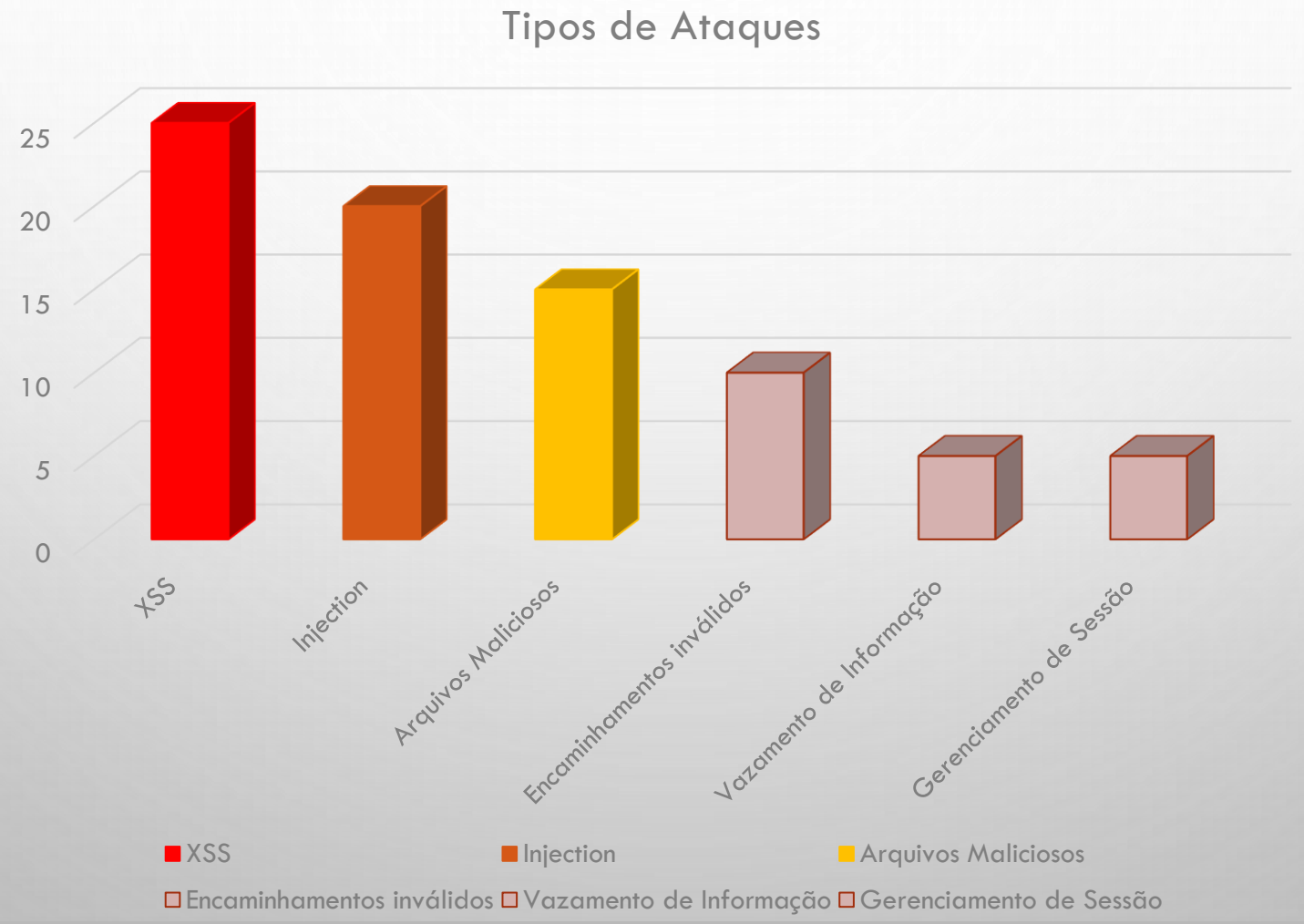
AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

Principais Ameaças em Aplicações WEB

The Top 10 Most Critical Web Application Security Risks



A **Open Web Application Security Project** (OWASP) é uma entidade sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança de softwares aplicativos reunindo informações importantes que permitem avaliar riscos de segurança e combater formas de ataques através da internet.

Os estudos e documentos da OWASP são disponibilizadas para toda a comunidade internacional, e adotados como referência por entidades como U.S. Defense Information Systems Agency (DISA), U.S. Federal Trade Commission, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo PCI Council.

O trabalho mais conhecido da OWASP é sua lista "**The Top 10 Most Critical Web Application Security Risks**", que reúne os riscos de ataque mais críticos exploráveis a partir de vulnerabilidades nas aplicações web.

A **OWASP** utiliza uma metodologia baseada na classificação do risco **(Risk Rating Methodology)** para priorizar sua lista **Top 10**, que é mantida atualizada periodicamente a partir de pesquisas e estatísticas sobre ataques identificados em todo o mundo.

Além de identificar os ataques de maior risco, a OWASP faz várias recomendações de segurança para que cada um daqueles ataques sejam evitados a partir das etapas do desenvolvimento das aplicações.

Para orientar o uso de critérios de segurança desde a codificação, a **OWASP** também recomenda adotar uma metodologia para modelagem de risco (**Threat Risc Modeling**) desde a fase de desenho da aplicação web, evitando assim desperdício de tempo, dinheiro, recursos e de controles inúteis, para que haja foco no mapeamento dos riscos reais já identificados.

https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf

Principais Anestésicos

Injeções

- Ocorre quando a aplicação envia dados não tratados para algum serviço interno.
- Pode ser feita via SQL, LDAP, Xpath, comandos de sistema operacional, argumentos de programas, etc.
- Descoberta por varreduras e/ou *fuzzers*
- Mais facilmente por verificação de código.

- Dependendo do tipo de injeção os danos causados podem ser:

  - ✓ Perda ou corrupção de dados
  - ✓ Negação de Serviço
  - ✓ Falhas de autenticação
  - ✓ Execução arbitrária de código e até comprometimento total do sistema.

- Não utilizar dados não confiáveis em comandos e/ou queries.
- Rotinas de validação ou “escape” de caracteres.
- É aconselhável o uso de validação positiva nas entradas.
- Utilizar canonicalização de dados.

XSS – Cross Site Scripting

Descrição

- Ocorre quando uma aplicação inclui dados não tratados em um objeto enviado ao navegador.
- A detecção pode ser feita via teste de injeção ou análise de código.
- Existem 3 principais tipos:
  - ✓ *Stored*
  - ✓ *Reflected*
  - ✓ *DOM based XSS*

Impactos

- Atacante pode executar scripts no navegador da vítima para:
  - ✓ Roubo de informações de sessão
  - ✓ Pichação de Sites
  - ✓ Inserção de conteúdo malicioso
  - ✓ Redirecionamento de usuários e etc.

- Além da exposição de informações dos usuários, tal falha pode denegrir a imagem da instituição responsável pela aplicação.

Como se Prevenir?

- “Escapar” caracteres vindo de fontes não confiáveis e que serão utilizados no contexto do navegador (body, atributos, JavaScript, CSS, URL).
- A validação positiva é sempre interessante mas é preciso atentar para peculiaridades da aplicação em questão pois caracteres especiais e codificações diversas podem fazer parte da rotina da aplicação.

Quebra de Autenticação / Sessão

Quebra de Autenticação / Sessão

- Restrição de conteúdos / recursos

- **Autenticação HTTP:**

Basic -> credenciais concatenadas separadas por “:” e codificadas em base64

Digest -> hash MD5

Quebra de Autenticação / Sessão

HTTP digest:

Força-bruta
Hydra
(http://freeworld.thc.org/thc-hydra/)

Replay de tráfego
TCPReplay
(http://tcpreplay.synfin.net/trac/)

Como se Prevenir

Quebra de Autenticação / Sessão

- Tunelameto por SSL
- Políticas de segurança
- CAPTCHA
- OWASP Authentication_Cheat_Sheet

Referência Direta a Objetos

Definição

Referência Direta a Objetos

- Exposição de informações internas
- Evite Controle de Acesso em camada de apresentação
- Modificações de informações para acesso a dados não autorizados

Referência Direta a Objetos

- Evite expor referências a objetos internos
- Validação de referências
- Mapas de referência

Ex: http://www.example.com/application?file=1

Cross Site Request Forgery

Definição

Cross Site Request Forgery (CSRF)

• Browsers enviam alguns tipos de credenciais automaticamente em cada requisição

Cookies
Cabeçalhos
Endereço IP
Certificados SSL

Cross Site Request Forgery (CSRF)

- A vítima acessa um site malicioso enquanto está logada no sistema vulnerável

- O atacante força a vítima a fazer tal
- requisição

Como se Prevenir

Cross Site Request Forgery (CSRF)

- Autenticações forçadas em requisições sensíveis

- Controle exposição de dados utilizados
- como credenciais

- OWASP: CSRF_Prevention_Cheat_Sheet

Falhas de Configuração

Falhas de Configuração

• Aplicações rodam em cima de serviços que rodam em cima de SOs

• Todos podem ser vetores de ataque

• *Exploits* (e *patchs*!) se aplicam à qualquer tipo de software

Como se Prevenir

Falhas de Configuração

- “Hardening” de servidores
- *Patchs* e atualizações
- Homologação de mudanças
- *Vulnerability Management*

Armazenamento com métodos Inseguros

DESCRIÇÃO

- FALHA MAIS COMUM E GRAVE: SIMPLESMENTE
- NÃO CRIPTOGRAFAR DADOS SENSÍVEIS
- FALHAS QUANDO A CRIPTOGRAFIA É EMPREGADA:
  - GERAÇÃO E ARMAZENAMENTO INSEGUROS DE CHAVES
  - NÃO IMPLANTAR POLÍTICAS DE ROTAÇÃO DE CHAVES
  - UTILIZAR ALGORITMOS DE CRIPTOGRAFIA FRACOS
  - UTILIZAR MÉTODOS DE CRIPTOGRAFIA EM UMA SÓ VIA (HASH) FRACOS OU SEM SALTO PARA PROTEGER SENHAS.

Impacto

- FREQUENTEMENTE COMPROMETEM TODOS OS
- DADOS PROTEGIDOS POR CRIPTOGRAFIA
- TIPICAMENTE, ESTES DADOS INCLUEM, MAS NÃO
- ESTÃO LIMITADOS À:
  - CREDENCIAIS DE ACESSO
  - DADOS PESSOAIS
  - REGISTROS DE SAÚDE
  - CARTÕES DE CRÉDITO, ETC.

Como se Prevenir?

- REQUISITOS MÍNIMOS PARA ARMAZENAMENTO
- DE DADOS EM APLICAÇÕES WEB:
  - ALGORITMOS DE CRIPTOGRAFIA E CHAVES UTILIZADOS DEVEM
  - SER APROPRIADAMENTE FORTES.
  - CHAVES E SENHAS DEVEM ESTAR PROTEGIDAS DE ACESSO
  - NÃO AUTORIZADO.
  - SENHAS DEVEM ARMAZENADAS EM HASH COM UM
  - ALGORITMO DE CRIPTOGRAFIA EM UMA SÓ VIA FORTE E COM
  - UM SALTO APROPRIADO.

Falha em restringir acesso à URL

DESCRIÇÃO

- FALHA EM PROTEGER REQUISIÇÕES DA PÁGINA APROPRIADAMENTE

- FALHAS BÁSICAS DE FÁCIL DETECÇÃO, UMA VEZ LISTADAS TODAS AS PÁGINAS (URLS) QUE EXISTEM PARA ATACAR.

IMPACTO

- FREQUENTEMENTE, CONTAS PRIVILEGIADAS SÃO O ALVO DESTE TIPO DE ATAQUE

- UMA VEZ BEM SUCEDIDO, O ATACANTE PODE FAZER QUALQUER COISA QUE A VÍTIMA PODERIA FAZER

COMO SE PREVENIR

- É FUNDAMENTAL TER MUITO BEM DEFINIDO O QUE SE TRATA DE INFORMAÇÃO PÚBLICA (NÃO REQUER CREDENCIAIS) E PRIVADA (REQUER CREDENCIAIS) E ENTÃO PROTEGER A INFORMAÇÃO PRIVADA.

- POLÍTICAS MAIS RESTRITIVAS (*BLOCK ALL, ALLOW SOME*) SÃO MAIS ADEQUADAS QUE AS MAIS PERMISSIVAS *(ALLOW ALL, BLOCK SOME*), POIS OS CASOS NÃO PREVISTOS SÃO BLOQUEADOS E O ACESSO É LIBERADO SOB DEMANDA.

Proteção Insuficiente no Transporte de Dados

DESCRIÇÃO

- FALHA EM PROTEGER O TRÁFEGO DE REDE ONDE PASSAM OS DADOS DA APLICAÇÃO
- UTILIZAÇÃO DE CRIPTOGRAFIA SOMENTE NA AUTENTICAÇÃO (EXPONDO DADOS E IDS DE SEÇÃO)
- UTILIZAÇÃO DE CERTIFICADOS EXPIRADOS OU MAL CONFIGURADOS

Impacto

- ESTAS FALHAS EXPÕE DADOS DE USUÁRIOS E PODEM CONDUZIR A ROUBO DE CONTAS.
- SE UMA CONTA DE ADMINISTRAÇÃO FOR COMPROMETIDA, O SITE INTEIRO PODE SER EXPOSTO.
- UTILIZAR DE MÉTODOS DE CRIPTOGRAFIA MAL CONFIGURADOS TAMBÉM PODEM FACILITAR ATAQUES DE PHISHING E MAN-IN-THE-MIDDLE (MITM)

Como se Prevenir

- É IMPORTANTE QUE A APLICAÇÃO NÃO ACEITE REQUISIÇÕES CONTENDO DADOS PRIVADOS POR CANAIS INSEGUROS

- A *FLAG 'SECURE*' DOS COOKIES ESTIPULA QUE O COOKIE SÓ PODE SER TRANSMITIDO ATRAVÉS DE UM CANAL SEGURO

Redirecionamentos e repasses não validados

DESCRIÇÃO

- FALHA EM VALIDAR O DESTINO DE REDIRECIONAMENTOS OU REPASSES UTILIZADOS
- PROBLEMAS MAIS COMUNS:
  - AUSÊNCIA DE VALIDAÇÃO DO DESTINO DE UM REDIRECIONAMENTO OU REPASSE
  - SIMILARIDADE ENTRE REDIRECIONAMENTO PARA DESTINOS INTERNOS (DA PRÓPRIA APLICAÇÃO) E EXTERNOS

Interação

- REDIRECIONAMENTOS PODEM INDUZIR USUÁRIOS A INSTALAR MALWARE OU REVELAR INFORMAÇÕES SENSÍVEIS.
- REPASSES INSEGUROS PODEM PERMITIR CONTORNAR CONTROLES DE ACESSO.

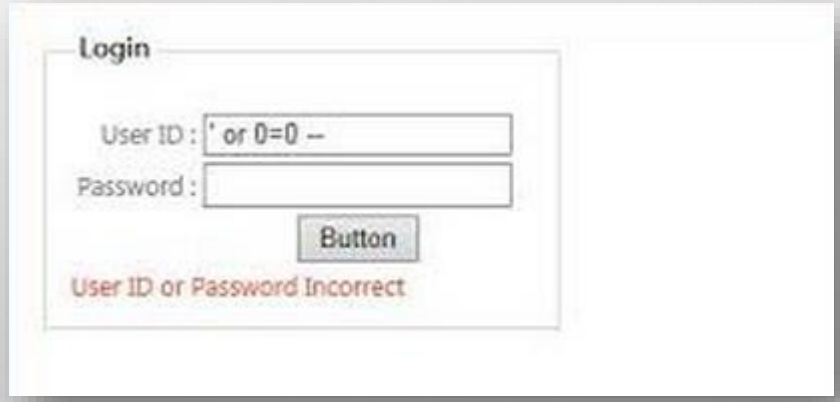
Como se Prevenir

- RECOMENDAÇÕES BÁSICAS PARA UTILIZAR REDIRECIONAMENTOS E REPASSES:
  - NÃO ENVOLVER PARÂMETROS DE USUÁRIO PARA CALCULAR O DESTINO
  - SE NÃO PUDER EVITAR, VALIDAR O PARÂMETRO E VERIFICAR AUTORIZAÇÃO DO USUÁRIO

The Top 10 Most Critical Web Application Security Risks

A1 – Injection Flaws

Falhas ocasionadas por "injeção" de códigos maliciosos, tais como SQL, OS, e injeção LDAP. Ocorrem quando dados não confiáveis são enviados para um intérprete, como parte de um comando ou consulta. Dados hostis do atacante pode enganar o interpretador para executar comandos não intencionais ou acessar dados não autorizados. Por exemplo, envio de dados via um formulário do site.

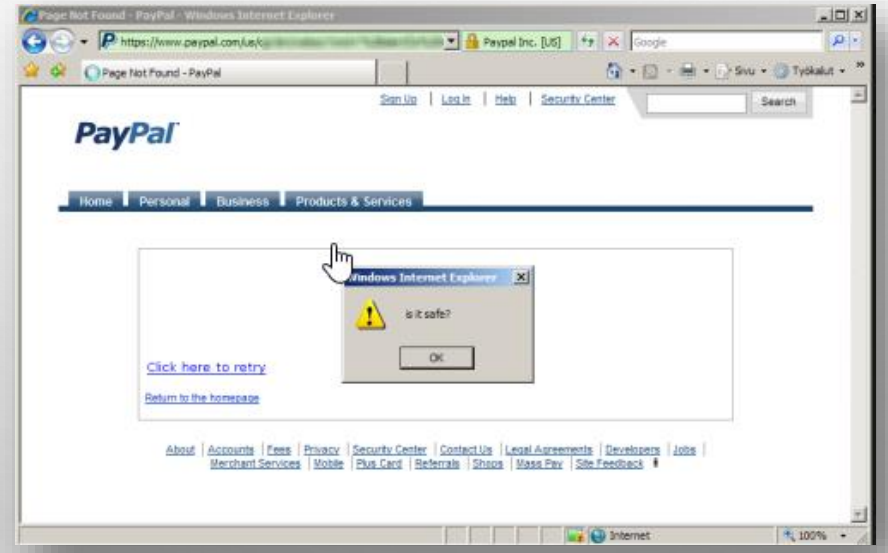


http://pt.wikipedia.org/wiki/Inje%C3%A7%C3%A3o_de_SQL

The Top 10 Most Critical Web Application Security Risks

A2 – Cross Site Scripting

Cross Site Scripting (XSS). XSS ocorrem sempre que um aplicativo usa dados não confiáveis e os envia para um navegador web sem a devida validação e o . XSS permite aos atacantes executarem scripts no navegador da vítima, que pode sequestrar sessões de usuários, desfigurar sites, ou redirecionar o usuário para sites maliciosos.

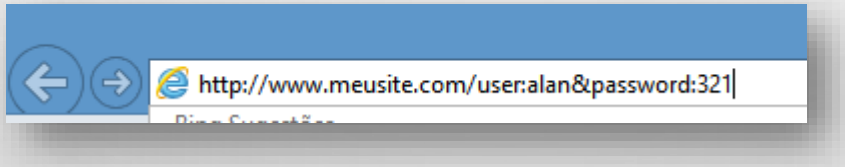


http://msdn.microsoft.com/pt-br/library/cc518054.aspx

The Top 10 Most Critical Web Application Security Risks

A4 - Referências diretas em objetos seguros

A referência de objeto direto ocorre quando um desenvolvedor expõe uma referência a um objeto de implementação interna, como um, diretório ou chave de banco de dados de arquivo. Sem uma verificação de controle de acesso ou outra proteção, os atacantes podem manipular estas referências para acessar dados não autorizados.



The Top 10 Most Critical Web Application Security Risks

A5 - Cross-Site Request Forgery (CSRF)

Um ataque CSRF força o navegador da vítima logada enviar um pedido HTTP forjado, incluindo cookie de sessão da vítima e qualquer outra informação de autenticação incluídos automaticamente, para uma aplicação web vulnerável. Isso permite que o invasor force o navegador da vítima para gerar pedidos e a aplicação vulnerável acha que são pedidos legítimos da vítima.

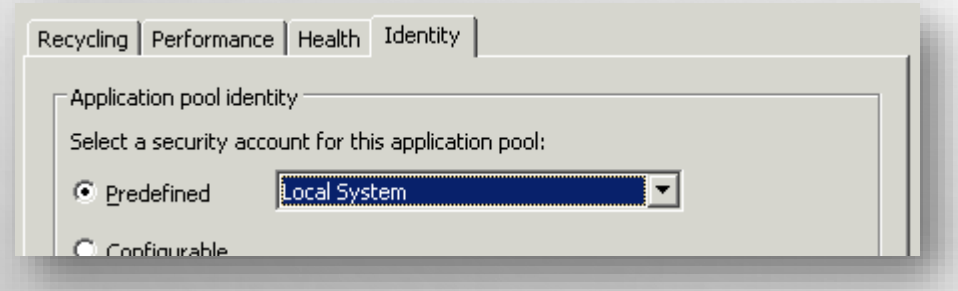
http://msdn.microsoft.com/pt-br/library/gg416514(v=vs.108).aspx

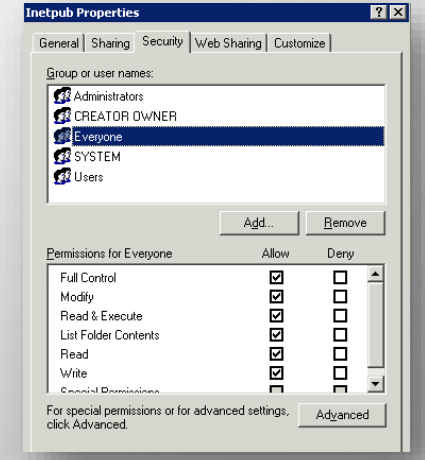
http://msdn.microsoft.com/pt-br/magazine/hh708755.aspx

The Top 10 Most Critical Web Application Security Risks

A6 - Configurações Gerais de Segurança

Uma boa segurança exige ter uma configuração segura definida e implantada para a aplicação, frameworks, servidor de aplicação, servidor web, servidor de banco de dados e plataforma. Todas essas definições devem ser definidas, implementadas e mantidas como muitos não são enviados com padrões seguros. Isso inclui manter todos os softwares atualizados, incluindo todas as bibliotecas de código usadas pela aplicação.





http://technet.microsoft.com/pt-br/subscriptions/t4ahd590(v=vs.80).aspx

The Top 10 Most Critical Web Application Security Risks

A7: Armazenamento de informações criptografados

Muitas aplicações web não protegem adequadamente os dados sensíveis, tais como cartões de crédito, CPFs e credenciais de autenticação, com criptografia ou hashing adequada. Os atacantes podem roubar ou modificar esses dados fracamente protegidos para realizar o roubo de identidade, fraude de cartão de crédito, ou outros crimes.

A8: Falha de restrição de acesso à URL

Muitas aplicações web devem verificar os direitos de acesso à URL antes de exibir links e botões protegidos. No entanto, as aplicações precisam, para executar essas verificações, de um controle de acesso cada vez que essas páginas são acessadas, ou atacantes serão capazes de forjar URLs para acessar essas páginas ocultas de qualquer maneira.

The Top 10 Most Critical Web Application Security Risks

A9: Proteção da camada de Transporte insuficiente

Aplicações frequentemente não conseguem autenticar, criptografar e proteger a confidencialidade e integridade do tráfego de rede sensível. Quando o fazem, eles às vezes suportar algoritmos fracos, uso expirado ou certificados inválidos, ou não usa-os corretamente.

The Top 10 Most Critical Web Application Security Risks

A10: Encaminhamentos e redirecionamentos inválidos

Aplicativos da Web frequentemente redirecionam e encaminham os usuários para outras páginas e site, e usa dados não confiáveis para determinar as páginas de destino. Sem a validação adequada, os atacantes podem redirecionar vítimas a sites de phishing ou malware.