

SEGURANÇA CIBERNÉTICA

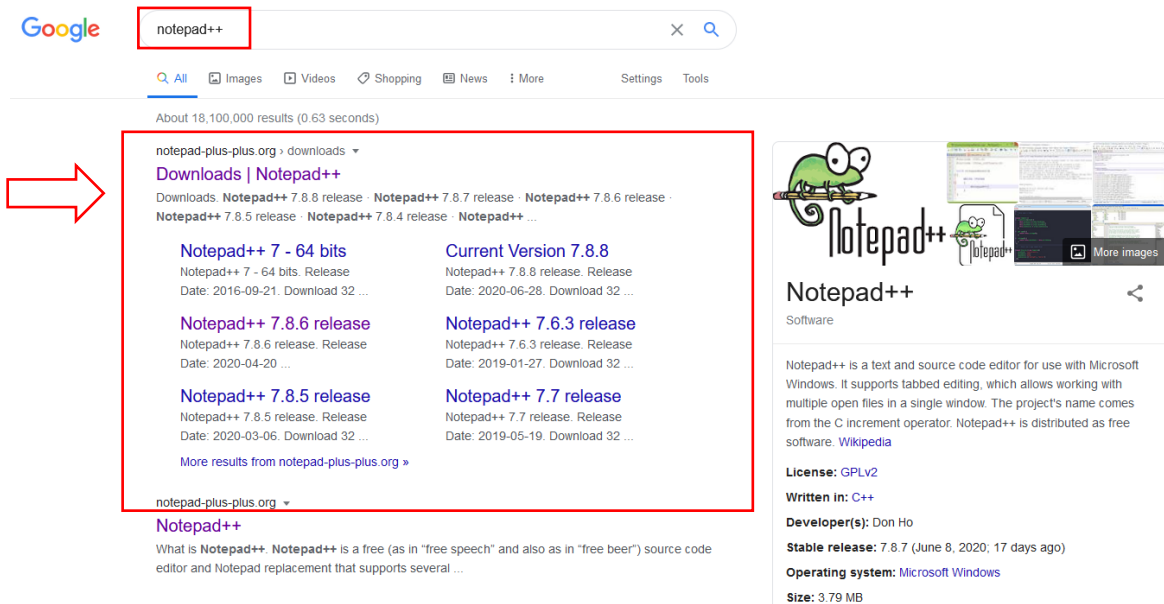
Sumário

Instalar de softwares necessários para realizar o tutorial	2
Notepad++	2
Xampp.....	6
Baixar arquivos para execução do tutorial	11
Manipular pasta www para Injeção de SQL	11
Importar base de dados, para simulação do ataque.....	13
Cadastrar um novo usuário na base de dados	16
Realizar a Injeção SQL no formulário de login.....	20
Brecha de segurança no formulário	21
Prevenir o ataque de Injeção de SQL	22
Corrigir o código para eliminar a falha de segurança.....	23

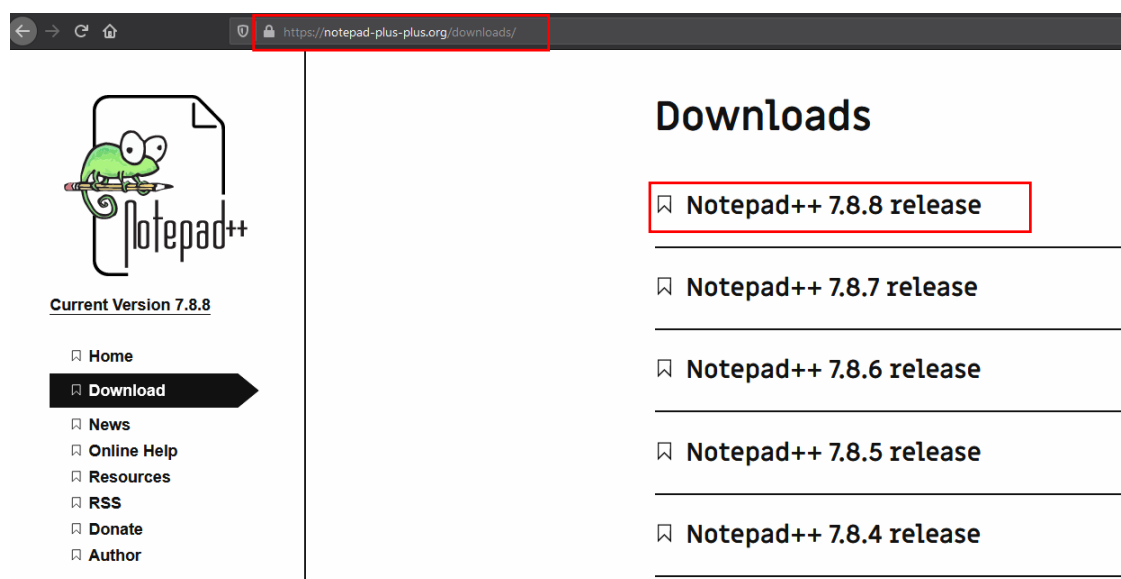
Instalar de softwares necessários para realizar o tutorial

Notepad++

Abre o navegador de sua preferência, entre no Google, e busque por: **notepad++**.




Acesse o primeiro link, se atente para acessar o site oficial do software (**note-plus-plus.org**). Faça o download da última versão disponível. Basta clicar na versão que deseja fazer download.



Ao clicar, você será direcionado para página de download.

Ao clique no botão do download, uma janela de pop-up será aberta solicitando que você salve o arquivo de instalação em seu computador. Salve o arquivo em sua pasta de preferência.

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media partners.




Current Version 7.8.8

- Home
- Download
- News
- Online Help
- Resources
- RSS
- Donate
- Author

Notepad++ 7.8.8 release

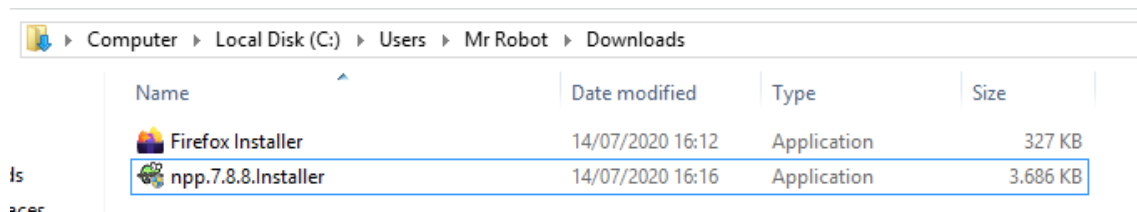
Release Date: 2020-06-28

Download 32-bit x86

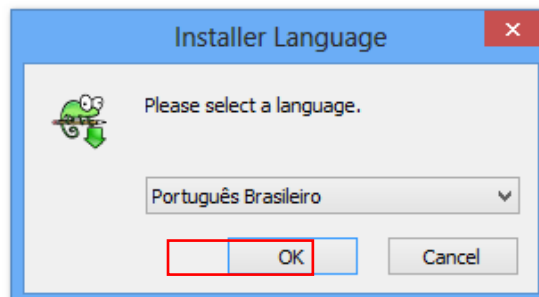


DOWNLOAD

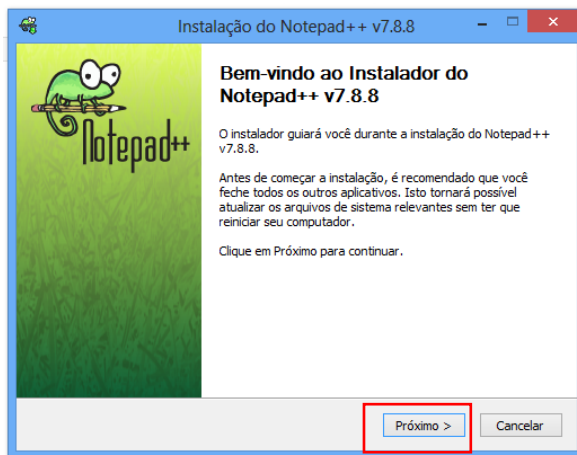
Acesse a pasta onde você salvou o arquivo de instalação e de um duplo clique:



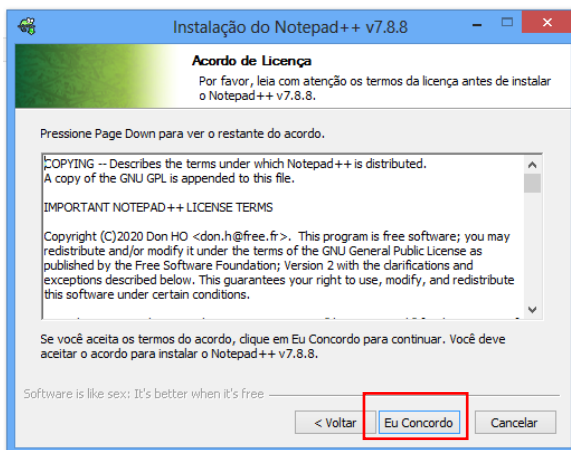
Escolha a opção de idioma **Português Brasileiro** e clique em **OK**.



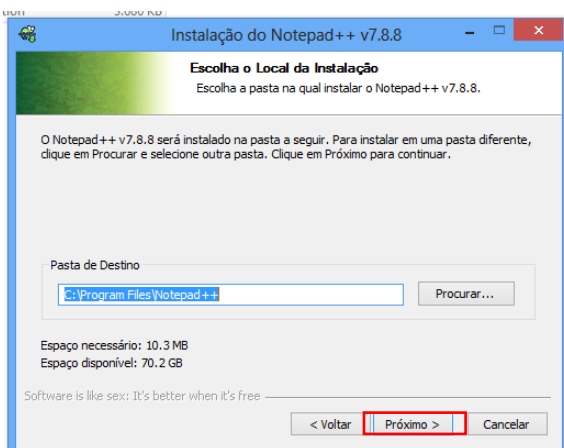
Na janela de instalação do programa, clique em **Próximo**.



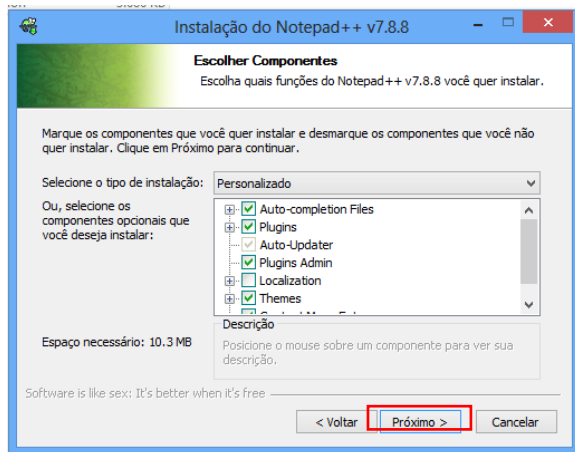
Se concordar com os termos do Acordo de Licença, clique em **Eu Concordo**.



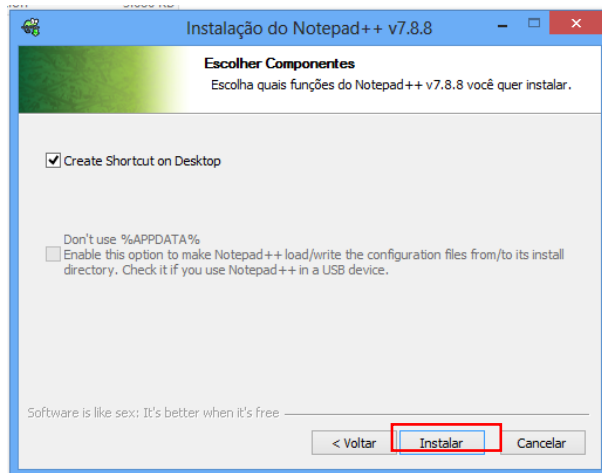
Clique em **Próximo**.



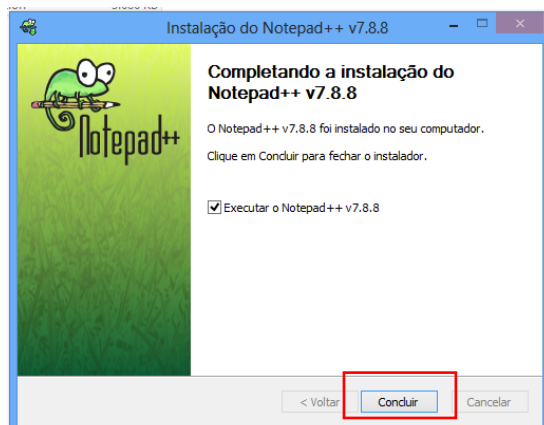
Clique em **Próximo** novamente.



Marque a opção **Create Shortcut on Desktop** e clique em **Instalar**.



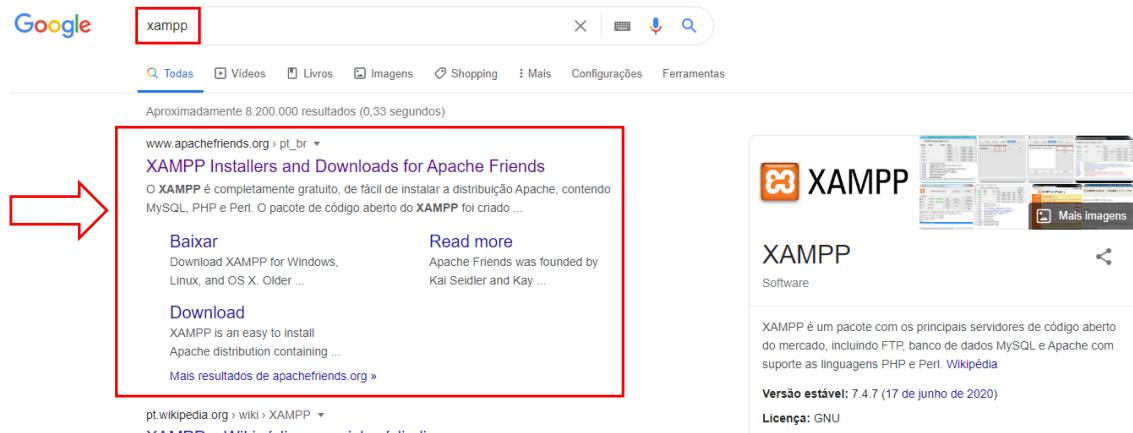
Clique em **Concluir**.



Após o término da instalação, o software será aberto automaticamente. Feche a janela, pois ele não será usado neste momento.

Xampp

Abre o navegador de sua preferência, entre no Google, e busque por **xampp**.

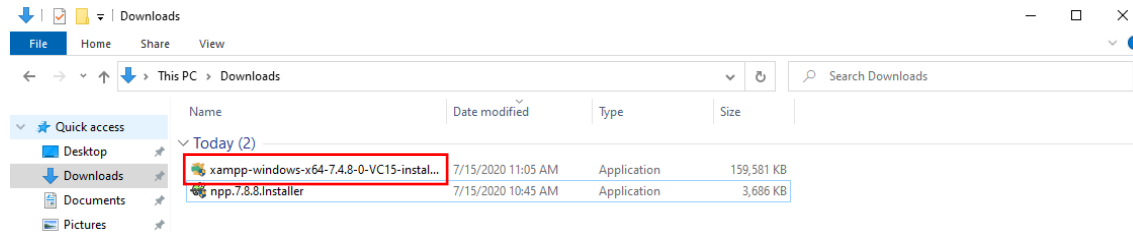


Acesse o primeiro link, se atente para acessar o site oficial do software (**apachefriends.org**). Faça o download da última versão disponível. Neste tutorial, usaremos o **XAMPP para Windows**.

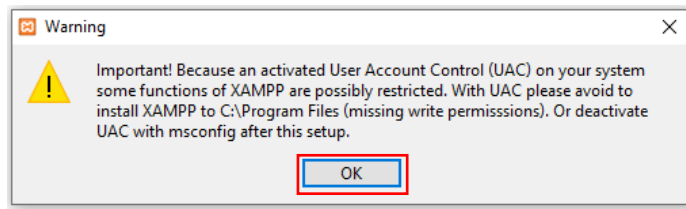


Uma janela de pop-up será aberta pedindo para você salvar o arquivo de instalação em seu computador. Salve-o em uma pasta de sua preferência.

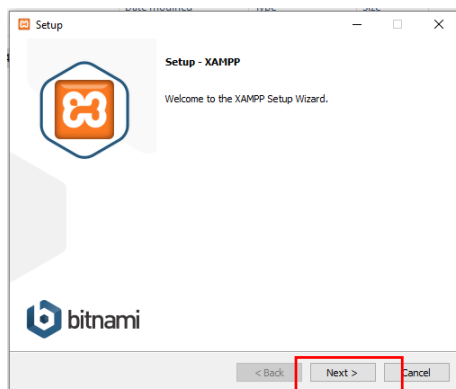
Acesse a pasta onde você salvou o arquivo de instalação, e de um duplo clique sobre o arquivo.



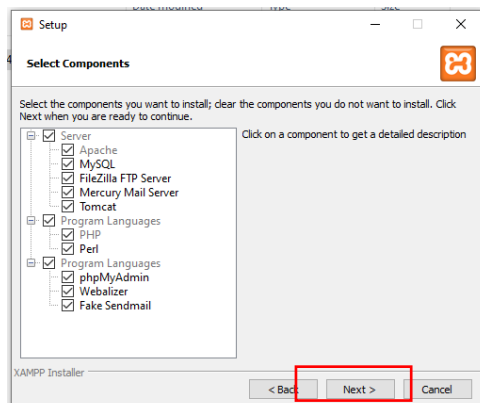
Uma mensagem de pop-up será aberta, apenas clique em **OK**.



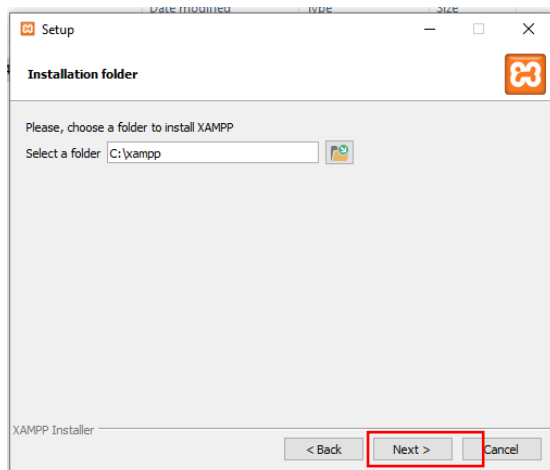
Clique em **Next**.



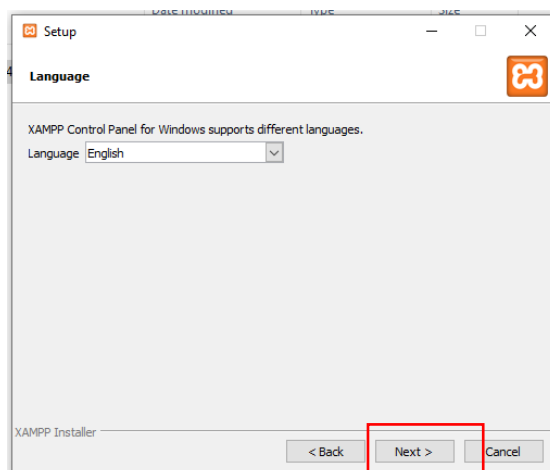
Clique em **Next**.



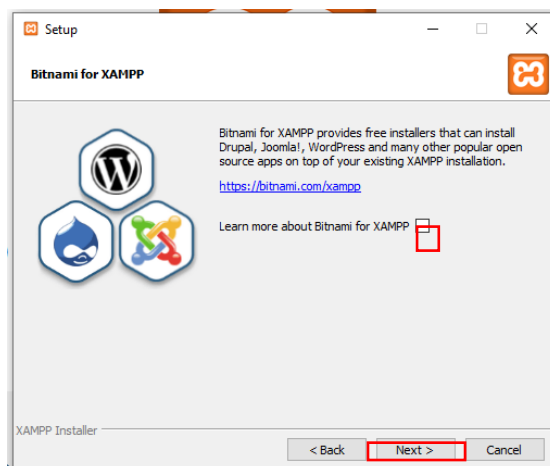
Clique em **Next** novamente.



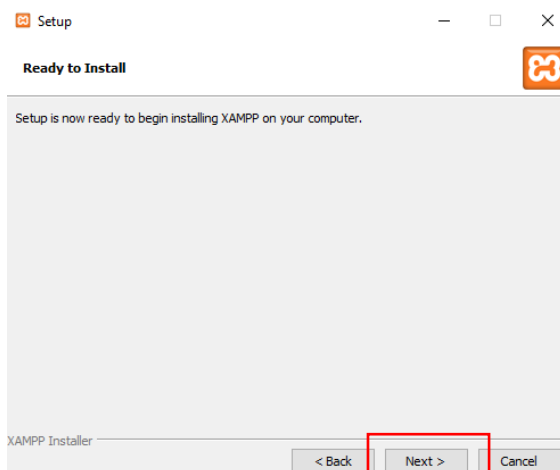
Selecione o idioma e clique em **Next**.



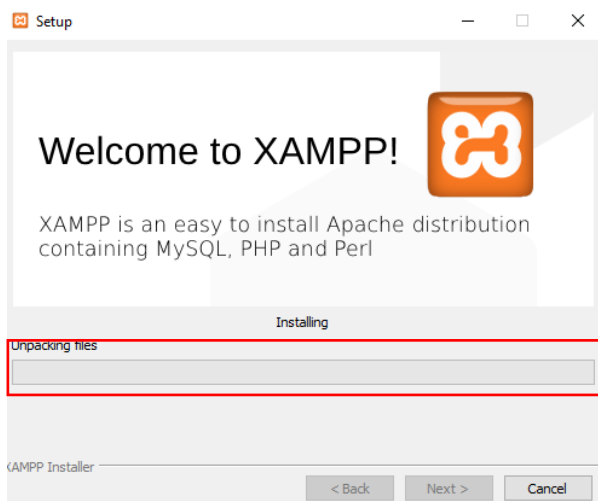
Desmarque a caixa de seleção **Learn more about Bitnami for XAMPP** e clique em **Next**.



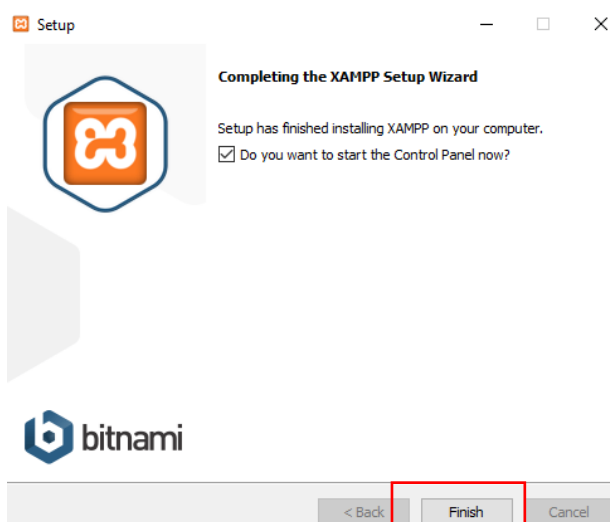
Clique em **Next**.



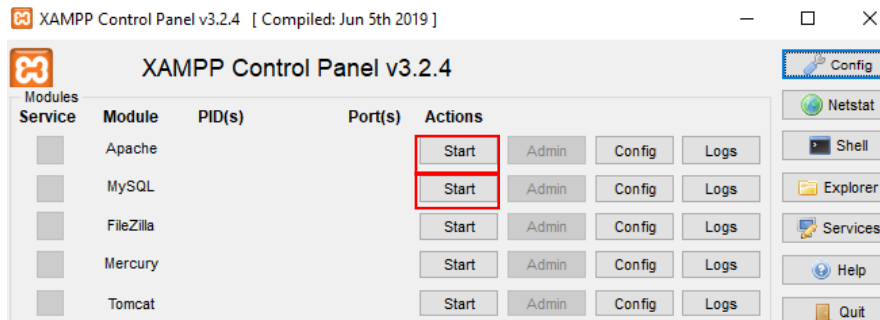
Espere a barra carregar totalmente.



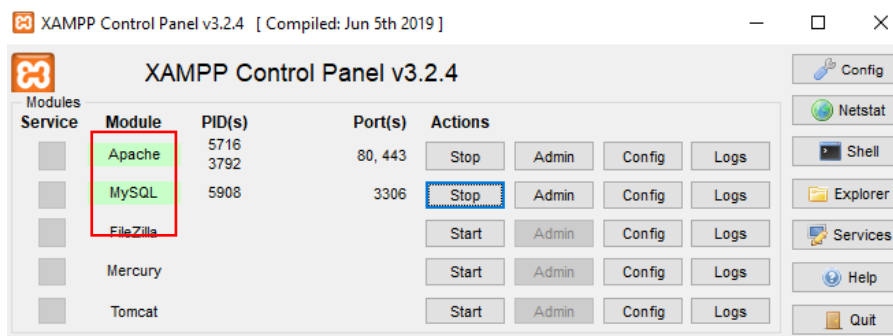
Clique em **Finish**.



Após o término da instalação, o software será aberto. Clique em **Start** nos botões destacados abaixo.

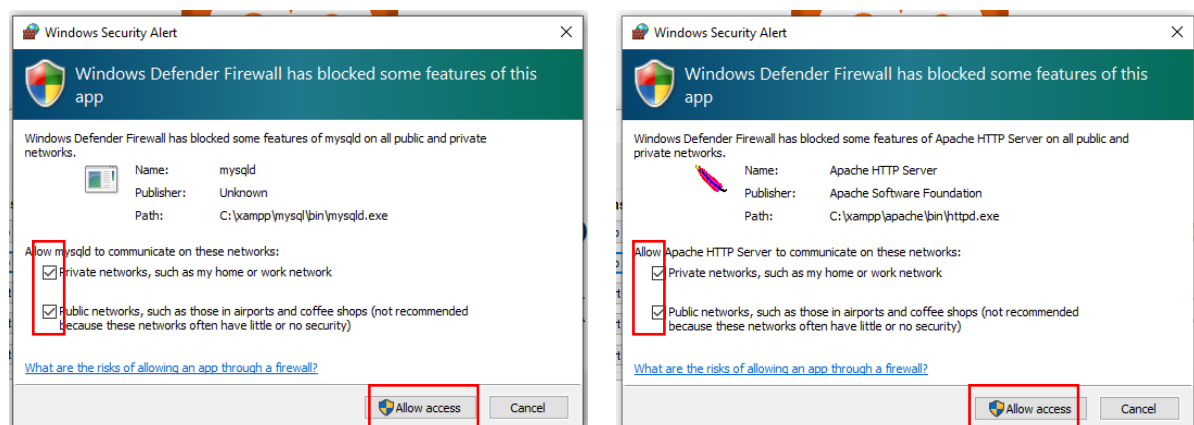


Após clicar nos botões de start, espere até que os serviços sejam carregados. O software sinalizará com a cor verde, conforme destacado.



Duas janelas de pop-up serão abertas solicitando que você permita que os softwares sejam executados em seu computador.

Marque as duas caixas de seleção, e clique em **Allow access**.

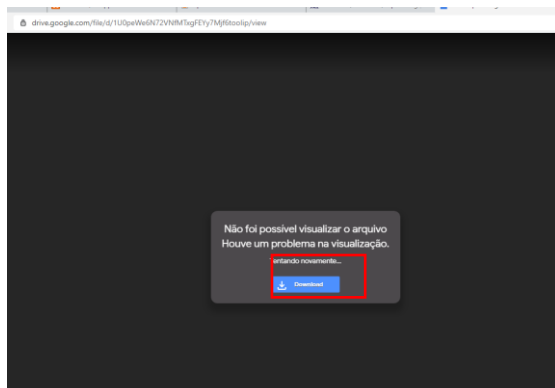


Baixar arquivos para execução do tutorial

Abra o navegador de sua preferência e acesse este link

<https://drive.google.com/file/d/1ULsKsXCQzqoxJfFiPzGW-SNrNHBZzCCK/view?usp=sharing>

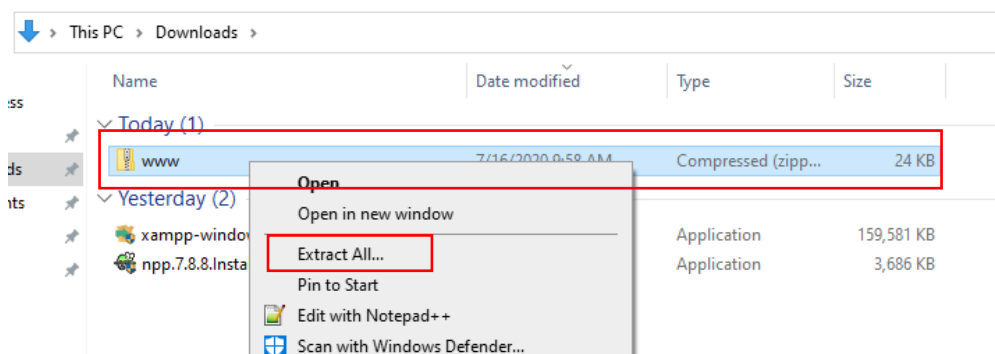
Você fará o download de alguns arquivos para simular a uma invasão SQL (SQL Injection)



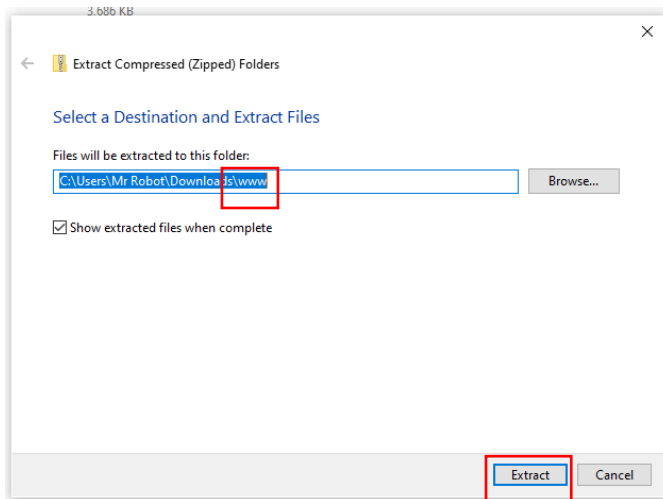
Ao clicar em download. Uma janela de pop-up abrirá solicitando que você salve o arquivo em seu computador. Salve o arquivo em sua pasta de preferência.

Manipular pasta www para Injeção de SQL

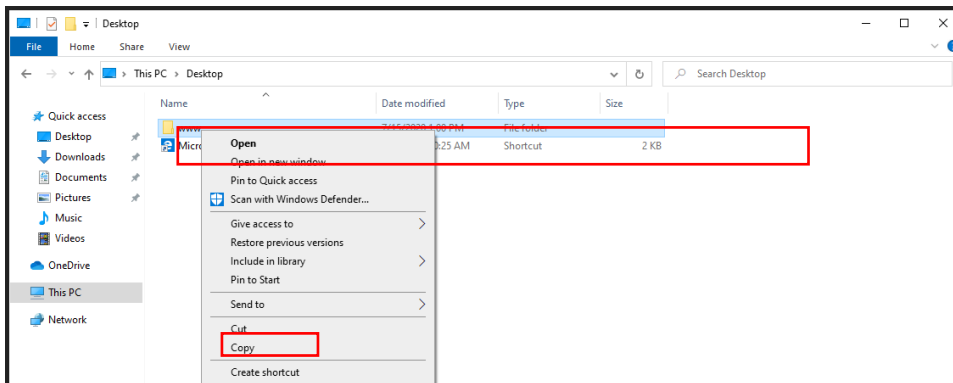
Acesse a pasta onde você salvou o arquivo, clique com o botão direito do mouse e clique na opção em **Extrair tudo**.



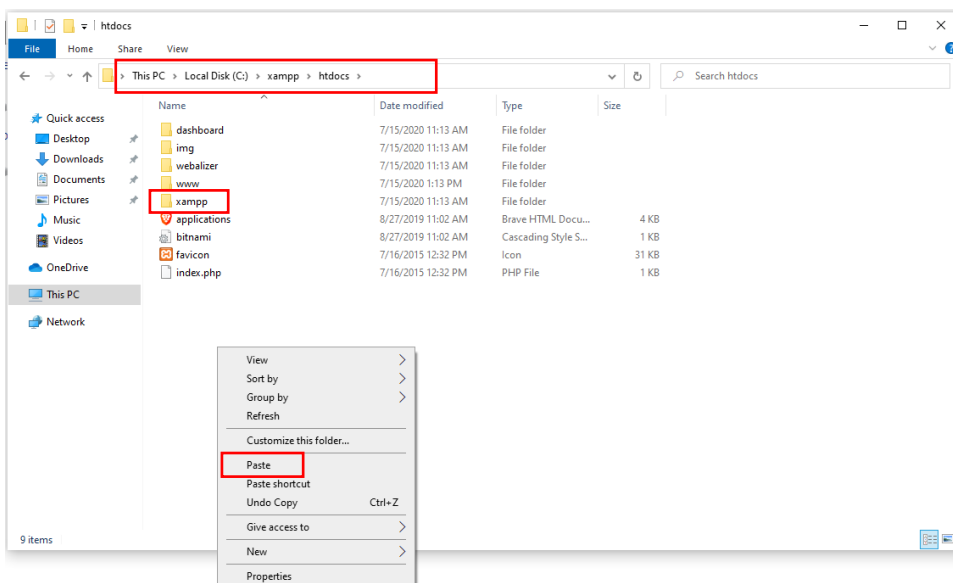
Uma janela de pop-up será aberta. Na barra, delete **www** e clique em **Extract**.



Acesse a pasta onde os arquivos foram extraídos e copie esta pasta.



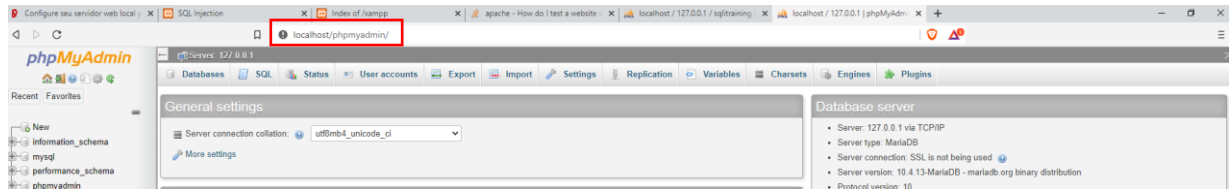
Cole este arquivo na pasta **Meu Computador\Disco Local C:\xampp\htdocs**:



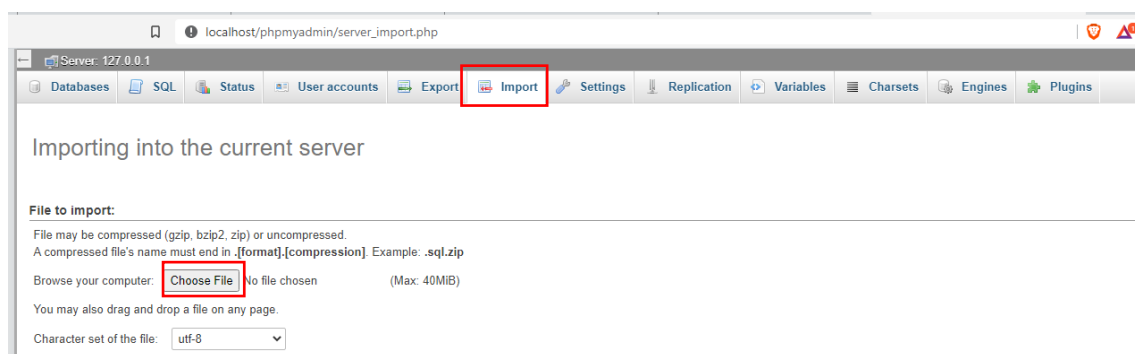
Importar base de dados, para simulação do ataque

Abra seu navegador e, na barra de busca, digite: localhost/phpmyadmin

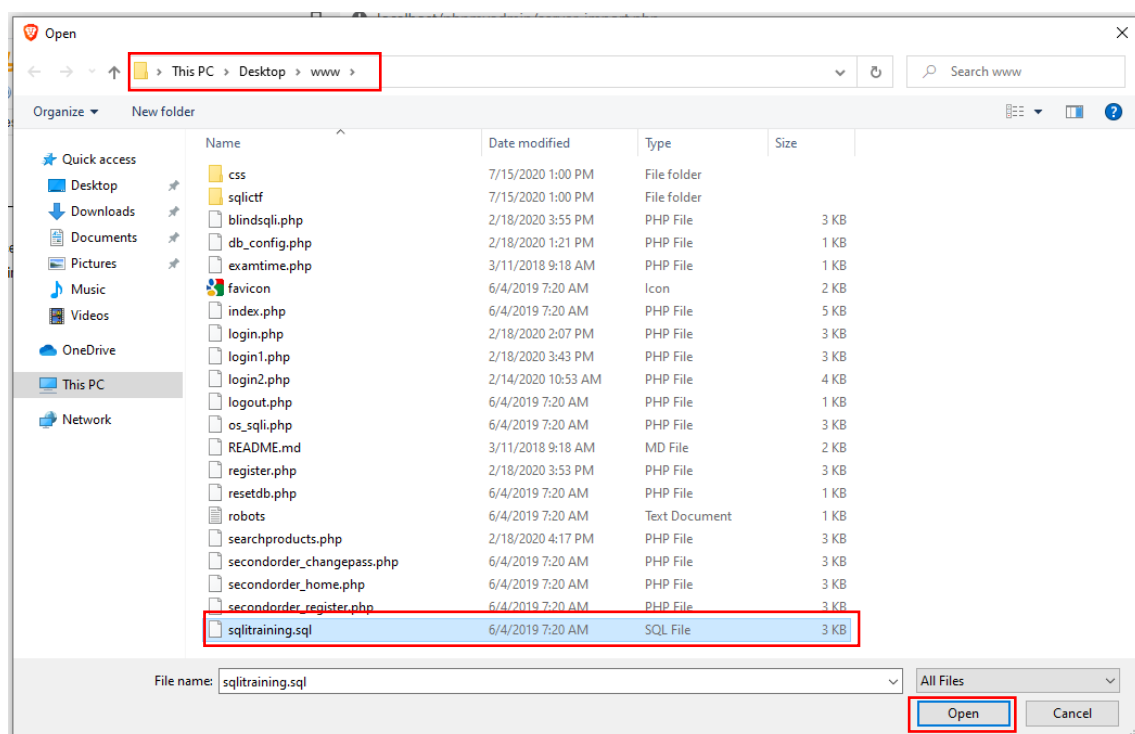
Você será redirecionado para seguinte página:



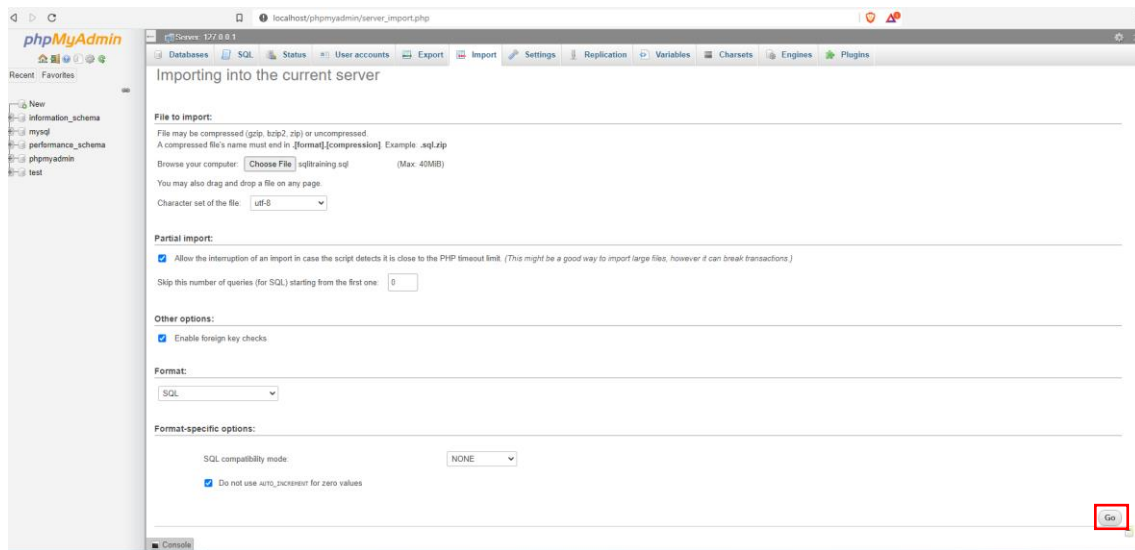
Clique na aba **Import** e em **Choose File**.



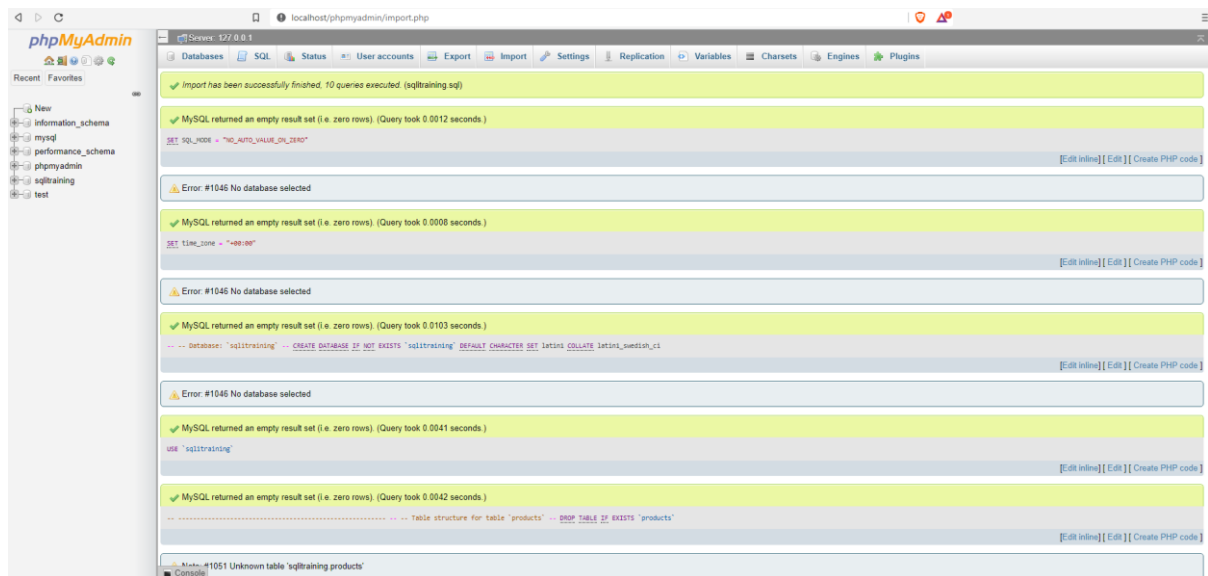
Na janela que será aberta, selecione o arquivo **sqltraining.sql** (Meu Computador\ Disco Local C:\xampp\htdocs). Dê um clique no arquivo indicado e clique em **Open**.



Depois clique em **Go**.

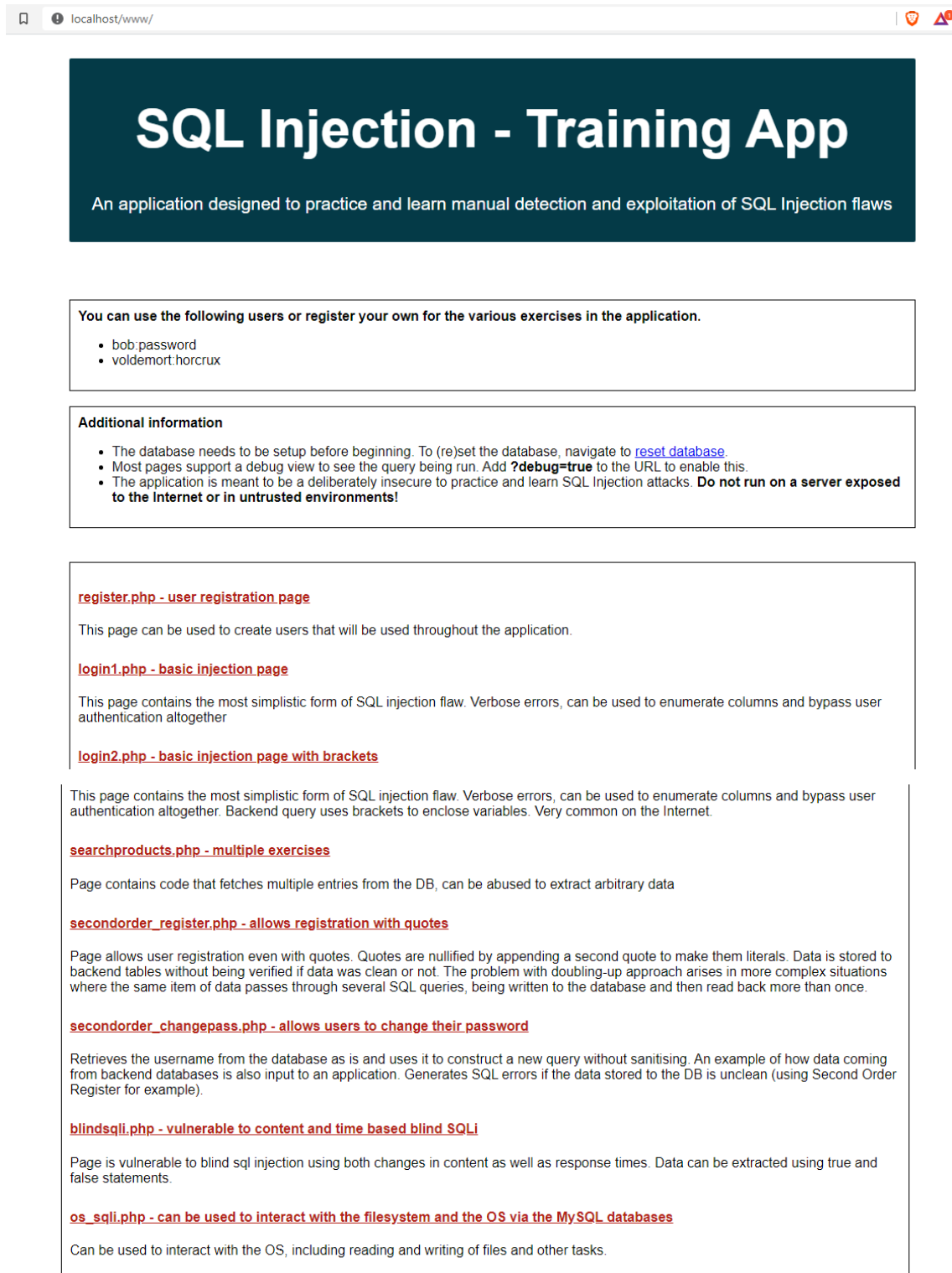


Espere o carregamento do arquivo. Você verá as seguintes mensagens caso o procedimento tenha sido feito de forma correta:



Abra uma nova guia do seu navegador, ou abra uma nova janela e digite **localhost/www/** na barra de busca.

Você será redirecionado para seguinte página:



The screenshot shows a web browser window with the address bar displaying 'localhost/www/'. The main content area has a dark blue header with the title 'SQL Injection - Training App' in white. Below the title, a subtitle reads: 'An application designed to practice and learn manual detection and exploitation of SQL Injection flaws'.

Below the header, there are several sections of text:

- You can use the following users or register your own for the various exercises in the application.**
 - bob:password
 - voldemort:horcrux
- Additional information**
 - The database needs to be setup before beginning. To (re)set the database, navigate to [reset database](#).
 - Most pages support a debug view to see the query being run. Add **?debug=true** to the URL to enable this.
 - The application is meant to be a deliberately insecure to practice and learn SQL Injection attacks. **Do not run on a server exposed to the Internet or in untrusted environments!**
- [register.php - user registration page](#)**

This page can be used to create users that will be used throughout the application.
- [login1.php - basic injection page](#)**

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether
- [login2.php - basic injection page with brackets](#)**

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether. Backend query uses brackets to enclose variables. Very common on the Internet.
- [searchproducts.php - multiple exercises](#)**

Page contains code that fetches multiple entries from the DB, can be abused to extract arbitrary data
- [secondorder_register.php - allows registration with quotes](#)**

Page allows user registration even with quotes. Quotes are nullified by appending a second quote to make them literals. Data is stored to backend tables without being verified if data was clean or not. The problem with doubling-up approach arises in more complex situations where the same item of data passes through several SQL queries, being written to the database and then read back more than once.
- [secondorder_changepass.php - allows users to change their password](#)**

Retrieves the username from the database as is and uses it to construct a new query without sanitising. An example of how data coming from backend databases is also input to an application. Generates SQL errors if the data stored to the DB is unclean (using Second Order Register for example).
- [blindsqli.php - vulnerable to content and time based blind SQLi](#)**

Page is vulnerable to blind sql injection using both changes in content as well as response times. Data can be extracted using true and false statements.
- [os_sqli.php - can be used to interact with the filesystem and the OS via the MySQL databases](#)**

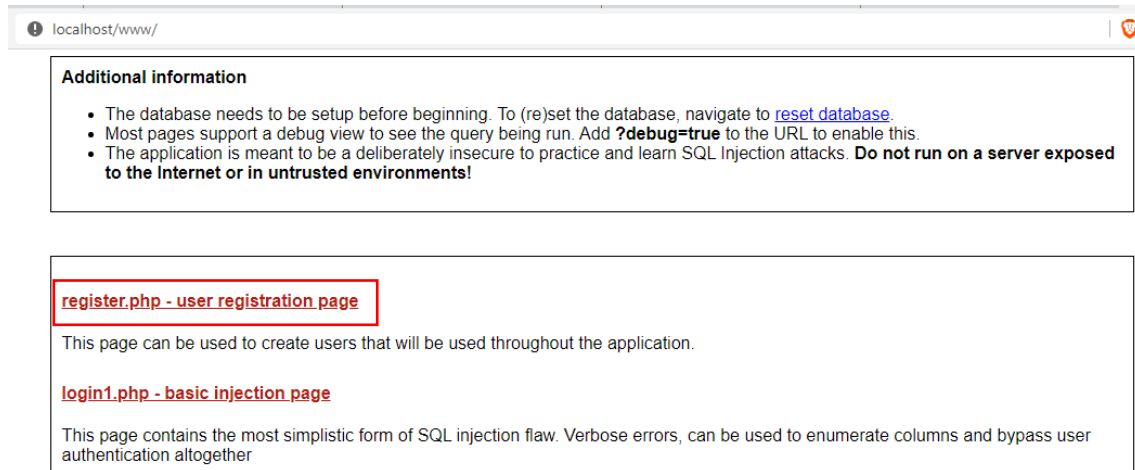
Can be used to interact with the OS, including reading and writing of files and other tasks.

Observe que você está dentro de um ambiente local, apropriado para fazer a Injeção de SQL. Este site contém brechas de segurança no código para que seja possível realizar o ataque de SQL.

Obs.: É possível que haja outros sites com esta brecha de segurança. Caso encontre esta falha em algum site online, é recomendável que entre em contato com a empresa de desenvolvimento e a informe sobre o erro.

Cadastrar um novo usuário na base de dados

Clique em **register.php** – user registration page



Additional information

- The database needs to be setup before beginning. To (re)set the database, navigate to [reset_database](#).
- Most pages support a debug view to see the query being run. Add **?debug=true** to the URL to enable this.
- The application is meant to be a deliberately insecure to practice and learn SQL Injection attacks. **Do not run on a server exposed to the Internet or in untrusted environments!**

register.php - user registration page

This page can be used to create users that will be used throughout the application.

login1.php - basic injection page

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether

Você será redirecionado para seguinte página:



Registro de usuários

Digite seu apelido:
 Digite uma senha:
 Digite o seu nome:

Descrição do seu perfil:

Enviar Limpar

Crie um usuário. Preencha todos os campos necessários. Como você estará em um servidor local, os dados nele inseridos não serão salvos e nem disponibilizados na web. Após preencher todos os campos, clique no botão **Enviar**.


Você será redirecionado para seguinte página:



The screenshot shows a web browser at the URL `localhost/www/searchproducts.php`. The page has a dark teal header with the text "Bem vindo senai!! Procure por produtos aqui". Below this is a search bar with the placeholder text "Procure por um produto:" followed by an input field and a "Busque!" button. Under the search bar is a table with four columns: "Nome do Produto", "Tipo do produto", "Descrição", and "Preço (R\$)". Below the table are links for "Perfil", "Logout", and "Home". At the bottom, there is a footer with the text "SENAI | Indústria 4.0 | Pós Graduação".

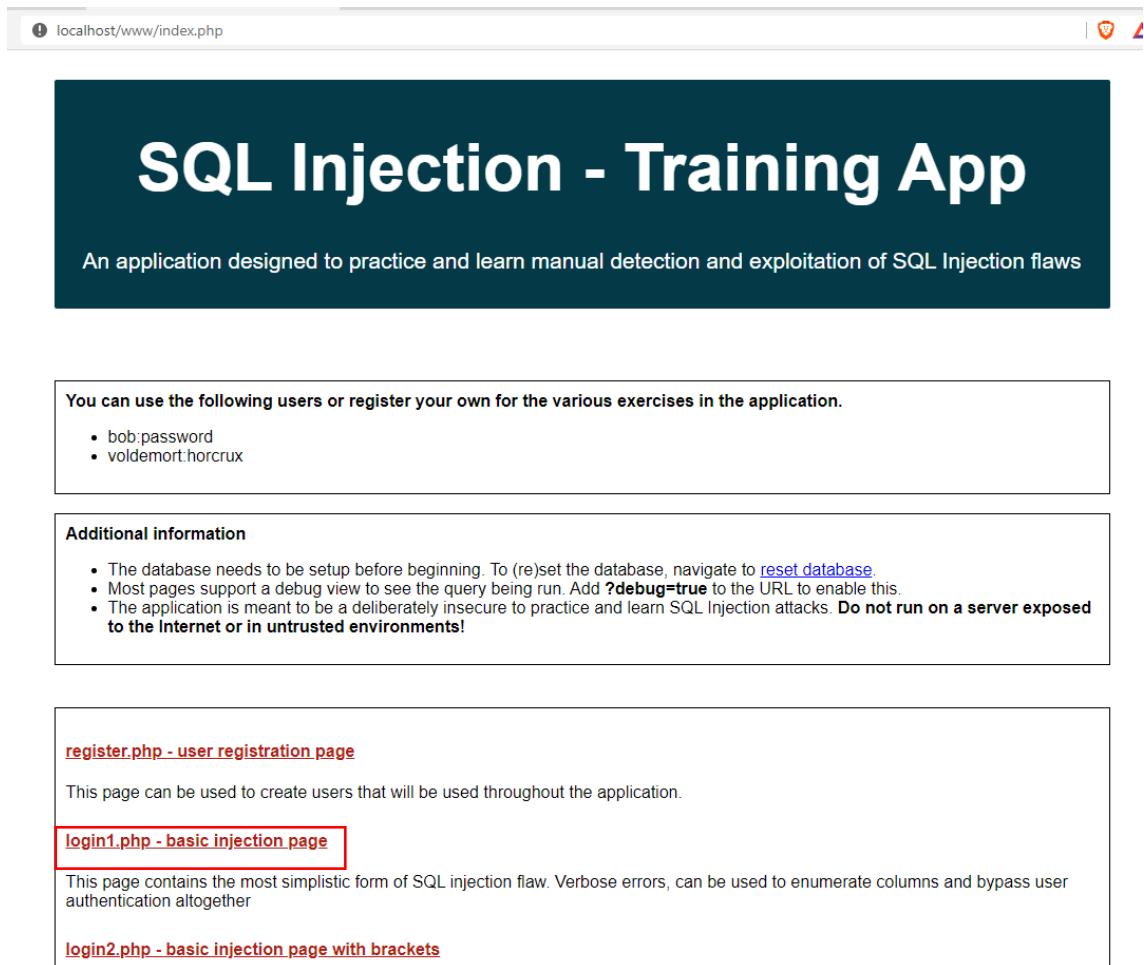
Depois de criar seu usuário e senha, você automaticamente entrará no sistema. Observe que não existem produtos cadastrados na base de dados. Este sistema nada mais é que um banco de dados de itens de supermercado.

Após este passo, clique em **Logout**.



This screenshot is identical to the previous one, showing the search products page. However, the "Logout" link in the navigation bar is highlighted with a red rectangular box.

Clique em **login1.php – basic injection page**.



localhost/www/index.php

SQL Injection - Training App

An application designed to practice and learn manual detection and exploitation of SQL Injection flaws

You can use the following users or register your own for the various exercises in the application.

- bob:password
- voldemort.horcrux

Additional information

- The database needs to be setup before beginning. To (re)set the database, navigate to [reset database](#).
- Most pages support a debug view to see the query being run. Add **?debug=true** to the URL to enable this.
- The application is meant to be a deliberately insecure to practice and learn SQL Injection attacks. **Do not run on a server exposed to the Internet or in untrusted environments!**

[register.php - user registration page](#)

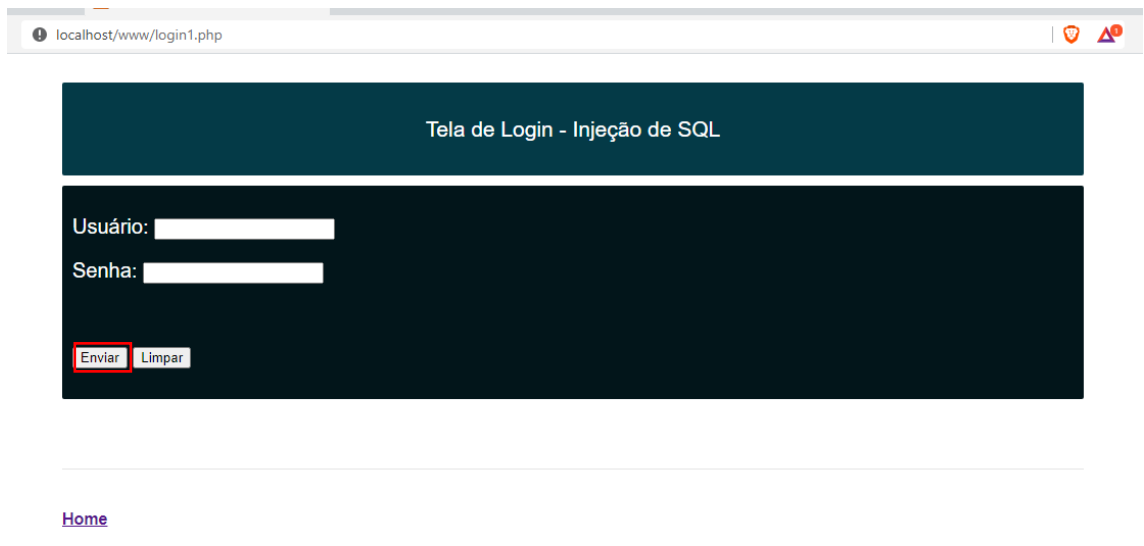
This page can be used to create users that will be used throughout the application.

[login1.php - basic injection page](#)

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether

[login2.php - basic injection page with brackets](#)

Faça login na página com a conta e senha que você criou no passo anterior.



localhost/www/login1.php

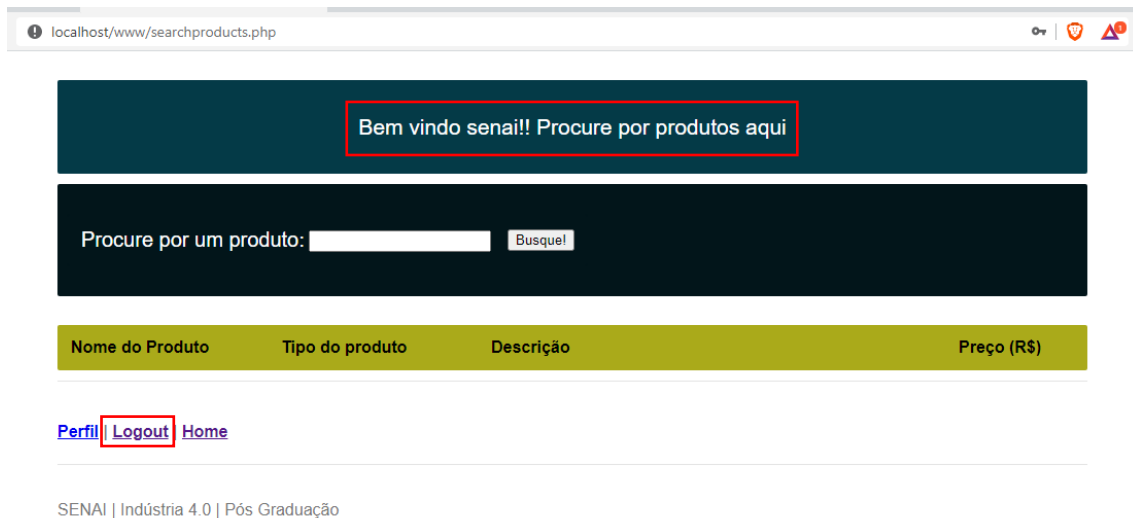
Tela de Login - Injeção de SQL

Usuário:

Senha:

[Home](#)

Após preencher os campos, e clicar em enviar, você entrará novamente no sistema.



localhost/www/searchproducts.php

Bem vindo senai!! Procure por produtos aqui

Procure por um produto:

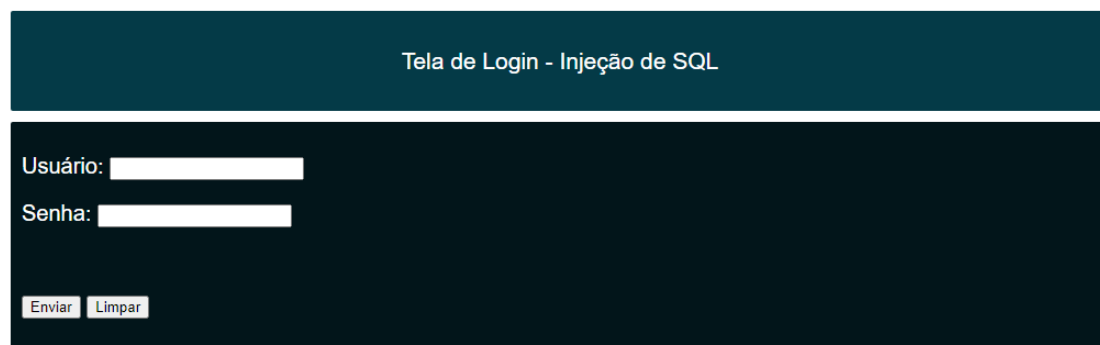
Nome do Produto	Tipo do produto	Descrição	Preço (R\$)
Perfil Logout Home			

SENAI | Indústria 4.0 | Pós Graduação

Fizemos este passo apenas para demonstrar que o usuário criado poderia entrar no sistema, uma vez que criou login e senha.

Você poderá voltar a página de login e tentar acessar a página com outro login e senha, para confirmar que não conseguirá entrar no sistema. O sistema irá notificar que você colocou a uma senha errada.

Clique em: “Home”, para voltar a página principal e inserir o código SQL para burlar a página de login.



Tela de Login - Injeção de SQL

Usuário:

Senha:

Invalid password!

[Home](#)

SENAI | Indústria 4.0 | Pós Graduação

Clique no tópico destacado para voltar a página de login.

[login1.php - basic injection page](#)

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether

Realizar a Injeção SQL no formulário de login

Copie e cole no campo **Usuário** um dos dois comandos listados abaixo.

asd' or 1=1 -- //

- ' OR 1=1 -- //

Clique em **Enviar**.

Tela de Login - Injeção de SQL

Usuário:
 Senha:

[Home](#)

SENAI | Indústria 4.0 | Pós Graduação

Observe que você entrou no sistema novamente. Mas desta vez, por meio de um código (SQL).

Bem vindo admin!! Procure por produtos aqui

Procure por um produto:

Nome do Produto	Tipo do produto	Descrição	Preço (R\$)
-----------------	-----------------	-----------	-------------

[Perfil](#) | [Logout](#) | [Home](#)

SENAI | Indústria 4.0 | Pós Graduação

Brecha de segurança no formulário

Isto ocorre **porque**:

Ao preencher o campo de usuário e senha, a aplicação web dispara uma consulta na tabela “USERS” (base de dados) para confirmação do cadastro do usuário.

Se um registro for encontrado, o username (usuário) será retornado e esta é a confirmação de que o usuário foi encontrado na base de dados e pode se autenticar na plataforma.

Se a consulta na tabela “USERS” não retornar registros, o usuário não será autenticado, e não entrará no sistema. Você confirmou este procedimento, ao tentar logar com um usuário e senha não cadastrados na plataforma.

O principal problema do código da tela de login em PHP é o trecho responsável pela montagem do comando SQL que será executado abaixo:

```
$q = "SELECT * FROM users where username='".$username.'" AND password =  
''.md5($pass).''";
```

Este código é problemático porque não realiza nenhum tipo de validação nos dados que foram digitados pelo usuário. Isso permite que um usuário mal intencionado consiga “burlar” a digitação dos campos de login e senha informando os seguintes parâmetros na tela de login

```
- ' OR 1=1 -- //
```

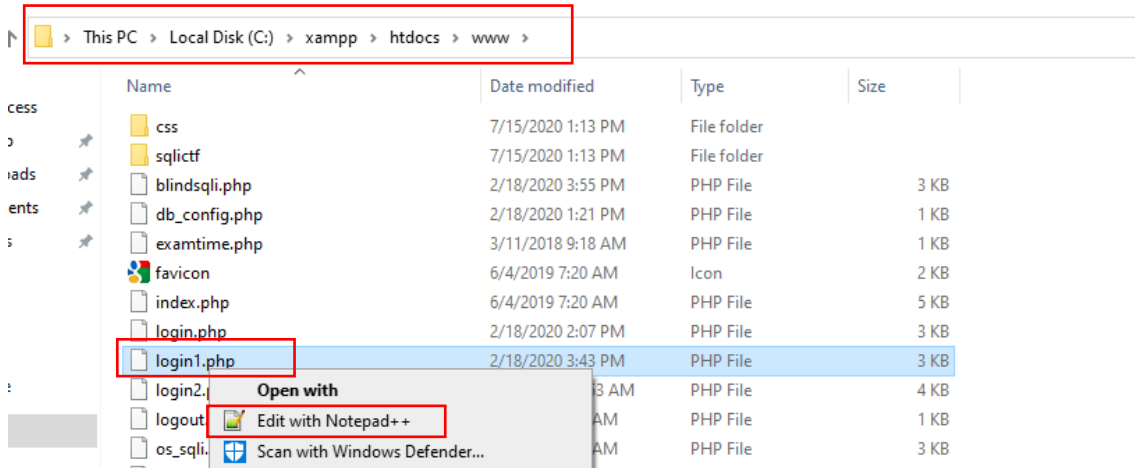
No trecho do código acima o usuário mal intencionado será autenticado com sucesso pois a sequência de caracteres “--” faz com que todo o restante do comando após esta sequência seja considerado como comentário. O comando será executado sem retornar erros, pois o código “'' AND password = '' .md5(\$pass).''”; não será processado.

Prevenir o ataque de Injeção de SQL

O erro se encontra no código php. Você fará a correção deste trecho do código.

Para isto acesse o arquivo **login1.php** (Meu Computador > Disco Local C > xampp > htdocs > www > htdocs > www >)

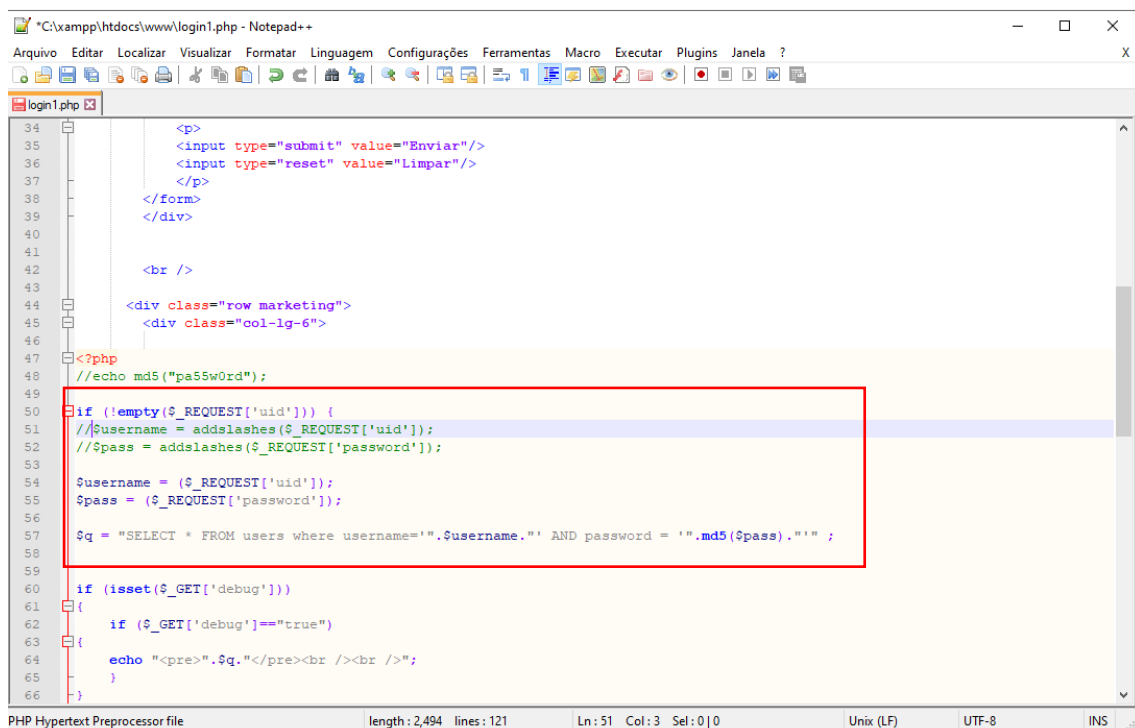
Clique com o botão direito do mouse, e escolha a opção **Editar com Notepad++**.



Na linha 51, remova "/" do trecho do código

Na linha 52, remova "/" do trecho do código

Comente as linhas 54 e 55 com "//"



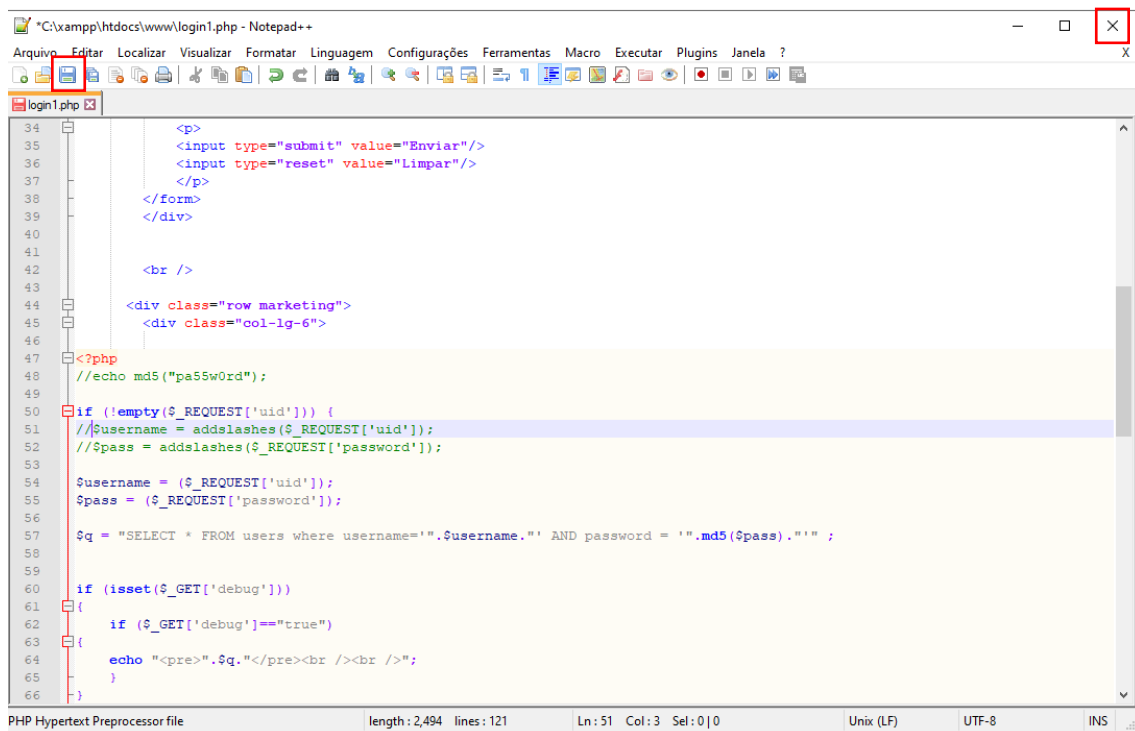
O código deverá ficar da seguinte forma:

```
<?php
//echo md5("pa55w0rd");

if (!empty($_REQUEST['uid'])) {
    $username = addslashes($_REQUEST['uid']);
    $pass = addslashes($_REQUEST['password']);

    // $username = ($_REQUEST['uid']);
    // $pass = ($_REQUEST['password']);
}
```

Clique no disquete, para salvar o arquivo e feche a janela.



Corrigir o código para eliminar a falha de segurança

O que você fez foi simplesmente utilizar a função addslashes nos campos de usuário e senha, essa função adiciona barras invertidas a uma string.

Isso faz com que o comando: "- ' OR 1=1 -- //" não consiga burlar o campo de usuário e não permite que a senha seja comentada, não possibilitado que o invasor entre no sistema sem digitar uma senha válida.

Para validação, você poderá repetir os procedimentos de criar um usuário, e se autenticar no sistema por meio da página de login. Ou fazer o login com o usuário e senha criados no início do tutorial.

Por fim, inserir os códigos de SQL listados abaixo no campo de usuário.

asd' or 1=1 -- //

- ' OR 1=1 -- //

Para isto acesse novamente a página de login. Preencha os campos, e clique em **Enviar**.

login1.php - basic injection page

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether

Tela de Login - Injeção de SQL

Usuário:

Senha:

Observe que você entrou no sistema. Agora você pode clicar em **Logout** para sair do sistema.

Bem vindo senai!! Procure por produtos aqui

Procure por um produto:

Nome do Produto	Tipo do produto	Descrição	Preço (R\$)
-----------------	-----------------	-----------	-------------

[Perfil](#) [Logout](#) [Home](#)

Acesse novamente a página de login.

`login1.php - basic injection page`

This page contains the most simplistic form of SQL injection flaw. Verbose errors, can be used to enumerate columns and bypass user authentication altogether

E tente fazer a injeção de SQL.

Tela de Login - Injeção de SQL

Usuário:

Senha:

Invalid password!

[Home](#)

SENAI | Indústria 4.0 | Pós Graduação

Observe que você não obteve sucesso desta vez, e o sistema retornou uma mensagem informando que a senha está incorreta.

Você finalizou este tutorial. Caso queira, poderá remover os programas instalados em seu computador e apagar os arquivos baixados do Google Drive.