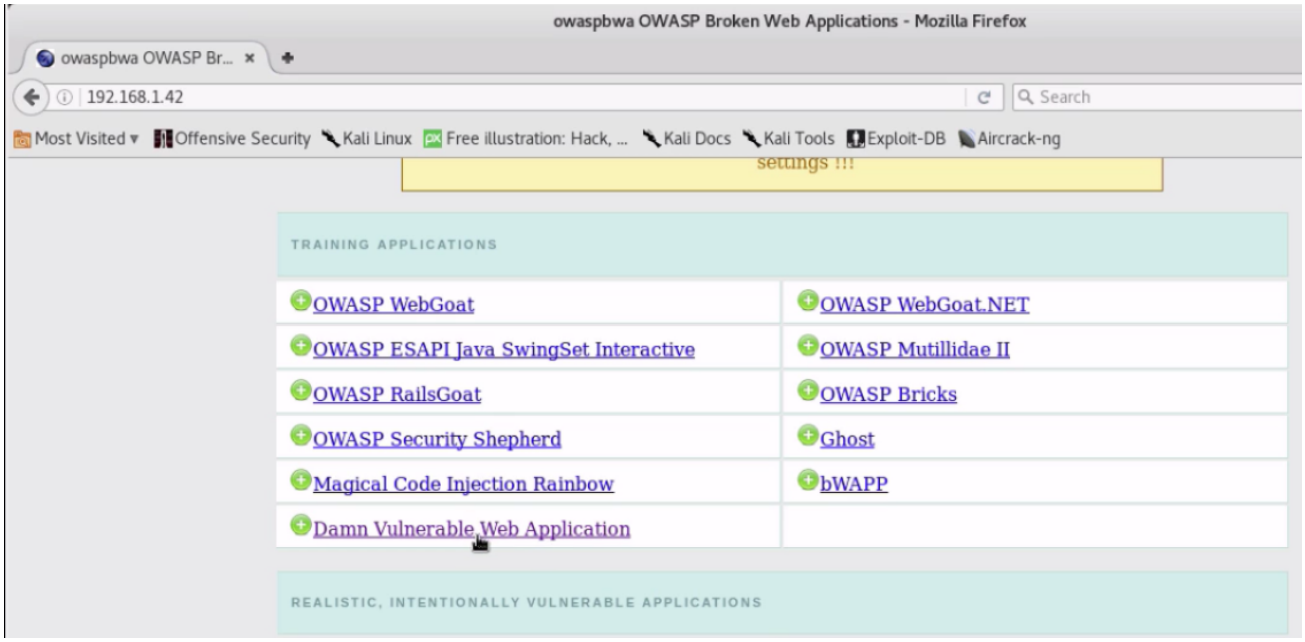
05

Upload de arquivos

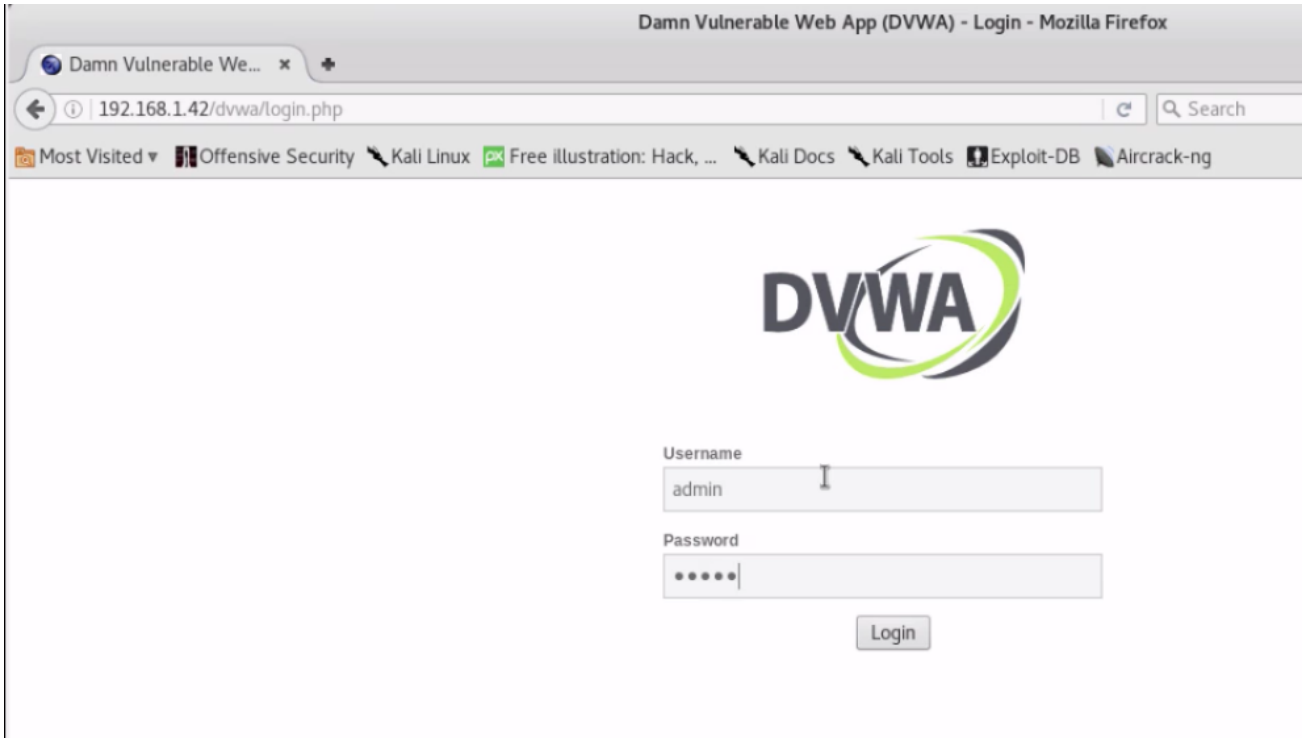
Transcrição

Vamos aprender a fazer o mapeamento do servidor!

Para tanto, acessamos o site "Damn Vulnerable Web Application" usando o endereço IP do *Multillidae*, o `192.168.1.42` (como trocamos a máquina, o endereço acabou se alterando). Nesta página, vamos acessar o link clicando no seguinte ícone:



Somos redirecionados para a seguinte página:



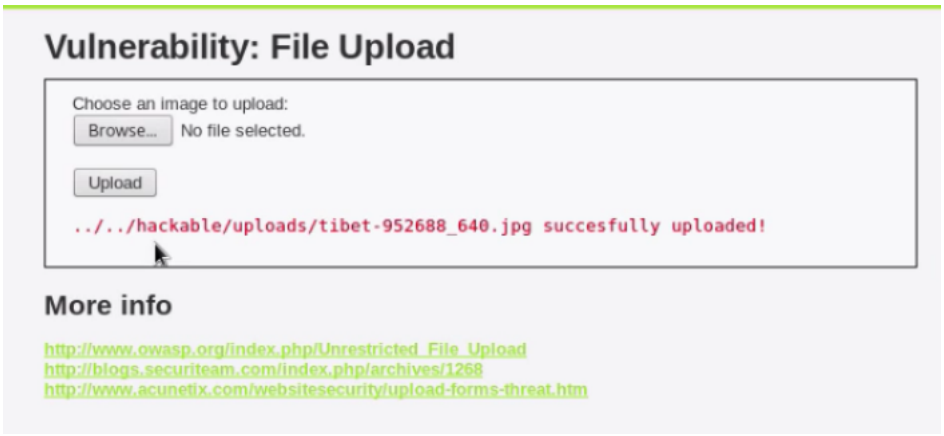
Quando acessamos um site e fazemos o **upload** de uma imagem, por exemplo, é normal que apareça uma mensagem dizendo que a tarefa foi realizada com sucesso ou não. Inclusive, às vezes, é descrito o caminho em que a imagem foi

salva e é justamente isso que buscamos.

Ao acessar o site podemos verificar, ao final da página, qual o nível de segurança do presente link. Ele deve estar demarcado como *low* e caso o nível esteja definido de outra maneira podemos modificá-lo por meio do "DWVA Security":

Estamos acessando a página como usuário comum e a primeira ação que faremos é o *upload* de uma imagem. Portanto, no menu que encontra-se à esquerda, selecionaremos o item "Upload" e depois, escolheremos a imagem desejada:

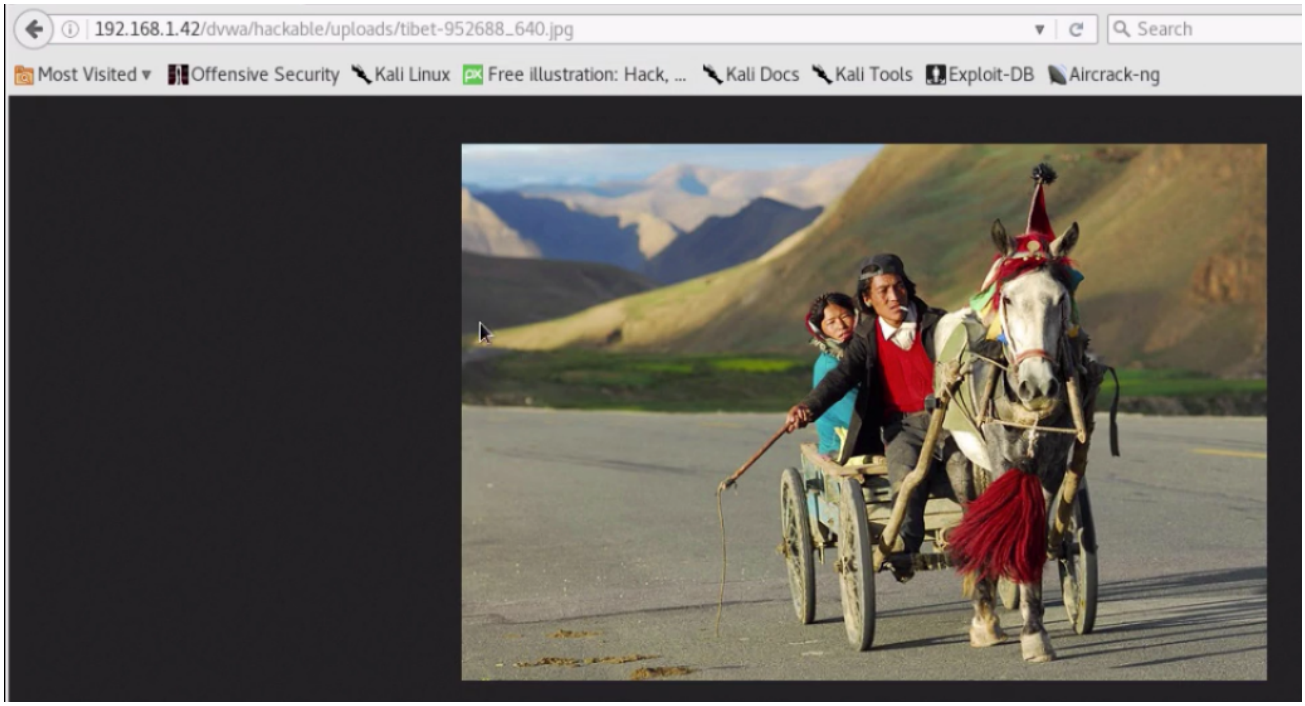
Teremos o seguinte:



A mensagem que aparece nos informa que a imagem foi salva e também onde ela foi guardada. Repare no `../`, isso significa que devemos retornar dois diretórios, o que fazemos à mão. Com o caminho arrumado podemos copiá-lo e colá-lo no navegador, teremos a URL abaixo.

```
192.168.1.42/dvwa/hackable/uploads/tibet-952688_640.jpg
```

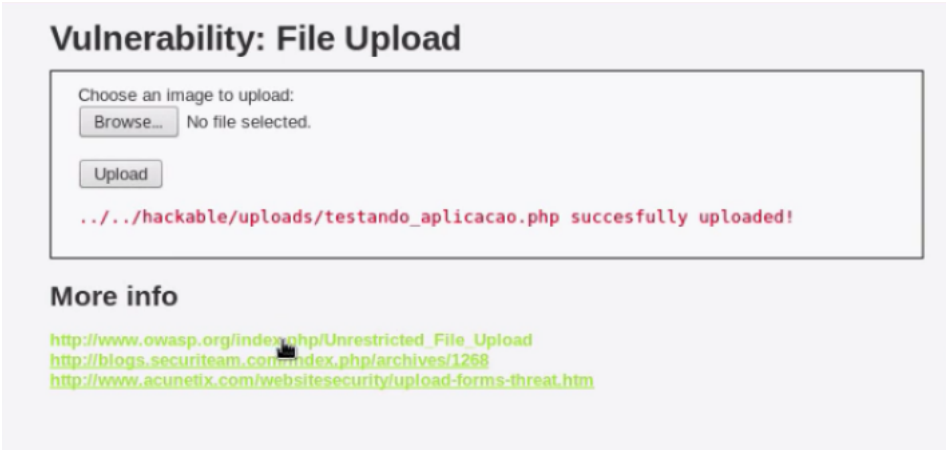
Ao digitarmos isso temos acesso a imagem!



Vamos testar o *upload* de uma imagem que contenha junto de si um código. Primeiro, criaremos um arquivo `php`, para tanto, abriremos o editor de texto `nano` e inserimos o nome do arquivo, `testando_aplicacao.php`. No Terminal teremos: `nano testando_aplicacao.php`. Feito isso podemos inserir um código `php` simples:

```
<?php echo ("Meu codigo PHP foi aceito pela aplicacao"); ?>
```

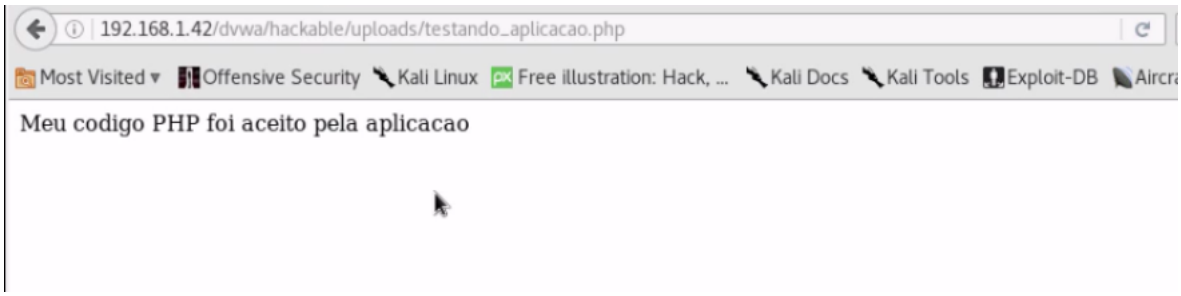
Agora, vamos verificar se o sistema aceita o arquivo da imagem que contenha o `php`. Retornamos ao site e faremos um *upload* do arquivo modificado:



Perceba que ele aceita a imagem e a carrega com sucesso. Vamos copiar a URL que aparece na página e verificar se conseguimos acessá-la usando o navegador. Utilizaremos a seguinte URL:

```
192.168.1.42/dvwa/hackable/uploads/testando_aplicacao.php
```

Dando um "Enter" temos a seguinte mensagem:

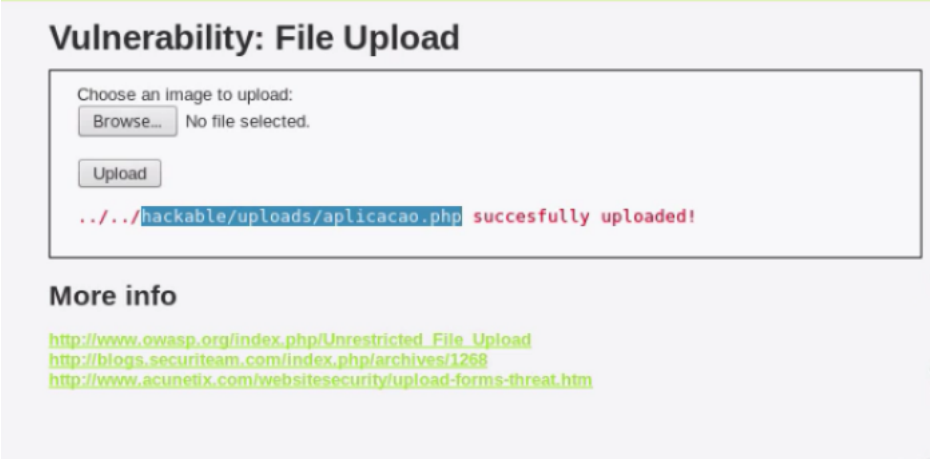


Ou seja, o sistema aceita arquivos que contem código.

Sabendo disso nós, como hackers, vamos fazer o *upload* de um arquivo que possibilita nosso acesso ao servidor. O tipo de arquivo que vamos criar é conhecido como *Backdoor*. Para nos auxiliar nessa tarefa, utilizaremos uma ferramenta, a *Weevely*. No Terminal digitamos `weevely` , pedimos para que gere uma senha e acrescentaremos o local onde queremos que o arquivo seja salvo:

```
> weevely generate 1234 aplicacao.php
Generated backdoor with password '1234' in 'aplicacao.php' of 1429 byte size
```

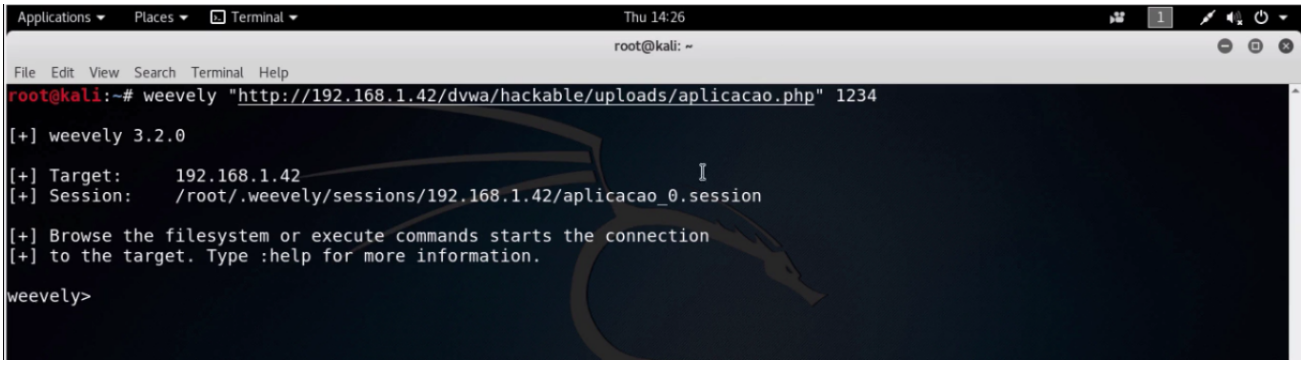
Nossa intenção, portanto, é fazer o `upload` de um arquivo para através dele nos conectarmos ao servidor. Retornando ao site e fazendo upload da `aplicacao.php` teremos o arquivo aceito:



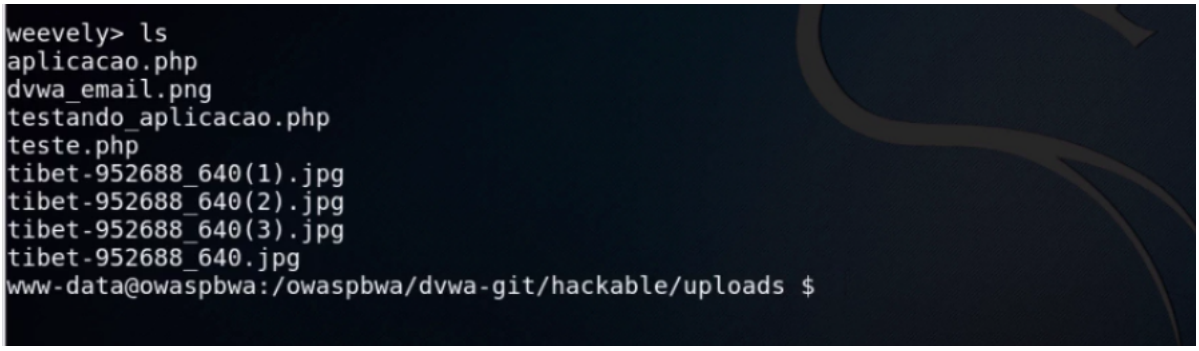
Copiamos o caminho da imagem e passamos, no Terminal, o `weevely` , a URL e a senha:

```
> weevely "http://192.168.1.42/dvwa/hackable/uploads/aplicacao.php" 1234
```

E temos o seguinte:

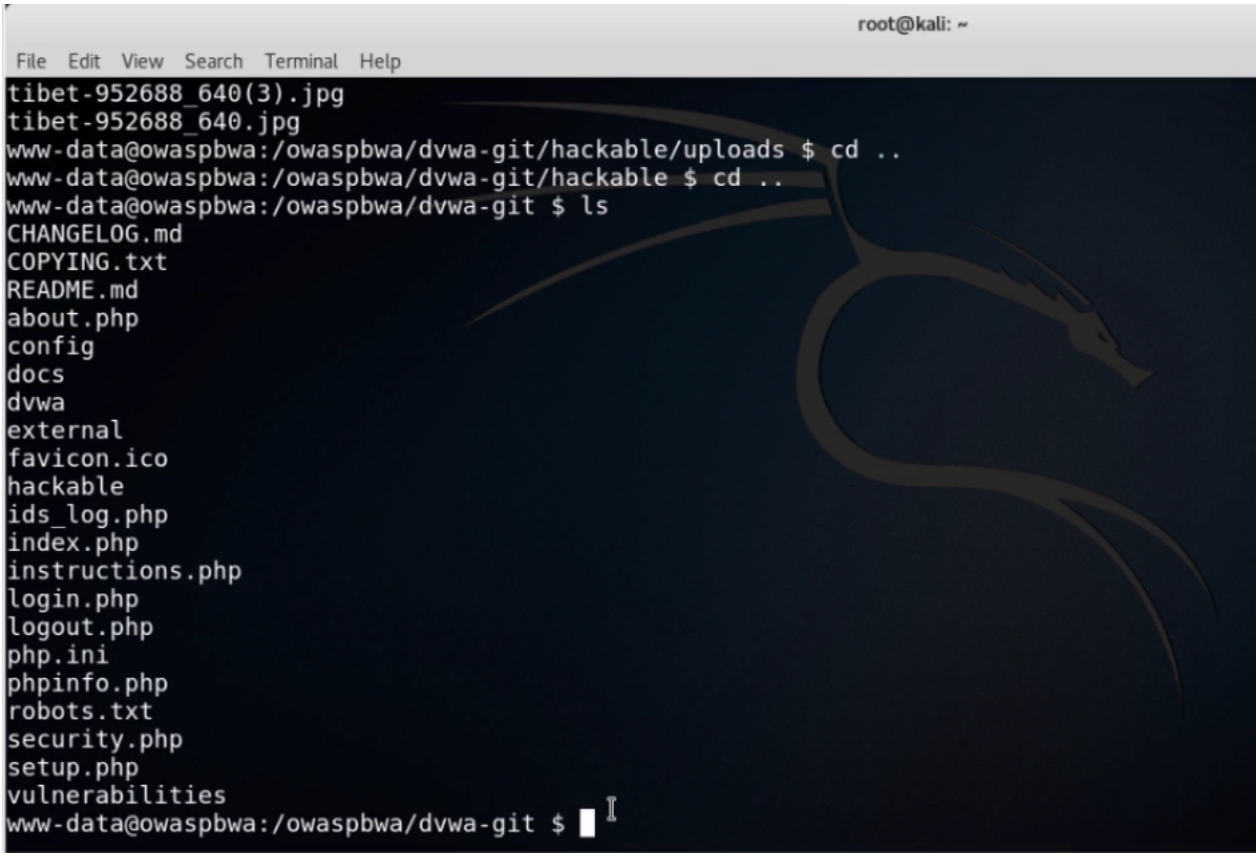


Desta maneira, é provável que o `weevely` tenha conseguido estabelecer conexão com o servidor. Para comprovar isso podemos digitar, no terminal, `ls`:



Observe o último item da lista, ele comprova que estamos, efetivamente, no servidor!

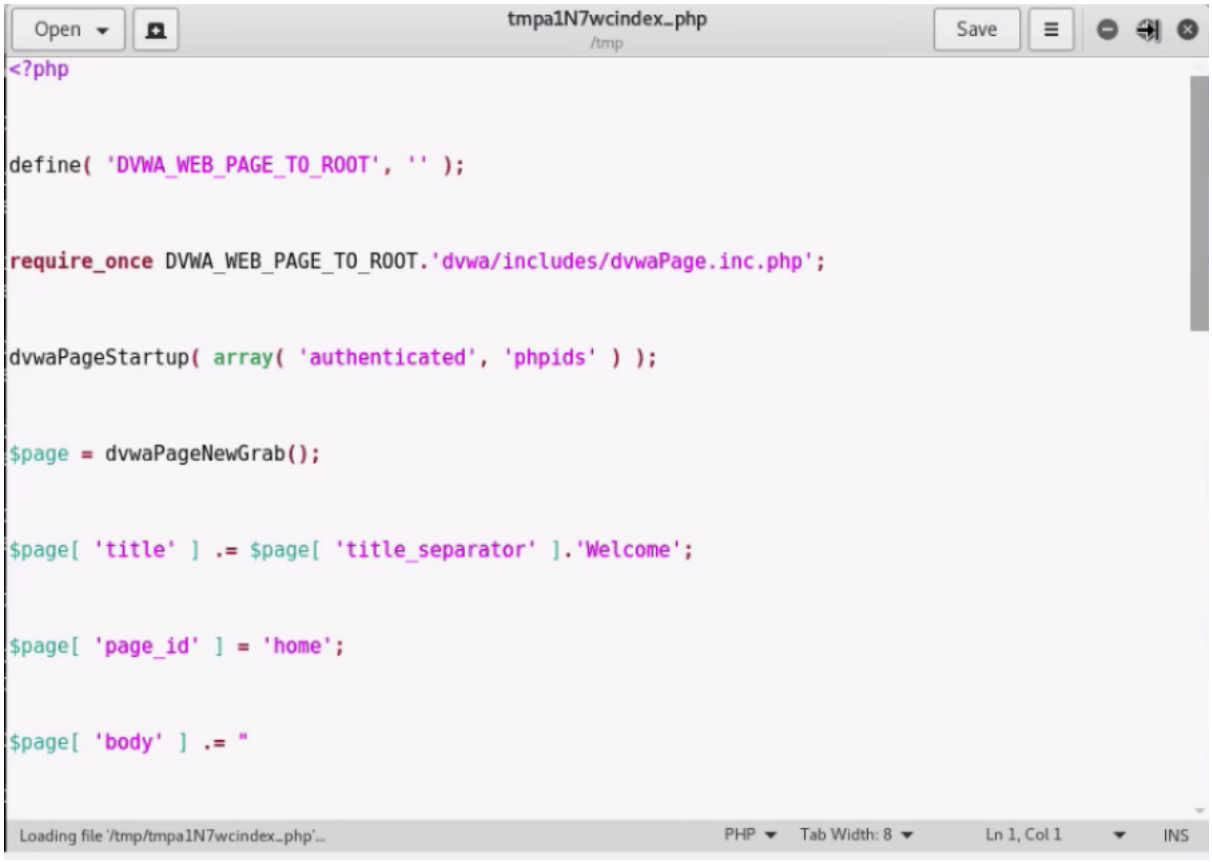
O próximo passo é inserir uma imagem que demonstre que um ataque foi realizado, escolheremos alguma figura que lembre o grupo *Anonymus*. Para isso, voltaremos dois diretórios escrevendo `cd ..` duas vezes e dessa maneira estaremos trabalhando no `"http://192.168.1.42/dvwa-git`. Vamos listar o que existe nesse diretório escrevendo `ls`. Na lista que aparece temos o `index.php`:



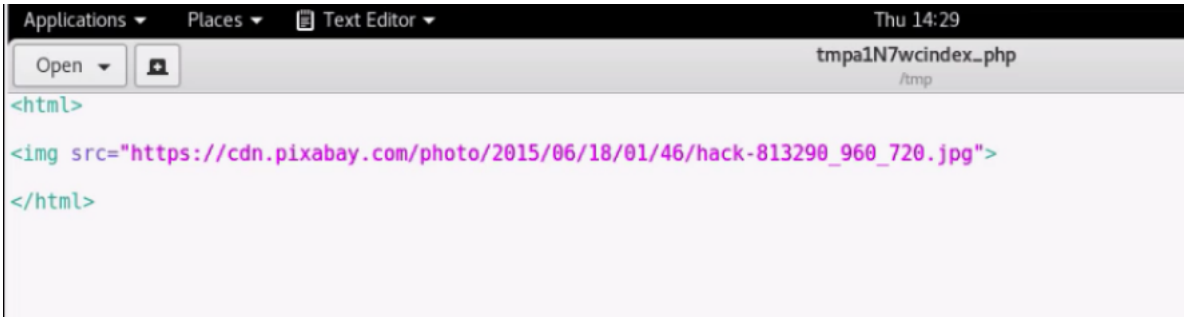
Vamos utilizar o editor de texto, `gedit`. Escreveremos isso no Terminal e também `index.php`:

```
> gedit index.php
```

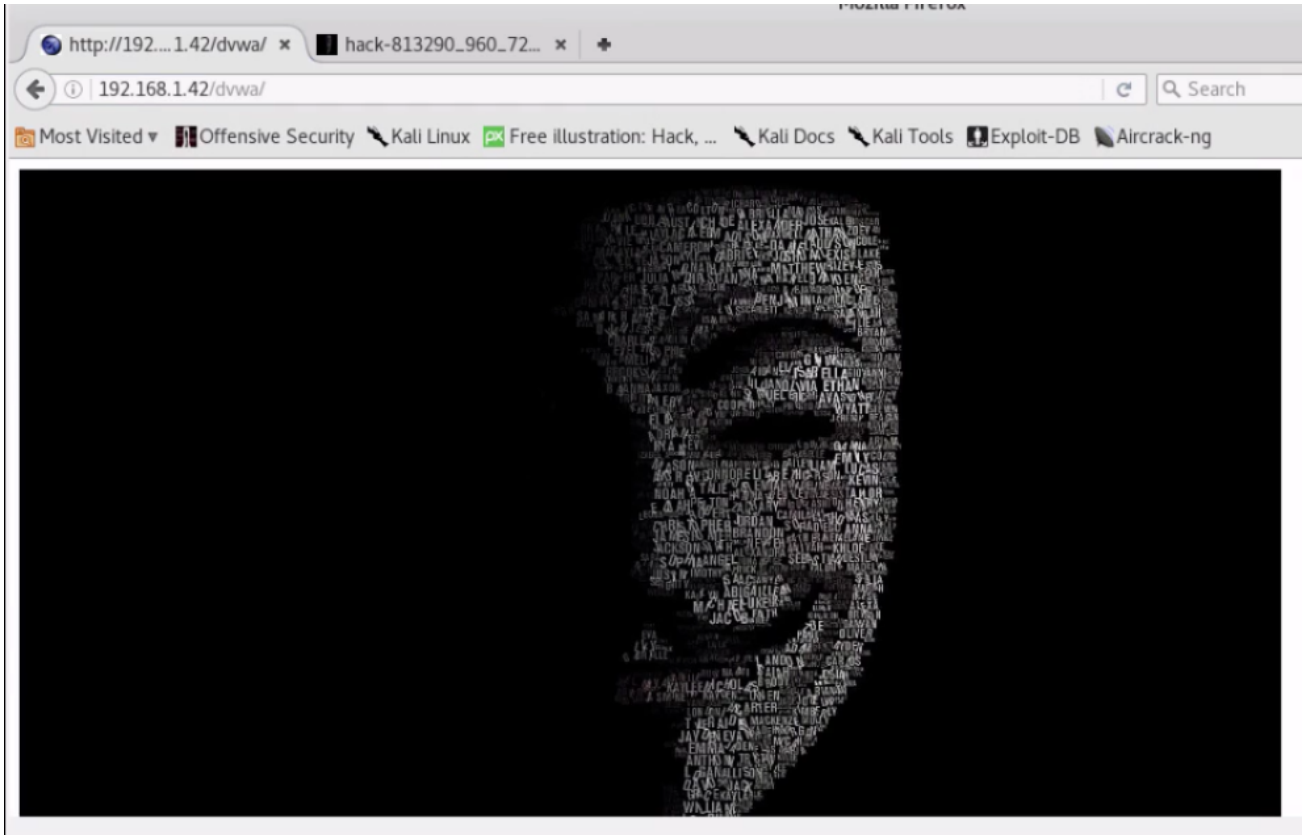
Abrirá o seguinte:



Primeiro, vamos guardar todas as informações contidas nesse arquivo, pois como desejamos modificá-lo inteiramente, se quisermos podemos retornar ao que era antes. Vamos inserir nele o `html`, o `img src` e a URL do *Anonymus* e fechamos o `html`. Teremos o seguinte:



Inserindo esse código, basta salvar o que acabamos de acrescentar. E para verificar se as informações foram alteradas escrevemos, no Terminal, `cat index.php`. Agora, teoricamente, se o hacker acessar a página da *DVWA* será possível verificar a imagem que adicionamos:



Como hackers conseguimos visualizar a imagem e como usuários comuns também. Ou seja, conseguimos tomar posse do site da pobre vítima!

Para que o site retorne a antiga aparência podemos, na máquina do hacker, recuperar o arquivo original. Para isso, digitamos no Terminal:

```
cat backup_dvwa.php
```

Fazendo isso, surgirá o arquivo original que havíamos salvo com o nome de `dvwa.php`. Copiaremos todo o seu conteúdo, depois, vamos retornar no **weevely** e usaremos o `gedit index.php` para abrir o arquivo referente à página alterada.

Apagamos o que havíamos inserido e colamos o código da página original. Salvamos e damos um `cat index.php` para verificar se a alteração foi de fato realizada. Agora, se retornarmos ao site veremos a página normal.