Generalist Web Agents: From Perception to Planning

Boyuan Zheng 04/04/2025



Outline

1 Introduction

2 Environment Perception

3 Planning

4 Self-Improvement

Outline

1 Introduction

2 Environment Perception

3 Planning

4 Self-Improvement

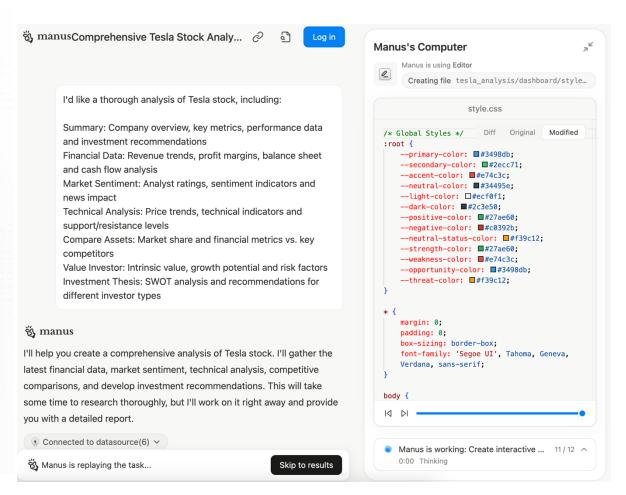
Coding Agent

Leave it to Manus

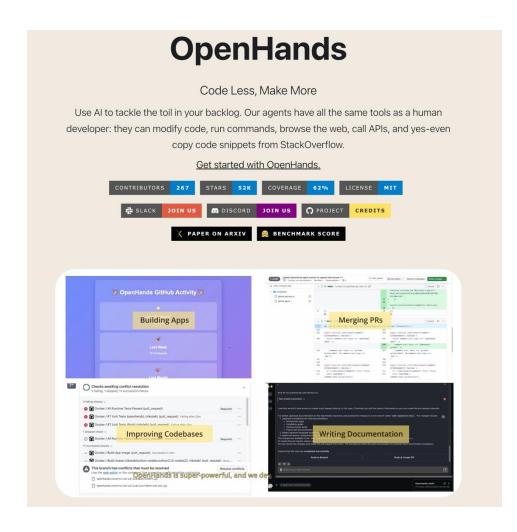
Manus is a general Al agent that bridges minds and actions: it doesn't just think, it delivers results. Manus excels at various tasks in work and life, getting everything done while you rest.

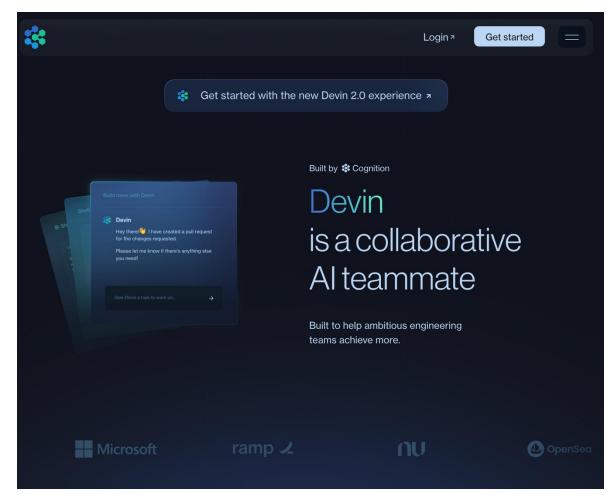


Try Manus



Coding Agent



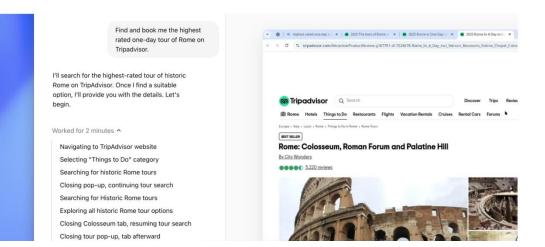


Web Agent

Introducing Operator

A research preview of an agent that can use its own browser to perform tasks for you. Available to Pro users in the U.S.

Go to Operator 7

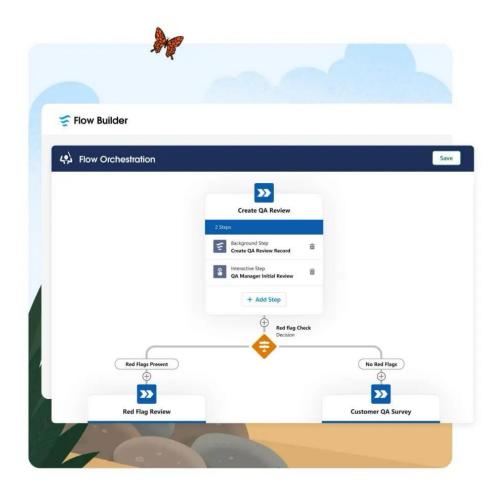


Introducing computer use, a new Claude 3.5 Sonnet, and Claude 3.5 Haiku

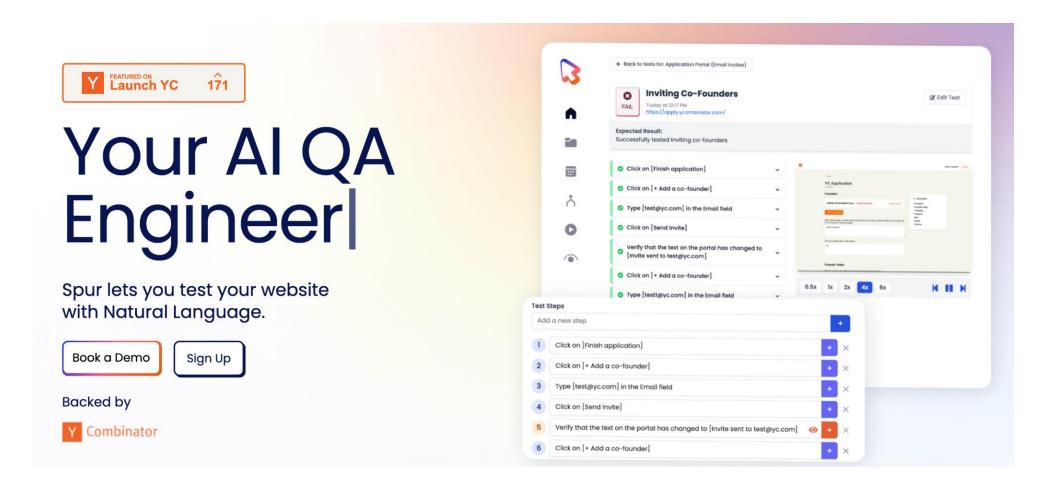
Oct 22, 2024 • 5 min read



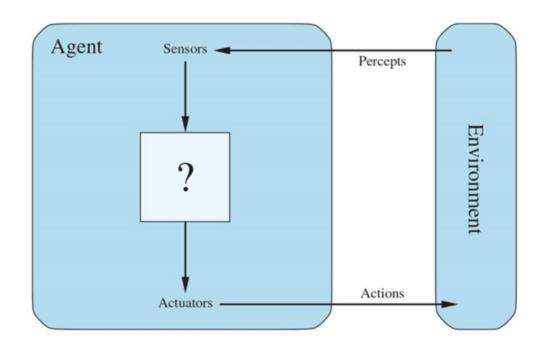
Web Agent Use Case: Process Automation



Web Agent Use Case: Auto-Testing



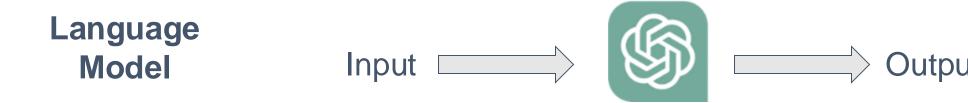
Why Agents Again?



"An **agent** is anything that can be viewed as perceiving its **environment** through **sensors** and acting upon that environment through **actuators**"

— Russel & Norvig, AI: A Modern Approach

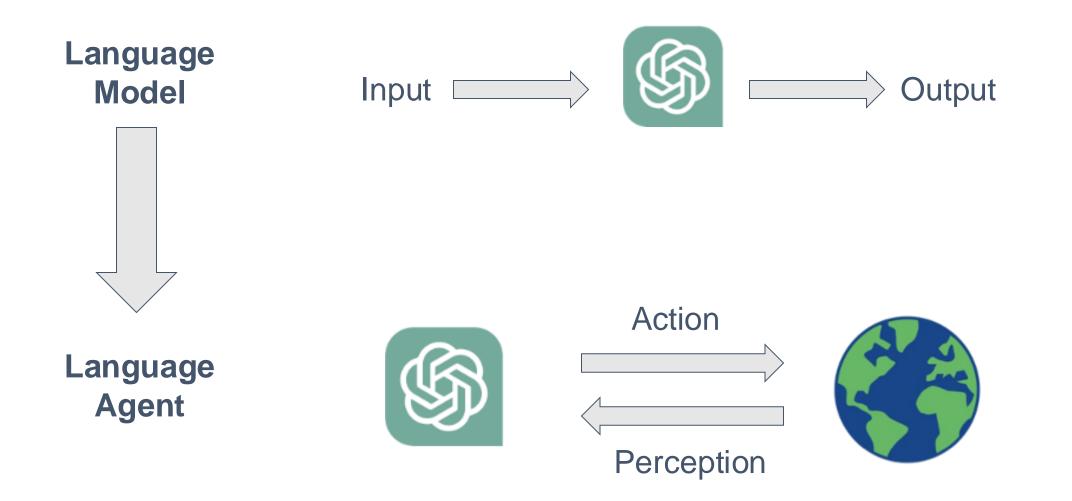
From Language Model to Language Agent



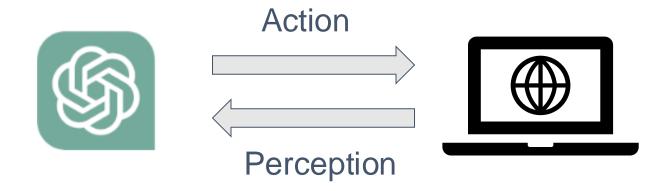
Opportunities of contemporary Al Agent with an integrated LLM:

- Environment Perception
- Generalist agent with language
- Reasoning for better acting

From Language Model to Language Agent



Web Agent



Web as playgrounds for agent research

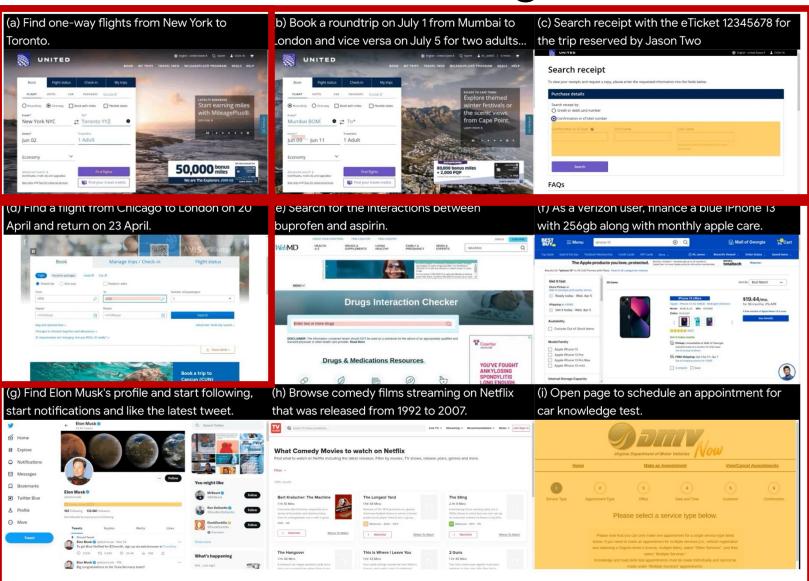
- Open, Diverse, Complex Environment
- Highly Structured Environment
- Low Cost
- Lower Safety Concern

Generalist Web Agent

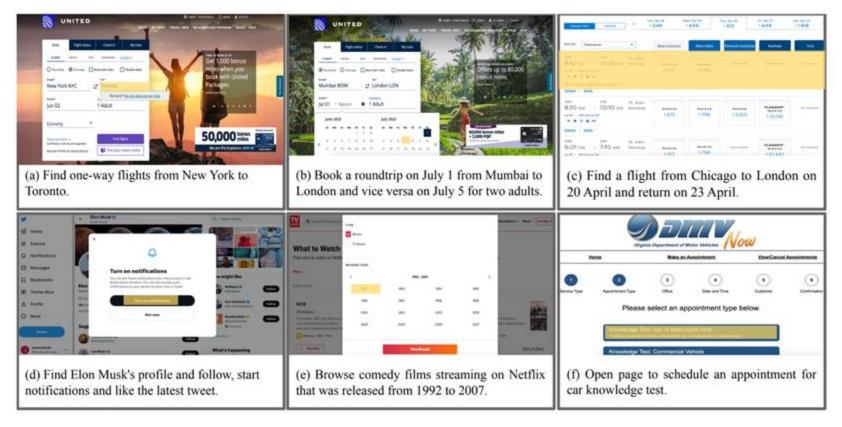
Cross-Task

Cross-Website

Cross-Domain

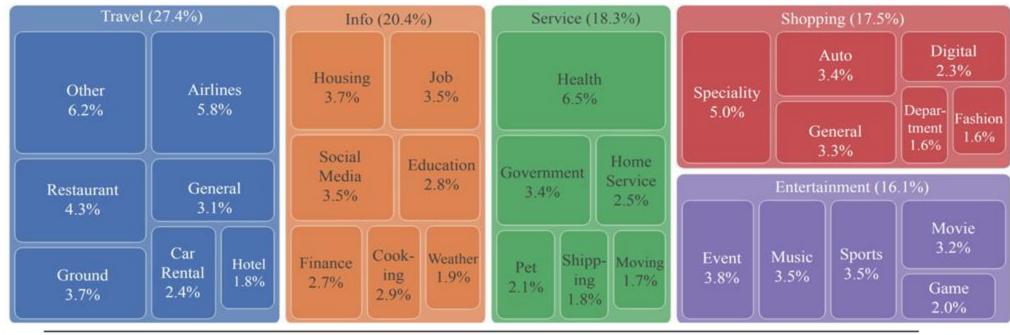


Why a Challenging Mission?



- User tasks: diverse, complex, requiring long-horizon planning
- Real-world websites: complex, dynamic
- Generalize to unseen websites/domains

Mind2Web: A Generalist Web Agent Benchmark



	# Dom.	# Env.	Env. Type	Avg. # Elements	# Tasks	Task Info.	Avg. # Actions
MiniWoB++ [22]	-	100	Simplified mobile websites	28	100	Low-level	3.6
WebShop [40]	1	1	Simplified shopping websites	38	12,000 products	High-level	11.3
RUSS [39]	_	22	Real-world websites	801	80	High & low	5.4
PixelHelp [21]	4	4	Mobile apps	_	187	High & low	-
META-GUI [35]	6	11	Mobile apps	79	1,125 dialogues	High-level	4.3
MoTIF [5]	15	125	Mobile apps	188	756	High & Low	4.4
MIND2WEB	5/31	137	Real-world websites	1,135	2,350	High-level	7.3

A task example in Mind2Web

Task Description:

Show me the reviews for the auto repair business closest to 10002.

Action Sequence:

	Target Element	Operation
1.	[searchbox] Find	TYPE: auto repair
2.	[button] Auto Repair	CLICK
3.	[textbox] Near	TYPE: 10002
4.	[button] 10002	CLICK
5.	[button] Search	CLICK
6.	[switch] Show BBB Accredited only	CLICK
7.	[svg]	CLICK
8.	[button] Sort By	CLICK
9.	[link] Fast Lane 24 Hour Auto Repair	CLICK
10.	[link] Read Reviews	CLICK

Webpage Snapshots:

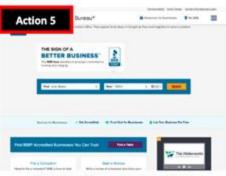










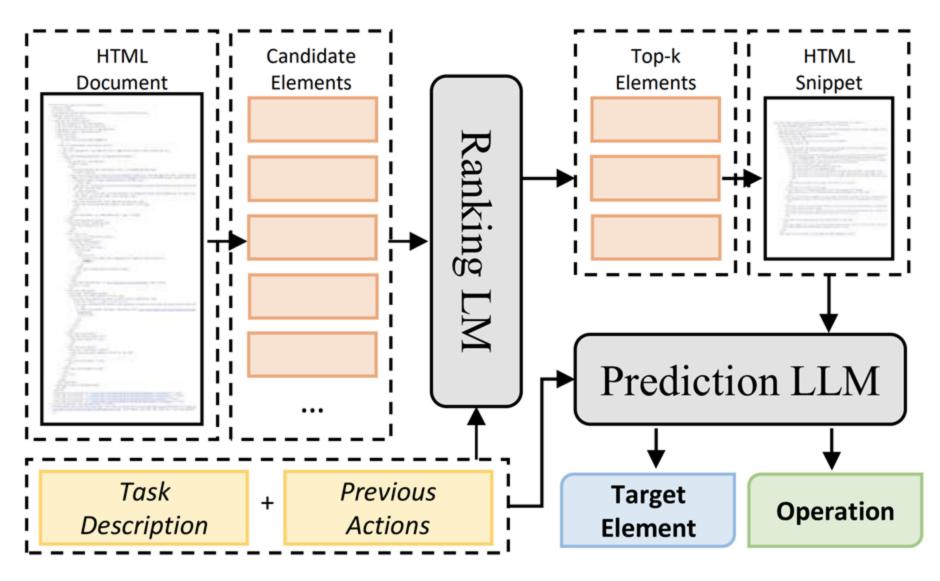


<button>Search</button>



Read Reviews

The first framework for building a generalist web agent



Our Proposed MindAct

MindAct

Environment Representation: Simplified HTML

```
Direct Generation
<html> <form id=0> <div meta="navigation; sitelinks">
                                                                                            Element: <select id=1 meta="Size; Select a Size">
 <a> Collect Renaissance </a> <a> Shop Le Meridien
                                                                                            Action: SELECT
</a> <a> Westin Store </a> <a> Sheraton Store </a>
                                                                                            Value: Queen
 </div> ... <div> <select id=1 meta="Size; Select a
Size"> <span meta=tablist> <button id=2 meta="button;</pre>
tab"> Description </button> ... <a id=3 meta="Shop
                                                                                                      Prediction LLM
Feather & Down Pillow"> <img meta="Product Feather &
Down Pillow">  <a> California Privacy Rights </a>
<a>> Privacy Statement </a> <a>> Terms of Use </a> <a
id=4> Loyalty Terms </a> ...
                                                                   Please select from the following choices (If the correct action is not in the page
Based on the HTML webpage above, try to complete the following
                                                                   above, please select A. 'None of the above'):
                                                                                                                                                  Action: SELECT
task:
                                                                                                                                                  Value: Queen
Task: Search for queen-size pillow protectors from the Marriot
                                                                        None of the above
                                                                   Α.
shop, and if found, add two pieces to the cart and checkout.
                                                                        <form id=0> <div meta="navigation; sitelinks">  <a> Collect
                                                                        Renaissance </a> <a> Shop Le Meridien </a> <a> Westin Store </a> <a>
Previous actions:
[button] Special Offers -> CLICK
                                                                        <select id=1 meta="Size: Select a Size">
[link] Shop Marriott Opens a new window -> CLICK
                                                                        <button id=2 meta="button; tab"> Description </button>
[menuitem] category pillows -> CLICK
                                                                        <a id=3 meta="Shop Feather & Down Pillow"> <img meta="Product Feather"
[span] Pillow Protector -> CLICK
                                                                        & Down Pillow"> <span> Feather & Down Pillow </span> </a>
What should be the next action?
                                                                        <a id=4> Loyalty Terms </a>
                                                                                                                                                         Multichoice
```

Results of MindAct

	Cross-Task			Cross-Website				Cross-Domain				
	Ele. Acc	Op. F1	Step SR	SR	Ele. Acc	Op. F1	Step SR	SR	Ele. Acc	Op. F1	Step SR	SR
Classification	26.8	_	_	_	21.6	_	_	_	24.5	_	_	
Generation	20.2	52.0	17.5	0.0	13.9	44.7	11.0	0.0	14.2	44.7	11.9	0.4
MINDACT												
w/ Flan-T5 _B	43.6	76.8	41.0	4.0	32.1	67.6	29.5	1.7	33.9	67.3	31.6	1.6
w/ Flan-T5 _L	53.4	75.7	50.3	7.1	39.2	67.1	35.3	1.1	39.7	67.2	37.3	2.7
w/ Flan-T5 _{XL}	55.1	75.7	52.0	5.2	42.0	65.2	38.9	5.1	$\boldsymbol{42.1}$	66.5	39.6	2.9
w/ GPT-3.5		-56.6	17.4	0.8	19.3	-48.8	-16.2	0.6	$-\bar{2}1.6^{-}$	52.8	18.6	$\bar{1.0}$
w/ GPT-4*	41.6	60.6	36.2	2.0	35.8	51.1	30.1	2.0	37.1	46.5	26.4	2.0

Step SR: success rate at each step

SR: Success rate for the whole task

Offline evaluation setting

GPT-4 (3-shot) is close to fine-tuned Flan-T5 models

Results of MindAct

	Cross-Task			Cross-Website			Cross-Domain					
	Ele. Acc	Op. F1	Step SR	SR	Ele. Acc	Op. F1	Step SR	SR	Ele. Acc	Op. F1	Step SR	SR
Classification	26.8	_	_	_	21.6	_	_	_	24.5	_	_	_
Generation	20.2	52.0	17.5	0.0	13.9	44.7	11.0	0.0	14.2	44.7	11.9	0.4
MINDACT												
w/ Flan-T5 _B	43.6	76.8	41.0	4.0	32.1	67.6	29.5	1.7	33.9	67.3	31.6	1.6
w/ Flan-T5 _L	53.4	75.7	50.3	7.1	39.2	67.1	35.3	1.1	39.7	67.2	37.3	2.7
w/ Flan-T5 _{XL}	55.1	75.7	52.0	5.2	42.0	65.2	38.9	5.1	42.1	66.5	39.6	2.9
w/ GPT-3.5	20.3	-56.6	17.4	0.8	19.3	-48.8	16.2^{-}	$^{-}0.6^{-}$	$-\bar{2}1.6$	52.8	18.6	$-\bar{1}.\bar{0}$
w/ GPT-4*	41.6	60.6	36.2	2.0	35.8	51.1	30.1	2.0	37.1	46.5	26.4	2.0

Step SR: success rate at each step

SR: Success rate for the whole task

Offline evaluation setting

GPT-4 (3-shot) is close to fine-tuned Flan-T5 models, but all models are terrible (2-7% whole task success rate)!

Around six months later ...

Model	C	Cross-Tas	k	Cross-Website			Cross-Domain		
1120001	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR
Supervised Fine-Tuning									
FLAN-T5-XL	57.1	75.7	53.5	43.8	67.7	41.1	41.4	65.9	38.9
BLIP-2-T5-XL	50.1	77.0	47.0	39.4	69.3	37.0	41.2	69.3	38.9
In-Context Learning									
GPT-3.5*	19.4	59.2	16.8	14.9	56.5	14.1	25.2	57.9	24.1
GPT-4*	40.8	63.1	32.3	30.2	61.0	27.0	35.4	61.9	29.7
COGAGENT	$\overline{22.4}$	53.0	$17.\overline{6}$	18.4	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	13.4		-42.0	15.5
	9.7	65.6	8.1	9.1	60.8	7.5	10.9	63.9	8.5
,	21.5	67.7	19.6	17.1	61.3	15.4	20.7	64.3	18.0
•	46.4	73.4	$\boldsymbol{40.2}$	38.0	67.8	$\bf 32.4$	42.4	69.3	36.8
	66.4	79.2	61.9	69.5	78.9	65.0	72.8	73.6	62.1

5~7% gain

Around six months later ...

Model	C	cross-Tas	k	Cross-Website			Cross-Domain		
	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR
Supervised Fine-Tuning									
FLAN-T5-XL	57.1	75.7	53.5	43.8	67.7	41.1	41.4	65.9	38.9
BLIP-2-T5-XL	50.1	77.0	47.0	39.4	69.3	37.0	41.2	69.3	38.9
In-Context Learning									
GPT-3.5*	19.4	59.2	16.8	14.9	56.5	14.1	25.2	57.9	24.1
GPT-4*	40.8	63.1	32.3	30.2	61.0	27.0	35.4	61.9	29.7
CogAgent	22.4	53.0	$17.\overline{6}$	18.4	$4\overline{2}.\overline{2}$	13.4		-42.0	15.5
-	0.7	05.0	0.1	0.1	60.0		10.0	60.0	0.5
	9.7	65.6	8.1	9.1	60.8	7.5	10.9	63.9	8.5
,	21.5	67.7	19.6	17.1	61.3	15.4	20.7	64.3	18.0
•	46.4	73.4	40.2	38.0	67.8	32.4	42.4	69.3	36.8
	66.4	79.2	61.9	69.5	78.9	65.0	72.8	73.6	62.1



	Offline ₀	Offline ₁	Online
FLAN-T5-XL	4.4	24.4	8.9
GPT-4	1.1	12.2	13.3
	3.3	12.2	37.8
	13.3	27.8	51.1

Whole task success rate

So, what did we do?

Model	C	cross-Tas	k	Cro	oss-Webs	ite	Cross-Domain		
	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR	Ele. Acc	Op. F1	Step SR
Supervised Fine-Tuning									
FLAN-T5-XL	57.1	75.7	53.5	43.8	67.7	41.1	41.4	65.9	38.9
BLIP-2-T5-XL	50.1	77.0	47.0	39.4	69.3	37.0	41.2	69.3	38.9
In-Context Learning									
GPT-3.5*	19.4	59.2	16.8	14.9	56.5	14.1	25.2	57.9	24.1
GPT-4*	40.8	63.1	32.3	30.2	61.0	27.0	35.4	61.9	29.7
COGAGENT	$\overline{22.4}$	53.0	$\begin{bmatrix} -17.ar{6} \end{bmatrix}$	18.4	$4\overline{2}.\overline{2}$	13.4	$\frac{1}{20.6}$	-42.0^{-}	15.5
	0.7	CT C	0.1	0.1	60.0	7 -	10.0	62.0	0 5
1	9.7	$65.6 \\ 67.7$	8.1	$9.1 \\ 17.1$	60.8	$7.5 \\ 15.4$	$10.9 \\ 20.7$	63.9	$8.5 \\ 18.0$
	$21.5 \\ 46.4$	73.4	19.6 40.2	38.0	61.3 67.8	32.4	42.4	64.3 69.3	36.8
	66.4	79.2	61.9	69.5	78.9	65.0	72.8	73.6	62.1



	Offline ₀	Offline ₁	Online
FLAN-T5-XL	4.4	24.4	8.9
GPT-4	1.1	12.2	13.3
7	3.3	12.2	37.8
	13.3	27.8	51.1

Whole task success rate

Outline

1 Introduction

2 Environment Perception

3 Planning

4 Self-Improvement

HTML -> Simplified HTML -> Image

```
origin median (cross type (inst/cut-) also-better type (inst/cut-) also-better type (inst/cut-) (installation ( installation (
  -script- $idecamenti_ready(function () ( ShewfesterLink - Function (id) ( 1915)"_stane-inscense").is("reintsible") ( 5("#" - 18).widerTopgle(); ) ); ));
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            100K
                                  -times herby for inner 16-bits inner more connected - connected of the best freek hertale/space-re-/in-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Tokens
                                             -u Mosfor/Name" titler/Madget Youch Assist" velorismer's
name identity professionity (billings/light" clauserflows-Srovacy'se Radget Youch Assist, illinoisme
                                            - only later or province - one characteristic bounds and province and 
             only the design products and the private of the pri
             Budget-Serbalt/images/sorten_secore_geg" style="bender-worth; does bender-style; enlat;" width="7" -- am-/die
   offic classe "model fiche" ide "myllicount" tabledoor "I" relectifulog" arise tabelledop "myllocillatel" arise hiddron' trus' o
             offer persons of the property of the person 
  out classe model-cities ide bit-Mark may the savings of his
 on Classe "mader in-body-copy"-fere 20% on truck restals picked up any day of the week. Available for booking and pick up through December 31, 2013, -/pi-
 -p-To recess this offer, customer must back online at wee-budgettruck.com and 24-hour advance reperied to customer upon confirmation of mental deposit. Offer is subject to availability at participating locations and 24-hour advance reservation required. Offer excluses mental
drop off in the states of South Carolina and Temessee. Offer is based on the US currency. Discount is 2Pk off time and milesge of "The Best Assistate any way by lacetime
and time of year, Taxes, fees, and surcharges are extra. Menter must seet Budget Truck's age, driver and credit requirements, he additional delity surcharge may apply for resters under 24 years of age. Optional products such as desage waters, features products, and other product services may apply and are extra.
 Offer is voic where probabiled by law and has no cash value. Best available rates defined as the lowest publicly available incline to disaper truck continents only.
 Offer is valid for reservations bushed and picked up through December 21, 2019 and must recove by January 12, 2020. The offer and length of the promotion period are subject to change without notice and may be amended, on placed or concelled by Mudget track Mental at any time. - show-makes may vary by pickup date,
     dir class-mentel-footer"- ductor class-"bts bis-cefault-payons pull-right" data-ba-dismiss-"mentel" mediche-"applyCodel" 2005/1/; return folias/"-extremy-Apply 20% dismounts/strong-schollers- schine-bette-
```

HTML -> Simplified HTML -> Image

```
offic backend node 164"33897"
      willy backend node 124" 30800"
        HILLY backend note 104"2030"
          vitiv backend_node_5d+"39581"
               -partners backend node 3d+ 301
                  -tours backerd rode 16-"HILL" type-"(Anys/witz)
                  -ing backerd rade 18" 18318" alto AMP mester discourt, here up to 200"/
            -SIV backend node 1dv*3912550
                wheat backend mode 38+"39520"-Save up to 29+critical
            or backend node ide" DESIST ESPERATE RECE".
               visus backend node (de"19112"-Learn Mares/tox
          vitiv backent note 18**191355**
           ---- backend node 16v*30139*
              to backend note $60"30148" $155ac"Dark 1175 a $510g. Det loading hets, "o
                 -ing backerd note 10-"Hill!" alto"burt lift a thing, Get loading belo," In
               court backend note 10-10055 -bort tift a thing, Get leading help, -/ test-
            or backent code_to-rossor' title-rossory frices's
          HILV Backend_node_lid+"33535"-
              to backend node ide"20100" titles"lend a Fick-Up Truck?"-
                -Ditturn backend_node_ld+"20171
                 common backend ends 164"35173" super"Importants".
                  -source backend node (de"20175" tuper"(not)
                 -try backend node 16-"3000" altorneed a Pick-on Truck?"
            HELV backend mode 14v*30183*>
               clear backend made 160"35350"-In need of a smaller moving truck? Subject-com offers pick-up trucks.crimes
            - Backend_mode_ld+"20189" $155er"Reserve Truck"-
               court backend mode boy 15/10/ cheserue Trucks/mort
is backend neer 10+"35227" name+"81224"2
 HIS BACKENE Node_List* 90231
          HILL Backens node (SACTOS) No.
            VICE backend node 164*30238*
              with backend node 184" 59048"
                     which backens note in 192001 Personal Restate County
```

```
-uption backend_node_id="38936" value="18:68 Per-
           stest backend node 56+"38537"-18:88 PMc/tests
         -sutton backend_node_sdv"38558" valuev"18158 Pt">
           "Sext backend_node_ld+"38939"-18138 PM-/18951
         -uption backend_node_ldv"38548" valuer"11:88 PM"-
           -best backend_node_16+"38541"-$1186 PROJECT
         rightion backend_node_id="38542" value="31:38 PM"=
          -trivt backend node 16-"38543"-11/38 PM:/10/1-
willy backend node lidy 18951"-
 willy backend node_ld+"38953"
     wint backend node id="3855" Will you return the truck to a different location / texts
     -input backend node_id="20000" type="radio" name="une-uny-radio" value="0" input_value="0" input_thecked="true"/>
     "spun backend_hode_id+"38962"
        etest backend_node_lde*38963*-Yes-/texts
     -irout backend node id="38965" type="radio" name="inc-way-radio" value="LIT input value="LIT"/-
     -sum backend node ide 1896
       shout backend node 1dy 18562" April 1871
  window backend mode id="38880" mase="dintctrizEll3Vie-SWPSchklitock!" value="false" input value="false"//
villy backend_node_lid+"limite"-
   villy backend_node_1d+"38994"
       steet backend node 16+"38997"-Where do you want to return your trucks/texts-
     «Input backend node 18**39080" type="text" placeholder="US City,State or Zip Code*/-
+it!/ backend node lide*30018"+
 HILV backend node_id+"39813"
   vicen backend node 1dx*39814*
     is backend node 164"38358":
        "Trivit backend node_16+"35819" name+"doi:11/338129/1mv9899509/fex151401"/-
     <!sbc! backend_mode_inc'35023" titles"flexible Sutes";</pre>
       stest backend_node_id="35824"-Flexible Dates=/test
   -tutton backend_node_id="38359" type="button"/-
-tilly backend node id-"39833">
 unity backend node ide 1000000
   HITV backend node 10+1398371
     -div backend node Id+"39839"+
       "in backend_node_184"35813">
         vited backend node, 16/730842"-And Discount Code-/1201-
        -dir backend_node_16+*39844*>-
         -rriv backend_node_16+*29840
           -label backend node ide 39848
```

HTML -> Simplified HTML -> Image

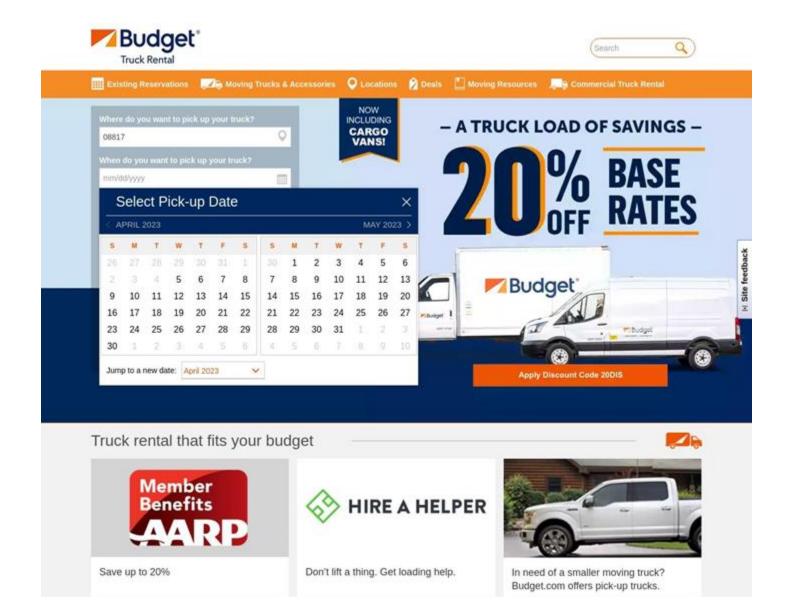
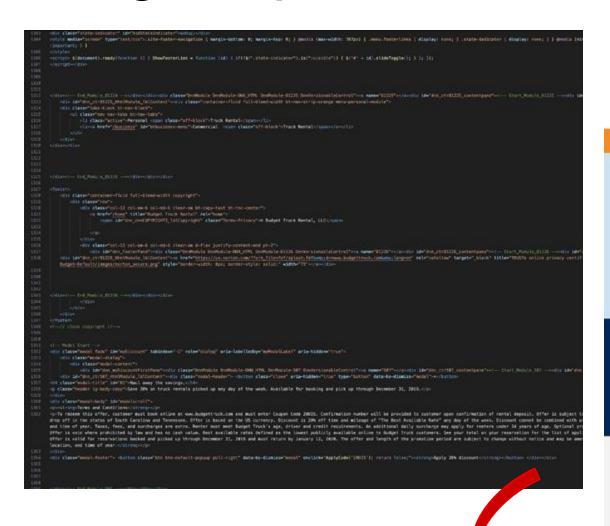
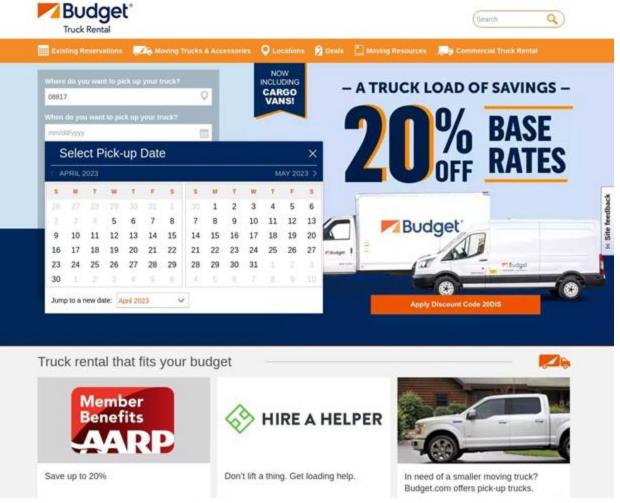
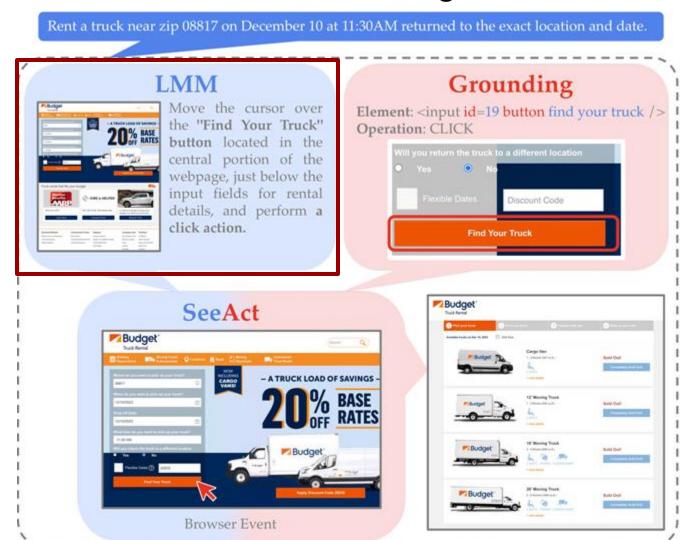


Image: A picture is worth thousands of words



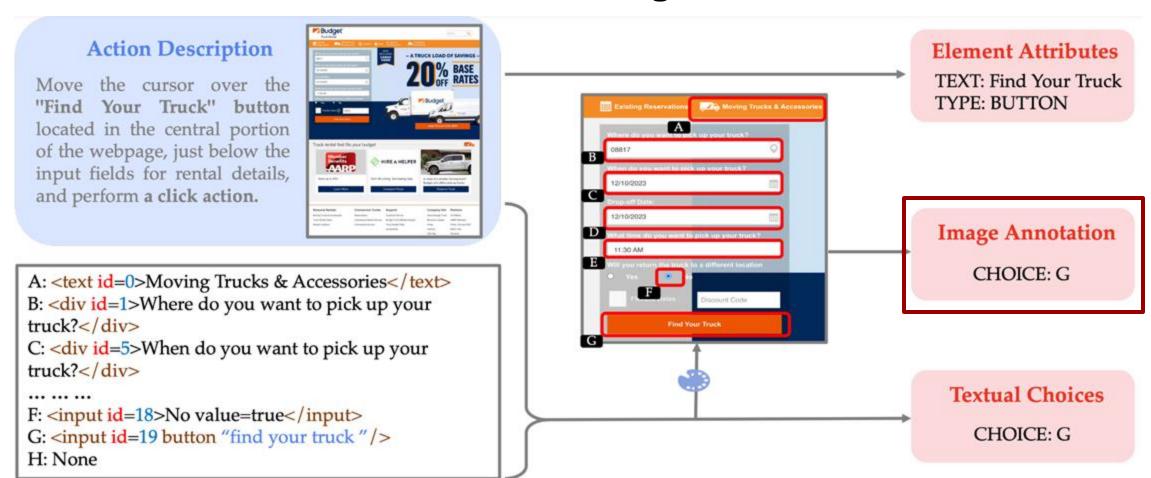






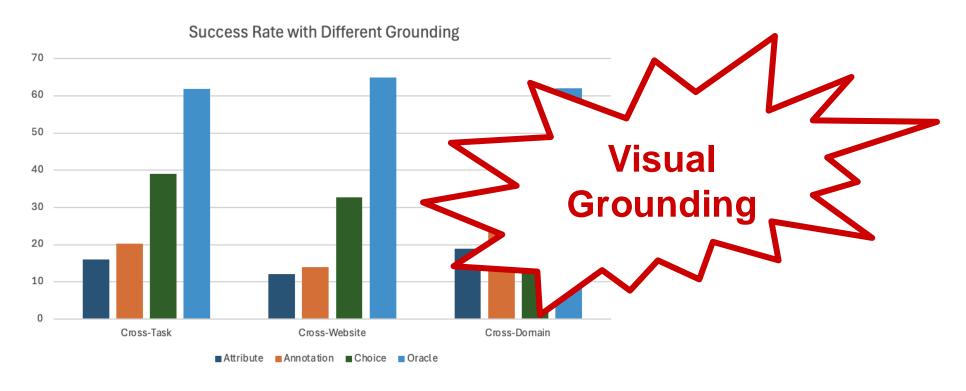






Grounding Strategies

Oracle: Ask humans to identify model's intended actions from Action Description Large Margin between Oracle and SOTA Grounding method so far



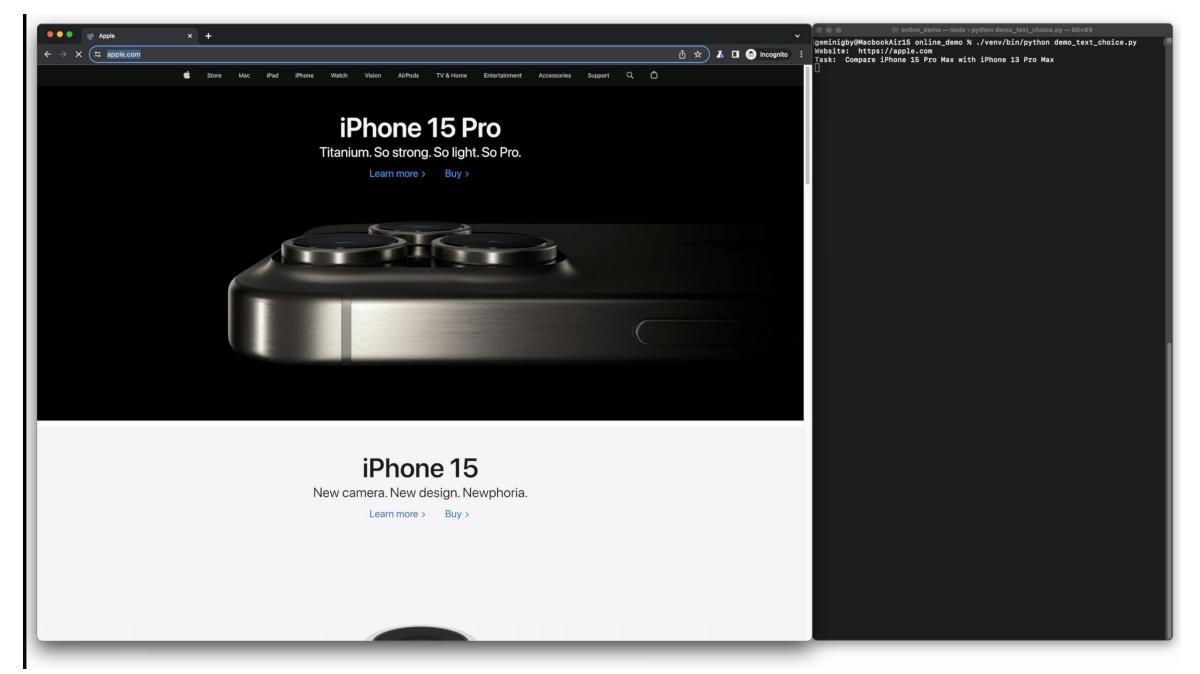
Single Step Success Rate on Mind2Web

Human-like Vision-centric Embodiment is the Future for Web/GUI Agents

- Most comprehensive evaluation of GUI Agents to date
- SeeAct-V + UGround outperforms prior SoTA despite its minimalist design



Figure 1: Examples of agent tasks across platforms and performance on **GUI grounding** (♣: ScreenSpot), **offline agent** (♠: Multimodal-Mind2Web, AndroidControl, and OmniAct), and **online agent benchmarks** (♥: Mind2Web-Live and AndroidWorld) when using GPT-4 as the planner.



Online evaluation tool that allows SeeAct to interact with live websites

Online Evaluation

	Offline ₀	Offline ₁	Online
FLAN-T5-XL	4.4	24.4	8.9
GPT-4	1.1	12.2	13.3
SEEACT _{Choice}	3.3	12.2	37.8
SEEACTOracle	13.3	27.8	51.1

Whole task success rate (%)

SeeAct Codebase

An interface between Agent and Website

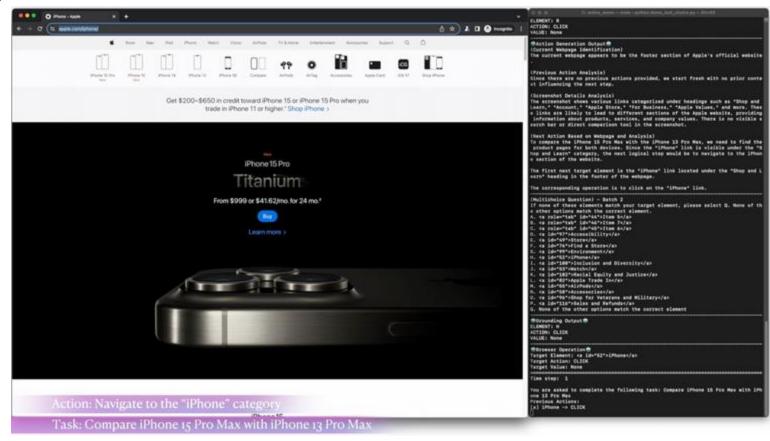
- Perception
- Action Execution

```
import asyncio
import os
from seeact.agent import SeeActAgent

# Setup your API Key here, or pass through environment
os.environ["OPENAI_API_KEY"] = "Your API KEY Here"

async def run_agent():
    agent = SeeActAgent(model="gpt-4-turbo")
    await agent.start()
    while not agent.complete_flag:
        prediction_dict = await agent.predict()
        await agent.execute(prediction_dict)
    await agent.stop()

if __name__ == "__main__":
    asyncio.run(run_agent())
```

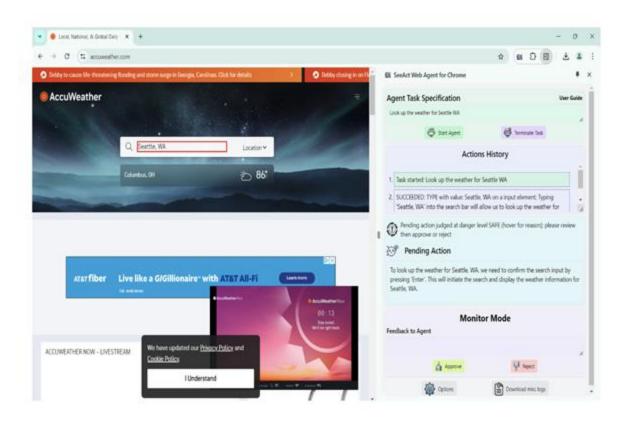


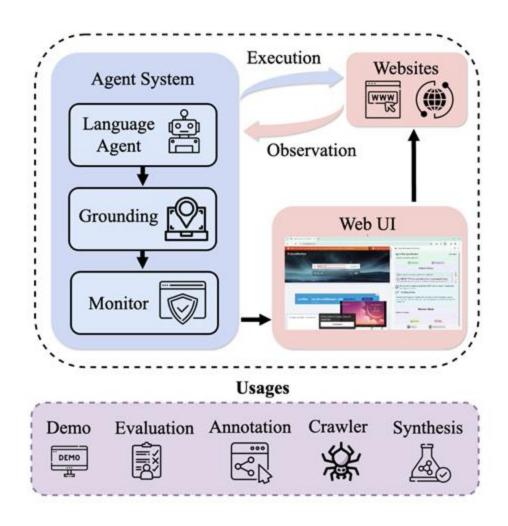




WebOlympus: An Ecosystem for Web Agent

An ecosystem for web agent



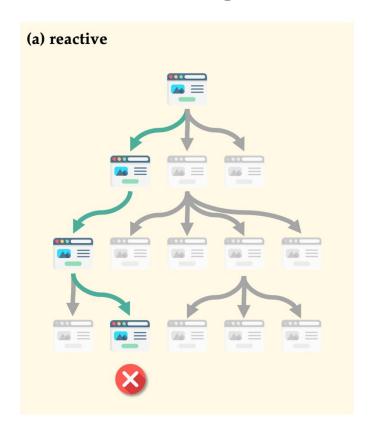


Outline

1 Introduction

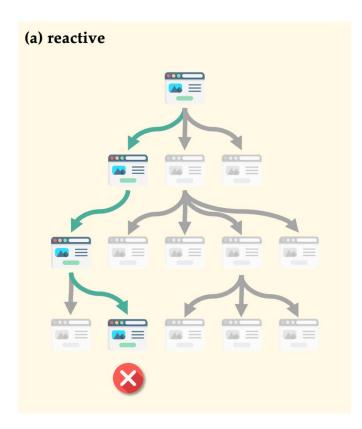
2 Environment Perception

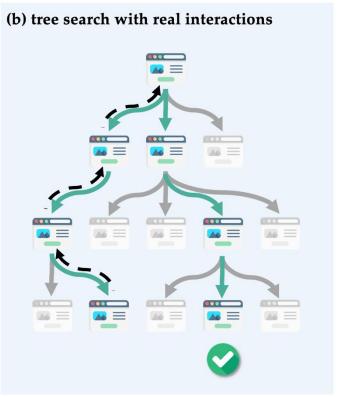
3 Planning



fast, easy to implement

greedy, short-sighted







fast, easy to implement



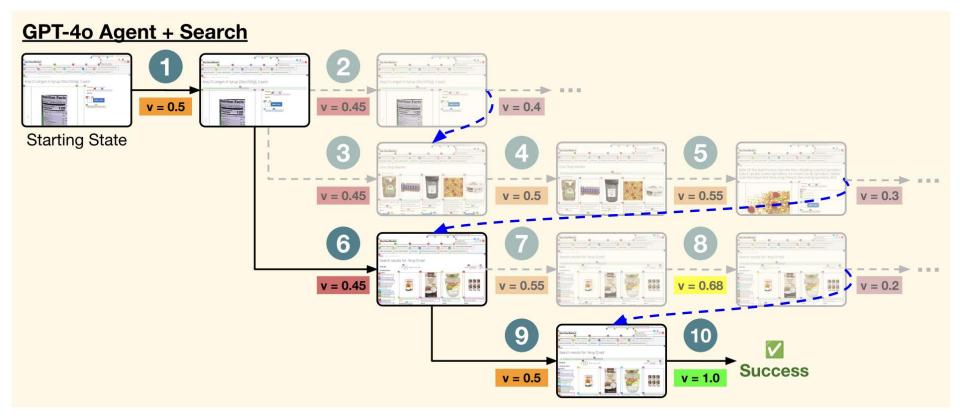
greedy, short-sighted



systematic exploration

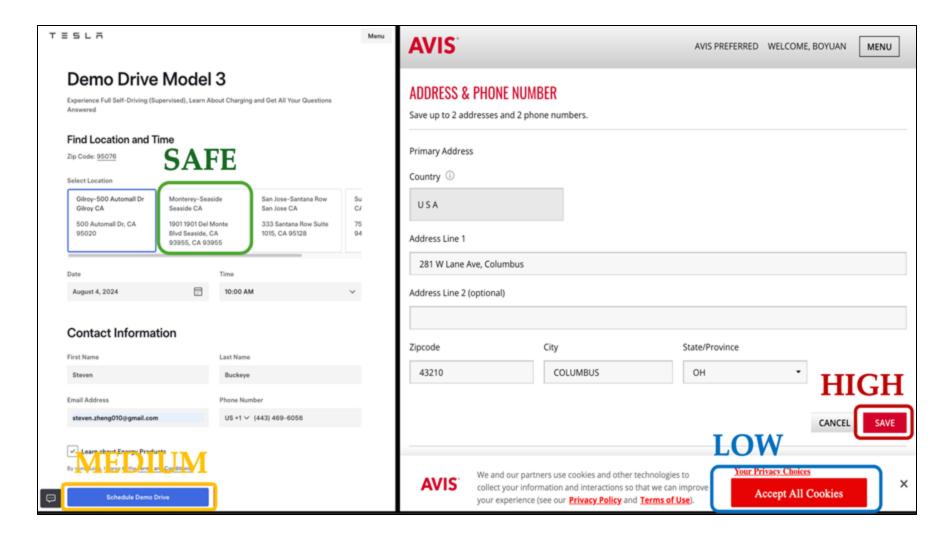


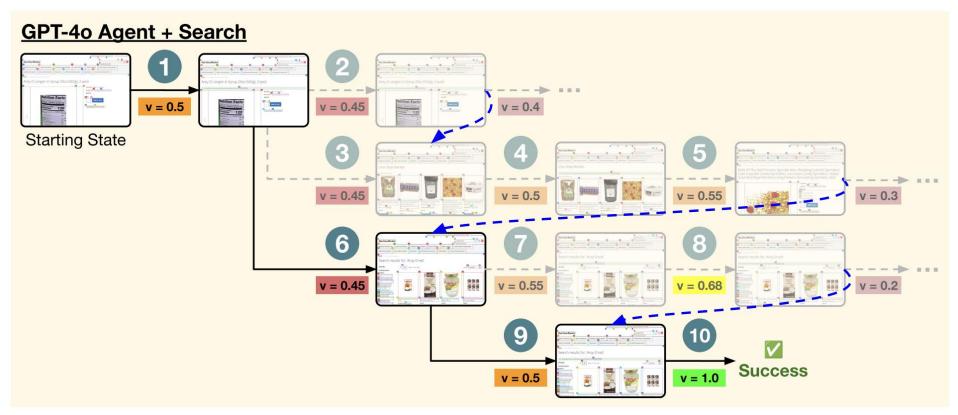
irreversible actions, unsafe, slow



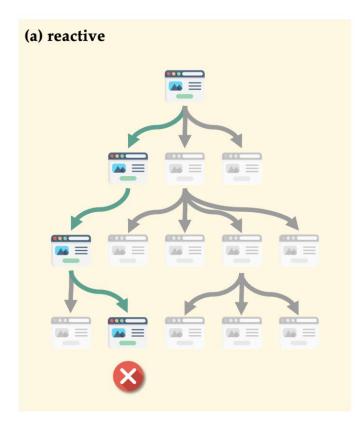
State-Changing Action

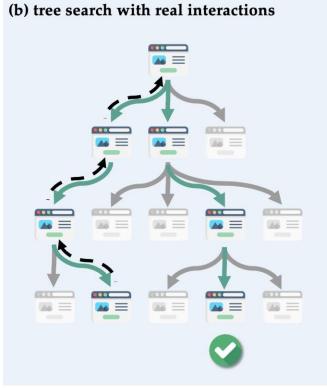
State-Changing Actions

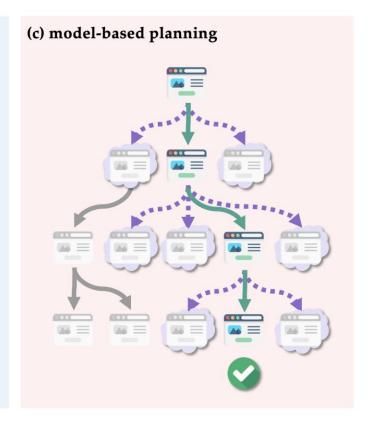


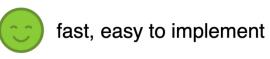


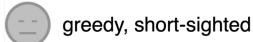
- State-Changing Action
- Tracing Back?
- Limited Efficiency





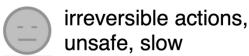








systematic exploration





faster, safer, systematic exploration



how to get a world model

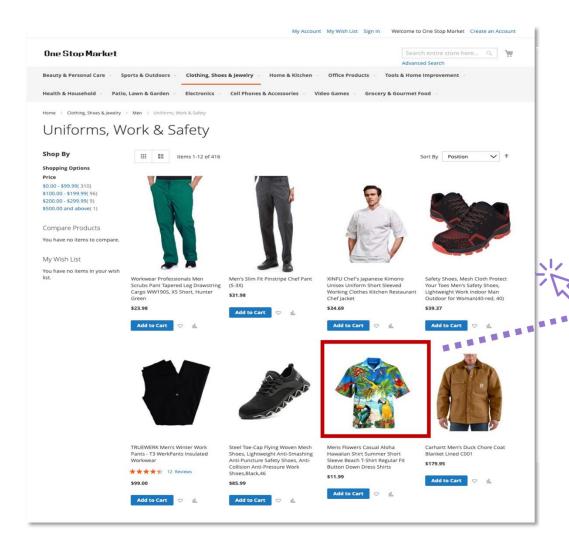
World Model

A model capable of predicting environment transition:

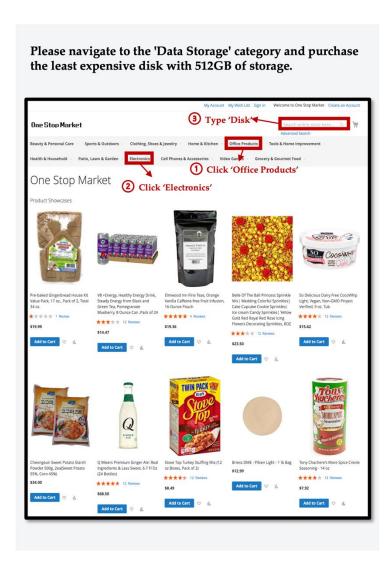
$$\widehat{T}: \mathcal{S} \times \mathcal{A} \to \mathcal{S}$$

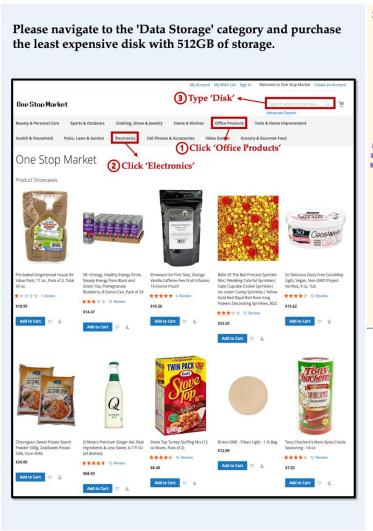
If I do this (a_t) on (s_t), what would happen next (s_t+1)?

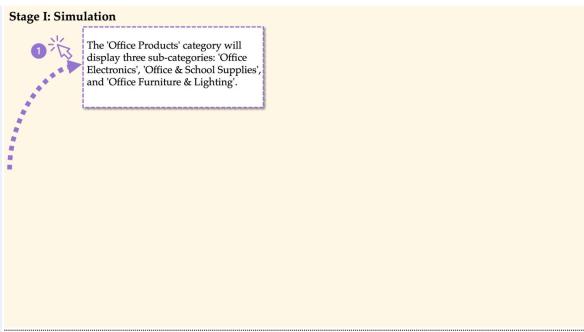
LLM can predict state transitions(reasonably good)

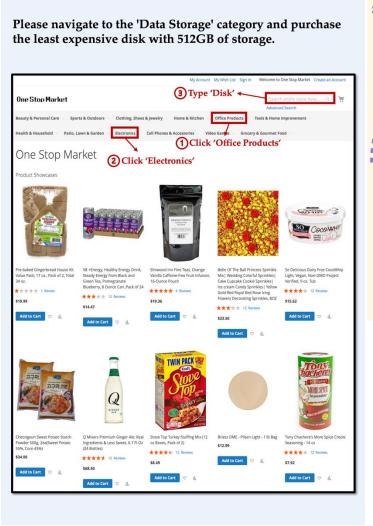


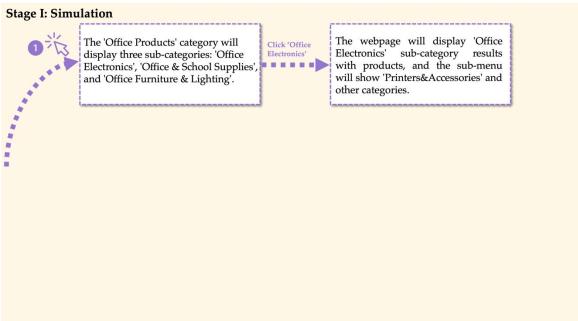
The page will navigate to a detailed product page for the "Mens Flowers Casual Aloha Hawaiian Shirt Summer Short Sleeve Beach T-Shirt Regular Fit Button Down Dress Shirts." This new page will likely contain additional information about the product including more detailed specifications, customer reviews, larger images, sizing options, and possibly a larger "Add to Cart" button. Other elements from the current category view like the grid of products will be replaced with the detailed view of this specific product.

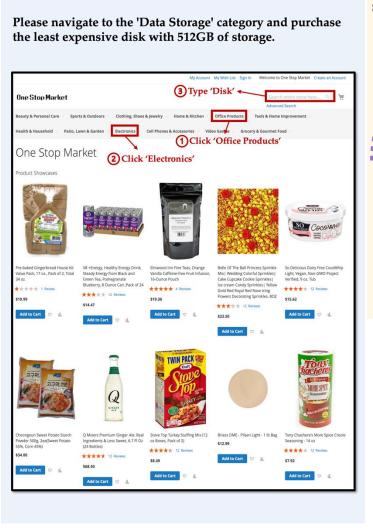


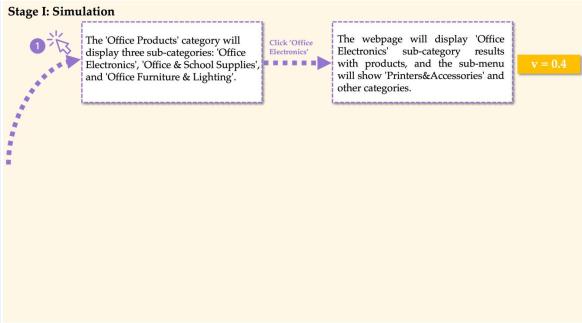


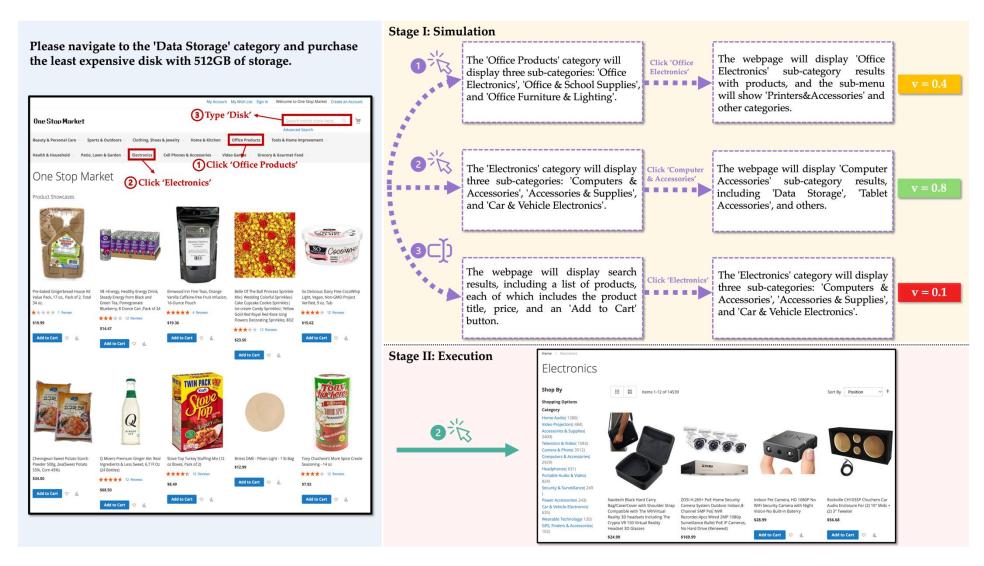






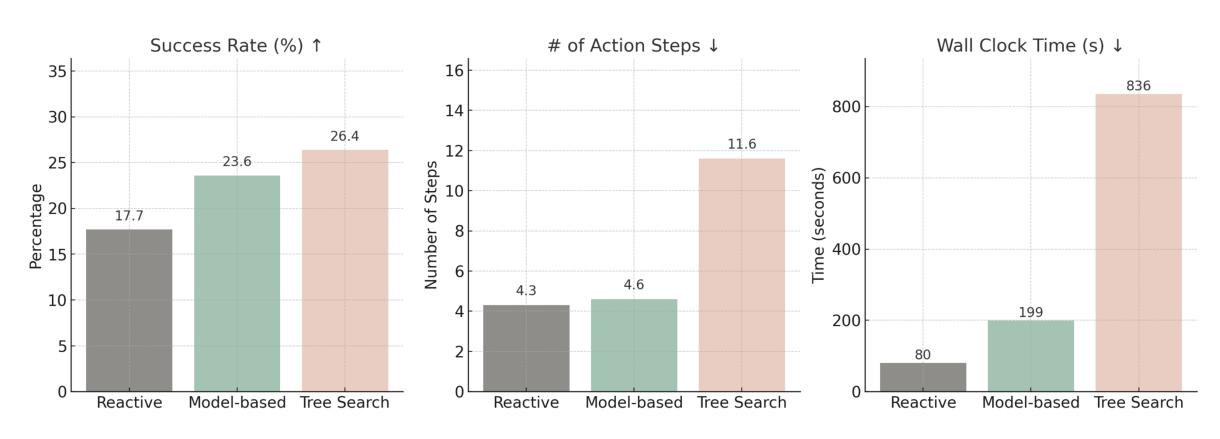






Results on VisualWebArena

Model-based planning is more accurate than reactive planning and more efficient than tree search



Outline

1 Introduction

2 Environment Perception

3 Planning

4 Self-Improvement

What's next step?

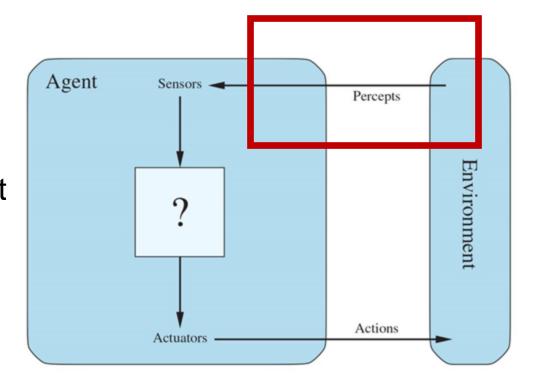
Where have we arrived at?

Perception

Perception:

HTML/DOM: MindAct

Screenshot: SeeAct, WebGUM, CogAgent

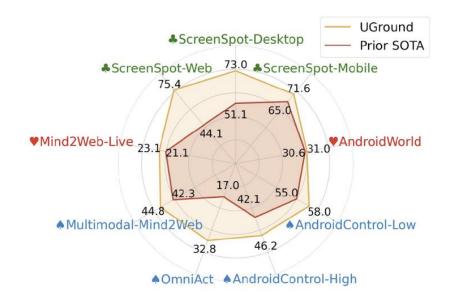


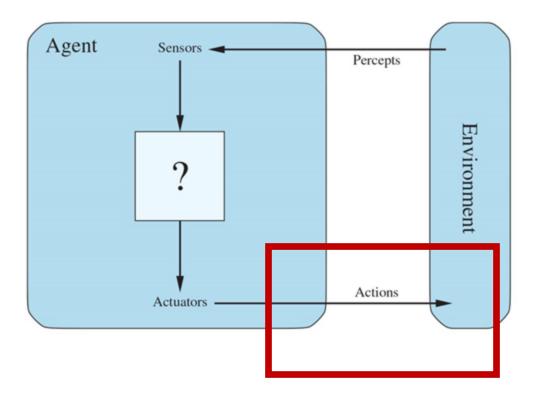
Action

Action:

Weak Grounding: SOM, SeeAct

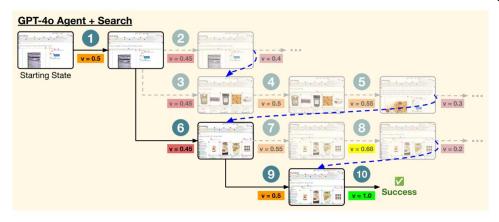
Pixel-Level: UGround, SeeClick, etc.



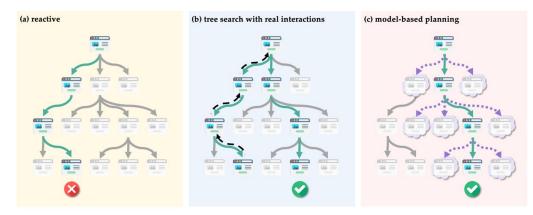


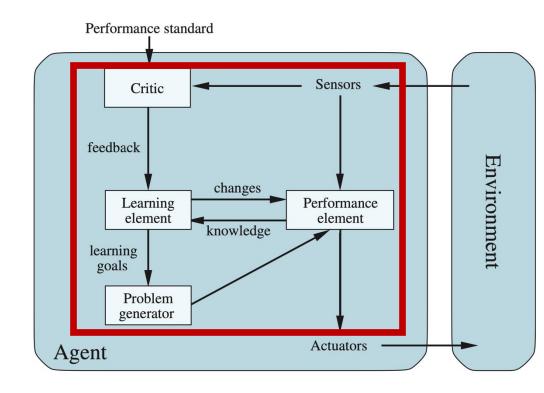
Planning

Search over the environment: Search-Agent



Planning with World Model: WebDreamer





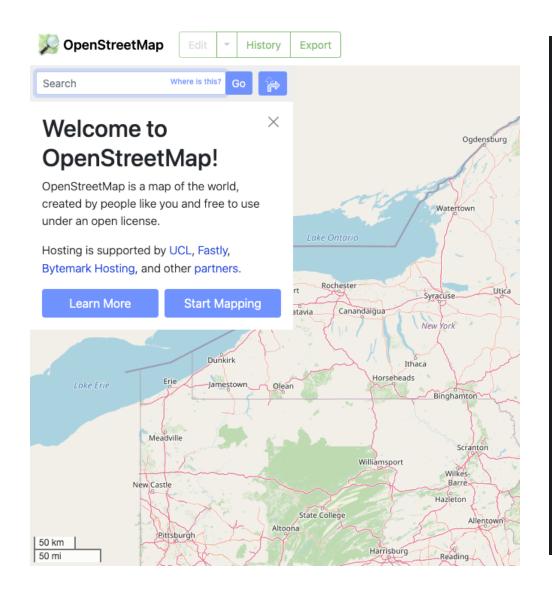
What's next step?

Agent has reached a decent performance of 30~50%.

How reach closer to 100% to be actually useful and robust?

What current agents are capable of?

Task Proposal



```
1. **Get Directions Between Two Points:**
   - Usefulness: 5 (Finding directions is a frequent task for users of a map service.)
   - Steps: Click on 'Find directions between two points' link, enter starting point, en
ter destination, click 'Go'. Total: 4 actions.
   - Total Rating: 9
2. **Export Map Data:**
   - Usefulness: 4 (Exporting map data is useful for offline usage or data analysis.)
   - Steps: Click on 'Export' link, select export options, click 'Export'. Total: 3 acti
ons.
   - Total Rating: 7
**Search for Location:**
   - Usefulness: 5 (Common and frequent usage of map services.)
   - Steps: Enter text into 'Search' textbox, click 'Go'. Total: 2 actions.
   - Total Rating: 7
4. **Show My Location:**
   - Usefulness: 4 (Useful for quickly finding your current location on the map.)
   - Steps: Click 'Show My Location' button. Total: 1 action.
   - Total Rating: 5
The skill 'Get Directions Between Two Points' has the highest total rating and usefulnes
s, making it the most beneficial skill to propose for this task.
```

Execution

Task Description:

Show me the reviews for the auto repair business closest to 10002.

Action Sequence:

	Target Element	Operation
1.	[searchbox] Find	TYPE: auto repair
2.	[button] Auto Repair	CLICK
3.	[textbox] Near	TYPE: 10002
4.	[button] 10002	CLICK
5.	[button] Search	CLICK
6.	[switch] Show BBB Accredited only	CLICK
7.	[svg]	CLICK
8.	[button] Sort By	CLICK
9.	[link] Fast Lane 24 Hour Auto Repair	CLICK
10.	[link] Read Reviews	CLICK

Webpage Snapshots:



type="search">





Auto Repair



Fast Lane 24 Hour Auto Repair



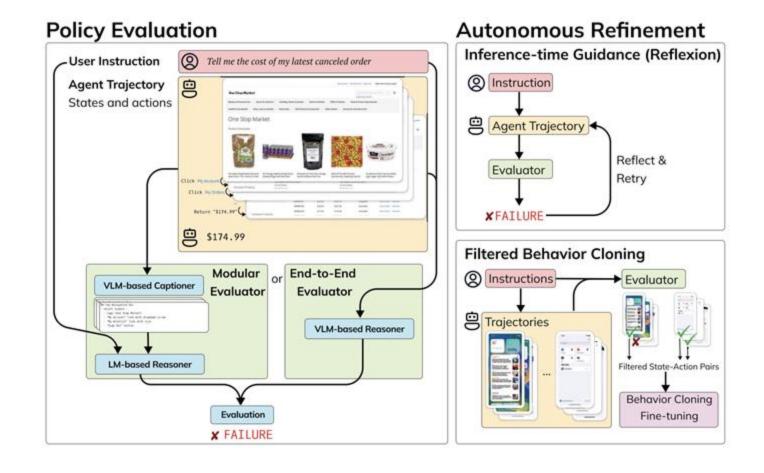
<button>Search</button>



Read Reviews

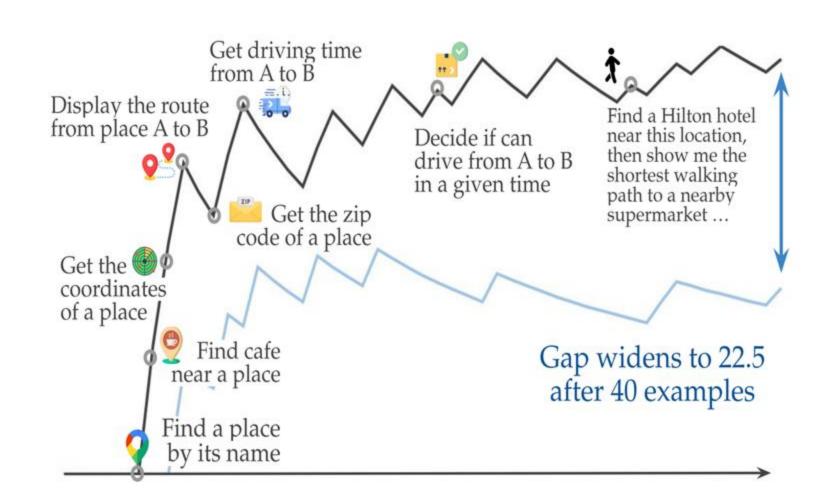
Critic

Given action sequence and instruction, label if the task is successfully completed



Self-Improvement through exploration

- 1.Propose tasks
- 2. Explore websites
- 3.Accumulate skills
- 4.Leverage knowledge



What's the Abstraction Level?

Trajectories: Accumulate knowledge in an inexplicit way

- Heavy: Training Policy
- Update & Adapt to new websites? Catastrophic forgetting
- Website changes?

Workflow: Textual Description of Procedure

- Lengthy
- How to update workflow?
- How to leverage multiple attempts into a workflow?

What's the Abstraction Level?

APIs:

- Light-Weighted
- Easy to Debug
- Easy for trail-and-error

```
async def identify_pill(page, imprint, color=None, shape=None):
    Automates the process of identifying a pill using the Pill Identifier
    feature on Drugs.com.
    Parameters:
    - page: The Playwright page object.
    - imprint: The imprint on the pill to be identified.
    - color: (Optional) The color of the pill.
    - shape: (Optional) The shape of the pill.
    This function navigates to the Pill Identifier page, agrees to the terms,
    inputs the pill's characteristics,
    and submits the information for identification.
    Usage Log:
    - Successfully navigated to the Pill Identifier page and submitted pill
    information for identification.
    - Inputted imprint '93 5510', color 'White', and shape 'Oval' and
    successfully submitted for identification.
    - Encountered issues with strict mode violations when attempting to click
    the 'Search' button due to multiple matches.
    - Updated to use a more specific selector for the 'Search' button to avoid
    strict mode violations.
    import re
    await page.goto("https://www.drugs.com/pill_identification.html")
    await page.get_by_role("link", name="Agree and Continue").click()
    await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
    if color:
        await page.get_by_role("group", name="Color and shape (optional)").
            get_by_role("combobox", name="Color
                  (optional)").select_option(color)
    if shape:
        await page.get_by_role("group", name="Color and shape (optional)").
            get_by_role("combobox", name="Shape
                   (optional)").select_option(shape)
    search_button =
           page.locator("button.ddc-btn.ddc-btn-block[data-submit-loading]")
    await search_button.click()
```

What if?

We have an algorithm:

Explore environment and accumulate skill&knowledge into APIs

A plug-and-play module for any agent capable of function calling

Overview

Skill Library



check_drug_interaction(drug_name)



subscribe_to_newsletters(email)



search_FDA_alert()



check_side_effects(drug_name)



identify_pill(imprint, color)

Skill Synthesis

Practice Skill → **Reward Model** → **API Synthesis**

```
async def identify_pill(page, imprint, color):
 # Automates the process of identifying a pill on Drugs.com.
 await page.goto("/pill_identification.html")
 await page.get_by_role("link", name="Agree and Continue").click()
 await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
 search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")
+ if color: await page.get_by_role("group", name="Color and shape (optional)").get_by_role(
+ "combobox", name="Color (optional)").select_option(color)
 await search_button.click()
```

Skill Proposal



Identify Pill Using Pill Identifier 3

Check Side Effects for a Drug

Search a Condition's Treatment

Browse Drugs by Letter

Environment



Verification

Test Cases

Execution

Error:



-> identify_pill(page, imprint, color)

The parameter 'color' is defined but never used in the function body

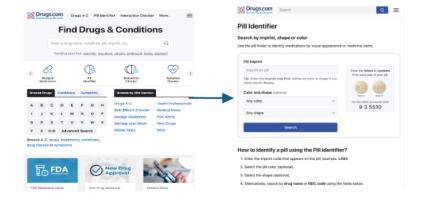
Error: Search results validation failed. API returned pills matching imprint '5510' but the wrong color (expected: yellow).

Added color selection using the dropdown menu Made color filtering optional

Uses 'if color': to make color filtering optional Properly implemented color parameter in the search function, locating the "Color and shape" group element

Skill Proposal

Environment



Skill Library





search_FDA_alert()

check_side_effects(drug_name)

identify_pill(imprint, color)

Skill Proposal

t	ime	me useful	
Identify Pill Using Pill Identifier	3	5	
Check Side Effects for a Drug	3	4	×
Search a Condition's Treatment	3	4	×
Browse Drugs by Letter	2	4	×

Skill Synthesis

Skill Library



check_drug_interaction(drug_name)



subscribe_to_newsletters(email)



search_FDA_alert()



check_side_effects(drug_name)



identify_pill(imprint, color)

Skill Synthesis

Practice Skill

Reward Model - AP

→ API Synthesis

```
async def identify_pill(page, imprint, color):
    # Automates the process of identifying a pill on Drugs.com.
    await page.goto("/pill_identification.html")
    await page.get_by_role("link", name="Agree and Continue").click()
    await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
    search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")

await search_button.click()
```

Execution

Task Description:

Show me the reviews for the auto repair business closest to 10002.

Action Sequence:

	Target Element	Operation
1.	[searchbox] Find	TYPE: auto repair
2.	[button] Auto Repair	CLICK
3.	[textbox] Near	TYPE: 10002
4.	[button] 10002	CLICK
5.	[button] Search	CLICK
6.	[switch] Show BBB Accredited only	CLICK
7.	[svg]	CLICK
8.	[button] Sort By	CLICK
9.	[link] Fast Lane 24 Hour Auto Repair	CLICK
10.	[link] Read Reviews	CLICK

Webpage Snapshots:



type="search">





Auto Repair



Fast Lane 24 Hour Auto Repair



<button>Search</button>



Read Reviews

Skill Synthesis

Skill Library



check_drug_interaction(drug_name)



subscribe_to_newsletters(email)



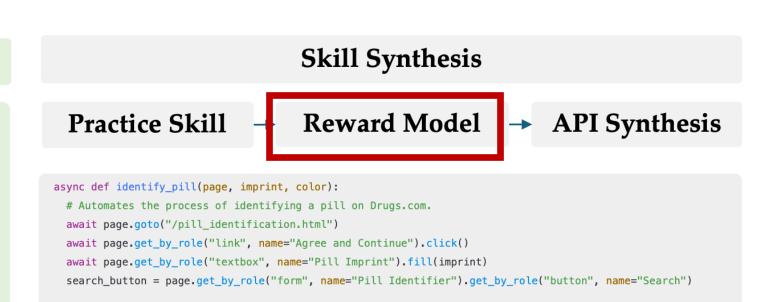
search_FDA_alert()



check_side_effects(drug_name)



identify_pill(imprint, color)



await search_button.click()

Skill Synthesis

Skill Library



check_drug_interaction(drug_name)



subscribe_to_newsletters(email)



search_FDA_alert()



check_side_effects(drug_name)



identify_pill(imprint, color)

Skill Synthesis



Practice Skill → **Reward Model**

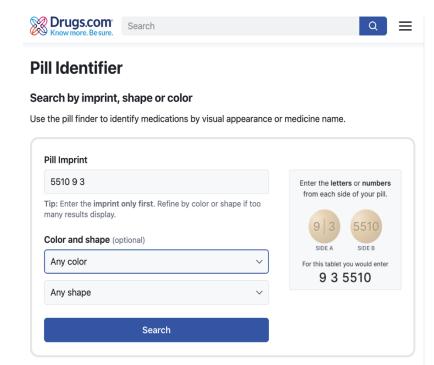
API Synthesis

```
async def identify_pill(page, imprint, color):
 # Automates the process of identifying a pill on Drugs.com.
 await page.goto("/pill_identification.html")
 await page.get_by_role("link", name="Agree and Continue").click()
 await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
 search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")
await search_button.click()
```

Verification

```
async def identify_pill(page, imprint, color):
    # Automates the process of identifying a pill on Drugs.com.
    await page.goto("/pill_identification.html")
    await page.get_by_role("link", name="Agree and Continue").click()
    await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
    search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")

await search_button.click()
```



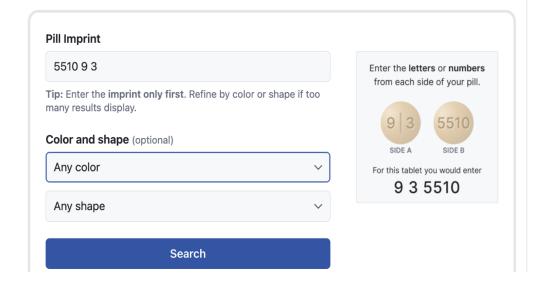
How to identify a pill using the Pill Identifier?

- 1. Enter the imprint code that appears on the pill, example: L484
- 2. Select the pill color (optional).
- 3. Select the shape (optional).
- 4. Alternatively, search by drug name or NDC code using the fields below.

Verification

```
async def identify_pill(page, imprint, color):
    # Automates the process of identifying a pill on Drugs.com.
    await page.goto("/pill_identification.html")
    await page.get_by_role("link", name="Agree and Continue").click()
    await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
    search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")

await search_button.click()
```



Verification

Test Cases



Error:

Warning: Unused parameter 'color'
 -> identify_pill(page, imprint, color)
 The parameter 'color' is defined but never used in
the function body

Error: Search results validation failed.

API returned pills matching imprint '5510' but the wrong color (expected: yellow).

Diagnosis:

Added color selection using the dropdown menu Made color filtering optional

Uses 'if color': to make color filtering optional

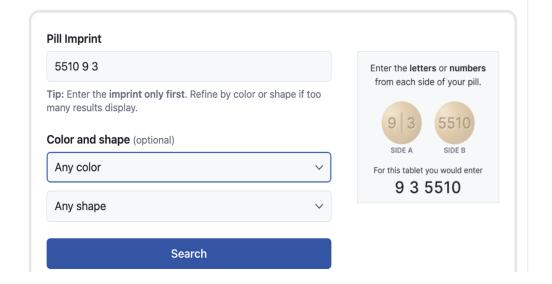
Properly implemented color parameter in the search

function, locating the "Color and shape" group element

Verification

```
async def identify_pill(page, imprint, color):
    # Automates the process of identifying a pill on Drugs.com.
    await page.geto("/pill_identification.html")
    await page.get_by_role("link", name="Agree and Continue").click()
    await page.get_by_role("textbox", name="Pill Imprint").fill(imprint)
    search_button = page.get_by_role("form", name="Pill Identifier").get_by_role("button", name="Search")

+ if color: await page.get_by_role("group", name="Color and shape (optional)").get_by_role(
    + "combobox", name="Color (optional)").select_option(color)
    await search_button.click()
```



Verification

Test Cases

Execution

Error:

Warning: Unused parameter 'color'
 -> identify_pill(page, imprint, color)
 The parameter 'color' is defined but never used in
the function body

Error: Search results validation failed.

API returned pills matching imprint '5510' but the wrong color (expected: yellow).

Diagnosis:

Added color selection using the dropdown menu Made color filtering optional

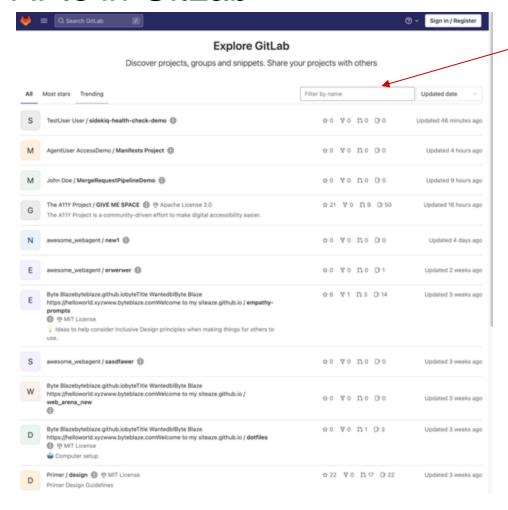
Uses 'if color': to make color filtering optional

Properly implemented color parameter in the search

function, locating the "Color and shape" group element

More Examples of Synthesized APIs

APIs in GitLab



```
async def search_projects_by_keyword(keyword: str):

Search for projects by a specific Neyword.

This function locates the 'Filter by name' search box, types the given Neyword, and presses 'Enter' to execute the search operation.

Usage:
Call this function with the desired Neyword to perform a search operation within the projects.

:param Neyword: The Neyword to search for in projects.

====

searchbox_locator = page.get_by_role('main', name='').get_by_role(
    'searchbox_locator.click()
ownit searchbox_locator.fill('')
amait searchbox_locator.type(keyword)
ownit page.keyboard.press('Enter')
```

```
Tollow and whom a project repository (project, need; att) - reject

This function automates the process of manipulary in the Visitors' section of the sensite,
selecting a project from the list, accessing the project maps, and retrieving the plane and interacting with the 'there' systems.

They

Did table provides with the 'project, need' of the arminal year with it shows. It will return the class project, need to the arminal year and to show a partners in the remediatry as a string.

[perse project, need the remediatry as a string.

[perse project, need to remediatry as a string.

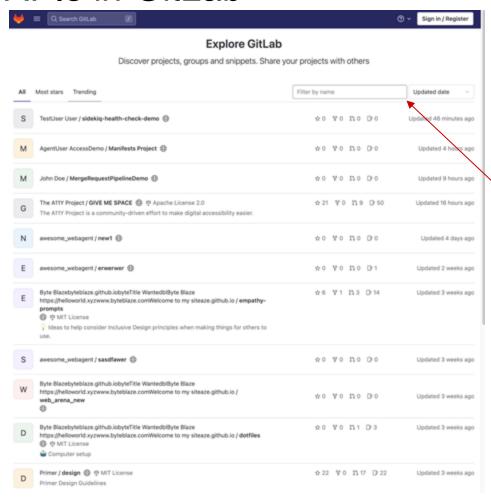
[perse project, need to remediatry to fill to also the arminal repository.

[perse project, need to need 'the project to addition and show, persent and page pert, by, relet' main', need "to also the arminal repository.

[perse pert, by, relet' main', need "to pert, by, relet'tion', need 'to be '
```

More Examples of Synthesized APIs

APIs in GitLab



```
async def search_projects_by_keyword(keyword: str):
    Search for projects by a specific keyword.
    This function locates the 'Filter by name' search box, types the given keyword,
    and presses 'Enter' to execute the search operation.
    Call this function with the desired keyword to perform a search operation
    within the projects.
    :param keyword: The keyword to search for in projects.
    searchbox_locator = page.get_by_role('main', name='').get_by_role(
        'searchbox', name='Filter by name')
    await searchbox_locator.click()
    await searchbox_locator.fill('')
    await searchbox_locator.type(keyword)
    await page.keyboard.press('Enter')
```

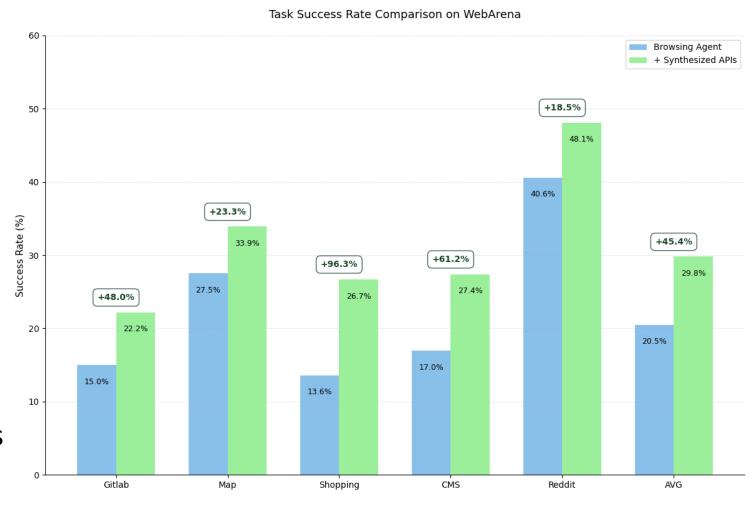
Evaluation on Sandbox

Exploration:

Synthesize APIs with 160 Iterations

Agents:

- Browsing Agent:
 - Browser Action
- +API Synthesis
 - Extend action space with APIs



How far are we from human-crafted APIs?

- Human Crafted APIs:
 - Mining APIs from sandbox source code

Not realistic, but can serve for a case study

```
# Commits
            ## GET /api/{id}/commits: Get a list of commits in a project.
             | Attribute | Type
                                            Description
   API
               `id`
                          integer/string | The ID or path of the project.
Documentation
                         | string
                                          | Only commits after or on this date.
              `since`
              `until`
                         | string
                                          | Only commits before or on this date. |
            Output: JSON containing all commits that meet the given criteria.
            <execute ipython>
 API Calling
            requests.get('gitlab.com/api/allyproject/commits')
            </execute ipython>
             [ . . . . . . {
                "id": "ed37a2f2",
                 "created at": "2023-03-13T21:04:49.000-04:00",
JSON Output
                 "title": "Update README.md",
                 "message": "Update README.md",
                 "author": "SaptakS",
```

Comparing with human crafted APIs

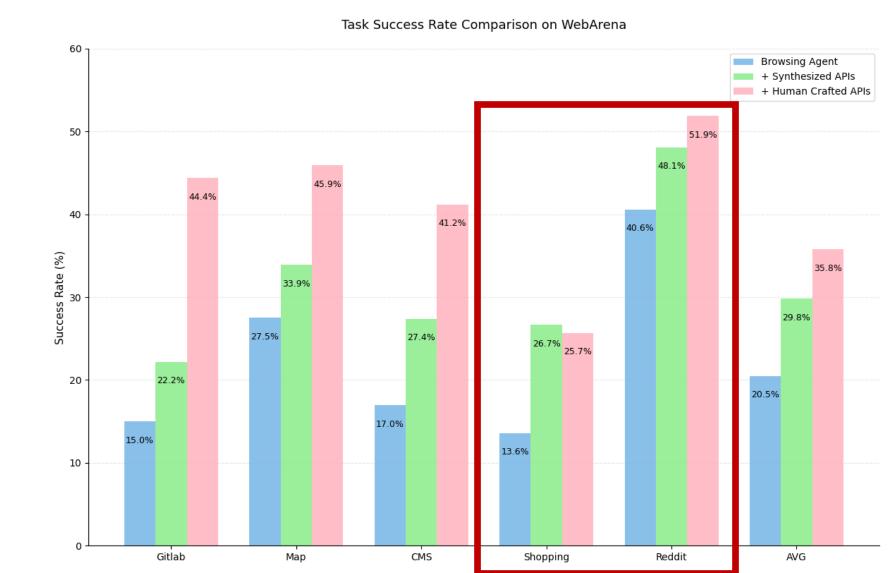
API Support Level

MEDIUM:

Admin Access Limited APIs

LOW:

Manually written automation Code



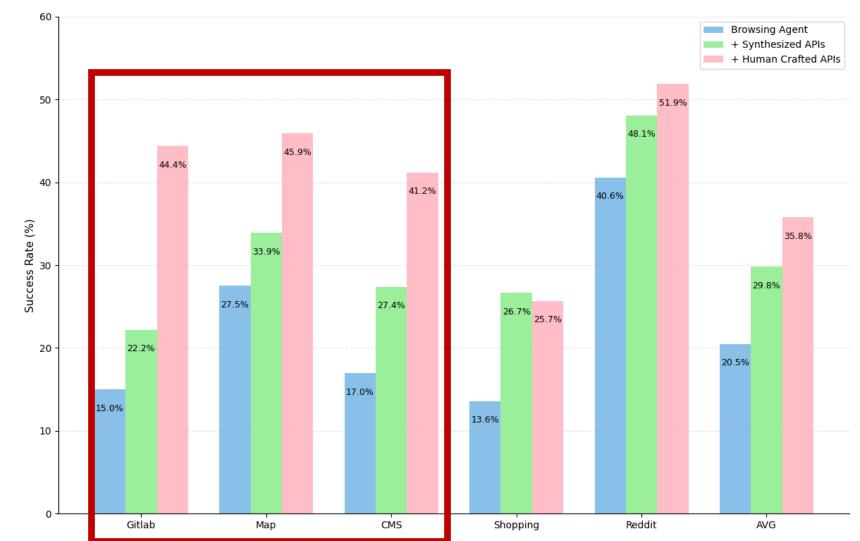
Comparing with human crafted APIs

HIGH API support:

Admin Access

High Quality API

Task Success Rate Comparison on WebArena



Generalization to weaker Agent

Empowering smaller models with APIs synthesized by larger models

• Exploration: GPT-40

• Inference: GPT-4o-mini

SKILLWEAVER						
GPT-4o	17.8	27.5	19.8	18.7	37.7	22.6
+ Skills	22.2	33.9	27.2	25.8	50.0	29.8
Δ	† 25%	† 23%	† 38%	† 38 %	† 33%	† 32%
GPT-4o-mini	6.1	10.3	11.8	3.3	18.9	9.2
+ Skills	8.9	16.7	17.1	7.7	26.4	14.1
Δ	† 46%	† 62%	† 46%	† 133%	† 40%	† 45%

Scaling to Live Websites

Exploration:

80 Iterations

Evaluation:

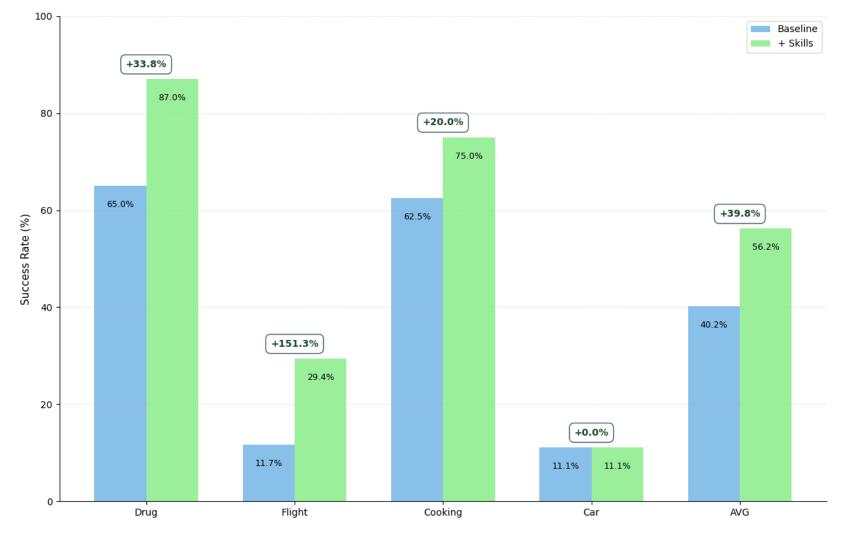
Drug: 23

Flight: 17

Cooking: 8

Car: 9





Thank you! & Questions?