitam sites públicos que postam vulnerabilidades e patches. Explorando esses problemas de configuração conhecidos, os hackers podem potencialmente criar um novo banco de dados que torna o banco de dados atual inutilizável pelo site.
11. Exploração de vulnerabilidades conhecidas	Controle de site	Algumas tecnologias web têm fraquezas inerentes que podem ser exploradas por um hacker persistente. Por exemplo, alguns hackers podem comandar um site inteiro porque eles sabem como acessar as senhas do administrador via tecnologia Microsoft® Active Server Page (ASP).
12. Exploração de vulnerabilidades dos serviços XML e de Web	Dano malicioso	Algumas infraestruturas e protocolos integrados que suportam aplicativos baseados em XML podem introduzir vulnerabilidades na infraestrutura, protocolos e conteúdo de um site. Além disso, alguns tipos de ataques – inclusive expansão de entidade, injeção XPatch, injeção de linguagem de consulta estruturada (SQL) em XQuery, e vários ataques de negação de serviço – exploram a flexibilidade e riqueza do XML para causar danos importantes em todos esses elementos

Destaques

Para proteger seus ativos baseados na web, as organizações podem construir a segurança em aplicativos de Web e testar as vulnerabilidades durante o ciclo de vida de desenvolvimento e entrega.

Construindo aplicativos mais resistentes a ataques maliciosos

Com tantas oportunidades para os hackers explorarem a tecnologia de Web, o que as organizações podem fazer para proteger seus ativos baseados na Web? Primeiro, pensar defensivamente. Ao invés de manterem o foco apenas em como atrair usuários para o site, presumir que alguns desses usuários tentarão manipular seus aplicativos. Ajudar a construir a segurança em seus aplicativos de web testando as vulnerabilidades durante o ciclo de vida de desenvolvimento e entrega. Utilizar ferramentas automatizadas para ajudar a garantir que estejam testando todos os aplicativos e detectando vulnerabilidades que possam escapar pelos vãos da verificação manual. Além disso, ter em mente a seguinte regra: nunca confiar em dados que venham de um usuário e nunca fazer suposições sobre os limites das tecnologias de um usuário.

Em outras palavras, todos os dados de fontes externas são potencialmente perigosos. Presuma que tudo que um usuário puder teoricamente manipular, será manipulado. Além disso, somente porque um usuário está supostamente empregando uma tecnologia específica, não significa que isso vai limitar suas ações. Por exemplo, mesmo se um navegador não mostrar campos ocultos em um código de página HTML, você deve presumir que alguns usuários ainda poderão encontrar e manipular tais campos antes de enviar as páginas de volta ao seu servidor.

Destaques

O IBM Rational AppScan Express Edition é uma ferramenta de teste de segurança para aplicativo de web que automatiza as avaliações de vulnerabilidade e oferece níveis inflexíveis de segurança para aplicativos de Web para empresas de porte médio.

Como a IBM pode ajudar

Organizações com pequenas ou limitadas equipes de desenvolvimento de aplicações também precisam considerar o teste de segurança como parte do ciclo de vida do desenvolvimento. Mas essas organizações frequentemente têm que sacrificar a funcionalidade em nome da viabilidade financeira. O IBM Rational AppScan Express Edition atende os requisitos de organizações de porte médio oferecendo a mesma funcionalidade de teste de segurança inflexível oferecida pelo IBM Rational AppScan Standard Edition a um preço atraente. Projetado para facilitar o desenvolvimento, o Rational AppScan Express Edition reduz significativamente o tempo e custo associados com a verificação manual de vulnerabilidade, permitindo que suas equipes se foquem em outras necessidades relacionadas à segurança e TI na organização.

Para mais informações

Para mais informações sobre como o IBM Rational AppScan pode ajudá-lo a criar aplicativos de web ricos em segurança e a evitar ataques maliciosos comuns, entre em contato com seu representante IBM ou parceiro de negócios IBM ou visite:

www-01.ibm.com/software/awdtools/appscan/express



IBM Brasil Ltda

Rua Tutóia, 1157
CEP 04007-900
São Paulo – Brasil

O site da IBM pode ser encontrado em:

ibm.com

IBM, o logotipo IBM, ibm.com, AppScan e Rational são marcas registradas da International Business Machines Corporation nos Estados Unidos, outros países, ou ambos.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviços de outros.

Os dados contidos neste documento são fornecidos somente para fins informativos. Embora todos os esforços tenham sido feitos para verificar a completude e exatidão das informações aqui contidas, elas são fornecidas "no estado em que se encontram", sem garantia de qualquer natureza, expressa ou implícita. Além disso, estas informações são baseadas nos planos e estratégia atuais de produto IBM, os quais estão sujeitos a alterações pela IBM sem aviso prévio. A IBM não deve ser responsabilizada por quaisquer danos que surjam do uso, ou que de outra forma se relacione com este documento ou qualquer outra documentação. Nada contido nesta documentação é destinado a, nem deve ter efeito de, criar quaisquer garantias ou representações por parte da IBM (ou seus fornecedores ou licenciadores), ou alterar os termos e condições do contrato de licença aplicável que rege o uso do software IBM.

Os clientes IBM são responsáveis por garantir sua própria conformidade com os requisitos legais. É da inteira responsabilidade do cliente obter conselho de órgão legal competente quanto à identificação e interpretação de quaisquer leis e requisitos regulatórios relevantes que possam afetar o negócio do cliente e quaisquer ações que o cliente possa ter que tomar para estar em conformidade com tais leis.

Produzido nos Estados Unidos da América
12-07

© Copyright IBM Corporation 2009
Todos os direitos reservados.