Web 安全测试

Himan

About Me

ID: Himan
Name: Lee Xue Qing
Company: 360buy.com
Responsibility : web security
Mail: winner__1@sohu.com

News


== 「全球Hack入侵X战群」 ==
我是中国人!
伟大的中华民族万岁!
The Great Chinese Nation Hooray!
西沙群岛，南沙群岛永远是中国不可分割的一部分!
如果有任何国家有损我国主权，我们就只有攻击!
NEWS.CN

News

#opsony

Congratulations, Sony.

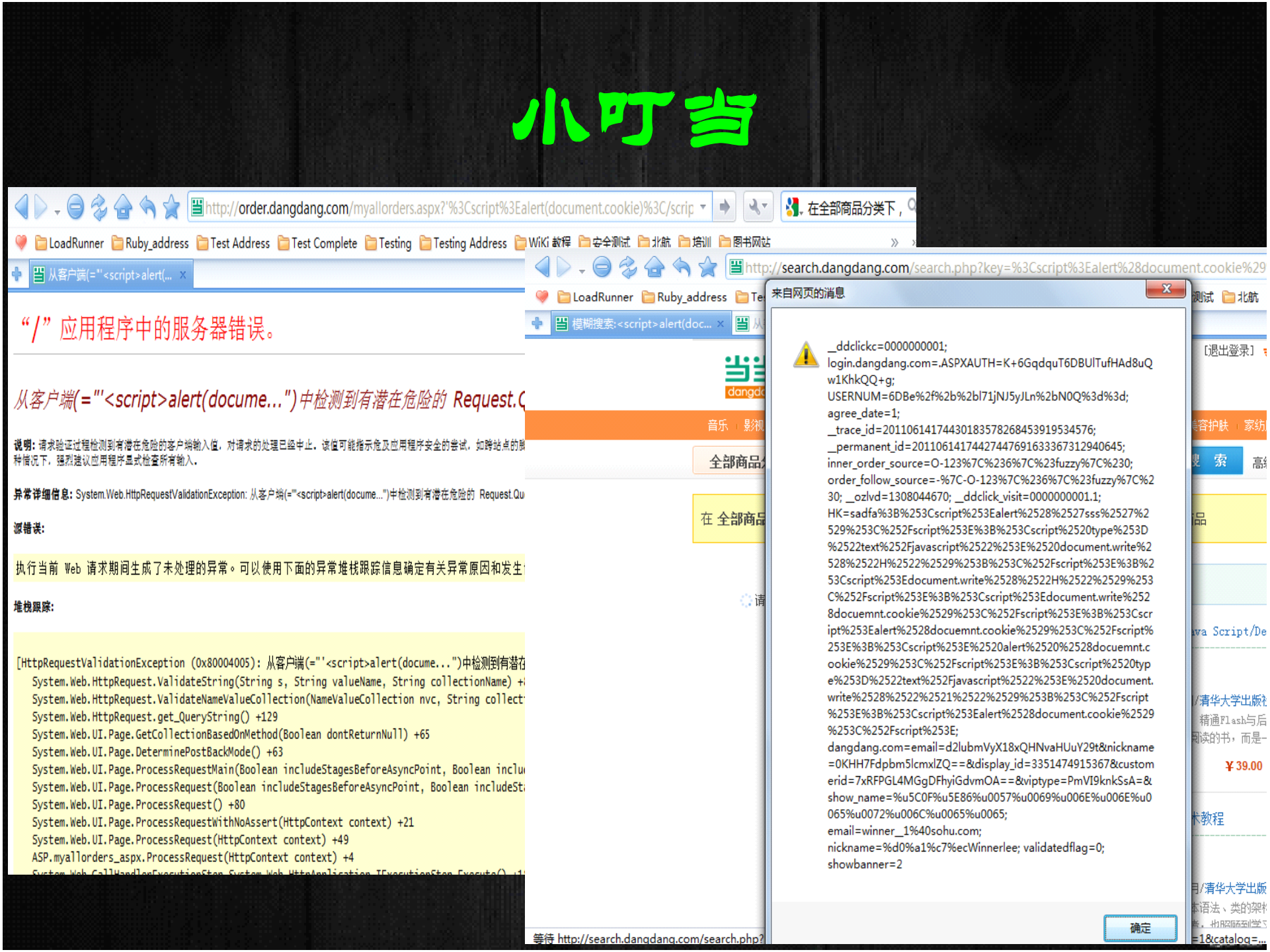
You have now received the undivided attention of Anonymous. Your recent legal action against our fellow hackers, GeoHot and Graf_Chokolo, has not only alarmed us, it has been deemed wholly unforgivable.

You have abused the judicial system in an attempt to censor information on how your products work. You have victimized your own customers merely for possessing and sharing information, and continue to target every person who seeks this information. In doing so you have violated the privacy of thousands. This is the information they were willing to teach to the world for free. The very same information you wish to suppress for sake of corporate greed and complete control of the users.

Now you will experience the wrath of Anonymous. You saw a hornets nest, and stuck your penises in it. You must face the consequences of your actions, Anonymous style.

Knowledge is Free.
We are Anonymous.
We are Legion.
We do not Forgive.
We do not forget.

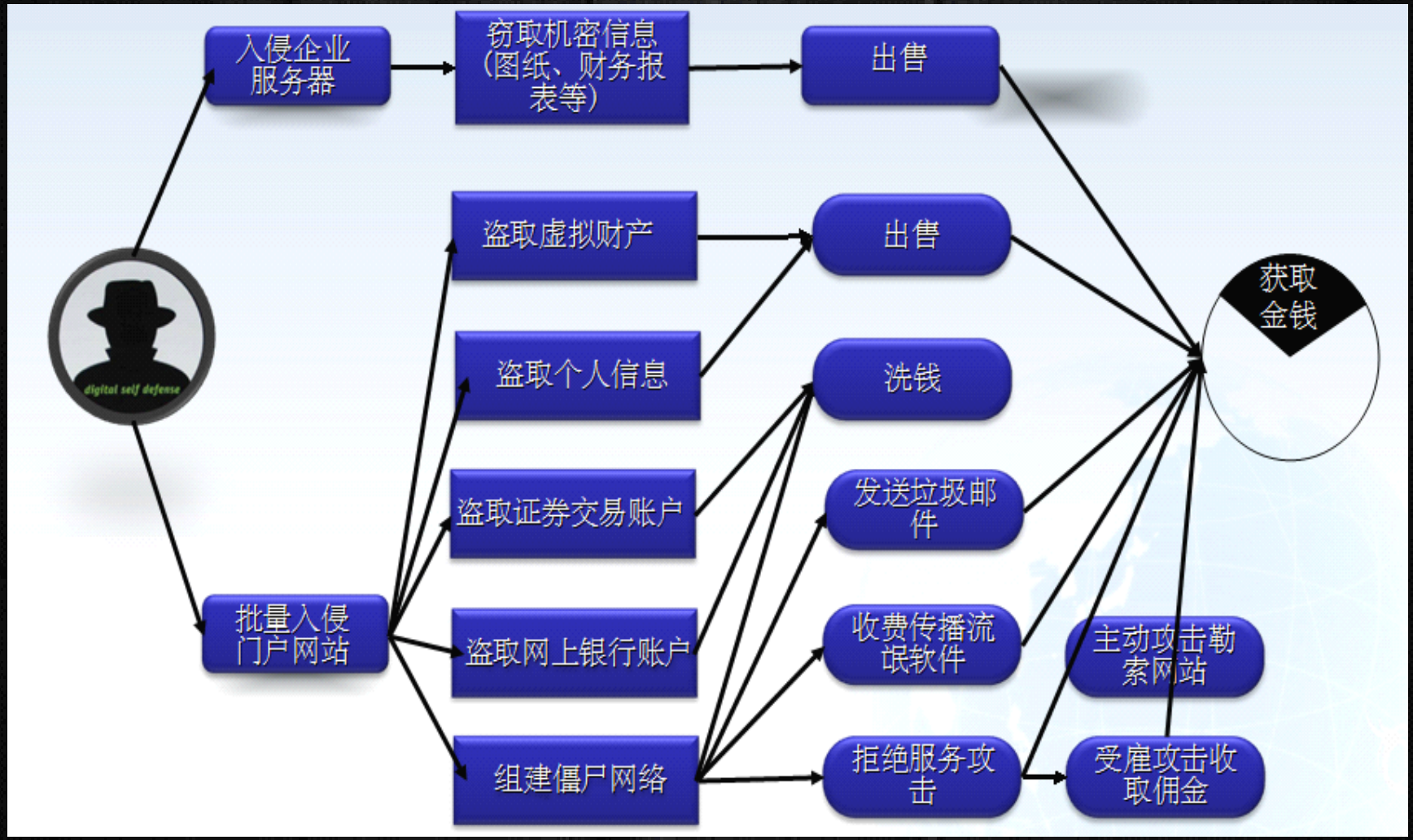
小叮当


http://order.dangdang.com/myallorders.aspx?'%3Cscript%3Ealert(document.cookie)%3C/scrip
在全部商品分类下，
LoadRunner
Ruby_address
Test Address
Test Complete
Testing
Testing Address
从客户端(="<script>alert(...
"/" 应用程序中的服务器错误。
从客户端(="'<script>alert(docume...")中检测到有潜在危险的 Request.Q
说明: 请求验证过程检测到有潜在危险的客户端输入值，对请求的处理已经中止。该值可能指示危及应用程序安全的尝试，如跨站点的脚
种情况下，强烈建议应用程序显式检查所有输入。
异常详细信息: System.Web.HttpRequestValidationException: 从客户端(="'<script>alert(docume...")中检测到有潜在危险的 Request.Qu
源错误:
执行当前 Web 请求期间生成了未处理的异常。可以使用下面的异常堆栈跟踪信息确定有关异常原因和发生
堆栈跟踪:
[HttpRequestValidationException (0x80004005): 从客户端(="'<script>alert(docume...")中检测到有潜在
System.Web.HttpRequest.ValidateString(String s, String valueName, String collectionName) +
System.Web.HttpRequest.ValidateNameValueCollection(NameValueCollection nvc, String collect
System.Web.HttpRequest.get_QueryString() +129
System.Web.UI.Page.GetCollectionBasedOnMethod(Boolean dontReturnNull) +65
System.Web.UI.Page.DeterminePostBackMode() +63
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean inclu
System.Web.UI.Page.ProcessRequest(Boolean includeStagesBeforeAsyncPoint, Boolean includeSt
System.Web.UI.Page.ProcessRequest() +80
System.Web.UI.Page.ProcessRequestWithNoAssert(HttpContext context) +21
System.Web.UI.Page.ProcessRequest(HttpContext context) +49
ASP.myallorders_aspx.ProcessRequest(HttpContext context) +4
http://search.dangdang.com/search.php?key=%3Cscript%3Ealert%28document.cookie%29
LoadRunner
Ruby_address
模糊搜索:<script>alert(doc...
来自网页的消息
__ddclickc=0000000001;
login.dangdang.com=.ASPXAUTH=K+6GqdquT6DBUlTufHAd8uQw1KhkQQ+g;
USERNUM=6DBe%2f%2b%2bl71jNJ5yJLn%2bN0Q%3d%3d;
agree_date=1;
__trace_id=20110614174430183578268453919534576;
__permanent_id=20110614174427447691633367312940645;
inner_order_source=O-123%7C%236%7C%23fuzzy%7C%230;
order_follow_source=-%7C-O-123%7C%236%7C%23fuzzy%7C%230; __ozlvd=1308044670; __ddclick_visit=0000000001.1;
HK=sadfa%3B%253Cscript%253Ealert%2528%2527sss%2527%2529%253C%252Fscript%253E%3B%253Cscript%2520type%253D%2522text%252Fjavascript%2522%253E%2520document.write%2528%2522H%2522%2529%253B%253C%252Fscript%253E%3B%253Cscript%253Edocument.write%2528%2522H%2522%2529%253C%252Fscript%253E%3B%253Cscript%253Edocument.write%2528docuemnt.cookie%2529%253C%252Fscript%253E%3B%253Cscript%253Ealert%2528docuemnt.cookie%2529%253C%252Fscript%253E%3B%253Cscript%253E%2520alert%2520%2528docuemnt.cookie%2529%253C%252Fscript%253E%3B%253Cscript%2520type%253D%2522text%252Fjavascript%2522%253E%2520document.write%2528%2522%2521%2522%2529%253B%253C%252Fscript%253E%3B%253Cscript%253Ealert%2528document.cookie%2529%253C%252Fscript%253E;
dangdang.com=email=d2lubmVyX18xQHNvaHUuY29t&nickname=0KHH7Fdpbm5lcmxlZQ==&display_id=3351474915367&customerid=7xRFPGL4MGgDFhyiGdvmOA==&viptype=PmVI9knkSsA=&show_name=%u5C0F%u5E86%u0057%u0069%u006E%u006E%u0065%u0072%u006C%u0065%u0065;
email=winner_1%40sohu.com;
nickname=%d0%a1%c7%ecWinnerlee; validatedflag=0;
showbanner=2
确定
等待 http://search.dangdang.com/search.php?
[退出登录]
音乐
影视
全部商品
在 全部商品
¥39.00

信息安全的现状

- 信息安全环境越来越复杂
- 黑客攻击越来越容易
- 漏洞利用速度越来越快
- 地下黑色产业链越来越庞大

地下黑客产业链


入侵企业服务器
窃取机密信息(图纸、财务报表等)
出售
盗取虚拟财产
出售
盗取个人信息
洗钱
盗取证券交易账户
发送垃圾邮件
批量入侵门户网站
盗取网上银行账户
收费传播流氓软件
主动攻击勒索网站
组建僵尸网络
拒绝服务攻击
受雇攻击收取佣金
获取金钱
digital self defense

Web安全测试的意义

1、增强网站的健壮性

2、预防非法用户的攻击

3、保护使用者的安全

4、使非法侵入的代价超过被保护信息的价值

Web安全测试的方法

- SQL注入
- 跨站脚本（XSS）
- 失效的身份认证和会话管理
- 不安全的直接对象引用
- 跨站请求伪造（CSRF）
- 安全配置错误（新）
- 不安全的加密存储
- 没有限制URL访问
- 传输层保护不足
- 未验证的重定向和转发（新）

Web安全测试的方法

- 地址栏关键字段加密
- 网站地址暴库
- 无过滤的上传功能
- 登录信息提示
- 提交请求防重入
- 网页脚本错误

SQL 注入

Web应用程序执行来自外部包括数据库在内的恶意指令，SQL Injection与Command Injection等攻击包括在内。如果没有阻止带有语法含义的输入内容，有可能导致对数据库信息的非法访问，在Web表单中输入的内容应该保持简单，并且不应包含可被执行的代码。

SQL 注入

测试对象：

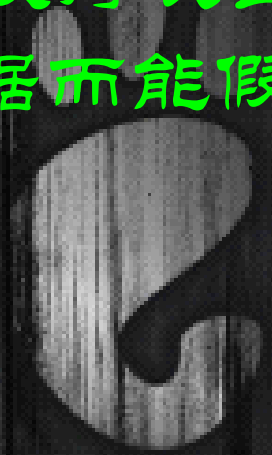
- 可以进行传参的URL

http://www.shuanghuipack.com/news_detail_cn.asp?id=81 and 1=2

http://bbs.360buy.com/forum.php?archiver=1

XSS跨站攻击

Web应用程序直接将来自用户的执行请求送回浏览器执行，使得攻击者可截取用户的Cookie或Session数据而能假冒直接登入为合法使用者。



XSS跨站攻击

测试对象：

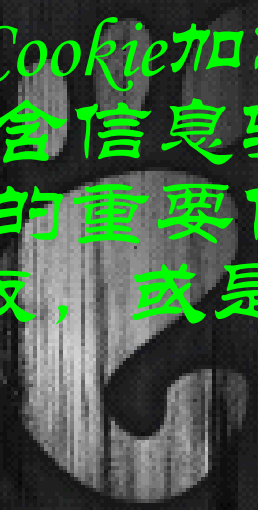
- 可以进行传参的URL
- 网页中可进行输入的表单

http://search.dangdang.com/search.php?key=<script>alert('xss')</script>

http://search.dangdang.com/search.php?key=%3cscript%3ealert('xss')%3c%2fscript%3e

注：IE6 浏览器对跨站拦截不彻底！

失效的身份认证和会话管理



只对首次传送的Cookie加以验证，程序没有持续对Cookie中内含信息验证比对，攻击者便可修改Cookie中的重要信息，以提升权限进行网站数据存取，或是冒用他人账号取得个人私密资料。

失效的身份认证和会话管理

测试对象：

- 可以进行传参的URL
- 提交请求页面
- 登录后的cookie

http://m.360buy.com/user/home.action?sid=a04d85503e040cbc7e2fe048ff7104ce

不安全的直接对象引用

在具导出/下载功能的页面参数中修改内容，WEB服务器便会导出/下载程序源代码或者指定文件。

不安全的直接对象引用

测试对象：

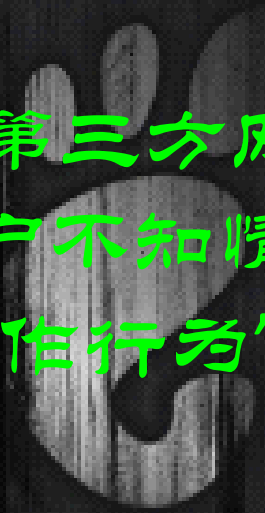
URL中有用户参数的地址

可以进行下载操作的地址

http://www.51btest.cn/FileDown_Show.aspx?did=1586

http://demo.testfire.net/default.aspx?content=/../../../../../../../../../boot.ini%00.htm

跨站伪造请求



攻击者通过调用第三方网站的恶意脚本来伪造请求，在用户不知情时攻击者强行提交构造的具有“操作行为”的数据包

跨站伪造请求

测试对象：

- 网页中可进行输入的表单
- 网页中地址栏进行传参的地址

安全配置错误

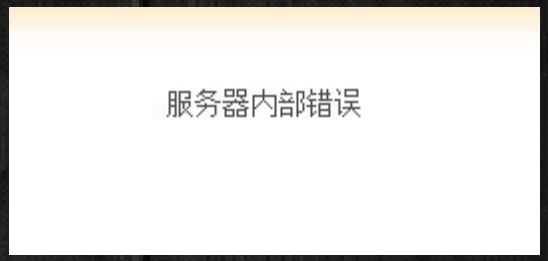
这些漏洞会导致系统完全被攻破。错误安全配置可以发生在一个应用程序堆栈的任何层面，包括平台、Web服务器、应用服务器、框架和自定义代码。

安全配置错误

测试对象：

多级目录地址

网站报错的页面



Forbidden

You don't have permission to access /activity/ on this server.

Apache/2.2.6 (Unix) mod_ssl/2.2.6 OpenSSL/0.9.7a DAV/2 Resin/3.0.25 Server at score.mail.sohu.com Port 80

http://w3.sapir.ac.il/pm/to_miriam/IMG_8522.jpg

http://collegial.360buy.com/collegial/userlogin/user_admin_login.aspx

所有的错误都只显示友好信息，不显示任何与实际错误相关的信息

不安全的加密存储

常见的问题是不安全的密钥生成和储存、不轮换密钥，和使用弱算法。使用弱的或者不带*salt*的哈希算法来保护密码也很普遍。外部攻击者因访问的局阻性很难探测这种漏洞。他们通常必须首先破解其他东西以获得需要的访问。

不安全的加密存储

测试对象：

敏感字段的数据库存储

身份证、密码、信用卡、个人信息在数据库中存储需要加密存放

没有阻制URL访问

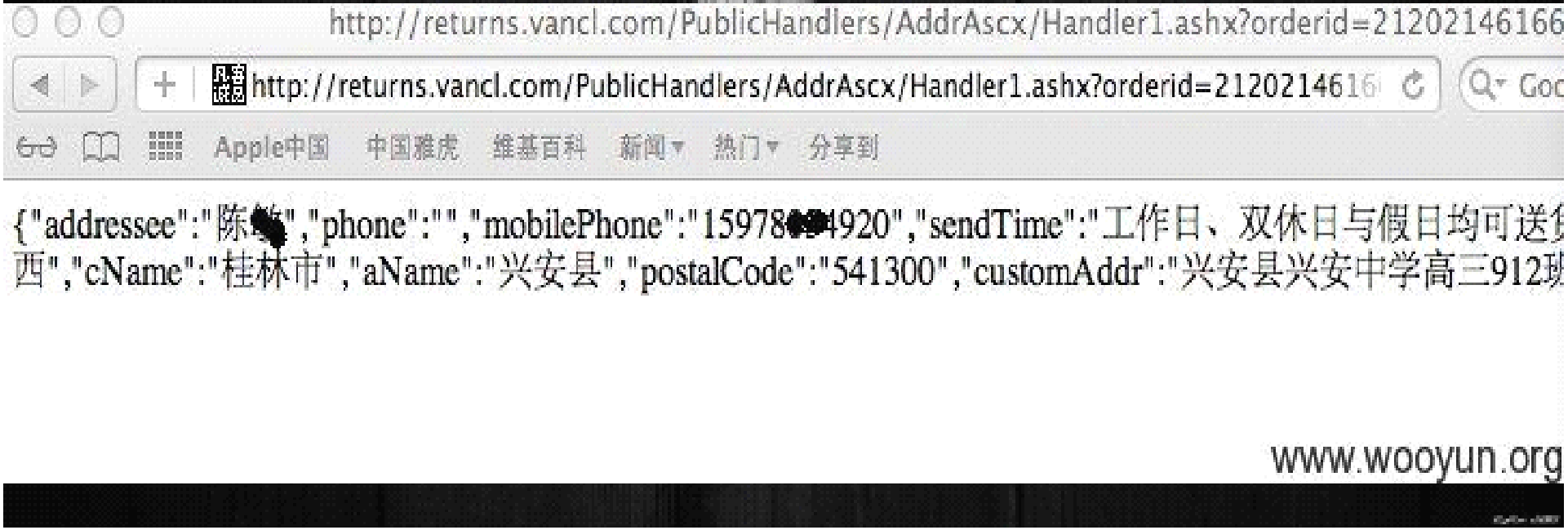
系统已经对URL的访问做了阻制，但这种阻制却实际并没有生效。攻击者能够很容易的就伪造请求直接访问未被授权的页面。

没有阻制URL访问

测试对象：

需要身份验证的页面

http://returns.vancl.com/ExStepTwo/StepTwo/212021461664



传输层保护不足

在身份验证过程中没有使用*SSL/TLS*，因此暴露传输数据和会话*ID*，被攻击者截听。它们有时还会使用过期或者配置不正确的证书。

传输层保护不足

测试对象：

网站登录模块

https://passport.360buy.com/new/login.aspx

未验证的重定向和转发

攻击者可以引导用户访问他们所要用户访问的站点。而最终造成的后果，重定向会使得用户访问钓鱼网站或是恶意网站

未验证的重定向和转发

测试对象：

- 有重定向的页面

http://jiaoyou.58.com/mmvideo/frameset?url=http://360buy.com

http://jd2008.360buy.com/purchase/shoppingcart_pop.aspx?backurl=http://product.dangdang.com/product.aspx?product_id=20230002

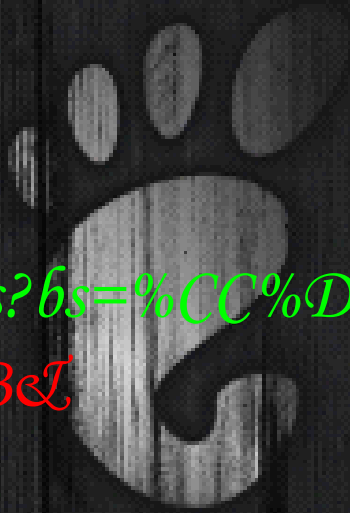
地址栏加密

地址栏中会透露出用户的敏感信息，使外界人员很容易搜集到有效信息

地址栏加密

测试对象：

带参数的地址



http://www.baidu.com/s?bs=%CC%D4%B1%A6QA&lf=8&wd=%C6%BB%B9%FB&l

暴库（%5C）

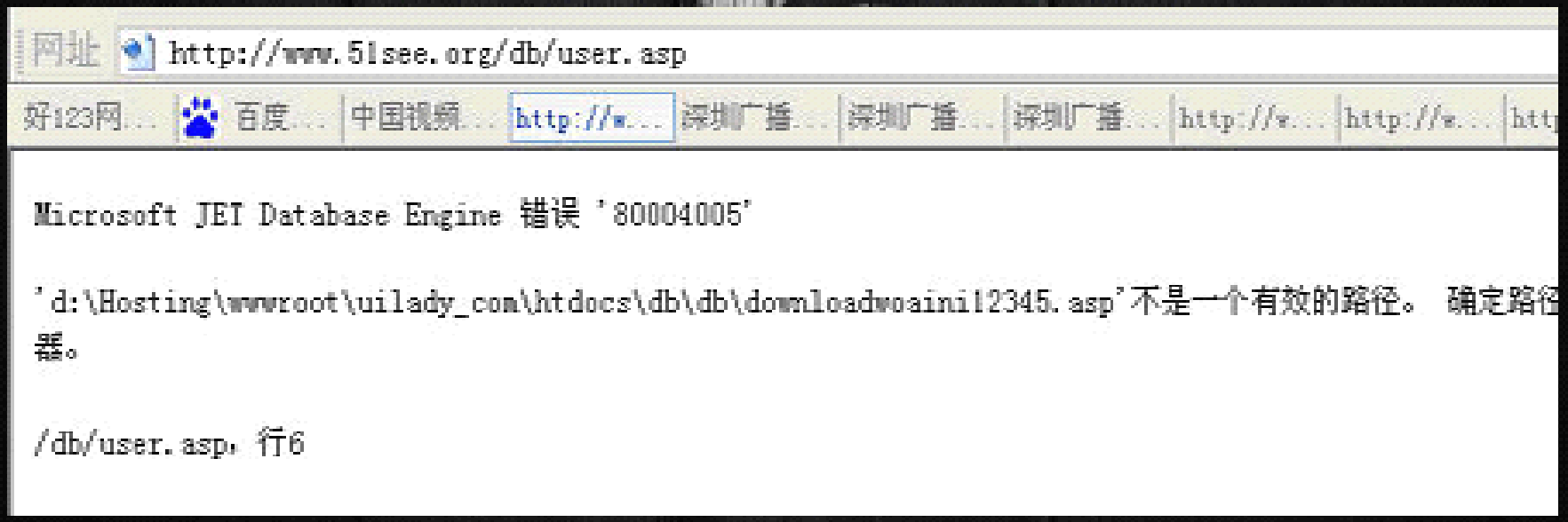
通过编码将数据非法下载到本地。通过数据得到网站用户的隐私信息，甚至得到服务器的最高权限。

暴库（%5C）

测试对象：

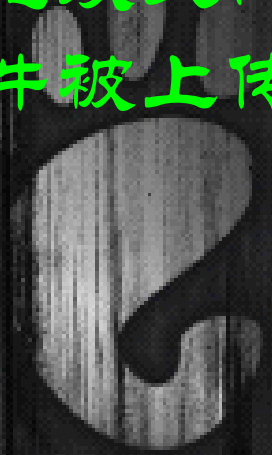
带参数的地址

http://jd2008.360buy.com%5cuser_refundment.aspx



无过滤的上传功能

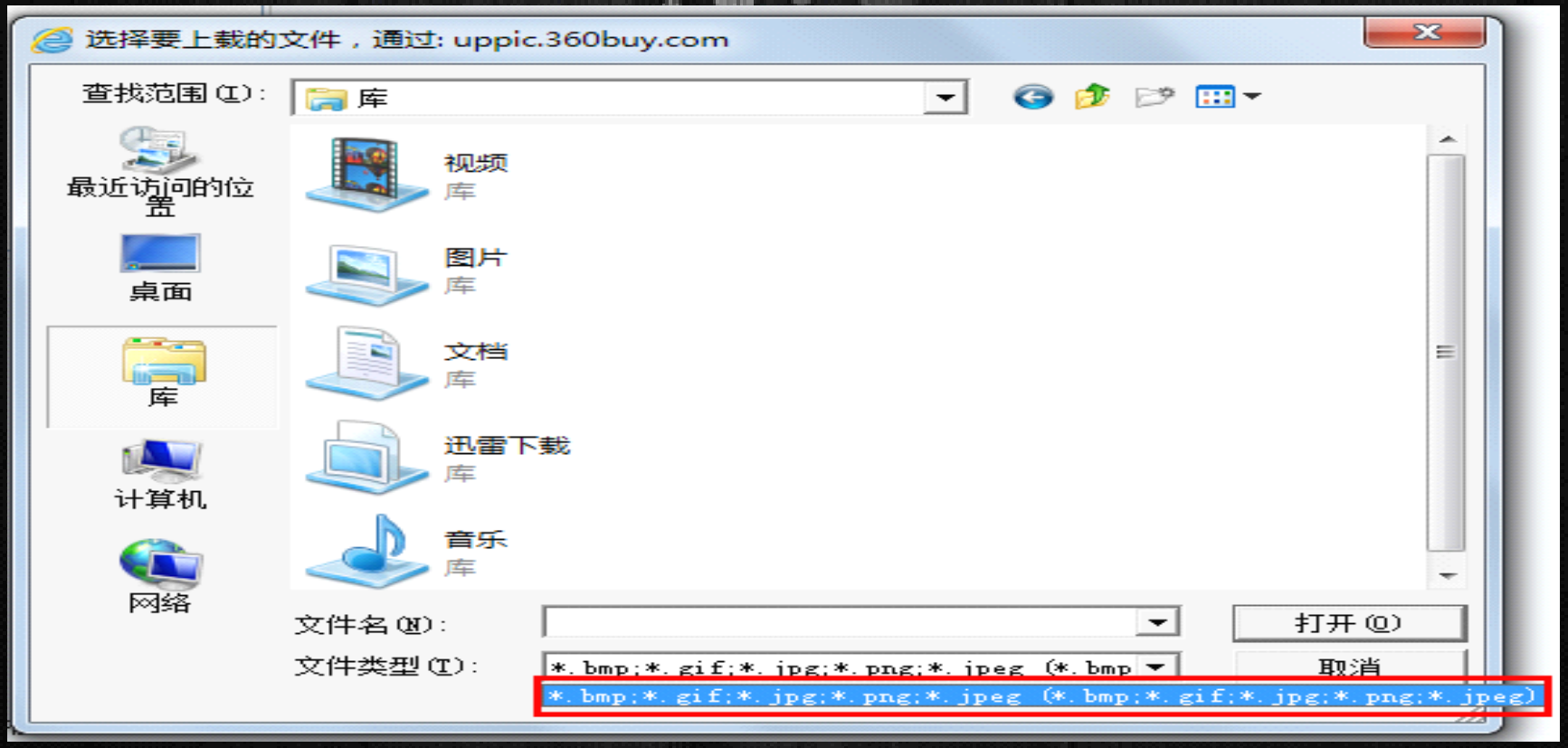
上传文件时容易出现不过滤文件类型的错误，从而导致一些无效文件被上传成功，严重时出现木马文件被上传成功，并完全控制服务器。



无过滤的上传功能

测试对象：

具有上传功能的模块（有病毒的文件上传）



登录提示信息

用户登录提示信息会给攻击者一些有用的信息，作为程序的开发人员应该做到对登录提示信息的模糊化，以防攻击者利用登录得知用户是否存在

登录提示信息

测试对象：

- 登录页面的提示信息

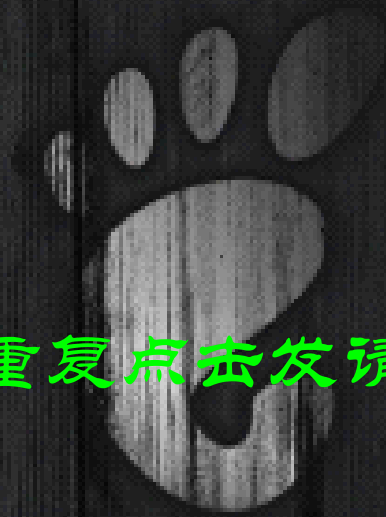
重复提交请求

程序员在代码中没有对重复提交请求做阻制，这样就会出现订单被多次下单，帖子被重复发布。恶意攻击者可能利用此漏洞对网站进行批量灌水，致使网站瘫痪

重复提交请求

测试对象：

- 提交请求的按钮



填写完必填项后，重复点击发请求的按钮

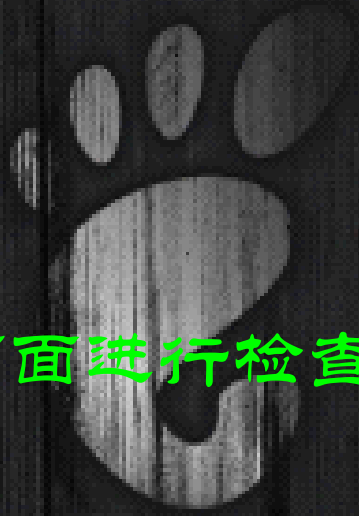
网页脚本错误

访问者所使用的浏览器不能完全支持页面里的脚本，形成“脚本错误”，也就是网站中的脚本没有被成功执行。遇到“脚本错误”时一般会弹出一个非常难看的脚本运行错误警告窗口

网页脚本错误

测试对象：

- 所有页面



对要上线的所有页面进行检查，网页中禁止出现脚本错误

Commnets: IE6 对脚本的支持稍差

Q & A


The End
http://www.不黑你黑谁.com