OWASP

O Projeto de Segurança de Aplicativos da Web Aberta (OWASP) é uma organização com a qual todos os desenvolvedores da Web devem estar familiarizados. É uma organização mundial sem fins lucrativos que existe com o único propósito de melhorar a segurança do software da web.

A OWASP foi fundada em 2001 e reconhecida pela primeira vez como uma organização sem fins lucrativos no início de 2004. A organização opera em todo o mundo, ajudando empresas e indivíduos a manterem aplicações seguras que podem ser de confiança de todos.

OWASP coordena listas de verificação de treinamento, diretrizes e desenvolvimento. Além disso, a organização analisa regularmente as vulnerabilidades da Web mais comuns no mercado e publica uma lista de recomendações para que os desenvolvedores possam ficar à frente do mercado.

Este é o último manual traduzido para o português:

https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP_Top_10_-_2013_Brazilian_Portuguese.pdf

Sempre que você estiver procurando por conselhos práticos de segurança na Web sobre segurança, o OWASP deve ser quase sempre o seu primeiro porto de escala.

Para obter ajuda com APIs, o OWASP também pode ajudar: eles publicaram a Folha de Dicas de Segurança REST (https://www.owasp.org/index.php/REST_Security_Cheat_Sheet). Website que não está ainda traduzido em português...

É claro que, como já discutimos durante o video, existem muitos padrões diferentes para a criação de APIs e o REST é apenas um deles; No entanto, existem algumas dicas genéricas úteis que podemos aproveitar deste guia.

Ao desenvolver a API REST, é preciso prestar atenção aos aspectos de segurança desde o início. Nesta postagem, analisarei e explicarei algumas diretrizes de segurança ao desenvolver e testar APIs REST.

REST (ou RE Representational State Transfer) é um meio de expressar entidades específicas em um sistema por elementos de caminho de URL. REST não é uma arquitetura, mas é um estilo arquitetônico para construir serviços no topo da web. O REST permite a interação com um sistema baseado na Web por meio de URLs simplificados em vez de um corpo de solicitação complexo ou parâmetros POST para solicitar itens específicos do sistema.

1- Autorização

Proteger métodos HTTP

Muitas vezes, a API RESTful usa GET (leitura), POST (criar), PUT (substituir / atualizar) e DELETE (para excluir um registro).

Nem todas são opções válidas para cada coleta, usuário ou ação de recursos. Certifique-se de que o método HTTP recebido seja válido para a chave de token / API da sessão e para a coleção, ação e registro de recursos associados.

Métodos permitidos da lista de permissões

É comum que os serviços RESTful permitam vários métodos para uma determinada URL para diferentes operações nessa entidade.

Por exemplo, uma solicitação GET pode ler a entidade enquanto a PUT atualizaria uma entidade existente, o POST criaria uma nova entidade e o DELETE excluiria uma entidade existente.

É importante para o serviço restringir adequadamente os verbos permitidos de forma que apenas os verbos permitidos funcionem, enquanto todos os outros retornarão um código de resposta apropriado (por exemplo, 403 Forbidden).

Proteger ações privilegiadas e coleções de recursos confidenciais

Nem todo usuário tem direito a todos os serviços da web. Isso é vital, pois você não deseja que os serviços da Web administrativos sejam usados incorretamente.

O token de sessão ou a chave de API deve ser enviado como um cookie ou parâmetro de corpo para garantir que as coleções ou ações privilegiadas sejam protegidas adequadamente contra uso não autorizado.

More resources on CSRF:

Cross-Site Request Forgery (CSRF) OWASP

OWASP CSRF Prevention Cheat Sheet

Afonso Alves

15 de maio 2018