The market for mobile applications is growing and more and more transactions are made on mobile devices. A variety from mobile payment systems is trying to attract the users and this creates a growing field for attackers to get into this systems and manipulate them.

Now, the shop webpages also have to work on various platforms and devices and special versions for each device are often created. This again gives attackers a big range of attack vectors.

There are mainly significant problems in the mobile application sector that is occuring mainly all time. The developers of the most mobile apps do not have the technical skills and experience to secure their applications. But this unsecure applications are provided for download at the big app stores. Thus affects finally the secure infrastructure of the mobile devices connected to shops like apple itunes, apple appstore, google app-store, open-market and windows market-place.

The publication control systems of these app-stores and market-places are proportinal low to the available safety risk that the manufacturer and vendor takes for the customer. As far as an attacker is able to compromise only one app, he can get control of the affected device. We saw that in the last 2 years by criminals and government acting agencies that try to evade the security concepts of the iOS product series at all instances. By watching the public sector you can see that there is a big need for criminals and government agencies to take control of mobile devices.

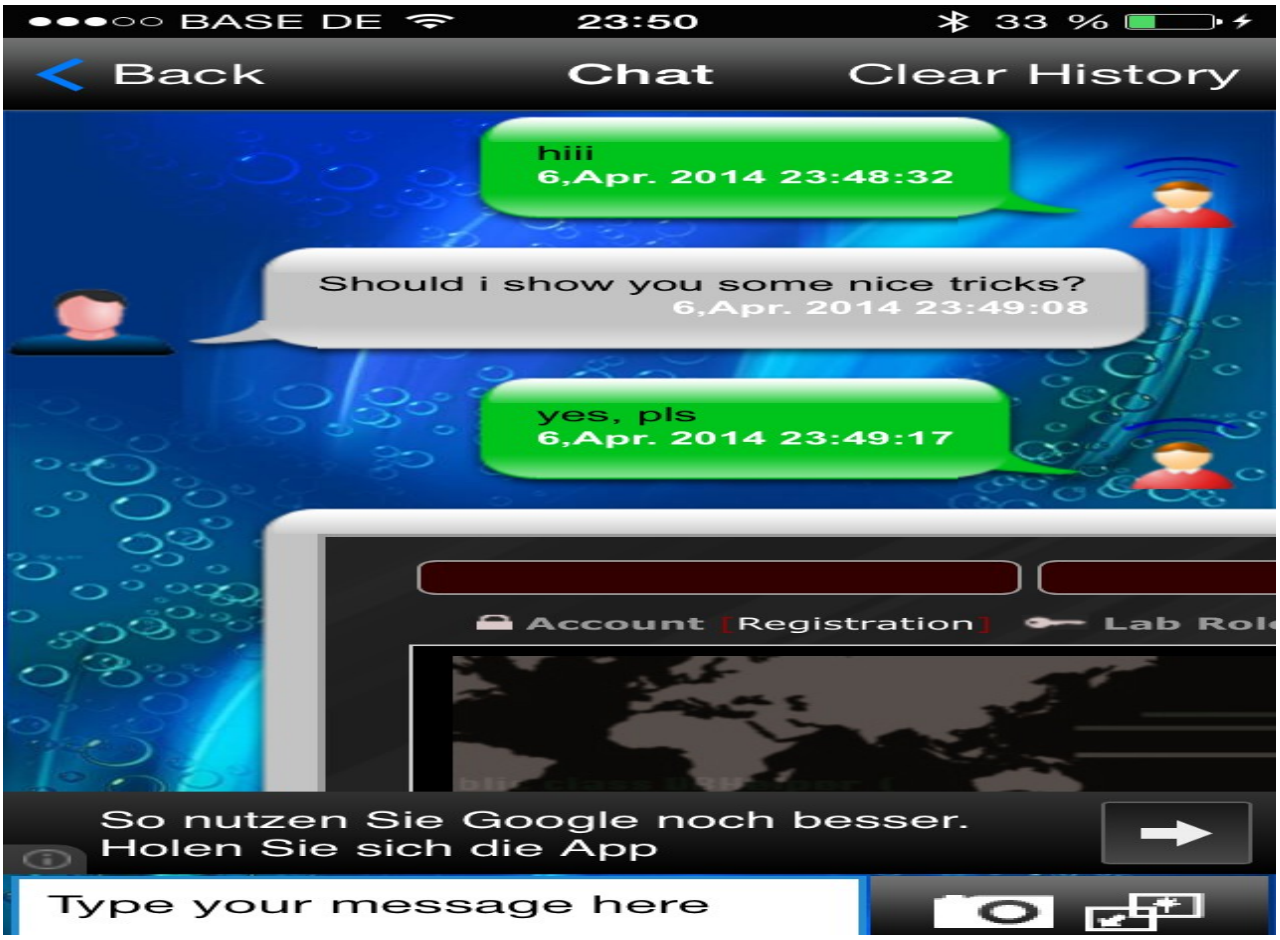
The main problem with application bugs is that they are produced by a third party to the manufacturer without correct responsibility. In case of a critical vulnerability the manufacturer (apple) does not care about the disclosure or risk. A researcher or coordinator has to get in contact with the developer (3rd party).

Normally the manufacturer of the product should take control about the notification and disclosure process because the products are running on there device finally. In such a case the apple product security team would like to say nothing and let the researcher interact with the developer. In 80% of the disclosed vulnerabilities in our mobile feed we got no reply by the developer which results in a full disclosure. Even after the release the manufacturer mostly would like to not become responsible for such bugs even if the customers are finally affected.

Facebook portal for example rushs to inform all application vedors about discovered bugs, even if they are created by a third party. Same should be done by manufacturer to secure the product line and grant that no backdoors or permanent exploitable security bugs are available over years.

An adopting problem occurs very often when the same issues are as well adopted to several other mobile applications. Lets say there is a manufacturer programming a web interface for wifi. Now he used the webkit and java coding language with the available programming engines. In case of that there are often old packages to generate simply functions for iOS or there are wrong tutorials publicly available that teaches the young developer the wrong way of implementation. In a lot of test cases we found a UI that was programmed by one developer and shared to different parties for adopting the modules.

The vulnerabilities we mention are actual treads to the mobile app and shop security. There is a lot of work for security researcher to make this systems more secure, the vendors are in charge to build internal security teams or let external researchers test the systems. Because of the actual laws against hacking the independent research is very limited in looking for vulnerabilities on their own. Without the acceptance of the vendor its against the law to test a computer system for common bugs and vulnerabilities. But sadly many vendors do not have internal security teams or book external experts to secure their systems.


●●●○○ BASE DE 23:50 33 %

Back Chat Clear History

hiii
6,Apr. 2014 23:48:32

Should i show you some nice tricks?
6,Apr. 2014 23:49:08

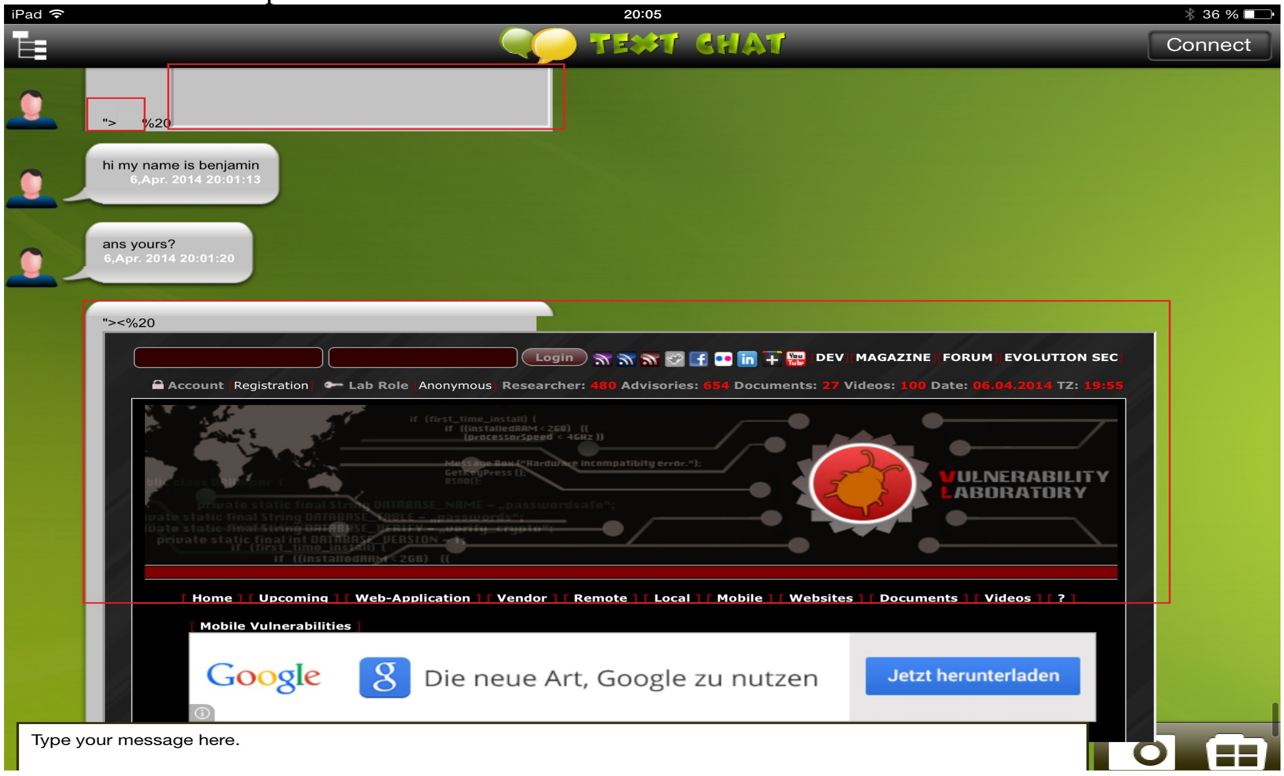
yes, pls
6,Apr. 2014 23:49:17

Account [Registration] Lab Rol

So nutzen Sie Google noch besser.
Holen Sie sich die App

Type your message here

The image above shows an application-side input validation vulnerability and filter bypass issue in a bluetooth chat software of the apple mobile iOS. The attacker can send malicious messages to the victim via bluetooth protocol of the iOS device.


iPad 20:05 36 %

TEXT CHAT Connect

"> %20

hi my name is benjamin
6,Apr. 2014 20:01:13

ans yours?
6,Apr. 2014 20:01:20

"><%20

Login DEV MAGAZINE FORUM EVOLUTION SEC

Account [Registration] Lab Role [Anonymous] Researcher: 480 Advisories: 654 Documents: 27 Videos: 100 Date: 06.04.2014 TZ: 19:55

VULNERABILITY LABORATORY

[Home] [Upcoming] [Web-Application] [Vendor] [Remote] [Local] [Mobile] [Websites] [Documents] [Videos] [?]

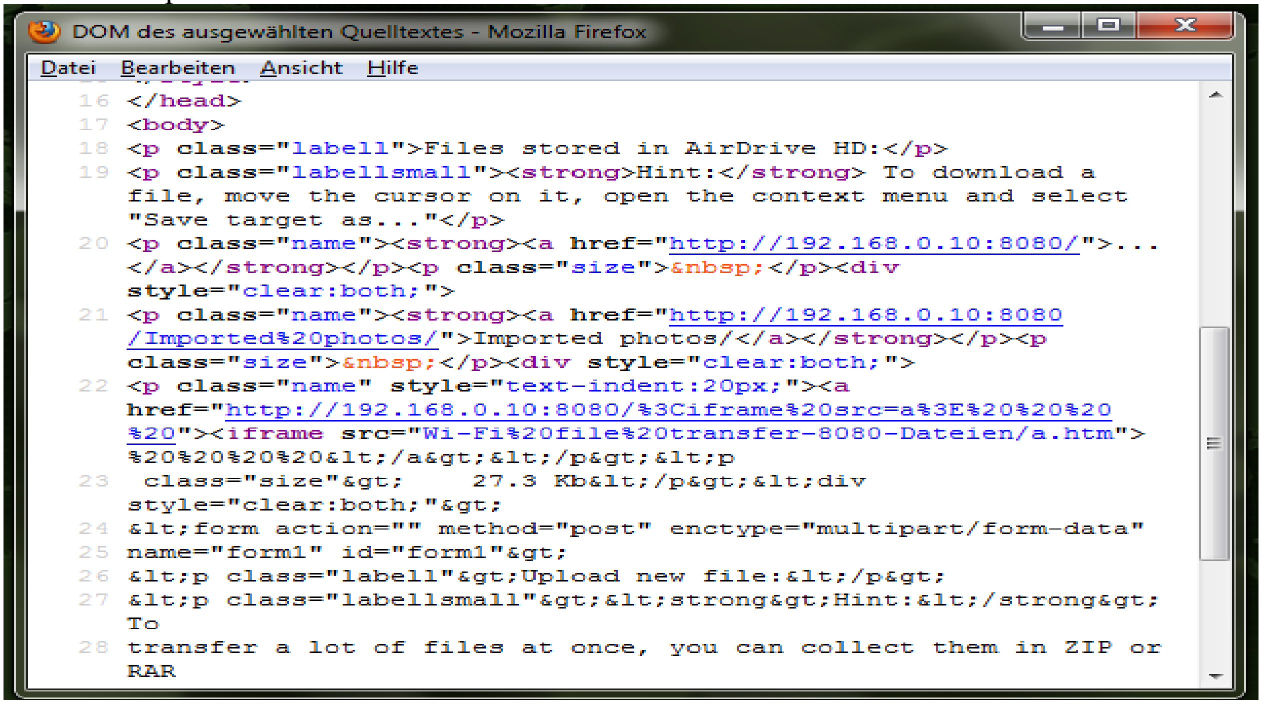
[Mobile Vulnerabilities]

Google Die neue Art, Google zu nutzen Jetzt herunterladen

Type your message here.

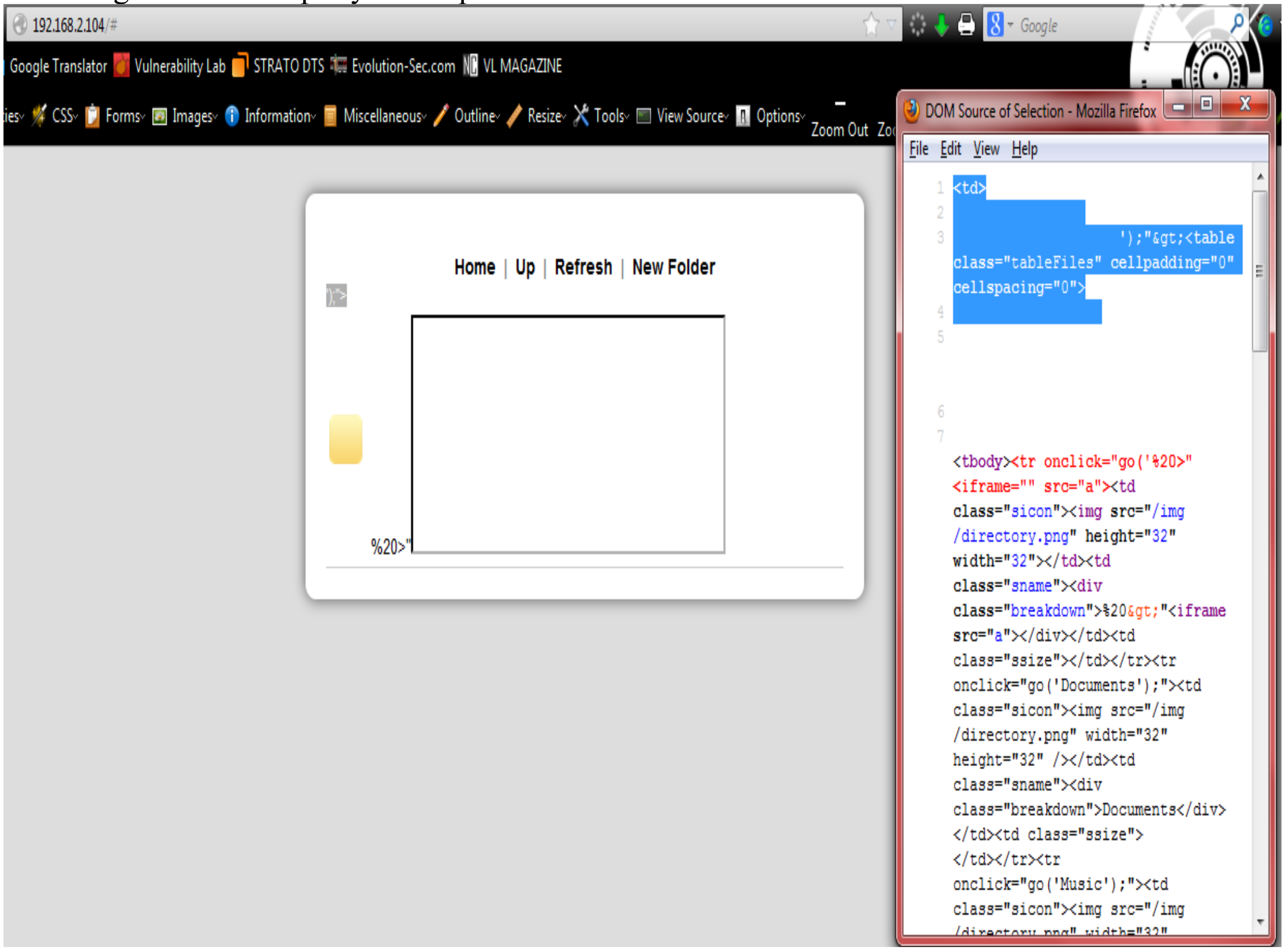
The picture above shows the same issue within another mobile application. The issue occurs in the same location of the application because of significant failure in validation procedure. The same module has been adopted to another software which results in a general security issue.

In the next picture we can see a vulnerability that occurs because of the wrong encoding of the device name (c:id) value. The bug allows to use the name value of a stored code to trigger a persistent script code execution.


DOM des ausgewählten Quelltextes - Mozilla Firefox
Datei Bearbeiten Ansicht Hilfe

```
</head>
<body>
<p class="label1">Files stored in AirDrive HD:</p>
<p class="label1small"><strong>Hint:</strong> To download a
file, move the cursor on it, open the context menu and select
"Save target as..."</p>
<p class="name"><strong><a href="http://192.168.0.10:8080/">...
</a></strong></p><p class="size">&nbsp;</p><div
style="clear:both;">
<p class="name"><strong><a href="http://192.168.0.10:8080
/Imported%20photos/">Imported photos/</a></strong></p><p
class="size">&nbsp;</p><div style="clear:both;">
<p class="name" style="text-indent:20px;"><a
href="http://192.168.0.10:8080/%3Ciframe%20src=a%3E%20%20%20
%20"><iframe src="Wi-Fi%20file%20transfer-8080-Dateien/a.htm">
%20%20%20%20&lt;/a&gt;&lt;/p&gt;&lt;p
 class="size"&gt;    27.3 Kb&lt;/p&gt;&lt;div
style="clear:both;"&gt;
&lt;form action="" method="post" enctype="multipart/form-data"
name="form1" id="form1"&gt;
&lt;p class="label1"&gt;Upload new file:&lt;/p&gt;
&lt;p class="label1small"&gt;&lt;strong&gt;Hint:&lt;/strong&gt;
To
transfer a lot of files at once, you can collect them in ZIP or
RAR
```

The same issue occurs also in the following code line of multiple other mobile apps with wifi interface. Reason is that apple does not prevent the device name because of allowing any char to rename it. Thus results in a permanent failure of validation in hundrets of application without knowledge of the third party developers.



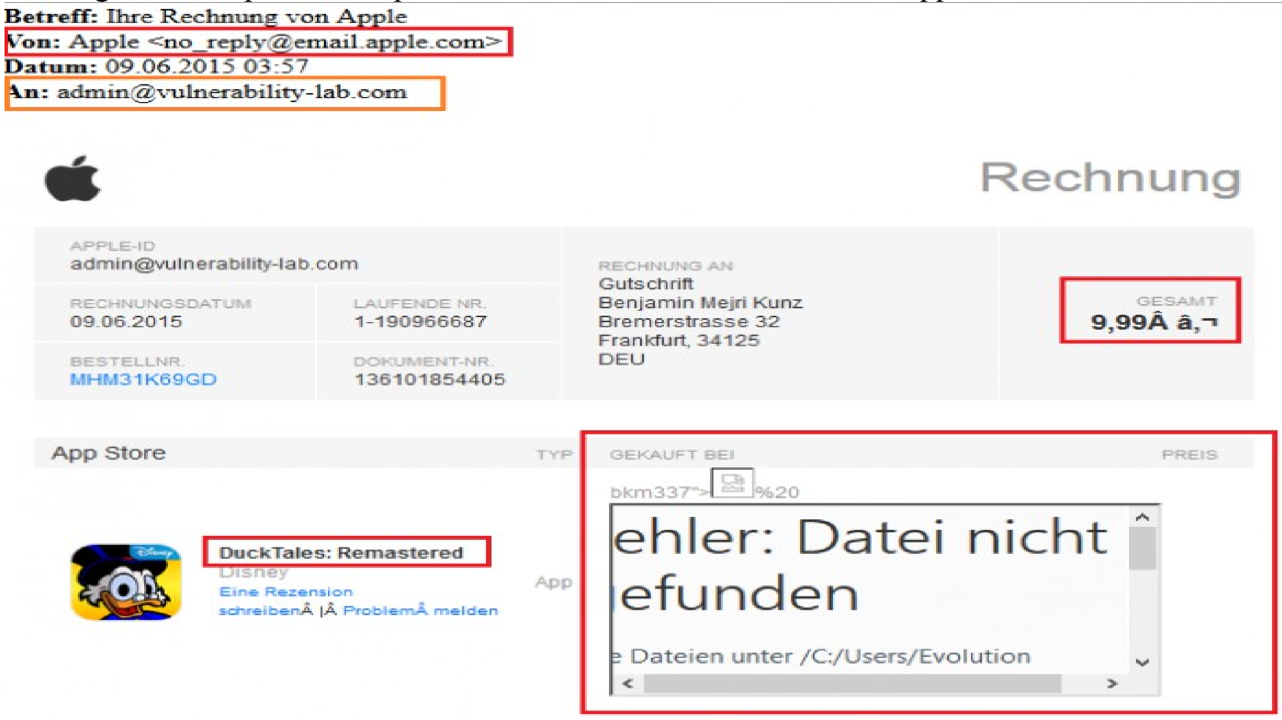
```
<td>

                ');"&gt;<table
class="tableFiles" cellpadding="0"
cellspacing="0">



<tbody><tr onclick="go('%20>"
<iframe="" src="a"><td
class="sicon"><img src="/img
/directory.png" height="32"
width="32"></td><td
class="sname"><div
class="breakdown">%20&gt;"<iframe
src="a"></div></td><td
class="ssize"></td></tr><tr
onclick="go('Documents');"><td
class="sicon"><img src="/img
/directory.png" width="32"
height="32" /></td><td
class="sname"><div
class="breakdown">Documents</div>
</td><td class="ssize">
</td></tr><tr
onclick="go('Music');"><td
class="sicon"><img src="/img
```

Beginning of the year 2015 the core researchers of the vulnerability laboratory revealed a backdoor in the invoices of apple itunes & appstore when processing to buy a mobile web-application. The vulnerability was connected to the shop infrastructure, hardware settings and email configuration. The bug had an impact to compromise another users device or mobile applications.

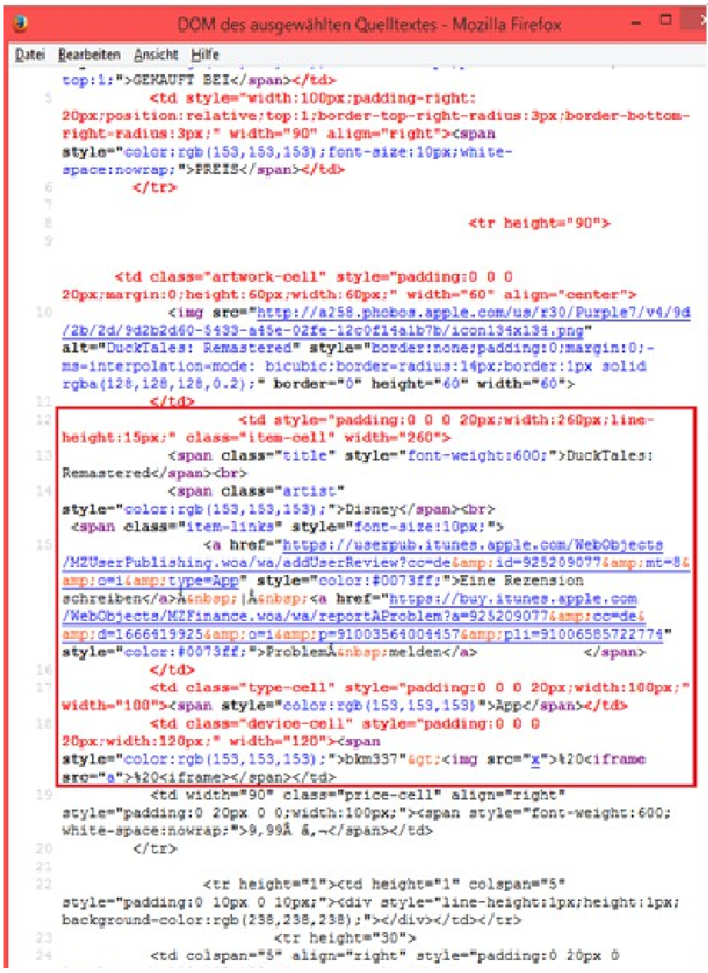


Betreff: Ihre Rechnung von Apple
Von: Apple <no_reply@email.apple.com>
Datum: 09.06.2015 03:57
An: admin@vulnerability-lab.com

Rechnung

APPLE-ID admin@vulnerability-lab.com		RECHNUNG AN Gutschrift Benjamin Mejri Kunz Bremerstrasse 32 Frankfurt, 34125 DEU	GESAMT 9,99Â â,¬
RECHNUNGSDATUM 09.06.2015	LAUFENDE NR. 1-190966687		
BESTELLNR. MHM31K69GD	DOKUMENT-NR. 136101854405		

App Store	TYP	GEKAUFT BEI	PREIS
DuckTales: Remastered Disney Eine Rezension schreibenÂ |Â ProblemÂ melden	App	bkm337">%20 ehler: Datei nicht efunden e Dateien unter /C:/Users/Evolution	



DOM des ausgewählten Quelltextes - Mozilla Firefox
Datei Bearbeiten Ansicht Hilfe

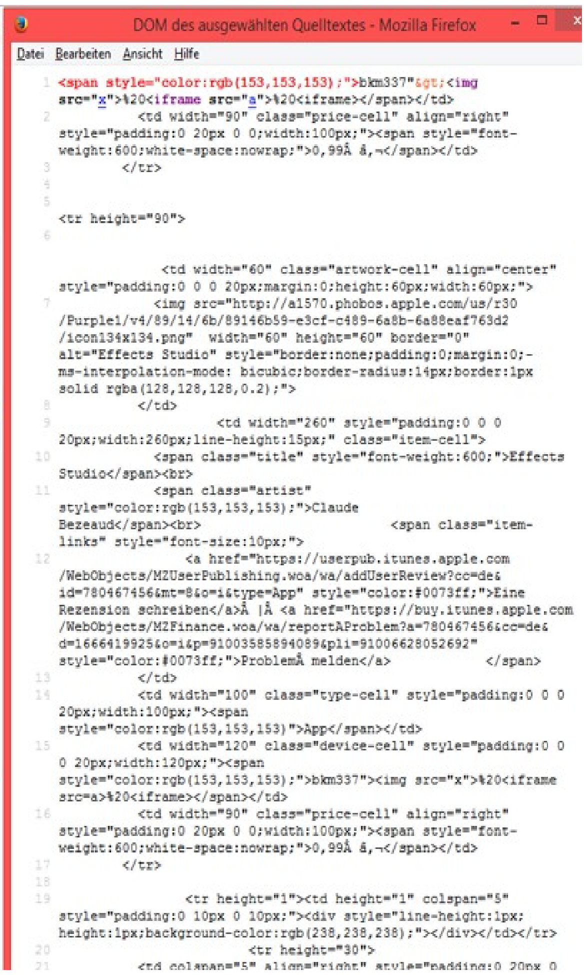
```
top:1;">GEKAUFT BEI</span></td>
            <td style="width:100px;padding-right:
20px;position:relative;top:1;border-top-right-radius:3px;border-bottom-
right-radius:3px;" width="90" align="right"><span
style="color:rgb(153,153,153);font-size:10px;white-
space:nowrap;">PREIS</span></td>
        </tr>


                                                <tr height="90">



        <td class="artwork-cell" style="padding:0 0 0
20px;margin:0;height:60px;width:60px;" width="60" align="center">
                <img src="http://a258.phobos.apple.com/us/r30/Purple7/v4/9d
/2b/2d/9d2b2d60-5433-a45e-02fe-12c0f14a1b7b/icon134x134.png"
alt="DuckTales: Remastered" style="border:none;padding:0;margin:0;-
ms-interpolation-mode: bicubic;border-radius:14px;border:1px solid
rgba(128,128,128,0.2);" border="0" height="60" width="60">
            </td>
                            <td style="padding:0 0 0 20px;width:260px;line-
height:15px;" class="item-cell" width="260">
                <span class="title" style="font-weight:600;">DuckTales:
Remastered</span><br>
                <span class="artist"
style="color:rgb(153,153,153);">Disney</span><br>
 <span class="item-links" style="font-size:10px;">
                    <a href="https://userpub.itunes.apple.com/WebObjects
/MZUserPublishing.woa/wa/addUserReview?cc=de&amp;id=925209077&amp;mt=8&
amp;o=i&amp;type=App" style="color:#0073ff;">Eine Rezension
schreiben</a>Â&nbsp;|Â&nbsp;<a href="https://buy.itunes.apple.com
/WebObjects/MZFinance.woa/wa/reportAProblem?a=925209077&amp;cc=de&
amp;d=1666419925&amp;o=i&amp;p=910035640044457&amp;pli=910065857227774"
style="color:#0073ff;">ProblemÂ&nbsp;melden</a>                </span>
            </td>
            <td class="type-cell" style="padding:0 0 0 20px;width:100px;"
width="100"><span style="color:rgb(153,153,153)">App</span></td>
            <td class="device-cell" style="padding:0 0 0
20px;width:120px;" width="120"><span
style="color:rgb(153,153,153);">bkm337"&gt;<img src="x">%20<iframe
src="a">%20<iframe></span></td>
            <td width="90" class="price-cell" align="right"
style="padding:0 20px 0 0;width:100px;"><span style="font-weight:600;
white-space:nowrap;">9,99Â â,¬</span></td>
        </tr>


                    <tr height="1"><td height="1" colspan="5"
style="padding:0 10px 0 10px;"><div style="line-height:1px;height:1px;
background-color:rgb(238,238,238);"></div></td></tr>
                        <tr height="30">
            <td colspan="5" align="right" style="padding:0 20px 0
```



DOM des ausgewählten Quelltextes - Mozilla Firefox
Datei Bearbeiten Ansicht Hilfe

```
<span style="color:rgb(153,153,153);">bkm337"&gt;<img
src="x">%20<iframe src="a">%20<iframe></span></td>
            <td width="90" class="price-cell" align="right"
style="padding:0 20px 0 0;width:100px;"><span style="font-
weight:600;white-space:nowrap;">0,99Â â,¬</span></td>
        </tr>



<tr height="90">



                <td width="60" class="artwork-cell" align="center"
style="padding:0 0 0 20px;margin:0;height:60px;width:60px;">
                <img src="http://a1570.phobos.apple.com/us/r30
/Purple1/v4/89/14/6b/89146b59-e3cf-c489-6a8b-6a88eaf763d2
/icon134x134.png"  width="60" height="60" border="0"
alt="Effects Studio" style="border:none;padding:0;margin:0;-
ms-interpolation-mode: bicubic;border-radius:14px;border:1px
solid rgba(128,128,128,0.2);">
            </td>
                        <td width="260" style="padding:0 0 0
20px;width:260px;line-height:15px;" class="item-cell">
                <span class="title" style="font-weight:600;">Effects
Studio</span><br>
                <span class="artist"
style="color:rgb(153,153,153);">Claude
Bezeaud</span><br>                        <span class="item-
links" style="font-size:10px;">
                    <a href="https://userpub.itunes.apple.com
/WebObjects/MZUserPublishing.woa/wa/addUserReview?cc=de&
id=780467456&mt=8&o=i&type=App" style="color:#0073ff;">Eine
Rezension schreiben</a>Â |Â <a href="https://buy.itunes.apple.com
/WebObjects/MZFinance.woa/wa/reportAProblem?a=780467456&cc=de&
d=1666419925&o=i&p=910035858940894&pli=910066280526292"
style="color:#0073ff;">ProblemÂ melden</a>            </span>
            </td>
            <td width="100" class="type-cell" style="padding:0 0 0
20px;width:100px;"><span
style="color:rgb(153,153,153)">App</span></td>
            <td width="120" class="device-cell" style="padding:0 0
0 20px;width:120px;"><span
style="color:rgb(153,153,153);">bkm337"><img src="x">%20<iframe
src=a>%20<iframe></span></td>
            <td width="90" class="price-cell" align="right"
style="padding:0 20px 0 0;width:100px;"><span style="font-
weight:600;white-space:nowrap;">0,99Â â,¬</span></td>
        </tr>


                    <tr height="1"><td height="1" colspan="5"
style="padding:0 10px 0 10px;"><div style="line-height:1px;
height:1px;background-color:rgb(238,238,238);"></div></td></tr>
                        <tr height="30">
            <td colspan="5" align="right" style="padding:0 20px 0
```

The last picture demonstrates how the code of the hardware has been used to the buy an app for final exploitation of the apple invoice.

Reference(s):
http://www.vulnerability-lab.com/show.php?cat=mobile
http://www.vulnerability-lab.com/search.php?search=apple+ios&submit=Search
http://www.vulnerability-lab.com/search.php?search=android&submit=Search
http://www.vulnerability-lab.com/get_content.php?id=1597
http://www.vulnerability-lab.com/get_content.php?id=1481
http://www.vulnerability-lab.com/get_content.php?id=1410
http://www.vulnerability-lab.com/get_content.php?id=1413
http://www.vulnerability-lab.com/get_content.php?id=1512