# Falha deixava apagar qualquer foto armazenada no Facebook

Problema foi descoberto por pesquisador indiano e corrigido por rede social. Facebook pagou US$ 12,5 mil pelas informações a Laxman Muthiyah.

**Altieres Rohr**Especial para o G1

Uma falha de segurança corrigida pelo Facebook foi revelada nesta quinta-feira (12) pelo pesquisador indiano Laxman Muthiyah, que descobriu e relatou o problema ao Facebook. A vulnerabilidade permitia que qualquer foto, e mesmo álbuns inteiros, fossem apagados de qualquer perfil do Facebook.

A remoção das fotos era possível porque, em um de seus sistemas, o Facebook não verificava se o comando de apagar a foto havia sido dado em uma imagem que pertence ao usuário.

O Facebook utiliza um canal de comunicação para interagir com os aplicativos que fazem uso da rede social. Esse canal é chamado de Graph API. O aplicativo móvel do Facebook, usado em celulares e tablets, também se comunica com o site por esse canal. Cada aplicativo do Facebook tem determinadas permissões (podendo ou não postar em sua timeline, por exemplo) e é o canal da Graph API que impõe essas restrições.

Muthiya descobriu que o canal usado pelo Facebook para Android simplesmente não verificava se a foto pertencia ao usuário antes de apagá-la. Quem usa o aplicativo não pode enxergar o botão para apagar uma foto que não é dele, o que esconde o erro. Mas "imitar" o botão e enviar o comando é bastante fácil. Foi isso que Muthiya tentou. E deu certo.

O Facebook foi notificado no dia 10 de fevereiro e, no mesmo dia, reconheceu a brecha e decidiu recompensar o pesquisador com um pagamento de US$ 12,5 mil (cerca de R$ 35 mil). O problema já foi corrigido. Enviar o comando para apagar uma foto que não pertence ao usuário agora retorna um erro de permissão.

É a segunda vez que uma vulnerabilidade no Facebook permite apagar qualquer foto na rede social. Em 2013, outro pesquisador de segurança descobriu um **erro no sistema para denunciar fotos inapropriadas** que também permitia que as imagens fossem removidas.

URL: http://g1.globo.com/tecnologia/noticia/2015/02/falha-deixava-apagar-qualquer-foto-armazenada-no-facebook.html

# Brasileiro ganha quase R$ 80 mil por descobrir falha grave no Facebook

## Por: Daniel Junqueira

24 de janeiro de 2014 às 14:21

Reginaldo Silva é um “caçador de bugs” e acaba de levar para casa uma bolada de quase R$ 80 mil. Isso porque ele descobriu uma falha no Facebook e recebeu o maior prêmio já dado pelo programa Facebook Bug Bounty, criado em 2011.

Silva é um engenheiro da computação formado no Instituto Tecnológico de Aeronáutica (ITA) e encontrou uma falha onde programas externos conseguiam ler arquivos dentro do servidor de web do Facebook. Ele relatou a falha em novembro e, em um post feito pelo próprio Facebook, o programa Facebook Bug County confirmou que já corrigiu a vulnerabilidade e dará o prêmio de quase R$ 80 mil para o brasileiro por sua descoberta.

No post, o Facebook detalha aspectos técnicos da falha e de como fez para corrigi-la. Você pode conferir aqui (em inglês).

Entramos em contato com Silva e ele descreveu rapidamente qual era a falha – e, de fato, era algo bem grave:

A falha estava presente na parte do Facebook que normalmente é acessada quando um usuário esquece a sua senha. Por causa de um erro de programação, era possível ler arquivos armazenados no servidor como, por exemplo, arquivos de configuração, bem como outras informações que só deveriam ser acessíveis pelos sistemas internos do Facebook. Além disso, descrevi um cenário que permitia tomar totalmente o controle do site e, embora não tenha testado tal cenário em primeira mão, pois não seria ético fazê-lo sem permissão, os engenheiros que cuidam da segurança do Facebook confirmaram que o ataque por mim descrito poderia ter sido executado na prática. Em resumo, descobri uma falha que permitiria a invasão do Facebook.

Segundo o Silva, a falha é bastante semelhante a uma outra que ele já tinha descoberto em 2012, e, ao ler um manual de software criado pelo Facebook, ele teve a ideia de tentar aplicá-la à rede social. Ela funcionou – e felizmente já foi corrigida.

Programas de caça a erros são comuns em empresas de internet e tecnologia em geral, e muitas vezes rendem prêmios bem gordos em dinheiro pela descoberta de vulnerabilidades de segurança. No caso do Facebook, não há um valor máximo a ser dado para quem detecta um bug – antes de Silva, um britânico recebeu US$ 20 mil pela descoberta de outra falha.

URL: http://gizmodo.uol.com.br/brasileiro-ganha-r-80-mil-por-descobrir-falha-grave-no-facebook/