SEMINÁRIO DE TECNOLOGIA, GESTÃO E EDUCAÇÃO
Período de 26 a 30 de outubro
Alcides Maya
FACULDADE E ESCOLA TÉCNICA

Artigo

VULNERABILIDADE CROSS-SITE SCRIPTING NOS SITES WEB

Marco Antonio Barbosa1
Anderson santos da silva [2]
Marcelo Pereira das Neves [3]

RESUMO

Uma vulnerabilidade a tempo conhecida é Cross Site Scripting (XSS[1]) ou também chamada como execução de comandos em sites cruzados, tem como base um injeção de código do lado do cliente, com isso, o site é usado como veículo para entregar um script malicioso ao navegador da vítima.

Palavras-chave: vulnerabilidade XSS, Cross-site Scripting, execução de comandos em sites cruzados.

ABSTRACT

A well-known vulnerability in time is Cross Site Scripting (XSS ou) or also called as execution of commands in cross sites, it is based on a client-side code injection, with that, the site is used as a vehicle to deliver a malicious script to the victim's browser.

Keywords: XSS vulnerability, Cross - site Scripting, execution of commands in cross sites.

[1]Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. marcoab@hotmail.com.br

[2]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br

[3]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. marcelo_neves@alcidesmaya.edu.br

Segurança com aplicações Web

Sobre a segurança com aplicações web é amplamente discutida pelas empresas. Porém, as vezes existem empresas que não se dão a devida atenção de segurança nesse ambiente, como isso requer tempo e custos, muitas vezes esses recursos são deixados de lado, tendo falta de atualizações e recursos de segurança em efetiva ação. Com isso um atacante pode explorar o ambiente até encontrar uma vulnerabilidade, forçando a aplicação a receber dados que ela não está preparada, causando assim falhas e abrindo brechas.

Na vulnerabilidade de Cross-Site Scripting ela permite que códigos maliciosos, por exemplo no JavaScript sejam executados em uma aplicação através do navegador da vítima, permitindo o sequestro de sessão do usuário, tendo inserção de conteúdo hostil, pode ocorrer roubo de dados, desconfiguração e redirecionar os usuários para páginas maliciosas.

A conscientização de equipes de segurança e desenvolvimento das causas e danos gerados por falhas em aplicações WEB é extrema importância, pois expõe os usuários utilizadores do serviço web a falhas e ataques maliciosos. Alguns dos métodos para prevenção dos ataques está com o uso de White Lists, Black Lists, e sempre está monitorando analisando o ambiente web com revisões e técnicas de proteção regulamentadas por entidade de padronização da Internet.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396
Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

REFERÊNCIAS

Rodrigues, Análise da Vulnerabilidade XSS[4] em Aplicações Web, Disponive em <https://www.researchgate.net/profile/Lucas_Montanheiro/publication/319205710_Analise_da_Vulnerabilidade_XSS_em_Aplicacoes_Web/links/599b183d45851574f4ac62fa/Analise-da-Vulnerabilidade-XSS-em-Aplicacoes-Web.pdf>; Acessado em 23 de outubro de 2020.

Desconhecido, Ataques virtuais; <https://www.solor.com.br/ataques-virtuais/>; Acessado em 23 de outubro de 2020.

[4] A sigla utilizada não é CSS, para não ser confundida com Cascade Style Sheets.