

Forum:[Hack Forums](#)

Thread: [Are we allowed to search for vulns in HF games and report them ?](#)

device - May 19, 2020, 7:32 am

Interested in searching exploits in HF games. Am I allowed to (locally) and report them by PM to an admin ?

What would you consider an exploit in the slots game ?

Digital - May 19, 2020, 7:34 am

Yes, if you find any. Please be aware that if you trigger something it will result in a IP ban.

Omni's HF bug bounty thread: <https://hackforums.net/showthread.php?tid=5259373>

Dotexe - May 19, 2020, 7:45 am

(May 19, 2020 07:34 AM)Digital Wrote: [\[CITE\]](#) Yes, if you find any. Please be aware that if you trigger something it will result in a IP ban.

Omni's HF bug bounty thread: <https://hackforums.net/showthread.php?tid=5259373>

That's where the confusing part comes. I will obviously trigger it when im onto something. Can someone clarify it for me ?

Neeeeeeeeeeel.- - May 19, 2020, 8:25 am

(May 19, 2020 07:45 AM)Dotexe Wrote: [\[CITE\]](#) That's where the confusing part comes. I will obviously trigger it when im onto something. Can someone clarify it for me ?

Well, if they have to disable security features for you to find a bug then what's the point?

QU?CKSILVER - May 19, 2020, 8:26 am

(May 19, 2020 07:45 AM)Dotexe Wrote: [\[CITE\]](#) That's where the confusing part comes. I will obviously trigger it when im onto something. Can someone clarify it for me ?

If HF defense systems detect potential exploitation attempts, your IP will be blacklisted. Maybe try your vulnerability research using a different IP than yours, so you don't raise red flags on your own account.

Prawnster - May 19, 2020, 8:30 am

(May 19, 2020 07:45 AM)Dotexe Wrote: [\[CITE\]](#) That's where the confusing part comes. I will obviously trigger it when im onto something. Can someone clarify it for me ?

I think the only chance of an IP ban is if you are using scanning software and sending too many requests to Hackforums (based off of that thread).

I'm sure if you do get IP banned though, you can use the contact form and explain the situation to Omni that you weren't using scanning software and that you would like to be unbanned and hope he's in a good mood haha

Dotexe - May 19, 2020, 8:32 am

(May 19, 2020 08:25 AM)Neeeeeeeeeeel.- Wrote: [\[CITE\]](#) Well, if they have to disable security features for you to find a bug then what's the point?

Please read which comment I quoted, I am not saying they should disable the security features, what I am asking is what is the point of me looking at bugs, when If i do find one, i will be most likely already be banned by the system, because I was previously flagged that i ran into some spots.

(May 19, 2020 08:30 AM)Mazl Wrote: [\[CITE\]](#) I think the only chance of an IP ban is if you are using

scanning software and sending too many requests to Hackforums (based off of that thread).

I'm sure if you do get IP banned though, you can use the contact form and explain the situation to Omni that you weren't using scanning software and that you would like to be unbanned and hope he's in a good mood haha

To be honest, scanning just automates the job, you can hit specific parameter with or without that tool. I don't believe Omni will be fine with whitelist feature, because only certain amount of people will have the possibilities to look for exploits. I'm waiting to see what's his opinion on that matter though.

ven0m - May 19, 2020, 8:46 am

Hence, he recommends using the myBB Vanilla software to try out first and focus on the custom coded part of Hack forums later.

device - May 19, 2020, 10:36 am

I've managed to change some slots parameters such as game speed and betting values but nothing major here.

Xerotic - May 19, 2020, 10:48 am

(May 19, 2020 10:36 AM)Worker Wrote: [\[CITE\]](#) I've managed to change some slots parameters such as game speed and betting values but nothing major here.

Yes, you can programatically send any "bet" between 1 and 1000.

device - May 19, 2020, 10:54 am

(May 19, 2020 10:48 AM)Xerotic Wrote: [\[CITE\]](#) Yes, you can programatically send any "bet" between 1 and 1000.

I guess a copy of the game is happening in the back-end, I can't find when the second dealer's card is dealt though.

Xerotic - May 19, 2020, 11:08 am

(May 19, 2020 10:54 AM)Worker Wrote: [\[CITE\]](#) I guess a copy of the game is happening in the back-end, I can't find when the second dealer's card is dealt though.

In Blackjack, the dealer's hand is revealed after all other players have placed their wagers and it is time to settle the bets.

device - May 19, 2020, 11:12 am

(May 19, 2020 11:08 AM)Xerotic Wrote: [\[CITE\]](#) In Blackjack, the dealer's hand is revealed after all other players have placed their wagers and it is time to settle the bets.

Yes but in Blackjack the dealer is dealt his cards at the same time as everyone else and then turns his second card once players turns have been played?

In the code I can't find when the dealer is dealt his second card, and if it has a value other than "XX". Not trying to find the value here.

Just asking if in the blackjack client script the dealer is dealt a second card that has a value attributed to it other than "XX", or if that happens on the server side.

[Xerotic](#) Mind sharing where "XX" is defined ?

POLY MATH - May 19, 2020, 4:42 pm

(May 19, 2020 07:32 AM)Worker Wrote: [\[CITE\]](#) Interested in searching exploits in HF games. Am I allowed to (locally) and report them by PM to an admin ?

What would you consider an exploit in the slots game ?

Hack safely(don't DoS resources, avoid targeting members, etc. common malicious behavior) and

report responsibly. You should be fine.

Omni wouldn't be so unreasonable to ban you for hacking the slots game unless you started spreading unlimited wealth and just being malicious...you know right from wrong.

I am not sure what you mean by "locally"? HF Games are "custom"(from what I remember it is built upon some other gaming script) not some plugin that can be added in MyBB.

I haven't looked at it in forever though so everything I am saying could be wrong. I'll probably look at the new features for the API when it drops...that's about it. I have to get OSCP so my focus is on that.

-EDIT

If you are a beginner, I would recommend starting with known vulnerable projects like "Damn Vulnerable Web Application".

Xerotic normally uses safe functions and practices secure coding throughout his SDLC. Def. not for the beginner.

-EDIT

I wonder if any Race Conditions exist within the Black Jack game?...

device - May 19, 2020, 6:57 pm

(May 19, 2020 06:38 PM)xadamxk Wrote: [\[CITE\]](#) ahahaha you changed a field value in a post request... ?

You think a game will expose all of the logic without a backend?

Are you a UI Dev by chance? ?

I did say nothing major lol. Of course not, I like putting things a part and trying to understand their functioning that's all. Yes I work on front end, no need to be an ass though.

Omniscient - May 20, 2020, 8:42 am

Quote:I wonder if any Race Conditions exist within the Black Jack game?...

We solved all race conditions on HF with a special custom function. It's implemented in any areas we feel could be exploited to generate Bytes.

Quote:Omni wouldn't be so unreasonable to ban you for hacking the slots game unless you started spreading unlimited wealth and just being malicious...you know right from wrong.

That's usually how it is. If someone wants to report a bug or exploit I am fine with that.

Scanning HF for Vulns with a bot or script is likely going to get your account closed. I review logs very regularly. Normally scans will show up there.

Quote:In the code I can't find when the dealer is dealt his second card, and if it has a value other than "XX". Not trying to find the value here.

Just asking if in the blackjack client script the dealer is dealt a second card that has a value attributed to it other than "XX", or if that happens on the server side.

Xerotic Mind sharing where "XX" is defined ?

It's in the database not shown to the member until the hand is over. It is dealt correctly as in Player->Dealer->P->D. Why would the dealer card be in the JS for you to view as the client? That would be stupid.

Cooligan - May 21, 2020, 5:38 am

(May 19, 2020 08:46 AM)ven0m Wrote: [\[CITE\]](#) Hence, he recommends using the myBB Vanilla software to try out first and focus on the custom coded part of Hack forums later.

This would definitely be the best approach to this if you're not going to directly let Omni know exactly what it is you'll be doing prior to you actually doing it; which is basically impossible seeing you're looking for potential exploits.

POLY MATH - May 21, 2020, 10:10 pm

(May 21, 2020 05:38 AM)Cooligan Wrote: [\[CITE\]](#) This would definitely be the best approach to this if you're not going to directly let Omni know exactly what it is you'll be doing prior to you actually doing it; which is basically impossible seeing you're looking for potential exploits.

Yeah. I must admit that looking for vulnerabilities in MyBB may be more productive but you don't need to let Omni know your looking for vulnerabilities unless you find one.

Any scanning software like Acunetix, etc. is typical disallowed in any VDP. Directory bruteforcing should be kept to a minimum(compile a custom list) and do a slow scan.

To be frank, I wouldn't look at BlackJack. The script itself it is built upon looked pretty good. And as for Race Conditions...Omni ended that curiosity haha.

Regardless, OP. My recommendation is the same. Start with known vulnerable projects before attempting to exploit MyBB or custom software on HF. If anything, it will save you a lot of time.

If you are serious then I would look into API V2 when it drops. Xerotic isn't perfect. He will fudge up eventually lolol...I hope(For my sanity).

I must say, I am impressed with the work they have accomplished from a security engineer perspective. I'll poke the bear again in a month or so. I'll get that BlackHat award eventually.

I think I've got one reported vulnerability under my sleeve. An open redirect in HF's new Marketplace Feature...barely worth mentioning.

It'll all come together though.

P.S. Expand your searches to HF Blogs and other domains/subdomains. You may have more luck there. I've yet to do it myself so Good Luck!

-Typing from mobile. I'm not going back to fix grammatical errors. Y'all will figure it out lol

Athr - May 21, 2020, 10:30 pm

Try registering on <https://knotbb.com> or ask Xerotic to get you an account.

Its where HF is developed for the most part.

(May 19, 2020 06:38 PM)xadamxk Wrote: [\[CITE\]](#) ahahaha you changed a field value in a post request... ?

Don't be mean to him, you meanie.

device - May 22, 2020, 5:51 am

(May 21, 2020 10:30 PM)Athr Wrote: [\[CITE\]](#) Try registering on <https://knotbb.com> or ask Xerotic to get you an account.

Its where HF is developed for the most part.

Will do, thanks Athr ?