ATAQUES WEB - BÁSICO

JOAS ANTONIO

SOBRE O LIVRO

- ✓ Aprender o básico de ataques web
- ✓ Colocar em prática os principais ataques web conhecidos
- ✓ Entender como funciona os ataques voltados a web
- ✓ Livro extremamente prático sem teoria

INTRODUÇÃO

- Os ataques webs são recorrentes, estima-se que 60% dos sites possuem vulnerabilidades graves aguardando suas descobertas

- A necessidade de entender como funciona os ataques, aumentou no decorrer do tempo, assim precisando de profissionais capacitados para proteger ambientes contra as principais vulnerabilidades

LABORATÓRIO

- https://pentesterlab.com/
- https://www.offensive-security.com/metasploit-unleashed/requirements/
- https://www.100security.com.br/bwapp/

PRÁTICA BÁSICA

HTML INJECTION

HTML INJECTION

- A injeção de HTML é um tipo de problema de injeção que ocorre quando um usuário é capaz de controlar um ponto de entrada e é capaz de injetar código HTML arbitrário em uma página da Web vulnerável. Essa vulnerabilidade pode ter muitas consequências, como a divulgação de cookies de sessão de um usuário que podem ser usados para representar a vítima ou, de maneira mais geral, pode permitir que o invasor modifique o conteúdo da página visto pelas vítimas.

- Essa vulnerabilidade ocorre quando a entrada do usuário não é higienizada corretamente e a saída não é codificada. Uma injeção permite que o invasor envie uma página HTML maliciosa para uma vítima. O navegador de destino não será capaz de distinguir (confiar) o legítimo das partes maliciosas e, consequentemente, analisará e executará tudo como legítimo no contexto da vítima.

HTML INJECTION: PRÁTICA

- https://www.youtube.com/watch?v=TE6Pt8-dRLk
- https://www.hackingarticles.in/beginner-guide-html-injection/
- https://www.youtube.com/watch?v=bkB3NAgOoaw
- https://www.youtube.com/watch?v=q4SVMPGASIU
- https://pentestlab.blog/2013/06/26/html-injection/

XSS (CROSS SITE SCRIPTING)

XSS (CROSS SITE SCRIPTING)

- Os ataques de cross-site scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites de outra forma benignos e confiáveis. Os ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código malicioso, geralmente na forma de um script do lado do navegador, para um usuário final diferente. As falhas que permitem que esses ataques sejam bem-sucedidos são bastante difundidas e ocorrem em qualquer lugar em que um aplicativo Web use entrada de um usuário na saída gerada sem validá-lo ou codificá-lo.
- Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário inocente. O navegador do usuário final não tem como saber que o script não deve ser confiável e o executará. Como ele acha que o script veio de uma fonte confiável, o script mal-intencionado pode acessar todos os cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

XSS (CROSS SITE SCRIPTING): TIPOS

Ataques XSS armazenados

Ataques armazenados são aqueles em que o script injetado é permanentemente armazenado nos servidores de destino, como em um banco de dados, em um fórum de mensagens, log de visitantes, campo de comentários etc. A vítima recupera o script malicioso do servidor quando solicita o armazenamento. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo I.

Ataques XSS refletidos

Ataques refletidos são aqueles em que o script injetado é refletido no servidor da Web, como em uma mensagem de erro, resultado da pesquisa ou qualquer outra resposta que inclua parte ou toda a entrada enviada ao servidor como parte da solicitação. Ataques refletidos são entregues às vítimas por outra rota, como em uma mensagem de email ou em outro site. Quando um usuário é enganado a clicar em um link malicioso, enviar um formulário especialmente criado ou até mesmo navegar em um site malicioso, o código injetado viaja para o site vulnerável, o que reflete o ataque ao navegador do usuário. O navegador então executa o código porque veio de um servidor "confiável". O XSS refletido também é conhecido como XSS não persistente ou tipo II.

XSS (CROSS SITE SCRIPTING): TIPOS

Ataques XSS baseado em DOM

É um ataque XSS em que o payload (Carga útil) do ataque é executada como resultado da modificação do "ambiente" DOM no navegador da vítima usado pelo lado do cliente original script, para que o código do lado do cliente seja executado de maneira "inesperada". Ou seja, a própria página (a resposta HTTP) não é alterada, mas o código do lado do cliente contido na página é executado de maneira diferente devido às modificações maliciosas que ocorreram no ambiente DOM.

XSS (CROSS SITE SCRIPTING): PRÁTICA

- https://pentest-tools.com/website-vulnerability-scanning/xss-scanner-online
- https://pentest-tools.com/blog/xss-attacks-practical-scenarios/
- https://xss-game.appspot.com/
- https://www.youtube.com/watch?v=cl7__XZVodE
- https://www.youtube.com/watch?v=LCv1AiliGJw
- https://www.youtube.com/watch?v=6-WM7K1Q_bA
- https://medium.com/@charithra/introduction-to-xss-e9eb90b4323d
- https://medium.com/@jamischarles/xss-aka-html-injection-attack-explained-538f46475f6c
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

SQL INJECTION

SQL INJECITON

- Um ataque de injeção SQL consiste na inserção ou "injeção" de uma consulta SQL por meio dos dados de entrada do cliente para o aplicativo. Uma exploração bem-sucedida de injeção SQL pode ler dados confidenciais do banco de dados, modificar dados (Inserir / Atualizar / Excluir), executar operações de administração no banco de dados (como desligar o DBMS), recuperar o conteúdo de um determinado arquivo presente no arquivo DBMS sistema e, em alguns casos, emita comandos para o sistema operacional. Os ataques de injeção SQL são um tipo de ataque de injeção , no qual os comandos SQL são injetados na entrada do plano de dados para efetuar a execução de comandos SQL predefinidos.

SQL INJECITON: MODELAGEM

- Os ataques de injeção SQL permitem que os invasores falsifiquem a identidade, violem os dados existentes, causem problemas de repúdio, como anular transações ou alterar saldos, permitir a divulgação completa de todos os dados no sistema, destruir os dados ou torná-los indisponíveis e tornar-se administradores do servidor de banco de dados.
- A injeção de SQL é muito comum em aplicativos PHP e ASP devido à prevalência de interfaces funcionais mais antigas. Devido à natureza das interfaces programáticas disponíveis, os aplicativos J2EE e ASP.NET têm menos probabilidade de explorar facilmente as injeções de SQL.
- A gravidade dos ataques de injeção de SQL é limitada pela habilidade e imaginação do atacante e, em menor grau, pela defesa em contramedidas profundas, como conexões de baixo privilégio com o servidor de banco de dados e assim por diante. Em geral, considere a injeção de SQL uma severidade de alto impacto.

SQL INJECITON: PRÁTICA

- https://www.youtube.com/watch?v=gtBRZFSF9pM
- https://www.youtube.com/watch?v=q2EkWm9kfKE
- https://www.youtube.com/watch?v=98SrzDwXuUY
- https://www.youtube.com/watch?v=eqxgHcQztLc
- https://www.youtube.com/watch?v=HklySclKjtY
- https://www.youtube.com/watch?v=oMLsMl3a89I
- https://www.youtube.com/watch?v=nH4r6xv-qGg
- https://www.devmedia.com.br/sql-injection-em-ambientes-web/9733
- https://hackersec.com/invadir-sites-usando-sql-injection/
- https://www.youtube.com/watch?v=WFFQw01EYHM
- https://www.youtube.com/watch?v=ciNHn38EyRc&t=763s

FILE UPLOAD

FILE UPLOAD

- Os arquivos enviados representam um risco significativo para os aplicativos. O primeiro passo em muitos ataques é obter algum código no sistema a ser atacado. Então o ataque precisa apenas encontrar uma maneira de executar o código. O uso de um upload de arquivo ajuda o invasor a executar a primeira etapa.

- As consequências do upload irrestrito de arquivos podem variar, incluindo controle completo do sistema, um sistema de arquivos ou banco de dados sobrecarregado, encaminhamento de ataques para sistemas de back-end, ataques do lado do cliente ou desfiguração simples. Depende do que o aplicativo faz com o arquivo carregado e, principalmente, de onde está armazenado.

FILE UPLOAD

- Existem realmente duas classes de problemas aqui. O primeiro é com os metadados do arquivo, como o caminho e o nome do arquivo. Eles geralmente são fornecidos pelo transporte, como codificação HTTP com várias partes. Esses dados podem induzir o aplicativo a substituir um arquivo crítico ou a armazená-lo em um local incorreto. Você deve validar os metadados com muito cuidado antes de usá-los.

- A outra classe de problemas está no tamanho ou no conteúdo do arquivo. A variedade de problemas aqui depende inteiramente do uso do arquivo. Veja os exemplos abaixo para obter algumas idéias sobre como os arquivos podem ser mal utilizados. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com arquivos e pensar cuidadosamente sobre o processamento e os intérpretes envolvidos.

FILE UPLOAD: RISCOS

- O impacto dessa vulnerabilidade é alto, o suposto código pode ser executado no contexto do servidor ou no lado do cliente. A probabilidade de detecção para o invasor é alta. A prevalência é comum. Como resultado, a gravidade desse tipo de vulnerabilidade é alta.
- É importante verificar os controles de acesso de um módulo de upload de arquivo para examinar os riscos corretamente.
- Ataques do lado do servidor: o servidor da Web pode ser comprometido carregando e executando um shell da Web que pode executar comandos, procurar arquivos do sistema, procurar recursos locais, atacar outros servidores ou explorar as vulnerabilidades locais e assim por diante.

FILE UPLOAD: RISCOS

- Ataques do lado do cliente: o upload de arquivos maliciosos pode tornar o site vulnerável a ataques do lado do cliente, como XSS ou seqüestro de conteúdo entre sites.
- Os arquivos enviados podem ser abusados para explorar outras seções vulneráveis de um aplicativo quando um arquivo no mesmo servidor ou em um servidor confiável é necessário (pode novamente levar a ataques no lado do cliente ou no lado do servidor)
- Os arquivos enviados podem acionar vulnerabilidades em bibliotecas / aplicativos quebrados no lado do cliente (por exemplo, excesso de buffer do iPhone MobileSafari LibTIFF).

FILE UPLOAD: RISCOS

- Os arquivos enviados podem acionar vulnerabilidades em bibliotecas / aplicativos quebrados no lado do servidor (por exemplo, falha do ImageMagick que se chama ImageTragick!).
- Os arquivos enviados podem acionar vulnerabilidades em ferramentas de monitoramento em tempo real quebradas (por exemplo, exploração do antivírus da Symantec ao descompactar um arquivo RAR)
- Um arquivo malicioso, como um script de shell Unix, um vírus do Windows, um arquivo do Excel com uma fórmula perigosa ou um shell reverso pode ser carregado no servidor para executar o código posteriormente por um administrador ou webmaster - na máquina da vítima.

FILE UPLOAD: RISCOS

- Um invasor pode colocar uma página de phishing no site ou desfigurá-lo.
- O servidor de armazenamento de arquivos pode ser abusado para hospedar arquivos problemáticos, incluindo malwares, software ilegal ou conteúdo adulto. Os arquivos enviados também podem conter dados de comando e controle de malwares, mensagens de violência e assédio ou dados esteganográficos que podem ser usados por organizações criminosas.
- Os arquivos confidenciais enviados podem estar acessíveis por pessoas não autorizadas.
- Os usuários que enviam arquivos podem divulgar informações internas, como caminhos internos do servidor, em suas mensagens de erro.

FILE UPLOAD: PRÁTICA

- https://www.youtube.com/watch?v=hUh1kaouyjo
- https://www.youtube.com/watch?v=gOR4Wv9dZ10
- https://www.youtube.com/watch?v=_BhaoQqpq2E
- https://www.youtube.com/watch?v=_QyGCev6fCk
- https://www.youtube.com/watch?v=jFRYPmCulh4
- https://www.youtube.com/watch?v=4lFCQGkcD7M
- https://www.youtube.com/watch?v=9TN7harvpkI

PATH TRAVERSAL

PATH TRAVERSAL

- Um ataque de travessia de caminho (também conhecido como travessia de diretório) visa acessar arquivos e diretórios armazenados fora da pasta raiz da web. Manipulando variáveis que referenciam arquivos com sequências “ponto-ponto-barra (../)” e suas variações ou usando caminhos de arquivo absolutos, pode ser possível acessar arquivos e diretórios arbitrários armazenados no sistema de arquivos, incluindo código-fonte ou configuração do aplicativo e arquivos críticos do sistema. Observe que o acesso aos arquivos é limitado pelo controle de acesso operacional do sistema (como no caso de arquivos bloqueados ou em uso no sistema operacional Microsoft Windows).
- Esse ataque também é conhecido como "barra de ponto", "passagem de diretório", "escalada de diretório" e "retorno".

PATH TRAVERSAL: PRÁTICA

- https://www.youtube.com/watch?v=DiP2MU_Ik_Q
- https://www.youtube.com/watch?v=L95M0F55Fp0
- https://www.youtube.com/watch?v=jJoijQ5pADE
- https://www.youtube.com/watch?v=aQlKNnxsxok
- https://www.youtube.com/watch?v=v7_jVpomTa4

CSRF

CSRF

- A falsificação de solicitação entre sites (CSRF) é um ataque que força um usuário final a executar ações indesejadas em um aplicativo Web no qual eles estão atualmente autenticados. Os ataques CSRF visam especificamente solicitações de alteração de estado, não roubo de dados, pois o invasor não tem como ver a resposta à solicitação forjada. Com uma pequena ajuda da engenharia social (como o envio de um link por email ou bate-papo), um invasor pode induzir os usuários de um aplicativo da Web a executar ações de sua escolha. Se a vítima for um usuário normal, um ataque CSRF bem-sucedido pode forçar o usuário a executar solicitações de alteração de estado, como transferência de fundos, alteração de endereço de email e assim por diante. Se a vítima for uma conta administrativa, o CSRF poderá comprometer todo o aplicativo da web.

CSRF

- O CSRF é um ataque que induz a vítima a enviar uma solicitação maliciosa. Ele herda a identidade e os privilégios da vítima para desempenhar uma função indesejada em nome da vítima. Para a maioria dos sites, as solicitações do navegador incluem automaticamente quaisquer credenciais associadas ao site, como o cookie da sessão do usuário, o endereço IP, as credenciais do domínio do Windows e assim por diante. Portanto, se o usuário estiver atualmente autenticado no site, o site não terá como distinguir entre a solicitação forjada enviada pela vítima e uma solicitação legítima enviada pela vítima.
- O CSRF ataca a funcionalidade de destino que causa uma alteração de estado no servidor, como alterar o endereço de e-mail ou a senha da vítima ou comprar algo. Forçar a vítima a recuperar dados não beneficia um invasor porque o atacante não recebe a resposta, a vítima recebe. Como tal, os ataques CSRF visam solicitações de alteração de estado.

CSRF: PRÁTICA

- https://www.youtube.com/watch?v=5joX1skQtVE
- https://www.youtube.com/watch?v=Cd8ZKH41jko
- https://www.youtube.com/watch?v=gWMoj9FYTj4
- https://www.youtube.com/watch?v=XRW_US5BCxk
- https://www.youtube.com/watch?v=medqWM5lDgo
- https://www.youtube.com/watch?v=zXPHlDmSkwc

COMMAND INJECTION

COMMAND INJECTION

- Injeção de comando é um ataque no qual o objetivo é a execução de comandos arbitrários no sistema operacional host por meio de um aplicativo vulnerável. Os ataques de injeção de comando são possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, cookies, cabeçalhos HTTP etc.) para um shell do sistema. Nesse ataque, os comandos do sistema operacional fornecidos pelo invasor geralmente são executados com os privilégios do aplicativo vulnerável. Os ataques de injeção de comando são possíveis em grande parte devido à validação de entrada insuficiente.

COMMAND INJECTION: PRÁTICA

- https://chris-young.net/2018/03/28/dvwa-command-injection/
- https://www.youtube.com/watch?v=NxSNTT627TQ
- https://www.youtube.com/watch?v=AoMtDmYVGmQ
- https://www.youtube.com/watch?v=5Tt3aSeusXU
- https://www.youtube.com/watch?v=tQ4GTXlUioc
- https://www.youtube.com/watch?v=XO_BLYvftQU
- https://www.youtube.com/watch?v=H1auWPjioeU
- https://www.youtube.com/watch?v=5-1QLbVa8YE
- https://www.owasp.org/index.php/Command_Injection

CONCLUSÃO

COMMAND INJECTION

- Esse é o básico de ataques web, saber esses ataques vai levantar o leque para aprender outros milhares que existem
- Eu recomendo analisar a metodologias OWASP e pesquisar mais afundo as top 10 vulnerabilidades web

- Além disso, estudar linguagens de programação voltada a web é essencial para compreender facilmente o funcionamento de vulnerabilidades
- Nada se resume a receita de bolo, poderia colocar um simples tutorial aqui, mas não iria adiantar, esses são os princípios básicos de ataques web
- Recomendo se aprofundar mais nesses ataques e analisar códigos fontes de sites que possuem cada uma dessas vulnerabilidades
- Assista palestras que vai ajudar mais ainda na compreensão.