Sessão 8: Teste do Mecanismo de autorização e da lógica de negócio

1. Atividade – Acesso direto a recursos

Esta atividade tem por objetivo ilustrar as diversas técnicas que podem ser usadas para acesso direto a recursos. Para iniciá-la, carregue as máquinas virtuais do aluno e do servidor (Fedora) e execute o roteiro na primeira delas.

Acesso direto a páginas

O objetivo deste exercício é estudar ataques de acesso direto a páginas do sistema, contornando o mecanismo de autorização.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse http://bssac.esr.rnp.br/.
3. Digite `guest` e `guest` nos campos Usuário e Senha, respectivamente, e clique em `Login`.
4. Anote a URL do link para a caixa de mensagens e, em seguida, clique nele.
5. Clique em `Encerrar sessão`.
6. Digite `esruser` e `esruser` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
7. Anote as URLs dos links exibidos.
8. Clique em `Caixa de mensagens`.
9. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
10. Clique em `Visualizar arquivos`.
11. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
12. Clique em `Operação não privilegiada`.
13. Clique em `Encerrar sessão`.
14. Digite `admin` e `admin` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
15. Anote as URLs dos links exibidos.
16. Clique em `Caixa de mensagens`.
17. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
18. Clique em `Função Administrativa #1`.
19. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
20. Clique em `Visualizar arquivos`.
21. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
22. Clique em `Função Administrativa #2`.
23. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
24. Clique em `Operação não privilegiada`.
25. Clique em `Encerrar sessão`.
26. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://bssac.esr.rnp.br/oper2.php
```

27. O acesso foi permitido? Clique em `Retornar à página de login`.

Resposta: não pois o usuário não está autenticado

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

```
http://bssac.esr.rnp.br/oper5.php
```

29. O acesso foi permitido? Clique em `Retornar à página de login`.

Resposta: não pois o usuário não está autenticado

30. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
31. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://bssac.esr.rnp.br/oper2.php
```

32. O que acontece?

Resposta: apareceu a mensagem `Se você chegou até aqui, só pode ser administrador!!`

33. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
34. Digite a seguinte URL na barra de endereços e clique no botão verde:

```
http://bssac.esr.rnp.br/oper5.php
```

35. O que acontece?

Resposta: apareceu a mensagem `Esta funcionalidade está disponível a usuários não privilegiados!!!`

36. Clique em Encerrar sessão.

Uso do cabeçalho HTTP Referer

Neste exercício, ficará claro por que o uso do cabeçalho HTTP Referer não serve para controlar o acesso a páginas da aplicação.

1. Acesse http://bssac.esr.rnp.br/admin/.
2. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
3. Clique em `Retornar à página de login`.
4. Abra o WebScarab e na aba `Proxy` marque a opção `Intercept requests`. Após, retorne ao Firefox e no plugin Multiproxy selecione WebScarab.
5. Digite `admin` e `admin` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
6. Na página `Edit Request` do WebScarab clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
7. Retorne ao Firefox e clique em `Caixa de mensagens`.

8. Na página `Edit Request` do WebScarab clique na aba `Raw` e anote o valor do atributo `Referer`. Após, clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
9. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior. Clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
10. Clique em `Função Administrativa #1`.
11. Na página `Edit Request` do WebScarab clique na aba `Raw` e anote o valor do atributo `Referer`. Após, clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
12. Retorne ao Firefox e clique em `Encerrar sessão`. Clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
13. Digite a seguinte URL na barra de endereços e clique no botão verde (clique no botão `Accept changes` até que a requisição seja enviada ao servidor):

    ```
    http://bssac.esr.rnp.br/admin/oper2.php
    ```

14. O que acontece?

    

    Resposta: exibiu a mensagem que o usuário não é autenticado

15. Clique em `Retornar à página de login`.
16. Digite a seguinte URL na barra de endereços e clique no botão verde (clique no botão `Accept changes` até que a requisição seja enviada ao servidor):

    ```
    http://bssac.esr.rnp.br/
    ```

17. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`. Clique no botão `Accept changes` até que a requisição seja enviada ao servidor
18. Digite a seguinte URL na barra de endereços e clique no botão verde (clique no botão `Accept changes` até que a requisição seja enviada ao servidor):

    ```
    http://bssac.esr.rnp.br/admin/oper2.php
    ```

19. Foi possível acessar a página?

    

    Resposta: apareceu a mensagem que a página foi acessada a partir de uma origem não permitida.

20. Novamente, repita a seguinte URL na barra de endereços e clique no botão verde:

    ```
    http://bssac.esr.rnp.br/admin/oper2.php
    ```

21. Agora, na página `Edit Request` do WebScarab, clique na aba `Parse` e no botão `Insert` e adicione o atributo `Referer` com o conteúdo http://bssac.esr.rnp.br/admin/menu.php. Clique em um outro parâmetro da lista e depois clique no botão `Accept changes` até que a requisição seja enviada ao servidor.
22. Foi possível acessar a funcionalidade?

    

    Resposta: sim pois é utilizado o atributo Referer

23. Feche o WebScarab mas antes desmarque a opção `Intercept requests` na aba `Proxy`.
24. No plugin Multiproxy do FireFox selecione Direct.
25. Clique em Encerrar sessão.

Acesso direto a objetos

O foco deste exercício é ilustrar como objetos de outros usuários podem ser acessados, quando se tem permissão de uso da funcionalidade e o mecanismo de autorização é vulnerável.

1. Retorne ao Firefox.
2. Acesse http://bssac.esr.rnp.br/
3. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
4. Clique no link `Caixa de mensagens`.
5. Clique na mensagem M#1 para visualizá-la.
6. Observe a barra de endereços do navegador web.
7. Clique em `Encerrar sessão`.
8. Forneça `esruser` e `esruser` para os campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
9. Clique em Caixa de mensagens.
10. Clique na mensagem `M#1` para visualizá-la.
11. Observe a barra de endereços do navegador web.
12. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
13. Clique na mensagem `M#2` para visualizá-la.
14. Observe a barra de endereços do navegador web.
15. Clique em `Encerrar sessão`.
16. Digite a seguinte URL na barra de endereços do navegador e clique na seta verde:

```
http://bssac.esr.rnp.br/view.php?mid=3
```

17. O que acontece?

Resposta: apareceu a mensagem usuário não autenticado

18. Clique em `Retornar à página de login`.
19. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
20. Digite a seguinte URL na barra de endereços do navegador e clique na seta verde:

```
http://bssac.esr.rnp.br/view.php?mid=1
```

21. Foi possível ver a mensagem de outro usuário?

Resposta: sim, apareceu a mensagem do usuário esruser

22. Repita o passo 20, variando o valor do parâmetro `mid` de 2 a 8.

23. Clique em Encerrar sessão.

Acesso direto a recursos estáticos

Nesta parte da atividade, são vistos ataques de acesso direto a recursos estáticos.

1. Digite `admin` e `admin` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
2. Clique em `Visualizar arquivos`.
3. Anote as URLs dos links apresentados.
4. Clique em `echo.txt`.
5. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
6. Clique em `Encerrar sessão`.
7. Digite a seguinte URL na barra de endereços do navegador e clique na seta verde:

```
http://bssac.esr.rnp.br/files/cat.txt
```

8. Foi possível acessar o arquivo, mesmo não estando autenticado? Explique por que isso é possível.

> **Resposta:** sim. Provavelmente a aplicação está mostrando o arquivo sem nenhum tipo de controle de acesso.

Tente acessar as demais URLs anotadas no passo 3.

9. Encerre o Firefox.

2. Atividade – Controle de acesso no lado cliente da aplicação

Confiar em controles que são executados no lado cliente da aplicação é uma prática ruim de segurança, pois podem ser facilmente violados, por usuários maliciosos. O propósito desta atividade é ilustrar alguns cenários em que essa vulnerabilidade está presente e os testes que podem ser efetuados para identificá-la. Os exercícios devem ser realizados na máquina virtual do aluno, e recomenda-se que se imagine o meio de resolvê-los, antes de seguir o roteiro fornecido.

Autorização no lado cliente da aplicação

Esta parte do exercício aborda uma aplicação que realiza o processo de autorização com código Javascript, a partir de uma matriz de controle de acesso obtida no servidor.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse http://bcsac.esr.rnp.br/js/.
3. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
4. Passe o mouse sobre os links e veja a URL de cada um deles.
5. Clique em Caixa de mensagens e veja a URL na barra de endereços.
6. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
7. Clique em `Função Administrativa #1`. O que acontece?

> **Resposta:** aparece um popup informando que você não tem permissão de acesso

8. Clique em OK.
9. Clique em `Visualizar arquivos`. O que acontece?

Resposta: aparece um popup informando que você não tem permissão de acesso

10. Clique em OK.
11. Pressione Ctrl+U para visualizar o código HTML.
12. Analise o código Javascript e os formatos dos links.
13. Feche a janela de código HTML.
14. No Firefox, clique em `Encerrar sessão`.
15. Digite `admin` e `admin` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
16. Passe o mouse sobre os links e veja a URL de cada um deles.
17. Clique em `Função Administrativa #1` e veja a URL na barra de endereços.
18. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
19. Clique em `Visualizar arquivos` e veja a URL na barra de endereços.
20. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
21. Pressione Ctrl+U, para visualizar o código HTML.
22. Analise o código Javascript e os formatos dos links. O que difere do visto no passo 12?

Resposta: tanto logado como guest ou como dummy os links estão apontando para o dummy.php. Para o usuário admin são criadas variáveis em javascript acm[1] =1; acm[2] =1; acm[3] =1; acm[4] =1; O índice da variável acm representa o id do link clicado -1

23. Feche a janela de código HTML.
24. No Firefox, clique em `Encerrar sessão`.
25. Digite a seguinte URL na barra de endereços do navegador e clique na seta verde:

```
http://bcsac.esr.rnp.br/js/oper2.php
```

26. O que acontece?

Resposta: apareceu a mensagem de usuário não autenticado.

27. Clique em `Retornar à página de login`.
28. Digite `guest` e `guest` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
29. Digite a seguinte URL na barra de endereços do navegador e clique na seta verde:

```
http://bcsac.esr.rnp.br/js/oper2.php
```

30. O acesso foi concedido? Onde se encontra a falha?

Resposta: apareceu a mensagem de acesso normal. Isso acontece porque o esquema de autenticação utilizado depende de código javascript executado no lado cliente.

31. Clique em Encerrar sessão.

Manutenção de perfil no lado cliente da aplicação

O objetivo deste exercício consiste em violar aplicações que mantêm o perfil de acesso do usuário, no lado cliente da aplicação.

1. Acesse http://bcsac.esr.rnp.br/.
2. Digite `esruser` e `esruser` nos campos `Usuário` e `Senha`, respectivamente, e clique em `Login`.
3. Passe o mouse sobre os links e veja a URL de cada um deles. O que chama a atenção?

Resposta: existe uma variável uid com o nome do usuário logado

4. Clique em Caixa de mensagens.
5. Passe o mouse sobre os links e veja a URL de cada um deles. Existe uma diferença fundamental entre essas URLs e as do Passo 3, do ponto de vista de um ataque. Qual é?

Resposta: Não tem a variável uid

6. Altere a URL na barra de endereços do navegador, adicionando as entradas abaixo, uma por vez, e clicando na seta verde a cada iteração:

```
&adm=Y
&adm=S
&adm=true
&admin=Y
&admin=S
&admin=true
&root=Y
&root=S
&root=true
```

7. Foi possível obter acesso mais privilegiado?

Resposta: não

8. Altere a barra de endereços para a URL abaixo e clique na seta verde:

```
http://bcsac.esr.rnp.br/oper1.php?uid=admin
```

9. O que aconteceu?

Resposta: foi possível acessar as mensagens do usuário admin

10. Clique em `M#1 de admin`. Foi possível ler a mensagem?

Resposta: sim

11. Acesse o WebGoat, clicando no ícone na barra de atalhos.
12. Forneça `guest` e `guest` como credenciais e clique em `OK`.
13. Clique em `Start WebGoat`.

14. Clique em `Admin Functions` e observe as funções disponíveis.
15. Clique em `Access Control Flaws` e, em seguida, em `Remote Admin Access`. Não deixe de clicar em `Restart this Lesson` antes de continuar.
16. Repita o passo 6, mas, adicionalmente, clique em `Admin Functions`, a cada interação, para ver se o ataque foi bem-sucedido.
17. Com que parâmetro a interface administrativa do WebGoat é liberada?

Resposta: &admin=true

18. Encerre o Firefox.

Proteção de referências a objetos

Neste exercício, serão estudadas abordagens inseguras utilizadas na proteção de referências a objetos internos da aplicação.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse `http://refp.esr.rnp.br/`.
3. Clique no link para a `RFC 2616`.
4. Observe a URL na barra de endereços e os valores dos parâmetros `f e t`.
5. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
6. Clique no link para a ` RFC 2617 `.
7. Observe a URL na barra de endereços e os valores dos parâmetros `f e t`. Que esquema de proteção é utilizado?

Resposta: t= 1 o valor de f esta de trás para frente

8. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
9. Clique no link para a `RFC 2821`.
10. Observe a URL na barra de endereços e os valores dos parâmetros `f e t`. Que esquema de proteção é utilizado?

Resposta: t=2 o valor de f contém dois sinais de igual no final da string o que parece ser um base64.

11. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
12. Clique no link para a `RFC 959`.
13. Observe a URL na barra de endereços e os valores dos parâmetros `f e t`. Que esquema de proteção é utilizado?

Resposta: t=3 é utilizado um codificação hexadecimal utilizando ASCII. Para exemplificar pode-se utilizar este conversor online https://codebeautify.org/hex-string-converter

14. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
15. Suponha a existência do arquivo `ylonen.2006.txt`. Como seria a URL para acessá-lo, quando o parâmetro t = 0? Tente visualizar o arquivo, no Firefox.

Resposta: funciona normalmente.

http://refp.esr.rnp.br/f=ylonen.2006.txt&t=0

16. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
17. Repita o passo 15, para t = 1. Empregue o utilitário `rev`, se necessário.
18. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
19. Repita o passo 15, para t = 2. Empregue o utilitário `base64`, se necessário, e cuidado com caracteres de final de linha.
20. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
21. Repita o passo 15, para t = 3 (observe que a codificação é hexadecimal assim utilize um conversor Hexa Online para gerar o valor de f).
22. Encerre o Firefox.

3. Atividade – Percurso de caminho

Aplicações que manipulam arquivos selecionados pelo usuário podem ser vulneráveis a ataques de percurso de caminho, que é o tema da presente atividade. Os roteiros devem ser executados na máquina virtual do aluno e recomenda-se que a estratégia de exploração seja traçada, antes de se ver a solução.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse http://path.esr.rnp.br/.
3. Passe o mouse sobre os links e observe atentamente as URLs, na barra de estado. O que chama a atenção para um possível ataque?

Resposta: parece o nome de um arquivo armazenado no sistema de arquivos.

4. Clique no link para a `RFC 2616` e observe a barra de endereços do navegador web.
5. Altere, na barra de endereços, o valor do parâmetro `f`, para o seguinte:

```
..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
```

6. O ataque de percurso de caminho funciona?

Resposta: sim pois o caminho ficou ../../../etc/passwd

7. Repita o passo 5, mas usando o valor a seguir:

```
fielding.1999.txt%00abcdef
```

8. O arquivo original foi exibido normalmente? Justifique o resultado.

Resposta: não. %00 é um caractere nulo

9. Repita o Passo 5, mas usando o valor abaixo, para ver o código fonte de `view.php`:

```
..%2Fview.php
```

10. Acesse http://path.esr.rnp.br/index2.php.
11. Passe o mouse sobre os links e observe atentamente as URLs na barra de estado. O que mudou em relação ao cenário anterior?

Resposta: não tem o parâmetro t

12. Clique no link para a `RFC 2616` e observe a barra de endereços do navegador web.
13. Altere, na barra de endereços, o valor do parâmetro `f` para o seguinte:

```
..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
```

14. O ataque funcionou? Qual seria o motivo do resultado obtido?

Resposta: não. O código implementado adiciona a extensão do arquivo ao nome informado. Ver pg 382

15. Repita o passo 13, mas adicionando um caractere nulo codificado (%00) ao final do valor.
16. O que aconteceu agora? Justifique o resultado.

Resposta: funcionou pois o valor nulo adicionado ao final da URL comenta qualquer valor adicionado a string pela aplicação.

17. Encerre o Firefox.

4. Atividade – Redirecionamento não validado

Esta atividade apresenta o problema de redirecionamento não validado, o qual favorece ataques de phishing. Execute o roteiro na máquina virtual de aluno e procure descobrir os passos, antes de ler os fornecidos.

1. Inicie o WebScarab, presente no menu `03 - Web Application Analysis`.
2. Inicie o Firefox, presente no menu `Usual applications\Internet`.
3. No Firefox, clique no Multiproxy SwitchOmega, na barra de estado, e selecione o WebScarab.
4. Acesse http://redir.esr.rnp.br/.
5. Clique em `Redirecionamento HTTP temporário`.
6. No WebScarab, verifique as requisições realizadas e as respostas fornecidas.
7. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
8. Clique em `Redirecionamento HTTP permanente`.
9. No WebScarab, verifique as requisições realizadas e as respostas fornecidas.
10. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
11. Clique em `Redirecionamento por meio de meta-tag "Refresf"`.
12. No WebScarab, verifique as requisições realizadas e as respostas fornecidas.
13. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
14. Clique em `Redirecionamento por meio de Javascript`.
15. No WebScarab, verifique as requisições realizadas e as respostas fornecidas.

16. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
17. Clique em `Redirecionamento por meio de .htaccess`.
18. No WebScarab, verifique as requisições realizadas e as respostas fornecidas.
19. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
20. Clique em `Redirecionamento não validado #1`.
21. No WebScarab, verifique as requisições realizadas e as respostas fornecidas após acessado a url http://redir.esr.rnp.br/end.php.
22. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
23. Clique com o botão direito sobre `Redirecionamento não validado #1` e selecione `Copy Link Location`.
24. Selecione a barra de endereços e cole a URL, pressionando Ctrl+V.
25. Altere o valor do parâmetro `url` para http://www.evil.org e clique na seta verde.
26. A aplicação é vulnerável a redirecionamento não validado?

Resposta: sim

27. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
28. Clique em `Redirecionamento não validado #2`.
29. No WebScarab, verifique as requisições realizadas e as respostas fornecidas. Que parâmetro foi passado e com que valor?

Resposta: target=/end.php

30. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
31. Clique com o botão direito sobre `Redirecionamento não validado #2` e selecione `Copy Link Location`.
32. Selecione a barra de endereços e cole a URL, pressionando Ctrl+V.
33. Altere o valor do parâmetro `target` para `.evil.org` e clique na seta verde.
34. A aplicação é vulnerável a redirecionamento não validado?

Resposta: sim. A URL final ficou http://redir.esr.rnp.br.evil.org. Só irá funcionar porque o atacante tem controle sobre o seu servidor de DNS portanto poderia criar um registro para atender a esta requisição. ver pg. 385

35. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
36. Clique em `Redirecionamento não validado #3`.
37. No WebScarab, verifique as requisições realizadas e as respostas fornecidas. Que parâmetro foi passado e com que valor?

Resposta: url=http://redir.esr.rnp.br/end.php

38. Retorne ao Firefox e pressione Alt + [Seta para esquerda], para voltar à página anterior.
39. Clique com o botão direito sobre `Redirecionamento não validado #3` e selecione `Copy Link Location`.

40. Selecione a barra de endereços e cole a URL, pressionando Ctrl+V.
41. Observe atentamente a URL e as partes que a compõem.
42. Altere o valor do parâmetro `url` para http://www.evil.org e clique na seta verde.
43. O ataque funcionou? Procure explicar o resultado.

Resposta: não funcionou.

44. Altere o valor do parâmetro `url` para http://www.evil.org/?u=http://redir.esr.rnp.br/ e clique na seta verde.
45. E agora? O ataque funcionou?

Resposta: sim. A solução ainda é vulnerável, pois fica satisfeita com a presença de `http://esr.rnp.br` em qualquer ponto do argumento. Graças a isso, uma maneira de quebrar o mecanismo de proteção envolve a submissão do valor: http://www.evil.org?u=http://esr.rnp.br/

46. Clique no Multiproxy SwitchOmega, na barra de estado, e selecione Direct.
47. Encerre o WebScarab.
48. Encerre o Firefox.
49. Inicie o nacegador Opera, presente no menu `Usual application\Internet`.
50. Acesse http://redir.esr.rnp.br/.
51. Clique em `Redirecionamento por meio de meta-tag Refresh` e espere ser redirecionado.
52. Clique no botão Retornar. O que acontece?

Resposta: se este exercício for realizado no Firefox nada estranho irá acontecer pois o navegador irá acessar a página principal porém se for realizado no Chrome ele irá retornar para a página de redirecionamento e depois de alguns segundos para a página inicial. Ver apostila pg 384

53. Encerre o Google Chrome.

6. Atividade – Condições de corrida

O objetivo desta atividade é ilustrar o que pode ocorrer quando uma condição de corrida é explorada, e a dificuldade de se executar ataques desse tipo. O roteiro abaixo deve ser seguido na máquina virtual do aluno, após traçada a estratégia de exploração.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse o WebGoat, a partir da barra de atalhos.
3. Autentique-se com as credenciais `guest` e `guest`.
4. Clique em `Start WebGoat`.
5. No menu presente no lado esquerdo, clique em `Concurrency` e, em seguida, em `Thread Safety Problems`. Não esqueça de clicar no link `Restart this Lesson` antes de continuar.
6. Leia a descrição do exercício fornecida.
7. Digite `jeff` em `Enter user name`.
8. Inicie o Google Chrome, presente no menu `Usual application\Internet`.

9. Acesse o WebGoat, digitando http://webgoat.esr.rnp.br:8080/webgoat/attack na barra de endereços.
10. Autentique-se com as credenciais `guest e guest`.
11. Clique em `Start WebGoat`.
12. No menu presente no lado esquerdo, clique em `Concurrency` e, em seguida, em `Thread Safety Problems`.
13. Digite `dave` em `Enter user name`.
14. Retorne ao Firefox e clique em `Submit`.
15. Retorne rapidamente ao Google Chrome e clique em `Submit`.
16. Compare as informações exibidas nos dois navegadores e veja se são do mesmo usuário. Em caso positivo, o ataque foi efetuado com sucesso. Se não, repita o processo até conseguir.
17. Encerre o Firefox.
18. Encerre o Google Chrome.

7. Atividade – Vulnerabilidades na lógica de negócio

Nesta atividade, dois cenários de lógica de negócio vulnerável serão estudados e explorados. Execute o roteiro na máquina virtual do aluno e procure quebrar as aplicações, por iniciativa própria, antes de acompanhar os passos disponibilizados.

1. Inicie o Firefox, presente no menu `Usual application\Internet`.
2. Acesse http://blogic.esr.rnp.br/.
3. Digite `100` no campo Valor da transferência e clique em `Transferir`.
4. Repita o passo 3, mas digitando `2000` no campo `Valor da transferência`.
5. Digite `400` no campo `Valor da transferência` e clique em `Transferir`. O que acontece?

> **Resposta:** funcionou

6. Repita o passo 5. Foi possível realizar mais essa transferência?

> **Resposta:** sim pois ele ainda tinha saldo.

7. Acesse http://blogic.esr.rnp.br:8080/overflow/.
8. Digite `500` no campo `Valor do empréstimo` e clique em `Emprestar`.
9. O que acontece?

> **Resposta:** o empréstimo foi realizado

10. Repita o passo 8, mas com o valor `12000` em vez de `500`.
11. Foi possível emprestar o montante especificado?

> **Resposta:** o empréstimo foi realizado

12. Repita o passo 8, agora, com o valor `9500`.
13. Tente emprestar `30000`, para causar um possível extravasamento de inteiro. O ataque foi bem-sucedido?

Resposta: não pois este valor é superior ao limite máximo.

14. Olhe a barra de endereços do navegador e identifique a tecnologia utilizada pela aplicação.
15. Abra uma nova janela do Firefox, e procure na internet, os tipos primitivos de Java.
16. Anote os maiores valores permitidos para os tipos `int e long` .
17. Retorne à aplicação e tente efetuar um empréstimo com o maior `int` , anotado no passo anterior.
18. O ataque foi bem-sucedido?

Resposta: O valor mínimo de uma variável int no java é de -2.147.483.648 e o valor máximo de 2.147.483.647. Ao digitar este valor o ataque funciona `2147483647` .

19. Encerre o Firefox.

ENTREGA DA TAREFA

Para que seja considerada entregue você deve anexar a esta atividade no AVA uma imagem mostrando que o ataque `Vulnerabilidades na lógica de negócio` foi bem sucedido.

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

Última atualização 2020-09-02 17:58:59 -0300