

Forum:[Hack Forums](#)

Thread: [Bounties?](#)

Intellectual - March 31, 2013, 3:28 am

Ok so I have a site that is completely exploitable. I got a 7100 email/pass list, and I think there might be some cc info ect. How do I go about telling them to fix it and make money? I dont feel like getting jailed for extortion but I dont want to hand over the data for free either. Thoughts or ideas on what to say/do?

So I sent this

"I have managed to breach your site while doing a pentest (penetration testing). I was wondering if there might be a reward for exposing your flaws and keeping your consumers safe? Everything, I repeat, everything is exploitable. I could have defaced your website and stolen every piece of data on there, but im not that kind of guy. If you need proof I can provide a screenshot of me inside of your website. A large reward would be appreciated if I told you where the error was at and how to avoid this."

amus3d - March 31, 2013, 3:33 am

You've already stolen the data? I'm sure they will not give you a 'reward' for stealing their users' credit card info, usernames, emails, passwords and shit.

Good job.

Intellectual - March 31, 2013, 3:35 am

Well, I took the login/pwd list so I can show as proof that they have a vulnerability.. But no I havent taken any cc, bank info, address, phone, zip ect...

??????? - March 31, 2013, 3:35 am

First of all Black Hat activity not allowed here, not even talking about.

And from my opinion there's 2 ways to make money in this situation, first inform them "That you while you were doing Pen-testing you found vulnerability etc...."

Or the other way pm me for it.

crossera - March 31, 2013, 3:36 am

(Mar 31, 2013 03:35 AM)Intellectual Wrote: [\[CITE\]](#) Well, I took the login/pwd list so I can show as proof that they have a vulnerability.. But no I haven't taken any cc, bank info, address, phone, zip ect...

They wouldn't know he has the information amu3ed ..

just tell them that they have sql vulnerability and you didn't exploited it.

And ask them if there is reward so is it worth to report it

Intellectual - March 31, 2013, 3:37 am

(Mar 31, 2013 03:36 AM)crossera Wrote: [\[CITE\]](#) They wouldn't know he has the information amu3ed

..

just tell them that they have sql vulnerability and you didn't exploited it.

And ask them if there is reward so is it worth to report it

Do I send them the proof that there is an exploit? Or do I just say you have one is there a reward?

amus3d - March 31, 2013, 3:43 am

(Mar 31, 2013 03:36 AM)crossera Wrote: [\[CITE\]](#) They wouldn't know he has the information amu3ed

..
just tell them that they have sql vulnerability and you didn't exploited it.
And ask them if there is reward so is it worth to report it
Implying that there are no logs defaultly stored.

If the vulnerability was SQLi (or whatever) then it wouldn't be hard to suss out what information was taken at all, by looking through the logs.

But sure.

(I love the irony in OP's user name ;3).

-?Divine- - March 31, 2013, 3:53 am

(Mar 31, 2013 03:36 AM)crossera Wrote: [\[CITE\]](#) They wouldn't know he has the information amu3ed

..
just tell them that they have sql vulnerability and you didn't exploited it.
And ask them if there is reward so is it worth to report it
Yea, because going through the logs when they see someone threatening is something they surely won't do.

(Mar 31, 2013 03:43 AM)amus3d Wrote: [\[CITE\]](#) Implying that there are no logs defaultly stored.

If the vulnerability was SQLi (or whatever) then it wouldn't be hard to suss out what information was taken at all, by looking through the logs.

Exactly. They can see exactly how he accomplished that, no need for PoC.

(Mar 31, 2013 03:35 AM)??????? Wrote: [\[CITE\]](#) First of all Black Hat activity not allowed here, not even talking about.

And from my opinion there's 2 ways to make money in this situation, first inform them "That you while you were doing Pen-testing you found vulnerability etc...."

Or the other way pm me for it.

You are making this site look pathetic.

Intellectual - March 31, 2013, 3:59 am

Ok so long story short, what do I do? I have 7100 login/passwords, thats all the data that I took. What do I do with it? Do I contact them and say "Hey I found a loophole in your system, is there a reward for telling you? Heres some proof that im not lying..."

Phizo - March 31, 2013, 3:59 am

(Mar 31, 2013 03:28 AM)Intellectual Wrote: [\[CITE\]](#) Ok so I have a site that is completely exploitable. I got a 7100 email/pass list, and I think there might be some cc info ect. How do I go about telling them to fix it and make money? I dont feel like getting jailed for extortion but I dont want to hand over the data for free either. Thoughts or ideas on what to say/do?

You may have voided your request for a reward, unless you be slightly unethical about it by neglecting to mention the fact you have access to said data.

(Mar 31, 2013 03:35 AM)??????? Wrote: [\[CITE\]](#) First of all Black Hat activity not allowed here, not even talking about.

And from my opinion there's 2 ways to make money in this situation, first inform them "That you while you were doing Pen-testing you found vulnerability etc...."

Or the other way pm me for it.

Educate yourself by reading the rules; this doesn't count as "Black Hat activity."

We recommend you take the time to read the [HF Help Documents](#) section. The answer to your questions should be contained in there.

Intellectual - March 31, 2013, 4:40 am

updated with what I sent, thoughts?

amus3d - March 31, 2013, 4:43 am

(Mar 31, 2013 03:28 AM)Intellectual Wrote: [\[CITE\]](#) "I have managed to breach your site while doing a pentest (penetration testing). I was wondering if there might be a reward for exposing your flaws and keeping your consumers safe? Everything, I repeat, everything is exploitable. I could have defaced your website and stolen every piece of data on there, but im not that kind of guy. If you need proof I can provide a screenshot of me inside of your website. A large reward would be appreciated if I told you where the error was at and how to avoid this."

That makes you look like you are under 14. I honestly do not believe they will take you seriously, I can barely stop laughing.

Intellectual - March 31, 2013, 4:44 am

(Mar 31, 2013 04:43 AM)amus3d Wrote: [\[CITE\]](#) That makes you look like you are under 14. I honestly do not believe they will take you seriously, I can barely stop laughing.

Lol? Write what you would have emailed them...

-?Divine- - March 31, 2013, 4:45 am

(Mar 31, 2013 04:44 AM)Intellectual Wrote: [\[CITE\]](#) Lol? Write what you would have emailed them...
"Good evening.

Recently approaching your website I come to realize that there is a very explicit vulnerability within it. As a penetration tester, my duty is to keep the websites secure and I'm here to help you. Not fixing this vulnerability leaves you open to malicious hackers and puts your sites security as a risk.

If you want to keep your website safe, reply with what I'd get from this.
Good luck. -Penetration Tester" - Haxor.

amus3d - March 31, 2013, 4:45 am

(Mar 31, 2013 04:44 AM)Intellectual Wrote: [\[CITE\]](#) Lol? Write what you would have emailed them...
OKAY.

Code [12:44:59] HaxOr - #Cut4Dyme: What about
[12:45:01] HaxOr - #Cut4Dyme: Good evening.

Recently approaching your website I come to realize that there is a very explicit vulnerability within it. As a penetration tester, my duty is to keep the websites secure and I'm here to help you. Not fixing this vulnerability leaves you open to malicious hackers and puts your sites security as a risk.

If you want to keep your website safe, reply with what I'd get from this.
Good luck. -Penetration Tester
That.

Intellectual - March 31, 2013, 4:49 am

(Mar 31, 2013 04:45 AM)amus3d Wrote: [\[CITE\]](#) OKAY.

Code [12:44:59] HaxOr - #Cut4Dyme: What about
[12:45:01] HaxOr - #Cut4Dyme: Good evening.

Recently approaching your website I come to realize that there is a very explicit vulnerability within it. As a penetration tester, my duty is to keep the websites secure and I'm here to help you. Not fixing this vulnerability leaves you open to malicious hackers and puts your sites security as a risk.

If you want to keep your website safe, reply with what I'd get from this.
Good luck. -Penetration Tester
That.
You didnt write it :P

OT: Copied, pasted and sent :D

amus3d - March 31, 2013, 4:52 am

(Mar 31, 2013 04:49 AM)Intellectual Wrote: [\[CITE\]](#) You didnt write it :P

OT: Copied, pasted and sent :D
Wait, you've sent them an email, then sent another one - about the same vulnerability?

You're not too good at this 'white hat thing' are you.

Maybe try this:

Code [12:51:54] HaxOr - #Cut4Dyme: Hello,
recently after discovering your website I came to realise that there is a very explicit vulnerability within it.
As a penetration tester, I feel it is my duty is to keep websites secure and I'm here to assist you in accomplishing that.
Failure to fix this vulnerability leaves you open to malicious hackers and puts not only your site's, but your users' security at risk as well.

If you wish to further secure your site, I'd like to know your reward policy regarding these types of vulnerability reports as soon as possible as a reply to this email.

Regards,
Penetration Tester.
or

Code Good evening.
Recently approaching your website I came to realize that there is an explicit vulnerability concerning it.
I'd like to notify you of its existance in order not to expose the website to any breaches that may occur.
Failure to fix this vulnerability leaves you open to blackhat hackers and puts not only your site's, but your users' security at risk as well.

Good luck. -Penetration Tester
I MADE THEM.

-?Divine- - March 31, 2013, 4:52 am

(Mar 31, 2013 04:49 AM)Intellectual Wrote: [\[CITE\]](#) You didnt write it :P

OT: Copied, pasted and sent :D
Wait what? You sent that as well? Imao
Send this too:
Code [13:53:05] Keeper: Good evening.
Recently approaching your website I came to realize that there is an explicit vulnerability concerning

it.

I'd like to notify you of its existence in order not to expose the website to any breaches that may occur.

Failure to fix this vulnerability leaves you open to blackhat hackers and puts not only your site's, but your users' security at risk as well.

Good luck. -Penetration Tester

-Made by me.

Intellectual - March 31, 2013, 4:55 am

3 emails sent, anybody else want me 2 send their version?

amus3d - March 31, 2013, 4:55 am

(Mar 31, 2013 04:55 AM)Intellectual Wrote: [\[CITE\]](#) 3 emails sent, anybody else want me 2 send their version?

They seriously won't take you seriously.

You may as well steal that CC info and buy some dildos to go and fuck yourself.

Intellectual - March 31, 2013, 4:56 am

(Mar 31, 2013 04:55 AM)amus3d Wrote: [\[CITE\]](#) They seriously won't take you seriously.

You may as well steal that CC info and buy some dildos to go and fuck yourself.

And when I send in proof that it is vulnerable? Should I send them the dildos as well?

amus3d - March 31, 2013, 4:57 am

(Mar 31, 2013 04:56 AM)Intellectual Wrote: [\[CITE\]](#) And when I send in proof that it is vulnerable? Should I send them the dildos as well?

No. You should also buy a gun and kill yourself. ;3

Intellectual - March 31, 2013, 4:58 am

(Mar 31, 2013 04:57 AM)amus3d Wrote: [\[CITE\]](#) No. You should also buy a gun and kill yourself. ;3
Lol, but remember, I sound like a 14 year old, and im doing 'white hat stuff' so I cant legally go out and buy a gun to do so... Next option?

Phizo - March 31, 2013, 4:59 am

(Mar 31, 2013 04:55 AM)amus3d Wrote: [\[CITE\]](#) They seriously won't take you seriously.

You may as well steal that CC info and buy some dildos to go and fuck yourself.

This is going in my signature.

Good job.

-?Divine- - March 31, 2013, 5:00 am

(Mar 31, 2013 04:58 AM)Intellectual Wrote: [\[CITE\]](#) Lol, but remember, I sound like a 14 year old, and im doing 'white hat stuff' so I cant legally go out and buy a gun to do so... Next option?

Gently penetrate the throat with the dildo until you choke on it.

Intellectual - March 31, 2013, 5:02 am

Everybody watch out for when I get that dildo! :59 second mark roughly...

[Video: <http://www.youtube.com/watch?v=ZNe1sjQxrSI>]

amus3d - March 31, 2013, 5:03 am

(Mar 31, 2013 04:58 AM)Intellectual Wrote: [\[CITE\]](#) Lol, but remember, I sound like a 14 year old, and im doing 'white hat stuff' so I cant legally go out and buy a gun to do so... Next option?

Well, obviously you would hack yourself a fake ID - via Havij.

Intellectual - March 31, 2013, 5:07 am

(Mar 31, 2013 05:03 AM)amus3d Wrote: [\[CITE\]](#) Well, obviously you would hack yourself a fake ID - via Havij.

But then I would need to learn how to use Dorks or an exploit scanner like sql poizon v1.1 and I dont know how to do that...

gomer_py - March 31, 2013, 5:57 am

I wouldn't mention anything about what you have already done.. thats will creep out most non techies..

sell me the data instead..

looping - March 31, 2013, 6:06 am

lol i cant stop laughing after reading the thread and all comments nice thread:D

Intellectual - March 31, 2013, 6:09 am

It only got slightly off topic... Somehow databases became dildos... But that's standard here apparently..

cyb3rblack - June 3, 2018, 3:49 pm

(Mar 31, 2013 03:59 AM)Intellectual Wrote: [\[CITE\]](#) Ok so long story short, what do I do? I have 7100 login/passwords, that all the data that I took. What do I do with it? Do I contact them and say "Hey I found a loophole in your system, is there a reward for telling you? Heres some proof that I'm not lying..."

I agree - you have voided your chance. If I was you, I would use an app like "File Shredder" and do a pass on that data you exfiltrated. Do it legitimately next time.

Maybe just send them an email and offer a service to them? Tell them you will offer them a free assessment, do about 2 percent (get halfway through the process) of your magic to convince them and charge them to complete the penetration test? But the current data you have, you should do a DOD pass on it IMO.

kainzerdick - June 4, 2018, 12:26 pm

I know what you feel..

Here's what I do:

When I found a bug I will email them

"hey! Do you have any bug bounty program? Like you will reward a person when he/she found a crucial bug that can compromise your system?"

If that company said no then it is up to you what will be your next move, if yes then report it and receive the reward.

Eccy - June 4, 2018, 12:28 pm

(Jun 3, 2018 03:49 PM)cyb3rblack Wrote: [\[CITE\]](#) I agree - you have voided your chance. If I was you, I would use an app like "File Shredder" and do a pass on that data you exfiltrated. Do it legitimately next time.

Maybe just send them an email and offer a service to them? Tell them you will offer them a free

assessment, do about 2 percent (get halfway through the process) of your magic to convince them and charge them to complete the penetration test? But the current data you have, you should do a DOD pass on it IMO.

I don't think he needs an answer anymore