INE5429-07208
Segurança em Computação

OWASP TOP 10 / 2017

Prof. Jean Everson Martina

OWASP TOP 10

- O Open Web Application Security Project, é uma comunidade on-line que produz artigos, metodologias, documentação, ferramentas e tecnologias disponíveis gratuitamente no campo de segurança de aplicações web.
- O OWASP Top Ten representa um amplo consenso sobre quais são as falhas de segurança mais críticas das aplicações web.
- A equipe OWASP lançou recentemente a versão revisada e atualizada de 2017 os dez riscos de segurança mais críticos de aplicações web.

INJEÇÃO

- O QUE É ISSO?
  - Websites e aplicativos ocasionalmente precisam executar comandos no banco de dados ou sistema operacional para adicionar ou excluir dados, executar um script ou iniciar outros aplicativos. Se entradas não verificadas forem adicionadas a uma cadeia de comandos ou a um comando do banco de dados, os atacantes podem executar comandos à vontade para assumir o controle de um servidor, de dispositivo ou adquirir dados.

INJEÇÃO

- COMO FUNCIONA?
  - Se um site, aplicativo ou dispositivo incorporar a entrada do usuário em um comando, O invasor pode inserir um comando de "carga útil" diretamente na entrada mencionada. Se essa entrada não é verificado, um invasor "injeta" e executa seus próprios comandos.
- Por que é ruim?
  - Uma vez que os invasores puderem executar comandos, eles poderão controlar seu website, aplicativos, e dados.

AUTENTICAÇÃO QUEBRADA

- O QUE É ISSO?
  - Autenticação é o processo para garantir que você mesmo esteja acessando suas contas e dados. Geralmente, é feito por uma combinação de nome de usuário e senha.
  - Uma certa complexidade é adicionada quando as pessoas esquecem ou mudam senhas ou desejam atualizar seus endereços de e-mail.
  - Fica ainda mais complexo como um site, aplicativo ou dispositivo em si torna-se maior, mais amplo e mais conectado com outros sites, aplicativos ou dispositivos.

AUTENTICAÇÃO QUEBRADA

- COMO FUNCIONA?
  - Nos ataques mais simples, as senhas podem ser adivinhadas ou roubadas se deixadas desprotegidas.
  - À medida que as complexidades são adicionadas, os invasores podem encontrar outras áreas em que as credenciais do usuário ou as sessões têm proteções inadequadas e, em seguida, seqüestram o acesso de um usuário e eventualmente, seus dados.
- Por que é ruim?
  - Se os invasores puderem seqüestrar a sessão de um usuário ou administrador, eles terão acesso a tudo disponível nessa conta, desde os dados até o controle da conta.

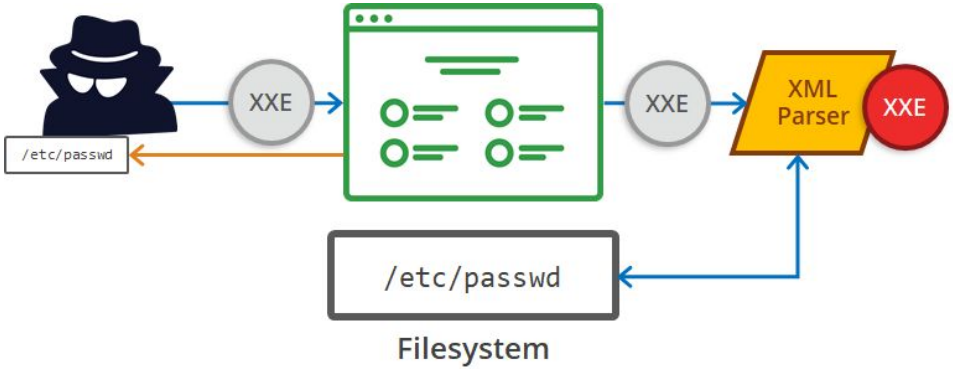
EXPOSIÇÃO DE DADOS SENSÍVEIS

- O QUE É ISSO?
  - Dados confidenciais, como números de cartão de crédito, dados de integridade ou senhas, tem proteção extra, dado o potencial de danos se cair no erro mãos.
  - Existem até regulamentações e padrões projetados para proteger tais dados. Mas, se os dados sensíveis forem armazenados, transmitidos ou protegidos por métodos fracos, podem ser exposto a atacantes.

EXPOSIÇÃO DE DADOS SENSÍVEIS

- COMO FUNCIONA?
  - Se os dados forem armazenados ou transferidos como texto claro, se a criptografia usada for mais antiga / mais fraca, ou se os dados forem decifrados de maneira descuidada, os invasores podem obter acesso e explorar os dados.
- Por que é ruim?
  - Quando um invasor tem senhas e números de cartão de crédito, eles podem fazer um dano considerável as pessoas e as reputações

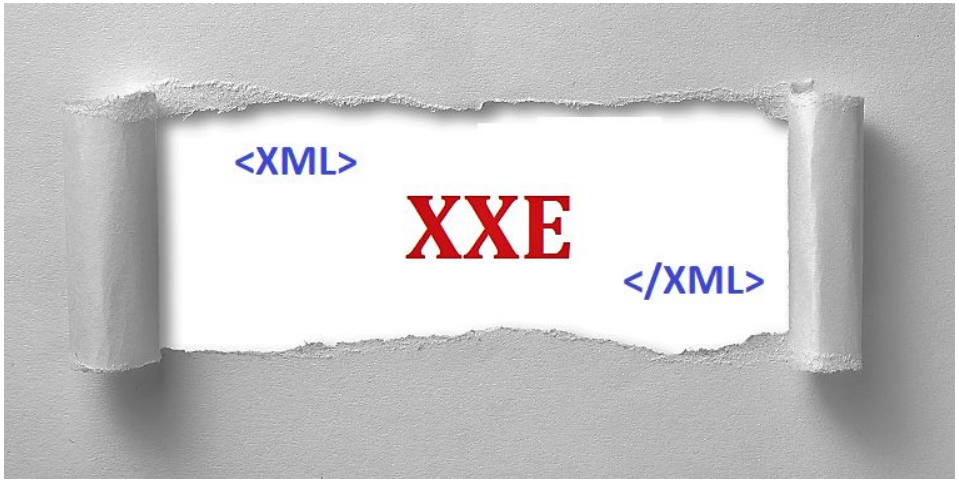
ENTIDADES XML ETERNAS



- O QUE É ISSO?
  - XML é um formato de dados usado para descrever diferentes elementos de dados.
  - XML também usa “Entidades” para ajudar a definir dados relacionados, mas as entidades podem acessar conteúdo, tão inofensivo quanto puxar o preço atual das ações de um site de terceiros.
  - As entidades podem, no entanto, ser usadas para solicitar dados ou arquivos locais, que podem ser devolvidos mesmo que esses dados nunca tenham sido destinados ao acesso externo.

ENTIDADES XML ETERNAS

- COMO FUNCIONA?
  - Um invasor envia valores de pesquisa de dados maliciosos solicitando ao site, ao dispositivo ou o aplicativo para solicitar e exibir dados de um arquivo local através de um entity XML. Se um desenvolvedor usa um nome de arquivo padrão em um local comum, o trabalho de um invasor é fácil.
- Por que é ruim?
  - Os invasores podem obter acesso a todos os dados armazenados localmente ou podem atacar outros sistemas internos.

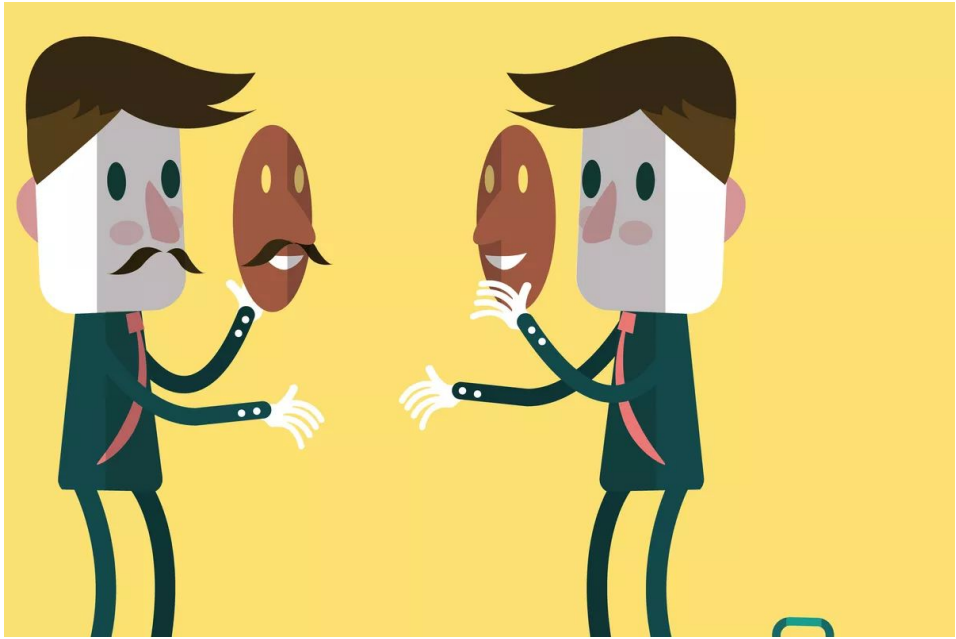


CONTROLE DE ACESSO QUEBRADO

- O QUE É ISSO?
  - Controle de acesso, ou autorização, é como os aplicativos da web permitem que diferentes usuários acessem conteúdo, dados ou funções diferentes.
  - É como o Netflix limita as pessoas em seu plano "padrão" para conteúdo em HD, enquanto os usuários "premium" podem assistir a 4K.
  - Quando está quebrado, você pode acessar mais do que deveria.

CONTROLE DE ACESSO QUEBRADO

- COMO FUNCIONA?
  - Às vezes, obter acesso não autorizado é tão simples quanto inserir manualmente uma URL desvinculada em um navegador, como http://example.com/admin.
- Por que é ruim?
  - Tal como acontece com outras vulnerabilidades, os invasores podem obter acesso a (e modificar) dados, contas e funções que não deveriam.



CONFIGURAÇÃO INCORRETA DE SEGURANÇA

- O QUE É ISSO?
  - Exatamente o que o nome indica, a configuração incorreta da segurança é quando você ignorou algumas vulnerabilidades.
  - Isso inclui o uso de credenciais padrão, deixando arquivos desprotegidos em servidores públicos, tendo conhecidos - mas sem correção falhas, e mais, e em qualquer camada da pilha de software.
  - Em outras palavras, é sua culpa.

CONFIGURAÇÃO INCORRETA DE SEGURANÇA

- COMO FUNCIONA?
  - As pessoas ficam ocupadas, as coisas passam despercebidas, as decisões de priorização são tomadas ...e vulnerabilidades são deixadas sem o correto tratamento..
- Por que é ruim?
  - Facilita que até mesmo invasores novatos encontrem e acessem seus valiosos sistemas e dados. Felizmente, a maioria desses tipos de vulnerabilidades também é fácil para você encontrar e consertar.

SCRIPTING CROSS-SITE (XSS)

- O QUE É ISSO?
  - O XSS permite que códigos mal-intencionados sejam adicionados a uma página da Web ou aplicativo, digamos, via comentários ou envios de formulários usados para definir a ação subsequente.
  - Como o HTML mistura instruções de controle, formatação e o conteúdo solicitado no código-fonte da página, ele permite que uma oportunidade de código inserido pelo atacante possa ser usado na página resultante.

SCRIPTING CROSS-SITE (XSS)

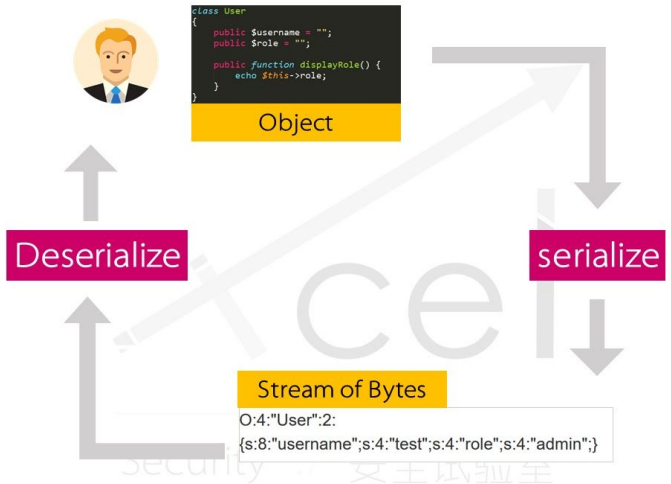
- COMO FUNCIONA?
  - Quando uma página ou aplicativo da Web utiliza conteúdo inserido pelo usuário como parte de uma página sem verificar as coisas ruins, um usuário mal-intencionado pode inserir conteúdo que muda o comportamento padrão da página
- Por que é ruim?
  - Os atacantes podem alterar o comportamento de um aplicativo, direcionar dados para seus próprios sistemas, ou corromper ou substituir dados existentes.

DESERIALIZAÇÃO INSEGURA

- O QUE É ISSO?
  - Antes dos dados serem armazenados ou transmitidos, os bits são muitas vezes serializados para pode ser restaurado posteriormente na estrutura original dos dados.
  - Remontando uma série de bits de volta em um arquivo ou objeto é chamado de desserialização.

DESERIALIZAÇÃO INSEGURA

- COMO FUNCIONA?
  - Os dados desserializados podem ser modificados para incluir códigos maliciosos, o que é suficiente para causar problemas se o aplicativo não verificar a origem ou o conteúdo dos dados antes da desserialização.
- Por que é ruim?
  - Os atacantes podem construir objetos ilegítimos que executam comandos dentro de um aplicação infectada



USANDO COMPONENTES COM VULNERABILIDADES CONHECIDAS

- O QUE É ISSO?
  - Quando as vulnerabilidades se tornam conhecidas, os fornecedores geralmente as consertam com um patch ou atualização. O processo de atualização do software elimina ou mitiga a vulnerabilidade.

USANDO COMPONENTES COM VULNERABILIDADES CONHECIDAS

- COMO FUNCIONA?
  - Às vezes, as organizações não conseguem manter o software atualizado, especialmente se pilhas de software são grandes ou complexas, ou se exigiria um compromisso significativo para validar seus sistemas ou produtos após uma atualização.
  - Quando um patch é lançado, os atacantes sabem que algumas organizações não irão agir imediatamente. Os atacantes agora têm uma janela, de dias a anos, para procurar sistemas ou aplicativos nos quais a vulnerabilidade conhecida ainda está em vigor.
- Por que é ruim?
  - Como são informações públicas, os invasores têm um caminho recomendado para explorar e as organizações têm pouca desculpa para deixar o caminho aberto.

REGISTRO E MONITORAMENTO INSUFICIENTES

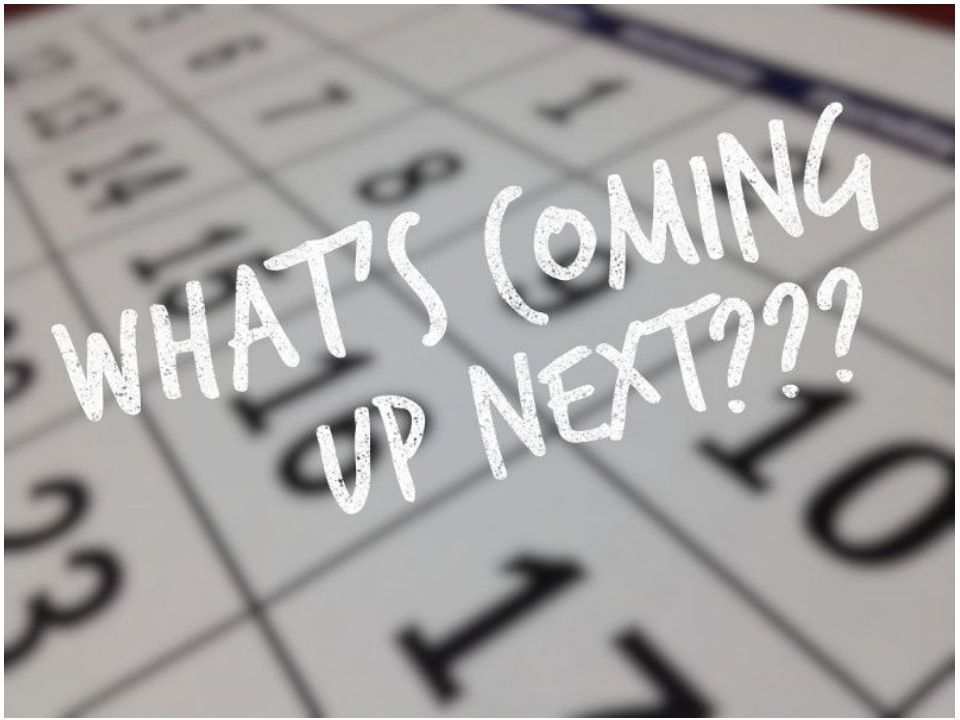
- O QUE É ISSO?
  - Se você não está procurando por invasores ou atividades suspeitas, você não vai encontrá-los.
- COMO FUNCIONA?
  - Software e sistemas têm habilidades de monitoramento para que as organizações possam ver logins, transações, tráfego e muito mais.
  - Ao monitorar atividades suspeitas, como logons com falha, as organizações podem ver e parar atividades suspeitas.

REGISTRO E MONITORAMENTO INSUFICIENTES

- Por que é ruim?
  - Os invasores confiam na falta de monitoramento para explorar vulnerabilidades antes de serem detectados.
  - Sem monitoramento e o registro para ver o que aconteceu, os atacantes podem causar danos agora e no futuro.

Próximas Aulas

- Prática:
  - Trabalho Individual IV
    - Envolve todo este conteúdo que vimos na aula de hoje e o que veremos nas próximas.



Perguntas?

jean.martina@ufsc.br