Explorando falhas de Local File Download (LFD)

2 de julho de 2015 / Anderson Barbosa

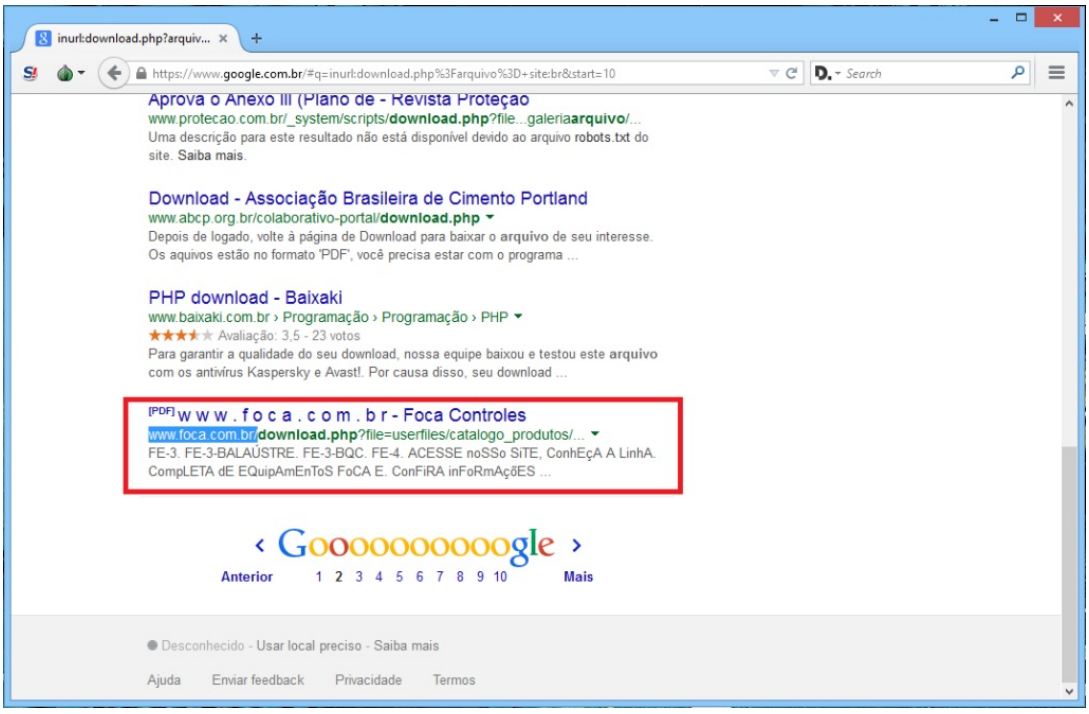
Nesse artigo estarei explicando como funciona e como explorar essa vulnerabilidade que mesmo após de descoberta existem ainda diversos websites vulneráveis.

O LFD (*Local File Download)* é uma vulnerabilidade de ocorre em aplicações Web PHP. Com essa vulnerabilidade, é possível obter (fazer o download) arquivos de configuração, usuários e senhas de banco de dados, entre outros dados. As quais podem comprometer não só o website, mas sim o servidor por completo.

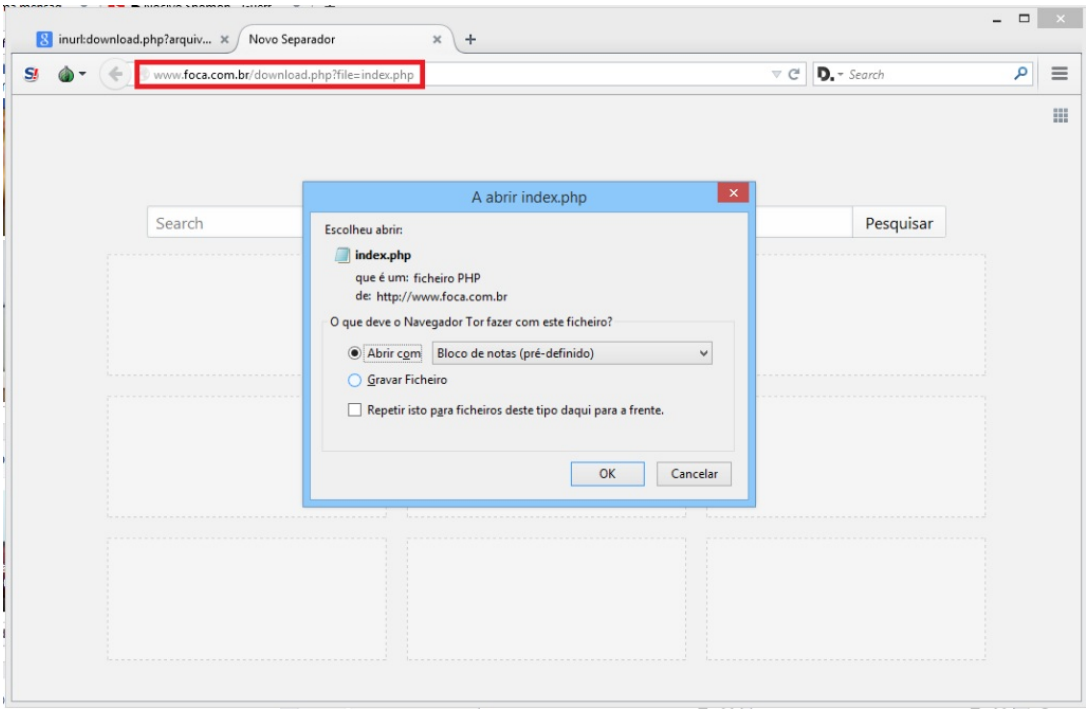
O que acontece nessa falha é que os GET's que passam pela URL após uma requisição de um download não são verificados, permitindo o download de arquivos críticos, como dito acima.

Para busca sites vulneráveis podemos usar o Google Hacking (como as *Dorks* a seguir)
inurl:download.php?file=
inurl:download.php?arquivo=
inurl:baixar.php?file=
inurl:baixar.php?arquivo=

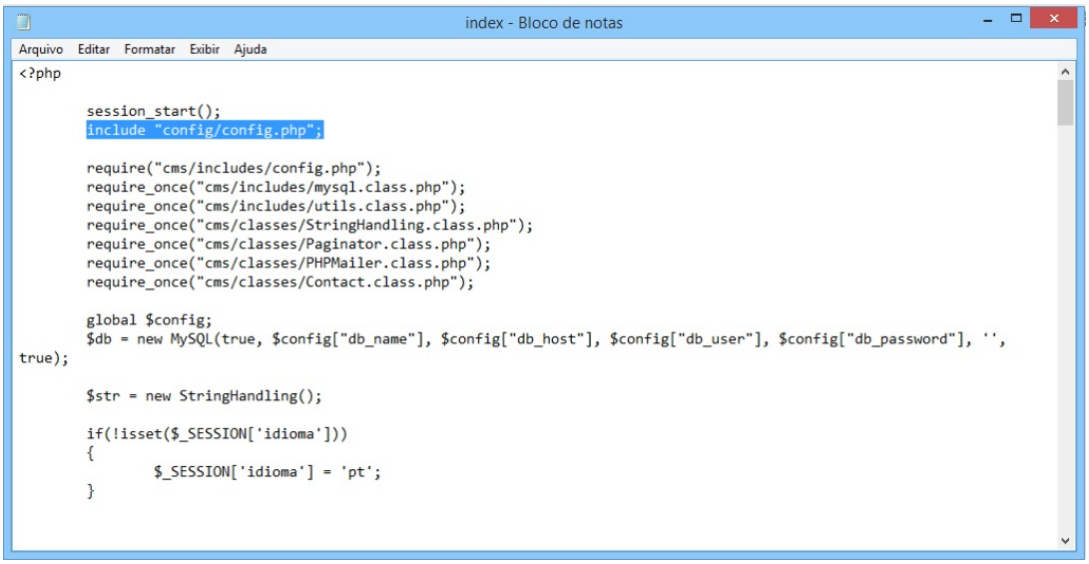
Usando uma das Dorks acima, vemos um site com uma possível vulnerabilidade, a qual se destaca em vermelho na imagem abaixo. A URL contém referência de um *Download* de um arquivo no formato PDF. Vamos analisar o site, e ver se está vulnerável.



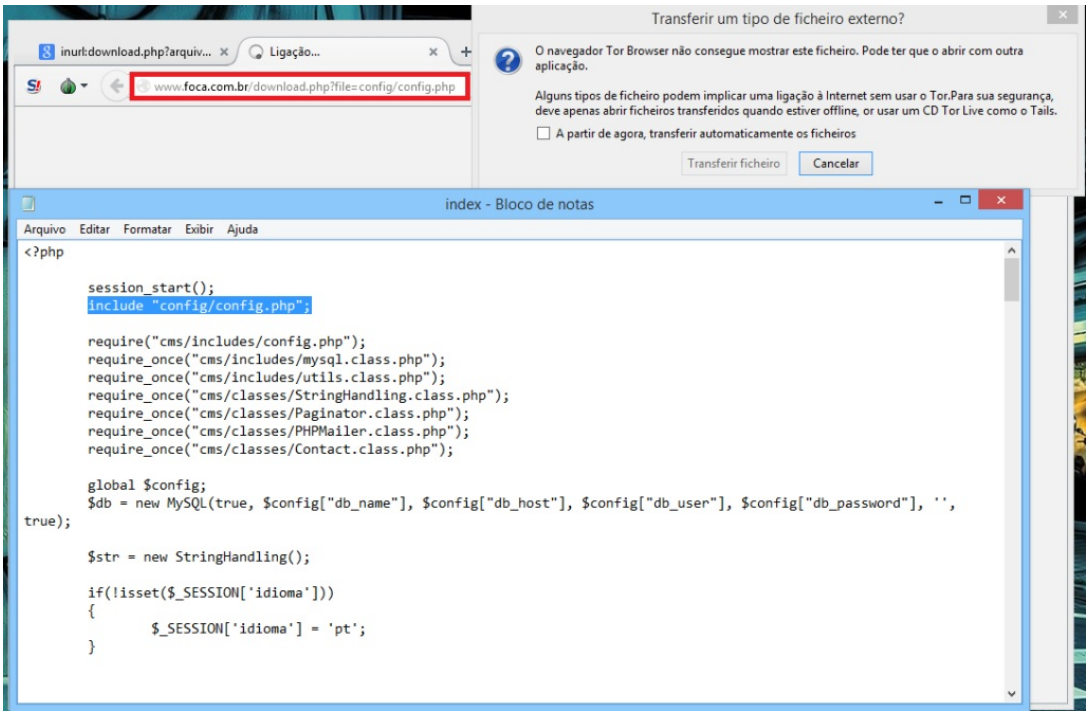
Note que na imagem abaixo ao invés de baixar o PDF alteremos para baixar o *index.php,* onde surge uma notificação de download. Faremos o download e mostrarei algumas informações.



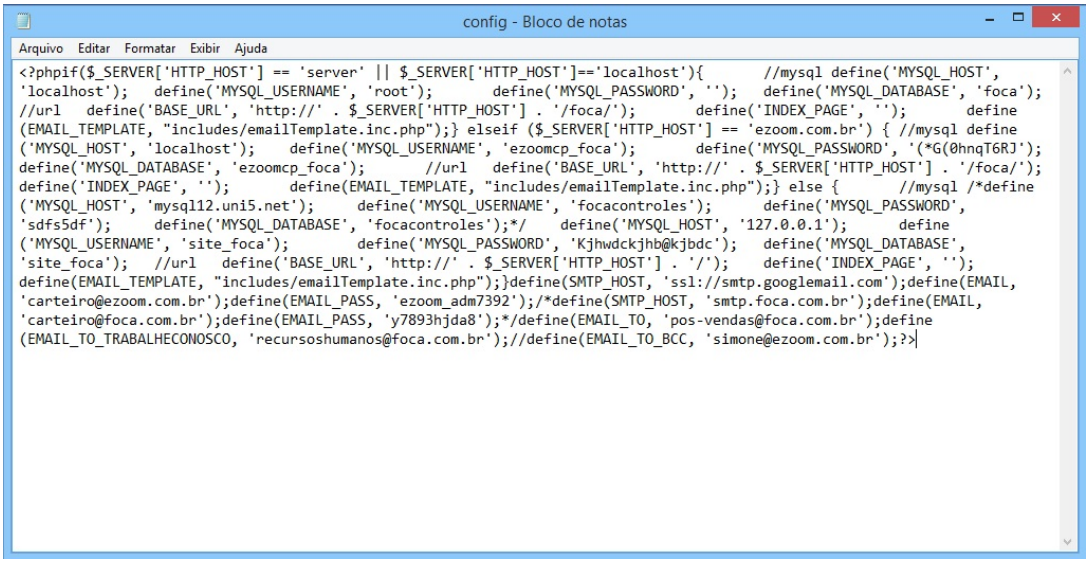
No arquivo que fiz download vieram alguns *Include* e *Require*, na qual seus nomes me chamaram atenção, da mesma forma que baixei a index, vou alterar e baixar outro arquivo. Abaixo a imagem da *index.php* com os nomes.



Alterei na URL, destaquei na imagem alguns detalhes, e outra notificação de download apareceu. Irei baixar e mostrar porquê essa vulnerabilidade pode ser perigosa em alguns casos. Abaixo a esse print você pode ver outro mostrando o arquivo de configuração, informando senhas de SMTP, MySQL e outros. Não farei login, nem alteração de qualquer dado.



Print dos dados do website:



Veja claramente os usuários de e-mail e suas respectivas senhas, é uma falha bem comum e que é possível explorar em diversos sites.