

Forum: [Hack Forums](#)

Thread: [AI-assisted / agent pentesting && example: CVE-2025-6554 PoC by mistymntncop](#)

Hackers - September 19, 2025, 8:18 pm

Do you think AI can be used like this in the future to help with pentesting, improving security, and keeping us all safer?

I think it can definitely be used

This is from an AI agent

Chat GPT recommended this PoC as a way to make sure you are not affected by this V8 issue.

The dev's note says how you can test on your patched system safely to ensure this won't be a concern for you!

Details:

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

[nvd.nist.gov /vuln/detail/CVE-2025-6554](https://nvd.nist.gov/vuln/detail/CVE-2025-6554)

gist.github.com/mistymntncop/37c652c2bf7373b4aa33bb50f52ee0f2

[web.archive.org](https://web.archive.org/web/20250904123249/https://gist.github.com/mistymntncop/37c652c2bf7373b4aa33bb50f52ee0f2/raw/bc897b44cadd072ecd43e2c8b2fbae1c6f75ef5a/CVE-2025-6554%20POC.js)

[/web/20250904123249/https://gist.github.com/mistymntncop/37c652c2bf7373b4aa33bb50f52ee0f2/raw/bc897b44cadd072ecd43e2c8b2fbae1c6f75ef5a/CVE-2025-6554%20POC.js](https://web/20250904123249/https://gist.github.com/mistymntncop/37c652c2bf7373b4aa33bb50f52ee0f2/raw/bc897b44cadd072ecd43e2c8b2fbae1c6f75ef5a/CVE-2025-6554%20POC.js)

[pastebin.com /raw/DBq4QG4y](https://pastebin.com/raw/DBq4QG4y)

[mega.nz /file/Qu1wkApQ#sKpyPzmiM5X01fUdk6T7mksEts5O-XsvKwU3zatw6TM\[/code\]](https://mega.nz/file/Qu1wkApQ#sKpyPzmiM5X01fUdk6T7mksEts5O-XsvKwU3zatw6TM[/code])

I do not know exactly what the script will do on your browser / OS, so use at your own risk to test your own system. The software developer says they have provided a way you can prove if your system is updated or not, like a proof for CVE-2025-6554.

What do you think of this specific V8 issue, and do you have any thoughts about AI cybersecurity agents/assistants?

ttbr0 - September 19, 2025, 8:22 pm

this script wont do anything dramatic to your browser. it wont even run as is but if you know any js at

all you can fix the small problem. this is just a poc to trigger the vulnerability, a full exploit needs so much more work.

Hackers - September 19, 2025, 8:27 pm

(Sep 19, 2025 08:22 PM)ttbr0 Wrote: [\[CITE\]](#) this script wont do anything dramatic to your browser. it wont even run as is but if you know any js at all you can fix the small problem. this is just a poc to trigger the vulnerability, a full exploit needs so much more work.

I hear you - I was editing the thread for few minutes. I meant to mostly focus on the AI agent aspect of searching the starting CVEs, identifying all details accurately, and finding related resources across the web.

Modern Chrome is 140x anyways, this is older

MadScientist - September 19, 2025, 8:30 pm

AI definitely will be useful in future pentesting, I'm sure we'll start seeing pentesting frameworks with build in AI. I've heard someone mention various backdoors/RAT's that have implemented AI but didn't see and solid examples.

Do you know what AI framework that is running on? Going to try to find a jailbroken AI framework this weekend, since my last ChatGPT update it's got even more strict >.<

ttbr0 - September 19, 2025, 8:33 pm

(Sep 19, 2025 08:27 PM)nodes Wrote: [\[CITE\]](#) I hear you - I was editing the thread for few minutes. I meant to mostly focus on the AI agent aspect of searching the starting CVEs, identifying all details accurately, and finding related resources across the web.

Modern Chrome is 140x anyways, this is older

i would say ai is just a faster way to google things. so much of the work still needs to be manual in the way you perform recon and then parse the output to start doing anything. the best you could do is feed all your tooling output into an ai and have it reply with some recommendations on the next steps. it will have lots of difficulty for any custom applications. like everything else, ai is just there to make the easy boring tasks go much quicker but the main bulk of the work always has been and will be enumerating edge cases. ai wont be able to help with a lot of that. and dont even think about pointing an agent at a production application or it could flood it inappropriately.

happy to be proven wrong.

Hackers - September 19, 2025, 8:52 pm

(Sep 19, 2025 08:33 PM)ttbr0 Wrote: [\[CITE\]](#) i would say ai is just a faster way to google things. so much of the work still needs to be manual in the way you perform recon and then parse the output to start doing anything. the best you could do is feed all your tooling output into an ai and have it reply with some recommendations on the next steps. it will have lots of difficulty for any custom applications. like everything else, ai is just there to make the easy boring tasks go much quicker but the main bulk of the work always has been and will be enumerating edge cases. ai wont be able to help with a lot of that. and dont even think about pointing an agent at a production application or it could flood it inappropriately.

happy to be proven wrong.

I didn't have to do anything and it searched all over the web for multiple CVEs. It found multiple test scripts just like this one that can then be used , modified, tweaked.

You can start doing this with a \$20/mo sub to gpt:

<https://mega.nz/file/Qu1wkApQ#sKpyPzmiM5X01fUdk6T7mksEts5O-XsvKwU3zatw6TM>

(video)

It went to over 30 different links

The key part here is that it was able to identify a specific code snippet corresponding to a POC, from a CVE advisory & successfully researched all CVEs and provided detailed paragraphs of the most important info, with works cited links.

I think it's been far proven that LLMs are capable of taking this type of information and starting code to create new test scripts, and you can run them against a test machine and feed errors back to the LLM.

Recursive coding & deployment via AI/LLM is pretty common & pentesting / cybersecurity is a huge market. Definitely recommend getting into it.

I'm surprised you are still so hesitant about AI & talking like we still "chat" with LLMs manually

I could fire up a dozen of these and have it analyze my specific website, app, or software, etc for all known vulns across all protocols

You can even have multiple agents talking with each other, performing different tasks.

AI is already here mate. Lol just saying. I truly hope you give things a go soon.

ttbr0 - September 19, 2025, 9:17 pm

(Sep 19, 2025 08:52 PM)nodes Wrote: [\[CITE\]](#) I didn't have to do anything and it searched all over the web for multiple CVEs. It found multiple test scripts just like this one that can then be used , modified, tweaked.

It cost me \$0 extra (\$20/mo) to do this, and I could do this daily, hourly, etc.

It went to over 30 different links

The key part here is that it was able to identify a specific code snippet corresponding to a POC, from a CVE advisory

I think it's been far proven that LLMs are capable of taking this type of information and starting code to create new test scripts, and you can run them against a test machine and feed errors back to the LLM.

Recursive coding & deployment via AI/LLM is pretty common & pentesting / cybersecurity is a huge market. Definitely recommend getting into it.

I'm surprised you are still so hesitant about AI & talking like we still "chat" with LLMs manually.....

I could fire up a dozen of these and have it analyze my specific website for all known vulns across all protocols.....

AI is already here mate. Lol just saying. I truly hope you give things a go soon.

you literally just said what i did. its google on steroids. and what you are describing is nessus. vuln scanning tools have existed for decades and they are not pentesting. basically what you have told me is you have never done a proper full pentest, let alone pentesting over multiple different environments and applications. i might even go as far as to say that you do not understand core

principles of hacking. llms do not have enough information about all the different ways a custom application behaves or interacts with unforeseen edge cases that only a human can experiment with and test. this is not coding. this is not vuln scanning. this is not googling for well defined or known domain knowledge. do not fall prey to the silent minority where businesses claim ai is the end all be all so they can justify more profits. you are a victim of marketing and hype. you are a victim of ignorance.

Hackers - September 19, 2025, 9:26 pm

(Sep 19, 2025 09:17 PM)ttbr0 Wrote: [\[CITE\]](#) you literally just said what i did. its google on steroids. and what you are describing is nessus. vuln scanning tools have existed for decades and they are not pentesting. basically what you have told me is you have never done a proper full pentest, let alone pentesting over multiple different environments and applications. i might even go as far as to say that you do not understand core principles of hacking. llms do not have enough information about all the different ways a custom application behaves or interacts with unforeseen edge cases that only a human can experiment with and test. this is not coding. this is not vuln scanning. this is not googling for well defined or known domain knowledge. do not fall prey to the silent minority where businesses claim ai is the end all be all so they can justify more profits. you are a victim of marketing and hype. you are a victim of ignorance.

Yeah, you're not really getting it man

You have been parroting the same nonsense for over a year...

You're going to fall behind & become unemployable as a coder if you can't get on the same page. Sorry, I hate to say it, but we see people like you and they are being left behind

Either learn the tools and stop pretending it can only act as google, or someone else will take your place.

Agent workflows can write code 100x faster & better than 99.99% of the users on this forum, including you and me.

ttbr0 - September 19, 2025, 9:42 pm

(Sep 19, 2025 09:26 PM)nodes Wrote: [\[CITE\]](#) Yeah, you're not really getting it man

You have been parroting the same nonsense for over a year...

You're going to fall behind & become unemployable as a coder if you can't get on the same page. Sorry, I hate to say it, but we see people like you and they are being left behind

Either learn the tools and stop pretending it can only act as google, or someone else will take your place.

Agent workflows can write code 100x faster & better than 99.99% of the users on this forum, including you and me.

neither are you. you do not know what i do. coding serves only a fraction of what i do. do not be arrogant and judge what you do not understand.

Hackers - September 19, 2025, 10:00 pm

(Sep 19, 2025 09:42 PM)ttbr0 Wrote: [\[CITE\]](#) neither are you. you do not know what i do. coding serves only a fraction of what i do. do not be arrogant and judge what you do not understand.

Same here, I'm not being arrogant, and not judging what I do not understand. If you can't even use Google to understand what real companies & real engineers are doing with AI/LLM/agentic workflows, then you probably shouldn't claim to have industry knowledge.

The fact that I am even having to teach you this is weird man, not going to lie. It's weird.

Unless you could create a mobile app for android, a mobile app for ios, a windows software, a mac software, a linux software, a website, and all inter-connected, for a real use case in the next 1-2 days, alone. If you can go do that, make a custom software/app/build on every single possible platform, in the next 8-16 hours (2 business days), then I'll say that you are the 1 guy who can do it. Bug-free, at least 1-2 core features, user auth / licensing, etc. All of it.

When you can actually come close to that, I'll take you at your word

Agentic workflows are not some BS marketing term. Not only can you finetune, train, and have 1 agent run its own recursive functions... You can have as many as you want, working on separate projects, or 1 project, who cares

You can have them research, create designs (figma, whatever format), write in any language, run test scripts, etc

Not only that, they install packages on our own machines, in whatever OS we want! We can run any command ever, and they have whitelists for safety. It's perfect - they commit to git, can fork for similar projects, etc.

The future is really bright, this is only the beginning.

I feel like you're just not in the industry man, ngl. I think you are posing. You have said this kind of shit for too long, you clearly have little to no experience with AI.

I'm not arrogant, you're just literally so far off the mark that it's really hard to take you seriously. It almost feels like you're purposefully trolling me, there's just no way tbh. Idk, or you're posing and actually don't know ..

it's really not personal bro... You're just kind of acting strange. I can't tell if you are trolling or honestly just don't know, and that's not on me.

ttbr0 - September 19, 2025, 10:12 pm

(Sep 19, 2025 10:00 PM)nodes Wrote: [\[CITE\]](#) Same here, I'm not being arrogant, and not judging what I do not understand. If you can't even use Google to understand what real companies & real engineers are doing with AI/LLM/agentic workflows, then you probably shouldn't claim to have industry knowledge.

The fact that I am even having to teach you this is weird man, not going to lie. It's weird.

Unless you could create a mobile app for android, a mobile app for ios, a windows software, a mac software, a linux software, a website, and all inter-connected, for a real use case in the next 1-2 days, alone. If you can go do that, make a custom software/app/build on every single possible platform, in the next 8-16 hours (2 business days), then I'll say that you are the 1 guy who can do it. Bug-free, at least 1-2 core features, user auth / licensing, etc. All of it.

When you can actually come close to that, I'll take you at your word

Agentic workflows are not some BS marketing term. Not only can you finetune, train, and have 1 agent run its own recursive functions... You can have as many as you want, working on separate projects, or 1 project, who cares

You can have them research, create designs (figma, whatever format), write in any language, run test scripts, etc

Not only that, they install packages on our own machines, in whatever OS we want! We can run any command ever, and they have whitelists for safety. It's perfect - they commit to git, can fork for similar projects, etc.

The future is really bright, this is only the beginning.

I feel like you're just not in the industry man, ngl. I think you are posing. You have said this kind of shit for too long, you clearly have little to no experience with AI.

I'm not arrogant, you're just literally so far off the mark that it's really hard to take you seriously. It almost feels like you're purposefully trolling me, there's just no way tbh. Idk, or you're posing and actually don't know ..

it's really not personal bro... You're just kind of acting strange. I can't tell if you are trolling or honestly just don't know, and that's not on me.

this thread is not coding or software engineering. it is about pentesting. why are you trying to apply logic to two different domains? you dont even understand what pentesting is fundamentally and you are trying to jam in ai as if you know understand how it fits in.

Hackers - September 19, 2025, 10:32 pm

(Sep 19, 2025 10:12 PM)ttbr0 Wrote: [\[CITE\]](#) this thread is not coding or software engineering. it is about pentesting. why are you trying to apply logic to two different domains? you dont even understand what pentesting is fundamentally and you are trying to jam in ai as if you know understand how it fits in.

It's not two different concepts, I just told you that we can have agents run any command line they want...

This isn't a hard concept, nor is it new:

You can have an LLM trigger functions, and run anything you want. You can hook into your OS, VMs, via SSH, whatever you want. doesn't matter, it can all hook right into the agent flows & task lists (usually recursive to a point of completion, with quit rules as needed).

You can give it an IP, a domain, whatever you want.

You can give it a file on your computer, a program if you want to run and analyze it.

Anything that you can do on a computer, an agent can trigger. You can get a custom workflow up & running even with a basic LLM if you know what you're doing. Just label your funcs properly, get a good input/output format for triggers, and you're good. Things are a lot more advanced now, but anyone can pentest automatically.

You can literally setup whatever you need to do man. Pentesting with agents is not much different than writing software with agents. It's just a different workflow, different functions, triggers, pre-training examples, and sets of logic. You can hook that into whatever you want, whether it's generating new code, running a program, using CLI for anything you want (and having ability to find, download, and install any deps you need), etc.

You can run any scanner you want, D/DoS, bruteforce, known web paths, ports, sql/i... whatever

you want.

You just create labels / func wrappers, and setup a small function that maps the LLM response to an actual OS' command line.