

Forum:[Hack Forums](#)

Thread: [SSL Poodle Exploit](#)

Omniscient - October 17, 2014, 5:17 pm

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

Some of you might be paying attention to these rather publicized exploits but some may not. In either case the latest exploit bug in SSL was released about a week ago and labeled "Poodle" which stands for "Padding Oracle On Downgraded Legacy Encryption".

It's basically a MITM exploit. Not really easy to take advantage of but considering this is now the 2nd time a huge SSL exploit was published I just wonder why members still send me requests for us to add SSL.

It's imho very dangerous to falsely assume your safe because your browser has a little lock icon. You should be relying on your own knowledge and your own connection for your own security.

We may one day add SSL/TLS to the site. Not sure when if ever but it might come. I just don't see why members are pushing for it at a time when SSL has been cracked twice. And I've not once had an account stolen via MITM.

We're more in need of other security options for accounts beyond an SSL connection like 2FA. Which I am currently working on.

Thanks everyone and enjoy.

Dr.Cooper - October 17, 2014, 5:17 pm

Thanks for the awesome info. Reading it right now Omni! :) Cheers!

Cyba - October 17, 2014, 5:19 pm

Adding SSL to a large site is a pain in the ass, speaking from personal experience. So many things you need to fix manually, not just installing the cert and editing htaccess.

Aura - October 17, 2014, 5:34 pm

Saw this yesterday. Google and Mozilla are supposed to adjust their browsers to make them more secure to use and prevent that exploit from hitting them but for now all of them (browsers) are vulnerable.

Fox™ - October 17, 2014, 5:34 pm

This is sad, and adding SSL to large sites, as stated above is a pain. I'm excited for 2FA though. c:

Wafflemonger - October 17, 2014, 6:56 pm

Yeah, I remember reading this last week and thinking the exact same thing, "Won't really be an issue for most networks out there unless there's a disgruntled employee or no one notices someone sitting there with a laptop for hours on end."

Inkling - October 17, 2014, 6:58 pm

Poodle's a rather old exploit, isn't it?

I remember reading about this exploit like a year ago.

Tuna - October 17, 2014, 7:00 pm

Glad to see you upgrading the website!

Tony Stark - October 17, 2014, 7:02 pm

Hopefully this provides answers to those pushy people.

Been waiting patiently for 2FA. Hopefully members will be at peace knowing their accounts will be more secure and their security is more in their control once it's implemented.

Omniscient - October 17, 2014, 7:08 pm

I like how the easy fix is as simple as "disable ssl". :)

Autopost - October 17, 2014, 7:14 pm

To be honest I just cant wait until 2FA, that's when I'll be happy.

ZuGgY - October 17, 2014, 7:16 pm

Oh damn, first Heartbleed and now this? o_O

Blazin - October 17, 2014, 7:25 pm

Wow more SSL shit being exposed wonderful.

Rote - October 17, 2014, 7:28 pm

Really glad that we got someone like you mate,
keeping yourself updated so we stay safe. :)

Omniscient - October 17, 2014, 8:00 pm

I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part. Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still.

Ahri????? - October 17, 2014, 9:36 pm

I fear these MITM because I tend to use public Wifi 40% of the time aka my college wifi. I'll have to just hope nothing happens.

Levi - October 17, 2014, 9:45 pm

(Oct 17, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part. Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still.

It's definitely improved since last year, disruption is minimal in comparison.

Ivy Mike - October 17, 2014, 11:07 pm

I find it quite funny how something which is meant to "protect us" has actually ended up doing the opposite. Luckily, Omniscient didn't implement it.

?Ñâzg?! - October 17, 2014, 11:19 pm

there is really no need of SSL

if a HF member ever goes on vacation or somewhere with public wifi he/she should use his own VPN client that connects back to HIS house which supports encryption

then all information that is transferred in that unsafe environment will stay safe from any man in the middle exploits

Ivy Mike - October 17, 2014, 11:21 pm

(Oct 17, 2014 11:19 PM)?Ñåzg?I Wrote: [\[CITE\]](#) No need of SSL

if a HF member ever goes on vacation he should use a VPN which supports encryption

then all information transferred in a unsafe environment (example: sketchy hotel room) will be safe

Not a smart idea actually. You can be merged/banned/closed if multiple HF members are using that same VPN. Hence, why it's not a good idea. Vacation ban is there for a reason.

?Ñåzg?I - October 17, 2014, 11:24 pm

(Oct 17, 2014 11:21 PM)Emma Watson™ Wrote: [\[CITE\]](#) Not a smart idea actually. You can be merged/banned/closed if multiple HF members are using that same VPN. Hence, why it's not a good idea. Vacation ban is there for a reason.

I corrected that I meant a VPN that connects to your house.

Your OWN VPN

not public, same IP.

Abdilo - October 17, 2014, 11:32 pm

(Oct 17, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part. Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still. See if i can guess what the ssh sessions are doing

One being:

```
tail -f access.log|grep '
```

The other:

```
root@hostname~:
```

also did you move domain registrars to one that cant get social engineered yet?, dont want egypt getting all 1337133ts0c1l3n1n3ring again, atleast hf's main page wasnt turned into an iframe to an ek.

People using vpns could work just buy a vps and setup openvpn on it/ssh tunnel and with a vps only you have that ip, since you are paying for it, but when you stop paying for it.... well i highly doubt someone is going to sit there and buy vpses all day trying to get the ip you used to connect to hf from to scam.

I would say use tor but tor cant protect your data on clearnet without relying on ssl, thats why some sites have a .onion address even though the site is accessable via clearnet the onion address will be there just so users can use tor and be more secure then if you used ssl.

So omni could ad a .onion accessible domain, it stops mitm attacks over tor as well. but then you have a shitload of anonymous accounts and unless you create some way that proves that they are actually human(besides captcha) and that they do use that account(GAUTH + TOR?) its sorta hard to see if accounts have been comprimised.

also block account creation via tor as well, you can get a public list of exitnodes from torproject

eXero - October 17, 2014, 11:34 pm

Thanks for everything you do Omni. You're ahead of the game.

420 Blaze It - October 17, 2014, 11:36 pm

Interesting, but wouldn't it cause problems once you disable SSL?

?Ñåzg?! - October 17, 2014, 11:39 pm

(Oct 17, 2014 11:32 PM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) People using vpns could work just buy a vps and setup openvpn on it/ssh tunnel and with a vps only you have that ip, since you are paying for it, but when you stop paying for it....

I was thinking instead of a VPS a VPN connecting back to your home would be better, then there is no multiple Ip conflict. I mean its pretty easy to set one up anyways and no paying is required

Abdilo - October 17, 2014, 11:42 pm

(Oct 17, 2014 11:39 PM)?Ñåzg?! Wrote: [\[CITE\]](#) I was thinking instead of a VPS a VPN connecting back to your home would be better, then there is no multiple Ip conflict. I mean its pretty easy to set one up anyways and no paying is requiredEDIT: fuck me i didnt read what you said properly i thought you meant while you at home, you vpn to your own ip, but that would be retarded if someone is already sniffing on your home network lawl

Skorp - October 17, 2014, 11:43 pm

Read about this couple days ago, thanks for the share again.

Omniscient Wrote:We may one day add SSL/TLS to the site.

I really hope you do not, saves alot of time and unnecessary drama. Time is golden as your todo list is never-ending. :)

Robust - October 18, 2014, 6:27 am

I've been keeping up with this as some of my clients use SSL. SSL for a forum is totally unnecessary. It causes so many issues, for example third party services. It's needed for PayPal and banks, sure, but not for a forum. There is no sensitive information except login, and SSL can already be used on that page.

(Oct 17, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part. Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still.

Don't have a laptop atm, so I usually have multiple JuiceSSH windows open haha. Few open atm. Mobile ssh client.

Meester - October 18, 2014, 12:57 pm

Good luck with 2FA. We are waiting eagerly for it.

Robust - October 18, 2014, 3:10 pm

Just finished disabling SSLv3 on all of my websites using SSL. Only TLSv1 now. I think that's the end of the SSLv3 life line now.

Simple fix:

ssl_ciphers SSLv3 TLSv1;

To

ssl_ciphers TLSv1;

Should be OK with all modern computers too

Cyrus - October 18, 2014, 9:21 pm

Two factor authentication should help around here alot - especially stopping accounts getting "hacked" which leads to stopping scams.

Comedic - October 19, 2014, 12:27 am

(Oct 17, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part. Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still.

And I thank you for that mate. :D

?

Robust - October 19, 2014, 12:42 am

(Oct 18, 2014 09:21 PM)Cyrus Wrote: [\[CITE\]](#) Two factor authentication should help around here alot - especially stopping accounts getting "hacked" which leads to stopping scams.

Half of the scams regarding hacked accounts here is the member pretending he was hacked and scamming.

Omniscient - October 19, 2014, 12:45 am

(Oct 19, 2014 12:42 AM)Robust Wrote: [\[CITE\]](#) Half of the scams regarding hacked accounts here is the member pretending he was hacked and scamming.

Or a sold account. Very few accounts are actually stolen.

Understalker - October 19, 2014, 12:46 am

Just because there is 2FA does not mean users will use them.

If I am not mistaken you plan on enabling 2FA for Ub3rs only right?

Koffee - October 19, 2014, 12:56 am

(Oct 19, 2014 12:46 AM)Understalker Wrote: [\[CITE\]](#) Just because there is 2FA does not mean users will use them.

If I am not mistaken you plan on enabling 2FA for Ub3rs only right? If this were the case and ub3rs would be the only ones taking advantage of this, I believe nothing would really be done, besides of course the obvious, which is account safety for ub3rs. As a whole, it would be beneficial to the entire site if everyone were enabled 2FA.

Crypto™ - October 19, 2014, 3:14 am

While I understand your points, having HTTPS is better than nothing at all. The exploit relies on a failover to SSL v3.0, which is coming up on 20 years old. The easy fix is to disable failover to SSL v3.0, not to disable SSL entirely. As for the second crack, I assume you're referring to Heartbleed, which only affected OpenSSL, a popular, but by far not the only, SSL library. Honestly, I think the SSL hacks are no excuse for not implementing some sort of SSL. It is of course dangerous to assume safety due to a single technology, but still, it's something to prevent basic MitM attacks.

(Oct 17, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) I actually spend a fair amount of time as a system admin for HF. It's time members are not aware I'm spending working for the most part.

Whether it's toying around with settings, updating services, or increasing security, I'm usually in multiple SSH sessions at any given time during the day. I have 2 open right now.

Realistically I think I've done a good job for the most part with keeping HF online and secure. Not perfect but pretty good still.

Nothing's ever perfect, but I think we all need to give Omni a round of applause for all the work he does.

Robust - October 19, 2014, 3:24 am

(Oct 19, 2014 03:14 AM)Crypto™ Wrote: [\[CITE\]](#) While I understand your points, having HTTPS is better than nothing at all. The exploit relies on a failover to SSL v3.0, which is coming up on 20 years old. The easy fix is to disable failover to SSL v3.0, not to disable SSL entirely. As for the second crack, I assume you're referring to Heartbleed, which only affected OpenSSL, a popular, but by far not the only, SSL library. Honestly, I think the SSL hacks are no excuse for not implementing some sort of SSL. It is of course dangerous to assume safety due to a single technology, but still, it's something to prevent basic MitM attacks.

Nothing's ever perfect, but I think we all need to give Omni a round of applause for all the work he does.

OpenSSL is very popular - a large percentage of websites use it, including Yahoo, CloudFlare etc. Heartbleed was important, whilst it was semi-hard to actually get some good data that was useful in my opinion, it was indeed important. SSL is something, sure, but when using a lot of external libraries or something you're going to have to update quite a lot to support SSL entirely. For example, I use SSL on my gaming forum and I can't embed from media sites that don't support SSL, namely Gamespot and IGN.

labroca - October 19, 2014, 12:36 pm

This was a very interesting thread, and I'm glad you once again brought this type of knowledge to my attention..

I'm still looking to alternative web solutions for a project/theory of mine..

dan ??? - October 19, 2014, 12:41 pm

Thanks Omni for this post. I really do appreciate the info and heads up. ?

Omniscient - October 19, 2014, 8:54 pm

Quote:I understand your points, having HTTPS is better than nothing at all.

That's false. SSL has now had 2 security exploits. It is actually better to have nothing than SSL. And I'm fairly confident more exploits in SSL and eventually TLS will be found.

Quote:but still, it's something to prevent basic MitM attacks.

MitM attacks are rare and difficult to take advantage of. 2FA is much more secure as an option for logins than SSL.

What's a real headache is the changes required for a site like HF to run full SSL correctly. It creates more problems than it solves and now has the added burden of 2 serious exploits.

While I won't say we'll never add SSL I can say that I'm in no hurry to do so.