2017年5月1日

-----代码审计笔记

### tjheer博客系统V1.10 审计记录:

搜索框Xss漏洞:

search.php分析:

elseif($\_GET['leirong']=="搜类容"){

$where=" where pDesc like '%".$\_GET['name']."%' ";

$rows=fetchnzd($ziduan=" Id,pName,Author,pubTime,Class,CliCks,zaiyao,pubTime ",$table,$where,$result\_type=MYSQL\_ASSOC);

//翻页数据+翻页条

$count=count($rows);

$pageclass= "name=".$\_GET['name']."&leirong=".$\_GET['leirong']."&" ;

$Page\_size="10";

$rows=pagex($rows,$Page\_size) ; //翻页条每页数据

$key=keys($count,$Page\_size,$pageclass) ; //翻页条

通过分析以下代码得到结论：

①$\_GET无任何过滤

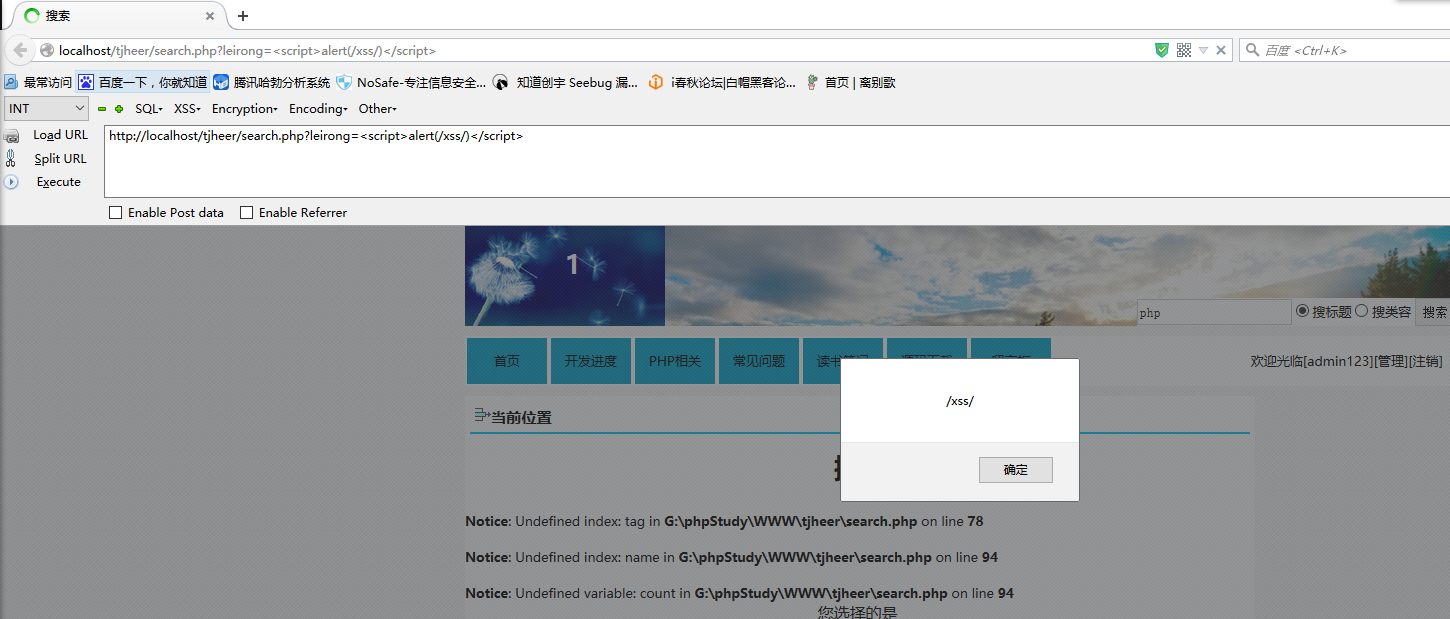
②存在Xss漏洞

③存在Sql注入漏洞

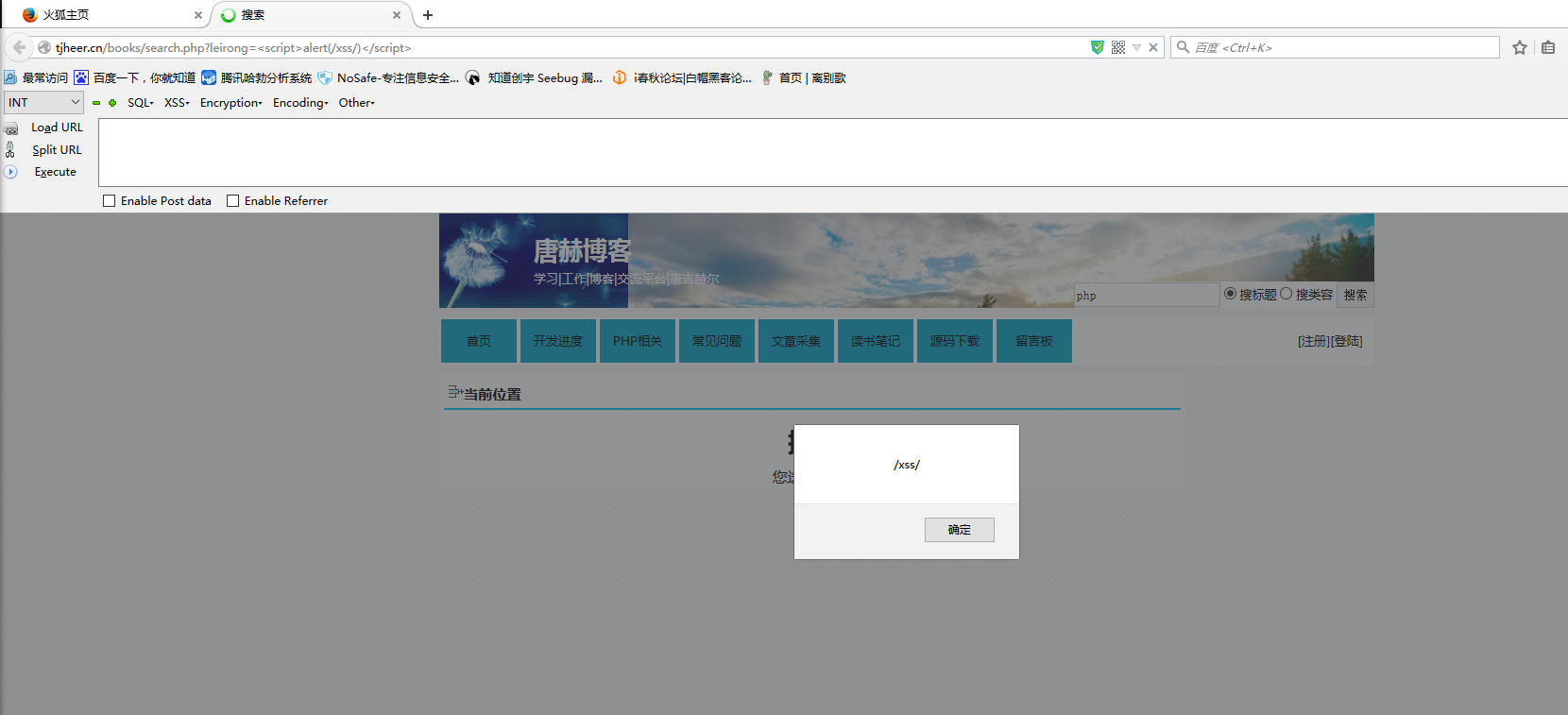
Payload:?leirong=<script>alert(/xss/)</script>

弹出/Xss/

验证:



官方网站:



成功利用