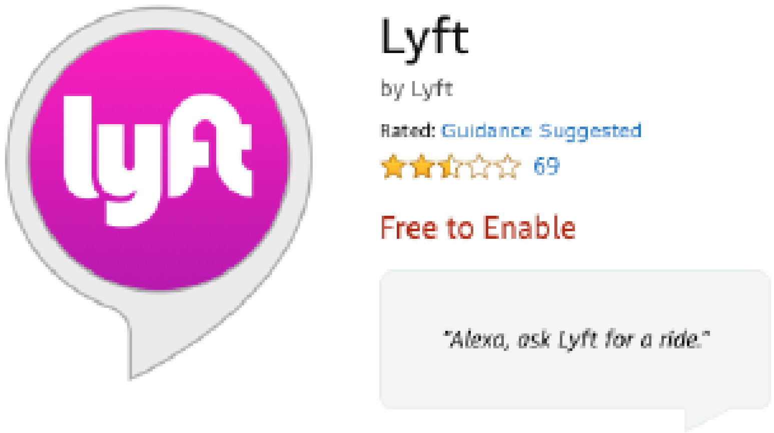
CPSC 8570 -Security in Advanced Networking technologies

Skill Squatting Techniques on Amazon Alexa – A Demonstration

Nandini Krupa Krishnamurthy

Recap

1. Objective – To demonstrate skill squatting attack on Amazon Alexa.
2. Skills – The third party applications that leverage Alexa voice services.
3. Alexa Skill Invocation



Lyft

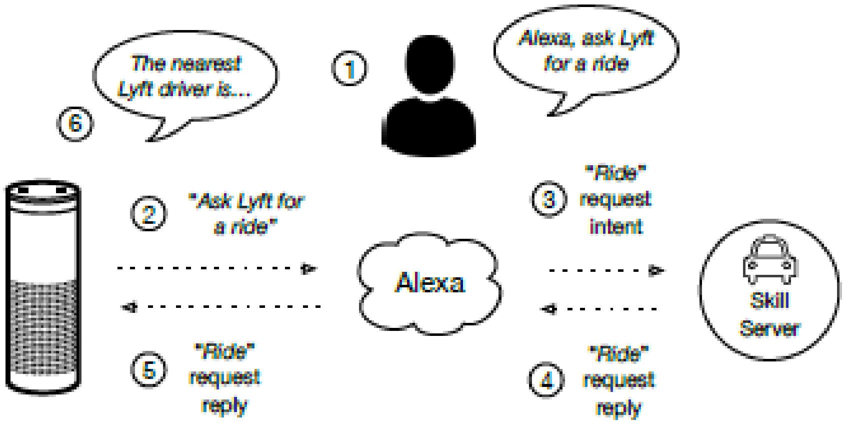
by Lyft

Rated: Guidance Suggested

69

Free to Enable

"Alexa, ask Lyft for a ride."



4. Types of errors :

    a. Homophones – same pronunciation. Sail-Sale, boil-Boyle

    b. Compound words – super-highway-superhighway, outdoors-out doors

    c. Phonetic Confusions – wet (W EH T)- what (W AH T)

    d. Other errors – no specificity

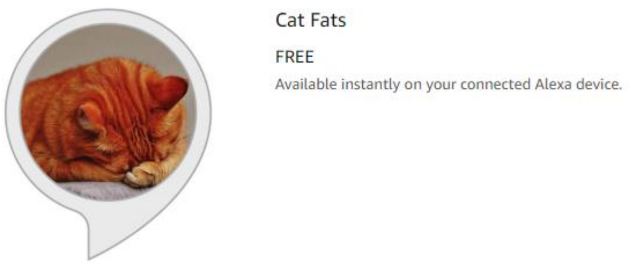
5. Skill Squatting Attack – Confusion in the systematic error from one word to another creates a possibility of invocation of a malicious skill instead of the target skill.

Method

1. Build pairs of skills (27) that are frequently confused by Alexa .

Skill 1	Skill 2
How much is the Time?	How much is the Dime?
Spell Sweden	Spell Sweeten
Wet Cloth	What Cloth
Adventures Out Doors	Adventures Outdoors
Lock Test	Luck Test
Sail Directions	Sale Directions
Cell Size	Sell size

2. Test these.
3. Squat existing Skills.

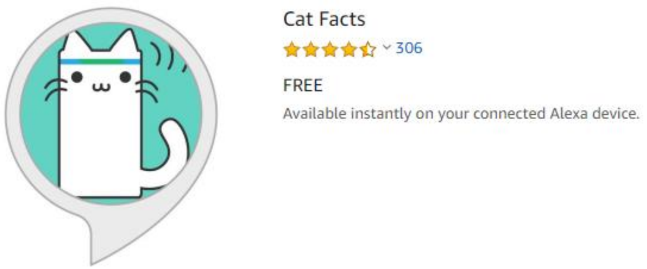


Cat Fats

FREE

Available instantly on your connected Alexa device.

Skill 1	Skill 2
Cat Fats	Cat Facts
Phish Geek	Fish Geek



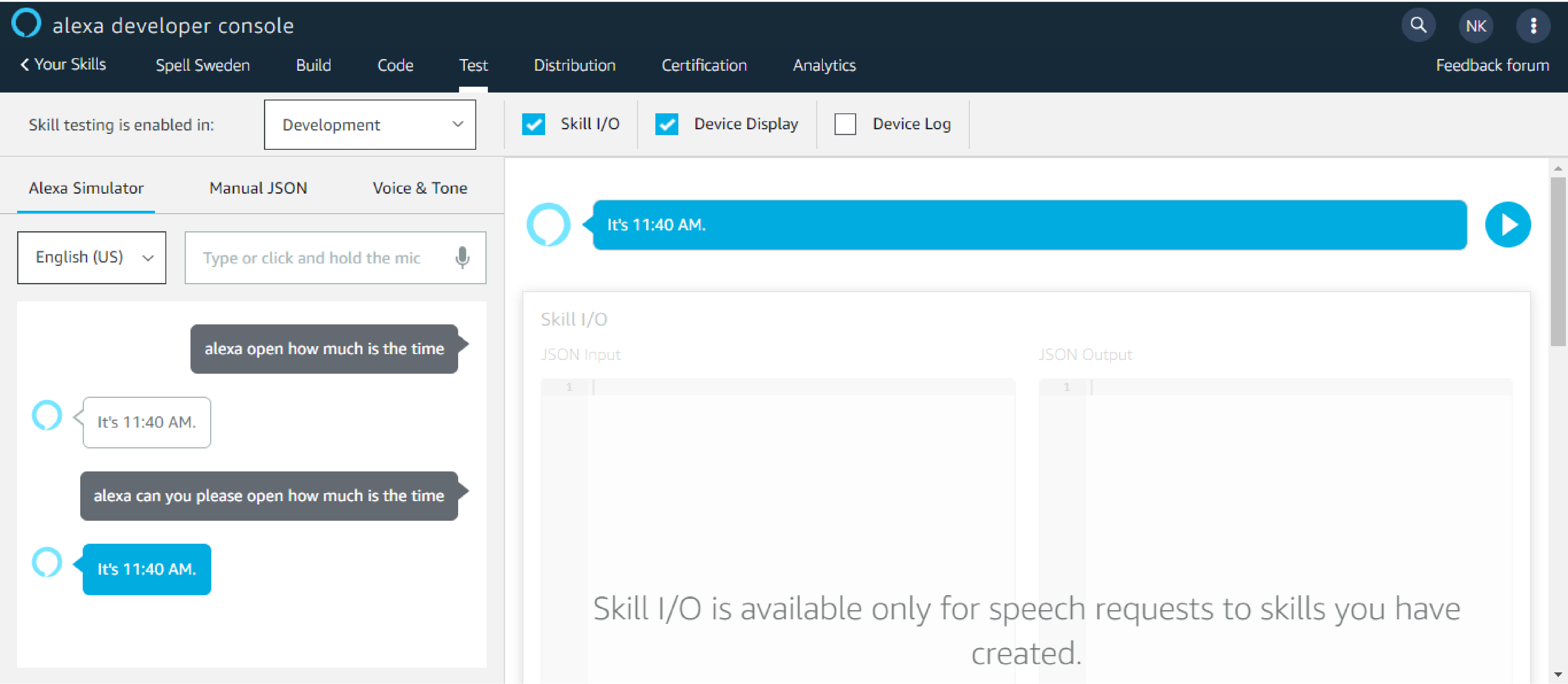
Cat Facts

★★★★☆ ˅ 306

FREE

Available instantly on your connected Alexa device.

“How much is the time” vs “How much is the dime”



Skill testing is enabled in: Development

☑ Skill I/O ☑ Device Display □ Device Log

alexa open how much is the time

It's 11:40 AM.

alexa can you please open how much is the time

It's 11:40 AM.

It's 11:40 AM.

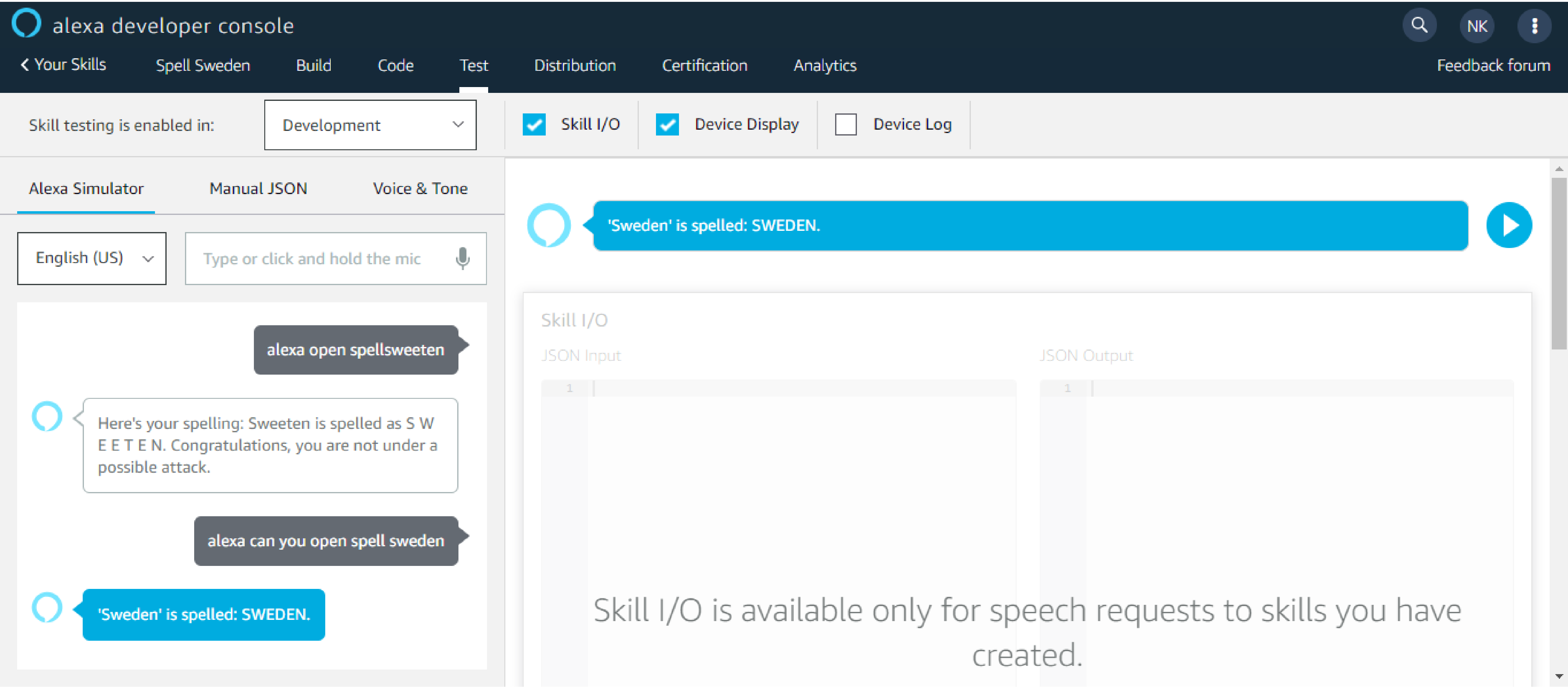
Skill I/O

JSON Input

JSON Output

Skill I/O is available only for speech requests to skills you have created.

“Sweden” vs “Sweeten”



Skill testing is enabled in: Development

☑ Skill I/O ☑ Device Display □ Device Log

English (US)

alexa open spellsweeten

Here's your spelling: Sweeten is spelled as S W E E T E N. Congratulations, you are not under a possible attack.

alexa can you open spell sweden

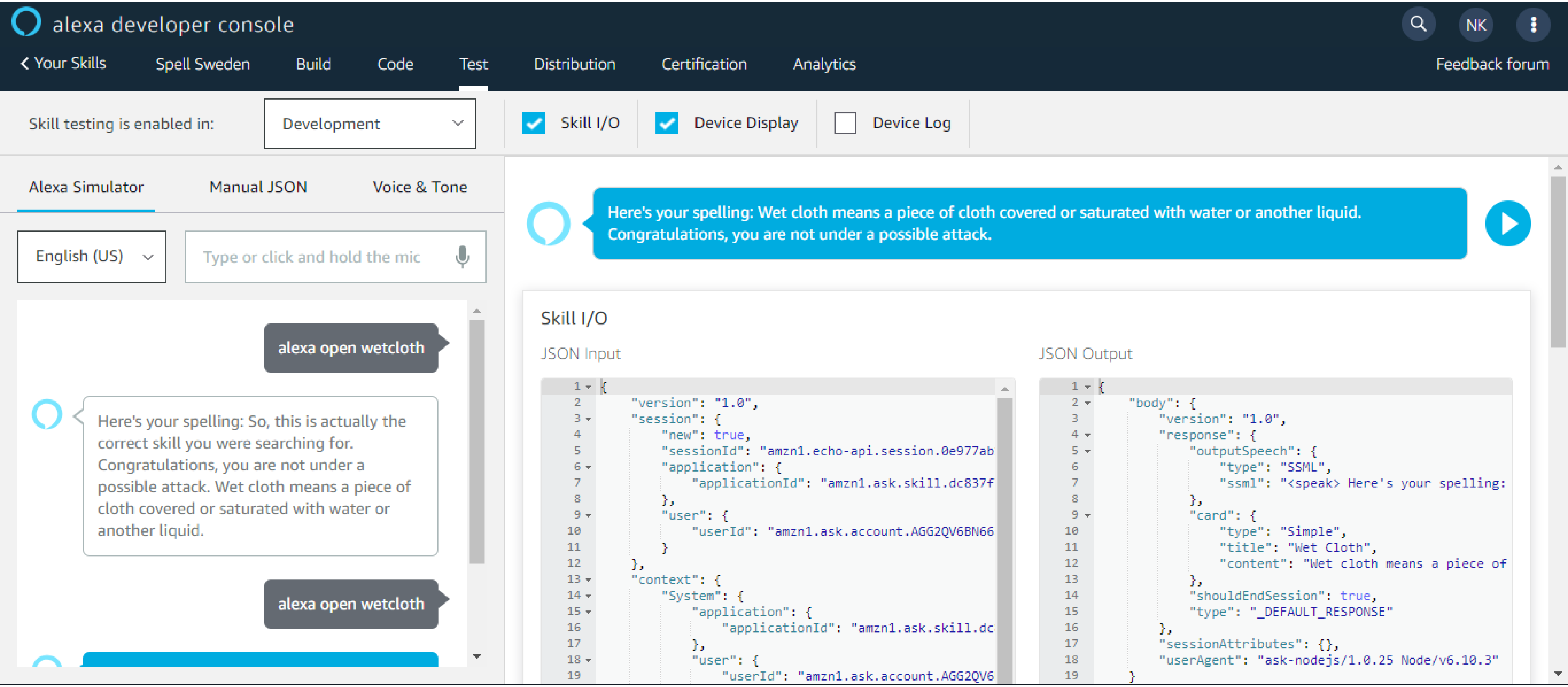
'Sweden' is spelled: SWEDEN.

'Sweden' is spelled: SWEDEN.

Skill I/O

Skill I/O is available only for speech requests to skills you have created.

“Wet” vs “What”



Skill testing is enabled in: Development

☑ Skill I/O ☑ Device Display □ Device Log

English (US)

alexa open wetcloth

Here's your spelling: So, this is actually the correct skill you were searching for. Congratulations, you are not under a possible attack. Wet cloth means a piece of cloth covered or saturated with water or another liquid.

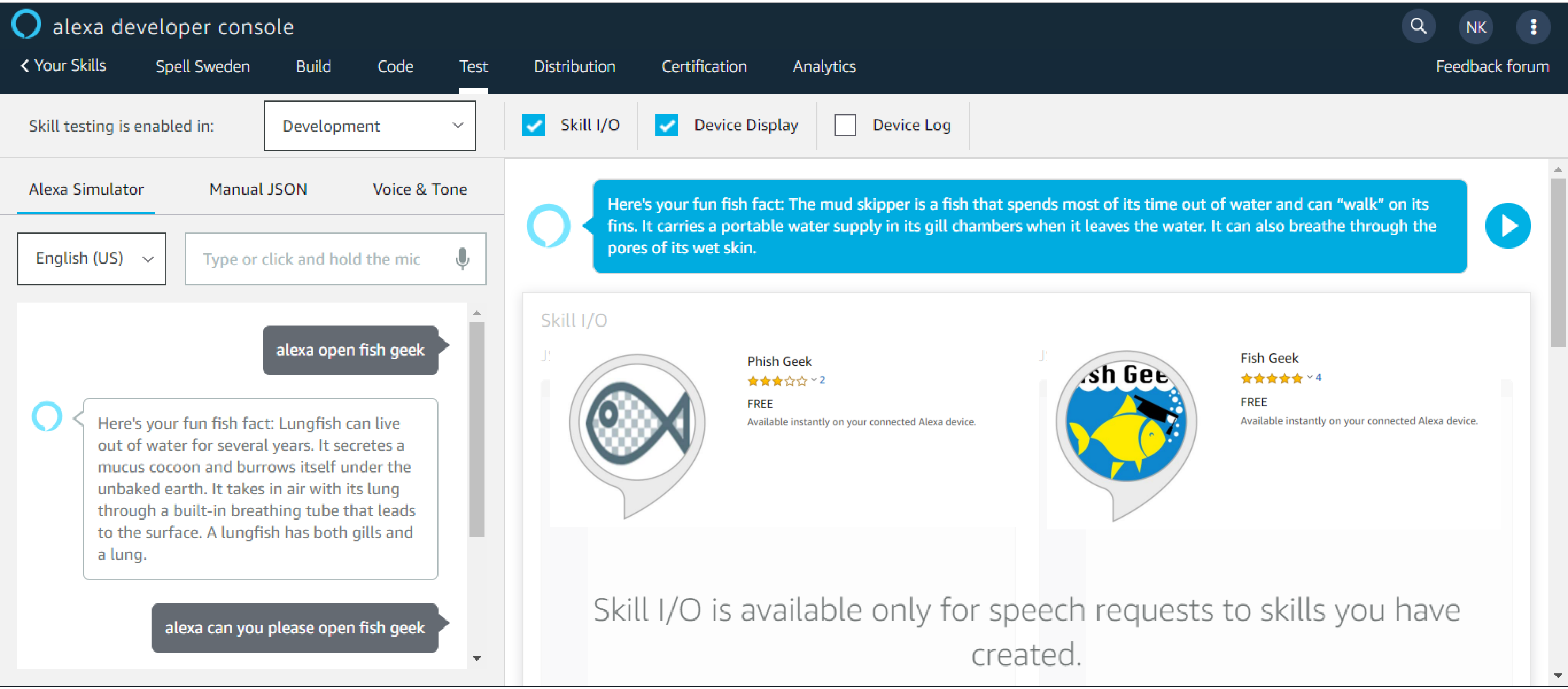
alexa open wetcloth

Here's your spelling: Wet cloth means a piece of cloth covered or saturated with water or another liquid. Congratulations, you are not under a possible attack.

```
{
    "version": "1.0",
    "session": {
        "new": true,
        "sessionId": "amzn1.echo-api.session.0e977ab
        "application": {
            "applicationId": "amzn1.ask.skill.dc837f
        },
        "user": {
            "userId": "amzn1.ask.account.AGG2QV6BN66
        }
    },
    "context": {
        "System": {
            "application": {
                "applicationId": "amzn1.ask.skill.dc
            },
            "user": {
                "userId": "amzn1.ask.account.AGG2QV6
```

```
{
    "body": {
        "version": "1.0",
        "response": {
            "outputSpeech": {
                "type": "SSML",
                "ssml": "<speak> Here's your spelling:
            },
            "card": {
                "type": "Simple",
                "title": "Wet Cloth",
                "content": "Wet cloth means a piece of
            },
            "shouldEndSession": true,
            "type": "_DEFAULT_RESPONSE"
        },
        "sessionAttributes": {},
        "userAgent": "ask-nodejs/1.0.25 Node/v6.10.3"
    }
```

“Phish” vs “Fish”



Skill testing is enabled in: Development

☑ Skill I/O ☑ Device Display □ Device Log

English (US)

alexa open fish geek

Here's your fun fish fact: Lungfish can live out of water for several years. It secretes a mucus cocoon and burrows itself under the unbaked earth. It takes in air with its lung through a built-in breathing tube that leads to the surface. A lungfish has both gills and a lung.

alexa can you please open fish geek

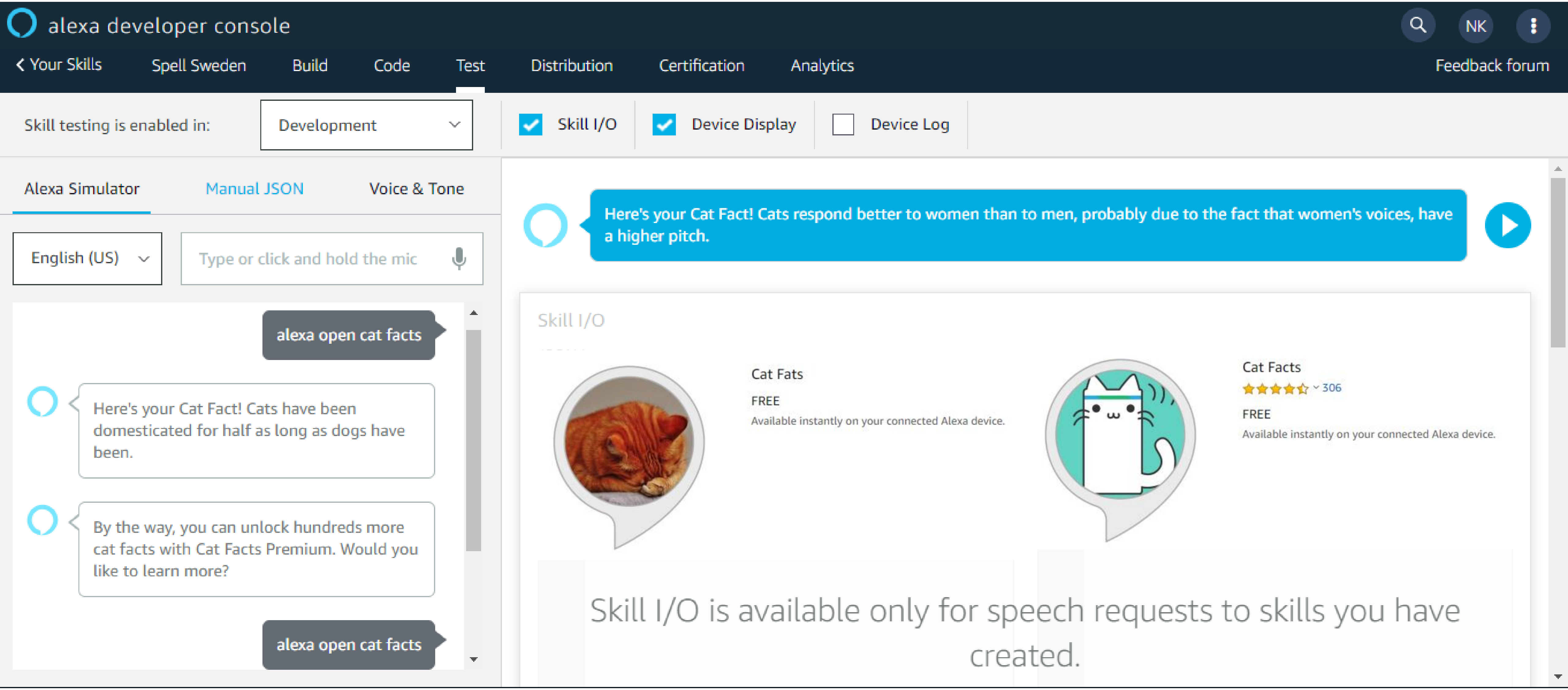
Here's your fun fish fact: The mud skipper is a fish that spends most of its time out of water and can “walk” on its fins. It carries a portable water supply in its gill chambers when it leaves the water. It can also breathe through the pores of its wet skin.

Phish Geek
★★★☆☆ 2
FREE
Available instantly on your connected Alexa device.

Fish Geek
★★★★★ 4
FREE
Available instantly on your connected Alexa device.

Skill I/O is available only for speech requests to skills you have created.

“Fats” vs “Facts”



Skill testing is enabled in: Development

☑ Skill I/O ☑ Device Display □ Device Log

English (US)

Type or click and hold the mic

alexa open cat facts

Here's your Cat Fact! Cats have been domesticated for half as long as dogs have been.

By the way, you can unlock hundreds more cat facts with Cat Facts Premium. Would you like to learn more?

alexa open cat facts

Here's your Cat Fact! Cats respond better to women than to men, probably due to the fact that women's voices, have a higher pitch.

Skill I/O

Cat Fats
FREE
Available instantly on your connected Alexa device.

Cat Facts
★★★★☆ 306
FREE
Available instantly on your connected Alexa device.

Skill I/O is available only for speech requests to skills you have created.

- Attacks in this project are tested only in a controlled, developer environment.

- Care is taken not to produce ay malicious skill to the public skill store.

Drawback

- Unavailability of NSP dataset.
- Until now testing is based on a single user.

Drawback

1. Testing with different user inputs for the same skills.

2. Extending skill squatting attacks to Spear Skill squatting attacks which is based on interpretation of words based on demography and gender.

3. Extend the project to Word Squatting attacks on the currently available Skills.

Next Steps

Thank You!