

Forum:[Hack Forums](#)

Thread: [Man In The Middle Attack on HTTPS ?](#)

odedor444 - February 9, 2019, 6:06 am

Hi,

Is there a way to sniff Https sites like facebook when using MITM attack ?

i tried to spoof facebook.com to a cloned site but chrome immediately stopped the connection and showed a big warning with no option to proceed ?

is there a way to bypass that ?

Thanks in Advance

Battalaxix - February 10, 2019, 3:03 am

I'm pretty sure google introduced something to help protect against phishing attacks (something to do with the URL). Sorry, I forgot what it was but it will be much harder now. You could possibly hijack a legit website and do it like that but it won't be permanent. Eh.

SysAdmin - February 11, 2019, 3:48 am

(Feb 10, 2019 04:03 AM)Battalaxix Wrote: [\[CITE\]](#) I'm pretty sure google introduced something to help protect against phishing attacks (something to do with the URL). Sorry, I forgot what it was but it will be much harder now. You could possibly hijack a legit website and do it like that but it won't be permanent. Eh.

You mean HSTS?

HTTP Strict Transport Security, in short, forces the server to only issue requests over HTTPS and refuses to downgrade the connection to HTTP, as many tools (for example sslstrip) would attempt to do.

What Battalaxix is going with is you could essentially clone a login website such as login.facebook.com and upload it to a web host. I won't go further into details as this is essentially phishing, but you could do this on local as well as on the world wide web.

LegendBegins - February 15, 2019, 2:04 pm

(Feb 11, 2019 04:48 AM)SysAdmin Wrote: [\[CITE\]](#) You mean HSTS?

HTTP Strict Transport Security, in short, forces the server to only issue requests over HTTPS and refuses to downgrade the connection to HTTP, as many tools (for example sslstrip) would attempt to do.

What Battalaxix is going with is you could essentially clone a login website such as login.facebook.com and upload it to a web host. I won't go further into details as this is essentially phishing, but you could do this on local as well as on the world wide web.

SSLStrip doesn't require a protocol downgrade. The client is required to add the SSLStrip server as a CA, allowing SSLStrip to sign its own communications. Facebook thinks SSLStrip is the client and the client thinks SSLStrip is Facebook, no HTTP involved. That's why it's effective for corporations, even when the website has HSTS enabled. I suppose you could downgrade if you wanted to, but it

wouldn't be very beneficial to do so. And even in that circumstance, the stripping server could also remove HSTC since it completely controls the content delivered to the client.

To OP: You won't be able to MiTM encrypted web traffic without first installing something on their device, which defeats the purpose of MiTM in the first place.

SysAdmin - February 15, 2019, 2:07 pm

(Feb 15, 2019 03:04 PM)LegendBegins Wrote: [CITE](#) SSLStrip doesn't require a protocol downgrade. The client is required to add the SSLStrip server as a CA, allowing SSLStrip to sign its own communications. Facebook thinks SSLStrip is the client and the client thinks SSLStrip is Facebook, no HTTP involved. That's why it's effective for corporations, even when the website has HSTS enabled.

To OP: You won't be able to MiTM encrypted web traffic without first installing something on their device, which defeats the purpose of MiTM in the first place.

See, that's what I was looking for! A good enough explanation of how something works.