



ME系统 安全性测试报告

该报告包含有关 ME 系统的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.0.0, 规则: 1699
扫描开始时间: 2016/6/17 9:20:17

目录

介绍

- 一般信息
- 登陆设置

管理综合报告

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- Flash 参数 AllowScriptAccess 已设置为 always ②
- SQL 盲注 ④
- 发现社会保险号模式 ①
- 发现数据库错误模式 ①
- 发现压缩目录 ⑤
- 归档文件下载 ⑤
- 会话 cookie 中缺少 HttpOnly 属性 ②
- 会话标识未更新 ③
- 跨站点脚本编制 ⑥
- 跨站点请求伪造 ③
- 链接注入（便于跨站请求伪造） ①
- 临时文件下载 ⑤
- 通过框架钓鱼 ①
- 已解密的登录请求 ⑨
- 永久 Cookie 包含敏感的会话信息 ①
- 在参数值中找到了内部 IP 公开模式 ①
- 自动填写未对密码字段禁用的 HTML 属性 ①
- HTML 注释敏感信息泄露 ⑧
- Microsoft FrontPage Htmimage.exe 命令执行和路径泄露 ①

- 发现电子邮件地址模式 4
- 发现可能的服务器路径泄露模式 15
- 发现内部 IP 泄露模式 3
- 检测到应用程序测试脚本 1
- 客户端（JavaScript）Cookie 引用 2
- 未分类站点的链接 2
- 无害站点的链接 3
- 应用程序错误 1

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题: 45
低严重性问题: 46
报告中包含的严重性问题总数: 91
扫描中发现的严重性问题总数: 91

一般信息

扫描文件名称: Me_test
扫描开始时间: 2016/6/17 9:20:17
测试策略: Default
主机: me.hxsd.jc
操作系统: Unknown
Web 服务器: Unknown
应用程序服务器: PHP




























登陆设置




































登陆方法: 自动
并发登陆: 已启用
JavaScript 执行文件: 已禁用
会话中检测: 已启用
会话中模式:
跟踪或会话标识 cookie:
跟踪或会话标识参数:
登陆序列:

管理综合报告

问题类型 27

TOC

问题类型	问题的数量
高 Flash 参数 AllowScriptAccess 已设置为 always	2 
高 SQL 盲注	4 
高 发现社会保险号模式	1 
高 发现数据库错误模式	1 
高 发现压缩目录	5 
高 归档文件下载	5 
高 会话 cookie 中缺少 HttpOnly 属性	2 
高 会话标识未更新	3 
高 跨站点脚本编制	6 
高 跨站点请求伪造	3 
高 链接注入（便于跨站请求伪造）	1 
高 临时文件下载	5 
高 通过框架钓鱼	1 
高 已解密的登录请求	9 
高 永久 Cookie 包含敏感的会话信息	1 
高 在参数值中找到了内部 IP 公开模式	1 
高 自动填写未对密码字段禁用的 HTML 属性	1 
低 HTML 注释敏感信息泄露	8 
低 Microsoft FrontPage Htmimage.exe 命令执行和路径泄露	1 
低 发现电子邮件地址模式	4 
低 发现可能的服务器路径泄露模式	15 
低 发现内部 IP 泄露模式	3 
低 检测到应用程序测试脚本	1 
低 客户端（JavaScript）Cookie 引用	2 
低 未分类站点的链接	2 
低 无害站点的链接	3 
低 应用程序错误	1 

URL		问题的数量
高	http://me.hxsd.jc/public/comm/assets/annex/video/jwplayer.js	3 
高	http://me.hxsd.jc/public/comm/assets/plupload/plupload.full.min.js	1 
高	http://me.hxsd.jc/home/home.html	6 
高	http://me.hxsd.jc/public/comm/assets/scripts/form-components.js	1 
高	http://me.hxsd.jc/home/resume/add	4 
低	http://me.hxsd.jc/home/index/index/	6 
高	http://me.hxsd.jc/public/comm/assets/annex/echarts/	1 
高	http://me.hxsd.jc/home/announcement/getcontentbyid/1	2 
高	http://me.hxsd.jc/home/announcement/getcontentbyid/5	2 
高	http://me.hxsd.jc/home/announcement/getcontentbyid/6	2 
高	http://me.hxsd.jc/home/announcement/getcontentbyid/7	2 
高	http://me.hxsd.jc/home/announcement/getcontentbyid/8	2 
高	http://me.hxsd.jc/	3 
高	http://me.hxsd.jc/home/student/login.html	3 
高	http://me.hxsd.jc/home/student/change_password	7 
高	http://me.hxsd.jc/home/student/check_login	4 
高	http://me.hxsd.jc/home/student/forgot_password	7 
高	http://me.hxsd.jc/home/feedback/save	1 
高	http://me.hxsd.jc/home/technicalsupport.html	2 
高	http://me.hxsd.jc/home/technicalsupport/index	5 
高	http://me.hxsd.jc/home/technicalsupport/save	2 
高	http://me.hxsd.jc/home/technicalsupport/saveComment	1 
高	http://me.hxsd.jc/public/comm/assets/faceimage/expressInstall.swf	2 
低	http://me.hxsd.jc/home/index/index/phone.html	3 
低	http://me.hxsd.jc/home/process.html	1 
低	http://me.hxsd.jc/home/resume/add.html	3 
低	http://me.hxsd.jc/public/comm/assets/scripts/bootstrap-datetimepicker.zh-CN.js	1 
低	http://me.hxsd.jc/public/comm/assets/scripts/form-validation.js	1 
低	http://me.hxsd.jc/home.html	1 
低	http://me.hxsd.jc/home/attendance.html	1 
低	http://me.hxsd.jc/home/feedback.html	1 
低	http://me.hxsd.jc/home/index.html	1 
低	http://me.hxsd.jc/home/index/index	1 
低	http://me.hxsd.jc/public/comm/assets/plugins/city/areadata.js	1 
低	http://me.hxsd.jc/public/comm/assets/plugins/jquery-hydx/hgz_hycode.js	1 

低	http://me.hxsd.jc/public/comm/assets/scripts/judgeResume.js	1	<div></div>
低	http://me.hxsd.jc/public/home/js/bindPhone.js	1	<div></div>
低	http://me.hxsd.jc/public/home/js/clazzfeedback.js	1	<div></div>
低	http://me.hxsd.jc/public/home/js/operationpdf.js	1	<div></div>
低	http://me.hxsd.jc/public/comm/assets/plugins/jquery.cookie.min.js	1	<div></div>
低	http://me.hxsd.jc/public/comm/assets/annex/pdf/flexpaper_handlers.js	1	<div></div>

修订建议 20

TOC

修复任务		问题的数量	
高	查看危险字符注入的可能解决方案	13	<div></div>
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	9	<div></div>
高	删除 Htimage.exe 和 Imagemap.exe 的所有副本	1	<div></div>
中	登录之后更改会话标识符值	3	<div></div>
中	拒绝恶意请求	3	<div></div>
低	避免在永久 cookie 中存储敏感的会话信息	1	<div></div>
低	除去 HTML 注释中的敏感信息	8	<div></div>
低	除去 Web 站点中的电子邮件地址	4	<div></div>
低	除去 Web 站点中的内部 IP 地址	4	<div></div>
低	除去 Web 站点中的社会保险号	1	<div></div>
低	除去服务器中的测试脚本	1	<div></div>
低	除去客户端中的业务逻辑和安全逻辑	2	<div></div>
低	除去虚拟目录中的旧版本文件	10	<div></div>
低	除去压缩目录文件或限制对它的访问	5	<div></div>
低	检查链接，确定它是否确实本应包含在 Web 应用程序中	5	<div></div>
低	将 AllowScriptAccess 参数设置为“sameDomain”，它会告诉 Flash 播放器仅从同一个域加载作为父级 SWF 的 SWF 文件才会对主管 Web 页面具有脚本访问权限	2	<div></div>
低	将“autocomplete”属性正确设置为“off”	1	<div></div>
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	15	<div></div>
低	向所有会话 cookie 添加“HttpOnly”属性	2	<div></div>
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	1	<div></div>

安全风险 15






TOC

风险	问题的数量
高 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从	17 <div></div>

	而使黑客能够以该用户身份查看或变更用户记录以及执行事务		
高	可能会查看、修改或删除数据库条目和表	5	
高	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	17	
高	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	5	
高	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	11	
高	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	2	
高	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件	1	
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	9	
高	可能会窃取保存在磁盘上作为永久 cookie 的会话信息（cookie）	1	
高	可能会绕过 Web 应用程序的认证机制	1	
低	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容	1	
低	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	15	
低	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	2	
低	不适用	5	
低	可能会收集敏感的调试信息	1	

原因 14

TOC

原因	问题的数量	
高 Web 应用程序编程或配置不安全	20	
高 未对用户输入正确执行危险字符清理	13	
高 在生产环境中留下临时文件	11	
高 Web 应用程序设置了缺少 HttpOnly 属性的会话 cookie	2	
高 应用程序使用的认证方法不充分	3	
高 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	9	
高 Web 应用程序将敏感的会话信息存储在永久 cookie 中（磁盘上）	1	
低 程序员在 Web 页面上留下调试信息	8	
低 在 Web 站点上安装了缺省样本脚本或目录	1	
低 未安装第三方产品的最新补丁或最新修订程序	15	
低 Cookie 是在客户端创建的	2	
低 不适用	5	
低 未对入局参数值执行适当的边界检查	1	
低 未执行验证以确保用户输入与预期的数据类型匹配	1	

WASC 威胁分类

TOC

威胁	问题的数量
SQL 注入	5
操作系统命令	1
传输层保护不足	9
恶意内容测试	5
功能滥用	2
会话定置	3
会话期限不足	1
可预测资源位置	11
跨站点脚本编制	6
跨站点请求伪造	3
内容电子欺骗	2
信息泄露	43

按问题类型分类的问题

Flash 参数 AllowScriptAccess 已设置为 always	
严重性:	高
URL:	http://me.hxsd.jc/public/comm/assets/annex/video/jwplayer.js
实体:	jwplayer.js (Page)
风险:	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因:	Web 应用程序编程或配置不安全
固定值:	将 AllowScriptAccess 参数设置为“sameDomain”，它会告诉 Flash 播放器仅从同一个域加载作为父级 SWF 的 SWF 文件才会对主管 Web 页面具有脚本访问权限

推理： 响应包含 AllowScriptAccess 参数设置为“always”的 Flash 对象
未经处理的测试响应：

```
...

Content-Type: application/x-javascript
Content-Length: 48318
Last-Modified: Mon, 02 May 2016 09:27:07 GMT
Connection: keep-alive
Vary: Accept-Encoding
Expires: Thu, 31 Dec 2037 23:55:55 GMT
Cache-Control: max-age=315360000
Accept-Ranges: bytes

if(typeof jwplayer=="undefined"){jwplayer=function(a){if(jwplayer.api){return
jwplayer.api.selectPlayer(a)}};jwplayer.version="6.8.";jwplayer.vid=document.createElement("video
");jwplayer.audio=document.createElement("audio");jwplayer.source=document.createElement("source"
);(function(g){var
c=document,r=window,o=navigator,s="undefined",h="string",f="object",d=true,j=false;var
q=g.utils=function(){q.exists=function(t){switch(typeof(t)){case h:return(t.length>0);case
f:return(t!==null);case s:return j}return d};q.styleDimension=function(t){return t+
(t.toString().indexOf("%")>0?"":"px")};q.getAbsolutePath=function(z,y){if(!q.exists(y))
{y=c.location.href;if(!q.exists(z)){return}if(i(z)){return z}var
A=y.substring(0,y.indexOf(":/")+3);var x=y.substring(A.length,y.indexOf("/",A.length+1));var
u;if(z.indexOf("/")===0){u=z.split("/")};else{var v=y.split("?")
[0];v=v.substring(A.length+x.length+1,v.lastIndexOf("/"));u=v.split("/").concat(z.split("/"))}var
```

```

t=[];for(var w=0;w<u.length;w++){if(!u[w]||!q.exists(u[w])||u[w]=="")
{continue}else{if(u[w]==".."){t.pop()}else{t.push(u[w])}}return A+x+"/"+t.join("/")};function
i(u){if(!q.exists(u)){return}var v=u.indexOf("://");var t=u.indexOf("?");return(v>0&&(t<0||
(t>v)))?q.extend=function(){var t=q.extend("arguments");if(t.length>1){for(var
u=1;u<t.length;u++){q.foreach(t[u],function(w,v){try{if(q.exists(v)){t[0][w]=v}}catch(x)
{}})}return t[0]}return null};var l=window.console=window.console||{log:function()
{}};q.log=function(){var t=Array.prototype.slice.call(arguments,0);if(typeof l.log===f)
{l.log(t)}else{l.log.apply(l,t)}};var k=q.userAgentMatch=function(u){var
t=o.userAgent.toLowerCase();return(t.match(u)!=null)};function m(t){return function(){return
k(t)}}q.isIE=q.isMSIE=m(/msie/i);q.isFF=m(/firefox/i);q.isChrome=m(/chrome/i);q.isIPod=m(/iPod(hone
lod)/i);q.isIPad=m(/iPad/i);q.isSafari602=m(/Macintosh.*Mac OS X 10_8.*6\.0\.\d*
Safari/i);q.isIETrident=function(t){if(t){t=parseFloat(t).toFixed(1);return k(new
RegExp("msie\\s*"+"+|trident/.+rv:\\s*"+"+,"i"))}return k(/msie|trident/i)};q.isSafari=function()
{return k(/safari/i)&&!k(/chrome/i)&&!k(/chromium/i)&&!k(/android/i)};q.isIOS=function(t){if(t)
{return k(new RegExp("iPod|ad|od).+\\sOS\\s*"+"+,"i"))}return
k(/iPod|ad|od/i)};q.isAndroid=function(t,v){var u=v?!k(/chrome/[23456789]/i):d;if(t){return
u&&k(new RegExp("android.*"+"+,"i"))}return u&&k(/android/i)};q.isMobile=function(){return
q.isIOS()||q.isAndroid()};q.saveCookie=function(t,u){c.cookie="jwplayer."+t+"="+u+"";
path="/";q.getCookies=function(){var w={};var v=c.cookie.split("; ");for(var u=0;u<v.length;u++)
{var t=v[u].split("=");if(t[0].indexOf("jwplayer.")===0)
{w[t[0].substring(9,t[0].length)]=t[1]}}return w};q.typeOf=function(u){var t=typeof u;if(t===f)
{if(!u){return null}}return(u instanceof Array)?"array":t}return
t};q.translateEventResponse=function(v,t){var
x=q.extend({},t);if(v==g.events.JWPLAYER_FULLSCREEN&&!x.fullscreen)
{x.fullscreen=x.message=="true"?d:j;delete x.message}else{if(typeof x.data===f){var
w=x.data;delete x.data;x=q.extend(x,w)}else{if(typeof x.metadata===f)
{q.deepReplaceKeyName(x.metadata,["__dot__","__spc__","__dsh__","__default__"],[".",",","-","__default__"])}var u=["position","duration","offset"];q.foreach(u,function(y,z){if(x[z])
{x[z]=Math.round(x[z]*1000)/1000}});return x};q.flashVersion=function(){if(q.isAndroid()){return
0}var t=o.plugins,u;try{if(t!==s){u=t["Shockwave Flash"];if(u){return
parseInt(u.description.replace(/\\D+(\\d+)\\.\\s*/,"$1"),10)}}catch(w){if(typeof r.ActiveXObject!=s)
{try{u=new r.ActiveXObject("ShockwaveFlash.ShockwaveFlash");if(u){return
parseInt(u.GetVariable("$version").split(" ")[1].split(",")[0],10)}}catch(v){}}return
0};q.getScriptPath=function(v){var t=c.getElementsByTagName("script");for(var u=0;u<t.length;u++)
{var w=t[u].src;if(w&&w.indexOf(v)>=0){return
w.substr(0,w.indexOf(v))}}return""};q.deepReplaceKeyName=function(w,u,t)
{switch(g.utils.typeOf(w)){case"array":for(var v=0;v<w.length;v++)
{w[v]=g.utils.deepReplaceKeyName(w[v],u,t)}break;case f:q.foreach(w,function(z,C){var B,A;if(u
instanceof Array&&t instanceof Array){if(u.length!=t.length){return}else{B=u;A=t}}var x=z;for(var y=0;y<B.length;y++){x=x.replace(new
RegExp(u[y],"g"),t[y])}w[x]=g.utils.deepReplaceKeyName(C,u,t);if(z!=x){delete
w[z]}}break}return w};var b=q.pluginPathType=
{ABSOLUTE:0,RELATIVE:1,CDN:2};q.getPluginPathType=function(u){if(typeof u!=h)
{return}u=u.split("?")[0];var v=u.indexOf("://");if(v>0){return b.ABSOLUTE}var
t=u.indexOf("/");var w=q.extension(u);if(v<0&&t<0&&(!w||!isNaN(w))){return b.CDN}return
b.RELATIVE};q.getPluginName=function(t){return t.replace(/^(.*\\)?([~]*)-?.*\.
(swfl|js)$/, "$2");q.getPluginVersion=function(t){return t.replace(/[~]*-?([~]....

```

问题 2 / 2

TOC

Flash 参数 AllowScriptAccess 已设置为 always

严重性: **高**

URL: <http://me.hxsd.jc/public/comm/assets/plupload/plupload.full.min.js>

实体: plupload.full.min.js (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: Web 应用程序编程或配置不安全

固定值: 将 AllowScriptAccess 参数设置为“sameDomain”，它会告诉 Flash 播放器仅从同一个域加载作为父级 SWF 的 SWF 文件才会对主管 Web 页面具有脚本访问权限

推理： 响应包含 AllowScriptAccess 参数设置为“always”的 Flash 对象
未经处理的测试响应：

```
...

* Released under GPL License.
*
* License: http://www.plupload.com/license
* Contributing: http://www.plupload.com/contributing
*
* Date: 2015-07-03
*/

!function(e,t){function n(e,t){for(var n,i=[],r=0;r<e.length;++r){if(n=s[e[r]]||o(e[r]),!n)throw"module definition dependency not found:"+"e[r];i.push(n)}t.apply(null,i)}function i(e,i,r){if("string"!==typeof e)throw"invalid module definition, module id must be defined and be a string";if(i===t)throw"invalid module definition, dependencies must be specified";if(r===t)throw"invalid module definition, definition function must be specified";n(i,function(){s[e]=r.apply(null,arguments)})}function r(e){return!s[e]}function o(t){for(var n=e,i=t.split(/[.\/]/),r=0;r<i.length;++r){if(!n[i[r]])return;n=n[i[r]]}return n}function a(n){for(var i=0;i<n.length;i++){for(var r=e,o=n[i],a=o.split(/[.\/]/),u=0;u<a.length-1;++u)r[a[u]]===t&&(r[a[u]]={}),r=r[a[u]];r[a[a.length-1]]=s[o]}var s={},u="moxie/core/Utils/Basic",c="moxie/core/Utils/Env",l="moxie/core/I18n",d="moxie/core/Utils/Mime",h="moxie/core/Utils/Dom",f="moxie/core/Exceptions",p="moxie/core/EventTarget",m="moxie/runtime/Runtime",g="moxie/runtime/RuntimeClient",v="moxie/file/FileInput",w="moxie/core/Utils/Encode",y="moxie/file/Blob",E="moxie/file/File",_="moxie/file/FileDrop",b="moxie/file/FileReader",x="moxie/core/Utils/Url",R="moxie/runtime/RuntimeTarget",A="moxie/file/FileReaderSync",I="moxie/xhr/Formdata",T="moxie/xhr/XMLHttpRequest",S="moxie/runtime/Transporter",O="moxie/image/Image",D="moxie/runtime/html5/Runtime",N="moxie/core/Utils/Events",L="moxie/runtime/html5/file/FileInput",C="moxie/runtime/html5/file/Blob",M="moxie/runtime/html5/file/FileDrop",F="moxie/runtime/html5/file/FileReader",P="moxie/runtime/html5/xhr/XMLHttpRequest",H="moxie/runtime/html5/Utils/BinaryReader",B="moxie/runtime/html5/image/JPEGHeaders",k="moxie/runtime/html5/image/ExifParser",U="moxie/runtime/html5/image/JPEG",G="moxie/runtime/html5/image/PNG",z="moxie/runtime/html5/image/ImageInfo",q="moxie/runtime/html5/image/MegaPixel",j="moxie/runtime/html5/image/Image",X="moxie/runtime/flash/Runtime",V="moxie/runtime/flash/file/FileInput",W="moxie/runtime/flash/file/Blob",Y="moxie/runtime/flash/file/FileReader",Z="moxie/runtime/flash/file/FileReaderSync",J="moxie/runtime/flash/xhr/XMLHttpRequest",K="moxie/runtime/flash/image/Image",Q="moxie/runtime/silverlight/Runtime",ee="moxie/runtime/silverlight/file/FileInput",te="moxie/runtime/silverlight/file/Blob",ne="moxie/runtime/silverlight/file/FileDrop",ie="moxie/runtime/silverlight/file/FileReader",re="moxie/runtime/silverlight/file/FileReaderSync",oe="moxie/runtime/silverlight/xhr/XMLHttpRequest",ae="moxie/runtime/silverlight/runtime/Transporter",se="moxie/runtime/silverlight/image/Image",ue="moxie/runtime/html4/Runtime",ce="moxie/runtime/html4/file/FileInput",le="moxie/runtime/html4/file/FileReader",de="moxie/runtime/html4/xhr/XMLHttpRequest",he="moxie/runtime/html4/image/Image";i(u,[],function(){var e=function(e){var t;return e===t?"undefined":null===e?"null":e.nodeType?"node":{}}.toString().call(e).match(/\\s([a-z|A-Z|+])/)[1].toLowerCase(),t=function(i){var r;return n(arguments,function(o,s){s>0&&n(o,function(n,o){n!==r&&(e(i[o]))===e(n)&&a(e(n),["array","object"])?t(i[o],n):i[o]=n)}),i),n=function(t,n){var i,r,o,a;if(t("number")===e(t.length)){for(o=0,i=t.length;i>o;o++)if(n(t[o],o)===!1)return}else if("object"===e(t))for(r in t)if(t.hasOwnProperty(r)&&n(t[r],r)===!1)return,i=function(t){var n;if(!t||"object"!==e(t))return!0;for(n in t)return!1;return!0},r=function(t,n){function i(r){function t(){return e(t[r])&&t[r](function(e){++r<o&&!e?i(r):n(e)})}var r=0,o=t.length;function t(){return e(n)&&(n=function(){}),t&&t.length|n(i),i(r)},o=function(e,t){var i=0,r=e.length,o=new Array(r);n(e,function(e,n){e(function(e){if(e)return t(e);var a=[];a.slice.call(arguments);a.shift(),o[n]=a,i++,i===r&&(o.unshift(null),t.apply(this,o)))})},a=function(e,t){if(t){if(Array.prototype.indexOf)return Array.prototype.indexOf.call(t,e);for(var n=0,i=t.length;i>n;n++)if(t[n]===e)return n}return-1},s=function(t,n){var i=[];"array"===e(t)&&(t=[t]),"array"===e(n)&&(n=[n]);for(var r in t)-1===a(t[r],n)&&i.push(t[r]);return i.length?i:!1},u=function(e,t){var i=[];return n(e,function(e){-1===a(e,t)&&i.push(e)}),i.length?i:null},c=function(e){var t,n=[];for(t=0;t<e.length;t++)n[t]=e[t];return n},l=function(){var e=0;return function(t){var n=(new Date).getTime().toString(32),i;for(i=0;5>i;i++)n+=Math.floor(65535*Math.random()).toString(32);return t||"o "+n+(e++)}.toString(32)}(),d=function(e){return e?String.prototype.trim:String.prototype.trim.call(e):e.toString().replace(/\\s*/,"").replace(/\\s$/,""):e},h=function(e){if("string"!==typeof e)return e;var t=t:1099511627776,g:1073741824,m:1048576,k:1024,n;return e=/^[0-9\\.|+]{1,64}$/.exec(e.toLowerCase()).replace(/^[^0-9\\.|+]{1,64}/g,""),n=e[2],e+=e[1],t.hasOwnProperty(n)&&(e*=t[n]),Math.floor(e)},f=function(t){var...
```

问题 1 / 4

TOC

SQL 盲注

严重性: 高

URL: http://me.hxsdsd.jc/home/home.html

实体: coachFeeling (Parameter)

风险: 可能会查看、修改或删除数据库条目和表

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

问题 2 / 4

TOC

SQL 盲注

严重性: 高

URL: http://me.hxsdsd.jc/home/home.html

实体: classFeedback (Parameter)

风险: 可能会查看、修改或删除数据库条目和表

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

问题 3 / 4

TOC

SQL 盲注

严重性: **高**

URL: http://me.hxsd.jc/home/home.html

实体: time (Parameter)

风险: 可能会查看、修改或删除数据库条目和表

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

问题 4 / 4

TOC

SQL 盲注

严重性: **高**

URL: http://me.hxsd.jc/home/home.html

实体: dekaron (Parameter)

风险: 可能会查看、修改或删除数据库条目和表

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

高

发现社会保険号模式 ①

TOC

问题 1 / 1

TOC

发现社会保险号模式

严重性: **高**

URL: <http://me.hxsd.jc/public/comm/assets/scripts/form-components.js>

实体: form-components.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的社会保险号

推理: 响应包含社会保险号。

未经处理的测试响应:

```
...  
  
$("#mask_currency").inputmask('â¬ 999.999.999,99', {  
    numericInput: true  
}); //123456 => â¬ _____.__1.234,56  
  
$("#mask_currency2").inputmask('â¬ 999,999,999.99', {  
    numericInput: true,  
    rightAlignNumerics: false,  
    greedy: false  
}); //123456 => â¬ _____.__1.234,56  
$("#mask_ssn").inputmask("999-99-9999", {  
    placeholder: " ",  
    clearMaskOnLostFocus: true  
}); //default  
}  
  
var handleIPAddressInput = function () {  
    $('#input_ipv4').ipAddress();  
    $('#input_ipv6').ipAddress({  
        v: 6  
    });  
}  
  
...
```

高

发现数据库错误模式 ①

TOC

问题 1 / 1

TOC

发现数据库错误模式

严重性: **高**

URL: http://me.hxsd.jc/home/resume/add

实体: student_info (Global)

风险: 可能会查看、修改或删除数据库条目和表

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性, 因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

未经处理的测试响应:

```
...

Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.9
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22b498e8adc7051e6c19a74a7286435252%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466127034%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7De173ee7676ebbaaeb794f0af04db0c2b744fd08; expires=Fri, 17-Jun-2016 03:30:34 GMT; path=/

<!DOCTYPE html>
<html lang="en">
<head>
<title>Database Error</title>
<style type="text/css">
...

...

p {
margin: 12px 15px 12px 15px;
}
</style>
</head>
<body>
<div id="container">
<h1>发生了一个数据库错误</h1>
<p>Error Number: 1064</p><p>You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'or
announcement.termid = or announcement.classid = )
GROUP BY (announcement' at line 4</p><p>
SELECT * FROM announcementtext
LEFT JOIN announcement ON announcementtext.announcementtextid = announcement.announcementtextid
WHERE announcementtext.deleted = 0
AND (announcement.campusid = or announcement.termid = or announcement.classid = )
GROUP BY (announcementtext.announcementtextid)
ORDER BY announcementtext.dateline DESC

</p><p>Filename: /data/hxsd/web_test/me_test/core/database/DB_driver.php</p><p>Line Number:
334</p> </div>
...
```


问题 1 / 5

TOC

发现压缩目录

严重性: 低

URL: http://me.hxsd.jc/home/index/index/

实体: index.zip (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

问题 2 / 5

TOC

发现压缩目录

严重性: 低

URL: http://me.hxsd.jc/home/index/index/

实体: index.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

问题 3 / 5

TOC

发现压缩目录

严重性: **低**

URL: <http://me.hxsd.jc/home/index/index/>

实体: index.rar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

问题 4 / 5

TOC

发现压缩目录

严重性: **低**

URL: <http://me.hxsd.jc/home/index/index/>

实体: index.tar (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

问题 5 / 5

TOC

发现压缩目录

严重性: **高**

URL: <http://me.hxsd.jc/public/comm/assets/annex/echarts/>

实体: echarts.gz (Page)

风险: 可能会检索服务器端脚本的源代码, 这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 除去压缩目录文件或限制对它的访问

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索

了所请求的文件的内容。

未经处理的测试响应:

```
GET /public/comm/assets/annex/echarts/echarts.gz HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/index/index/phone.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.2.0</center>
</body>
</html>
...
```

归档文件下载	
严重性:	高
URL:	http://me.hxsd.jc/home/announcement/getcontentbyid/8
实体:	8 (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

未经处理的测试响应：

```
...
GET /home/announcement/getcontentbyid/8.arc HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
...
```

归档文件下载

严重性: **高**

URL: <http://me.hxsd.jc/home/announcement/getcontentbyid/6>

实体: 6 (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容, 表示源代码检索已成功。

未经处理的测试响应:

```
...
GET /home/announcement/getcontentbyid/6.arc HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
...
```

问题 3 / 5

TOC

归档文件下载

严重性: **高**

URL: <http://me.hxsd.jc/home/announcement/getcontentbyid/5>

实体: 5 (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容, 表示源代码检索已成功。

未经处理的测试响应:

```
...
GET /home/announcement/getcontentbyid/5.arc HTTP/1.1
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A2222%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A7Bs%3A10%3A22student_id%22%3Bs%3A2%3A2297%22%3Bs%3A12%3A22student_name%22%3Bs%3A14%3A22xuehaoxuesheng%22%3Bs%3A16%3A22student_password%22%3Bs%3A32%3A224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A22student_number%22%3Bs%3A13%3A220010116070001%22%3Bs%3A17%3A22student_temp_pass%22%3Bs%3A6%3A22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

问题 4 / 5

TOC

归档文件下载

严重性: **高**

URL: http://me.hxsd.jc/home/announcement/getcontentbyid/1

实体: 1 (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容, 表示源代码检索已成功。
未经处理的测试响应:

```
...
GET /home/announcement/getcontentbyid/1.arc HTTP/1.1
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A2222%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A7Bs%3A10%3A22student_id%22%3Bs%3A2%3A2297%22%3Bs%3A12%3A22student_name%22%3Bs%3A14%3A22xuehaoxuesheng%22%3Bs%3A16%3A22student_password%22%3Bs%3A32%3A224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A22student_number%22%3Bs%3A13%3A220010116070001%22%3Bs%3A17%3A22student_temp_pass%22%3Bs%3A6%3A22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
```

```
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

归档文件下载

严重性: **高**

URL: <http://me.hxsd.jc/home/announcement/getcontentbyid/7>

实体: 7 (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

未经处理的测试响应:

```
...
GET /home/announcement/getcontentbyid/7.arc HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udmele122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

会话 cookie 中缺少 HttpOnly 属性**严重性:** 高**URL:** http://me.hxsd.jc/home/student/login.html**实体:** PHPSESSID (Cookie)**风险:** 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务**原因:** Web 应用程序设置了缺少 HttpOnly 属性的会话 cookie**固定值:** 向所有会话 cookie 添加“HttpOnly”属性**推理:** AppScan 发现所用的会话 cookie 没有“HttpOnly”属性。**原始响应**

```
...  
  
Server: nginx/1.2.0  
Date: Fri, 17 Jun 2016 01:18:38 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
Vary: Accept-Encoding  
X-Powered-By: PHP/5.4.9  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Set-Cookie: PHPSESSID=21v2mqbqnmuh2tvm6asd6t3jb7; path=/  
x-ua-compatible: IE=edge  
  
<!DOCTYPE html>  
<!--  
Template Name: Metronic - Responsive Admin Dashboard Template build with Twitter Bootstrap 3.0.2  
Version: 1.5.4  
Author: KeenThemes  
Website: http://www.keenthemes.com/  
Purchase: http://themeforest.net/item/metronic-responsive-admin-dashboard-template/4021469?  
ref=keenthemes  
  
...
```


会话 cookie 中缺少 HttpOnly 属性

严重性: **高**

URL: <http://me.hxsd.jc/>

实体: ci_session (Cookie)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: Web 应用程序设置了缺少 HttpOnly 属性的会话 cookie

固定值: 向所有会话 cookie 添加“HttpOnly”属性

推理: AppScan 发现所用的会话 cookie 没有“HttpOnly”属性。

原始响应

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.9
Location: http://me.hxsd.jc/home/student/login.html
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a; expires=Fri, 17-Jun-2016 03:18:37 GMT; path=/

GET /home/student/login.html HTTP/1.1
...
```

问题 1 / 3

TOC

会话标识未更新

严重性: 低

URL: http://me.hxsd.jc/home/student/check_login

实体: check_login (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: Web 应用程序编程或配置不安全

固定值: 登录之后更改会话标识符值

推理: 测试结果似乎指示存在脆弱性，因为“原始请求”（左侧）和“响应”（右侧）中的会话标识相同。这些标志应该已在响应中更新。

问题 2 / 3

TOC

会话标识未更新

严重性: 高

URL: http://me.hxsd.jc/home/student/forgot_password


实体: forgot_password (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: Web 应用程序编程或配置不安全

固定值: 登录之后更改会话标识符值

推理: 测试结果似乎指示存在脆弱性，因为“原始请求”（左侧）和“响应”（右侧）中的会话标识相同。这些标志应该已在响应中更新。

会话标识未更新**严重性:**  高**URL:** http://me.hxsd.jc/home/student/change_password**实体:** change_password (Page)**风险:** 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务**原因:** Web 应用程序编程或配置不安全**固定值:** 登录之后更改会话标识符值

推理: 测试结果似乎指示存在脆弱性，因为“原始请求”（左侧）和“响应”（右侧）中的会话标识相同。这些标志应该已在响应中更新。

问题 1 / 6

TOC

跨站点脚本编制

严重性: 高

URL: http://me.hxsd.jc/home/technicalsupport/save

实体: save (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

```
...

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: '"></a><script>alert(1026)</script>
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:28:15 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ec923b1f0476614efc9552b41403ee8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126895%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D0c20c3c955a9951b0ad32644e81465738ffe2e4e; expires=Fri, 17-Jun-2016 03:28:15 GMT; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<html lang="zh-CN">

...

...

.logo_bg{position:absolute;z-index:-1;width:100%;height:100%;top:0px;left:0px;}
```

```

</style>
<body>
<div class="logo_bg"></div>
<div class="panel panel-primary error">
<div class="panel-heading"><h3 class="panel-title">提示信息</h3></div>
<div class="panel-body">
<h3>
请填写您的问题描述, <span id="redirecttime">3</span>秒后自动跳转!
<a href=""></a><script>alert(1026)</script>">点击跳转! </a>
</h3>
</div>
</div>

<script type="text/javascript">
$(document).ready(function(){

...

```

问题 2 / 6

TOC

跨站点脚本编制

严重性: **高**

URL: http://me.hxsd.jc/home/technicalsupport.html

实体: technicalsupport.html (Page)

风险: 可能会窃取或操纵客户会话和 cookie, 它们可能用于模仿合法用户, 从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性, 因为 Appscan 在响应中成功嵌入了脚本, 在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

```

...

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/index/index/phone.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:58:52 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ad356e593e87acc500216705c78082d4%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3

```

```

A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B
+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466128
732%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D3d9340073394fe42374c83f830adc5866a6c7ee2;
expires=Fri, 17-Jun-2016 03:58:52 GMT; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<!--[if IE 8]> <html lang="en" class="ie8 no-js"> <![endif]-->

...

...

</td>
</tr>

</tbody>

</table>
</div>
</div>
<!--question info-->
<div class="col-xs-12 clearfix" style="padding-top:10px;border-top:1px solid #e0e0e0;">
  <div class="task_zhu">请对已提交的问题进行评价, 如果您在24小时之内未进行评价, 将默认结束此任务
</div>
  <div class="pages_style" id="pages" > 133 条记录 1/9 页 <a
href='http://me.hxsd.jc/home/technicalsupport/index?'>'><script>alert(3130)</script>=&p=2'>下一页
</a>
    <span class='current'>1</span><a href='http://me.hxsd.jc/home/technicalsupport/index?
>'><script>alert(3130)</script>=&p=2'>2</a><a
href='http://me.hxsd.jc/home/technicalsupport/index?'>'><script>alert(3130)</script>=&p=3'>3</a>
<a href='http://me.hxsd.jc/home/technicalsupport/index?'>'><script>alert(3130)
</script>=&p=4'>4</a><a href='http://me.hxsd.jc/home/technicalsupport/index?'>'>
<script>alert(3130)</script>=&p=5'>5</a> <a href='http://me.hxsd.jc/home/technicalsupport/index?
>'><script>alert(3130)</script>=&p=6' >下5页</a> <a
href='http://me.hxsd.jc/home/technicalsupport/index?'>'><script>alert(3130)</script>=&p=9' >最后一
页</a></div>
  </div>
</div>
</div>
<!-- END TAB SWITCH-->
</div>
<!-- END PAGE -->

<!-- END CONTAINER -->

...

```

问题 3 / 6

TOC

跨站点脚本编制

严重性: **高**

URL: http://me.hxsd.jc/home/feedback/save

实体: save (Page)

风险: 可能会窃取或操纵客户会话和 cookie, 它们可能用于模仿合法用户, 从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性, 因为 Appscan 在响应中成功嵌入了脚本, 在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

```
...

Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 126

categoryid=%3E%22%27%3E%3Cscript%3Ealert%28969%29%3C%2Fscript%3E&content=%3E%22%27%3E%3Cscript%3E
alert%28969%29%3C%2Fscript%3E

HTTP/1.1 500 Internal Server Error
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:28:02 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.9
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22fc8a4089159e5232562029a593e82004%22
%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3
A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B
+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126
881%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Db72b63c8646e629d41c2fde29fac270d7b78fd29;
expires=Fri, 17-Jun-2016 03:28:01 GMT; path=/

<!DOCTYPE html>
<html lang="en">
<head>
<title>Database Error</title>
...

...

p {
margin: 12px 15px 12px 15px;
}
</style>
</head>
<body>
<div id="container">
<h1>发生了一个数据库错误</h1>
<p>Error Number: 1054</p><p>Unknown column 'campusid' in 'field list'</p><p>INSERT INTO
`feedback` (`title`, `content`, `categoryid`, `studentid`, `classid`, `campusid`, `facultyid`,
`dateline`) VALUES (0, '>\"'\>[removed]alert&#40;969&#41;[removed]', '>\"'\><script>alert(969)
</script>', '97', '3953', '1', '5', 1466126881)</p><p>Filename:
/data/hxsd/web_test/me_test/core/database/DB_driver.php</p><p>Line Number: 334</p> </div>
</body>
</html>
...
```

跨站点脚本编制

严重性: **高**

URL: <http://me.hxsd.jc/home/technicalsupport/saveComment>

实体: saveComment (Page)

风险: 可能会窃取或操纵客户会话和 cookie, 它们可能用于模仿合法用户, 从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性, 因为 Appscan 在响应中成功嵌入了脚本, 在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

```
...

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: "</a><script>alert(1043)</script>"
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:28:15 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%220492b681140636ad6d01cae4c7c0c671%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126895%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D29a753ad0c2f1c9eaf3af09179f84b5f35f6d2d4; expires=Fri, 17-Jun-2016 03:28:15 GMT; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<html lang="zh-CN">

...

...

.logo_bg{position:absolute;z-index:-1;width:100%;height:100%;top:0px;left:0px;}
</style>
<body>
<div class="logo_bg"></div>
<div class="panel panel-primary error">
  <div class="panel-heading"><h3 class="panel-title">提示信息</h3></div>
  <div class="panel-body">
    <h3>
      评价失败, 请联系技术支持协助处理, <span id="redirecttime">3</span>秒后自动跳转!
      <a href=""></a><script>alert(1043)</script>">点击跳转! </a>
    </h3>
  </div>
</div>

<script type="text/javascript">
$(document).ready(function(){
```


...

跨站点脚本编制

严重性: **高**

URL: <http://me.hxsd.jc/home/technicalsupport/index>

实体: index (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

...

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/technicalsupport.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 02:00:27 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%229652c9d54f15cb6be50d447956ed0605%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466128827%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D51c33f8605994f0974c880d718225e904f50b4b0; expires=Fri, 17-Jun-2016 04:00:27 GMT; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<!--[if IE 8]> <html lang="en" class="ie8 no-js"> <![endif]-->

...

...

</td>
</tr>

</tbody>

</table>
</div>
</div>
```

```

<!--question info-->
<div class="col-xs-12 clearfix" style="padding-top:10px;border-top:1px solid #e0e0e0;">
  <div class="task_zhu">请对已提交的问题进行评价，如果您在24小时之内未进行评价，将默认结束此任务
</div>
  <div class="pages_style" id="pages"> 140 条记录 1/10 页 <a
href='http://me.hxsd.jc/home/technicalsupport/index?'"><script>alert(3757)</script>=&p=2'>下一页
</a>
    <span class='current'>1</span><a href='http://me.hxsd.jc/home/technicalsupport/index?
'"><script>alert(3757)</script>=&p=2'>2</a><a
href='http://me.hxsd.jc/home/technicalsupport/index?'"><script>alert(3757)</script>=&p=3'>3</a>
<a href='http://me.hxsd.jc/home/technicalsupport/index?'"><script>alert(3757)
</script>=&p=4'>4</a><a href='http://me.hxsd.jc/home/technicalsupport/index?'">
<script>alert(3757)</script>=&p=5'>5</a> <a href='http://me.hxsd.jc/home/technicalsupport/index?
'"><script>alert(3757)</script>=&p=6' >下5页</a> <a
href='http://me.hxsd.jc/home/technicalsupport/index?'"><script>alert(3757)</script>=&p=10' >最后
一页</a></div>
  </div>
</div>
</div>
<!-- END TAB SWITCH-->
</div>
<!-- END PAGE -->

<!-- END CONTAINER -->

...

```

问题 6 / 6

TOC

跨站点脚本编制

严重性: **高**

URL: http://me.hxsd.jc/home/technicalsupport/index

实体: ttaskid (Parameter)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应:

```

...

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/technicalsupport.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:37:47 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

```

```

Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ae8cb6e1ca46fc10bbef51ec4931e9d7%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466127467%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D5b70f534131aa2e9d286d19a105c4d9eb6d965ac;
expires=Fri, 17-Jun-2016 03:37:47 GMT; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<!--[if IE 8]> <html lang="en" class="ie8 no-js"> <![endif]-->

...

...

<!-- BEGIN TAB SWITCH -->
<div class="portlet-body">
  <div class="tabbable-custom">
    <div class="tab-content">
      <!--question info-->
      <div class="row">

        <div class="col-xs-12 ">
          <form class="form-horizontal" method="post" action="/home/technicalsupport/save"
onsubmit="return checkSubmitTimes()" ">
            <input type="hidden" name="tstaskid" value=""/><script>alert(1288)</script>">
            <div class="task_tit_bg padt15" >
              <div class="form-group">
                <label class="control-label fl pl35 mt5">问题描述:</label>
                <div class="col-md-8">
                  <input type="text" class="form-control" maxlength="50"
required value=""
name="description"/>
                </div>
                <button id="sbt" type="submit" class="btn green ">快来帮帮我</button>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>

```

高

跨站点请求伪造 3

TOC

问题 1 / 3

TOC

跨站点请求伪造

严重性: 高

URL: http://me.hxsd.jc/home/student/forgot_password

实体: forgot_password (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 拒绝恶意请求

推理： 测试结果似乎指示存在漏洞，因为右侧的测试响应与左侧的原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。



跨站点请求伪造	
严重性：	高
URL：	http://me.hxsd.jc/home/student/change_password
实体：	change_password (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求

推理： 测试结果似乎指示存在漏洞，因为右侧的测试响应与左侧的原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。



跨站点请求伪造	
严重性:	高
URL:	http://me.hxsd.jc/home/student/check_login
实体:	check_login (Page)
风险:	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因:	应用程序使用的认证方法不充分
固定值:	拒绝恶意请求

推理: 测试结果似乎指示存在漏洞，因为右侧的测试响应与左侧的原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应



测试响应



高	链接注入（便于跨站请求伪造） 1	TOC
---	------------------	-----

链接注入（便于跨站请求伪造）

严重性： **高**

URL： <http://me.hxsd.jc/home/technicalsupport/index>

实体： **tstaskid (Parameter)**

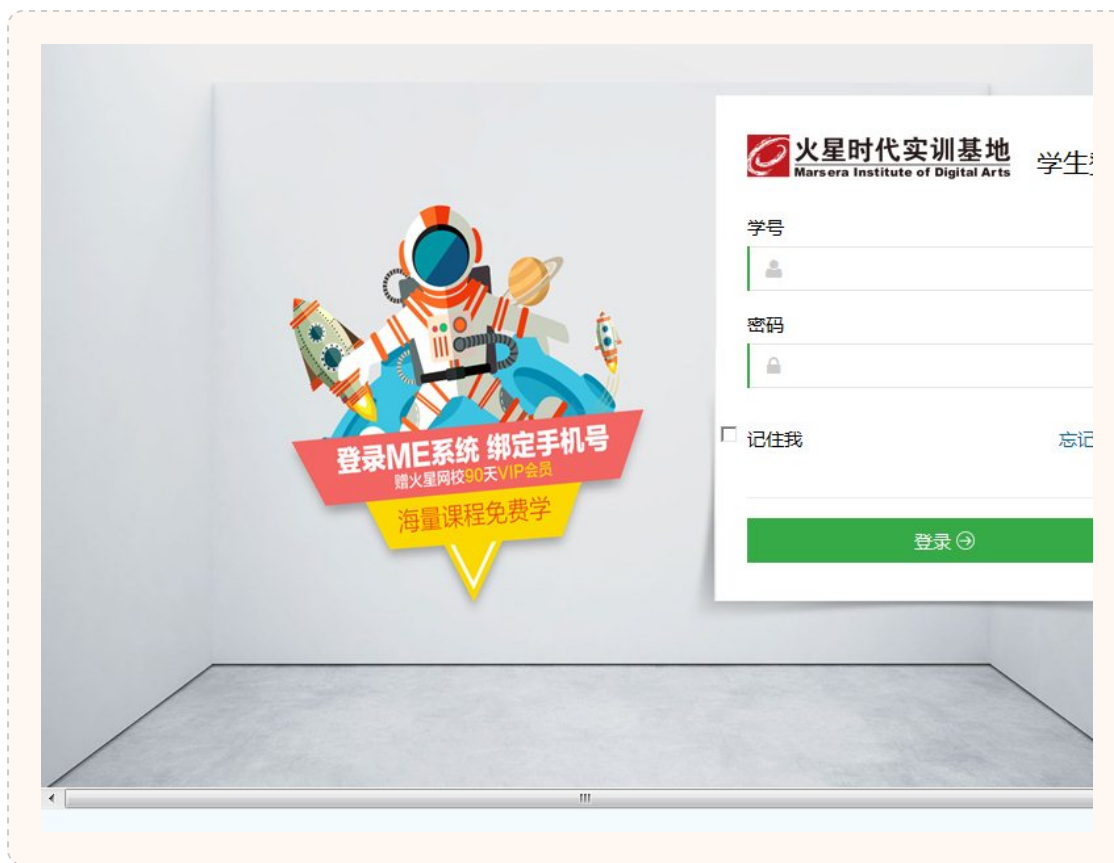
风险： 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

原因： 未对用户输入正确执行危险字符清理

固定值： 查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试响应



高

临时文件下载 5

TOC

临时文件下载	
严重性:	高
URL:	http://me.hxsd.jc/home/announcement/getcontentbyid/8
实体:	8 (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
未经处理的测试响应：

```
...
GET /home/announcement/getcontentbyid/8.old HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfc23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
...
```

临时文件下载	
严重性:	高
URL:	http://me.hxsd.jc/home/announcement/getcontentbyid/6
实体:	6 (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
未经处理的测试响应：

```
...
GET /home/announcement/getcontentbyid/6.old HTTP/1.1
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A222%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A7Bs%3A10%3A22student_id%22%3Bs%3A2%3A2297%22%3Bs%3A12%3A22student_name%22%3Bs%3A14%3A22xuehaoxuesheng%22%3Bs%3A16%3A22student_password%22%3Bs%3A32%3A224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A22student_number%22%3Bs%3A13%3A220010116070001%22%3Bs%3A17%3A22student_temp_pass%22%3Bs%3A6%3A22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

临时文件下载	
严重性：	高
URL：	http://me.hxsd.jc/home/announcement/getcontentbyid/1
实体：	1 (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。
未经处理的测试响应：

```
...
GET /home/announcement/getcontentbyid/1.old HTTP/1.1
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A222%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A7Bs%3A10%3A22student_id%22%3Bs%3A2%3A2297%22%3Bs%3A12%3A22student_name%22%3Bs%3A14%3A22xuehaoxuesheng%22%3Bs%3A16%3A22student_password%22%3Bs%3A32%3A224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A22student_number%22%3Bs%3A13%3A220010116070001%22%3Bs%3A17%3A22student_temp_pass%22%3Bs%3A6%3A22236985%22%3B%7D
Accept-Language: en-US
```



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

问题 4 / 5

TOC

临时文件下载

严重性: **高**

URL: http://me.hxsd.jc/home/announcement/getcontentbyid/5

实体: 5 (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去虚拟目录中的旧版本文件

推理: 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

未经处理的测试响应:

```
...
GET /home/announcement/getcontentbyid/5.sav HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

临时文件下载	
严重性:	高
URL:	http://me.hxsd.jc/home/announcement/getcontentbyid/7
实体:	7 (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去虚拟目录中的旧版本文件

推理： 测试尝试检索源代码文件。响应未产生错误且包含非 HTML 内容，表示源代码检索已成功。

未经处理的测试响应：

```
...
GET /home/announcement/getcontentbyid/7.old HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfc23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/announcement/index.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

通过框架钓鱼

严重性: **高**

URL: <http://me.hxsd.jc/home/technicalsupport/index>

实体: **tstaskid** (Parameter)

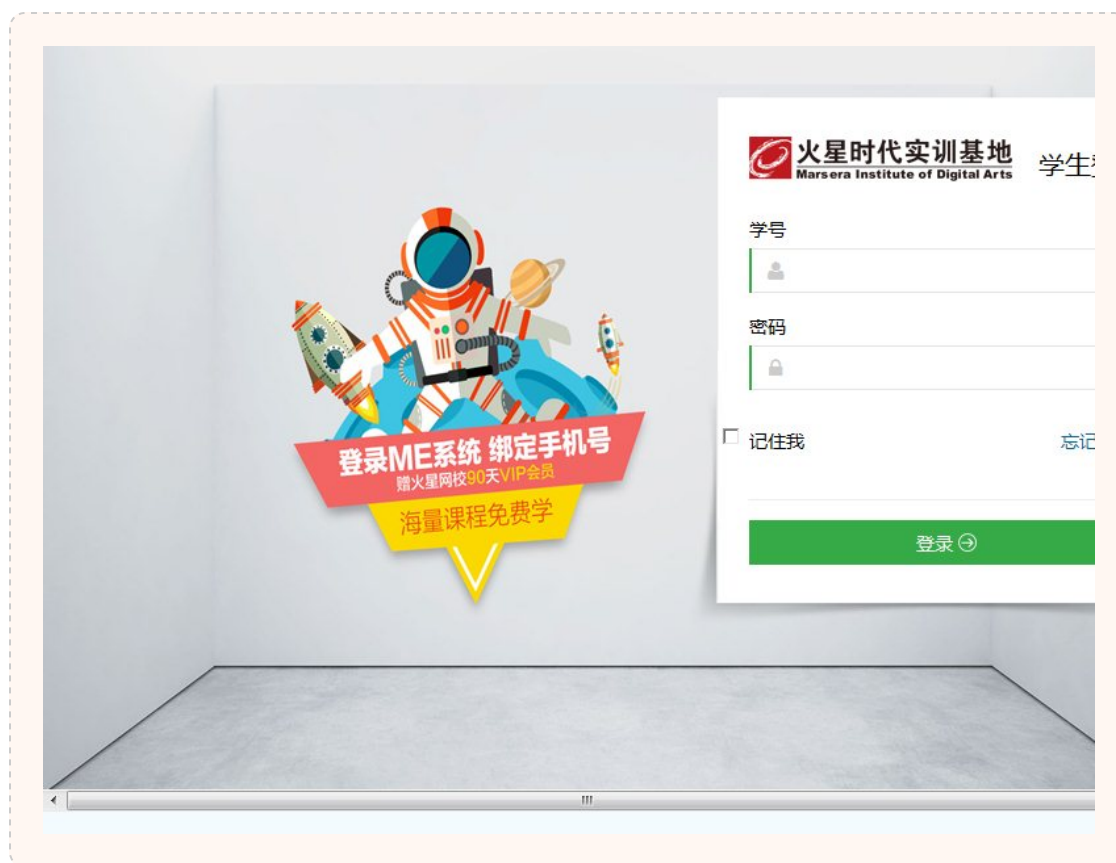
风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: 未对用户输入正确执行危险字符清理

固定值: 查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "<http://demo.testfire.net/phishing.html>" 的 frame/iframe。

测试响应



问题 1 / 9

TOC

已解密的登录请求

严重性: 低

URL: http://me.hxsd.jc/home/student/check_login

实体: password (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

问题 2 / 9

TOC

已解密的登录请求

严重性: 高

URL: http://me.hxsd.jc/home/student/forgot_password

实体: forgot_password (Page)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

原始请求

```
username=0010116070001&stunumber=9876543210&idpepal=0010116070001&password=236985&rpasword=236985
```

已解密的登录请求	
严重性:	高
URL:	http://me.hxsd.jc/home/student/forgot_password
实体:	password (Parameter)
风险:	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因:	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

```
...
Content-Type: application/x-www-form-urlencoded
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a;
PHPSESSID=21v2mqbqnmuh2tvm6asd6t3jb7
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/forgot_password
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 98

username=0010116070001&stunumber=9876543210&idpepal=0010116070001&password=236985&rpassword=236985

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:44 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
...
```

已解密的登录请求

严重性: **高**

URL: http://me.hxsd.jc/home/student/forgot_password

实体: rpassword (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

```
...

Content-Type: application/x-www-form-urlencoded
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A22%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a;
PHPSESSID=21v2mqbqnmuh2tvm6asd6t3jb7
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/forgot_password
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 98

username=0010116070001&stunumber=9876543210&idpepal=0010116070001&password=236985&rpassword=236985

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:44 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9

...
```

已解密的登录请求

严重性: **高**

URL: http://me.hxsd.jc/home/student/change_password

实体: change_password (Page)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

原始请求

```
username=0010116070001&password=236985&rpasword=236985
```

问题 6 / 9

TOC

已解密的登录请求

严重性: **高**

URL: http://me.hxsd.jc/home/student/change_password

实体: username (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

```
...
Content-Type: application/x-www-form-urlencoded
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ad7e6923b1b8b012bd75cb1611d37c8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126331%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D9b2300f53988058fe000fc593d9ab3dbb92a816e;
PHPSESSID=q90ft7punl8802kprfgm8g5o10;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/change_password.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 55
```

```
username=0010116070001&password=236985&rpasword=236985
```

```
HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:19:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
```

```
...
```

问题 7 / 9

TOC

已解密的登录请求

严重性: **高**

URL: http://me.hxsd.jc/home/student/change_password

实体: password (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

```
...

Content-Type: application/x-www-form-urlencoded
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ad7e6923b1b8b012bd75cb1611d37c8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126331%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D9b2300f53988058fe000fc593d9ab3dbb92a816e;
PHPSESSID=q90ft7punl8802kprfgm8g5o10;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/change_password.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 55

username=0010116070001&password=236985&rpasword=236985
```

```
HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:19:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
```


X-Powered-By: PHP/5.4.9

...

问题 8 / 9

TOC

已解密的登录请求

严重性: **高**

URL: http://me.hxsd.jc/home/student/change_password

实体: rpassword (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

...

Content-Type: application/x-www-form-urlencoded

Cookie:

ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ad7e6923b1b8b012bd75cb1611d37c8%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126331%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D9b2300f53988058fe000fc593d9ab3dbb92a816e; PHPSESSID=q90ft7pun18802kprfgm8g5o10; student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D

Accept-Language: en-US

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Referer: http://me.hxsd.jc/home/student/change_password.html

Host: me.hxsd.jc

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

Content-Length: 55

username=0010116070001&password=236985&rpassword=236985

HTTP/1.1 200 OK

Server: nginx/1.2.0

Date: Fri, 17 Jun 2016 01:19:16 GMT

Content-Type: text/html


Transfer-Encoding: chunked

Connection: keep-alive

Vary: Accept-Encoding

X-Powered-By: PHP/5.4.9

...

已解密的登录请求**严重性:**  **高****URL:** http://me.hxsd.jc/home/student/check_login**实体:** check_login (Page)**风险:** 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息**原因:** 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递**固定值:** 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。**推理:** AppScan 识别了不是通过 SSL 发送的登录请求。

问题 1 / 1

TOC

永久 Cookie 包含敏感的会话信息

严重性: 高

URL: http://me.hxsd.jc/

实体: ci_session (Cookie)

风险: 可能会窃取保存在磁盘上作为永久 cookie 的会话信息 (cookie)

原因: Web 应用程序将敏感的会话信息存储在永久 cookie 中 (磁盘上)

固定值: 避免在永久 cookie 中存储敏感的会话信息

推理: AppScan 发现会话标识 cookie 存储在客户机中。

原始响应

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:37 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.9
Location: http://me.hxsd.jc/home/student/login.html
Set-Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a; expires=Fri, 17-Jun-2016 03:18:37 GMT; path=/

GET /home/student/login.html HTTP/1.1
...
```

高

在参数值中找到了内部 IP 公开模式 ①

TOC

问题 1 / 1

TOC

在参数值中找到了内部 IP 公开模式

严重性: 高

URL: http://me.hxsd.jc/public/comm/assets/faceimage/expressInstall.swf

实体: upload_url (Parameter)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的内部 IP 地址

推理: 参数值包含内部 IP 地址, 这些地址可能会帮助攻击者计划进一步进攻。

高

自动填写未对密码字段禁用的 HTML 属性 ①

TOC

问题 1 / 1

TOC

自动填写未对密码字段禁用的 HTML 属性

严重性: 高

URL: http://me.hxsd.jc/home/student/change_password

实体: change_password (Page)

风险: 可能会绕过 Web 应用程序的认证机制

原因: Web 应用程序编程或配置不安全

固定值: 将“autocomplete”属性正确设置为“off”

推理: AppScan 发现密码字段没有强制禁用自动填写功能。

未经处理的测试响应:

```
POST /home/student/change_password HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A%22ad7e6923b1b8b012bd75cb1611d37c8%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B
```

```
+ .NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126
331%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D9b2300f53988058fe000fc593d9ab3dbb92a816e;
PHPSESSID=q90ft7punl8802kprfgm8g5o10;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%2
2%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a
0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%2
2student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/change_password.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 55

username=0010116070001&password=236985&rpasword=236985

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:19:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
...
```

问题 1 / 8

TOC

HTML 注释敏感信息泄露

严重性: 低

URL: http://me.hxsd.jc/home/student/login.html

实体: Template Name: Metronic - Responsive Admin Dashboard Template build with Twitter Bootstrap 3.0.2 (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理: AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...

X-Powered-By: PHP/5.4.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=2lv2mqbqnmuh2tvm6asd6t3jb7; path=/
x-ua-compatible: IE=edge

<!DOCTYPE html>
<!--
Template Name: Metronic - Responsive Admin Dashboard Template build with Twitter Bootstrap 3.0.2
Version: 1.5.4
Author: KeenThemes
Website: http://www.keenthemes.com/
Purchase: http://themeforest.net/item/metronic-responsive-admin-dashboard-template/4021469?ref=keenthemes
-->
<!--[if IE 8]> <html lang="en" class="ie8 no-js"> <![endif]-->
<!--[if IE 9]> <html lang="en" class="ie9 no-js"> <![endif]-->
<!--[if !IE]><!--> <html lang="en" class="no-js"> <!--<![endif]-->
<!-- BEGIN HEAD -->
<head>
<meta charset="utf-8" />
<title>学生登录</title>
<meta http-equiv="X-UA-Compatible" content="IE=edge">

...
```

HTML 注释敏感信息泄露	
严重性:	低
URL:	http://me.hxsd.jc/home/student/forgot_password
实体:	<div class="form-group"> (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	程序员在 Web 页面上留下调试信息
固定值:	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
GET /home/student/forgot_password HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a; PHPSESSID=21v2mqbqnmuh2tvm6asd6t3jb7
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/student/login.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:44 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
...
```

HTML 注释敏感信息泄露

严重性: **低**

URL: http://me.hxsd.jc/home/student/login.html

实体: <div class="mr_top15"><i class="fa fa-use... (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理: AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
GET /home/student/login.html HTTP/1.1
Cookie:
ci_session=a%3A5%3A7Bs%3A10%3A22session_id%22%3Bs%3A32%3A22279141aeab85a0fbdb3092a76477beec%22%3Bs%3A10%3A22ip_address%22%3Bs%3A11%3A2210.2.20.176%22%3Bs%3A10%3A22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A22user_data%22%3Bs%3A0%3A2222%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:38 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
...
```

问题 4 / 8

TOC

HTML 注释敏感信息泄露

严重性: **低**

URL: http://me.hxsd.jc/home/student/forgot_password

实体: Template Name: Metronic - Responsive Admin Dashboard Template build with Twitter Bootstrap 3.0.2 (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。
原始响应

```
...

Vary: Accept-Encoding
X-Powered-By: PHP/5.4.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
x-ua-compatible: IE=edge

<!DOCTYPE html>
<!--
Template Name: Metronic - Responsive Admin Dashboard Template build with Twitter Bootstrap 3.0.2
Version: 1.5.4
Author: KeenThemes
Website: http://www.keenthemes.com/
Purchase: http://themeforest.net/item/metronic-responsive-admin-dashboard-template/4021469?ref=keenthemes
-->
<!--[if IE 8]> <html lang="en" class="ie8 no-js"> <![endif]-->
<!--[if IE 9]> <html lang="en" class="ie9 no-js"> <![endif]-->
<!--[if !IE]><!--> <html lang="en" class="no-js"> <!--<![endif]-->
<!-- BEGIN HEAD -->
<head>
<meta charset="utf-8" />
<title>找回密码</title>
<meta http-equiv="X-UA-Compatible" content="IE=edge">

...

```

HTML 注释敏感信息泄露	
严重性：	低
URL：	http://me.hxsd.jc/home/index/index/phone.html
实体：	<i class="fa fa fa-comment"></i> 建议和投诉 (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

HTML 注释敏感信息泄露

严重性: **低**

URL: `http://me.hxsd.jc/home/index/index/phone.html`

实体: `<script src="http://me.hxsd.jc/public/admin/js/pageview_logs.js"></script>` (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理: AppScan 发现了包含看似为敏感信息的 HTML 注释。

问题 7 / 8

TOC

HTML 注释敏感信息泄露

严重性: **低**

URL: `http://me.hxsd.jc/home/process.html`

实体: `<li class="">` (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理: AppScan 发现了包含看似为敏感信息的 HTML 注释。

问题 8 / 8

TOC

HTML 注释敏感信息泄露

严重性: **低**

URL: `http://me.hxsd.jc/home/resume/add`

实体: `<link href="http://me.hxsd.jc/public/comm/assets/plugins/jquery-hydx/zyzn_2.css" type="text/css" rel...>` (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: 程序员在 Web 页面上留下调试信息

固定值: 除去 HTML 注释中的敏感信息

推理: AppScan 发现了包含看似为敏感信息的 HTML 注释。

低

Microsoft FrontPage Htimage.exe 命令执行和路径泄露 1

TOC

问题 1 / 1

TOC

Microsoft FrontPage Htimage.exe 命令执行和路径泄露

严重性: 低

URL: http://me.hxsd.jc/home/index/index/

实体: htimage.exe (Page)

风险: 可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容

原因: 在 Web 站点上安装了缺省样本脚本或目录

固定值: 删除 Htimage.exe 和 Imagemap.exe 的所有副本

推理: 响应包含服务器上文件的绝对路径和/或文件名。

低

发现电子邮件地址模式 4

TOC

问题 1 / 4

TOC

发现电子邮件地址模式

严重性: 低

URL: http://me.hxsd.jc/public/comm/assets/scripts/form-validation.js

实体: form-validation.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的电子邮件地址

推理: 响应包含可能是专用的电子邮件地址。

未经处理的测试响应:

...

```
    },
    qq: {
      required: '请输入QQ',
      maxlength: jQuery.format("请输入 {0} 位以上的数字"),
      minlength: jQuery.format("请输入 {0} 位以上的数字"),
      digits: '请输入数字'
    },
    email: {
      required: '请输入email',
      email: '(example@example.com) 请输入正确的email'
    },
    intentionjob: {
      required: '请输入意向岗位'
    },
    'workexperience[startdate][]': {
      required: '请输入开始时间'
    },
    'workexperience[enddate][]': {
      required: '请输入结束时间'
    }
  },
  ...
}
```

发现电子邮件地址模式	
严重性:	低
URL:	http://me.hxsd.jc/home/resume/add.html
实体:	add.html (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	除去 Web 站点中的电子邮件地址

推理: 响应包含可能是专用的电子邮件地址。

未经处理的测试响应:

```
...
    </div>
  </div>
</div>
<div class="form-group row">
  <label for="" class="col-md-2 col-sm-2 text-right control-label"><b
class="alertred">*</b>电子邮箱:</label>
  <div class="col-md-5 col-sm-4">
    <input type="text" name="email" style="width:188px;" class="form-
control email"
      maxlength="30" id="" placeholder="请输入您的联系邮箱"
      value="" />
    <span style="color:#b94a48;display:none;">(example@example.com) 请输入正确的
email</span>
  </div>
</div>
</div>
  <div class="form-group row" >
    <label class=" text-right col-sm-2"><b class="alertred">*</b>上传证件照片 :
  </label>
  <div class="col-md-4" id="container">
```

```
<input id="preview_path" value="" name="picture" type="hidden">
    <div id="imagePlug">
...

```

发现电子邮件地址模式	
严重性:	低
URL:	http://me.hxsd.jc/public/comm/assets/scripts/bootstrap-datetimepicker.zh-CN.js
实体:	bootstrap-datetimepicker.zh-CN.js (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	除去 Web 站点中的电子邮件地址

推理： 响应包含可能是专用的电子邮件地址。
未经处理的测试响应：

```
...

Content-Length: 813
Last-Modified: Mon, 02 May 2016 09:27:07 GMT
Connection: keep-alive
Expires: Thu, 31 Dec 2037 23:55:55 GMT
Cache-Control: max-age=315360000
Accept-Ranges: bytes

/**
 * Simplified Chinese translation for bootstrap-datetimepicker
 * Yuan Cheung <advanimal@gmail.com>
 */
;(function($){
$.fn.datetimepicker.dates['zh-CN'] = {
  days: ["星期日", "星期一", "星期二", "星期三", "星期四", "星期五", "星期六", "星期日"],
  daysShort: ["周日", "周一", "周二", "周三", "周四", "周五", "周六", "周日"],
  daysMin:  ["日", "一", "二", "三", "四", "五", "六", "日"],
  months: ["一月", "二月", "三月", "四月", "五月", "六月", "七月", "八月", "九月", "十月", "十一月", "十二月"],
  monthsShort: ["一月", "二月", "三月", "四月", "五月", "六月", "七月", "八月", "九月", "十月", "十一月", "十二月"],
  today: "今日",
  ...

```

发现电子邮件地址模式

严重性: 低

URL: http://me.hxsd.jc/home/resume/add

实体: add (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的电子邮件地址

推理: 响应包含可能是专用的电子邮件地址。

未经处理的测试响应:

```
...
        </div>
      </div>
    </div>
    <div class="form-group row">
      <label for="" class="col-md-2 col-sm-2 text-right control-label"><b
class="alertred">*</b>电子邮箱:</label>
      <div class="col-md-5 col-sm-4">
        <input type="text" name="email" style="width:188px;" class="form-
control email"
          maxlength="30" id="" placeholder="请输入您的联系邮箱"
          value="" />
        <span style="color:#b94a48;display:none;">(example@example.com) 请输入正确的
email</span>
      </div>
    </div>
  </div>
  <div class="form-group row" >
    <label class=" text-right col-sm-2"><b class="alertred">*</b>上传证件照片 :
    </label>
    <div class="col-md-4" id="container">
      <input id="preview_path" value="" name="picture" type="hidden">
      <div id="imagePlug">
    </div>
  </div>
  ...
```

低

发现可能的服务器路径泄露模式 15

TOC

问题 1 / 15

TOC

发现可能的服务器路径泄露模式

严重性: 低

URL: <http://me.hxsd.jc/home/index/index>

实体: index (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
$.ajax({
    type: "POST",
    url: "/home/index/getoneworks",
    async: false,
    dataType: 'json',
    success: function(msg){
        if(msg.code == 200) {
            $('#paoren').html(msg.data.per + '%');
            option = returnOption(msg.data.weekInfo, msg.data.valInfo);
            var nend = $("#worksMain").attr("data-end") - 1;
            var nstar = msg.data.week;
            wid = (984 / nend) * (nend - nstar + 1);
        }
    }
});

$.post('/home/index/setEvaluation',
    { whisperid: whisperid , evaluation: sInfo},
    function(data){
        if(data.code == 200){
            $('#evaluation').attr('evaluation', data.data);
        }
    }, "json");
});
...

```

发现可能的服务器路径泄露模式

严重性: **低**

URL: <http://me.hxsd.jc/public/home/js/bindPhone.js>

实体: bindPhone.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...

$.extend({
  isBindPhone : function(isBindPhone){
    var objThis = this;
    var pattern = /^1[34578]\d{9}$/;
    this.oInterval = {};
    //是需要绑定手机号,不绑定直接返回
    if(!isBindPhone) return false;
    //修改浏览器URL地址
    history.pushState({}, '', '/');
    $.getJSON('/home/bindphone/isBindPhone', '', function(result, status, xhr){
      if(xhr.status !== 200) return false;
      if(result.code == 200){
        //显示绑定手机页面
        objThis.showPhoneHtml();
        //页面添加学生姓名
        $('#bindPhoneStudentName').val(result.data.name);
        //页面添加学生学号
        $('#bindPhoneStudentNumber').val(result.data.number);
      }
    })
  }
});

...

$.fn.getPhoneCode = function(){
  $(this).click(function(){
    var phone = $('#bindPhoneStudentPhoneNum').val();
    if(phone.length != 11 || !pattern.test(phone)){
      $('#bindPhoneDiv').removeClass('no-has-error');
      $('#bindPhoneDiv').addClass('has-error');
      $('#bindPhoneError').html('手机号不正确!');
      return false;
    }
    $.post('/home/bindphone/getCode', {phone:phone}, function(result, textStatus,
jqXHR){
      if(jqXHR.status != 200){
        $('#bindPhoneGetCodeSave').html('服务器出错,请稍后再试!');
        $('#bindPhoneGetCodeSave').removeClass('green');
        $('#bindPhoneGetCodeSave').addClass('btn-danger');
        setTimeout(function(){
          $('#bindPhoneGetCodeSave').html('马上绑定');
          $('#bindPhoneGetCodeSave').removeClass('btn-danger');
          $('#bindPhoneGetCodeSave').addClass('green');
          $('#bindPhoneGetCodeSave').removeAttr('disabled');
        }, 1000);
      }
      ...

      if(code.length != 4){
        $('#bindCodeDiv').removeClass('no-has-error');
        $('#bindCodeDiv').addClass('has-error');
        $('#bindCodeError').html('验证码不正确!');
        return false;
      }
    });
  });
};
```



```
    }
    $('#bindPhoneGetCodeSave').attr('disabled', 'disabled');
    $('#bindPhoneGetCodeSave').html('绑定中...');
    $.ajax({
        url: "/home/bindphone/setPhone",
        data:{phone:phone, code:code},
        async: false,
        dataType: 'json',
        type: 'POST',
        success: function (result, textStatus, jqXHR) {
            if(jqXHR.status != 200){
                $('#bindPhoneGetCodeSave').html('服务器出错,请稍后再试!');
                $('#bindPhoneGetCodeSave').removeClass('green');
                $('#bindPhoneGetCodeSave').addClass('btn-danger');
            }
        }
    });
    ...
}
```

发现可能的服务器路径泄露模式	
严重性:	低
URL:	http://me.hxsd.jc/home/attendance.html
实体:	attendance.html (Page)
风险:	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因:	未安装第三方产品的最新补丁或最新修订程序
固定值:	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...

    signin.attr('disabled', 'disabled');
}
//签到
signin.click(function(){
    if('--' == oTd[2].innerHTML)
    {
        var source = 'bcac20cb4ad3fbf12747593312aea8db';
        signin.html('<i class="fa fa-check-square"></i> 签到');
        $.ajax({
            url: '/home/attendance/signin',
            type: 'post',
            async: false,
            data: {
                attendancedate: oTd[0].innerHTML,
                source:source
            },
            success: function(sSaveInfo)
            {
                var oErrorInfo = eval('(' + sSaveInfo + ')');
            }
        });
    }
    ...
    ...

    if(!$('#createdate').val() || $('#createdate').val() == '请选择结束日期' ||
    $('#createdate').val() == '请先选择开始日期')
```

```

        {
            $('#endButt').addClass('has-error');
            $('#createdate').addClass('c_red');
            $('#createdate').val('请选择结束日期');
            return false;
        }

        $.ajax({
            url: '/home/attendance/searchInfo',
            type: 'post',
            async: false,
            data: {
                startTime: $('#createdate').val(),
                endTime: $('#enddate').val()
            },
            success: function(sSaveInfo)
            {
                var oErrorInfo = eval('(' + sSaveInfo + ')');
            }
        });

        ...

        ...

        }

        function setSignOut()
        {
            var source = 'bcac20cb4ad3fbf12747593312aea8db';
            var signout = $('#signout');
            signout.attr('disabled', 'disabled');
            signout.html('<i class="fa fa-sign-out"></i> 签退');
            $.ajax({
                url: '/home/attendance/signout',
                type: 'post',
                async: false,
                data: {
                    attendanceid: $('#signout').attr('key'),
                    cid: $('#cidFeedback').val(),
                    studentid: $('#studentidFeedback').val(),
                    teacherid: $('#teacheridFeedback').val(),
                    clazzcourseday: $('#clazzcoursedayFeedback').val(),
                    source:source
                }
            });
        }

        //拓展视频提示
        function spreadHite()
        {
            $.ajax({
                type:'post',
                url:'/home/home/countSpread',
                dataType:'json',
                success:function(res){
                    if(0 == res.code){
                        //有拓展视频
                        layershow();
                    }else{
                        //没有拓展视频
                        console.log('返回码:' + res.code + '返回信息:' + res.message)
                    }
                }
            });
        }

        ...

        ...

        });

        //layer插件
        function layershow()
        {
            layer.confirm('您有拓展视频可供学习, 是否立即前往?', {
                btn: ['前往', '取消'] //按钮
            }, function(){
                //前往
            }, function(){
                //取消
            });
        }
    }
}

```

```

    }, function(){
        //layer.msg('的确很重要', {icon: 1});
        window.location.href = '/home/home/index?spread=1';
    }, function(){
        //layer.msg('记得前来观看哦...', {
        //    time: 10000, //10s后自动关闭
        //    btn: ['知道了']
        //});
    });
}
</script>
<!-- END CONTAINER -->

...

```

问题 4 / 15

TOC

发现可能的服务器路径泄露模式

严重性: 低

URL: http://me.hxsd.jc/public/comm/assets/scripts/judgeResume.js

实体: judgeResume.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
    url: "/home/resume/judgeResume",
...

```

问题 5 / 15

TOC

发现可能的服务器路径泄露模式

严重性: 低

URL: <http://me.hxsd.ic/home/index/index/phone.html>

实体: phone.html (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
$.ajax({
    type: "POST",
    url: "/home/index/getoneworks",
    async: false,
    dataType: 'json',
    success: function(msg){
        if(msg.code == 200) {
            $('#paoren').html(msg.data.per + '%');
            option = returnOption(msg.data.weekInfo, msg.data.valInfo);
            var nend = $("#worksMain").attr("data-end") - 1;
            var nstar = msg.data.week;
            wid = (984 / nend) * (nend - nstar + 1);
        }
    }
});

$.post('/home/index/setEvaluation',
    { whisperid: whisperid , evaluation: sInfo},
    function(data){
        if(data.code == 200){
            $('#evaluation').attr('evaluation', data.data);
        }
    }, "json");
});
...

```

发现可能的服务器路径泄露模式

严重性: **低**

URL: <http://me.hxsd.jc/home/feedback.html>

实体: feedback.html (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...

var firstclent = $(this).attr('first');
if(firstclent!=score && firstclent!=0){
var mes=confirm("确定更改吗? ");
if(mes==true){
    if(!replyid) {
        alert('错误: 请刷新页面后重试! ');
    }else{
        var obj = this;
        $.ajax({
            url: '/home/feedback/setScore',
            type: 'POST',
            dataType: 'json',
            async: false,
            data: {feedbackreplyid: replyid, score: score},
            success: function (msg) {
                if(msg.code == 200){
                    $(obj).attr('scoreid', msg.data.feedbackscoreid)
                    $(obj).attr('score', score)
                    alert('评价成功');
                }
            }
        })
    }
}

if(firstclent==0){
    if(!replyid) {
        alert('错误: 请刷新页面后重试! ');
    }else{
        var obj = this;
        $.ajax({
            url: '/home/feedback/setScore',
            type: 'POST',
            dataType: 'json',
            async: false,
            data: {feedbackreplyid: replyid, score: score},
            success: function (msg) {
                if(msg.code == 200){
                    $(obj).attr('scoreid', msg.data.feedbackscoreid)
                    $(obj).attr('score', score)
                    $(obj).attr('first', score)
                }
            }
        })
    }
}

//禁止重复提交
```

```

function checkSubmitTimes(){
    //获取最新一条信息的时间戳(无论接收与否)
    $("#sbt").attr('disabled',true);
    $.ajax({
        type: 'post',
        url: '/home/technicalsupport/getTimeNow',
        data: {},
        async: false,
        //cache: false,
        dataType:'json',
        success: function (msg)
        {
            var ttask = $("#ttask").val();
            var timestamp = msg.time;
            if(timestamp - ttask >= 300)
        }
    });
    ...
}

```

问题 7 / 15

TOC

发现可能的服务器路径泄露模式

严重性: **低**

URL: <http://me.hxsd.jc/home/technicalsupport.html>

实体: technicalsupport.html (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
}

//禁止重复提交
function checkSubmitTimes(){
    //获取最新一条信息的时间戳(无论接收与否)
    var ttask = $("#ttask").val();
    $("#sbt").attr('disabled',true);
    $.ajax({
        type: 'post',
        url: '/home/technicalsupport/getTimeNow',
        data: {},
        async: false,
        //cache: false,
        dataType:'json',
        success: function (msg)
        {
            var timestamp = msg.time;
            //是否是修改 有id
            var ttaskid = $("input[name='ttaskid']").val();
        }
    });
    ...
}

```

发现可能的服务器路径泄露模式**严重性:** 低**URL:** http://me.hxsd.jc/home.html**实体:** home.html (Page)**风险:** 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息**原因:** 未安装第三方产品的最新补丁或最新修订程序**固定值:** 为 Web 服务器或 Web 应用程序下载相关的安全补丁**推理:** 响应包含服务器上文件的绝对路径和/或文件名。**未经处理的测试响应:**

```
...

$.ajax({
  type: "POST",
  url: "/home/index/getoneworks",
  async: false,
  dataType: 'json',
  success: function(msg){
    if(msg.code == 200) {
      $('#paoren').html(msg.data.per + '%');
      option = returnOption(msg.data.weekInfo, msg.data.valInfo);
      var nend = $("#worksMain").attr("data-end") - 1;
      var nstar = msg.data.week;
      wid = (984 / nend) * (nend - nstar + 1);

...

...

$.post('/home/index/setEvaluation',
  { whisperid: whisperid , evaluation: sInfo},
  function(data){
    if(data.code == 200){
      $('#evaluation').attr('evaluation', data.data);
    }
  }, "json");
  })
});
...
```

发现可能的服务器路径泄露模式

严重性: 低

URL: <http://me.hxsd.jc/home/index.html>

实体: index.html (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
$.ajax({
    type: "POST",
    url: "/home/index/getoneworks",
    async: false,
    dataType: 'json',
    success: function(msg){
        if(msg.code == 200) {
            $('#paoren').html(msg.data.per + '%');
            option = returnOption(msg.data.weekInfo, msg.data.valInfo);
            var nend = $("#worksMain").attr("data-end") - 1;
            var nstar = msg.data.week;
            wid = (984 / nend) * (nend - nstar + 1);
        }
    }
});

$.post('/home/index/setEvaluation',
    { whisperid: whisperid , evaluation: sInfo},
    function(data){
        if(data.code == 200){
            $('#evaluation').attr('evaluation', data.data);
        }
    }, "json");
});
...

```


发现可能的服务器路径泄露模式

严重性: 低

URL: <http://me.hxsd.jc/public/home/js/clazzfeedback.js>

实体: clazzfeedback.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...
$.ajax({
    url: '/home/process/getFeedresultInfo',
    type: 'post',
    dataType: 'json',
    data: {
    },
    success: function(dataInfo)
    {
        if (200 == dataInfo.code)
        {
            require(
...
...
function ajaxGetData(showType, showContent)
{
    $.ajax({
        url: '/home/process/getProcessInfo',
        type: 'post',
        dataType: 'json',
        data: {
            showType: showType,
            showContent: showContent
        },
        success: function(dataInfo)
        {
            if (200 == dataInfo.code)
...

```

发现可能的服务器路径泄露模式

严重性: 低

URL: <http://me.hxsd.jc/>

实体: (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```

...
$.ajax({
  type: "POST",
  url: "/home/index/getoneworks",
  async: false,
  dataType: 'json',
  success: function(msg){
    if(msg.code == 200) {
      $('#paoren').html(msg.data.per + '%');
      option = returnOption(msg.data.weekInfo, msg.data.valInfo);
      var nend = $("#worksMain").attr("data-end") - 1;
      var nstar = msg.data.week;
      wid = (984 / nend) * (nend - nstar + 1);
    }
  }
});

$.post('/home/index/setEvaluation',
  { whisperid: whisperid , evaluation: sInfo},
  function(data){
    if(data.code == 200){
      $('#evaluation').attr('evaluation', data.data);
    }
  }, "json");
});
...

```

发现可能的服务器路径泄露模式

严重性: **低**

URL: <http://me.hxsd.jc/public/home/js/operationpdf.js>

实体: operationpdf.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...

// var iNowYear = oDate.getFullYear();
// var iNowMonth = oDate.getMonth() + 1;
// var iNowDate = oDate.getDate();
// var iNowHours = oDate.getHours();
// var iNowMinutes = oDate.getMinutes();
// 学习攻略PDF,学习攻略ZIP和FLV, 任务和挑战 (包含PDF,ZIP,FLV)
var bArr = {bShowStudyPDF: false, bShowStudyZIPAndFLV: false, bShowComm: false};

$.ajax({
  url: '/home/home/diffDate',
  type: 'GET',
  dataType: 'json',
  async: false,
  data: {diffDate: classesDate}
})
  .done(function (json) {

    bArr.bShowStudyPDF = json.bShowStudyPDF;
    bArr.bShowStudyZIPAndFLV = json.bShowStudyZIPAndFLV;

...

    bArr.bShowComm = json.bShowComm;

  })
  .fail(function () {
    console.log("error");
  });

$.ajax(
{
  url: "/home/home/getpdfinfo",
  type: "post",
  data: "classesDate=" + classesDate + "&classesId=" + classesId + "&classesDay=" +
classesDay + "&studentId=" + studentId + "&teacherid=" + teacherid,
  dataType: 'json',
  success: function (pdfInfo)
  {
    var obj = pdfInfo;
    if ($("#pt_myTab >li").eq(0).html() != undefined)
    {
      $("#pt_myTab").html("");
    }

...

    $("#message").html("任务/挑战已经上传,请在当天15:30之后上传").show();
  }
}
```

```

    }
    });

    // 获取点击的课程是否还能上传作业
    $.ajax({
        url: '/home/home/getUploadTimelimit',
        type: 'POST',
        dataType: 'json',
        data: {courseId: classesId}
    })
        .done(function (json) {
            // 如果课程资料没上传, 不提示
            if (parseInt(json.flag) == 0)
            {
                // $("#myform").hide();
            }
        })
        .fail(function () {
            console.log("error");
        });

    //获取周任务标准
    $.ajax({
        type: 'post',
        url: '/home/home/gettaskstandard',
        data: {date: classesDate, day: classesDay},
        dataType: 'html',
        success: function (res, status)
        {
            if (status == 'success') {
                $('#tab_1_7').html(res);
                //初始化colorbox
                $('.colorboximg_0').colorbox({rel: 'attachimgStore_0', width: '90%', title: '卓越: A+
(90-100) 实例大图浏览'});
                $('.colorboximg_1').colorbox({rel: 'attachimgStore_1', width: '90%', title: '优秀:
A、A- (80-89) 实例大图浏览'});
            }
        }
    });

    //拓展视频信息获取
    $('#spreadvideotab').hide();
    $.ajax({
        type: 'post',
        url: '/home/home/getSpreadinfo',
        data: {courseid: classesId, day: classesDay},
        dataType: 'json',
        success: function (obj) {
            if ($("#spread_Tab >li").eq(0).html() != undefined)
            {
                $("#spread_Tab").html("");
            }

            if (0 == obj.code) {
            }
        }
    });

```

发现可能的服务器路径泄露模式

严重性: **低**

URL: http://me.hxsd.jc/public/comm/assets/plugins/jquery-hydx/hgz_hycode.js

实体: hgz_hycode.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理: 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...  
  
    hysrVar += "          <table style=\"width:700px;\" class=\"options-table\">";  
    hysrVar += "          <tbody class=\"item-list\" >";  
  
    var znhycode = new Array();  
    $.ajax({  
        type: "POST",  
        url: "/home/resume/getJob",  
        data: {},  
        async:false,  
        dataType: 'json',  
        //成功获取到数据执行的程序  
        success: function(msg){  
  
        ...
```

问题 14 / 15

TOC

发现可能的服务器路径泄露模式

严重性: **低**

URL: <http://me.hxsd.jc/home/technicalsupport/index>

实体: index (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。
未经处理的测试响应：

```
...
}

//禁止重复提交
function checkSubmitTimes(){
    //获取最新一条信息的时间戳(无论接收与否)
    var ttask = $("#tstask").val();
    $("#sbt").attr('disabled',true);
    $.ajax({
        type: 'post',
        url: '/home/technicalsupport/getTimeNow',
        data: {},
        async: false,
        //cache: false,
        dataType:'json',
        success: function (msg)
        {
            var timestamp = msg.time;
            //是否是修改 有id
            var ttaskid = $("input[name='tstaskid']").val();
        }
    });
    ...
}
```

发现可能的服务器路径泄露模式	
严重性:	低
URL:	http://me.hxsd.jc/public/comm/assets/plugins/city/areadata.js
实体:	areadata.js (Page)
风险:	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因:	未安装第三方产品的最新补丁或最新修订程序
固定值:	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。
未经处理的测试响应：

```
...

    })
    });
    selectProvince('all', null, '');
}

var __LocalDataCities = new Array();
$.ajax({
    type: "POST",

    url: "/home/resume/getCity",

    data: {},

```

```
        async: false,

        dataType: 'json',
        //成功获取到数据执行的程序
        success: function(msg) {

            ...
        }
    }
}
```

发现内部 IP 泄露模式	
严重性:	低
URL:	http://me.hxsd.jc/home/resume/add
实体:	add (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 应用程序编程或配置不安全
固定值:	除去 Web 站点中的内部 IP 地址

推理: AppScan 在响应中发现了看似为内部 IP 地址的内容。
未经处理的测试响应:

```
...
GET /home/resume/add HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/resume/index
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
...
```

发现内部 IP 泄露模式**严重性:** 低**URL:** http://me.hxsd.jc/home/home.html**实体:** home.html (Page)**风险:** 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置**原因:** Web 应用程序编程或配置不安全**固定值:** 除去 Web 站点中的内部 IP 地址**推理:** AppScan 在响应中发现了看似为内部 IP 地址的内容。**未经处理的测试响应:**

```
...

//设置cookie
function setCookie(name, value, iDay) {
    var oDate = new Date();
    var oNextTime = Date.parse(oDate.getFullYear() + '/' + (oDate.getMonth() + 1) + '/' +
oDate.getDate() + 86400000;
    oDate.setTime(oNextTime);
    document.cookie = name + '=' + value + ';expires=' + oDate;
}
</script>
<!--课程反馈弹出框-->
<script src="http://10.2.20.204/js/plupload.full.min.js" type="text/javascript"></script>
<script>

    // 这里手动的传入地址, 以免在js文件里面写死。
    var clazzid = '3953';
    var studentid = '97';

    //转化文件大小格式
    function bytesToSize(bytes) {
        if (bytes === 0) return '0 B';

...

...

        //return (bytes / Math.pow(k, i)) + ' ' + sizes[i];
        //return (bytes / Math.pow(k, i)).toFixed(3) + ' ' + sizes[i];
    }

    //plupload
    var uploader = new plupload.Uploader({
        runtimes: 'html5,gears,flash,silverlight,html4',
        //unique_names: true,
        browse_button: 'upload', // you can pass in id...
        container: document.getElementById('container'),
        url: 'http://10.2.20.204/studentworkplupload.php',
        flash_swf_url: 'http://10.2.20.204/js/Moxie.swf',
        silverlight_xap_url: 'http://10.2.20.204/js/Moxie.xap',
        multi_selection: false, //选择多个文件
        chunk_size: '20mb', //每片大小
        filters: { //使用该参数来限制上传文件的类型, 大小等
            mime_types: [{title: "zip files", extensions: "zip"}]}
    },
    //上传时的附加参数
```



```

multipart_params: {'type': 'studentwork'},
init: { //当Plupload初始化完成后触发
    PostInit: function () { //当Init事件发生后触发

...

...

        filename: file.name,
        homeworkpath: res.filepath,
        size: file.size,
        // data_uuid: uuid,
        type: $('#work_type').val(),
        courseid: $("#courseid").val(),
        time: $("#time").val(),
        classesdate: $("#time").val(),
        studentworkid: studentworkid,
        host: 'http://10.2.20.204/'
    }
}).done(function (response, status, xhr) {
    // 成功文件清楚对象
    if (response.status == 1)
    {
        if (response.type == 1)
        {
            $('#work_type').val(0);
            if (response.workid !== true)
...

```

问题 3 / 3

TOC

发现内部 IP 泄露模式

严重性: **低**

URL: http://me.hxsd.jc/home/resume/add.html

实体: add.html (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的内部 IP 地址

推理: AppScan 在响应中发现了看似为内部 IP 地址的内容。

未经处理的测试响应:

```

...
GET /home/resume/add.html HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22e9f59943f07c2ddfca23efaeae34b79f%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126557%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D437c598231c800740d727693e64b8fa43027ea5b;
PHPSESSID=9hm6ib5udme1e122fk4eh7ruu2;
student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

```

```
Referer: http://me.hxsd.jc/home/resume/add
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK

...
```

低

检测到应用程序测试脚本 ①

TOC

问题 1 / 1

TOC

检测到应用程序测试脚本

严重性: 低

URL: http://me.hxsd.jc/home/index/index/

实体: test.dbf (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

低

客户端 (JavaScript) Cookie 引用 ②

TOC

问题 1 / 2

TOC

客户端 (JavaScript) Cookie 引用

严重性: **低**

URL: <http://me.hxsd.jc/public/comm/assets/plugins/jquery.cookie.min.js>

实体: **/*! (Page)**

风险: 此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

原因: Cookie 是在客户端创建的

固定值: 除去客户端中的业务逻辑和安全逻辑

推理: AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
...
Accept-Ranges: bytes

/*!
 * jQuery Cookie Plugin v1.3.1
 * https://github.com/carhartl/jquery-cookie
 *
 * Copyright 2013 Klaus Hartl
 * Released under the MIT license
 */
(function(a){if(typeof define=="function"&&define.amd){define(["jquery"],a)}else{a(jQuery)}})
(function(e){var a=/\+/g;function d(g){return g}function b(g){return
decodeURIComponent(g.replace(a," "))}function f(g){if(g.indexOf("'")==0){g=g.slice(1,-
1).replace(/\\/\\/g,"'").replace(/\\\\\\/g,"\\")}try{return c.json?JSON.parse(g):g}catch(h){}}var
c=e.cookie=function(p,o,u){if(o!=undefined){u=e.extend({},c.defaults,u);if(typeof
u.expires=="number"){var q=u.expires,s=u.expires=new Date();s.setDate(s.getDate()+q)}o=c.json?
JSON.stringify(o):String(o);return (document.cookie=[c.raw?p:encodeURIComponent(p),"=",c.raw?
o:encodeURIComponent(o),u.expires?" expires="+u.expires.toUTCString():"",u.path?"
path="+u.path:""",u.domain?" domain="+u.domain:""",u.secure?" secure":""].join(""))}var g=c.raw?
d:b;var r=document.cookie.split("; ");var v=p?undefined:{};for(var n=0,k=r.length;n<k;n++){var
m=r[n].split("=");var h=g(m.shift());var j=g(m.join("="));if(p&&p===h){v=f(j);break}if(!p)
{v[h]=f(j)}return v};c.defaults={};e.removeCookie=function(h,g){if(e.cookie(h)!=undefined)
{e.cookie(h,"",e.extend({},g,{expires:-1}));return true}return false}});
...

```

问题 2 / 2

TOC

客户端 (JavaScript) Cookie 引用

严重性: **低**

URL: <http://me.hxsd.jc/public/comm/assets/annex/video/jwplayer.js>

实体: **if(typeof jwplayer=="undefined"){jwplayer=function(a){if(jwplayer.api){return jwplayer.api.selectPla... (Page)**

风险: 此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

原因: Cookie 是在客户端创建的

固定值: 除去客户端中的业务逻辑和安全逻辑

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
GET /public/comm/assets/annex/video/jwplayer.js HTTP/1.1
Cookie:
ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22279141aeab85a0fbd3092a76477beec%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466126317%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%3B%7Db63d2f822b659fe39f0edfda42d9865add4c128a; PHPSESSID=21v2mqbqnmuh2tvm6asd6t3jb7; student_info=a%3A5%3A%7Bs%3A10%3A%22student_id%22%3Bs%3A2%3A%2297%22%3Bs%3A12%3A%22student_name%22%3Bs%3A14%3A%22xuehaoxuesheng%22%3Bs%3A16%3A%22student_password%22%3Bs%3A32%3A%224fcb6bfc663e78a0909f9d59319d87d9%22%3Bs%3A14%3A%22student_number%22%3Bs%3A13%3A%220010116070001%22%3Bs%3A17%3A%22student_temp_pass%22%3Bs%3A6%3A%22236985%22%3B%7D
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/index/index/phone.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)

HTTP/1.1 200 OK
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:18:47 GMT
Content-Type: application/x-javascript
Content-Length: 48318
Last-Modified: Mon, 02 May 2016 09:27:07 GMT
Connection: keep-alive
Vary: Accept-Encoding
Expires: Thu, 31 Dec 2037 23:55:55 GMT
Cache-Control: max-age=315360000
Accept-Ranges: bytes
...
```

低

未分类站点的链接 2


TOC

问题 1 / 2

TOC

未分类站点的链接	
严重性:	低
URL:	http://me.hxsd.jc/home/home.html
实体:	http://10.2.20.204/js/plupload.full.min.js (Link)
风险:	不适用
原因:	不适用
固定值:	检查链接，确定它是否确实本应包含在 Web 应用程序中

推理： 推理不适用于此问题。

 The Malware Link Analysis module could not classify this link

未分类站点的链接

严重性: 低

URL: http://me.hxsd.jc/public/comm/assets/annex/video/jwplayer.js

实体: https://ssl./ (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

推理: 推理不适用于此问题。



The Malware Link Analysis module could not classify this link

低

无害站点的链接 3

TOC

无害站点的链接

严重性: 低

URL: http://me.hxsd.jc/public/comm/assets/faceimage/expressInstall.swf

实体: http://fpdownload.macromedia.com/pub/flashplayer/update/current/swf/autoUpdater.swf (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

推理: 推理不适用于此问题。

无害站点的链接

严重性: **低**

URL: http://me.hxsd.jc/public/comm/assets/annex/pdf/flexpaper_handlers.js

实体: <http://www.google.com/> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

推理: 推理不适用于此问题。



The Malware Link Analysis module classified this link as:

无害

- 搜索机/网页目录/综合性网站

问题 3 / 3

TOC

无害站点的链接

严重性: **低**

URL: <http://me.hxsd.jc/home/resume/add.html>

实体: <http://www.adobe.com/go/getflashplayer> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

推理: 推理不适用于此问题。

低

应用程序错误 1

TOC

问题 1 / 1

TOC

应用程序错误

严重性: **低**

URL: http://me.hxsd.jc/home/technicalsupport/save

实体: ttaskid (Parameter)

风险: 可能会收集敏感的调试信息

原因: 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配

固定值: 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理: 应用程序以错误消息响应, 表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应:

```
...

Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://me.hxsd.jc/home/technicalsupport.html
Host: me.hxsd.jc
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Content-Length: 32

ttaskid%5B%5D=&description=1234

HTTP/1.1 500 Internal Server Error
Server: nginx/1.2.0
Date: Fri, 17 Jun 2016 01:38:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.9
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%229786c2426e8300f7b2d9acb8c1688329%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A11%3A%2210.2.20.176%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A120%3A%22Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+Win64%3B+x64%3B+Trident%2F4.0%3B+.NET+CLR+2.0.50727%3B+SLCC2%3B+.NET+CLR+3.5.3072%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1466127487%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7De02bf28dceec10e8334fbac13a1b1f440809d7ef; expires=Fri, 17-Jun-2016 03:38:07 GMT; path=/

<!DOCTYPE html>
...
```