Sessão 2: Reconhecimento e Mapeamento

1. Atividade - Ferramentas básicas

Nesta atividade, o aluno se familiarizará com as ferramentas básicas que são utilizadas nas diversas etapas de um teste de invasão. Para iniciá-la, carregue as máquinas virtuais do aluno e do servidor (Fedora) e execute os roteiros na primeira delas.

> **Imporante:**
>
> Os passos do Roteiro 1 tem como objetivo verificar se as ferramentas estão configuradas corretamente. Na prática você pode ir para a próxima atividade.
>
> Para este treinamento não existe a necessidade de atualizar o Burp Suite portanto ignore este pedido.

Proxies de interceptação

Para utilizar proxies de interceptação, é necessário configurar a ferramenta para escutar a porta desejada e o navegador para direcionar todo tráfego para ela. Os roteiros abaixo ilustram como isso pode ser realizado nos proxies Burp Suite, Paros e WebScarab e nos navegadores Firefox, Opera e Chrome.

Configuração de porta no Burp Suite

1. Inicie o Burp Suite, presente no menu `03 - Web Application Analysiss` e crie um projeto `Temporary project` com opção `Use Burp defaults` selecionada (para isso clique no botão Next duas vezes).
2. Clique na aba Proxy e, em seguida, na aba-filha `Options`.
3. Selecione a primeira linha da tabela e clique no botão `Edit`.
4. Verifique se a porta 8080 no campo `Bind to port` e mantenha `Bind do address: loopback only` habilitado.
5. Para finalizar, clique em `OK`.

Configuração de porta no Paros

1. Inicie o Paros, presente no menu `03 - Web Application Analysis`.
2. Clique no menu Tools e no sub-menu `Options...`.
3. Selecione na parte esquerda da janela, a opção Local proxy.
4. Verifique a porta no campo `Port (eg 8080)`. Para este curso, informe a porta `9000` (caso não seja).
5. Para finalizar, clique em OK.

Configuração de porta no WebScarab

1. Inicie o WebScarab, presente no menu `03 - Web Application Analysis`.
2. Clique na aba Proxy e, em seguida, na aba-filha `Listeners`.
3. Selecione a primeira linha da tabela e clique no botão Stop.
4. Digite a porta desejada no campo Port (neste caso mantenha `8008`), abaixo da tabela.
5. Para finalizar, clique em Start.

Configuração do Firefox

Configuração do Multiproxy SwitchOmega

O Multiproxy SwitchOmega é um complemento para Firefox, que permite selecionar um proxy a partir de uma lista pré-cadastrada, simplificando muito o trabalho de configuração.

O roteiro abaixo mostra como incluir o proxy Paros na lista de proxies cadastrados no Multiproxy SwitchOmega.

1. Inicie o Firefox, presente no menu `Usual applications\Internet`.
2. Clique no ícone `Multiproxy SwitchOmega` ao lado da barra de URL, e observe que já existem alguns itens cadastrados.
3. Selecione `Options`.
4. Clique em `New Profile`.
5. Preencha Profile name com `Paros` e clique no botão `Create`
6. Clique em `Show Advanced` e na linha http da tabela selecione `HTTP` na coluna `Protocol`, em Server informe `localhost` e em Port `9000`.
7. Clique em `Apply changes` e feche a aba do Firefox.

Testando o WebScarab

1. Inicie o Firefox, presente no menu `Usual applications\Internet`.
2. Inicie o proxy desejado. Para este exercício, utilize o `WebScarab`, presente no menu `03 - Web Application Analysis`.
3. No Firefox, clique no ícone `SwitchOmega` ao lado da barra de URL e selecione `WebScarab`.
4. No WebScarab, selecione a aba `Proxy` e a aba-filha `Manual Edit`.
5. Desmarque as opções `Intercept Requests` e `Intercept Responses`.
6. Clique na aba `Summary` e veja que não há nada nas tabelas.
7. Retorne ao Firefox e acesse http://exemplo.esr.rnp.br.
8. Volte ao WebScarab e veja que as tabelas na aba `Summary` foram preenchidas com as requisições efetuadas pelo acesso acima.
9. Encerre o WebScarab.

Testando o Burp Suite

1. Os passos seguintes são para testar o acesso via Burp Suite, mas sem interceptação de nenhuma das requisições.
2. No Burp Suite, selecione a aba `Proxy` e a aba-filha `Options`.
3. Role a tela até encontrar a seção `intercept client requests`.
4. Desabilite a opção `intercept if` da seção `intercept client requests`.
5. Desabilite a opção `intercept if` da seção `intercept server responses`.
6. Ainda na aba `Proxy`, clique na aba-filha `HTTP History` e veja que a tabela está vazia.
7. Retorne ao Firefox, clique no ícone SwitchOmega ao lado da barra de URL e selecione Burp Suite.
8. Acessa a URL http://bodgeit.esr.rnp.br:8080/bodgeit/
9. Volte ao Burp Suite e veja que a tabela na aba `HTTP History` foi preenchida com as requisições efetuadas pelo acesso acima.
10. Encerre o Burp Suite.

Testando o Paros

1. Os passos seguintes são para testar o acesso via Paros, mas sem interceptação de nenhuma das requisições.
2. No Paros, selecione a aba `Trap`.
3. Limpe os check-boxes `Trap request` e `Trap response`.
4. Clique na aba `History`, localizada na parte inferior da tela, e veja que não há itens listados ali.
5. Retorne ao Firefox, clique no ícone SwitchOmega ao lado da barra de URL e selecione Paros.
6. Acessa a URL http://dvwa.esr.rnp.br/login.php
7. Volte ao Paros e veja que a lista na aba History foi preenchida com as requisições efetuadas pelo acesso acima.
8. Encerre o Paros.

2. Atividade - Varredores de portas e serviços

O representante mais conhecido deste tipo de software é o Nmap, cuja interface gráfica oficial é o Zenmap. Siga o roteiro abaixo para um contato inicial com a ferramenta.

1. Abra uma janela de terminal.
2. Veja a documentação do Nmap:

```
~$ man nmap
```

3. Execute uma varredura local básica e analise o relatório apresentado:

```
~$ nmap localhost
```

4. Encerre o terminal.

Outras ferramentas

Há outras ferramentas que podem ser utilizadas em testes de invasão de aplicações web, das quais, nesta atividade, serão abordadas o Netcat, o OpenSSL e o Nikto.

Netcat

O roteiro abaixo emprega o Netcat para implementar um modelo cliente-servidor simples.

1. Abra uma janela de terminal.
2. Veja a documentação do Netcat:

```
~$ man netcat
```

3. Digite o comando abaixo para que o Netcat escute conexões na porta 7000:

```
~$ nc -l -p 7000 -vv
```

4. Abra outro terminal.
5. Conecte-se à primeira instância do Netcat, por meio do comando:

```
~$ nc localhost 7000
```

6. Digite alguns textos e veja que são refletidos no outro terminal.
7. Encerre o cliente pressionando `Control+D`.
8. Encerre uma das janelas de terminal.

Curl

Como se sabe, o Netcat não é capaz de tratar os protocolos SSL e TLS nativamente e, assim, o roteiro abaixo ilustra como o curl pode preencher esta lacuna.

1. Mude o foco para a janela de terminal da última atividade.
2. Conecte-se ao servidor w3s.esr.rnp.br, com o comando:

```
~$ curl -k https://w3s.esr.rnp.br -v
```

3. Role a janela para visualizar a saída do curl (procure no início para visualizar os dados do certificado digital).

Nikto

1. Mude o foco para a janela de terminal da última atividade.
2. Veja a documentação do Nikto:

```
~$ man nikto
```

3. Execute o nikto (não se preocupe agora com o resultado)

```
~$ nikto -h exemplo.esr.rnp.br
```

4. Encerre a janela de terminal.

3. Atividade – Reconhecimento

O objetivo desta atividade é exercitar os diversos passos que fazem parte da etapa de reconhecimento de um teste de invasão, cujo propósito é levantar o máximo possível de informações da aplicação alvo.

Levantamento de informações em fontes públicas

Muitas informações úteis para um teste de invasão podem ser obtidas em fontes públicas, como redes sociais, grupos de discussão e anúncios de emprego. Com o roteiro abaixo, que deve ser executado em uma janela de terminal, algumas das informações sobre a organização em que trabalha serão identificadas.

Considere as redes sociais de que participa. Identifique que informações sobre tecnologias utilizadas pela organização em que trabalha podem ser extraídas de seus perfis e das comunidades de que faz parte.

1. Consulte as informações de registro de domínio da sua organização e identifique informações relevantes para testes de invasão.

```
~$ whois <nome_de_domínio_da_empresa>
```

2. Identifique os servidores de nome e de e-mail da sua organização, com o seguinte comando:

```
~$ dig ANY <nome_de_domínio_da_empresa>
```

3. Tente executar uma transferência de zona DNS para o domínio da sua organização. Na remota possibilidade desta funcionalidade estar habilitada, uma vulnerabilidade acaba de ser encontrada e precisa ser corrigida.

```
~$ dig -t AXFR <nome_de_domínio_da_empresa>
```

Google hacking

Mecanismos de busca como o do Google permitem encontrar muitas informações sobre uma aplicação e, assim, são muito úteis em testes de invasão. Nesta prática, o aluno executará diversas consultas ao Google, para explorar as opções existentes. Para cada pesquisa, observe o total de itens encontrados, o tempo de execução e as páginas listadas.

1. Inicie o navegador de sua preferência e acesse `www.google.com`.
2. Para encontrar páginas em inglês sobre testes de invasão em aplicações web, submeta a seguinte pesquisa:

```
web application penetration testing
```

3. Altera a pesquisa para a seguinte e observe o que muda nos resultados:

```
web application OR penetration testing
```

4. Aplique a seguinte alteração para buscar páginas que possuam web application ou penetration testing:

```
'web application' OR 'penetration testing'
```

5. Execute a pesquisa abaixo para listar varredores de vulnerabilidades:

```
vulnerability scanners
```

6. Se não estiver interessado no Nessus, por exemplo, inclua `-nessus`:

```
vulnerability scanners -nessus
```

7. Veja o que o Google encontra sobre a sua empresa, digitando:

```
nome_da_empresa_em_que_trabalha
```

8. Para restringir a busca ao domínio da sua empresa, empregue o operador `site`:

```
site:<domínio_da_empresa>
```

9. Verifique se sua empresa possui algum sistema web voltado para internet com uma página de autenticação de usuário:

```
site:<domínio_da_empresa> login OR logon
```

10. Procure na internet sítios web com listagem de diretórios habilitada:

```
intitle:'Index of'
```

11. Para encontrar arquivos `.bak`, utilize a pesquisa:

```
intitle:'Index of' filetype:bak
```

12. Localize na internet relatórios gerados pelo Nessus:

```
'This file was generated by Nessus'
```

Identificação de sistema operacional, serviços e portas

Neste exercício, será realizada a identificação do sistema operacional, serviços e portas do servidor que hospeda `exemplo.esr.rnp.br`.

1. Inicie uma janela de terminal.
2. Execute o comando e analise o relatório gerado:

```
~$ nmap exemplo.esr.rnp.br
```

3. O comando acima apenas identificou as portas e serviços do servidor, mas não exibiu nada sobre o sistema operacional e plataformas que fornecem os serviços. Isso pode ser obtido com a opção `-A`:

```
~$ nmap -A exemplo.esr.rnp.br
```

Quantos e quais servidores web foram identificados?

4. Aparentemente, a opção `-A` fez apenas metade do trabalho esperado, pois não identificou o sistema operacional. O motivo disso é que, para essa funcionalidade ser executada corretamente, o programa deve ser executado por um usuário privilegiado. Assim, chame o Nmap via sudo e forneça a sua senha quando solicitada:

```
~$ sudo nmap -A exemplo.esr.rnp.br
```

5. O Nmap possui uma interface gráfica oficial, chamada de Zenmap. Inicie-a, a partir do menu 01 - Informatin Gathering. Caso queira executa-lo com permissão de root abra o terminal e execute (não esqueça de informar a senha esruser):

```
~$ sudo zenmap
```

6. Explore as opções disponíveis na interface gráfica.
7. Digite `exemplo.esr.rnp.br` no campo Target e observe como o campo `Command` é atualizado em tempo real.
8. Clique no botão `Scan` e aguarde até que a tarefa seja executada.
9. Analise o resultado, percorrendo as abas `Saída Nmap`, `Ports / Hosts`, `Topology`, `Detalhes da Máquina` e `Scans`.
10. Feche a janela do Zenmap, mas mantenha o terminal aberto para a próxima atividade.

Identificação do servidor web

Na atividade anterior, o Nmap já realizou um ótimo trabalho na identificação de servidores web. Apesar disso, é sempre bom conhecer métodos alternativos de se realizar a mesma tarefa. Assim, nesta atividade, serão estudadas técnicas adicionais para identificar o tipo de servidor web em uso.

1. Inicie o Firefox, presente no menu `Usual applications\Internet` e verifique se o SwitchProxy Omega esta configurado para não utilizar nenhum proxy.
2. Acesse `http://exemplo.esr.rnp.br/blabla` e veja se a mensagem de erro dá alguma pista sobre o servidor. É o mesmo que o identificado pelo Nmap? Esta técnica é robusta?

---

3. Repita o passo anterior para as seguintes URLs:

```
http://exemplo.esr.rnp.br:81/blabla
http://exemplo.esr.rnp.br:8080/blabla
http://exemplo.esr.rnp.br:8090/blabla
```

4. Outra técnica consiste na análise do cabeçalho Server, fornecido pelo servidor como parte das respostas. Para realizar este teste, abra uma nova janela de terminal e digite o texto abaixo, finalizando com [Enter] duas vezes:

```
~$ nc exemplo.esr.rnp.br 80
HEAD / HTTP/1.1
Host: exemplo.esr.rnp.br
```

   O valor do cabeçalho supracitado está de acordo com o tipo de servidor identificado pelo Nmap? Esta técnica é robusta?

---

5. Repita o Passo 4, substituindo a porta 80 por 81, 8080 e 8090.
6. Houve algum problema ao realizar o teste para a porta 81? Provavelmente sim, e o motivo é que o lighttpd, na versão 1.4, somente aceita linhas terminadas pelos caracteres CR e LF, enquanto que o sistema operacional Linux adota apenas o caractere LF. Para corrigir isto, utilize a opção `-C` do Netcat.
7. A última técnica envolve o uso do utilitário httprint. Para inicia-lo abra o terminal e execute:

```
~$ wine /usr/share/httprint_301/win32/httprint_gui.exe
```

8. Na tabela localizada abaixo do campo `Signature File`, insira uma linha para cada uma das portas no conjunto {80, 81, 8080, 8090}, com Host igual a `exemplo.esr.rnp.br` e com o check-box marcado. Para incluir uma nova linha, basta pressionar a tecla [Enter], quando o foco estiver em Host ou Port.
9. Clique no botão `Options`, desabilite a opção `ICMP Enable` e clique em `OK`.
10. Para iniciar a execução, clique no botão que contém uma seta verde.
11. Compare o resultado com o Nmap, por meio das colunas `Banner Deduced` e `Banner Reported`, e observe que não foi muito satisfatório. Esse resultado, contudo, pode ser melhorado por meio da adição de assinaturas de servidores web ao arquivo signatures.txt do httprint. A localização deste arquivo pode ser observada no campo `Signature File`, que, no exercício, aparece como um subdiretório do drive `Z`, porque o utilitário está sendo executado via Wine.
12. Selecione na tela do httprint a linha do servidor lighttpd e copie para a área de transferência (Control-C) a região abaixo da tabela, contendo nome do servidor e cinco linhas em hexadecimal.
13. Abra uma janela de terminal e digite o seguinte comando, fornecendo a senha quando solicitada:

```
~$ sudo gedit /usr/share/httprint_301/win32/signatures.txt
```

14. Logo após a linha `# $AUTOGENERATED: {version}`, cole o que copiou do httprint, deixando uma linha em branco antes da seção seguinte.
15. Salve o arquivo e execute novamente o httprint. O que acontece?

16. Feche as janelas do gedit, httprint e terminais.

Levantamento dos métodos suportados pelos servidores web

Neste roteiro, por meio do método `OPTIONS`, o aluno deve identificar os métodos suportados pelos quatro servidores web instalados na máquina virtual Fedora.

1. Abra uma janela de terminal e digite o texto abaixo. Não esqueça que para os comandos serem executados é necessário apertar o [Enter] duas vezes:

```
~$ nc exemplo.esr.rnp.br 80
OPTIONS / HTTP/1.1
Host: exemplo.esr.rnp.br
```

2. Repita o processo para as portas 81, 8080 e 8090, lembrando-se como proceder, no caso do lighttpd.
3. Feche a janela de terminal.

Detecção de hosts virtuais

Nesta atividade, serão exercitados métodos para a detecção dos hosts virtuais.

1. Inicie o navegador de sua preferência.
2. Acesse `http://dvwa.esr.rnp.br`.
3. Acesse `http://exemplo.esr.rnp.br`.
4. Abra uma janela de terminal.
5. Digite o comando abaixo e anote o endereço IP:

```
~$ ping -c 1 dvwa.esr.rnp.br
```

6. Digite o comando abaixo e anote o endereço IP:

```
~$ ping -c 1 exemplo.esr.rnp.br
```

7. Quando os dois endereços IP são iguais e os dois sítios são acessados pela mesma porta, significa que são hospedados virtualmente pelo mesmo servidor, que os discerne pelo nome de domínio. A desvantagem deste método, porém, é que nem sempre haverá dois nomes de domínio diferentes à disposição, para realizar o teste descrito.
8. Uma técnica diferente, que depende de sorte para funcionar, consiste em acessar o sítio web por meio do endereço IP. Assim, considere que a aplicação alvo seja `dvwa.esr.rnp.br` e a acesse em um navegador web utilizando o endereço IP descoberto no Passo 5. Observe que a página exibida pertence ao domínio `exemplo.esr.rnp.br`, o

que implica que a hospedagem virtual por nomes é utilizada. O fator azar está relacionado à chance do sítio web alvo ser exatamente o host padrão do servidor web.

Neste caso, o teste não é conclusivo.

9. Repita o exercício anterior para os servidores web que escutam nas portas 81, 8080 e 8090 da mesma máquina. Primeiro, observe a página obtida pelo acesso com a URL `http://exemplo.esr.rnp.br:<porta>;` e, em seguida, por meio de endereço IP, com a URL `http://192.168.213.200:<porta>;`. Quais estão utilizando hospedagem virtual?

---

10. A última técnica envolve o uso de uma ferramenta web para mapear endereços IP para nomes de domínio. Inicie acessando uma janela de terminal.
11. Digite o comando abaixo para descobrir o endereço IP do servidor web da sua empresa:

```
~$ dig <URL_do_sítio_web_da_sua_empresa>
```

12. Acesse `https://www.ultratools.com/tools/ipWhoisLookup` em um navegador, digite o endereço IP encontrado no passo anterior e clique em `Go`.
13. Se domínios de empresas diferentes forem listados, o sítio web de sua empresa está armazenado em um servidor com hospedagem virtual habilitada.
14. Feche o navegador e a janela de terminal.

Descoberta de arquivos e diretórios

Para finalizar as atividades sobre reconhecimento, o aluno executará a ferramenta Nikto para descoberta de arquivos e diretórios instalados por padrão nos servidores web.

1. Inicie uma janela de terminal.
2. Digite o comando abaixo e observe o relatório gerado:

```
~$ nikto -C all -host exemplo.esr.rnp.br -port 80
```

3. Anote todos os recursos encontrados para uso na fase de mapeamento.
4. Repita o exercício acima, trocando a porta 80 por 81, 8080 e 8090.
5. Encerre a janela de terminal.

4. Atividade – Mapeamento

Nesta atividade, o aluno realizará o mapeamento de uma aplicação web, contida na máquina virtual Fedora. A ferramenta básica que será utilizada é o web spider, para cópia local das páginas e recursos que compõem a aplicação.

Nesta atividade, o aluno poderá comparar os web spiders que fazem parte das suítes integradas de teste Burp Suite, WebScarab e Paros.

Uso do spider do Paros

1. Inicie o Firefox, presente no menu `Usual applications\Internet`, e acesse a URL `about:preferences`.

2. Vamos limpar o histórico do navegador. Para isso clique em `Privacy & Security` e na janela que aparece, clique em `Clear History`, em `Time range to clear` selecione `Everything` e marque todos os itens da caixa `Details` e clique em `Clear Now`. Após, clique em `Clear Data`, `Clear` e `Clear Now` e por fim feche a aba `about:preferences#privacy`
3. Inicie o Paros, presente no menu `03 - Web Application Analysis`.
4. Encerre e execute novamente o Firefox. Agora clique no Multiproxy SwitchOmega, na barra de estado, e selecione o Paros.
5. Clique no marcador Mutillidae (http://mutillidae.esr.rnp.br), para acessar a aplicação.
6. Percorra os links `Register`, `Login`, `Logout`, `Show log`, `Credits`, `User info`, `DNS Lookup`, `Add to your blog`, `View someone's blog`, `Browser info`, `Text file viewer` e `Source viewer` e submeta quaisquer formulários que forem apresentados.
7. No Paros, percorra e analise o mapa criado na aba Sites.
8. Clique em `Tools`, seguido de `Options...`.
9. Selecione Spider na parte esquerda da janela.
10. Inclua a URL `http://mutillidae.esr.rnp.br/setupreset.php` em `URLs to be skipped and not read`.
11. Desmarque `POST forms`.
12. Clique em `OK`.
13. Selecione `http://mutillidae.esr.rnp.br` na aba Sites e clique com o botão direito.
14. Selecione Spider e clique em `Start`. O processo demorará alguns minutos.
15. Analise novamente o mapa criado na aba Sites.
16. Selecione a aba Spider, na parte inferior da tela.
17. Observe que as URLs encontradas no processo de cópia são listadas no quadro inferior da tela.
18. Não encerre o Paros.

Uso do spider do WebScarab

1. Inicie o Firefox, presente no menu `Usual applications\Internet`, e acesse a URL `about:preferences`.
2. Vamos limpar o histórico do navegador. Para isso clique em `Privacy & Security` e na janela que aparece, clique em `Clear History`, em `Time range to clear` selecione `Everything` e marque todos os itens da caixa `Details` e clique em `Clear Now`. Após, clique em `Clear Data`, `Clear` e `Clear Now` e por fim feche a aba `about:preferences#privacy`
3. Inicie o WebScarab, presente no menu `03 - Web Application Analysis`.
4. Encerre e execute novamente o Firefox. Clique no Multiproxy SwitchOmega, na barra de estado, e selecione o WebScarab.
5. Clique no marcador Mutillidae, para acessar a aplicação.
6. Percorra os links `Register`, `Login`, `Logout`, `Show log`, `Credits`, `User info`, `DNS Lookup`, `Add to your blog`, `View someone's blog`, `Browser info`, `Text file viewer` e `Source viewer` e submeta quaisquer formulários que forem apresentados.
7. No WebScarab, selecione a aba `Summary`.
8. Analise o mapa da aplicação, organizado em árvore, e as requisições na tabela localizada abaixo deste. Observe as colunas existentes nas duas partes.

9. Selecione a aba Spider.
10. Preencha o campo `Allowed Domains` com `.esr\.rnp\.br.`.
11. Marque `Synchronise cookies` e `Fetch Recursively`.
12. Expanda a árvore referente à aplicação Mutillidae e selecione a URL.
13. Clique em `Fetch Tree`. Infelizmente, o WebScarab não possui uma barra de progressão da tarefa e, assim, a única maneira de saber que o processo terminou é quando nenhum item for adicionado ou removido da tela.
14. Retorne à aba `Summary` e analise novamente o mapa da aplicação.
15. Observe na tabela de requisições que algumas linhas com `Origin` igual a Spider foram incluídas pelo Passo 14.
16. Não encerre o WebScarab.

Uso do spider do Burp Suite

1. Inicie o Firefox, presente no menu `Usual applications\Internet`, e acesse a URL `about:preferences`.
2. Vamos limpar o histórico do navegador. Para isso clique em `Privacy & Security` e na janela que aparece, clique em `Clear History`, em `Time range to clear` selecione `Everything` e marque todos os itens da caixa `Details` e clique em `Clear Now`. Após, clique em `Clear Data`, `Clear` e `Clear Now` e por fim feche a aba `about:preferences#privacy`
3. Inicie o BurpSuite, presente no menu `03 - Web Application Analysis`.
4. No BurpSuite clique na aba Proxy e Intercept e desmarque o botão intercept is on.
5. Encerre e execute novamente o Firefox. Clique no Multiproxy SwitchOmega, na barra de estado, e selecione o Burp Suite.
6. Clique no marcador Mutillidae, para acessar a aplicação.
7. Percorra os links `Register`, `Login`, `Logout`, `Show log`, `Credits`, `User info`, `DNS Lookup`, `Add to your blog`, `View someone's blog`, `Browser info`, `Text file viewer` e `Source viewer` e submeta quaisquer formulários que forem apresentados.
8. No Burp Suite, selecione a aba `Target` e a aba-filha `Site map`.
9. Analise o mapa da aplicação na parte esquerda da tela, a lista de requisições e os detalhes destas e das respostas.
10. No mapa da aplicação, clique com o botão direito sobre o item referente ao Mutillidae e selecione `Add to scope`. Responda `Yes` na mensagem que aparece (se aparecer).
11. Clique novamente com o botão direito sobre o item referente ao Mutillidae, selecione `Spider this host` e clique no botão `Yes`, na mensagem que aparece (se aparecer).
12. Neste processo, algumas janelas para submissão de formulários aparecerão. Preencha os campos com qualquer informação e clique em `Submit form`, sempre que isso acontecer.
13. Observe que novos elementos foram adicionados ao mapa da aplicação, ao fim do processo.
14. Procure pelo arquivo config.inc e selecione-o. Na janela inferior esquerda clique no botão `Response` para observar o seu conteúdo. Que conteúdo interessante ele revela?

Agora, procure pelo arquivo passwords/accounts.txt, selecione-o. Na janela inferior esquerda clique no botão `Response` para observar o seu conteúdo. Qual a utilidade das informações encontradas?

---

15. Não encerre o Burp Suite.

Identificação dos pontos de entrada de informação

A partir das páginas e recursos copiados no primeiro passo do mapeamento, é necessário identificar pontos de entrada de informação, que serão empregados para testar a presença de uma série de vulnerabilidades. As anotações podem ser feitas em uma planilha, listando método, URL, parâmetros, cabeçalhos e quaisquer outras informações que possam ser úteis para o teste de invasão.

No Paros

1. Retorne à janela do Paros.
2. Selecione a aba `Request`.
3. Selecione a aba inferior `History`.
4. Percorra os itens do histórico, um a um, analisando a requisição que foi realizada e identificando parâmetros passados em requisições `GET e POST`.
5. Repita o processo para o mapa da aplicação.
6. Selecione a aba Response.
7. Percorra os itens do histórico, um a um, analisando a resposta fornecida e observando cabeçalhos não padronizados e definições de cookies.
8. Repita o processo para o mapa da aplicação.
9. Feche a janela do Paros.

No WebScarab

1. Retorne à janela do WebScarab.
2. Selecione a aba `Summary`.
3. Percorra os itens do mapa da aplicação, um a um, analisando as colunas marcadas e a dica que fornecem.
4. Analise os itens contidos na tabela de requisições e observe os parâmetros passados em requisições `GET e POST`.
5. Role a tabela até o item com menor `ID`.
6. Dê um duplo clique sobre ele e veja que uma tela com detalhes da requisição e da resposta aparece.
7. Esta janela é dividida em quatro seções separadas por uma barra fina, contendo setas no lado esquerdo. Clique nas setas que apontam para baixo na primeira e terceira barras. Isto ocultará o corpo das mensagens.
8. Na seção de requisição, clique na aba `Raw`.
9. Percorra os diversos itens, clicando no botão `Next`, e, durante esta tarefa, observe os parâmetros passados em requisições `GET e POST`, cabeçalhos não padronizados e pontos em que cookies são definidos.
10. Feche a janela do WebScarab.

No Burp Suite

1. Retorne à janela do Burp Suite.
2. Selecione a aba `Target` e a aba-filha `Site map`.
3. Clique na barra `Filter` e marque o campo `Show only in-scope items`.
4. Clique novamente na barra para recolher a janela.
5. Selecione a aba `Request`, abaixo da tabela de requisições, e a aba-filha `Raw`.

6. Percorra os itens do mapa da aplicação, um a um, analisando a requisição que foi realizada e identificando parâmetros passados em requisições `GET` e `POST`.
7. Selecione a aba Response, abaixo da tabela de requisições, e a aba-filha `Raw`.
8. Percorra os itens do mapa da aplicação, um a um, analisando a resposta gerada pelo servidor e identificando cabeçalhos não padronizados e pontos em que são definidos cookies.
9. Clique com o botão direito na raiz do mapa da aplicação e selecione `Copy links in this host`.
10. Abra o gedit, localizado no menu `Aplicativos\Acessórios`, e pressione `Ctrl+V`, para colar os links existentes nas páginas da aplicação. Veja se encontra alguma coisa interessante.
11. Feche a janela do Burp Suite.

5. Atividade – Descoberta e exploração de vulnerabilidades

O propósito da presente atividade é introduzir ao aluno o processo de descoberta e exploração de vulnerabilidades. Será abordada a exploração de controles no lado cliente, que, muitas vezes, constitui o único ponto de validação das informações fornecidas pelos usuários. Como se sabe, tal prática é censurável, pois, normalmente, é uma tarefa trivial quebrar este tipo de mecanismo. Nos exercícios que se seguem, recomenda-se que o aluno tente traçar a estratégia de exploração, antes de seguir o roteiro fornecido.

Acesso ao WebGoat

Os exercícios desta atividade serão executados no OWASP WebGoat, uma aplicação contendo vulnerabilidades propositais, para o estudo de segurança em aplicações web.

1. Inicie o Firefox, presente no menu `Usual applications\Internet`.
2. Inicie o WebScarab, presente no menu `03 - Web Application Analysis`.
3. Selecione a aba-filha `Manual Edit`, sob a aba `Proxy`, e desmarque a opção `Intercept requests`.
4. No Firefox, clique no Multiproxy Switch, na barra de estado, e selecione o WebScarab.
5. Clique no marcador WebGoat e forneça `guest e guest`, quando usuário e senha forem solicitados.
6. Clique em Start WebGoat.

Evasão de restrições em campos HTML

Neste exercício, um formulário contendo diversos campos com restrições é apresentado pela aplicação e o aluno deve violar todas as regras definidas. Para facilitar na solução, pense qual elemento é responsável por honrar as restrições dos campos.

1. Selecione a aba `Summary` no WebScarab e identifique o `ID` da última requisição.
2. No WebGoat, clique no menu `Parameter Tampering` e no sub-menu `Bypass HTML Field Restrictions`. No formulário clique em Clique em `Restart this lesson`.
3. Verifique as restrições definidas para cada campo do formulário.
4. Submeta o formulário, clicando em `Submit`.
5. Retorne ao WebScarab, dê um duplo clique na primeira requisição `POST` posterior à identificada no passo 1 e observe os parâmetros passados via `POST`. Repare que o campo desabilitado não é submetido ao servidor.
6. Feche a janela.
7. Volte ao Firefox e pressione Ctrl+U para visualizar o código-fonte.
8. Pressione Ctrl+F e digite `Disabled input field:`, para encontrar o campo desabilitado.

9. Anote o nome do campo, definido no elemento <input>, e feche a janela de visualização de código-fonte.
10. Retorne ao Webscarab e clique na aba `Proxy` e na aba-filha `Manual Edit`.
11. Marque a opção `Intercept requests` e desmarque as demais.
12. Retorne ao Firefox e clique no botão `Submit` novamente. Uma janela do Webscarab aparece, contendo a requisição que será efetuada. Para alterar o valor de um parâmetro, basta dar um duplo clique na coluna Value, na linha correspondente, e digitar a nova informação.
13. Clique em `Insert`.
14. Substitua o nome `Variable` pelo identificado no Passo 11 (neste caso `disabledinput`).
15. Altere os seis parâmetros para o valor `blabla`.
16. Clique em `Accept changes`.
17. O exercício é finalizado com sucesso e a mensagem `* Congratulations. You have successfully completed this lesson.` é exibida.

Evasão de validação Javascript

O objetivo deste exercício é ilustrar como a validação de informações, por meio de Javascript, pode ser facilmente quebrada, quando ela não é ratificada pelo servidor.

1. No WebScarab, selecione a aba Proxy e a aba-filha `Manual Edit`.
2. Desmarque todas as opções.
3. Retorne ao WebGoat e clique no menu `Parameter Tampering` e no sub-menu `Bypass Client Side JavaScript Validation`.
4. Leia as regras definidas para cada campo, altere-os para valores inválidos e submeta o formulário, clicando em `Submit`.
5. Veja que a validação local identifica problemas nos campos e impede que a requisição seja realizada. Feche a janela de mensagem.
6. Clique em `Restart this lesson`.
7. Retorne ao WebScarab e clique em `Intercept requests`.
8. Volte ao Firefox e submeta o formulário novamente. Uma janela aparece, contendo a requisição que será efetuada.
9. Insira o caractere `!` ao final dos valores dos parâmetros.
10. Clique em `Accept changes`.
11. O exercício é finalizado com sucesso e a mensagem `* Congratulations. You have successfully completed this lesson.` é exibida.

Exploração de campo escondido

Esta atividade simula uma aplicação para suporte a cliente, que permite enviar uma mensagem ao administrador, por meio do formulário fornecido. O objetivo é enviar mensagens a pessoas arbitrárias, mesmo sem a existência de tal opção.

1. No WebScarab, selecione a aba `Proxy` e a aba-filha `Manual Edit`.
2. Desmarque todas as opções.
3. Retorne ao WebGoat e clique no menu `Parameter Tampering` e no sub-menu `Exploit Unchecked Email`. Na página clique no link `Restart this Lesson`

4. Role a página até o final do formulário, preencha-o e clique em `Send!`.
5. Veja no final da página apresentada o formato da mensagem submetida.
6. Retorne ao WebScarab e clique em `Intercept requests`.
7. Volte ao Firefox e submeta uma nova mensagem pelo sistema. Uma janela aparece, contendo a requisição que será efetuada.
8. Observe a existência do parâmetro `to`. Este é um campo escondido do formulário, que teria sido encontrado na fase de mapeamento da aplicação. Isto é um exemplo da importância de não se pular etapas.
9. Altere o valor do parâmetro `to` para `friend@owasp.org`.
10. Clique em `Accept changes`.
11. Role até o final da página e verifique que a mensagem foi enviada ao e-mail `friend@owasp.org`, em vez de `webgoat.admin@owasp.org`. A página de sucesso não aparece, porque este roteiro é apenas parte do esperado.
12. No OmegaSwtich altere o Proxy para `Directy` e encerre o WebScarab

ENTREGA DA TAREFA

Para que seja considerada entregue você deve anexar a esta atividade no AVA arquivo em formato PDF ou DOC contendo a resposta de todas as perguntas realizadas ao longo desta atividades.

Última atualização 2022-05-16 15:22:34 -0300