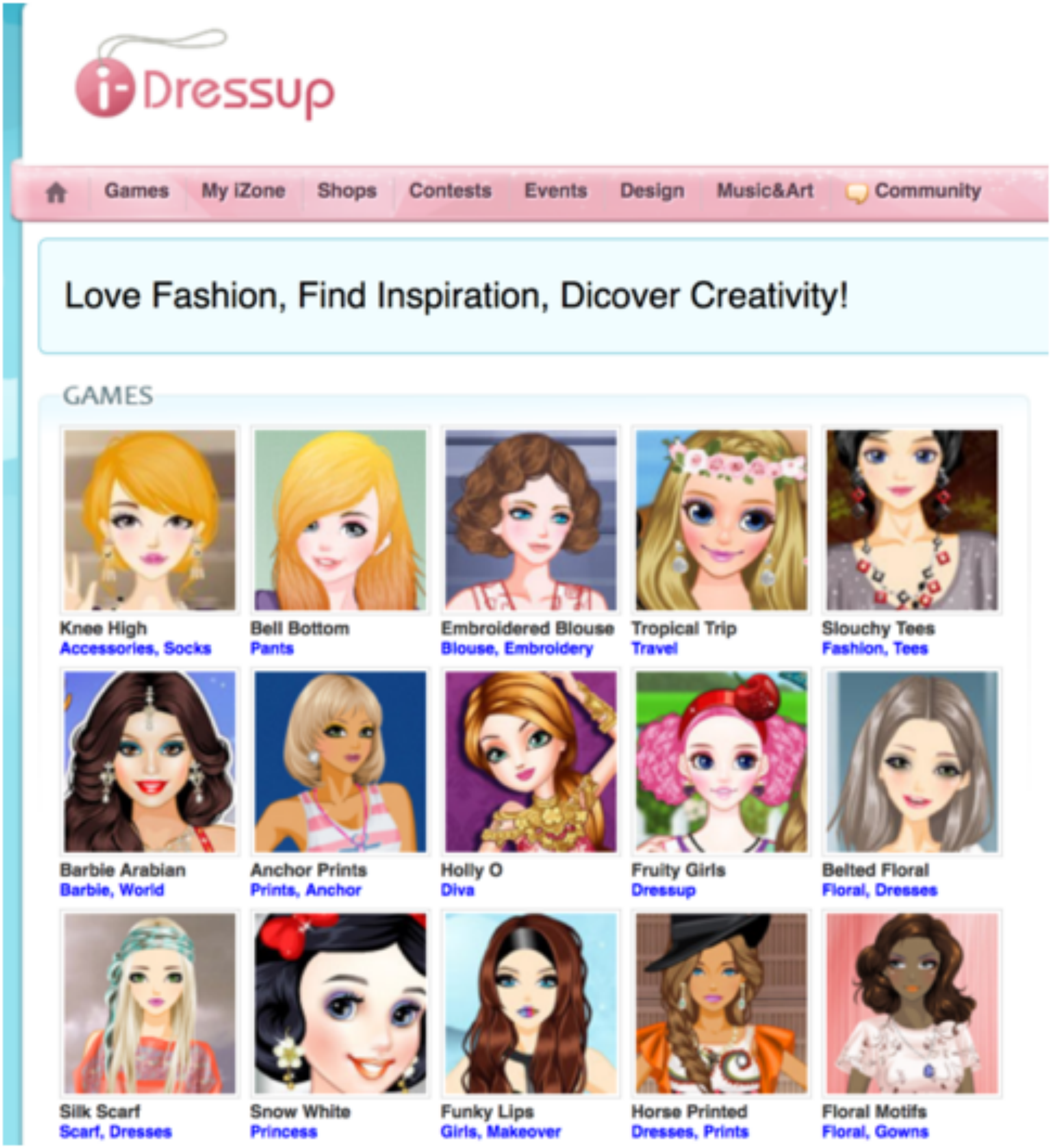
RISK ASSESSMENT —

As we speak, teen social site is leaking millions of plaintext passwords

i-Dressup operators fail to fix bug that exposes up to 5.5 million credentials.

DAN GOODIN - 9/26/2016, 11:20 AM



Love Fashion, Find Inspiration, Dicover Creativity!

63

A social hangout website for teenage girls has sprung a leak that's exposing plaintext passwords protecting as many as 5.5 million user accounts. As this post went live, all attempts to get the leak plugged had failed.

Operators of i-Dressup didn't respond to messages sent by Ars informing them that a hacker has already downloaded more than 2.2 million of the improperly stored account credentials. The hacker said it took him about three weeks to obtain the cache and that there's nothing stopping him or others from downloading the entire database of slightly more than 5.5 million entries. The hacker said he acquired the e-mail addresses and passwords by using a SQL injection attack that exploited vulnerabilities in the i-Dressup website.

The hacker provided the 2.2 million account credentials both to Ars and breach notification service Have I Been Pwned?. By plugging randomly selected e-mail addresses into the forgotten password section of i-Dressup, both Ars and Have I Been Pwned? principal Troy Hunt found that they all were used to register accounts on the site. Ars then used the contact us page on i-Dressup to privately notify operators of the vulnerability, but more than five days later, no one has responded and the bug remains unfixed.

It's only the latest mass leak to expose plaintext passwords in recent days. As Ars reported two weeks ago, plaintext passwords, usernames, e-mail addresses, and a wealth of other personal information were recently published for more than 2.2 million people who created accounts with online survey website ClixSense. The hackers who dumped the collection claimed to have data for a total of 6.6 million accounts and were offering to sell the unpublished 4.4 million entries.

FURTHER READING
6.6 million plaintext passwords exposed as site gets hacked to the bone

I-Dressup bills itself as a secure site that goes out of its way to protect the privacy of its users, particularly those who are under the age of 13 years old. But those assurances don't hold up to even casual scrutiny. It's bad enough that a SQL-injection vulnerability that dumps passwords remained unfixed even after it was privately reported. It's even worse that the database contained plaintext passwords. Industry standards dictate that passwords be converted into a cryptographic hash that requires an attacker to spend time and computing resources to restore to a human-readable form.

Anyone who had an account on i-Dressup should strongly consider closing it. Users should also be on the alert for scam e-mails that make use of the data. Users should change passwords on any other websites that used the same or similar credentials.

FURTHER READING
The secret to online safety: Lies, random characters, *and* a password manager

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 63

SHARE THIS STORY

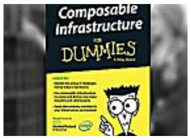
← PREVIOUS STORY

NEXT STORY →

Related Stories

Sponsored Stories

Powered by



Boost Your Business By Streamlining Your Data Center

Hewlett Packard Enterprise

The New Sheets You Need to Buy

GQ

Unexplained Phenomena In Our Universe

CoolTechLists

25 Times The Wedding Photographer Captured More Than Expected

Auto Overload

Man Unearths Ancient Two-Ton Buried Mystery

Detonate

Estream is a personal hydroelectric generator for charging your gadgets

Digital Trends

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS