

Forum:[Hack Forums](#)

Thread: [\[Tut\]What you should do if the target site is not vuln to anything\[Tut\]](#)

?Criminal - February 27, 2017, 7:52 am

Security is getting a lot better these days and many sites that are popular simply aren't vuln to trivial things anymore, however this should not demotivate you because theres other ways into the site, all sites have a sysadmin/team of staff so you want to target these people and not the web application it self, if the web app is hardened against most things this will literally be your only way to breach the target. If the site you're targeting is a forum for example a good thing to do is abuse the features to your advantage use the PM feature to get in contact with an admin, use a good lure tactic and hopefully get targeted malware opened up giving you access to the workstation. XSS and CSRF are still riddled all over the place so client side attacks are key to your success. Same-Site Cookies may have been added to chrome but barely any CMS has implemented the flag yet despite the support being there so CSRF will especially still be useful for the time being. A lot of major databases were taken with client side attacks and not exploits like a lot of people think, I mean there was the vbulletin vulns but aside from that it was mainly all client side. Beef hooks can also be used even if theres no XSS on the target site however if an XSS is found you can extend it's capabilities, you can always link a sysadmin a beef hook placed on a third party site however. To some people I'm stating the obvious, to others well they may have a different outlook when messing with web apps now. Another thing I want to stress is error code 403 which means Forbidden, this usually indicates the site has an IP whitelisting system enabled so aside from XSS, CSRF and DNS rebinding, a client side attack against the staff again would be your only option to bypass it.

Description - February 27, 2017, 7:58 am

You need a blackhat award, but there are things we simply can not talk about.