

Forum:[Hack Forums](#)

Thread: [Advice to people who enjoy pwning school related stuff](#)

?Criminal - May 5, 2016, 7:18 pm

Oracle peoplesoft is a common java based CMS hosted on some school subdomains that handles student records and grades, PS auth pages have no account lockout policy so you can attempt a bruteforce/dictionary attack, you can also attempt to access their weblogic administration panel via directory enum(default location is /console/ if the sites running weblogic), some directorys have no authorization checks bypassing the authentication page so you don't always need weblogic credentials. Theres been a few people who got caught pwning peoplesoft doing internal attacks if you dig around google, with internal access its alot easier to escalate privs you can run wireshark and view the SQL queries in plain text and possibly get tons of admin credentials.

thales - May 5, 2016, 7:19 pm

My advice: Don't drop the soap while in prison for hacking your school's shit.

?Criminal - May 5, 2016, 7:24 pm

(May 5, 2016 07:19 PM)thales Wrote: [\[CITE\]](#) My advice: Don't drop the soap while in prison for hacking your school's shit.

Usually its minors in middle school that would do something risky like this and in that case they usually get a verbal warning or juvi it all depends on the state/countrys police jurisdiction and applicable laws but anyways this CMS is also used in other sectors such as government, retail, food industry, IT, etc.But most people would probably mess with the schools it seems unless you're a hacktivist into pwning government stuff(ex: anons).

Poroshenko - May 8, 2016, 6:40 am

(May 5, 2016 07:24 PM)?Criminal Wrote: [\[CITE\]](#) Usually its minors in middle school that would do something risky like this and in that case they usually get a verbal warning or juvi it all depends on the state/countrys police jurisdiction and applicable laws but anyways this CMS is also used in other sectors such as government, retail, food industry, IT, etc.But most people would probably mess with the schools it seems unless you're a hacktivist into pwning government stuff(ex: anons).

Could you help me out with something? You seem like someone who'd be good at what I need done.

?Criminal - May 8, 2016, 7:01 am

(May 8, 2016 06:40 AM)AnonLoyalty Wrote: [\[CITE\]](#) Could you help me out with something? You seem like someone who'd be good at what I need done.

Specify exactly what you need for some insight theres no guarantee I just provide advice I don't fully spoonfeed anything besides I barely do anything nowadays anyway.

Poroshenko - May 8, 2016, 7:16 am

(May 8, 2016 07:01 AM)?Criminal Wrote: [\[CITE\]](#) Specify exactly what you need for some insight theres no guarantee I just provide advice I don't fully spoonfeed anything besides I barely do anything nowadays anyway.

hackforums.net/showthread.php?tid=5263011

Kyle1995 - May 8, 2016, 2:41 pm

Hahahahahahaha What?!? I'm done with hack forums for today. Really delete this thread it's giving me cancer. You have absolutely no idea what you're talking about

?Criminal - May 8, 2016, 6:10 pm

(May 8, 2016 02:41 PM)Involution Wrote: [\[CITE\]](#) Hahahahahahaha What?!? I'm done with hack forums for today. Really delete this thread it's giving me cancer. You have absolutely no idea what you're talking about

are you trolling or serious? there was a presentation on this and everything im gonna assume you're just trying to troll this thread because everything I stated is factual you can capture plain text traffic internally since its set up that way if you read the lansweeper article its set up in a similar way where you can escalate privs easily if you have internal access but externally its much trickier. Possibly how I worded it made you interpret it wrong but other then that all the attacks I mentioned still work the only thing they pretty much patched as far as I know is the PS_TOKEN cookie exploit allowing you to capture a cookie via anonymous logins, don't think they enabled a lockout policy yet. Ever heard of forced browsing? thats what I meant by directory enumeration, some directories you can view without needing admin credentials.

#Skyline - May 8, 2016, 8:59 pm

Advice from experience, don't brag to anyone about it if you do happen to gain access.

But I wouldn't recommend hacking your school, as your school is there for a reason, and so is there network.

Mr. WAVES - May 8, 2016, 9:52 pm

Just don't hack your school! If you do, DO NOT tell your friends. KEEP IT FOR YOU.

But just don't try to hack your school

?Criminal - May 8, 2016, 9:54 pm

(May 8, 2016 09:52 PM)YOLOnline Wrote: [\[CITE\]](#) Just don't hack your school! If you do, DO NOT tell your friends. KEEP IT FOR YOU.

But just don't try to hack your school

Definitely all it takes is one person to snitch with sufficient evidence.

Rolex? - May 9, 2016, 5:10 am

Yeah you shouldn't hack you school. We can see A TON of things that you may not realize.

?Criminal - May 9, 2016, 6:45 pm

(May 9, 2016 05:10 AM)SysAdmin Wrote: [\[CITE\]](#) Yeah you shouldn't hack you school. We can see A TON of things that you may not realize.

aside from the obvious event logs(programs opened, timestamp of when opened, window name, other metadata, etc) say theres multiple computer labs and 1 single external IP because the entire school uses a NAT, how would you track the student down since theres multiple computers if they did internal related stuff from the schools computer? schools usually force you to log in with a username and pass, so does each username tied with the event logs and time stamps how you track down a specific computer? im assuming it will be like name/username here - computer number 7 timestamp here or something to find a specific computer where the action is taking place, I just always wondered how IT does this.

Rolex? - May 9, 2016, 7:03 pm

(May 9, 2016 06:45 PM)?Criminal Wrote: [\[CITE\]](#) aside from the obvious event logs(programs opened, timestamp of when opened, window name, other metadata, etc) say theres multiple computer labs and 1 single external IP because the entire school uses a NAT, how would you track the student down since theres multiple computers if they did internal related stuff from the schools computer? schools usually force you to log in with a username and pass, so does each username tied with the event logs and time stamps how you track down a specific computer? im assuming it will be like name/username here - computer number 7 timestamp here or something to find a specific computer where the action is taking place, I just always wondered how IT does this.

A couple of different ways.

Let's say you were to login to powerschool from a teacher's account from a computer lab computer. Powerschool is hosted on our Active Directory which is powered by DNS.

Externally, myps.horrycountyschools.net -> Public IP. Internally, myps.horrycountyschools.net -> Internal IP. When accessed internally, powerschool will also log your internal IP and not your external. This alone points us to a single computer in the entire district. Let's assume that for whatever reason the internal IP wasn't logged. All web requests are processed by filter.horrycountyschools.net(LightSpeed Systems Rocket 2U server). The filter applies permissions based on your domain user. So when you make a request to access myps.horrycountyschools.net our lightspeed server will receive LAN IP, Computer name(Specifically named for ease identification, Domain User). Finding you through this method would require a little more work but is totally doable.

Let's assume that our LightSpeed server has been disabled and all internet traffic is being routed directly after RaaS. You will probably tell your friends, a teacher will see you, or process of elimination. Regardless we'll know what school it came from. More than likely what AP it came from which can, in most cases tell us what room you're in.

?Criminal - May 9, 2016, 7:08 pm

(May 9, 2016 07:03 PM)SysAdmin Wrote: [\[CITE\]](#) A couple of different ways.

Let's say you were to login to powerschool from a teacher's account from a computer lab computer. Powerschool is hosted on our Active Directory which is powered by DNS.

Externally, myps.horrycountyschools.net -> Public IP. Internally, myps.horrycountyschools.net -> Internal IP. When accessed internally, powerschool will also log your internal IP and not your external. This alone points us to a single computer in the entire district. Let's assume that for whatever reason the internal IP wasn't logged. All web requests are processed by filter.horrycountyschools.net(LightSpeed Systems Rocket 2U server). The filter applies permissions based on your domain user. So when you make a request to access myps.horrycountyschools.net our lightspeed server will receive LAN IP, Computer name(Specifically named for ease identification, Domain User). Finding you through this method would require a little more work but is totally doable.

Let's assume that our LightSpeed server has been disabled and all internet traffic is being routed directly after RaaS. You will probably tell your friends, a teacher will see you, or process of elimination. Regardless we'll know what school it came from. More than likely what AP it came from which can, in most cases tell us what room you're in.

interesting and once you have the room tracked down I assume you just check each computer that matches up to the sites from the traffic but anyways just was curious.

Rolex? - May 9, 2016, 7:28 pm

(May 9, 2016 07:08 PM)?Criminal Wrote: [\[CITE\]](#) interesting and once you have the room tracked down I assume you just check each computer that matches up to the sites from the traffic but anyways just was curious.

If we knew the room, we would notify the particular principal(s) and the IT staff there and have them handle the rest.

libc - May 10, 2016, 10:58 pm

(May 9, 2016 07:28 PM)SysAdmin Wrote: [\[CITE\]](#) If we knew the room, we would notify the particular principal(s) and the IT staff there and have them handle the rest.

Eh, this will only catch the idiots. If I were to hack my school, I would do it externally from my personal laptop at home and of course I would use Tor/VPN/proxies.

And I obviously wouldn't use my own school account to sign into the network.

Have an ounce of common sense (no bragging / telling anyone, changing your grades, etc) and

there's no way you're getting caught.