Segurança em CGI

A programação em CGI lhe oferece algo surpreendente: tão logo seu script esteja online, ele é disponibilizado imediatamente para todo o mundo. Qualquer pessoa, de quase qualquer lugar, pode executar o aplicativo que você criou em seu servidor web. Isso pode chegar a excitá-lo, mas também deve assustá-lo. Nem todos que usam a Internet têm intenções honestas. Crackers (invasores) podem tentar vandalizar suas páginas web, para mostrar a amigos. Competidores ou investidores podem tentar acessar informações internas sobre sua empresa e seus produtos.

Nem todos os aspectos de segurança envolvem usuários maléficos. A disponibilidade mundial de seu script CGI significa que alguém pode executar seu script sob determinadas circunstâncias as quais você nunca imaginou e, certamente, nunca testou. Seu script web não deve apagar arquivos porque aconteceu de alguém colocar uma apóstrofe em um campo de formulário, mas isso é possível e aspectos como esses também representam preocupações com segurança.

A importância da segurança na web

Muitos projetistas de CGI não levam a segurança tão a sério quando deveriam. Assim, antes de olharmos como tornar scripts CGI mais seguros, vamos ver porque deveríamos nos preocupar com segurança, em primeiro lugar:

1. Na Internet, seu web site representa sua imagem pública. Se suas páginas web não estão disponíveis, ou foram vandalizadas, isso afeta as impressões dos outros quanto à sua empresa, ainda que o foco de sua empresa nada tenha a ver com a tecnologia da web.

2. Você pode ter valiosas informações em seu servidor web. Você pode ter informações sensíveis ou valiosas disponíveis em uma área restrita que pode querer preservar contra pessoas não autorizadas a acessar. Por exemplo, você pode ter conteúdo ou serviços disponíveis a membros pagantes, que não deseja que clientes não-pagantes ou não-membros acessem. Até arquivos que não fazem parte de sua árvore de documentos do servidor web e portanto, não está disponível online a ninguém (por exemplo, números de cartão de crédito), podem ser comprometidos.

3. Alguém que tenha invadido seu servidor web tem acesso mais fácil ao restante de sua rede. Se você não tiver informações valiosas em seu

servidor web, provavelmente você não pode dizer o mesmo sobre toda a rede. Se alguém invadir seu servidor web, é muito mais fácil entrar em outro sistema em sua rede, especialmente se o seu servidor web estiver dentro do firewall de sua empresa (o que, por este motivo, em geral é uma má idéia).

4. Você sacrifica o rendimento em potencial quando seu sistema está fora do ar. Se a sua empresa gera recursos diretamente de seu web site, certamente você perde lucros quanto seu sistema está indisponível. Entretanto, mesmo que você não caia neste grupo, pode ser que você ofereça literatura mercadológica. ou informações de contato online. Clientes em potencial, que não sejam capazes de acessar estas informações, podem buscar em outro lugar ao tomar suas decisões.

5. Você desperdiça tempo e recursos corrigindo problemas. Você precisa realizar muitas tarefas quando seus sistemas são comprometidos. Primeiro, você precisa determinar a extensão do prejuízo. Depois, provavelmente, você precisa recuperar a partir de backups (cópias de segurança). Você precisa ainda determinar o que aconteceu de errado. Se um cracker conseguiu acesso ao seu servidor web, então você precisa determinar como o cracker conseguiu isso, para evitar futuras invasões. Se um script CGI tem arquivos danificados, então você precisa localizar e corrigir o bug (erro) para evitar futuros problemas.

6. Você se expõe a riscos. Se você desenvolveu scripts CG I para outras empresas e um daqueles scripts CGI é responsável por um grande problema de segurança, então você pode ser considerado o responsável. No entanto, ainda que seja a sua empresa para quem você está desenvolvendo scripts CGI, você pode ser responsabilizado por terceiros. Por exemplo, se alguém invadir seu servidor web, pode usar isto como uma base de ataques para outras empresas. Da mesma forma, se sua empresa armazena informações que outros consideram sensíveis (por exemplo, os números de cartão de créditos de seus clientes), você pode ser responsabilizado por ele, se aquelas informações vazarem.

Estas são apenas algumas das muitas razões pelas quais a segurança da web é tão importante. Você mesmo pode ser capaz de ter outros motivos. Assim, agora que você reconhece a importância de criar scripts CGI seguros, pode estar imaginando o que torna seguro um script CGI. Isso pode ser resumido em uma máxima simples: nunca confie em

quaisquer dados vindos do usuário. Isso parece bem simples, mas na prática não é. No restante deste capítulo, exploraremos como fazer isso.