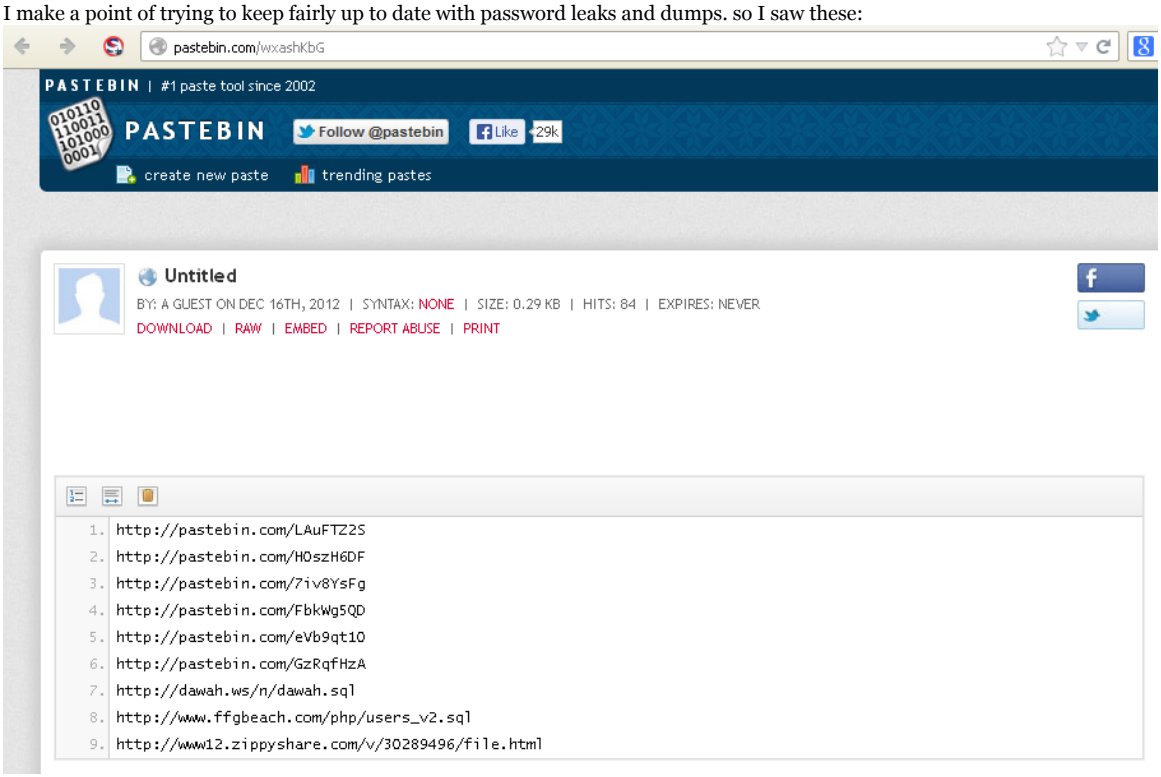
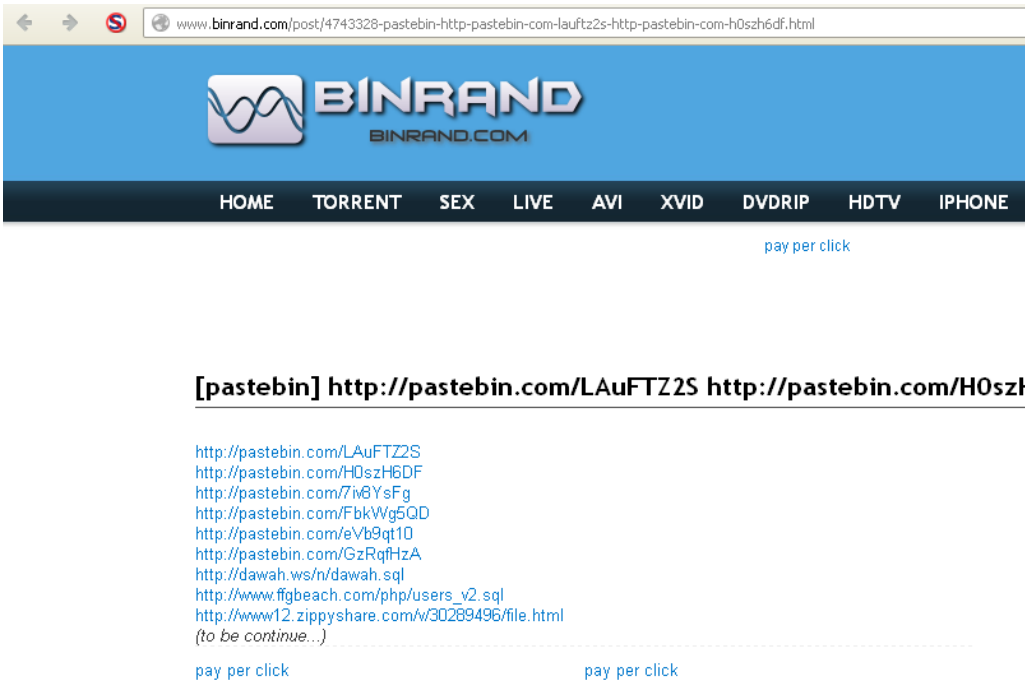
FFGBEACH = HEAD+DESK

Let me start by saying I was not sure about writing this particular article but after some serious thought I figured not doing so would be doing more harm then doing it. This article is a documentation of a tragedy of errors that shows how bad things can be, the lies a company can tell and just general stupidity (I make no apologies for using that term by the way). Before we start, all screenshots I show come from the last 2 days. This is important as you will see...

I make a point of trying to keep fairly up to date with password leaks and dumps. so I saw these:

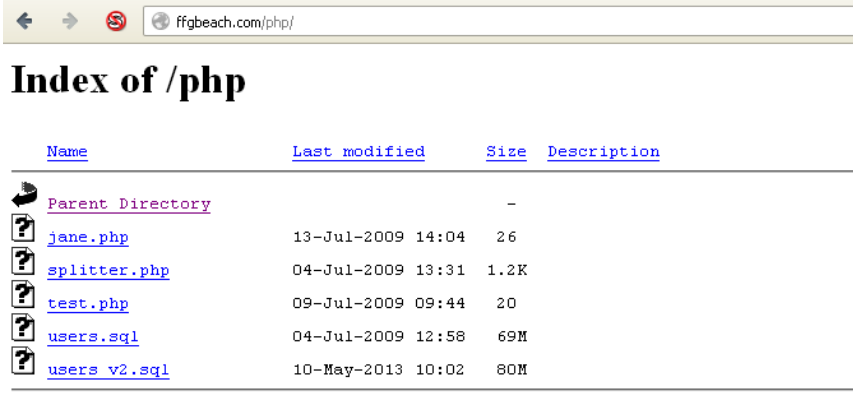


..and

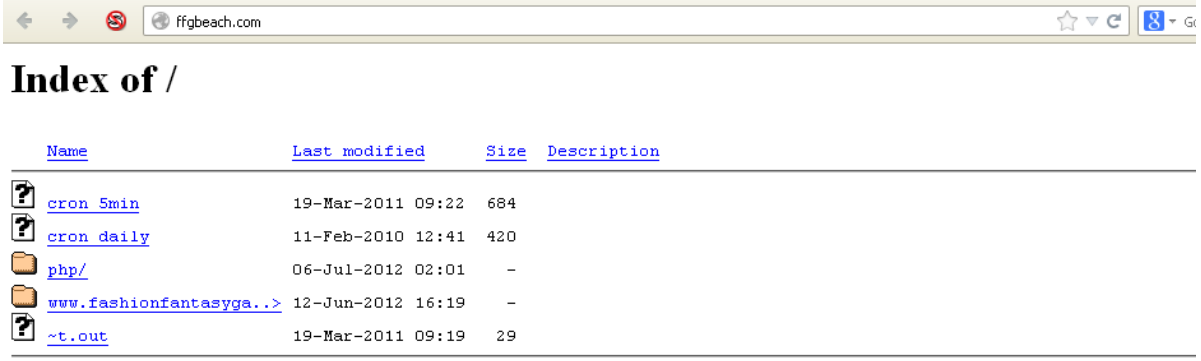


Now the pastebin link shows when it was posted - December 2012. So I thought "no way is this still valid, this would be gone by now. I mean I am 4 months late!". But I still went to go take a look optimist that I am (silly, silly me). And I see this:

WTF! Directly after seeing this I am telling myself "No way is this real, this is a fake dump! Still live after 4 months? Has to be fake.". So I looked around I little. I went to the "php" folder in the url:



I went back to the root of the site:



I went digging a bit and saw:

Index of /www.fashionfantasygame.com/var/auth

Name	Last modified	Size	Description
Parent Directory		-	
id	17-Oct-2009 17:24	1.6K	
id for ffgadm1	06-Oct-2009 05:55	1.6K	
id for nobody	17-Oct-2009 19:54	1.6K	
known_hosts	28-May-2010 11:02	1.0K	

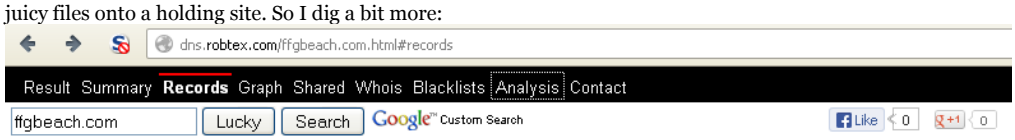

```
# provide info for the servers in the server farm
# name IP user document_root
#
qs2237 209.68.17.43 ffgadm1 /usr/www/users/ffgadm1/www.fashionfantasygame.com/production
qs2238 216.92.127.197 ffgadm2 /usr/www/users/ffgadm2/www.fashionfantasygame.com/production
```


```
qs2238,216.92.127.197 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAu8dzZ+cKbw+EzFZjQ86cyO2JWBvEqWNOCCEfroxECOOhxKK1PXTCM4op7WCnHdd6
www.comagna.com,74.220.215.86 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAuhevdaqYUDfXboEwwn3dE7IlmTxNK4nvmUuB+P7TSL6jd4cUGfDifQzv
qs2239.pair.com,216.92.127.231 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAu8dzZ+cKbw+EzFZjQ86cyO2JWBvEqWNOCCEfroxECOOhxKK1PXTCM4o
```

ffgbeach.com/www.fashionfantasygame.com/var/auth/id

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEArbOQGhyGSHzBNde2ODBT/FrYxkNXjjxZ2JKTRUvyth6YhG9d
OSTsdasS1GsLVix47e9tbrivUscQ53z714/kU3Zr+yLu4pe3/+OcpgYONylA792R
OpMJKWnSJZpC7xjE+cF+enAu/C6NqKtwKC4p38p+y7+xpSYl8sPb5ZfOKv4pXKrL
Tr12EGCMHFPzhT2zXDUpIzDGTEbvObgwyuoPACgHguI2FWZHAC9qwLNdi7Jgrx8Y
mFcCewyZguGgKl2DO2LjaiHOAD9NB4QVGtPrLosJBL/mzto5ZDVyvkw9QVAArHrE
YoCxpI+zkr/QJfO6aZjI2NBQuXYnUj1Li6eD1wIBIwKCAQEAhgbgiSvyj7CyThtv
T+rEcjdOBqj6ZmkSHBlNCZJcJheaOkdH6kEOLuMOhpu4ScqJLJQhOCgSOIrvyIT8
mX2hgjbIVAUBbPiyg5moYtGV/qrLsbmNv7NBlPncoKozooDSd4ajZcRBgLYyw/H3
b3QRrKOGYqnSLvGK/Rq/k9uByWO1o9dsFoLZZ4djDdJnoqu36wd+4fNulYQOCNqx
sWgHB3qdGPT4jufxrClsLmMJCa7RbZEZUX8PiX43T7YMoQHgBdjp2BLytxHqW+uM
7e3TAvB2jcT3MJfRj/bBWxG8XA8wxkw7jJxklKVLUyCFThFIiMSe9miB6AUCQhHB
SVFhOwKBgQDcXqrDwu+95Vt0449qVOAJFeQArWuaM2AEvvUwo4EObc7Ylt3MQRZ7
W1vZhJ/6T8Fyn64ahuzjASIYaiTCB+l45lF1g5MdwfWt6F5XOTQFRoS3CxxOPAnc
U+HLuOKr6+wQpwYMF2oSzlwsf4A/v82Jfiugeh8mqp5o6ByLqkaHvwKBgQDJ1EeX
4GJ4a+1K93FrIjuC+TR6gEc97snEEMPz4p+iDWToBI34N4HxLfMOaD2s2g5QW3wD
LIMLVegTeIUGpxLMFOVIQD08uUVcXCPOTmIgOYw9CPlOgzr4E1Ynn/KTrqWUWbyR
Bpe9o7wSeBVoVkis98OcrX8GZtFAOmiMb1/J6QKBgGsJaOK9xOcO4OdnNwfD+ogR
8ma6ofpwuZvnuOu9IX/dkFqSa7r7Cut1hGJWXFUCKsKlVJCKrZLUqikdnNNFq+pD
+64bVhXEm+bBUmThRSciQHYp9+CvcoD1iu3tPaP2P3XNd/c+kptri9sZW4ytnli5
oC1f4z6qpLacoCaUiKhVAoGAbZB+oueF6Zmss6rlzHGrRxmRhFRD7muvW86WQpD3
knxMuHeAROruxMEsQQVjTzSLbXN91dZVxFMO116unTYgJaTxfv5NIPbcgphrNXsC
EX5TcZcoVTFL5cFap8vbdL3k24Er2bMfLG7Tz4METpU9ZTYLGooRwaWHiURHYi3U
6fMCgYAOP4OCHeb+jAlyvgOV+LGDc/r99ZtE34rnuPCJ/K8TjkqZ9y/j4lqF6zFU
kEUN+7rDB5RbObtiUSaryR74nL3H1dx9SZdBdpg+TaVdYw5tAsQKDHpUuyE2U/pt
Fnn/7OyFj9PMSHrS/6Pg4J2Ny+g7rbXOJcwgrwE8UyOYO3allg==
-----END RSA PRIVATE KEY-----
```

Once again.... WTF!! So a large part of me still thinks this fake, but now I start thinking maybe (looking at the folder structure) someone has compromised a site and has moved the juicy files onto a holding site. So I dig a bit more:



route name
as name
ip location
information age

Base	Record	Pref	Name	IP-number	Reverse	Route	Autonomous System
ffgbeach.com	a			209.68.17.43 Pittsburgh, PA, United States	fashionfantasygame.com	209.68.0.0/18 Creating route for E-xpedient	AS7859
	ns		ns7.ns0.com	2607:f440::d85c:97fe		2607:f440::/32	
				216.92.151.254 Pittsburgh, PA, United States		216.92.0.0/16 Creating route for E-xpedient	
			ns2.quickserve.com	66.39.65.254 Pittsburgh, PA, United States		66.39.0.0/17 Creating route for E-xpedient	
	mx	50	qs2237.pair.com	216.92.127.17 Pittsburgh, PA, United States		216.92.0.0/16 Creating route for E-xpedient	

com ns0.com pair.com quickserve.com

Ffgbeach.com is a domain controlled by two domain name servers at ns0.com and quickserve.com having a total of three IP numbers. All three of them are on different IP networks. Incoming mail for ffgbeach.com is handled by one mail server at pair.com. Ffgbeach.com has one IP number (209.68.17.43), but the reverse is fashionfantasygame.com.

Fashionfantasygame.com and www.fashionfantasygame.com point to the same IP. Windmillmarket.net, jl-digital-image.com, mooseofthemonth.com, versatex.mx, officeofdevelopment.com and at least 176 other hosts share name servers with this domain. Qs2237.pair.com share mail servers with this domain.

All together now.... W. T. F. !! So I was wrong. "fashionfantasygame.com" is very much linked to "ffgbeach.com". So what can I find about "fashionfantasygame.com"? Lets start with the whois/dns information:

Fashionfantasygame.com is a domain controlled by two domain name servers at hover.com. Both are on different IP networks. Incoming mail for fashionfantasygame.com is handled by one mail server at google.com having a total of 16 IP numbers. Some of them are on the same IP network. Fashionfantasygame.com has one IP number (209.68.17.43), which also has a corresponding reverse pointer.

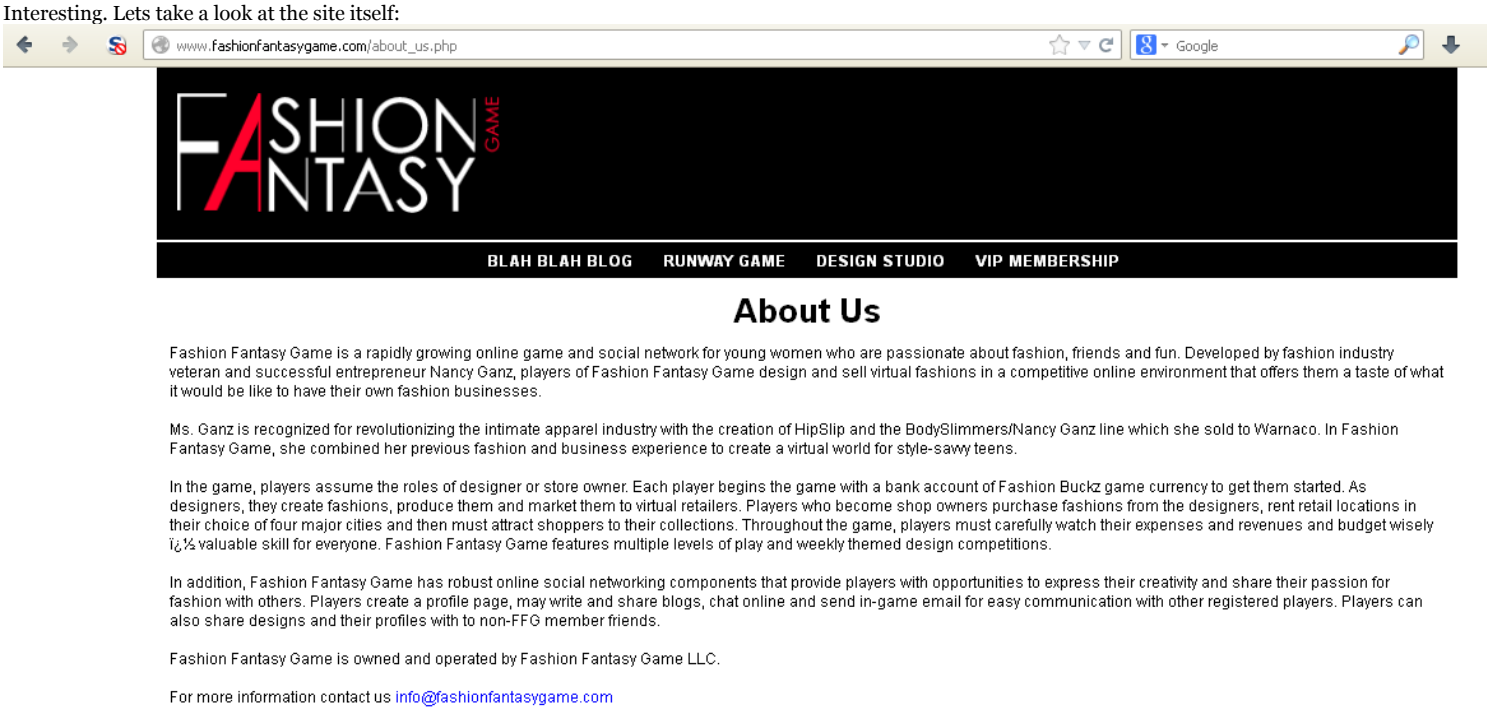
Www.fashionfantasygame.com point to the same IP. Vailguy.com, westwoodiiihoa.org, nanodust.info, ciudad1.biz, jonathanmounce.com and at least 91 other hosts share name servers with this domain. Onlinelearningdemos.com, thisisafrica.me economicessentials.com, jordiamela.com, kaftor.org and at least 94 other hosts share mail servers with this domain. Jewishoutreachnetwork.com, pachet.com, pidster.com, altervista.it, warrenandjan.com and at least seven other hosts share mail servers under another name with this domain. Fashionfantasygame.net.emailmx.com are similar domain names.

route name
as name
ip location
information age

Base	Record	Pref	Name	IP-number	Reverse	Route	Autonomous System
fashionfantasygame.com	a			209.68.17.43 Pittsburgh, PA, United States		209.68.0.0/18 Creating route for E-xpedient	AS7859
	ns		ns1.hover.com	216.40.47.26 Toronto, ON, Canada		216.40.32.0/20 VeriSign Customer Route	AS15348 TUCOWS
			ns2.hover.com	64.98.148.13 Toronto, ON, Canada	- ns2.hughesnetwebservices.com	64.98.0.0/16 TUCOWS-ASH-BLK1.9	AS32491 TUCOWS-3
	mx	10	aspmx.l.google.com	2607:f8b0:4002:c04::1a	ye-in-x1a.1e100.net	2607:f8b0::/32	AS15169 Google
				2607:f8b0:400d:c01::1a	qc-in-x1a.1e100.net -		
				2607:f8b0:400d:c02::1b	qe-in-x1b.1e100.net		
				2607:f8b0:400e:c00::1b	da-in-x1b.1e100.net		
				2607:f8b0:400e:c01::1b	pb-in-x1b.1e100.net		
				2607:f8b0:400e:c02::1a	?		
				2607:f8b0:400e:c03::1a	pa-in-x1a.1e100.net		
				2a00:1450:400c:c03::1a	we-in-x1a.1e100.net	2a00:1450::/32	
				74.125.25.27 Mountain View, CA, United States	pa-in-f27.1e100.net	74.125.25.0/24 Google	
				74.125.129.27 Mountain View, CA, United States	?	74.125.129.0/24 Google	
				74.125.137.27 Mountain View, CA, United States	yh-in-f27.1e100.net	74.125.137.0/24 Google	
				74.125.141.27 Mountain View, CA, United States	da-in-f27.1e100.net	74.125.141.0/24 Google	
				173.194.67.27 Mountain View, CA, United States	wi-in-f27.1e100.net	173.194.67.0/24 Google	
				173.194.74.26 Mountain View, CA, United States	qe-in-f26.1e100.net	173.194.74.0/24 Google	
				173.194.76.26 Mountain View, CA, United States	qo-in-f26.1e100.net	173.194.76.0/24 Google	
				173.194.76.27 Mountain View, CA, United States	qo-in-f27.1e100.net		

com google.com l.google.com net 1e100.net hover.com hughesnetwebservices.com

Interesting. Lets take a look at the site itself:



Read that very carefully. Look at the audience of this site. Now lets look at the privacy policy:

5. Your/Your Parent's Changes

This Web site gives users options for changing and modifying information previously provided. If you are a registered visitor, you are welcome to view, change or delete your registration information at any time, or to update the contact information we have for you or to inform us that you do not want to receive new product or other information from us. Simply go to the Parent Portal on this Web site and follow the directions.

Kids under 13 cannot change registration information. Only their parent or guardian can do that. If you wish to review, correct or delete information that we may have about you or your child, or wish to inform us that you do not permit further collection or use of your child's information, please contact us at the following address:

Fashion Fantasy Game, R Lilly Tuckerwear, 120 East End Avenue, New York, NY 10028; info@rlillytuckerwear.com.

Or go to the Parent Portal.

6. Security

We have implemented safeguards to maintain data security and correctly use the information we collect online. The hosting site sits behind a Cisco PIX Firewall. The database is protected with username/password and firewall rules for access. Because we are sensitive to visitors' security concerns about the use of credit cards to purchase products over the Internet, for online orders we use a technology that encrypts credit card data while information is being transmitted over the Internet, provided that the visitor's browser supports the Secure Socket Layer (SSL) protocol.

Again, read section 6 well. Credit card information? Allow me to explain to "fashionfantasygame.com" a technical term that is appropriate for describing your security measures and privacy policy, it's "BULLSHIT". This is a site aimed at "young ladies" where paypal and credit cards are used, where social interaction is encouraged, and this is the level of care you think is appropriate!! That sql file has been known to the less savoury parts of the internet for at least the last 4 months! But...take a deep breath... is it that bad? In a word, yes. The hashes are unsalted md5 hashes. I took a quick run through them and I cracked over 80%. To be exact at this exact moment as I write this (and it is still running), I have 68245 hashes left. I have taken a quick look through the passwords as well, there was very poor password enforcement if anything - the password "123456" is used thousands of times.

So lets recap:
We have a site ("fashionfantasygame.com") that deals with credit card and paypal data, is aimed at young ladies and has had a sql dump of their users publicly available to the internet for at least 4 months. They did not salt the passwords. They did not enforce good password standards. I cannot express the amount of "FAIL" this encompasses.

When I first started looking at this, I thought "someone else must have written on this. someone else must have mentioned this." Well, I could not find anything. If someone did, then good on you. But what about now? My personal suggestions are:
1) All users of "fashionfantasygame.com" past and present - please, please change your passwords. All of them. Check your online accounts to make sure nothing has been tampered with.
2) All users of "fashionfantasygame.com" present - quit "fashionfantasygame.com". Or if you feel like giving them a chance in spite of their documented lack of care, then raise your voice and get them to notify their users and change their process and setup. Get them to take measurable steps to earn your trust back.
3) "fashionfantasygame.com" - ....I actually have no words. Or to be more exact, I have no polite words for this level of due care with the data of minors. Find someone who knows what the hell they are doing and let them do what they need to.

Ok, I have had enough ranting, go and be good.