

Sessão 4: Teste do gerenciamento de sessões

1. Atividade – Introdução ao gerenciamento de sessões

Esta atividade tem por objetivo introduzir os mecanismos de gerenciamento de sessões usados pelas aplicações web, para suprir a deficiência apresentada pelo protocolo HTTP nessa arena. Para iniciá-la, carregue as máquinas virtuais do aluno e do servidor (Fedora) e execute os roteiros na primeira delas.

Identificação do tipo de gerenciamento de sessões

O primeiro passo, para testar um esquema de gerenciamento de sessões, é entender como são transportados os identificadores de sessão. Neste exercício, o leitor identificará como isso é realizado em diversas aplicações web.

1. Inicie o WebScarab, presente no menu 03 - Web Application Analysis .
2. Clique na aba Proxy, depois em Manual Edit e, por fim, desmarque a opção Intercept requests .
3. Inicie o Firefox, presente no menu Usual applications\Internet .
4. No Firefox, clique no Multiproxy SwitchOmega, na barra de estado, e selecione o WebScarab.
5. Acesse o DVWA, por meio da barra de atalhos.
6. No WebScarab, clique na aba Summary .
7. Role a janela até encontrar a coluna Set-Cookie e dê um duplo clique na linha contendo um valor.
8. Na parte inferior da janela de conversação, clique na aba Raw e observe como o cabeçalho Set-Cookie foi definido.
9. Feche a janela de conversação.
10. Retorne ao Firefox e acesse o Bodgeit Store , por meio da barra de atalhos.
11. Repita os passos 6 a 9.
12. Retorne ao Firefox e acesse o site web do lugar em que trabalha.
13. Verifique no WebScarab que tipo de mecanismo é utilizado para gerenciamento de sessão.



Resposta: Esta é uma resposta pessoal e depende de qual site o aluno irá acessar.

14. Encerre o WebScarab.
15. Encerre o Firefox.

2. Atividade – Descoberta de vulnerabilidades e exploração

O propósito desta atividade é introduzir ao aluno os métodos que podem ser utilizados para a descoberta e exploração de vulnerabilidades, em mecanismos de gerenciamento de sessões. Todos os exercícios devem ser realizados na máquina virtual do aluno e é altamente recomendado que se tente traçar a estratégia de exploração antes de seguir o roteiro fornecido.

Identificadores de sessão previsíveis

O objetivo deste exercício é analisar a previsibilidade dos identificadores de sessão, com auxílio das ferramentas WebScarab e Stompy, além de realizar a engenharia reversa de um mecanismo proprietário de gerenciamento de sessão.

Parte I – Análise da qualidade dos identificadores de sessão – WebScarab

1. Inicie o WebScarab, presente no menu 03 - Web Application Analysis .

2. Clique na aba Proxy , depois em Manual Edit e, por fim, desmarque a opção Intercept requests .
3. Inicie o Firefox, presente no menu Usual applications\Internet .
4. No Firefox, clique no Multiproxy SwitchOmega, na barra de estado, e selecione o WebScarab.
5. Acesse o DVWA, por meio da barra de atalhos.
6. No WebScarab, clique na aba Summary .
7. Role a tela até encontrar a coluna Set-Cookie e anote o número da linha contendo o valor PHPSESSID .
8. Clique na aba SessionID Analysis e, em seguida, na aba Collection .
9. Em Previous Requests , selecione a linha anotada no passo 7 (ou passo 19).
10. Clique no botão Test , observe os cookies que foram definidos e clique em OK .
11. Digite 200 em Samples e clique em Fetch .
12. Clique na aba Analysis .
13. Em Session Identifier , selecione a linha contendo PHPSESSID .
14. Clique na aba Visualization e observe o gráfico. Os identificadores de sessão são previsíveis?



Resposta: Não são pois os pontos não formam um padrão.

15. Retorne ao Firefox e acesse o WackoPicko, por meio da barra de atalhos.
16. Clique no link Admin , na parte inferior da tela.
17. Forneça admin para os campos Username e Password e clique em Submit .
18. No WebScarab, clique na aba Summary .
19. Role a tela até encontrar a coluna Set-Cookie para o site WackoPicko e anote o número da linha contendo o valor session (normalmente será session=xxxx, não confundir com PHPSessionID).
20. Dê um duplo clique na linha para ver a requisição.
21. Clique na aba Raw logo abaixo do botão Next .
22. Selecione a requisição inteira e pressione Ctrl + C.
23. Abra o gedit, localizado no menu Usual applications\Acessorios\Editor de texto .
24. Pressione Ctrl + V, para colar a requisição no gedit.
25. Pressione Ctrl + S, para salvar o arquivo no diretório /tmp , usando o nome wacko.req , e clique no botão Salvar .
26. Feche a janela do gedit.
27. Encerre a janela de conversação do WebScarab.
28. Repita os passos 8 a 12, mas considerando a linha anotada no passo 19.
29. Na aba Analysis , no campo Session Identifier , selecione a linha contendo wackopicko.esr.rnp.br .
30. Clique na aba Visualization e observe o gráfico. Os identificadores de sessão são previsíveis?



Resposta: Sim, os pontos estão agrupados e formam uma linha.

Parte II – Engenharia reversa de identificadores de sessão

1. Acesse o WebGoat, por meio do Firefox, clicando na barra de atalhos.

2. Digite as credenciais `guest/guest` e clique em `OK`.
3. Clique no botão `Start WebGoat`.
4. No menu do lado esquerdo, clique em `Session Management Flaws`.
5. Clique em `Spoof an Authentication Cookie`. Na página clique no link `Restart this Lesson`
6. Na tela que aparece, autentique-se com `webgoat/webgoat` e veja a mensagem `Welcome, webgoat`.
7. No `WebScarab`, clique em `Summary`.
8. Role a tela até encontrar a coluna `Set-Cookie` e dê um duplo clique na linha de maior número contendo o valor `AuthCookie`.
9. Anote o valor do cabeçalho `Cookie: AuthCookie`, contido na parte inferior da tela, aba `Raw` abaixo do botão `Next`.
10. Encerre a janela de conversação.
11. Retorne ao Firefox e clique no link `Logout`, acima de `Refresh` e em `Restart this Lesson`.
12. Autentique-se, agora, com `aspect/aspect` e veja a nova mensagem de boas-vindas.
13. Repita os passos 7 a 10.
14. Clique na aba `Proxy` e marque `Intercept requests`.
15. Iniciando a engenharia reversa dos identificadores, observe que as cinco primeiras posições são constantes e correspondem ao número 65432.
16. Qual a relação entre os tamanhos da parte composta por letras e do respectivo identificador de usuário?


Resposta: Ambas strings tem o mesmo tamanho:

Tabela 1. Lista de Cookie



Usuário	Cookie
webgoat	AuthCookie=65432ubphcfx
aspect	AuthCookie=65432udfqtb

17. Existe alguma letra que se repete nos identificadores de usuário (`webgoat` e `aspect`)? E nos identificadores de sessão (`ubphcfx` e `udfqtb`)?



Resposta: sim, são repetidas as letras `a`, `e` e `t` nos identificadores de usuário. sim, são repetidas as letras `b`, `f` e `u` nos identificadores de sessão.

18. Como fica o identificador de sessão para `alice`?

- Observa-se que o identificador, exceto o número 65432 que inicia o valor, tem uma quantidade de caracteres igual ao texto.
- Se inverter a ordem das letras do nome do usuário temos:

Tabela 2. Calculo identificador Alice

Nome Usuário	Nome Invertido						
webgoat	taogbew	t	a	o	g	b	e w
aspect	tcepsa	t	c	e	p	s	a

Tabela 3. Calculo identificador Alice

ubphcfx	u	b	p	h	c	f	x
udfqtb	u	d	f	q	t	b	

Observando a tabela é possível identificar o deslocamento de 1 letra a direita, assim:

A = B
B = C
C = D

- Utilizando estes processo para o nome **alice** temos:
 - inverter o nome alice
 - ecila
 - Deslocando uma letra para a direita
 - fdjmb
- Adicionando o início 65432 temos
 - 65432fdjmb

19. Retorne ao Firefox e clique no link **Refresh**.

20. Clique na aba **Raw**.

21. Troque o valor de **AuthCookie**, no cabeçalho **Cookie**, para o determinado no passo 18.

22. Clique em **Accept Changes**.

23. Retorne ao Firefox e veja a mensagem exibida.

24. Encerre o WebScarab.

25. No Firefox, clique no Multiproxy SwitchOmega, na barra de estado, e selecione **Direct**.

26. Encerre o Firefox.

27. Encerre o Editor de Texto.

Domínio de identificadores de sessão com baixa cardinalidade

Quando os identificadores de sessão são selecionados a partir de conjuntos que contêm poucos elementos, fica fácil descobrir elementos válidos que tenham sido atribuídos a conversações ativas, mesmo que a escolha seja aleatória. O objetivo deste exercício é analisar uma sequência de valores, por meio do Stompy, para verificar a entropia da amostra coletada.

1. Inicie uma janela de terminal.
2. Acesse o diretório Arquivos do curso/sessao-04:

```
~$ cd ~/Arquivos\ do\ Curso/sessao-04
```

3. Veja o conteúdo do arquivo ids.txt:

```
~$ less ids.txt
```

4. Analise o arquivo com o Stompy:

```
~$ /usr/sbin/stompy -R ids.txt
```

5. Role a janela de terminal e veja a saída do utilitário. Qual o diagnóstico fornecido?



Resposta: os ids listados no arquivo ids.txt são previsíveis

6. Encerre a janela de terminal.

Transmissão em claro de identificador de sessão

O objetivo deste exercício é capturar o identificador de sessão, por meio da escuta dos pacotes de rede, em um cenário em que nenhuma proteção é utilizada no transporte de informações.

1. Inicie o Firefox, presente no menu Usual applications\Internet .
2. Inicie o Wireshark

```
~$ sudo wireshark
```

3. No menu superior clique em Capture → Options . Selecione a interface eth1 , no campo Capture filter , digite tcp port http e clique em Start , para iniciar a captura de pacotes.
4. Acesse com o Firefox o DVWA, a partir da barra de atalhos.
5. Pare a captura de pacotes no Wireshark, clicando no quarto botão da barra de ferramentas (Stop the running live capture).
6. Procure pela linha contendo HTTP/1.1 302 Found e a selecione.
7. Na segunda parte da tela, expanda o item Hypertext Transfer Protocol e procure pelo cabeçalho Set-Cookie . Observe que o cookie PHPSESSID é transmitido em claro.
8. Encerre o Wireshark e o Firefox.

Manipulação de identificador de sessão por meio de scripts

Neste exercício, o aluno acessará o identificador de sessão por meio de scripts no lado cliente da aplicação.

1. Inicie o Firefox, presente no menu Usual applications\Internet .
2. Acesse o DVWA, a partir da barra de atalhos.

3. Forneça para os campos Username e Password, respectivamente, os valores admin e password, para se autenticar no sistema.

4. No menu de opções, clique em XSS reflected.

5. Digite no campo What's your name o valor:

```
<script>alert(document.cookie)</script>
```

6. Clique em Submit para ver a caixa de mensagem exibida. Anote o número PHPSESSID.

7. Clique em OK.

8. Digite no campo What's your name o valor:

```
<script>document.write('')</script>
```

9. Clique em Submit.

10. Pressione Ctrl + N, para abrir uma nova janela do Firefox.

11. Acesse o arquivo de trilhas de auditoria do servidor www.evil.org, por meio da URL:

```
http://www.evil.org/logs/evil.org-access_log
```

12. Procure o registro da requisição realizada pelo elemento injetado no passo 8. O valor do cookie é o mesmo que o identificado no passo 5?



Resposta: sim

13. Encerre o Firefox.

Atributos de cookies

O propósito deste exercício é fixar os conceitos sobre os atributos que podem ser utilizados por cookies e o impacto que têm em segurança.

1. Inicie o Firefox, presente no menu Usual applications\Internet.

2. No Firefox, clique no Multiproxy Switch, na barra de estado, e selecione Direct.

3. Acesse https://cookies.esr.rnp.br/. O Firefox exibe uma mensagem de erro porque o certificado apresentado pelo servidor é autoassinado.

4. Clique em Advanced.

5. Clique em Add Exception.

6. Desmarque Permanently store this exception e clique em Confirm Security Exception.

7. Clique no link Atributo "secure".

8. Clique no ícone do Cookie Editor ao lado da barra URL e veja que um cookie ESRSID foi definido.

9. Retorne ao Firefox e clique em Acesso via HTTPS.

10. Clique no ícone do Cookie Editor ao lado da barra URL e veja que o cookie ESRSID foi definido.

11. No Firefox, retorne à página anterior e clique em Acesso via HTTP.

12. Clique no ícone do Cookie Editor ao lado da barra URL e veja que o cookie não foi definido, porque o navegador honrou o atributo secure.

13. Retorne duas páginas no Firefox, para acessar novamente a página inicial.
14. Clique no link Atributo "HttpOnly".
15. Clique no ícone do Cookie Editor ao lado da barra URL e veja que um novo cookie, ESRSIDH0, foi definido.
16. Retorne ao Firefox e clique em Ler Cookie. Os dois cookies são exibidos?



Resposta: não. É exibido apenas o Cookie ESRSID

17. Clique em Criar Novo Cookie e, depois, novamente em Ler Cookie. Veja que um cookie foi adicionado.
18. Pressione Alt + [Seta para esquerda], para retornar à página anterior.
19. Clique no link Atributo "Domain".
20. Veja, por meio do Cookie Editor, que um novo cookie, ESRSIDDO, foi definido.
21. Clique no link Domínio exemplo.esr.rnp.br.
22. Clique no ícone do Cookie Editor ao lado da barra URL e veja que o cookie ESRSIDDO foi definido.
23. No Firefox, retorne à página anterior e clique em Domínio "other.rnp.br".
24. Veja pela mensagem de erro que nenhum cookie (basta clicar no ícone do Cookie Editor) foi enviado pelo navegador.
25. Pressione Alt + [Seta para esquerda] duas vezes.
26. Clique no link Atributo "Path".
27. Clique no ícone do Cookie Editor ao lado da barra URL e veja que um novo cookie, ESRSIDPA, foi definido.
28. Clique no link Subdiretório da pasta "path".
29. No Cookie Editor, veja que o cookie ESRSIDPA foi definido.
30. No Firefox, retorne à página anterior e clique em Outro diretório.
31. Clique no ícone do Cookie Editor ao lado da barra URL e veja que o cookie ESRSIDPA não foi enviado.
32. Encerre o Firefox.

Sequestro de sessão

Uma vez descoberto o identificador de uma sessão válida, o próximo passo consiste no sequestro dessa sessão. Neste exercício, o leitor verá como isso pode ser realizado.

1. Inicie o Google Chrome, presente no menu Usual applications\Internet.
2. Inicie o Wireshark:

```
~$ sudo wireshark
```

3. No menu superior clique em Capture → Options. Selecione a interface eth1 e, em seguida, no campo Capture filter, digite tcp port http e clique em Start, para iniciar a captura de pacotes.
4. Retorne ao Google Chrome e acesse <http://dvwa.esr.rnp.br>.
5. Autentique-se fornecendo admin e password para os campos Username e Password, respectivamente.
6. No Wireshark, procure pelo penúltimo GET e anote o PHPSESSID.
7. Inicie o Firefox, presente no menu Usual applications\Internet.
8. Acesse o DVWA, digitando a URL:

`http://dvwa.esr.rnp.br/vulnerabilities/xss_r/`

Veja que a aplicação o redireciona para a tela de autenticação.

9. Clique no ícone **Cookie Editor** ao lado da barra de URL.
10. Clique no cookie **PHPSESSID** definido para o domínio `dvwa.esr.rnp.br`
11. Altere o valor **Value** para o valor anotado no passo 6 e clique no ícone **Save**.
12. Tente novamente o acesso do passo 8. O que aconteceu?



Resposta: foi possível acessar a aplicação como usuário admin.

13. Encerre o Wireshark, o Google Chrome e o Firefox.

Fixação de sessão

Diferentemente de um sequestro de sessão, no qual o usuário malicioso precisa descobrir um identificador de sessão válido, no ataque de fixação de sessão, utiliza-se um valor já conhecido. Nesta prática, o leitor aprenderá a detectar aplicações vulneráveis a esse tipo de ataque e como o defeito pode ser explorado.

Parte I – Detecção de aplicação vulnerável

1. Inicie o Firefox, presente no menu **Usual applications\Internet**. Não esqueça de limpar os cookies do navegador.
2. Acesse o DVWA, a partir da barra de atalhos.
3. Clique no ícone **Cookie Editor** ao lado da barra URL.
4. Anote o valor do cookie **PHPSESSID** definido para `dvwa.esr.rnp.br`.
5. Feche a janela do **Cookie Editor**.
6. Autentique-se no DVWA, fornecendo as credenciais `admin` e `password`.
7. Clique novamente no ícone **Cookie Editor** ao lado da barra URL.
8. Compare contra o valor anterior o cookie **PHPSESSID** definido para `dvwa.esr.rnp.br`. A aplicação é vulnerável à fixação de sessão?



Resposta: Sim pois os dois valores de **PHPSESSID** são iguais.

9. Encerre o **Cookie Editor**.

Parte II – Exploração

1. Clique na opção **Logout** do DVWA.
2. Clique no ícone **Cookie Editor** ao lado da barra URL.
3. Clique no cookie **PHPSESSID**.
4. Substitua o valor do campo **Value** para `12345` e clique no ícone **Save**.
5. Encerre a janela do **Cookies Editor**
6. Autentique-se na aplicação com as credenciais `admin` e `password`.
7. Clique no menu **Tools** e em **Cookie Editor**.

8. Verifique o valor de `PHPSESSID`. O ataque é possível? O mecanismo de gerenciamento de sessões é estrito ou permissivo?



Resposta: Sim pois o valor foi mantido, mesmo sendo realizado uma nova autenticação. O mecanismo é permissivo.

9. Encerre o `Cookie Editor`.

10. Feche a janela do `Firefox`.

Encerramento vulnerável de sessão

O objetivo deste exercício é aprender como explorar aplicações que não encerram corretamente uma sessão de usuário.

1. Inicie o `Firefox`, presente no menu `Usual applications\Internet`.
2. Acesse o `Gruyere`, a partir da barra de atalhos.
3. Clique em `Sign in`.
4. Autentique-se com as credenciais `esruser/esruser`.
5. Clique no ícone `Cookie Editor`.
6. Anote o valor do cookie `GRUYERE`.
7. Encerre a janela `Cookie Editor`.
8. Clique em `Sign out`.
9. Clique em `Home` e veja que a página permanece no estado não autenticado.
10. Clique no ícone `Cookie Editor`.
11. Selecione o cookie `GRUYERE`.
12. Altere o valor do campo `Valor` para o anotado no passo 6.
13. Clique no ícone `Save` e encerre a janela `Cookie Editor`.
14. Clique em `Home` novamente. O que acontece?



Resposta: a aplicação entende que o usuário está autenticado

15. Encerre a janela do `Firefox`.

Sessões simultâneas de um mesmo usuário

Embora o compartilhamento de contas de usuário não seja recomendável, é comum que os sistemas nada façam para impedir tal comportamento inseguro. Neste exercício, o aluno testará uma aplicação para verificar se ela impõe limites no número de sessões paralelas de um mesmo usuário.

1. Inicie o `Firefox`, presente no menu `Usual applications\Internet`.
2. Acesse o `DVWA`, a partir da barra de atalhos.
3. Autentique-se com as credenciais `admin` e `password`.
4. Inicie o `Google Chrome`, presente no menu `Usual applications\Internet`.
5. Acesse o `DVWA`, digitando a URL `http://dvwa.esr.rnp.br` na barra de endereços.
6. Autentique-se com as mesmas credenciais utilizadas no passo 3. O sistema permitiu o acesso?



Resposta: sim

7. Encerre as janelas do Google Chrome e do Firefox.

Cross-site request forgery

O objetivo deste exercício consiste na exploração de cross-site request forgery, baseado em método GET e em método POST. Também será abordado o mecanismo de proteção que utiliza tokens anti-CSRF.

Parte I – CSRF com método GET

1. Inicie o Firefox, presente no menu Usual applications\Internet .
2. Acesse o DVWA, a partir da barra de atalhos.
3. Autentique-se com as credenciais admin e password .
4. Clique na opção de menu CSRF .
5. Observe que a aplicação não pede a senha atual, para substituí-la por um novo valor.
6. Pressione Ctrl + U e analise o código HTML da página, principalmente a estrutura do formulário para alteração de senha. Existe algum item que seja dependente da sessão do usuário?



Resposta: não

7. Pressione Ctrl + N, para abrir uma nova janela do Firefox.
8. Acesse <http://www.evil.org/get/get.html>.
9. Retorne ao DVWA e clique em Logout .
10. Tente se autenticar novamente com as mesmas credenciais.
11. Tente, agora, com as credenciais admin e pwd . Note que a senha foi alterada em decorrência da visita ao site www.evil.org .
12. Retorne à janela do site www.evil.org .
13. Pressione Ctrl + U, para ver o código HTML. Veja que a página csrf.html é carregada em um iframe com opacidade 0.00.
14. Feche a janela de visualização de código HTML.
15. Acesse a página <http://www.evil.org/get/csrf.html>.
16. Pressione Ctrl + U, para ver o código HTML. Como a operação de troca de senha é realizada automaticamente?



Resposta: na URL da imagem que é carregada é realizado um submit com a senha pwd

17. Encerre a janela de visualização de código HTML.
18. Retorne ao DVWA, acesse a opção CSRF e altera a senha para password novamente.

Parte II – CSRF com método POST

1. Retorne à janela do site www.evil.org .
2. Acesse <http://www.evil.org/post/post.html>.
3. Retorne ao DVWA e clique em Logout .
4. Autentique-se com as credenciais admin e password .

5. Tente, agora, com as credenciais `admin` e `pwd`. Note que a senha foi alterada em decorrência da visita ao site `www.evil.org`.
6. Retorne à janela do site `www.evil.org`.
7. Pressione `Ctrl + U`, para ver o código HTML. Veja que a página `csrf.html` é carregada em um `iframe` com opacidade 0.00.
8. Feche a janela de visualização de código HTML.
9. Acesse a página `http://www.evil.org/post/csrftoken.html`, para ver o código fonte HTML da página `csrf.html`.
10. Retorne ao DVWA, acesse a opção `CSRF` e altera a senha para `password` novamente.

Parte III – Token anti-CSRF

1. Clique na opção de menu `DVWA Security`.
2. Altere o nível de segurança de `low` para `medium` e clique em `Submit`.
3. Clique na opção de menu `CSRF`.
4. Pressione `Ctrl + U` e veja se algum item específico de página foi incluído.
5. Encerre a janela de visualização de código HTML.
6. Retorne à janela do site `www.evil.org`.
7. Acesse `http://www.evil.org/post/post.html`.
8. Retorne ao DVWA e clique em `Logout`.
9. Autentique-se com as credenciais `admin` e `password`. O ataque foi impedido?



Resposta: sim pois agora existe um campo chamado `hidden` chamado `csrf_token`

10. Encerre o Firefox.

Clickjacking

Clickjacking é um ataque relativamente novo e que já evoluiu para formas mais perigosas de exploração. Neste exercício, o aluno testará diversos sites web, para ver se são vulneráveis, e quebrará o mecanismo baseado em token anti-CSRF.

Parte I – Teste de vulnerabilidade

1. Inicie o Google Chrome, presente no menu `Usual applications\Internet`.
2. Acesse `http://cjtest.esr.rnp.br`.
3. Digite a URL da página institucional do lugar em que trabalha e clique em `Teste de Clickjacking` (não esqueça de iniciar com `http://`). A página foi exibida no `iframe`?



Resposta: resposta pessoal mas normalmente não deve ser exibida.

4. Repita o teste para `http://www.facebook.com`. A página foi carregada normalmente?



Resposta: não

5. Repita o teste para `http://twitter.com`. A página foi carregada normalmente?



Resposta: não

6. Repita o teste para <http://www.paypal.com>. A página foi carregada normalmente? Que mecanismo de proteção foi utilizado?



Resposta: não. Foi utilizado o cabeçalho HTTP X-frame-options = SAMEORIGIN com isso o navegador não pode colocar a página em um iframe.

7. Pressione Alt + [Seta para esquerda], para retornar à página de teste.

8. Repita o teste para <http://dvwa.esr.rnp.br>. A página foi carregada normalmente?



Resposta: sim

9. Marque `Usar sandbox` e repita o Passo 3. Houve alguma alteração no resultado?



Resposta: resposta pessoal mas normalmente não deve ser exibida.

10. Marque `Usar sandbox` e repita o Passo 4. Houve alguma alteração no resultado?



Resposta: não

11. Marque `Usar sandbox` e repita o Passo 5. Houve alguma alteração no resultado?



Resposta: não

12. Marque `Usar sandbox` e repita o Passo 6. Houve alguma alteração no resultado?



Resposta: não

13. Encerre o Google Chrome.

Parte II – Quebra de token anti-CSRF

1. Inicie o Firefox, presente no menu `Usual applications\Internet`.
2. Acesse o DVWA, a partir da barra de atalhos.
3. Autentique-se com as credenciais `admin` e `password`.
4. Clique na opção de menu `DVWA Security`.
5. Altere o nível de segurança de `low` para `medium` e clique em `Submit`.
6. Clique na opção de menu `CSRF`.
7. Pressione Ctrl + U e veja se algum item específico de página foi incluído.
8. Encerre a janela de visualização de código HTML.
9. Pressione Ctrl + N, para abrir uma nova janela do Firefox.
10. Acesse <http://clickjacking.evil.org>.
11. Arraste 1. `RSA` para Cifra assimétrica.

12. Arraste 2. AES para Cifra simétrica.
13. Clique em Conferir .
14. Retorne à janela do DVWA.
15. Clique em Logout .
16. Tente se autenticar com as mesmas credenciais. Algum erro ocorreu?



Resposta: não. A senha do admin foi trocada para pwd

17. Tente se autenticar com as credenciais admin e pwd .
18. Clique na opção de menu CSRF .
19. Altere a senha para password novamente.
20. Retorne à janela do domínio evil.org.
21. Acesse <http://clickjacking.evil.org/index2.html> e observe a sobreposição de páginas.
22. Pressione Ctrl + U, para ver o código HTML.
23. Feche a janela de visualização de código HTML.
24. Encerre o Firefox.



ENTREGA DA TAREFA

Para que seja considerada entregue você deve anexar a esta atividade no AVA uma imagem contendo o resultado do teste de Clickjacking → Parte I – Teste de vulnerabilidade demonstrando se o site de sua empresa esta vulnerável a este tipo de ataque.

Última atualização 2020-09-02 10:45:11 -0300