

Forum:[Hack Forums](#)

Thread: [Hacking Facebook with phishing page \(Curious\)](#)

allsystems2 - August 11, 2019, 1:53 pm

Hi All,

I was just curious if I was to build a phishing page exact replica of a Facebook page and send it out to the victim will I be able to retrieve the login details?

Thank you

Systems out

Ramb0x - August 11, 2019, 1:59 pm

Why not

use \$_POST
then fwrite
if you want to send a mail use mail() function.

Prawnster - August 11, 2019, 2:00 pm

Yup phishing pages are able to steal login data...

Rodrigo Moya - August 11, 2019, 3:50 pm

I wonder if somebody could teach me how to create a Phishing page for Aberoth.com

BestHackTools - August 11, 2019, 5:42 pm

(Aug 11, 2019 01:53 PM)allsystems2 Wrote: [\[CITE\]](#) Hi All,

I was just curious if I was to build a phishing page exact replica of a Facebook page and send it out to the victim will I be able to retrieve the login details?

Thank you

Systems out

You can do it bro, its easy to do. Just open your web browser, wait for it to load fully, then press ctrl+s and save it as Full Webpage. After saving, open the .html file with your notepad. You may need to add some simple PHP script to email the form login details to you on submit.

Host the page on your own webserver and spam the link.

cheers!!!

mObile - August 11, 2019, 6:32 pm

I used to use a fake KFC voucher on multiple hacked websites to get FB logins.

<https://imgur.com/a/cXm6OIB>

You'd be surprised how many people like KFC Chicken. ?

bravetoaster - August 11, 2019, 8:04 pm

Yes If you know what your doing. I have a few variants of FB I can link you to if you want em. One's a verbatim copy, One incorporates iframes, and one is 99% PHP that looks like a nightmare when you open the index file, but it's just loading all the js libraries fb uses and solves some CORS problems because it was originally a PoC and I didn't give a shit about self-signing certs or getting legit ones.

Anyways. Yes you definitely can. This relies 80% on social engineering. Getting them to visit your link, getting them to believe it as authentic, and proceed with credential entry. How you do that...well there's literally an infinite number of possibilities. A quick few:

- 1.) DNS Poisoning - either via exploitation of their LAN, or common destination such as a coffee shop
- 2.) If you have any knowledge of web app dev you can incorporate it into an iframe or a page built up to look like some other thing that'd peak their interest and simply using OAuth to sign-in/up.
- 3.) Sending of links - shorteners like bitly, utilizing Google API for custom shortening service, etc. Get them to visit it by sending it directly to them
- 4.) Embedding in email. Whether its "Account compromised, reset password", etc. etc. and then they follow it from email (Now here's where you could run into problems. Chrome uses some funky ass heuristics to blacklist / flag sites. I locked on example down harder than any C2 I've ever setup. I'm talking python scripts to generate custom IDs/tokens that are then read by Apache's rewrite module which then in turn feeds results to both HTTP_AUTH_DIGEST and a PHP function elsewhere. I did it to ensure you couldn't try and come back to phish page after you've submitted creds. That cut down on incident response by like 77% for me. I also had specific robots.txt explicitly stating user-agent * disallow / - so no crawling. Was a sub-domain takeover and fucking chrome still somehow was trying to flag it. I deduced they recognized an aspect of their login page and since they didn't own the domain, and I wasn't incorporating oAuth anywhere I suppose I'm 'suspicious.'

TL:DR - Sending links via email has a lot of independent variables you're taking a gamble on - where you sending it from? If from phishing domain / setup then you're gambling you make it past the filters. If sent from custom gmail or personal gmail then you got all the content-filters to worry about in message-body. So depending on email service they often employ web crawlers that will detect "HTTP://" and then issue an asych GET request or HEAD request and then render page image or some meta variable that's some type of media for a thumbnail. Here you could find yourself getting flagged again. Then if you don't get flagged on the inbox, the message body, the link content, then you have to gamble on the SE aspects of it. If your sending from personal email or spoofed email for a friend of theirs you have to garner their attention and trust. Why should they follow the link? What context would cause interest, urgency, or curiosity? Then once they visit do they have good reason to login? Does your cloned site look legit?

so yea...a lot of things to think about, a lot of ways to do it. I wrote up a PoC not too long ago where I exploited some 'features' of chrome's browser. One in mobile and one on desktop. I used a JS library that enabled fullscreen, some png images libraries I made that are rendered depending on my JS script that identifies their browser type (user-agent) and overlays them at the top. So bye bye URL bar. I didn't try it for malicious purposes but fooled 8/10 peers with it.

You can likely find (if not mine) a million versions of cloned popular social HTML pages. Try it out in a few browsers, make sure your PHP script writes to a file only you have permissions to write/read to, or go way out of scope beyond default web root to write to file. I write to DB, file, and remote IP personally. Then I'd put most of your energy into SE aspects. If they're a friend then compile some recon, if they're not even more reason to. Phishing is successful because of good SE more times than clever browser flaws, good code, etc.

oaxha uaxha - September 8, 2019, 7:12 am

Please can you help with the Facebook phishing page especially the PHP.?

(Aug 11, 2019 05:42 PM)BestHackTools Wrote: [\[CITE\]](#) You can do it bro, its easy to do. Just open your web browser, wait for it to load fully, then press ctrl+s and save it as Full Webpage. After saving, open the .html file with your notepad. You may need to add some simple PHP script to email the form login details to you on submit.

Host the page on your own webserver and spam the link.

cheers!!!

BestHackTools - September 9, 2019, 2:52 pm

(Sep 8, 2019 07:12 AM)oaxha uaxha Wrote: [\[CITE\]](#) Please can you help with the Facebook phishing page especially the PHP.?

Yes, PM me for that

Venture - September 9, 2019, 4:14 pm

Yeah you use the credential harvester in kali, and then open a remote connection using ngrok. Its beautiful because it usually isnt detected by a browsers anti-phishing protection because its not flagged as malicious