

Forum:[Hack Forums](#)

Thread: [\[Unity\] Hacking Help Desk](#)

Crystallize. - February 12, 2018, 6:06 am

We are only as strong as we are united, as weak as we are divided.

Welcome to our Hacking Help Desk, we are here to answer every question of yours, that is related to hacking. Starting from SQLi to Shelling, and much much more! Don't be shy to ask, we are here for you!

Helper/s EasyGhost
Elitas
Anxuein
Mad76e
Monster Energy

Faith Connors - February 12, 2018, 8:29 am

just a heads up your last divider thing is off centre because you didnt close the list tag haha.
lots of nice friends helping out here, lookin good friends :)

Crystallize. - February 12, 2018, 8:45 am

(Feb 12, 2018 09:29 AM)Faith Connors Wrote: [\[CITE\]](#) just a heads up your last divider thing is off centre because you didnt close the list tag haha.
lots of nice friends helping out here, lookin good friends :)
Thanks buddy, Im terrible when it comes to thread formatting :(.

mrpizzahut - February 13, 2018, 4:39 am

Never know -- think big enough and your entity here could development into a sizeable company.

[BLANK] - February 13, 2018, 9:25 pm

This is a good idea, hopefully it gets some traction.

Lime95 - February 13, 2018, 10:27 pm

How can i get people to log into a WiFi so i can view there information? what do i need to learn to do that what are some steps to start that?

smart77 - February 14, 2018, 1:16 am

How do I bypass WAF in sqlmap when I'm getting warning message "WAF is dropping suspicious blabla". Also, when sqlmap is unable to retrieved the database. Thanks in advance

Mad76e - February 14, 2018, 2:35 am

(Feb 13, 2018 11:27 PM)Lime95 Wrote: [\[CITE\]](#) How can i get people to log into a WiFi so i can view there information? what do i need to learn to do that what are some steps to start that?
Conflict of interest!

Hi. I dont feel comfortable answering wireless qrestions in this helpdesk, feel free to ask the same

question in my other helpdesk in the Wireless SF. (If no one can answer it in here)

[BLANK] - February 14, 2018, 7:35 am

(Feb 13, 2018 11:27 PM)Lime95 Wrote: [\[CITE\]](#) How can I get people to log into a WiFi so I can view their information? What do I need to learn to do that? What are some steps to start that?

You will need to use a bit of social engineering to get people to access your WiFi. This is usually easiest when out in public because many people will connect to any free open WiFi. For instance if you are in a Starbucks you could name your WAP "Free Coffee House Wifi" or something along those lines.

For equipment, you will need to have a Wireless Access Point and something to capture packets. I highly recommend the Hak5 Pineapple for this purpose:

<https://hakshop.com/collections/wifi-pineapple-kits>

It was specifically designed to do what you are asking about. It should even come with a book on how to use it. There are also some YouTube videos for tutorials.

<https://www.youtube.com/watch?v=6iZcZclxGs8>

See also:

Evil Twin Attacks:

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/>

Rogue Wireless Access Points:

https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

(Feb 14, 2018 02:16 AM)smart77 Wrote: [\[CITE\]](#) How do I bypass WAF in sqlmap when I'm getting warning message "WAF is dropping suspicious blabla". Also, when sqlmap is unable to retrieve the database. Thanks in advance

This is complicated because the main job of a WAF is to block common attack vectors such as SQL injections, XSS, XSE and so forth. Even if the application behind the WAF is vulnerable, the WAF will protect it, which is why companies pay a hundred grand a year for that kind of protection. To be able to bypass the WAF you will need to do a lot of research. Find the make and model of the WAF being used, find the version number of the firmware and hope there is a known bypass rule.

Here is an example of bypassing F5 WAF:

<https://packetstormsecurity.com/files/131781/F5-BIG-IP-ASM-11.4.1-Filter-Bypass.html>

One common way of bypassing WAF is if the WAF is being used as a proxy then an attacker may be able to bypass the proxy and go straight to the source public IP address of the application. Some administrators forget that just because the domain name transfer is going through a proxy doesn't mean the public IP is not reachable. Administrators should be blocking all incoming traffic to their public IP except for the WAF. Overall there is not just one sure way of bypassing a WAF, you will have to fuzz the filters to see if anything gets through, check for known filter issues, and check for insecure configuration on the server side.