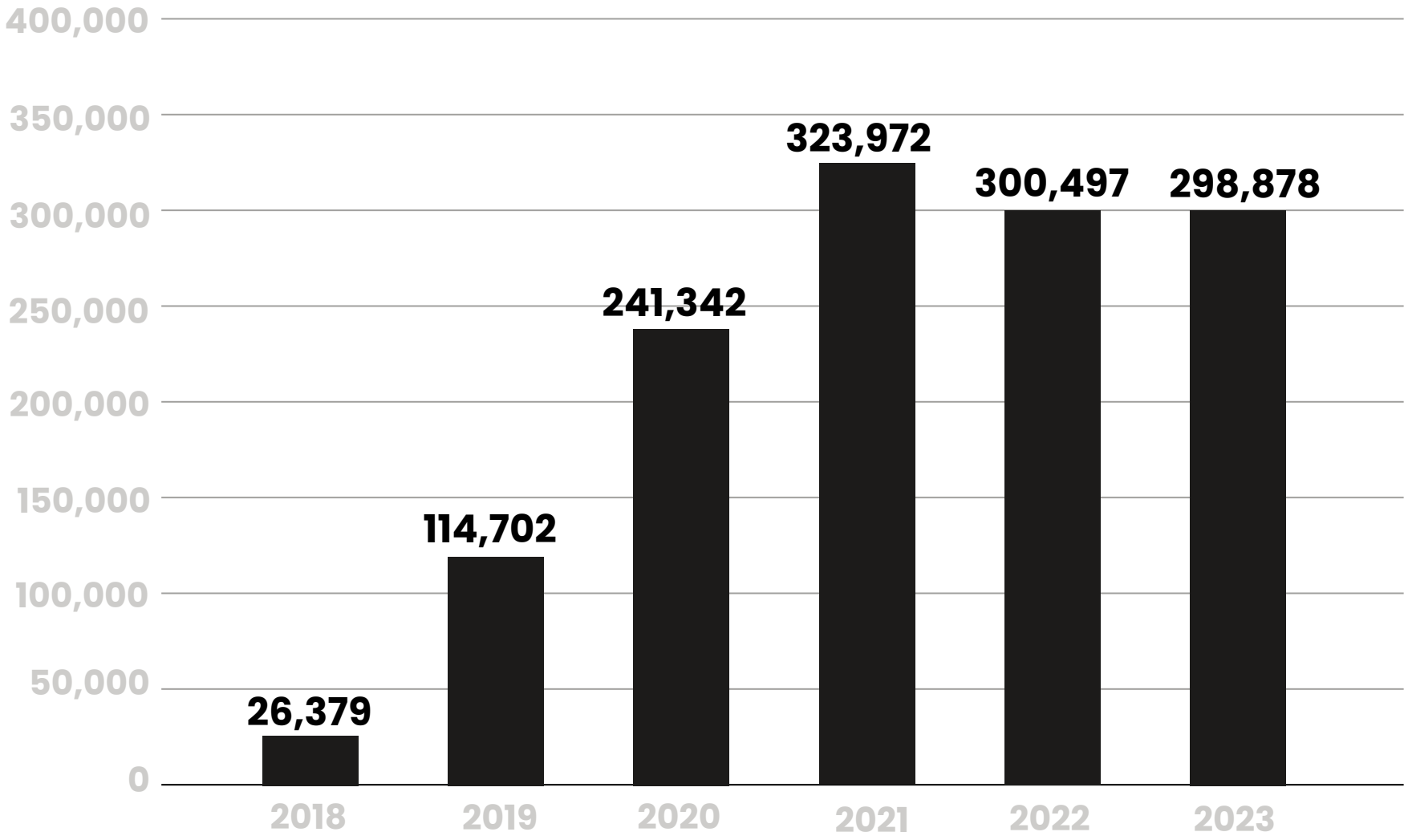
Less Defined Knowledge and More True Alarms: Reference-based Phishing Detection without a Pre-defined Reference List

Ruofan Liu, Yun Lin, Xiwen Teoh,
Gongshen Liu, Zhiyong Huang, Jin Song Dong

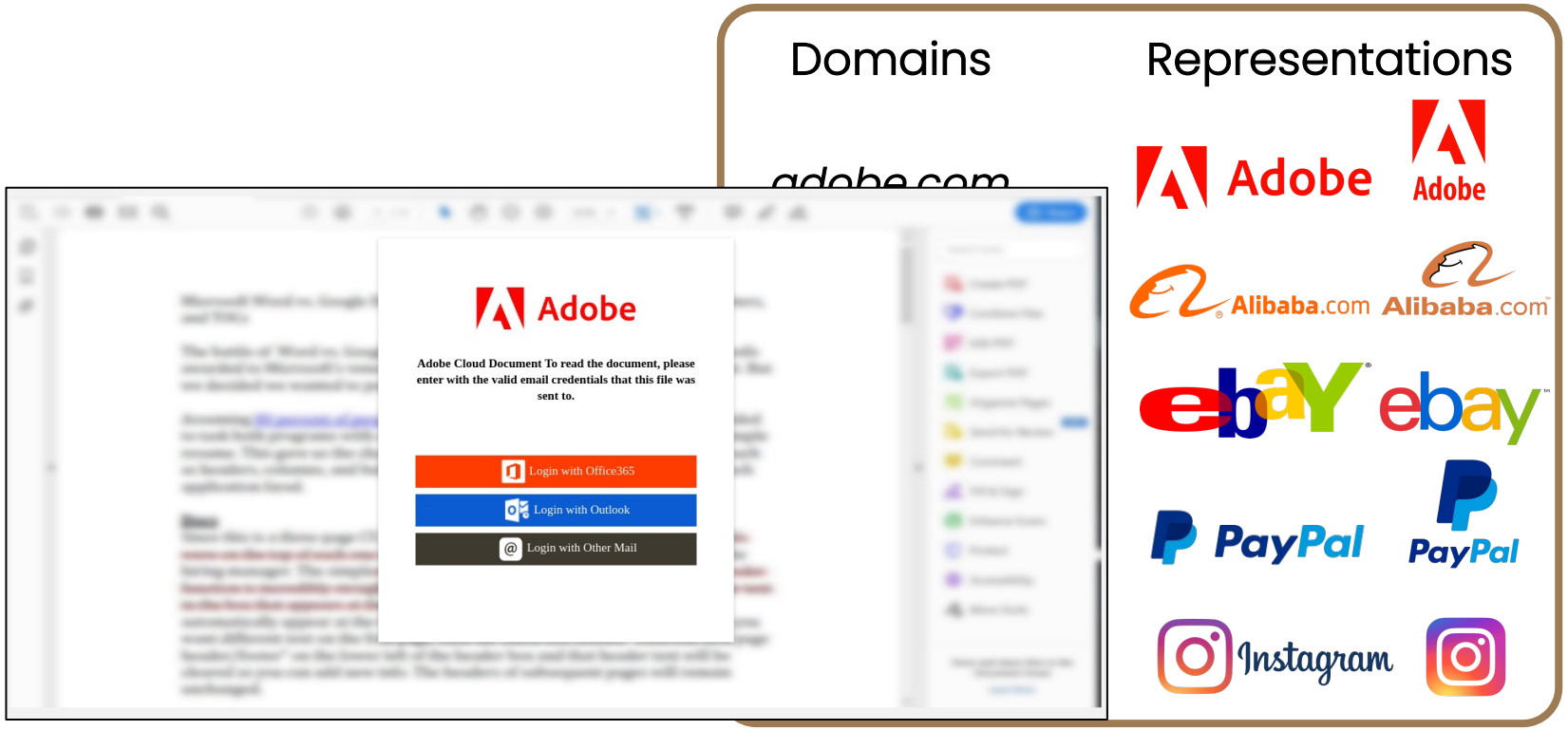
Shanghai Jiao Tong University,
National University of Singapore



Number of phishing attack victims in the United States [1]

[1] Statista. https://www.statista.com/statistics/1390362/phishing-victim-number-us/

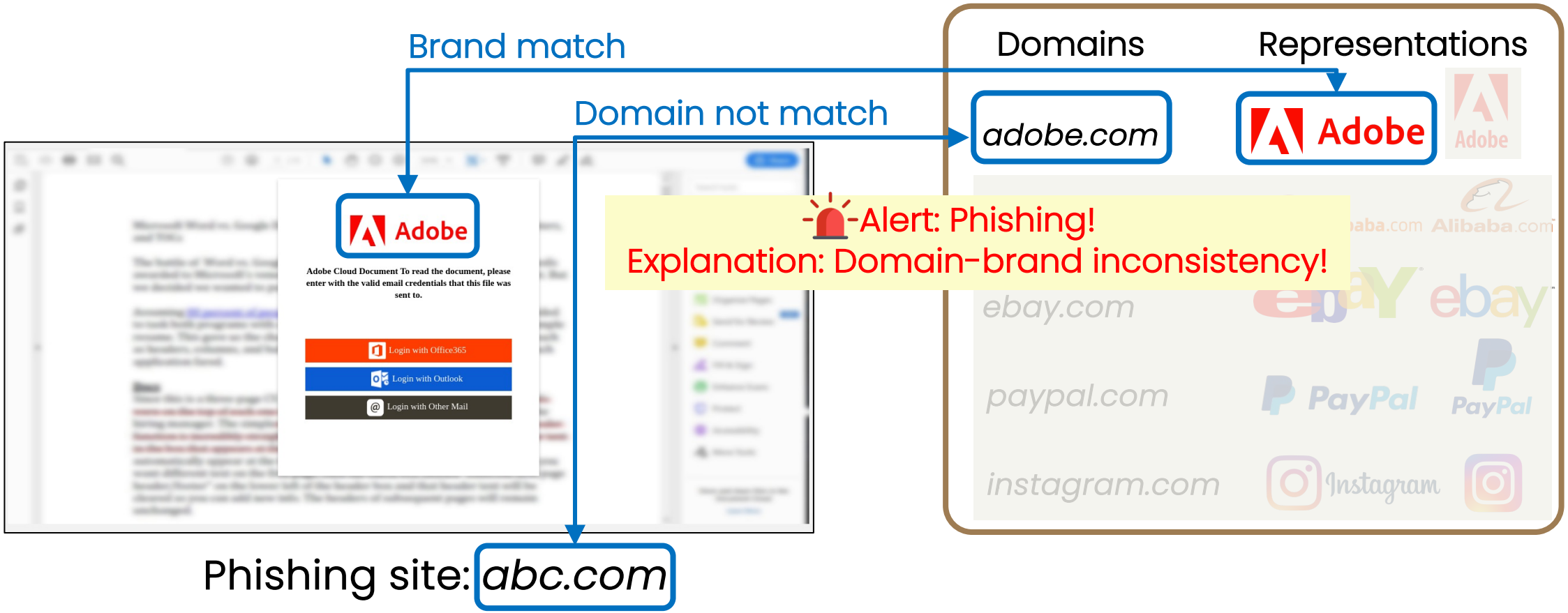
Reference-based Phishing Detection

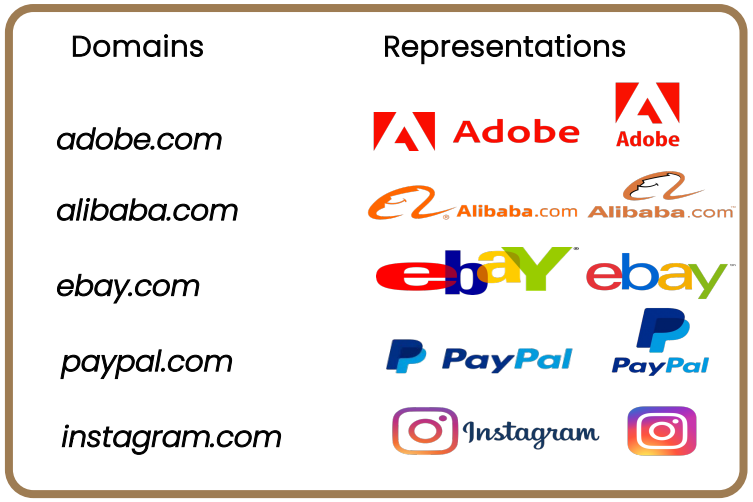


Phishing site: *abc.com*

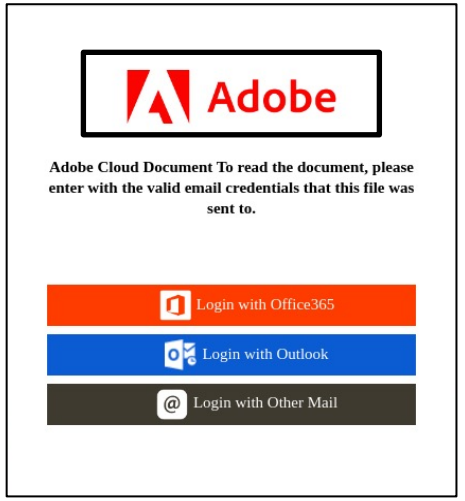
Reference list

Reference-based Phishing Detection





Reference list



"Look" at the logo

2020 — VisualPhishNet (CCS)

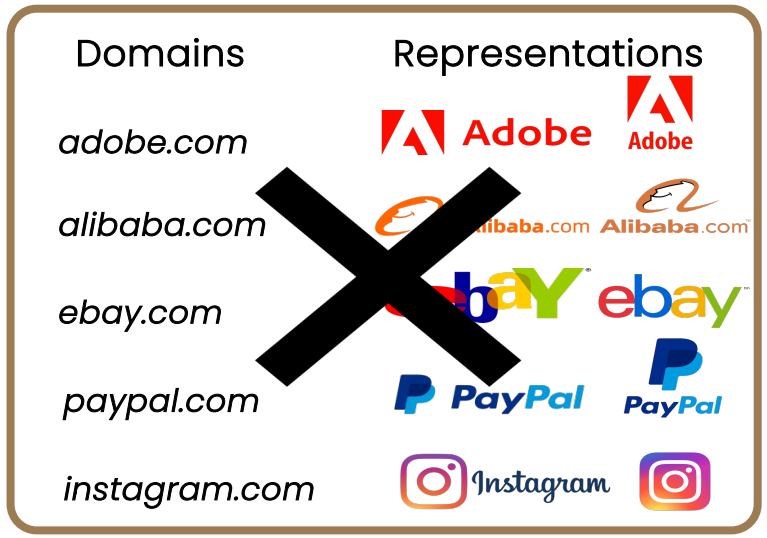
2021 — Phishpedia (USENIX Sec)

2022 — PhishIntention (USENIX Sec)

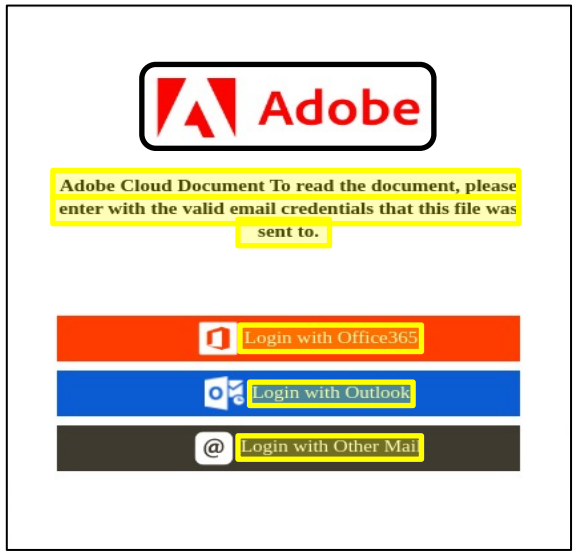
2023 — DynaPhish (USENIX Sec)

2024 — NEW — PhishLLM (Ours)

PhishLLM

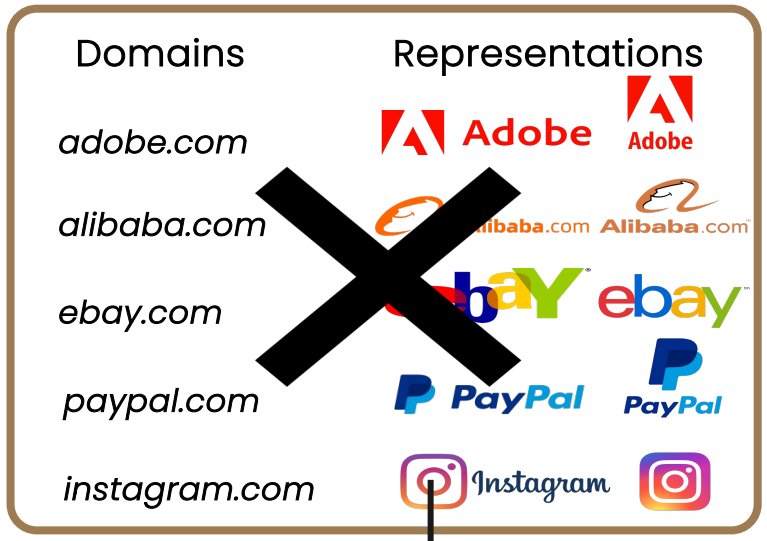


Reference list free



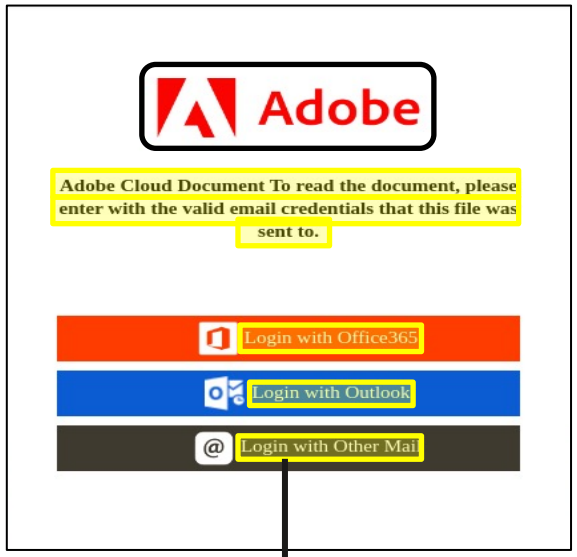
"Look" and "Read"

PhishLLM



Reference list free

LLM is a comprehensive knowledge base



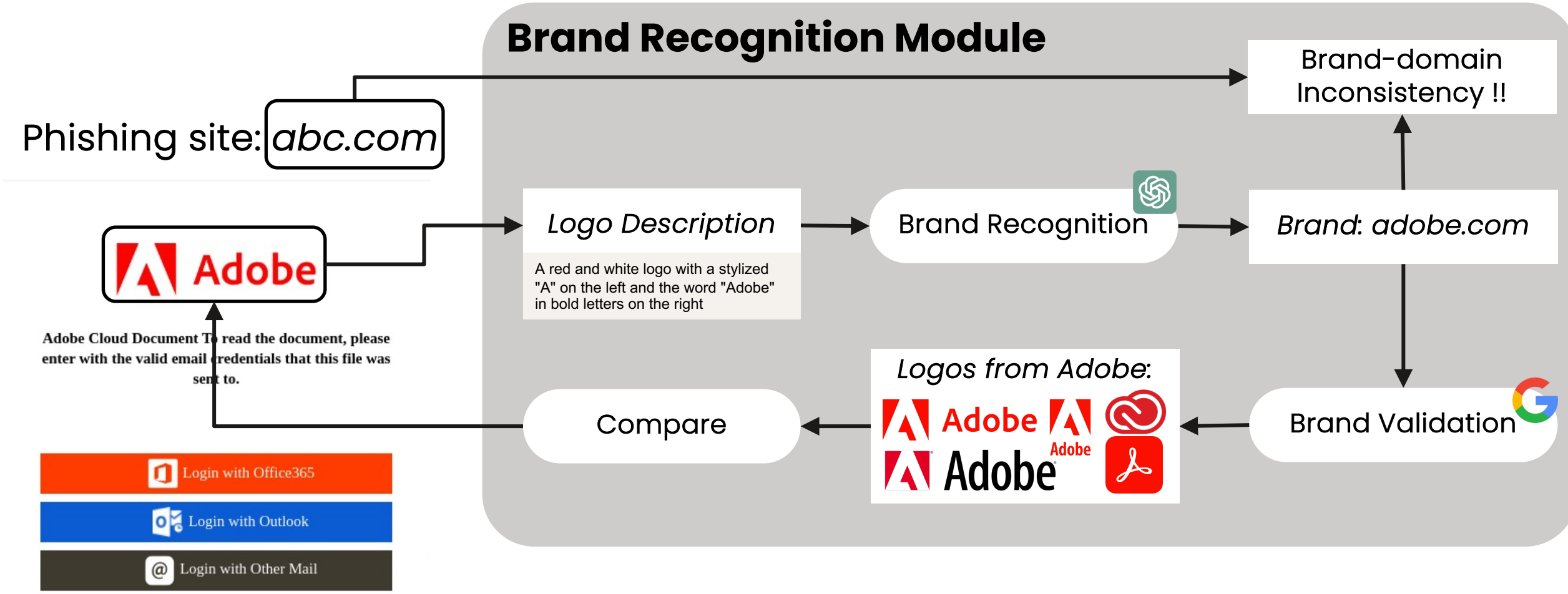
"Look" and "Read"

LLM is good at understanding and reasoning with textual semantics

Reference list free

"Look" and "Read"

PhishLLM

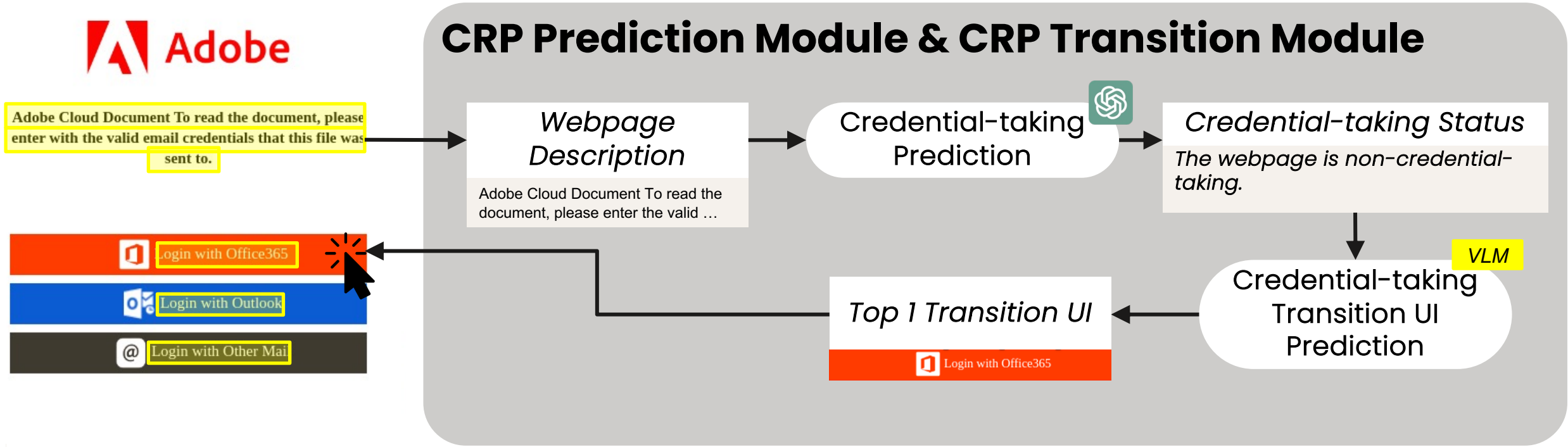


Reference list free

"Look" and "Read"

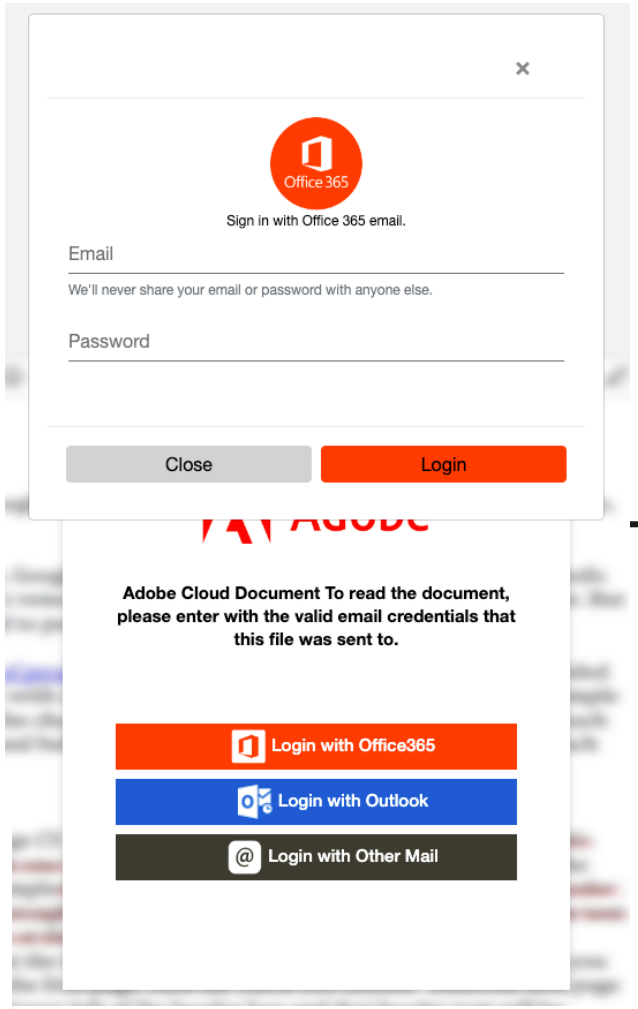
PhishLLM

Phishing site: *abc.com*



PhishLLM

Phishing site: *abc.com*



CRP Prediction Module & CRP Transition Module

Webpage Description

Sign in with Office 365 email. Email. Password. Close. Login

Credential-taking Prediction

Credential-taking Status

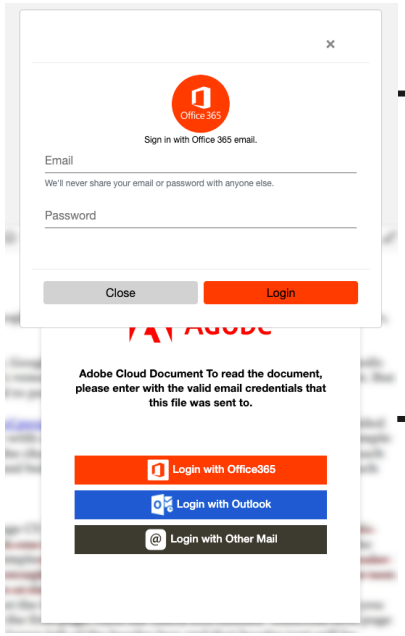
The webpage is credential-taking.

Reference list free

"Look" and "Read"

PhishLLM

Phishing site: *abc.com*



Brand Recognition Module

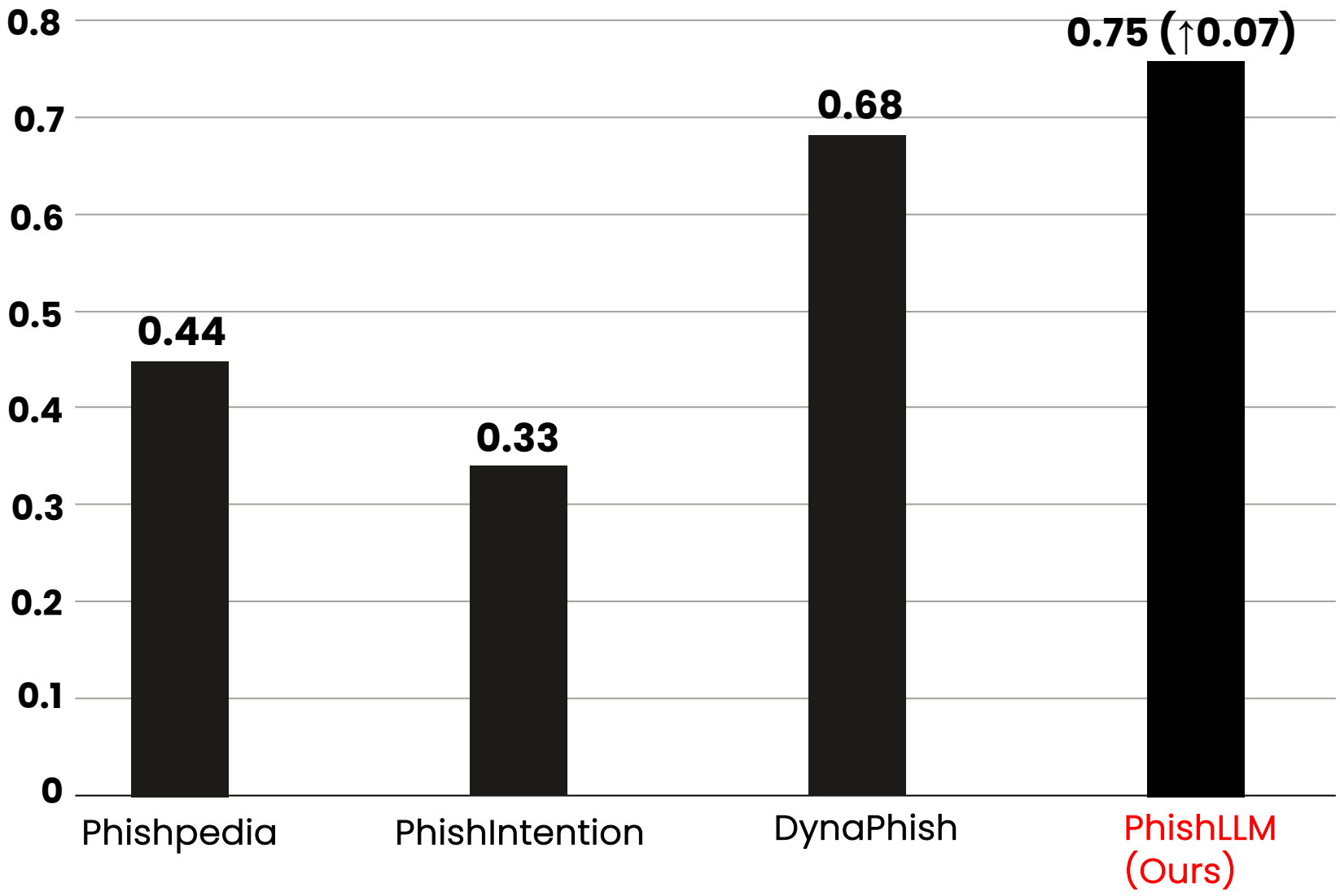
Logo Description → Brand Recognition → *Brand: office.com* → Brand-domain Inconsistency

CRP Prediction Module & CRP Transition Module

Webpage Description → *CRP Prediction* → *Credential-taking Status* → Credential-taking Intention

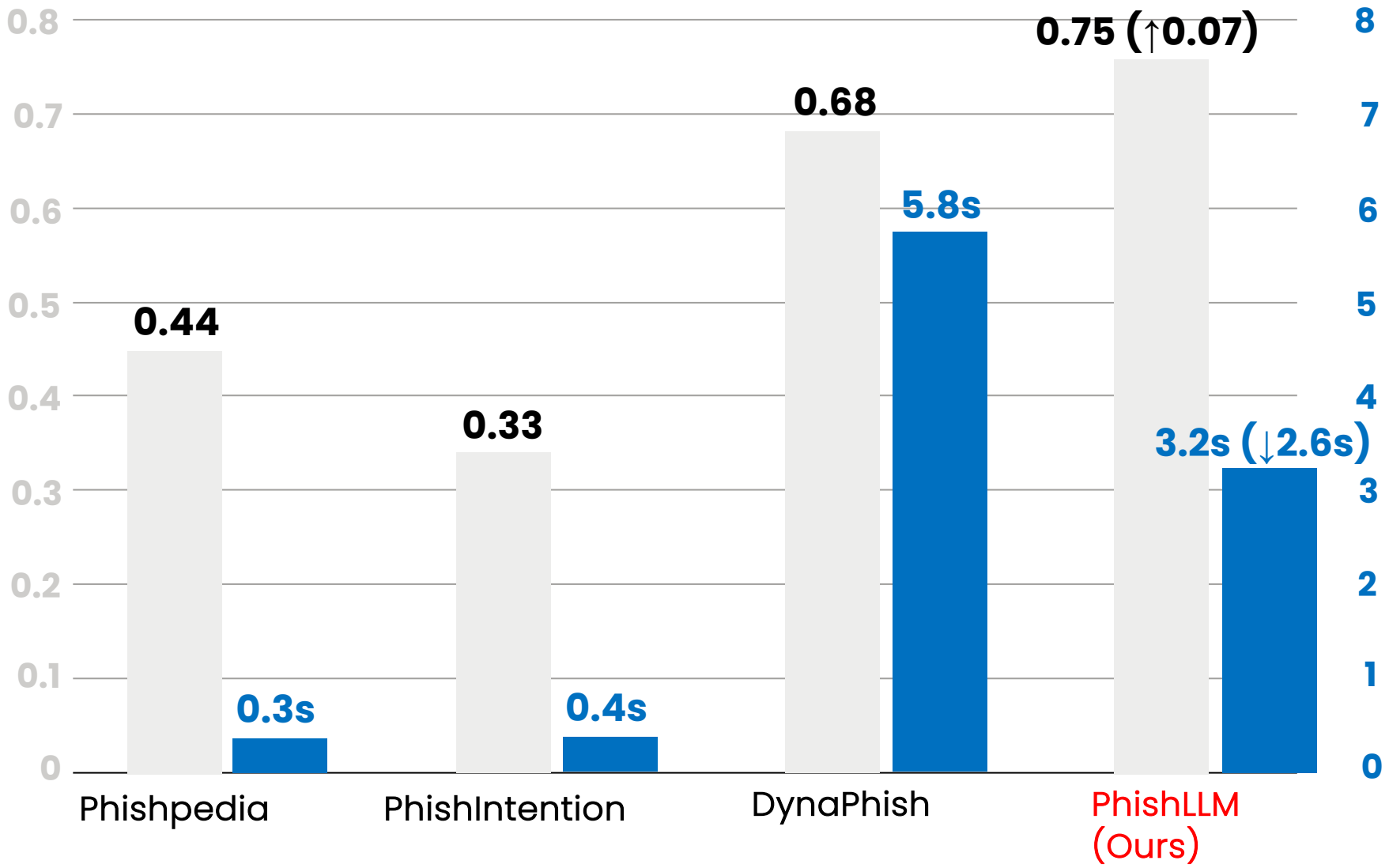
Brand-domain Inconsistency, Credential-taking Intention → Phishing Alert

Recall on DynaPD [2] Dataset



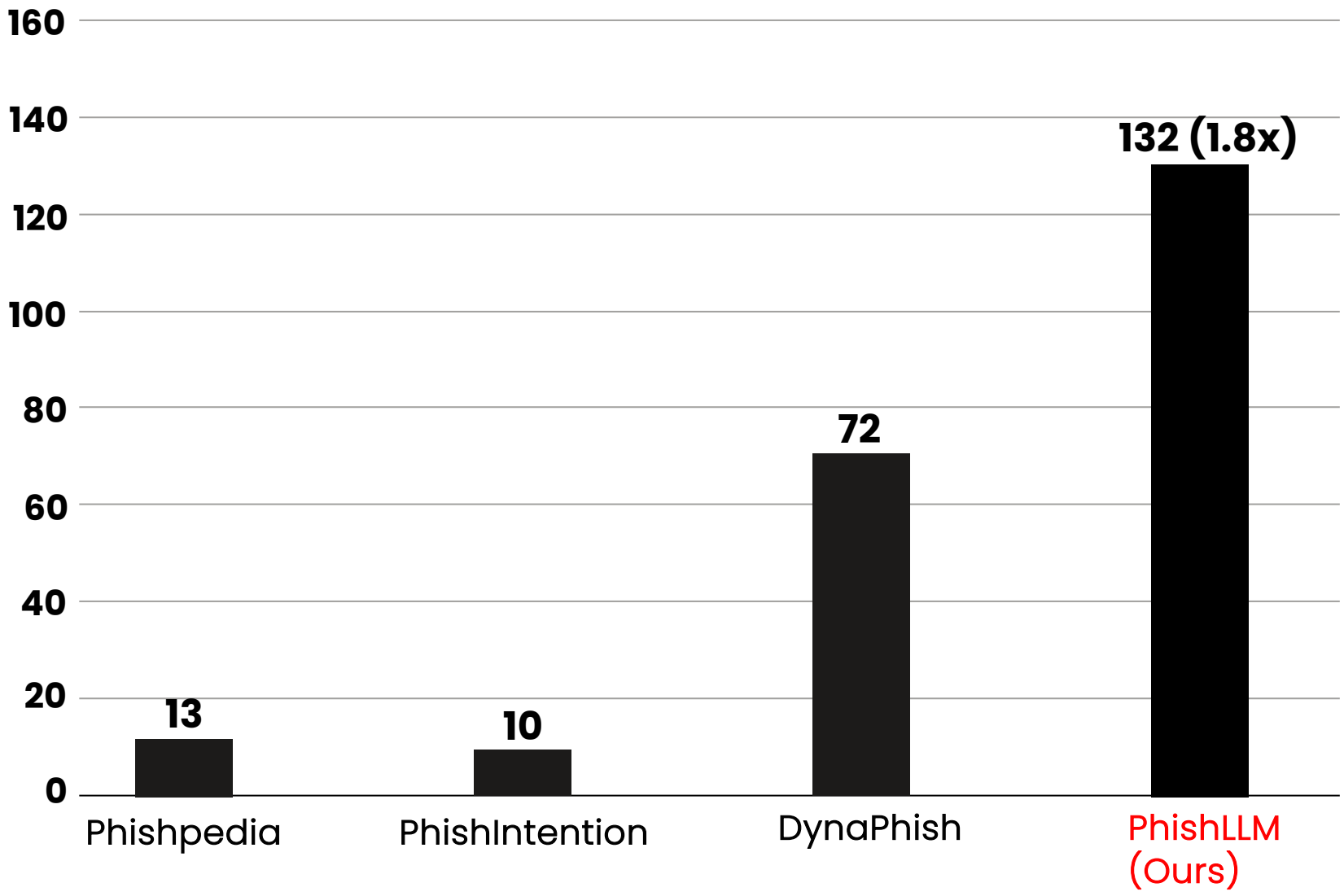
[2] Liu, R., Lin, Y., Zhang, Y., Lee, P. H., & Dong, J. S. (2023). Knowledge Expansion and Counterfactual Interaction for {Reference-Based} Phishing Detection. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 4139-4156).

Runtime on DynaPD [2] Dataset

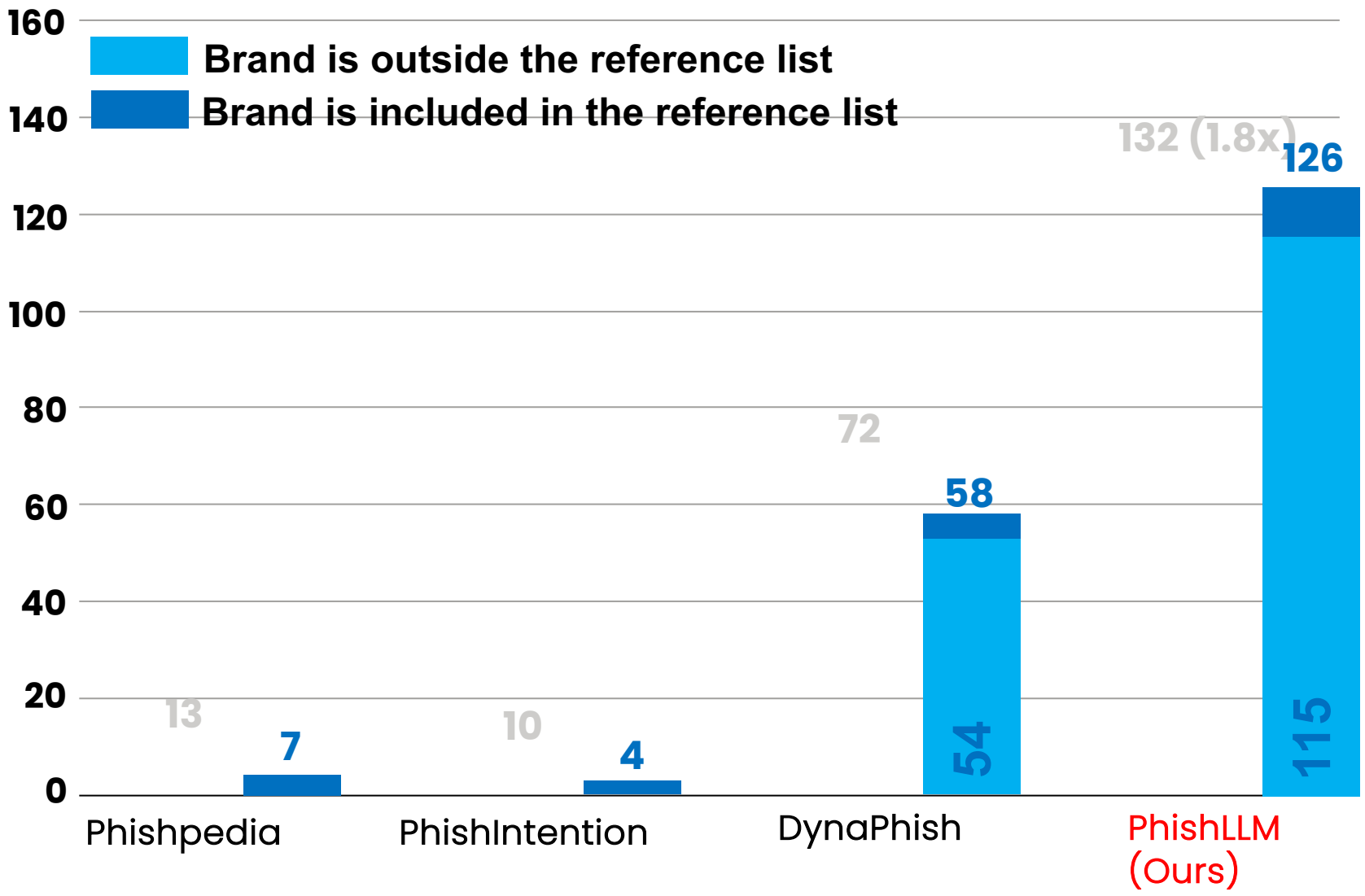


[2] Liu, R., Lin, Y., Zhang, Y., Lee, P. H., & Dong, J. S. (2023). Knowledge Expansion and Counterfactual Interaction for {Reference-Based} Phishing Detection. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 4139-4156).

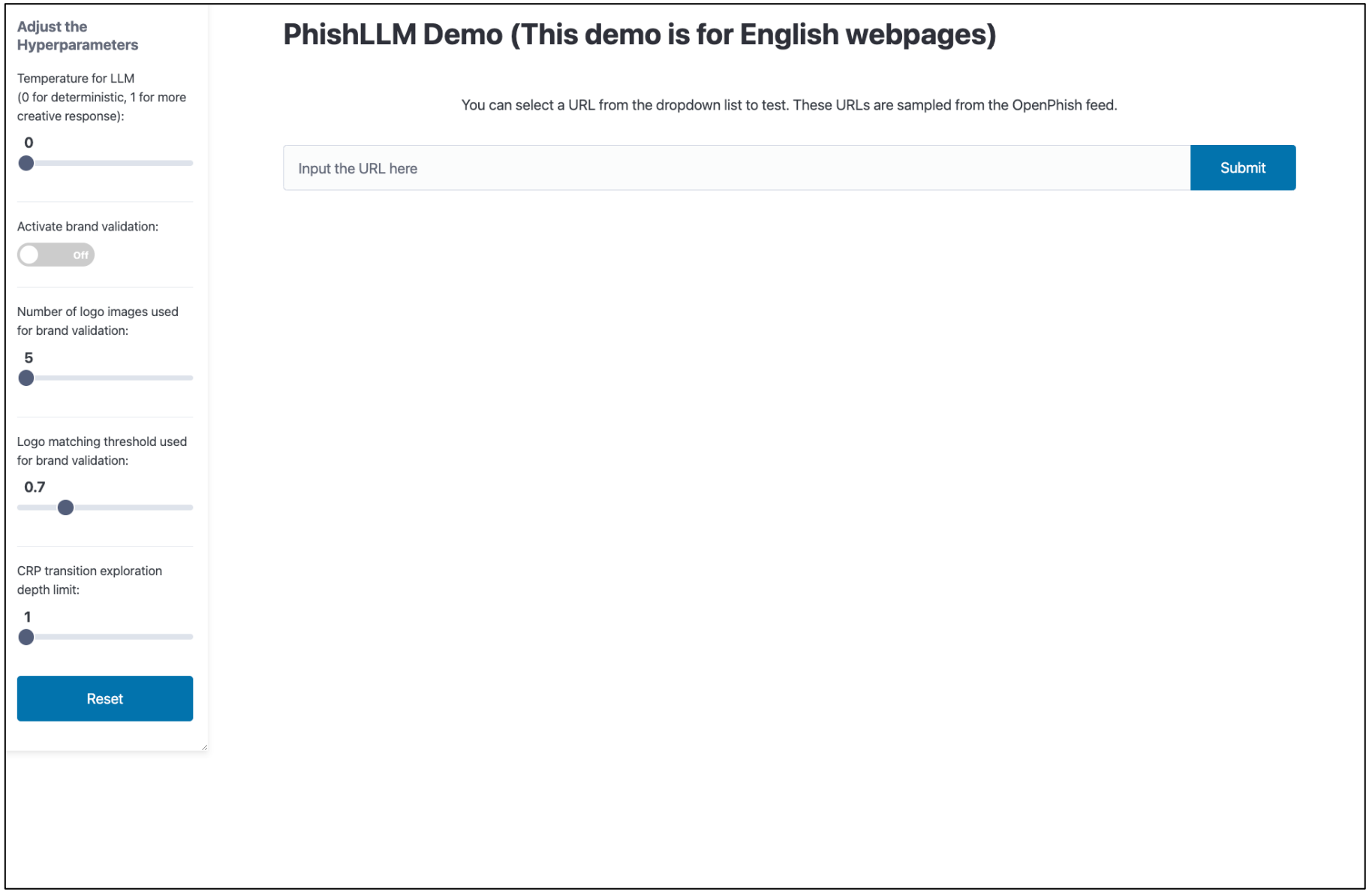
Reported Phishing in the Wild (one-week)



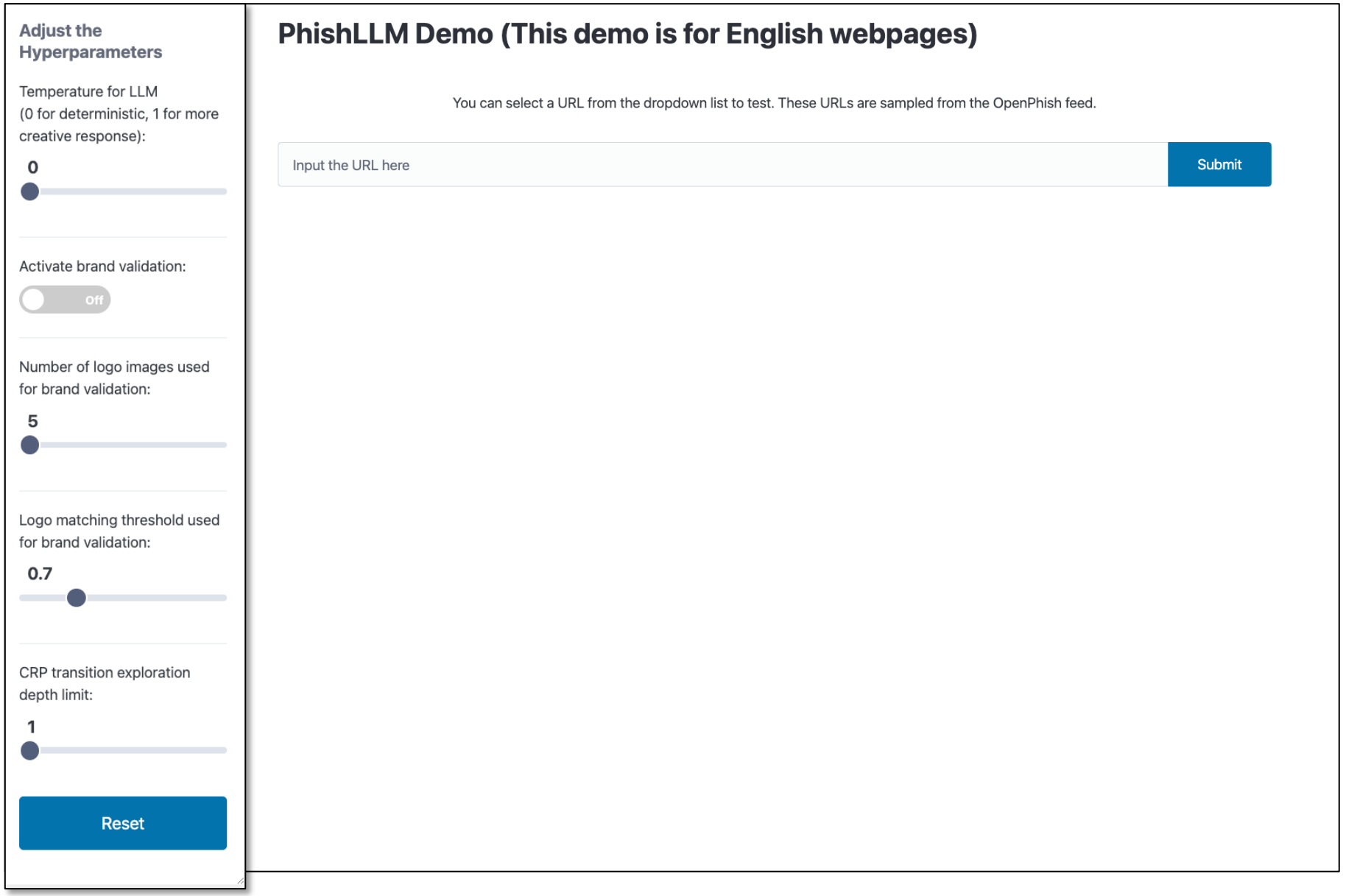
No. Distinct Target Brands Covered by the Reported Phishing



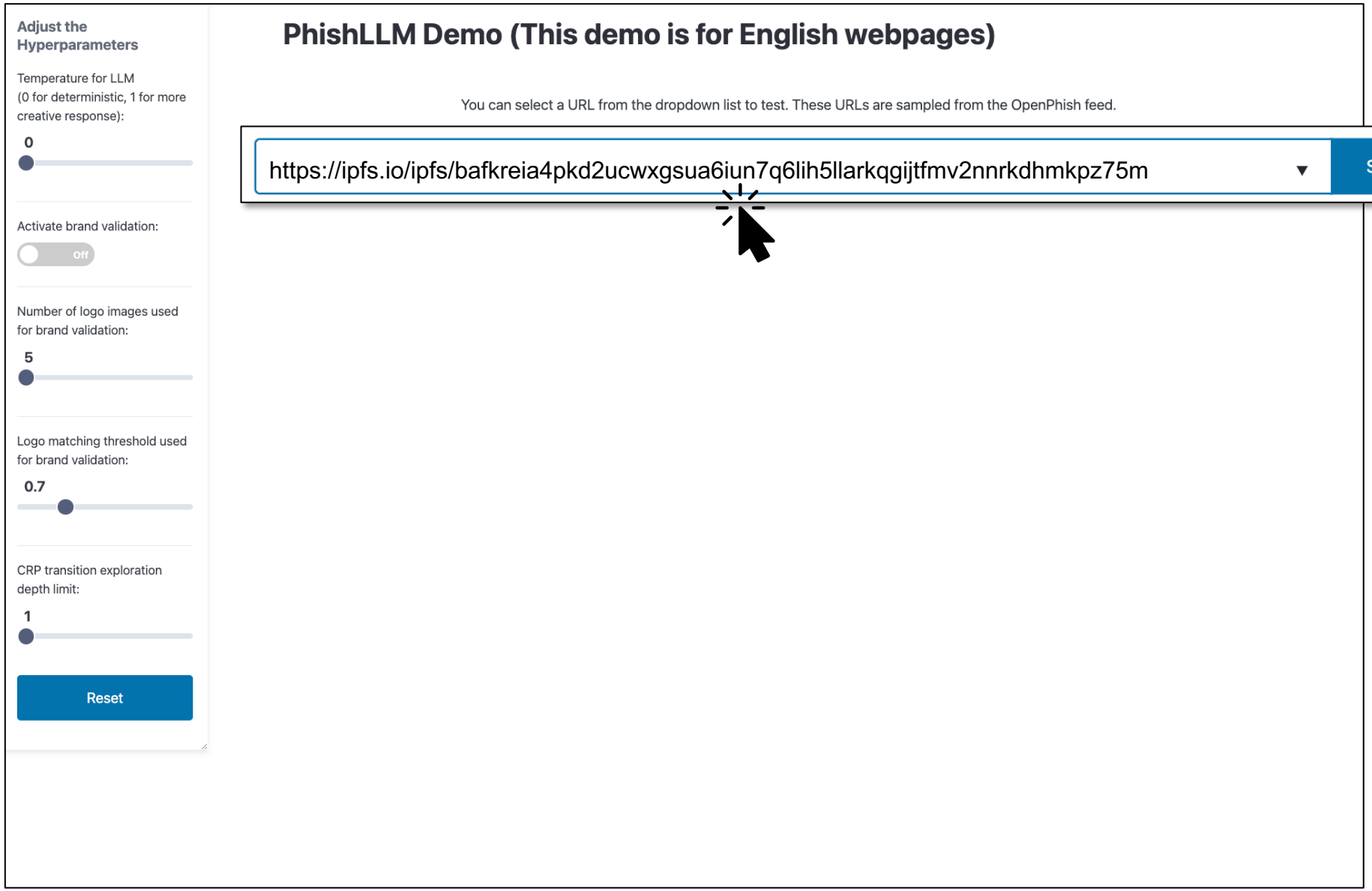
Demo Site: http://34.204.95.231:6789/



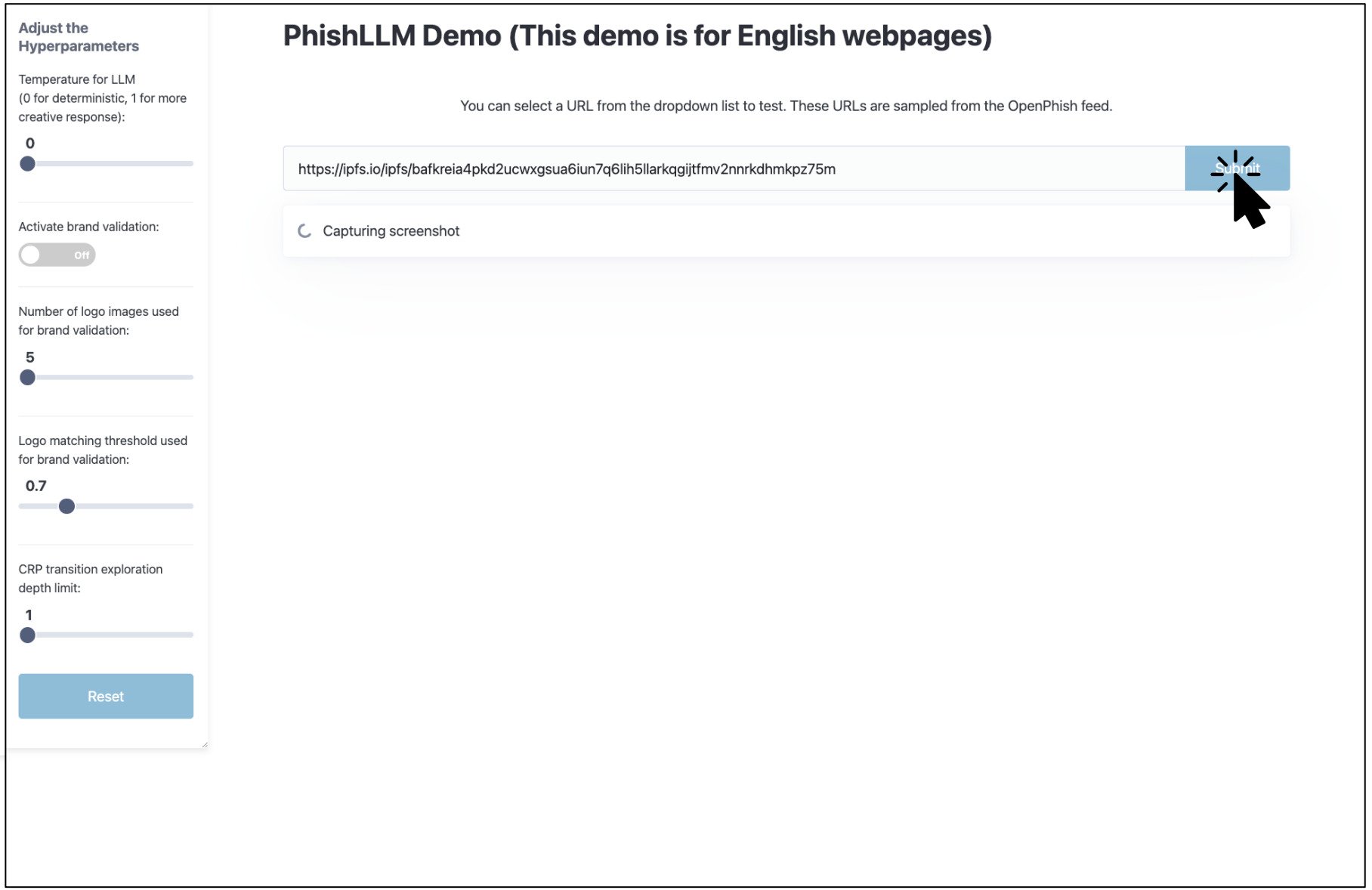
Demo Site: http://34.204.95.231:6789/



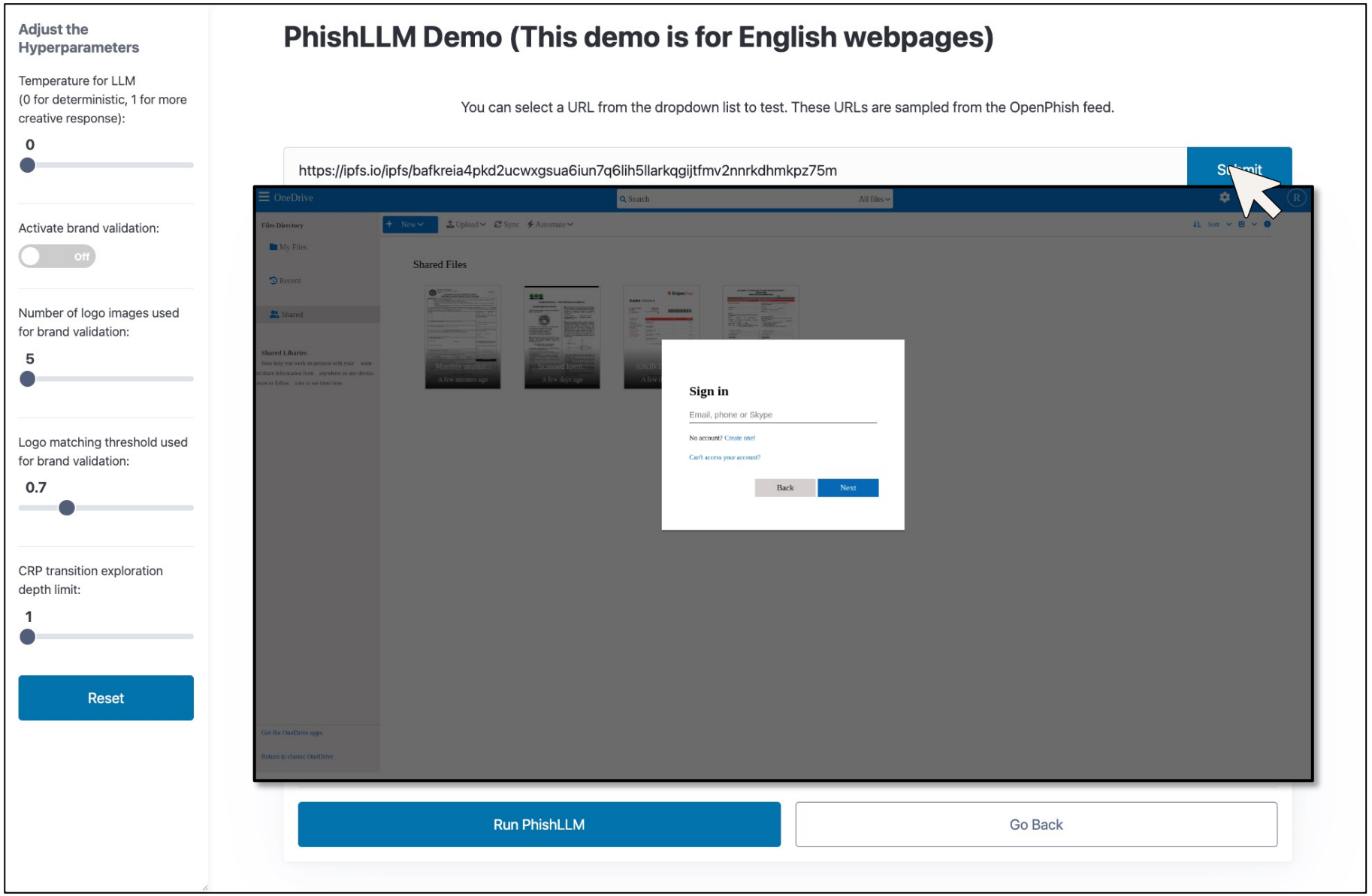
Demo Site: http://34.204.95.231:6789/



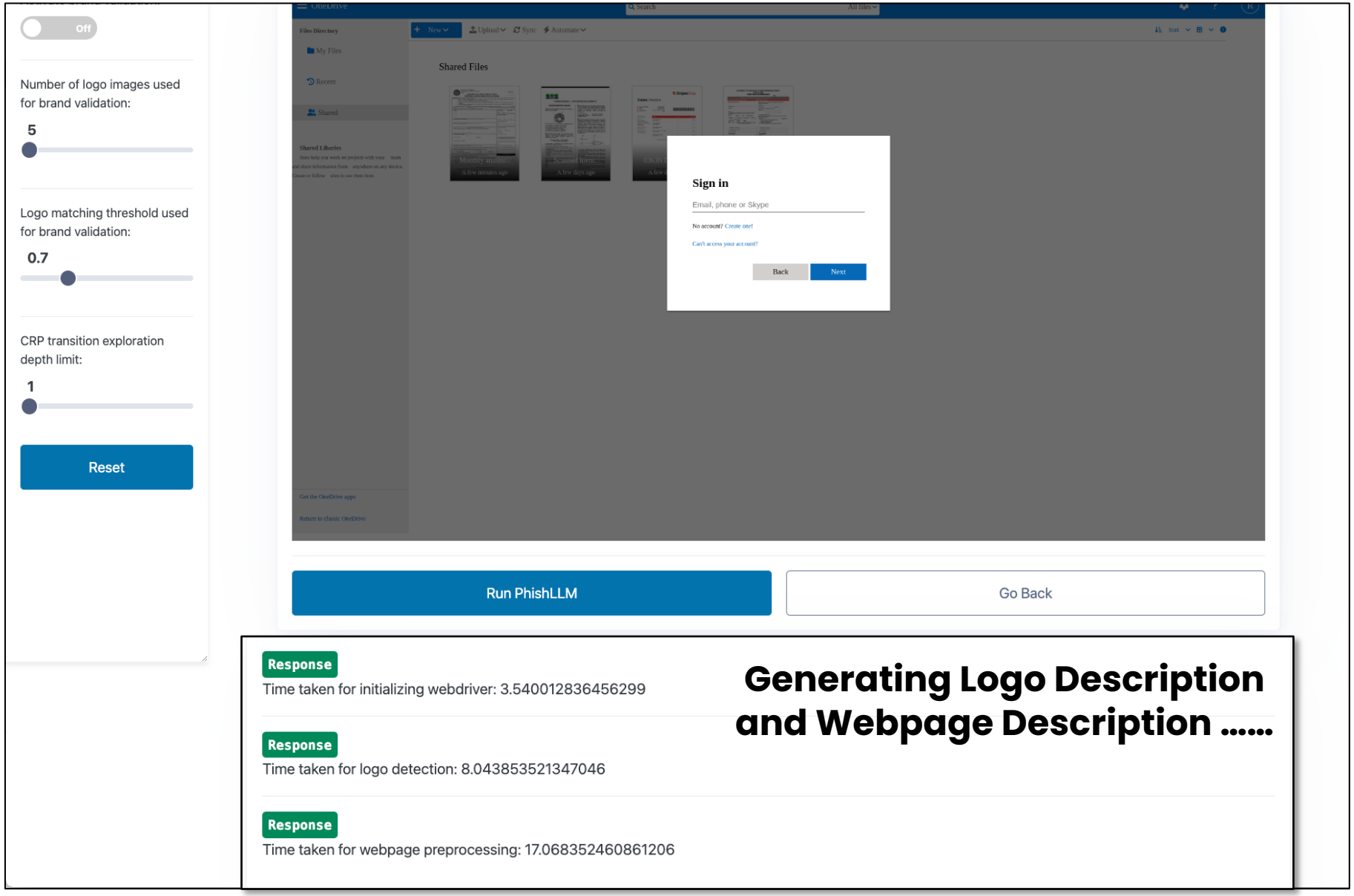
Demo Site: http://34.204.95.231:6789/



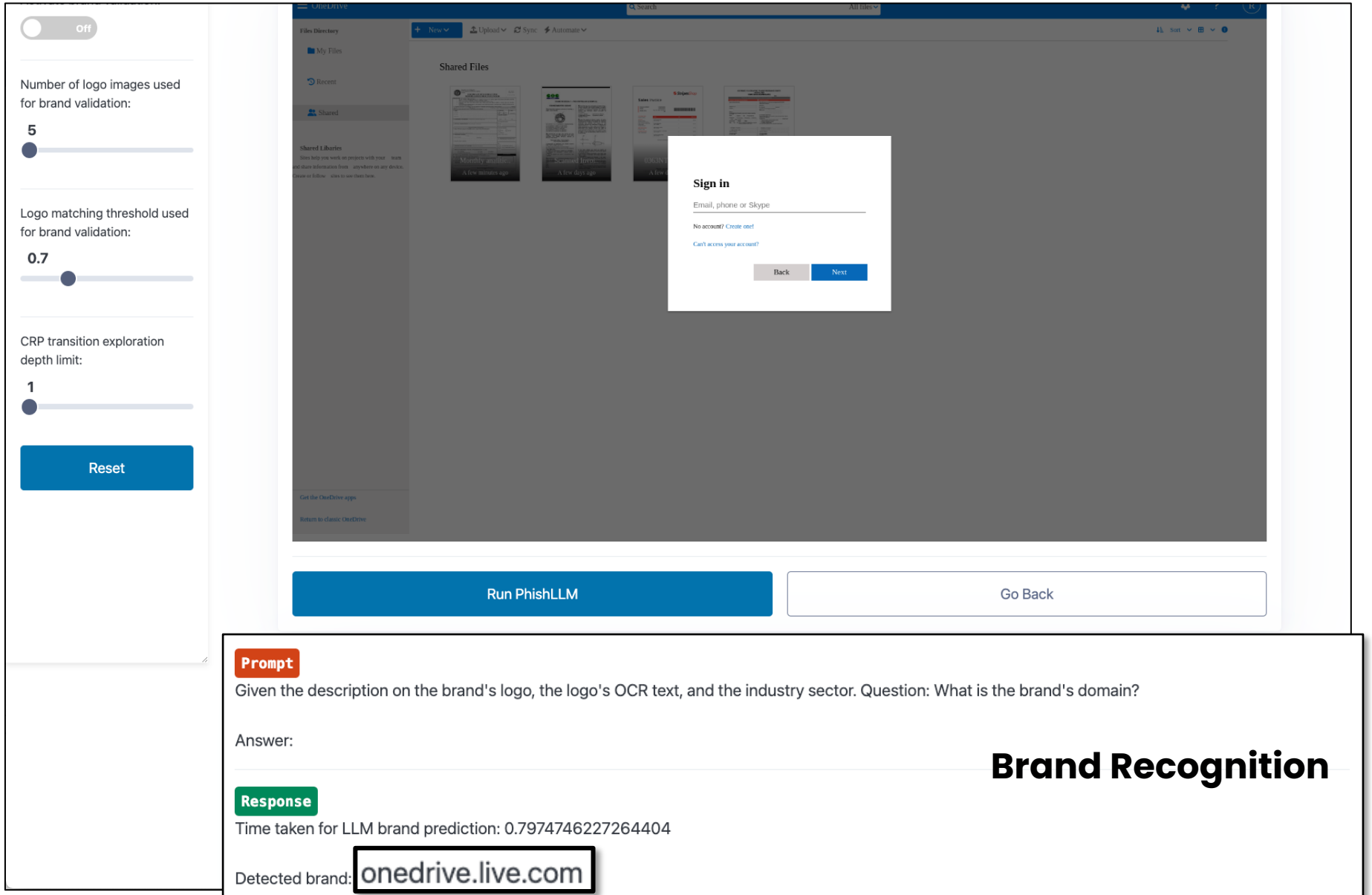
Demo Site: http://34.204.95.231:6789/



Demo Site: http://34.204.95.231:6789/

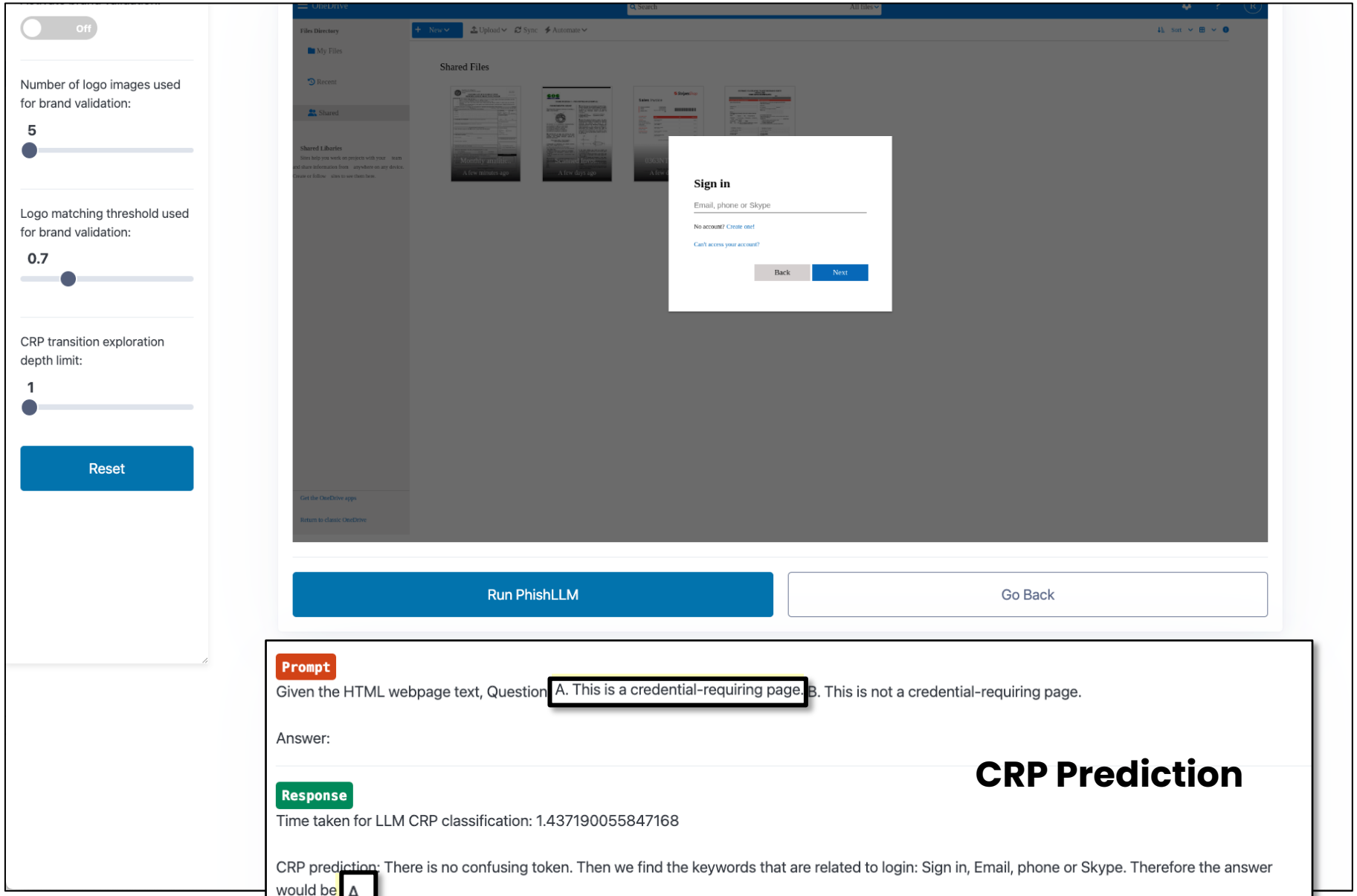


Demo Site: http://34.204.95.231:6789/

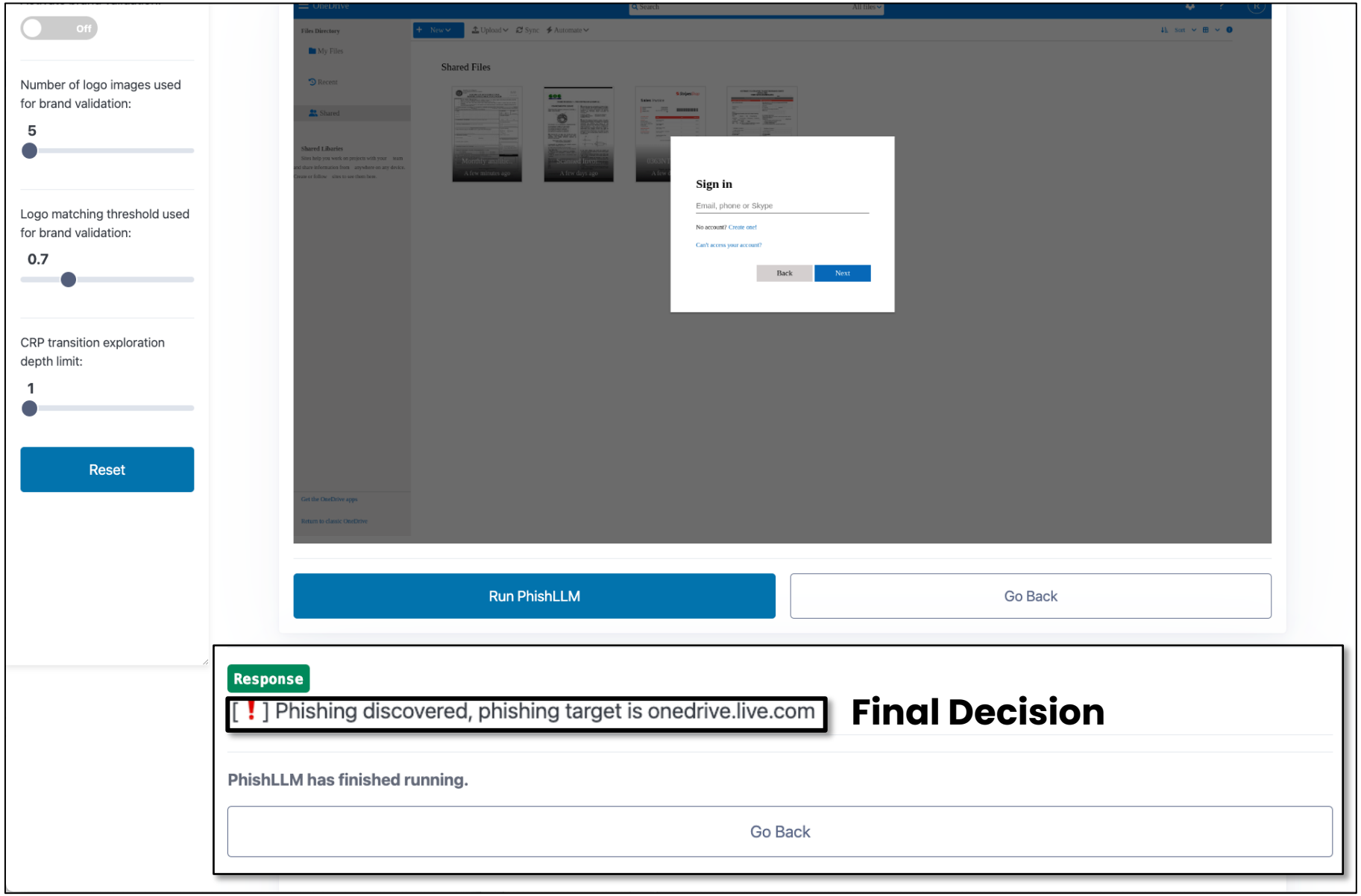


Brand Recognition

Demo Site: http://34.204.95.231:6789/

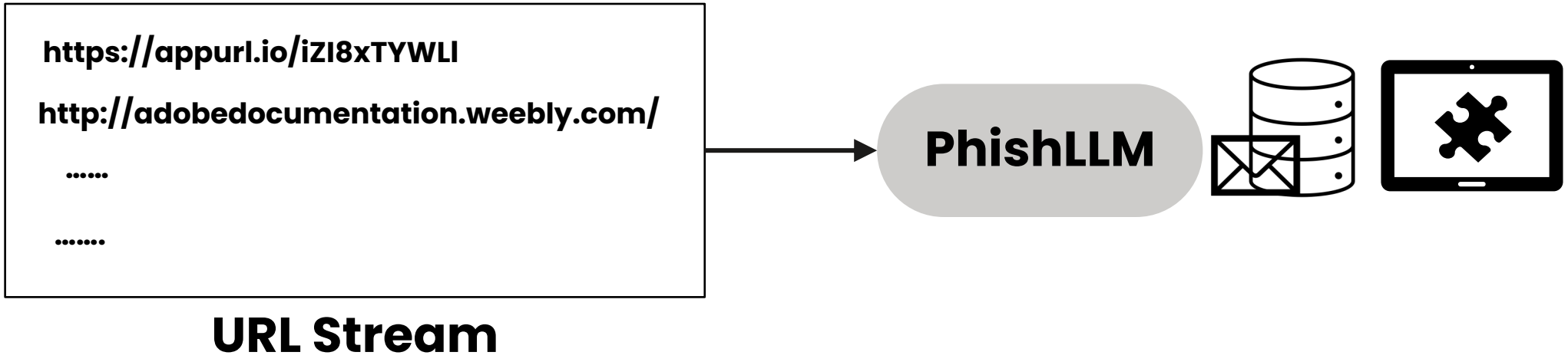


Demo Site: http://34.204.95.231:6789/



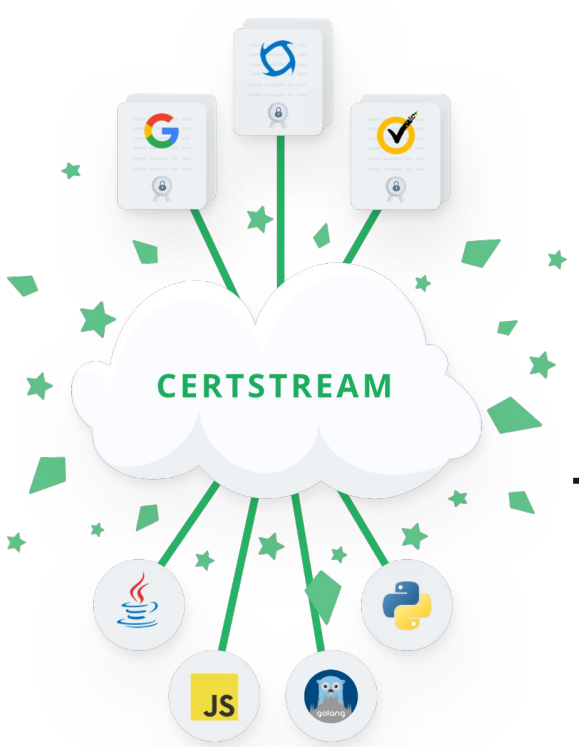
Deployment Scenarios

S1: URL consumption service



URL Stream

Deployment Scenarios



Emerging Websites Feed

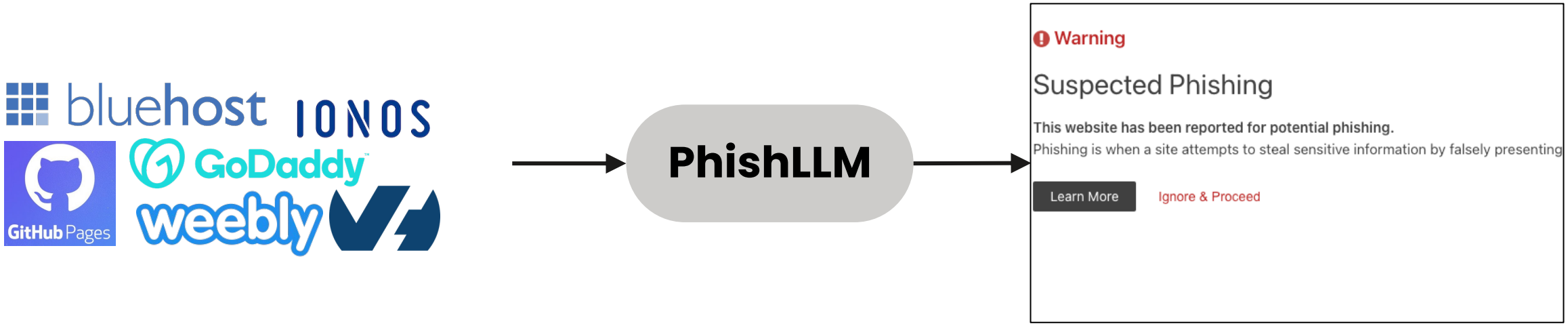
S2: Threat intelligence feed

PhishLLM

Zero-day Phishing Alerts

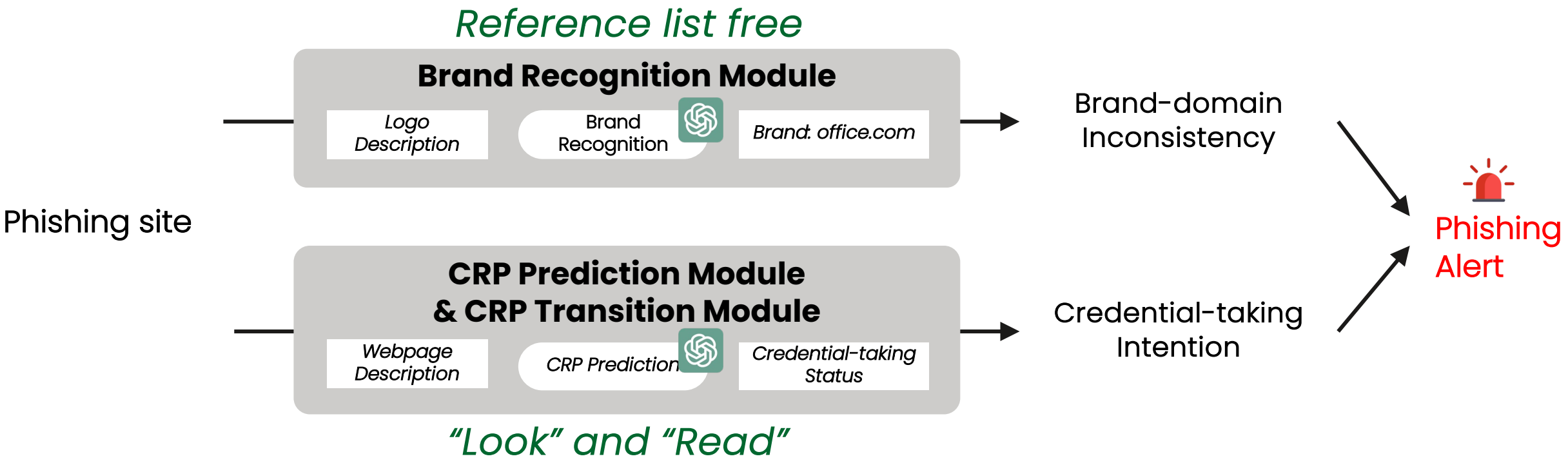
Deployment Scenarios

S3: Service for Hosting Providers



Web Hosting Providers

PhishLLM


Reference list free
Brand Recognition Module
Logo Description
Brand Recognition
Brand: office.com
Phishing site
CRP Prediction Module & CRP Transition Module
Webpage Description
CRP Prediction
Credential-taking Status
"Look" and "Read"
Brand-domain Inconsistency
Credential-taking Intention
Phishing Alert

Interested to Know More?

Code: https://github.com/code-philia/PhishLLM/

Website: https://sites.google.com/view/phishllm/home

Email: liu.ruofan16@u.nus.edu

National University of Singapore