Cross Site Scripting

XSS

Como funciona?

Algumas aplicações Web costumam permitir que seus usuários postem conteúdo contendo trechos de código HTML

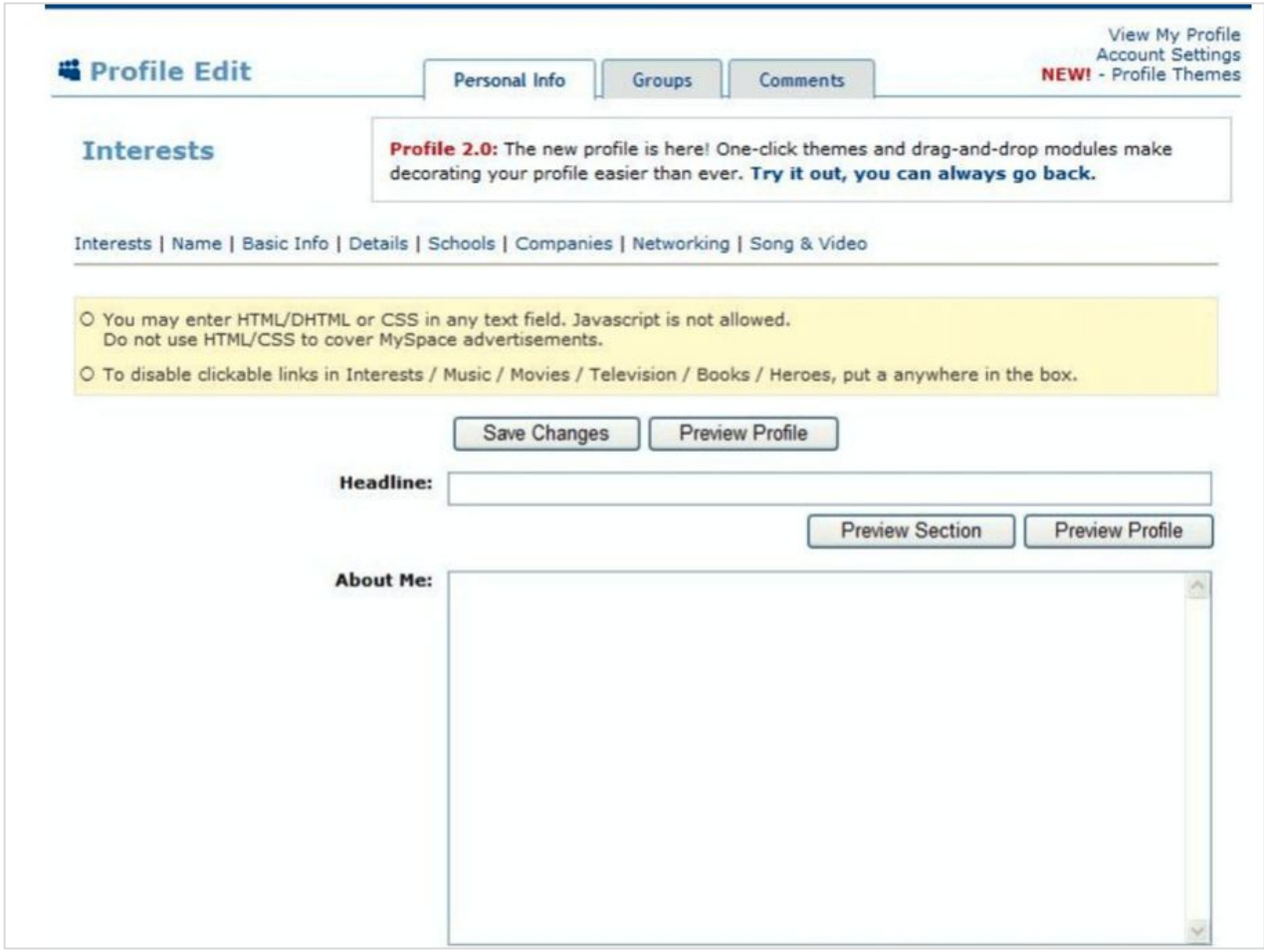
Este ataque explora a falta de tratamento adequado das informações digitadas pelos usuários.

O Maior ataque

No dia 04 de outubro de 2005, Samy Kamkar, um hacker com 19 anos de idade, escreveu um código JavaScript malicioso. Este explorava uma vulnerabilidade presente no site do Myspace, que naquela época era considerada a maior rede social da internet.

O script que Samy escreveu fazia com que o usuário que visitasse seu perfil automaticamente o adicionasse como amigo, e além disso, também adicionava na página da vítima uma categoria chamada My heroes com o texto: but most of all, Samy is my hero.

O script ficou conhecido como Samy Worm


Profile Edit
Personal Info
Groups
Comments
View My Profile
Account Settings
NEW! - Profile Themes
Interests
Profile 2.0: The new profile is here! One-click themes and drag-and-drop modules make decorating your profile easier than ever. Try it out, you can always go back.
Interests | Name | Basic Info | Details | Schools | Companies | Networking | Song & Video
You may enter HTML/DHTML or CSS in any text field. Javascript is not allowed.
Do not use HTML/CSS to cover MySpace advertisements.
To disable clickable links in Interests / Music / Movies / Television / Books / Heroes, put a anywhere in the box.
Save Changes
Preview Profile
Headline:
Preview Section
Preview Profile
About Me:

Código JavaScript mascarado

```
<img
    src=""
    onerror="&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70
    &#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53
    &#x53&#x27&#x29">
```

Como proteger uma aplicação?

- Não confie nos seus usuários
- Valide as informações de entrada e faça o escape das informações de saída
- Utiliza bibliotecas AntiSamy

Exemplo Prático