

Forum:[Hack Forums](#)

Thread: [HELP Cracking http Basic Authentication for Archival Purposes](#)

EM55SUEZ - April 29, 2024, 7:01 pm

Hey, I'm new here.

I've been trying to get into hacking recently. It's less a passion though, and more out of necessity.

I have some incredibly outdated hardware. It hasn't been supported by the manufacturer since 2003. Despite this, it's very important to me. I'd like to be able to write code for this hardware, but to do so requires a tailored Compiler Software. The Compiler outputs a single bin file which is then burned to a ROM and inserted into the hardware.

While I am not much of a hacker (my accomplishments so far are limited to patching a few old installers to bypass the need for serial numbers), I consider myself adept at internet sleuthing. I've determined quite confidently that the installer for the compiler that I need publicly exists on only a single website present day. (And yeah I've been all over the Wayback Machine, multiple opportunities for the installer to be crawled, but it never was.) The issue is, the website in question is protecting all the Compilers and Datasheets on it with Basic http Authentication, using GET. It also has not been maintained since 2009. I've made contact with multiple people associated with the website, they don't acknowledge that the website still exists today, and maintain that they no longer have the Compiler that I require. Similarly, I have made contact with multiple relevant departments of the company that originally distributed the Software and Datasheets, they also claim to no longer have the compiler after so long.

All of this has lead me to really only 2 options. Hack the website myself, or pay somebody to do so. I've put about a week into the former and have not really gotten anywhere so far. I've tried a dictionary attack using Burpsuite but it was going really slow. I don't think that I have the machine required to Brute Force the credentials. I've also got Kali installed and have looked into Hydra, but got a bit overwhelmed. Another huge setback is that I don't know either the Username or the Password, what characters exactly they contain, or even the length of the credentials. The website is running Apache 2.2.22 with Fedora, it really seems like it should be a walk in the park. I just don't know what I'm doing. Ideally I'd like to get the legitimate credentials and use them to archive everything hosted on the site for future reference, in the case that the site inevitable goes offline. But there are only about 5 files on there that I could say that I genuinely NEED at this time. Its also worth noting, I went over the site's terms and conditions. It pretty boldly states that every user is allowed one copy of all files on the site. No mention of the authentication system, no mention of working around it. So I'm not even sure that this is illegal. It does feel more like a 'grey hat' project though.

So here I am, you know my Hack Forums origin story. Any input whatsoever would be incredibly appreciated. I don't feel comfortable sharing links publicly on here. These are good people and I don't want somebody wreaking havoc on their site, even if they don't know that it still exists. If you want to reach out to me in PMs for more information or context, I encourage you to do so.

Thank you for reading,
EM55SUEZ

InspectorGadget - April 30, 2024, 3:12 am

I would stick to the Hydra route, maybe setup your own web server using basic auth, then use hydra

to attack it. Then when it works, you'll know you have the syntax etc correct and can swap it to your target site.

At the end of the day, humans are the ones logging in, so it's doubtful the usernames and passwords are massively long.

If this matters so much, and if they have no protection against bruteforcing, maybe start from the start and bruteforce both username and password. Do some recon too, try and find common words for the company, company name etc - there's also a good chance the username and password are the exact same. Defo run some common passwords lists as both username and password.

Lastly, i'd suggest using nmap to look for other services running on the server thats hosting the site, maybe there are different ways other than the basic auth to get onto the server.

EM55SUEZ - April 30, 2024, 3:41 am

(Apr 30, 2024 03:12 AM)InspectorGadget Wrote: [\[CITE\]](#) I would stick to the Hydra route, maybe setup your own web server using basic auth, then use hydra to attack it. Then when it works, you'll know you have the syntax etc correct and can swap it to your target site.

At the end of the day, humans are the ones logging in, so it's doubtful the usernames and passwords are massively long.

If this matters so much, and if they have no protection against bruteforcing, maybe start from the start and bruteforce both username and password. Do some recon too, try and find common words for the company, company name etc - there's also a good chance the username and password are the exact same. Defo run some common passwords lists as both username and password.

Lastly, i'd suggest using nmap to look for other services running on the server thats hosting the site, maybe there are different ways other than the basic auth to get onto the server.

Those are some great tips, thank you! I've also seen your PM, I still need to unlock chats though. Working on it right now. Hope to talk more soon.

SilentNuke - April 30, 2024, 8:35 am

(Apr 29, 2024 07:01 PM)EM55SUEZ Wrote: [\[CITE\]](#) Hey, I'm new here. I've been trying to get into hacking recently. It's less a passion though, and more out of necessity.

I have some incredibly outdated hardware. It hasn't been supported by the manufacturer since 2003. Despite this, it's very important to me. I'd like to be able to write code for this hardware, but to do so requires a tailored Compiler Software. The Compiler outputs a single bin file which is then burned to a ROM and inserted into the hardware.

While I am not much of a hacker (my accomplishments so far are limited to patching a few old installers to bypass the need for serial numbers), I consider myself adept at internet sleuthing. I've determined quite confidently that the installer for the compiler that I need publicly exists on only a single website present day. (And yeah I've been all over the Wayback Machine, multiple opportunities for the installer to be crawled, but it never was.) The issue is, the website in question is protecting all the Compilers and Datasheets on it with Basic http Authentication, using GET. It also has not been maintained since 2009. I've made contact with multiple people associated with the website, they don't acknowledged that the website still exists today, and maintain that they no longer have the Compiler that I require. Similarly, I have made contact with multiple relevant departments of the company that originally distributed the Software and Datasheets, they also claim to no longer have the compiler after so long.

All of this has lead me to really only 2 options. Hack the website myself, or pay somebody to do so. I've put about a week into the former and have not really gotten anywhere so far. I've tried a dictionary attack using Burpsuite but it was going really slow. I don't think that I have the machine required to Brute Force the credentials. I've also got Kali installed and have looked into Hydra, but got a bit overwhelmed. Another huge setback is that I don't know either the Username or the Password, what characters exactly they contain, or even the length of the credentials. The website is running Apache 2.2.22 with Fedora, it really seems like it should be a walk in the park. I just don't know what I'm doing. Ideally I'd like to get the legitimate credentials and use them to archive everything hosted on the site for future reference, in the case that the site inevitable goes offline. But there are only about 5 files on there that I could say that I genuinely NEED at this time. Its also worth noting, I went over the site's terms and conditions. It pretty boldly states that every user is allowed one copy of all files on the site. No mention of the authentication system, no mention of working around it. So I'm not even sure that this is illegal. It does feel more like a 'grey hat' project though.

So here I am, you know my Hack Forums origin story. Any input whatsoever would be incredibly appreciated. I don't feel comfortable sharing links publicly on here. These are good people and I don't want somebody wreaking havoc on their site, even if they don't know that it still exists. If you want to reach out to me in PMs for more information or context, I encourage you to do so.

Thank you for reading,
EM55SUEZ

You have many options available to you. If you PM me, i can try assist you.

EM55SUEZ - May 8, 2024, 4:18 pm

(Apr 30, 2024 08:35 AM)SilentNuke Wrote: [\[CITE\]](#) You have many options available to you. If you PM me, i can try assist you.

Thank you very much, message sent.