

Forum:[Hack Forums](#)

Thread: [Protecting the site](#)

Carl Elias - January 10, 2014, 10:30 am

Hey everyone I think this is my first post here so hopefully it is in the right place.

I am working on a website and we are trying to protect it from a few things. Recently someone hacked it using a bot using proxies to crack one of the staff members passwords. Then the next day we were going on and offline so I assume we were having a DDoS Attack.

We do use Cloudflare so the DDoS attack was fine after we enabled that.

My question is what is the best ways to protect a MyBB Forum from these types of incidents? Currently we have a few things in place such as, Cloudflare, proxy blocker on registration page, and a few other things probably I am forgetting. Mainly we are trying to avoid another crack like that, and keep the site up under DDoS Attacks.

Also any advice on how to add a MX Record to Cloudflare but keep the site protected from people resolving the site itself?

I would really like to see some answers!

Thanks

-Ty

incogneat0 - January 10, 2014, 3:42 pm

Limit login attempts and ban users, that should help a little bit...also make sure passwords with lower, upper, special, and numeric characters are being used in ALL admin/mod passwords...Otherwise if someone is running rainbow tables trying to bruteforce you may end up hacked real quick...

Only things I can think of, I am not too good at security issues...Kinda why i joined this site...

xhflhkeuhwguu34 - January 10, 2014, 3:43 pm

If you don't want your site to be resolved, don't host your email on the webserver. Or obtain a VPS/dedicated server that has protection already in front of it.

Carl Elias - January 10, 2014, 3:50 pm

Thanks Xen0n that was one answer I was looking for.

-Ty

PA?ADOX - January 11, 2014, 6:14 am

Google Apps provides exceptional email (basically the same as GMail) I don't think they have free service anymore but it's \$5 a month or \$50 a year. It's google so you don't need to worry about it being down. <http://www.google.com/enterprise/apps/business/pricing.html>

bazookajoe - January 11, 2014, 7:59 am

I experienced so many issues on my site that I financially resorted to contracting with a professional server maintenance company who took multiple steps to optimize and harden my new dedicated

server. Its a few bucks a month but I have had zero issues since I hired them, but I am less that a genius in security issues.

Carl Elias - January 11, 2014, 7:46 pm

(Jan 11, 2014 07:14 AM)PA?ADOX Wrote: [\[CITE\]](#) Google Apps provides exceptional email (basically the same as Gmail) I don't think they have free service anymore but it's \$5 a month or \$50 a year. It's google so you don't need to worry about it being down.

<http://www.google.com/enterprise/apps/business/pricing.html>

Ok I will look into this then. Google has everything I just do not know where to look a lot of the times

-Ty

ASLR - January 11, 2014, 9:08 pm

To prevent cracking just use really strong passwords. Try adding some code to the login function so after like 10 failed login attempts it disables login for that account and the user gets sent an email with a link to reactivate their account.

Approach - January 12, 2014, 5:11 am

First off check whether you're getting DDoSed or not.

Run "httpd status" to check Apache's status and see whether you're getting attacked or not.

If all the spots are taken up (no dots) then you might want to consider getting a basic firewall.

You can also run:

Code `netstat -n -p|grep SYN_REC | wc -l`

The value given should be max. 6.

If it's above that then you're most likely getting attacked.

If the attackers don't have your server's IP (not the Cloudflare one) you might want to consider upgrading your Cloudflare account and use their advanced DDoS mitigation service. You can also switch the security level to "I'm Under Attack" which will block/slow the attackers.

To prevent brute-force and dictionary attacks make sure to:

1. Use a strong password (> 10 characters including special characters and upper- & lower case letters).
2. Log the attempts and only allow 3 attempts per IP.

xhflhkeuhwguu34 - January 12, 2014, 12:12 pm

(Jan 12, 2014 06:11 AM)JackDeRips Wrote: [\[CITE\]](#) First off check whether you're getting DDoSed or not.

Run "httpd status" to check Apache's status and see whether you're getting attacked or not.

If all the spots are taken up (no dots) then you might want to consider getting a basic firewall.

You can also run:

Code `netstat -n -p|grep SYN_REC | wc -l`

The value given should be max. 6.

If it's above that then you're most likely getting attacked.

If the attackers don't have your server's IP (not the Cloudflare one) you might want to consider upgrading your Cloudflare account and use their advanced DDoS mitigation service. You can also switch the security level to "I'm Under Attack" which will block/slow the attackers.

To prevent brute-force and dictionary attacks make sure to:

1. Use a strong password (> 10 characters including special characters and upper- & lower case letters).

2. Log the attempts and only allow 3 attempts per IP.

[img]http://imgs.xkcd.com/comics/password_strength.png[/img]

Approach - January 18, 2014, 2:04 pm

(Jan 12, 2014 01:12 PM)Xen0n Wrote: [\[CITE\]](#)

[img]http://imgs.xkcd.com/comics/password_strength.png[/img]

Bear in mind that this only applies to brute-force attacks.

Dictionary attacks are the most common form of attacks.

Either way, as long as your password isn't something like "password" (one word, all lower caps) or "hello" you should be fine.

Carl Elias - January 18, 2014, 2:32 pm

Well is there any way that efficiently can block most proxies but not block legit IP's that have port 80 or something open because of the ISP? I am one of the team members and one of the other on the team has that issue since most plugins simply look for proxy ports being opened such as 80, 8080, 443, etc.

-Ty