

Forum:[Hack Forums](#)

Thread: [Huge vulnerability found in AllCrypt.com](#)

Abraham Lincoln - January 18, 2015, 7:21 pm

EDIT: They still haven't fixed the issue. 3 months and the site is still vulnerable. I'd recommend you pull out all your coins from them.

So back in early December I was messing around on AllCrypt.com, working on some automation methods to save myself time, and I came across a huge vulnerability in their system. Essentially it would allow me to withdraw as much of any coin as I wanted from their hot wallet. I would estimate that to easily be in the 5+ digits USD wise.

I immediately contacted their support and reported the issue to them. They respond within a few hours and I communicated with them closely for the next day giving them information. In a few days they had it patched up. There was just one catch that surprised me, they locked my AllCrypt account, put my coin balances on hold, and stopped responding to my support inquiries. I messaged them asking for my BTC back.

39 days and 4 messages later, they finally responded with this: (I've edited it to remove any hints as to what the vulnerability was)

Quote:It took us forever to clean up the mess. Don't get snippy with "and I want [my BTC and OMC] back" - you were violating the terms and conditions of the site by [what you did]. By the terms you agreed to by your usage of the site, we have every right to leave it on lockdown. So you'll excuse us if we have other matters to attend to and repairing your account isn't top priority.

The balance has been restored. We added safeguards to protect against that sort of thing again. Don't go [doing what you did]. They will be flagged in the future and might result in an auto-IP ban from the intrusion detection system.

It seemed quite odd to me that they would treat someone who found, did not abuse, and reported such a major bug in this manner. To make it even more unusual a couple of months before I had been messing around and found a mysql bug in their system. Even though it was a tiny, completely safe bug, they gave me a decent bounty and thanked me for finding it. But now it seems everything has changed and suddenly I'm on the wrong moral ground. What is up with that?

Now, let me clarify some things:

I was in violation of their TOS. They had every right to do what they did. I do not deserve anything, no do I expect to be given a reward.

I am not complaining about the fact that I didn't receive a bounty.

I am simply posting this as I thought it would be fun to share.

No, I'm not going to give any details of this attack out. Don't bother asking.

tl;dr: I could have stolen a bunch of the money from AllCrypt.com, but reported the bug instead. They then blocked me from the system and ignored me, which seemed odd to me, considering my actions.

Doctor Blue - January 18, 2015, 7:26 pm

This is one of those cases where you wish they'd get mad before you actually did it. Then you'd probably just have publicized it ^^

Weeping Angel - January 18, 2015, 7:59 pm

Well it seems quite odd that they would punish you for telling them an issue to fix.

My old school did crap like that. Like.. if you found some kind of weird method that someone could use to get into the teacher's files or something and immediately went and told them, they'd get you put in detention for days for "hacking".

Chief - January 18, 2015, 8:11 pm

That's fucked on their part. You could've easily stolen a lot of money, but you didn't.

FRANKIE - January 18, 2015, 8:13 pm

They should be a bit more understanding and compassionate with you. You literally had access to their money and didn't take it.

They sound like (judging from the response) arrogant pricks.

Also: Congrats on finding the exploit.

Illuminati? - January 18, 2015, 8:15 pm

That's what you get for helping someone nowadays.

You should have just withdrew a lot of money and bailed.

This is beyond fucked up.

Supreme??????? - January 18, 2015, 8:16 pm

Eh, this is one of the outcomes for doing a good deed. At least you reported the vulnerability.

webdev77 - January 18, 2015, 8:16 pm

I think I'm done with allcrypt for good. Their site hasn't improved any since I started using it and it's kind of unreliable.

VRUMM - January 18, 2015, 8:16 pm

Seems odd they would do that, but something tells me someone took advantage of the exploit you found already.

(Jan 18, 2015 09:16 PM)webdev77 Wrote: [\[CITE\]](#) I think I'm done with allcrypt for good. Their site hasn't improved any since I started using it and it's kind of unreliable.

I couldn't find any reliable alt-coins exchange except for btc-e

NiktoKan - January 18, 2015, 8:29 pm

Locking members' account who warn them is a bad practice. Who will help them next time?

Few months back there is a white hat hacker who exploit a vulnerable exchange but return back money later on. Maybe next time you can do the same way.

Since AllCrypt.com is not good, maybe we should find other exchange for OMC.

Abraham Lincoln - January 18, 2015, 8:51 pm

(Jan 18, 2015 09:29 PM)NiktoKan Wrote: [\[CITE\]](#) Locking members' account who warn them is a bad practice. Who will help them next time?

Few months back there is a white hat hacker who exploit a vulnerable exchange but return back money later on. Maybe next time you can do the same way.

Since AllCrypt.com is not good, maybe we should find other exchange for OMC.

I would really like to get it on Cryptsy.com. From what I've heard it's a pretty good exchange for altcoins.

Raoul Duke - January 18, 2015, 9:00 pm

There is one thing I hate from Allcrypt: withdrawals fee change very often without any warnings from them. Sometimes my BTC's get stuck because I'm under the "minimum withdrawal amount" and the next day it's ok ...

Fudster - January 18, 2015, 9:05 pm

Thats sooo stupid. Why would they restrict your account and then respond to you like that? They should be thankful that you didn't take their \$\$\$\$.

Also about the other exchange comment.

<https://bleutrade.com/> Maybe?

adampelletgun - January 18, 2015, 10:30 pm

That's a dick move by them.

Congrats on finding the vuln though.

Vigor - January 18, 2015, 10:31 pm

Dude seriously? Fucking post it. Don't let people treat you like your their little bitch. Show them that YOU'RE THE ONE IN CONTROL.

B?ue - January 18, 2015, 10:34 pm

Thats so fucking shitty of them, Personally I'd be planning an attack right now.

Same thing happened with my school I found a network exploit, showed them, They patched it and they gave me a detention.

So I did a bigger one a fucked it up quite bad and got in very serious shit.

That fucking sucks man, Can't believe you lost your stuff.

Fuck them, assholes.

Abraham Lincoln - January 18, 2015, 10:41 pm

(Jan 18, 2015 11:31 PM)Scoundrel Wrote: [\[CITE\]](#) Dude seriously? Fucking post it. Don't let people treat you like your their little bitch. Show them that YOU'RE THE ONE IN CONTROL.

It has already been patched. Posting it wouldn't necessarily cause any damage to them, which isn't really my goal anyways.

Vigor - January 18, 2015, 10:42 pm

(Jan 18, 2015 11:41 PM)Abraham Lincoln Wrote: [\[CITE\]](#) It has already been patched. Posting it wouldn't necessarily cause any damage to them, which isn't really my goal anyways.

If it's been patched then post it still. What harm could it do?

Abraham Lincoln - January 18, 2015, 10:42 pm

(Jan 18, 2015 11:34 PM)BlueLights Wrote: [\[CITE\]](#) That fucking sucks man, Can't believe you lost your stuff.

I haven't lost anything. They eventually returned my BTC and OMC.

Jason™ - January 18, 2015, 10:43 pm

The team over at AllCrypt seem a bit salty on occasions.

Abraham Lincoln - January 18, 2015, 10:44 pm

(Jan 18, 2015 11:42 PM)Scoundrel Wrote: [\[CITE\]](#) If it's been patched then post it still. What harm could it do?

It could result in other glitches being found and abused. And Tbh I don't know if they even fully patched it. From what they said it sounds like they just stuck a bandaid on it.

Vigor - January 18, 2015, 10:46 pm

(Jan 18, 2015 11:44 PM)Abraham Lincoln Wrote: [\[CITE\]](#) It could result in other glitches being found and abused. And Tbh I don't know if they even fully patched it. From what they said it sounds like they just stuck a bandaid on it.

Exactly. So post it. Those guys fucked you over. You owe them NOTHING. They owe you. You know what to do when people don't pay up.

Poutine - January 18, 2015, 10:50 pm

(Jan 18, 2015 11:46 PM)Scoundrel Wrote: [\[CITE\]](#) Exactly. So post it. Those guys fucked you over. You owe them NOTHING. They owe you. You know what to do when people don't pay up.

Thats because he's lying.

He clearly found nothing.

Vigor - January 18, 2015, 10:50 pm

(Jan 18, 2015 11:50 PM)Poutine Wrote: [\[CITE\]](#) Thats because he's lying.

He clearly found nothing.

Tbh that must be the case. Doesn't make any sense why he wouldn't post it.

Compl3xx - January 18, 2015, 11:06 pm

You should of just fucked them over.

Cyrus - January 18, 2015, 11:10 pm

That's why if I ever found a bug like that in some site, I wouldn't report it, I would get rich.

No companies ever seem to appreciate honest and decent people whom help them out.

M3llerite - January 18, 2015, 11:28 pm

It's very nice to be of good to others do not let their Tos policy let you down

I raise my hat for good pple around the globe....

They are given instances to the insurance coy to be nabbed and we should all beware It may lead going down

because the digital currency coy(s) are full of that

DamienVC - January 19, 2015, 2:18 am

You should have made an eBook and sold it for \$100 per copy ? ?

Azraelstear - January 19, 2015, 2:40 am

OP: try to find new vuln and stole everything and let them eat their own shit if they are this much stupid.

mti1993 - January 19, 2015, 2:57 am

shit , they didn't even thank you
we must have another exchange site for OMC

Gook - January 19, 2015, 4:14 am

next time report it to me, ill do the job 50/50 for you

Doctor Blue - January 19, 2015, 4:23 am

(Jan 19, 2015 12:10 AM)Cyrus Wrote: [\[CITE\]](#) That's why if I ever found a bug like that in some site, I wouldn't report it, I would get rich.

No companies ever seem to appreciate honest and decent people whom help them out.

I found one. Although it's very small and the exploit only allowed me to steal baby books.

Most others get cranky indeed. I don't disclose bugs like those anymore, the companies can get crazy mad. Furthermore it's not even legal to pentest a website without permission, not in Denmark anyway.

Algo-rhythm - January 19, 2015, 4:37 am

Well mate, you proved that you are a genius.

And I think you really are one.

Glad that we have people like you on these forums. Take a bow man! ?

Moneybookers - January 19, 2015, 4:48 am

(Jan 19, 2015 05:14 AM)Gook Wrote: [\[CITE\]](#) next time report it to me, ill do the job 50/50 for you
Indeed, you get threatened like an idiot for helping them basicly.

Would have done it for less.

doodie - January 19, 2015, 7:05 am

I would report this to Bitcointalk and other BTC related forums, copy/pasting this will take you one minute and it'll cost them alot.

And they deserve to suffer as they are awful in both business and human approach

Mons - January 19, 2015, 7:15 am

What terms did you violate this time that you didn't violate the previous time finding and reporting a vulnerability.

Aceman - January 19, 2015, 9:11 am

I've had problem with AllCrypt's support in the past as well. The employees I had dealt with in support were quite rude and acted as if I was the problem when I was simply trying to solve an issue on their end. Guess that's what I get for asking them to update their wallet's nodes so that their wallets aren't offline for 5 hours. ?

Yoshikage Kira - January 19, 2015, 9:18 am

That's quite rude of them, i'd report their behavior on bitcointalk.

webdev77 - January 19, 2015, 10:36 am

(Jan 18, 2015 09:16 PM)Sh1eld Wrote: [\[CITE\]](#) Seems odd they would do that, but something tells me someone took advantage of the exploit you found already.

I couldn't find any reliable alt-coins exchange except for btc-e
I use BTC-e and haven't had any trouble, so I will continue to use them for my small trades.

Raoul Duke - January 19, 2015, 1:54 pm

(Jan 19, 2015 10:11 AM)Aceman Wrote: [\[CITE\]](#) I've had problem with AllCrypt's support in the past as well. The employees I had dealt with in support were quite rude and acted as if I was the problem when I was simply trying to solve an issue on their end. Guess that's what I get for asking them to update their wallet's nodes so that their wallets aren't offline for 5 hours. ?

That's the problem with the person who have a big "ego". When you try to help them they think you attack them. Because they can't have done something wrong, they are the one's in charge. Sometimes they need a lesson from grey hat hacker's... keep the money in hostage disclose the vuln and send it back once they patched it... but acting like that make you a criminal.

420 Blaze It - January 19, 2015, 2:16 pm

Interesting, AllCrypt is glitchy anyways and the addresses are always down!

Forezza - January 20, 2015, 2:28 am

Companies don't care if you report vulnerabilities to them. Unless they ask you through a disclosure program, they act like you just killed their dog. I can sort of understand it coming from the company because if someone came up to you and said "I've found a major security hole in your company and it could lead to massive losses", they generally won't be very happy about it. Companies like this think that the bugs will remain un-noticed but in reality, they won't. People with malicious purposes will find them and then they'll lose all their money.

I was in a situation when I was a bit younger where I enjoyed finding holes in large companies and reporting it to them because I thought I was doing "good". A few companies (mainly the smaller ones) were happy and noted that they would fix the issue. There was this large company once who I better not name but they absolutely lost it when I told them they had a serious vulnerability which could lead to all customer details being stolen. I said it in a way that I had just come across it and I was trying to be a good citizen and report it. They (looked like some random from the IT department) sent a message back telling me that what I was doing was totally illegal and that they had reported me to the authorities (I just laughed it off as I was sitting on an RDP -> VPN -> TOR so I wasn't too worried at the time) but the random alias email that I emailed from was disabled later that week. The most entertaining part was that they didn't even fix the security hole for 2 months after it had been reported. Quite sad for a company making millions in revenue p/week.

Most companies don't take security seriously, that's their mistake. Next time just report it under some random alias.

Allcrypt is probably one of the worst exchanges I've ever seen. They use basic PHP with very little security by the looks of it. They seem quite cocky reading <https://www.allcrypt.com/blog/2014/03/post-hack-update-and-statement/> and make sure you look at Code White hat hackers who want to help find holes? Don't. You'll be banned with the very first hit you make that doesn't fit normal AllCrypt.com usage patterns. Again, I won't say we're hack proof, but we're 10x as stringent with security now.

Sudsy - January 20, 2015, 5:21 am

Damn I'm scum I guess bc I wouldn't have reported that lmao

NoMercy - January 20, 2015, 7:17 am

You should have done what that white hat hacker did for BTC before. Took all the money and refuse to give it back until they fix the error.

FaberCastell - January 20, 2015, 7:30 am

People don't appreciate shit nowadays, should have taken everything you could.

DamienVC - January 20, 2015, 7:56 am

AllCrypt is just small time skid who pretend to act like big time companies.

They're hardly worth 30k\$ af

Abraham Lincoln - February 27, 2015, 9:18 am

Well, I just tested again today, and the site is still vulnerable to this exploit. I've also found multiple other exploits in their site that could easily result in the emptying of all their coin wallets.

I'd highly recommend that either not use AllCrypt at all, or if you do, only keep small amounts of money in your balance and withdraw them as soon as you've made your trade.

And no, I'm not selling any of these exploits.

Smexy - February 27, 2015, 9:22 am

(Feb 27, 2015 10:18 AM) Abraham Lincoln Wrote: [\[CITE\]](#) Well, I just tested again today, and the site is still vulnerable to this exploit.

I'd highly recommend that either not use AllCrypt at all, or if you do, only keep small amounts of money in your balance and withdraw them as soon as you've made your trade.

Would you sell this exploit? I mean they fucked you over, time to hurt em.

Handsome Banana - February 27, 2015, 9:24 am

(Feb 27, 2015 10:18 AM) Abraham Lincoln Wrote: [\[CITE\]](#) Well, I just tested again today, and the site is still vulnerable to this exploit.

I'd highly recommend that either not use AllCrypt at all, or if you do, only keep small amounts of money in your balance and withdraw them as soon as you've made your trade.

You should abuse it. Show that the money isn't safe and wait for them to sort it out if they want the BTC back. Or just keep it, their loss. You tried to help once and they didn't listen so instead of someone else finding it and taking it you should. ? ? ?

HIGH PAID FELLA - February 27, 2015, 9:26 am

Oh dude, you have really, too much morals, holy fuck.

Lord.Baltimore - February 27, 2015, 9:29 am

The design of the site is a very shit.

For an exchange service, the objectif is to attract the client, with a design like Allcrypt, it's not a succes.

Shrooms - February 27, 2015, 9:29 am

Fuck that dude, if I was in your situation and I knew they'd respond like that AllCrypt would have been bankrupt over night and I'd be chilling in my private jet on my way to Jamaica or somewhere hot with a fat joint in my mouth.

hiphopherooin - February 27, 2015, 9:36 am

Thanks for the heads up about the site Abraham, Moved my coins.

Aceman - February 27, 2015, 1:08 pm

(Feb 27, 2015 10:24 AM) Doing it Wrote: [\[CITE\]](#) You should abuse it. Show that the money isn't safe and wait for them to sort it out if they want the BTC back. Or just keep it, their loss. You tried to help

once and they didn't listen so instead of someone else finding it and taking it you should. ? ? ?Would be kind of awkward if a member of the OMC team performed a 51%, wouldn't it?

HIGH PAID FELLA - February 27, 2015, 1:09 pm

(Feb 27, 2015 02:08 PM)Aceman Wrote: [\[CITE\]](#) Would be kind of awkward if a member of the OMC team performed a 51%, wouldn't it?

Well, if he doesn't let people know it's him he's alright.
Anyway, I would get all those coins if I could.

Abraham Lincoln - February 27, 2015, 1:21 pm

(Feb 27, 2015 02:08 PM)Aceman Wrote: [\[CITE\]](#) Would be kind of awkward if a member of the OMC team performed a 51%, wouldn't it?

I'm not talking about a 51% attack, although that is another one of their weaknesses.

I've found some other bugs that would allow me to empty all of their wallets, not just OMC.

Also, I have performed a 51% attack on Omnicoin before :)

HIGH PAID FELLA - February 27, 2015, 1:22 pm

(Feb 27, 2015 02:21 PM)Abraham Lincoln Wrote: [\[CITE\]](#) I'm not talking about a 51% attack, although that is another one of their weaknesses.

I've found some other bugs that would allow me to empty all of their wallets, not just OMC.

Also, I have performed a 51% attack on Omnicoin before :)

Would you be interessted in selling the exploit? People on the deepweb like this. I still don't get why you don't abuse it.

P3TE - February 27, 2015, 1:23 pm

You should of just rekt them and taught them a lesson.

Abraham Lincoln - February 27, 2015, 1:31 pm

(Feb 27, 2015 10:24 AM)Doing it Wrote: [\[CITE\]](#) You should abuse it. Show that the money isn't safe and wait for them to sort it out if they want the BTC back. Or just keep it, their loss. You tried to help once and they didn't listen so instead of someone else finding it and taking it you should. ? ? ?

I'm not going to abuse it. I've issued a warning and I hope all users stop using the site.

Also now that I've posted a thread about it, it's pretty obvious I know about it. If an attack occurred I'd be a prime suspect on their list.

(Feb 27, 2015 02:22 PM)Asterea Wrote: [\[CITE\]](#) Would you be interessted in selling the exploit? People on the deepweb like this. I still don't get why you don't abuse it.

No, I'm not going to sell the exploit.

Mr.Peanut - February 27, 2015, 1:33 pm

If you wouldn't take the money, what i'd rather do is..

1. Take everything from the site
2. Make a new site letting users claim every cent back with proof of their account

What that does in the process is, make altcrypt look HORRIBLE, you seem like a hero, and you get to keep coins that aren't claimed in say 6 months. haha

Genicus - February 27, 2015, 1:36 pm

Morale aside , shoulda taken it all. Probably haven't even fixed the big

Abraham Lincoln - February 27, 2015, 1:41 pm

(Feb 27, 2015 02:36 PM)Genicus Wrote: [\[CITE\]](#) Morale aside , shoulda taken it all. Probably haven't even fixed the big

Nope, they haven't. It's been almost 3 months. So far all they've done is just ignore me and insult me.

(Feb 27, 2015 02:33 PM)Mr.Peanut Wrote: [\[CITE\]](#) If you wouldn't take the money, what i'd rather do is..

1. Take everything from the site
2. Make a new site letting users claim every cent back with proof of their account

What that does in the process is, make altcrypt look HORRIBLE, you seem like a hero, and you get to keep coins that aren't claimed in say 6 months. haha

Well, I would have no way of getting the user database without working with AllCrypt, which I'm sure they wouldn't be interested in doing.

Mix - February 27, 2015, 1:55 pm

They really over did it on this one as you did violate there T.o.S BUT you did the right thing and told them what was wrong and helped fix the problem before it could have gone into the wrong hands now yes i understand that they are worried that you could of went out and sold this method and shit but u didnt u stayed loyal to your keepings and thoughts and did the right thing now then they come out like this is kinda right and wrong at the same time meaning they did the right and the wrong thing as you had no harm to them they should have made you number one priority due to everyone know that customers come first out of everything its how business works. But i guess im wrong cos they dont see us that way.... im ashamed of them tbh