Instruções de uso da hospedagem no serviço Sites@UFSC

17/05/2024 05:30:50

Imprimir artigo da FAQ

Categoria:	Hospedagem no serviço Sites@UFSC::Procedimentos	**Votos:**	0
Estado:	público (todos)	**Resultado:**	0.00 %
		Última atualização:	Qua 06 Dez 10:55:02 2023

Problema (público)

Quais são as formas de uso, limitações e restrições da hospedagem no serviço Sites@UFSC?

Solução (público)

1) O acesso ao servidor é feito via sFTP (porta 2200). Este servidor não possui FTP (porta 21);

2) Para acesso de fora da UFSC, utilizar [1]VPN;

3) Recomendamos usar o Filezilla para o acesso;

4) Todo conteúdo público que será acessado pelo site, deverá estar dentro da pasta "public_html", ou em alguns casos na pasta "www";

5) Alguns sites necessitam disponibilizar arquivos e/ou pastas fora do public_html (por questões de segurança), então estes deverão ser colocados dentro da pasta "private" que está no mesmo nível do public_html;

6) O caminho absoluto para a pasta de hospedagem do usuário (home) é "/home/<usuario_do_sftp>";

7) Por questões de segurança, não é permitido a criação de arquivos ou pastas diretamente no "home" do usuário, somente nas sub-pastas "public_html" e "private", conforme a necessidade.

8) O servidor deste serviço, disponibiliza um módulo do apache que permite os scripts em PHP serem executados pelo próprio usuário dono do arquivo (o <usuario_do_sftp>), então não há necessidade de atribuir permissões 777 em pastas ou arquivos;

9) IMPORTANTE: Aconselhamos, por questões de seguraça, que sejam colocadas permissões 640 (-rw-r-----) em todos os arquivos de scripts PHP (*.php). Opcionalmente, para arquivos de script PHP que não precisem de permissão de escrita (não serão alterados/reescritos), restringir com permissão "somente para leitura" para o dono e o grupo, seria mais seguro ainda, ou seja permissões 440 (-r--r-----). A permissão 0 (zero) para os grupamento "outros" (others) é importante para evitar ataques de hackers vindos de outros sites que estejam hospedados no mesmo servidor, evitando assim que estes tenham acesso a senhas de banco de dados e outros dados sigilosos contidos nos scripts.

10) Caso seu site possua banco de dados MySQL, para gerenciá-lo acesse: [2]http://pma.setic.ufsc.br/?server=mysql.sites.ufsc.br

ATENÇÃO: As configurações e permissões de segurança em arquivos, pastas e banco de dados são de inteira responsabilidade dos usuários responsáveis pelos sites hospedados. Solicitamos que sempre apliquem as melhores práticas de programação e segurança, dificultando assim as tentativas de invasão, defacement e SQL injection por hackers. Lembrem-se que pastas ou arquivos com permissões de escrita excessivos são as principais portas de invasão de sites, bem como a não validação de parâmetros passados aos scripts, permitindo assim a alteração de arquivos, upload de scripts maliciosos e a exploração de vulnerabilidades, tais como SQL injection.

A SeTIC RESERVA-SE AO DIREITO DE RETIRAR O SITE DO AR, CASO ELE APRESENTE PROBLEMAS DE SEGURANÇA, SEJA INVADIDO, OU VIOLE A [3]POLÍTICA DE USO VIGENTE, RELATIVOS AOS SERVIÇOS OFERECIDOS. O SITE SÓ VOLTARÁ AO AR, DEPOIS QUE OS RESPONSÁVEIS PELO MESMO RESOLVEREM AS CAUSAS DO PROBLEMA, CONSERTANDO A VULNERABILIDADE, SEJA POR UMA ATUALIZAÇÃO DE ALGUM CÓDIGO, OU MÓDULO PROBLEMÁTICO E CERTIFICANDO-SE DE QUE NÃO HÁ NOVAS AMEAÇAS QUE POSSAM COMPROMETER A SEGURANÇA DO SITE E DO SERVIDOR DE HOSPEDAGEM.

[1] https://faq.setic.ufsc.br/vpn
[2] http://pma.setic.ufsc.br/?server=mysql.sites.ufsc.br
[3] http://setic.ufsc.br/politicas-de-uso-servicos/