

Forum:[Hack Forums](#)

Thread: [.Net Core API security resources?](#)

severos - May 25, 2017, 8:45 am

I was wondering if you guys could share some resources for building secure API using .net core, not looking for stuff like XSS or some javascript stealing since I'm building API only.

Currently I'm looking at authentication & authorization, but I'd like to know if there are some hidden tricks, maybe there's some exploit in the data binder MVC uses? or something in the MVC it self? or??? of course I'll be looking into each of them, but having some resources could save quite a good amount of time.

Thanks in advance.

Ninja - May 25, 2017, 9:17 am

I find it hard to understand what you want.

You want to know how to build a Web API in .NET Core? There are plenty of results on Google, such as:

<https://docs.microsoft.com/en-us/aspnet/core/tutorials/first-web-api>

severos - May 25, 2017, 9:58 am

(May 25, 2017 09:17 AM)Ninja Wrote: [\[CITE\]](#) I find it hard to understand what you want.

You want to know how to build a Web API in .NET Core? There are plenty of results on Google, such as:

<https://docs.microsoft.com/en-us/aspnet/core/tutorials/first-web-api>

I'm looking to build a secure API, building an API is fairly easy, just copy&paste codes around, but I want to learn about securing it.

Maybe things like this link: https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet it provides some nice notes, but some of them don't apply to API since they're related to the html such as cookies, unvalidated redirect, Anti Forgery and XSS (do they apply to API??)

marvinn - May 25, 2017, 10:22 am

(May 25, 2017 09:58 AM)severos Wrote: [\[CITE\]](#) I'm looking to build a secure API, building an API is fairly easy, just copy&paste codes around, but I want to learn about securing it.

Maybe things like this link: https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet it provides some nice notes, but some of them don't apply to API since they're related to the html such as cookies, unvalidated redirect, Anti Forgery and XSS (do they apply to API??)

No. God no! Don't copy paste code for your API. please.

Ninja - May 25, 2017, 11:44 am

(May 25, 2017 09:58 AM)severos Wrote: [\[CITE\]](#) I'm looking to build a secure API, building an API is fairly easy, just copy&paste codes around, but I want to learn about securing it.

Maybe things like this link: https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet it provides some nice notes, but some of them don't apply to API since they're related to the html such

as cookies, unvalidated redirect, Anti Forgery and XSS (do they apply to API??)

APIs are vulnerable to SQL injection attacks, and XSS attacks as well (maybe even persistent ones).

(May 25, 2017 09:58 AM)severos Wrote: [\[CITE\]](#) just copy&paste codes around
Oh god...

ubbelol - May 25, 2017, 11:49 am

This is such a wide question it's impossible to answer. If you can provide some more specific scenarios or examples maybe someone could contribute.

0xDEAD10CC - May 25, 2017, 3:29 pm

(May 25, 2017 11:44 AM)Ninja Wrote: [\[CITE\]](#) APIs are vulnerable to SQL injection attacks, and XSS attacks as well (maybe even persistent ones).

Oh god...

You're assuming they all use SQL, and certain false assumptions are also being made on your part here to include XSS vulnerabilities also. :/ I can guarantee that my RESTful Philips Hue system API is not vulnerable to either of those. That's not a universally true statement that you've made, only in a handful of cases.

@OP - You could look at building an API using OAuth 2.0 with Two factor authentication, and have a RESTful back end for a scalable platform agnostic solution; HTTP requests and XML and/or JSON.

severos - May 25, 2017, 9:13 pm

(May 25, 2017 11:44 AM)Ninja Wrote: [\[CITE\]](#) APIs are vulnerable to SQL injection attacks, and XSS attacks as well (maybe even persistent ones).

Oh god...I understand the SQL part, but how would they be vulnerable to XSS??? didn't XSS happen only when rendering pages? how would that affect JSON objects for example??

(May 25, 2017 11:49 AM)ubbelol Wrote: [\[CITE\]](#) This is such a wide question it's impossible to answer. If you can provide some more specific scenarios or examples maybe someone could contribute. I know it's wide, but that's the nature of the question, I'm trying to get a hold on many things, if you know a scenario it'd be awesome if you provide info about it, then I'll just collect the info from whatever is provided here.

As a start, I'm looking into what vulnerabilities would exist if I'm using the default MVC for .Net Core, maybe something that can break the routing? data binding? also, what are other possible attacks and how to prevent them (slowloris for example, or local/remote file execution).

(May 25, 2017 03:29 PM)0xDEAD10CC Wrote: [\[CITE\]](#) You're assuming they all use SQL, and certain false assumptions are also being made on your part here to include XSS vulnerabilities also. :/ I can guarantee that my RESTful Philips Hue system API is not vulnerable to either of those. That's not a universally true statement that you've made, only in a handful of cases.

@OP - You could look at building an API using OAuth 2.0 with Two factor authentication, and have a RESTful back end for a scalable platform agnostic solution; HTTP requests and XML and/or JSON.

So for authentication OAuth is best option? far as I understood OAuth is used when you want to let other services access someone's data, not when you want someone him self to access his own data, right? or I got lost somewhere while reading??

what if I don't want 2FA, what would be the best option?

The API will be using JSON, and looking to make it scalable as much by making every component independent and can run alone, so it allows running multiple instances on different machines (something like micro-services?)

Ninja - May 26, 2017, 7:52 am

(May 25, 2017 03:29 PM)0xDEAD10CC Wrote: [\[CITE\]](#) You're assuming they all use SQL, and certain false assumptions are also being made on your part here to include XSS vulnerabilities also. :/ I can guarantee that my RESTful Philips Hue system API is not vulnerable to either of those. That's not a universally true statement that you've made, only in a handful of cases.

@OP - You could look at building an API using OAuth 2.0 with Two factor authentication, and have a RESTful back end for a scalable platform agnostic solution; HTTP requests and XML and/or JSON.

Of course its not universally true, dipshit. I never claimed all APIs use SQL and they are all vulnerable to SQL attacks or XSS attacks. Why do you always nit pick on everything I say?

(May 25, 2017 09:13 PM)severos Wrote: [\[CITE\]](#) I understand the SQL part, but how would they be vulnerable to XSS??? didn't XSS happen only when rendering pages? how would that affect JSON objects for example??

If you have an API with a front end, or a registration panel, or anything a user interacts with, then it can be vulnerable to XSS.

severos - May 26, 2017, 9:05 am

(May 26, 2017 07:52 AM)Ninja Wrote: [\[CITE\]](#) If you have an API with a front end, or a registration panel, or anything a user interacts with, then it can be vulnerable to XSS.

I see, so I'll need to filter/escape whatever string I get from users? is this the only solution to use? or there are hidden tricks that bypass this and will need other solutions??

+Haze - May 26, 2017, 11:40 am

Just use a good framework and you'll be good on most things, I'm not so sure about .NET frameworks but I know in PHP, frameworks like Laravel do most of the heavy lifting for you including security.

Ninja - May 26, 2017, 7:14 pm

(May 26, 2017 09:05 AM)severos Wrote: [\[CITE\]](#) I see, so I'll need to filter/escape whatever string I get from users? is this the only solution to use? or there are hidden tricks that bypass this and will need other solutions??

I think (but Im no expert) that with url encoding (UTF8 or whatever it is called) it will be fine.

0xDEAD10CC - May 26, 2017, 7:17 pm

(May 26, 2017 07:52 AM)Ninja Wrote: [\[CITE\]](#) Of course its not universally true, dipshit. I never claimed all APIs use SQL and they are all vulnerable to SQL attacks or XSS attacks. Why do you always nit pick on everything I say?

If you have an API with a front end, or a registration panel, or anything a user interacts with, then it can be vulnerable to XSS.

You clearly did claim it by your general statement about API's being vulnerable to both SQL and XSS. All you said was "API's are vulnerable to_ and ____". You didn't say "some" or provide any further context to not suggest that you were talking about it as a universal thing; basic literacy.

And if you know what you're doing... <https://msdn.microsoft.com/en-us/library/ff649310.aspx>

The same thing applies to SQL vulnerabilities which are JUST as easy to avoid.

Ninja - May 28, 2017, 8:26 am

(May 26, 2017 07:17 PM)0xDEAD10CC Wrote: [\[CITE\]](#) You clearly did claim it by your general statement about API's being vulnerable to both SQL and XSS. All you said was "API's are vulnerable to _ and ____". You didn't say "some" or provide any further context to not suggest that you were talking about it as a universal thing; basic literacy.

And if you know what you're doing... <https://msdn.microsoft.com/en-us/library/ff649310.aspx>

The same thing applies to SQL vulnerabilities which are JUST as easy to avoid.

Are you retarded? In no way does that mean ALL apis.

Stop misinterpreting things I say fucking retard.

0xDEAD10CC - May 28, 2017, 4:41 pm

(May 28, 2017 08:26 AM)Ninja Wrote: [\[CITE\]](#) Are you retarded? In no way does that mean ALL apis.

Stop misinterpreting things I say fucking retard.

Maybe if you wrote proper english you wouldn't have to become so hostile when people point things out. You're acting foolish here but you obviously need to re-visit preschool English, that's exactly what it reads.

>> "APIs are vulnerable to SQL injection attacks, and XSS attacks as well"

It's the difference between "apples are red" and "some apples are red". Use some common sense here and maybe you would actually learn. ?

Ninja - May 28, 2017, 7:43 pm

(May 28, 2017 04:41 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Maybe if you wrote proper english you wouldn't have to become so hostile when people point things out. You're acting foolish here but you obviously need to re-visit preschool English, that's exactly what it reads.

>> "APIs are vulnerable to SQL injection attacks, and XSS attacks as well"

It's the difference between "apples are red" and "some apples are red". Use some common sense here and maybe you would actually learn. ?

Its a matter of speech or however you say it.

If I say "politicians are corrupt" do you think I mean all politicians over the world are corrupt?

Its a common saying "grass is green". I saw yellow grass before. Its not green. You going to correct everyone every saying "grass is green"?

I am sorry for not being a native English speaker and not using proper grammar and whatever on an online forum.

Please do me a favor and go over every single thread in this forums as I have seen a LOT more people speaking even more broken English than me in this forum.

I never see you correcting them... how strange...

severos - May 28, 2017, 9:26 pm

0xDEAD10CC and Ninja, would you guys mind not to turn this thread into a fight please? you can fight all you want in your PMs.

Anyone got more resources to share?

0xDEAD10CC - May 29, 2017, 12:08 pm

(May 28, 2017 07:43 PM)Ninja Wrote: [\[CITE\]](#) Its a matter of speech or however you say it.

If I say "politicians are corrupt" do you think I mean all politicians over the world are corrupt?

Its a common saying "grass is green". I saw yellow grass before. Its not green. You going to correct everyone every saying "grass is green"?

I am sorry for not being a native English speaker and not using proper grammar and whatever on an online forum.

Please do me a favor and go over every single thread in this forums as I have seen a LOT more people speaking even more broken English than me in this forum.

I never see you correcting them... how strange...

Why would I correct someone who speaks bad English if they can at least state their sentences properly? It's not about poor spelling and grammar here for the most part; they are easier to dismiss in comparison to a contextually false statement when OP is looking for answers, not your semi-applicable opinions.

Seeing that not all grass is green is much easier than determining what vulnerabilities API's have especially for a beginner that doesn't have much insight into them (which is probably the reason why he's asking about it in the first place). I don't know why you're having such a hard time with comprehension here. Look at the bigger picture.

I'll remember you as the guy who tried to argue about using .NET 2.0 for older machines like Win95 even though it doesn't support the .NET framework. You're definitely just stubborn.

(May 28, 2017 09:26 PM)severos Wrote: [\[CITE\]](#) 0xDEAD10CC and Ninja, would you guys mind not to turn this thread into a fight please? you can fight all you want in your PMs.

Anyone got more resources to share?

You've been given many examples. Look through MSDN being a large resource for .NET. If there is something you see which has potential to be exploited, then do some more research on that area of your API. Unless you're building a huge API with several layers and different endpoints, I'm not sure what else you're looking for. You haven't even explained what kind of API you're looking to build or what you'll be using it for. For shooting in the dark, I think you have enough resources by now. :/

You should have read ubbelol's post by now: "This is such a wide question it's impossible to answer" - You need to provide more information. Your question is about as vague as "what is the best footwear?". Footwear for hiking? A particular sport? ?

Ninja - May 29, 2017, 9:21 pm

(May 29, 2017 12:08 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Why would I correct someone who speaks bad English if they can at least state their sentences properly? It's not about poor spelling and grammar here for the most part; they are easier to dismiss in comparison to a contextually false statement when OP is looking for answers, not your semi-applicable opinions.

Seeing that not all grass is green is much easier than determining what vulnerabilities API's have especially for a beginner that doesn't have much insight into them (which is probably the reason why he's asking about it in the first place). I don't know why you're having such a hard time with comprehension here. Look at the bigger picture.

I'll remember you as the guy who tried to argue about using .NET 2.0 for older machines like Win95 even though it doesn't support the .NET framework. You're definitely just stubborn.

I met lots and lots of guys like you and eventually they all get bored of their superiority complex and see what dicks they really were.

I'll give you some time.

ntisback - May 29, 2017, 9:43 pm

ninja you're fucking retarded

Bud_Banshee - May 30, 2017, 6:51 am

I cant say this enough, use IDENTITY SERVER 4!

It may take you some time to get your head around the concept but the advantages are huge.

iNCEPTION_V - May 30, 2017, 8:03 am

(May 29, 2017 09:43 PM)ntisback Wrote: [\[CITE\]](#) ninja you're fucking retarded

Nahh ninja knows his stuff one of the most active users in the .net section.

0xDEAD10CC - May 30, 2017, 6:36 pm

(May 30, 2017 08:03 AM)iNCEPTION_V Wrote: [\[CITE\]](#) Nahh ninja knows his stuff one of the most active users in the .net section.

I'll leave this here:

Spoiler [\(Click to View\)](#)

<https://hackforums.net/showthread.php?tid=5599849&pid=54659455#pid54659455>

>> Assault: seems the other way. why the hell would any company want to use .net 2?

>> Ninja: Think about anything that runs on a terminal or whatever. Self-checkout at a supermarket. ATM. Most run on old windows versions and the software should be ready to deploy instantly without much tinkering. Or old people who still use a single core pentium with 1GB RAM and Windows 95 or whatever.

<https://msdn.microsoft.com/en-us/library/ms973853.aspx>

Quote:The first thing to notice is that the .NET Framework will not run at all on Windows 95. This is consistent with other Microsoft® products like Microsoft® Office XP that also do not support Windows 95.

Truly inspiring knowledge he has on .NET. ? This thread is consistent with the last - he simply can't admit when he is wrong even though the evidence is right in front of him.

Ninja - May 30, 2017, 7:51 pm

(May 30, 2017 06:36 PM)0xDEAD10CC Wrote: [\[CITE\]](#) I'll leave this here:

Spoiler [\(Click to View\)](#)

<https://hackforums.net/showthread.php?tid=5599849&pid=54659455#pid54659455>

>> Assault: seems the other way. why the hell would any company want to use .net 2?

>> Ninja: Think about anything that runs on a terminal or whatever. Self-checkout at a supermarket. ATM. Most run on old windows versions and the software should be ready to deploy instantly

without much tinkering. Or old people who still use a single core pentium with 1GB RAM and Windows 95 or whatever.

<https://msdn.microsoft.com/en-us/library/ms973853.aspx>

Truly inspiring knowledge he has on .NET. ? This thread is consistent with the last - he simply can't admit when he is wrong even though the evidence is right in front of him.

So because Windows 95 doesn't support .NET (and it was an exaggerated example) my whole argument is invalid? My point still stands. One fault in an EXAMPLE doesn't disprove my statement.

0xDEAD10CC - May 30, 2017, 8:54 pm

(May 30, 2017 07:51 PM)Ninja Wrote: [\[CITE\]](#) So because Windows 95 doesn't support .NET (and it was an exaggerated example) my whole argument is invalid? My point still stands. One fault in an EXAMPLE doesn't disprove my statement.

Yes because you were explaining why somebody would want .NET 2.0 for supporting a particular operating system when you clearly knew nothing about the minimum supported .NET frameworks on each Windows OS version... Lol, I can't believe you're even willing to argue this, now you claim it to be an exaggerated example to somehow justify it. Are you ever not stubborn enough to admit you're wrong about something I wonder? :/ I'm sure many people who are reading this are laughing inside.

You basically made the statement that you would use .NET 2.0 to support Windows 95. You have an excuse for everything though don't you?

- Not a native English speaker, but I don't criticize other people on their English apparently, and for some reason you're still willing to argue English semantics with me even though you've claimed your English is not good.

- Windows 95 being an exaggerated example when you used it as an example for why someone should use .NET 2.0 somehow doesn't make your point about .NET 2.0 invalid. (We did provide tables that prove v3.5 is pretty much all the support you'd ever need if not v3.0.)

I wonder what's next lol. I'm done here though, I have no more interest arguing with a kid who claims to have experience that is realistically non-existent out in the real world. When you talk to the experts, and learn a few things, then I'll talk.

This thread is meaningless until OP replies with more details anyways, as many members before me have also stated.