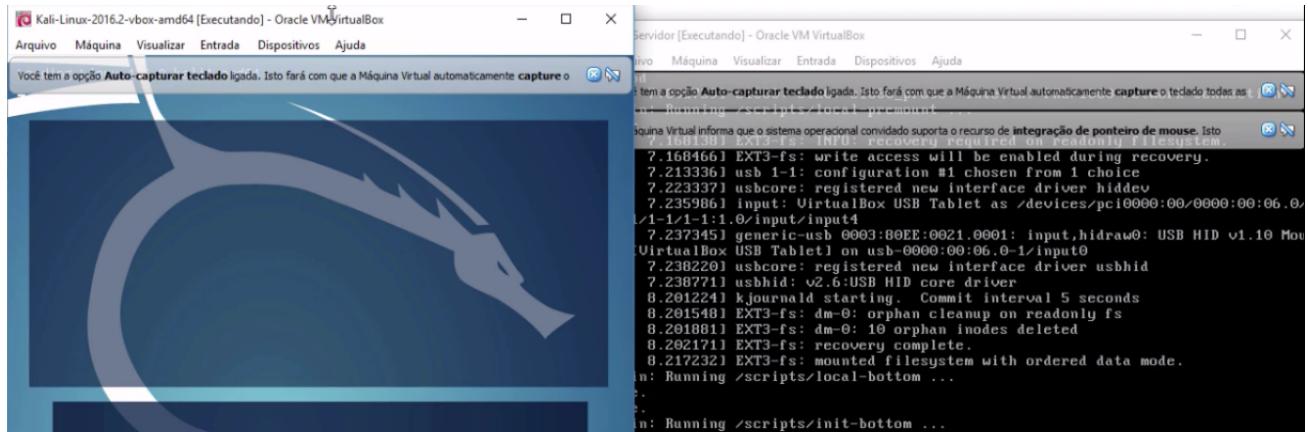


05

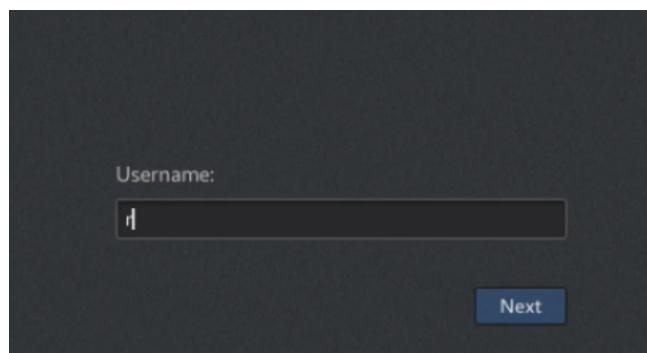
SQL Injection

Transcrição

Chegou o momento de inicializar as máquinas para realizar os primeiros ataques. Para fazer isso precisamos selecionar os dois ambientes e clicar em "Iniciar". Fazendo isso teremos duas abas com os respectivos ambientes rodando:

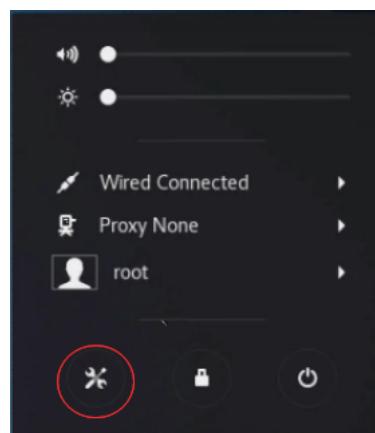


O Kali Linux (o ambiente referente ao hacker) demora um pouco para carregar. Ao finalizar o *boot* do Kali Linux aparece a seguinte tela:



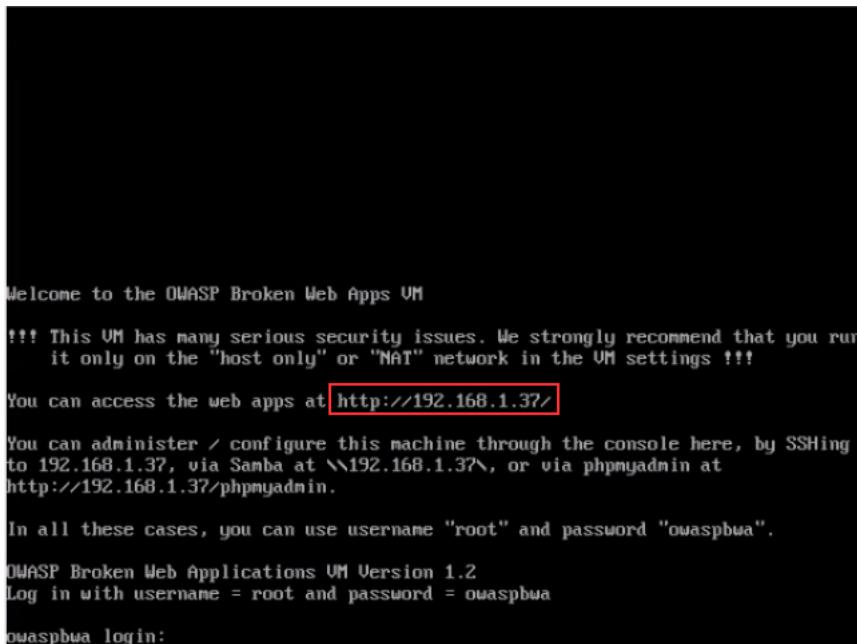
Basta preencher um *Username*, criar a *password* e dar um "Sign up", assim, aparecerá na tela o Kali Linux.

Antes de simular ataques vamos alterar uma pequena configuração do teclado. Nós selecionamos a seta na parte inferior direita da tela do Kali Linux e clicaremos no símbolo das ferramentas:



Abrirá uma janela com várias áreas e nós selecionamos o "Region & Language". Surgirá um formulário, o *Input sources*, e nele vamos clicar no símbolo de "+" e escolhemos o "Português(Brazil)". Por fim, basta clicar em "Add" e a opção escolhida será adicionada. Com o teclado configurado da maneira correta podemos acessar as páginas do servidor.

Para navegar nelas é preciso conhecer a URL de acesso, então, vamos retornar a aba do servidor:



Nessa tela podemos verificar o endereço fornecido. Voltamos no Kali Linux, abrimos o navegador e inserimos a URL para acessar a página vulnerável. Digitamos 192.168.1.37 e teremos o seguinte:

owaspbwa OWASP Broken Web Applications - Mozilla Firefox

owaspbwa OWASP Br... x +

192.168.1.37

Search

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

 **owaspbwa**

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable applications which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see <https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=modified>

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS

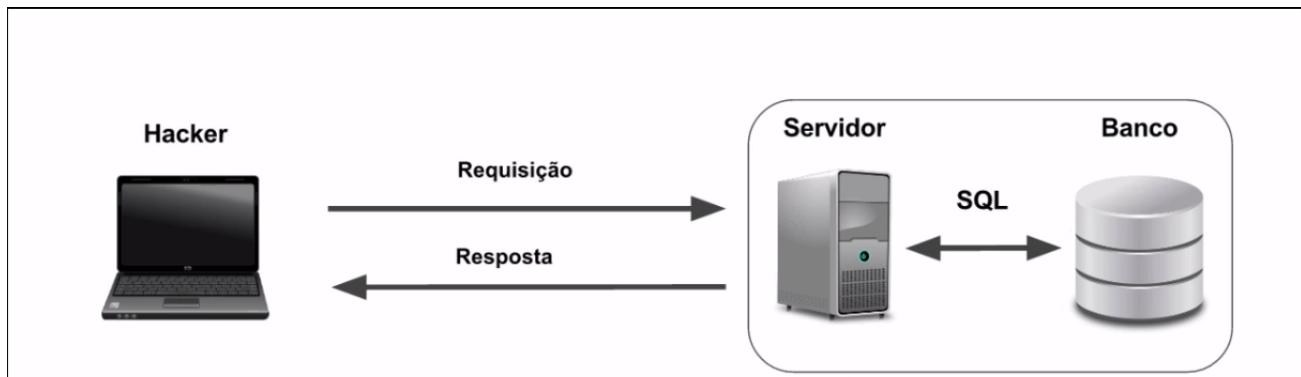
Dando um scroll na página, clicaremos no item OWASP Multillidae II que será o primeiro site vulnerável com que trabalharemos. Teremos o seguinte:

The screenshot shows a web browser window with the URL <http://192.168.1.37/mutillidae/>. The page title is "OWASP Mutillidae II: Web Pwn in Mass Production". It displays a sidebar with links to OWASP 2013, 2010, 2007, Web Services, HTML 5, Others, Documentation, and Resources. Below this is a "Getting Started" section with a document icon. The main content area features several buttons: "Like Mutillidae? Check out how to help" (with a thumbs-up icon), "What Should I Do?" (with a question mark icon), "Help Me!" (with a red button icon), "Bug Tracker" (with a person icon), "Video Tutorials" (with a YouTube icon), and "Listing of vulnerabilities" (with a red lightbulb icon). At the bottom of the page, there's a "Mutillidae: Deliberately Vulnerable Web Pen-Testing Area" banner.

O *security level* dessa página é zero e nesse momento não estamos logados. Portanto, vamos clicar no "*Login register*" e aparecerá uma nova janela que pede usuário e senha. Podemos preencher isso com "Rafael" e "alura" (usuário e senha), por exemplo.

Quando preenchemos as informações e apertamos o botão de login, fazemos uma requisição ao servidor. Isto é, nós passamos para o servidor os parâmetros que estão no usuário e o servidor consulta no banco de dados verificando se o registro existe. Dependendo do que o banco verificar a resposta retornada ao servidor será: existe ou não existe!

A partir disso o servidor dá uma resposta ao usuário (no caso o hacker). Se o acesso for permitido, nós teremos o acesso ao site, caso contrário, receberemos uma mensagem negando. A comunicação que ocorre entre o Servidor e o Banco é feita usando a linguagem SQL. Resumindo:



O que nós faremos para resolver esse problema é induzir o banco a um comportamento indevido, portanto, vamos inserir códigos SQL. Feita essa introdução teórica, vamos retornar ao site. Se nós inserirmos o nome "Rafael" e "alura", como login e senha respectivamente, teremos o acesso negado:

The screenshot shows a login interface with the following elements:

- Back** button with a blue arrow icon.
- Help Me!** button with a red button icon.
- Hints** button with a downward arrow icon.
- Login** button.
- An error message box containing the text "Account does not exist".
- A second error message box containing the text "Please sign-in".
- Input fields for **Username** and **Password**.

A mensagem devolvida afirma que a conta inserida não existe. Podemos interpretar essa mensagem da seguinte maneira: se inserirmos um usuário que existe, mas uma senha incorreta, é esperado uma resposta diferente, pois, a conta vai existir mesmo que a senha esteja errada.

Como podemos realizar o login na máquina se não temos nem a informação do login nem a do usuário? É preciso conhecer um ou outro. No caso do presente exercício, nós temos conhecimento de que o *Username* é `admin`. Ao preencher o usuário como `admin` e a senha como qualquer coisa, nós teremos uma mensagem avisando: *Password incorrect*.

The screenshot shows a login interface with the following elements:

- Username** field containing the value `admin`.
- Password** field.
- Login** button.
- An error message box containing the text "Password incorrect".
- A second error message box containing the text "Please sign-in".

A mensagem que recebemos nos fornece a certeza de que o `admin` existe!

A segunda pergunta que podemos fazer para burlar o sistema é: "será que o desenvolvedor filtra o que pode ser escrito nos campos?" Por exemplo, vamos escrever `admin` e o password nós colocaremos apenas uma aspas simples. As aspas simples delimita *strings* e caracteres permitindo a inserção de códigos SQL para serem interpretados no banco de dados. Então, se o desenvolvedor não previu o uso de aspas simples, podemos verificar a reação:

The screenshot shows a login interface with the following elements:

- Username** field.
- Login** button.
- An error message box containing the text "Exception occurred".
- A second error message box containing the text "Please sign-in".

Essa mensagem avisa que uma exceção aconteceu. Isso significa que o sistema não se comportou da maneira como deveria. Acima, na mesma página, temos as informações do porquê da exceção:

Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	<pre>connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT username FROM accounts WHERE username='admin' AND password=''; (0) [Exception]</pre>
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT username...') #1 /owaspbwa/mutillidae-git/SQLQueryHandler.php(273): MySQLHandler->executeQuery('SELECT username...') #2 /owaspbwa/mutillidae-git/includes/process-login-attempt.php SQLQueryHandler->authenticateAccount('admin', '') #3 /owaspbwa/mutillidae-git/index.php(277): include_once('/owaspbwa/mutil...') #4 {main}
Diagnostic Information	Error querying user account

[Click here to reset the DB](#)

Isso nos informa que ocorreu um erro na sintaxe. Essa falha deve-se às aspas simples que nós inserimos e que não são fechadas. Outra dica é verificar o Manual da SQL. Ainda, ele também nos informa a *query* que vai para o banco de dados.

Com essa *Exception*, foi possível mapear diversas informações! Com isso nós sabemos como a query é construída e qual o banco de dados é utilizado. Em seguida, vamos copiar a *query* e colá-la no banco de notas para analisar com mais tranquilidade. Teremos:

```
SELECT username FROM accounts WHERE username='admin' AND password=''
```

Nós havíamos preenchido de forma incorreta, portanto, vamos deixar representado como `x`. O que pode ser feito diante disso? Nós podemos utilizar as aspas simples para delimitar o caractere e acrescentar uma mensagem que é sempre verdadeira, por exemplo, `a=a`. Como podemos juntar essas duas informações o `x` e o `a=a` de maneira que ambas se tornem verdadeiras? Simples! Nós podemos adicionar o `or`, assim:

```
SELECT username FROM accounts WHERE username='admin' AND password='x' or a=a'
```

Com isso estamos dizendo: a password é `x` ou `a=a`. Desta maneira, não é preciso que as duas sejam verdadeiras, mas apenas uma. Portanto, toda a informação que acabamos de inserir junto a `password` é verdadeira. Ainda, se deixarmos o segundo `a` com apenas uma aspas parece que ele fica aberto e isso acusará um erro sintático. Portanto, é preciso inserir aspas no outro lado dele para que continue igual: `'a'='a'`.

Lembrando que a primeira aspas que está junto do `x` faz parte do sistema e a última que acompanha o segundo `a` também. Teremos:

```
SELECT username FROM accounts WHERE username='admin' AND password='x' or 'a'='a'
```

Vamos verificar se inserirmos `x` ou `'a'='a'` no lugar da senha da página se isso nos permite ter acesso à página. Pois, estaremos preenchendo um `username`, `admin`, que já sabemos ser verdadeiro e uma senha que também é. Vamos testar? Preencheremos o `username` como `admin` e a senha como `x` ou `'a'='a'` e teremos o seguinte:

The screenshot shows a web browser window with the URL <http://192.168.1.37/mutillidae/index.php?popUpNotificationCode=AU1>. The page title is "OWASP Mutillidae II: Web Pwn in Mass Production". The top navigation bar includes links for Home, Logout, Toggle Hints, Show Popup Hints, Toggle Security, Enforce SSL, Reset DB, View Log, and View Captured Data. A banner at the top states "Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Logged In Admin: admin (g0t r00t?)". Below the banner, there's a "Mutillidae: Deliberately Vulnerable Web Pen-Testing Application" section with a "Like Mutillidae? Check out how to help" button and links for "What Should I Do?" and "Video Tutorials". On the left, a sidebar lists "OWASP 2013", "OWASP 2010", "OWASP 2007", "Web Services", and "HTML 5".

Ou seja, estamos logados como admin.

O que fizemos nesse caso foi inserir código SQL para que o banco de dados se comportasse de maneira indevida. Resumindo, inserimos um usuário verdadeiro e uma senha onde o 'a'='a' é verdadeiro. Portanto, com o *username* e o *login* sendo verídicos, nós temos acesso à página restrita do site!