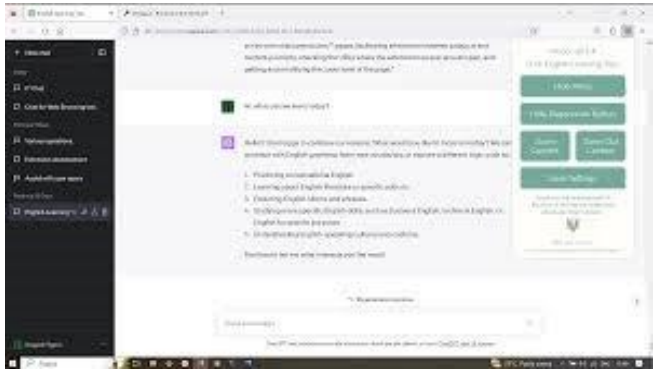
Detecting Vulnerabilities in PHP-Based Web Programs Using Graph Models

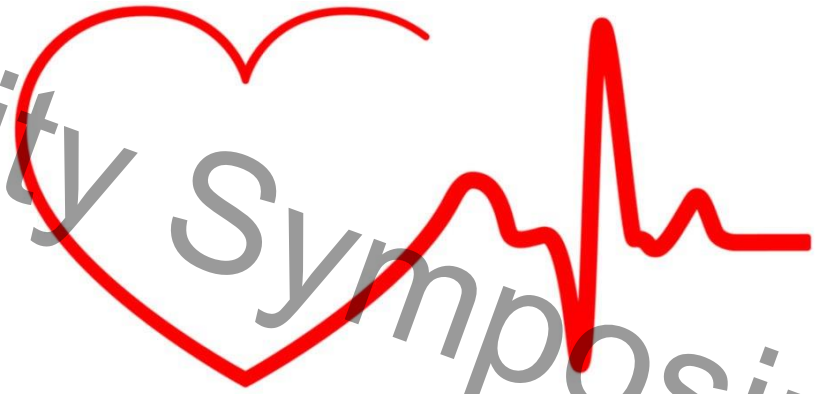
Junjie Zhang

Dept. of Computer Science and Engineering

Wright State University

Web Server – The Beating Heart of The Internet





PHP-Based Web Servers

Is PHP Dead? No! At Least Not According to PHP Usage Statistics

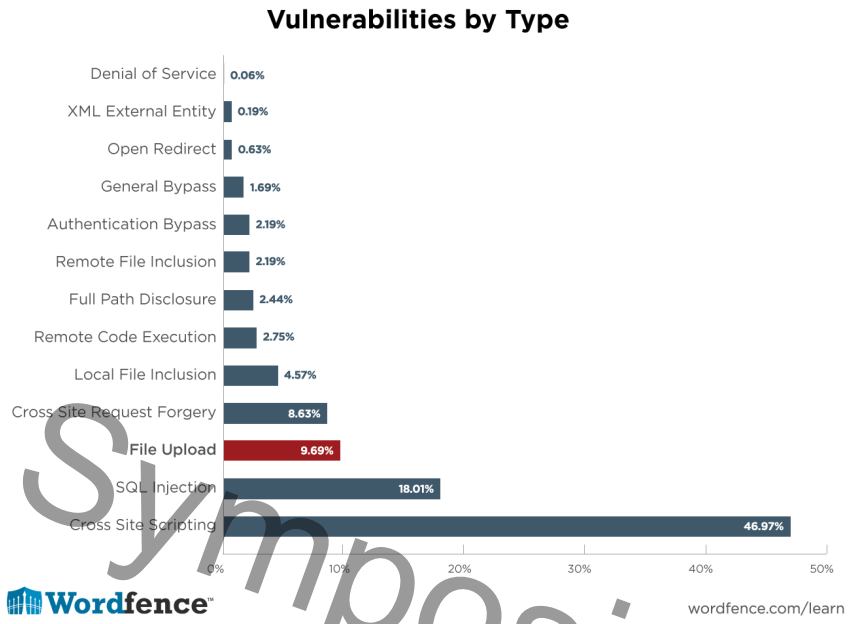
Updated on August 7, 2024 • Technology • Rating — 5 (9 votes)

The phrase "PHP is dead" has been floating around for a couple of years now, but judging by its usage numbers, PHP can't kick the bucket just yet! There are nearly **2 billion websites and 77.4% of them use PHP**, making it one of the most popular technologies out there.

Vulnerable Web Servers – Significant Threats

ID	Added	Title
9219	2019-02-14	WP Cost Estimation < 9.644 - Arbitrary File Upload and Delete
9191	2019-01-07	Audio Record 1.0 - Arbitrary File Upload
9190	2019-01-07	Baggage Freight Shipping Australia 0.1.0 - Unauthenticated Arbitrary Fil...
9136	2018-10-19	Tajer - Unauthenticated Arbitrary File Upload
9110	2018-08-09	Ultimate Member <= 2.0.21 - Unauthenticated Arbitrary File Upload
8977	2017-12-19	AccessPress Anonymous Post Pro < 3.2.0 - Unauthenticated Arbitrary File ...
8908	2017-09-25	WP Job Manager <= 1.26.1 - Unauthenticated Arbitrary File Upload
8865	2017-07-19	WooCommerce Catalog Enquiry - Arbitrary File Upload
8803	2017-05-02	flickr-picture-backup <= 0.7 - Unauthenticated File Upload
8774	2017-03-08	Wp2android 1.1.4 - Unauthenticated File Upload
8773	2017-03-08	Webapp builder 2.0 - Unauthenticated File Upload
8772	2017-03-08	WordPress Mobile app Builder 1.05 - Unauthenticated File Upload
8771	2017-03-08	mobile-friendly-app-builder-by-easytouch 3.0 - Unauthenticated File Upload
8743	2017-03-01	Mobile App Native <= 3.0 - Remote File Upload
8694	2016-12-11	Delete All Comments 2.0 - Unauthenticated Arbitrary File Upload
8642	2016-10-18	WP Marketplace - Arbitrary File Upload
8632	2016-09-27	Front end file upload and manager Plugin <= 3.9 - Arbitrary File Upload
8630	2016-09-27	WooCommerce Product Addons <= 1.1 - Arbitrary File Upload
8627	2016-09-26	W3 Total Cache <= 0.9.4.1 – Authenticated Arbitrary File Upload
8623	2016-09-21	N-Media Website Contact Form with File Upload - Arbitrary File Upload
8622	2016-09-20	Neosense Theme <= 1.7 - Unrestricted File Upload
8593	2016-08-12	Estatik 2.2.5 - Arbitrary File Upload
8592	2016-08-12	Adblock Blocker 0.0.1 - Arbitrary File Upload
8527	2016-06-23	WordPress File Upload <= 3.8.5 - Insufficient File Extension Blacklisting
8526	2016-06-23	Contus Video Comments - Unauthenticated Remote JPG File Upload
8515	2016-06-14	Remote Upload <= 1.2.1 - Unrestricted File Upload
8511	2016-06-07	Wordpress Levo-Slideshow - Arbitrary File Upload
8505	2016-06-03	WP Mobile Detector <= 3.5 - Arbitrary File Upload
8482	2016-05-03	Tevolution <= 2.2.7 - Unrestricted File Upload
8412	2016-03-11	Beauty & Clean Theme 1.0.8 - Arbitrary File Upload

← 1 2 3 4 5 6 7 8 9 →



Source: Wordfence

Vulnerability Detection

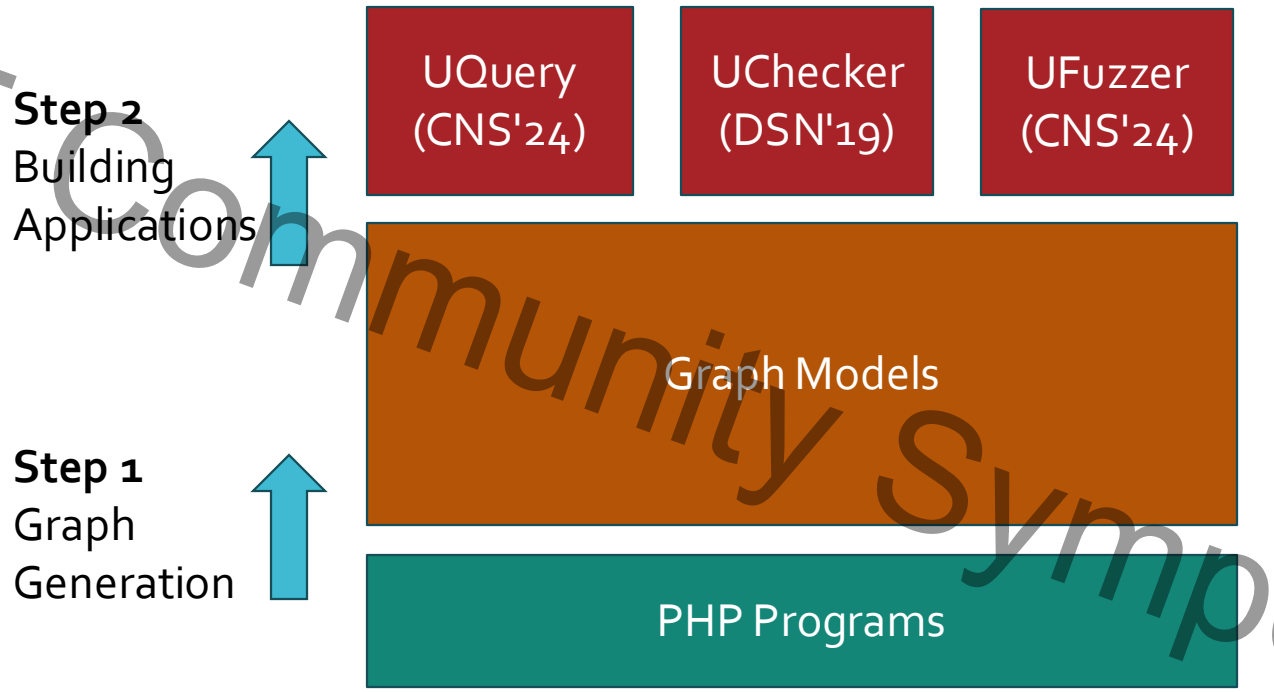
- Challenges
  - Complexity
  - Syntactical Variety
  - Emerging Vulnerabilities

The development and deployment of vulnerability detection solutions often fall behind the discovery of new vulnerabilities.

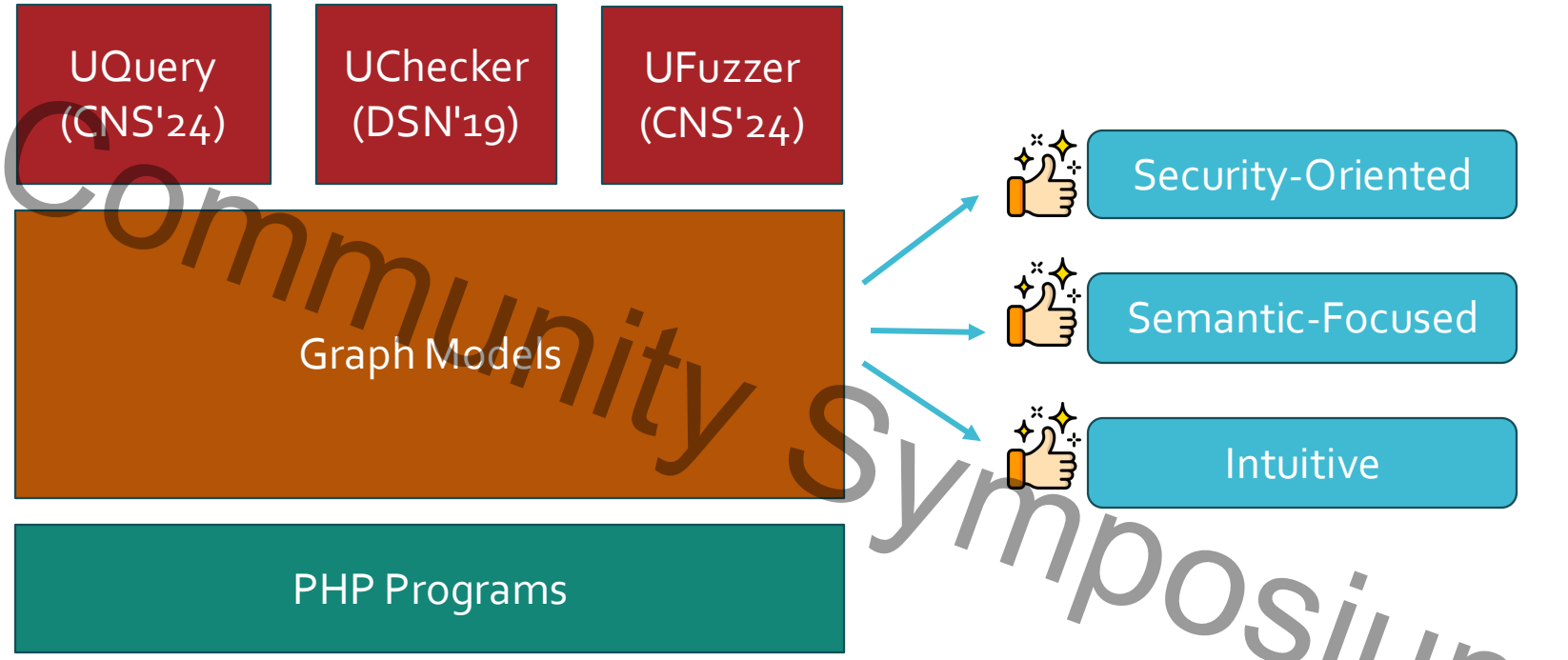
Goal

To design a framework for the agile development and deployment of server-side PHP web programs.

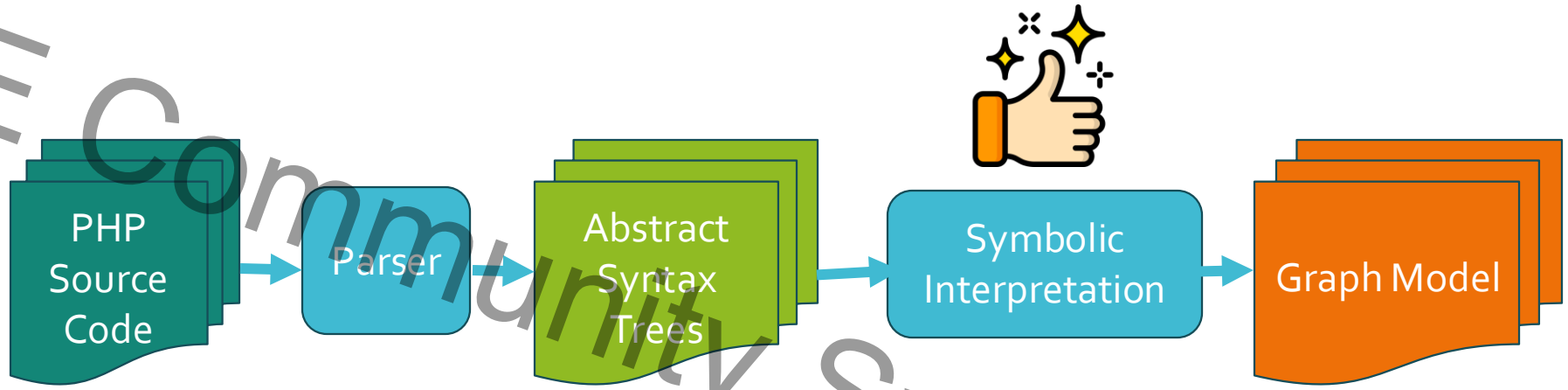
Framework



Framework

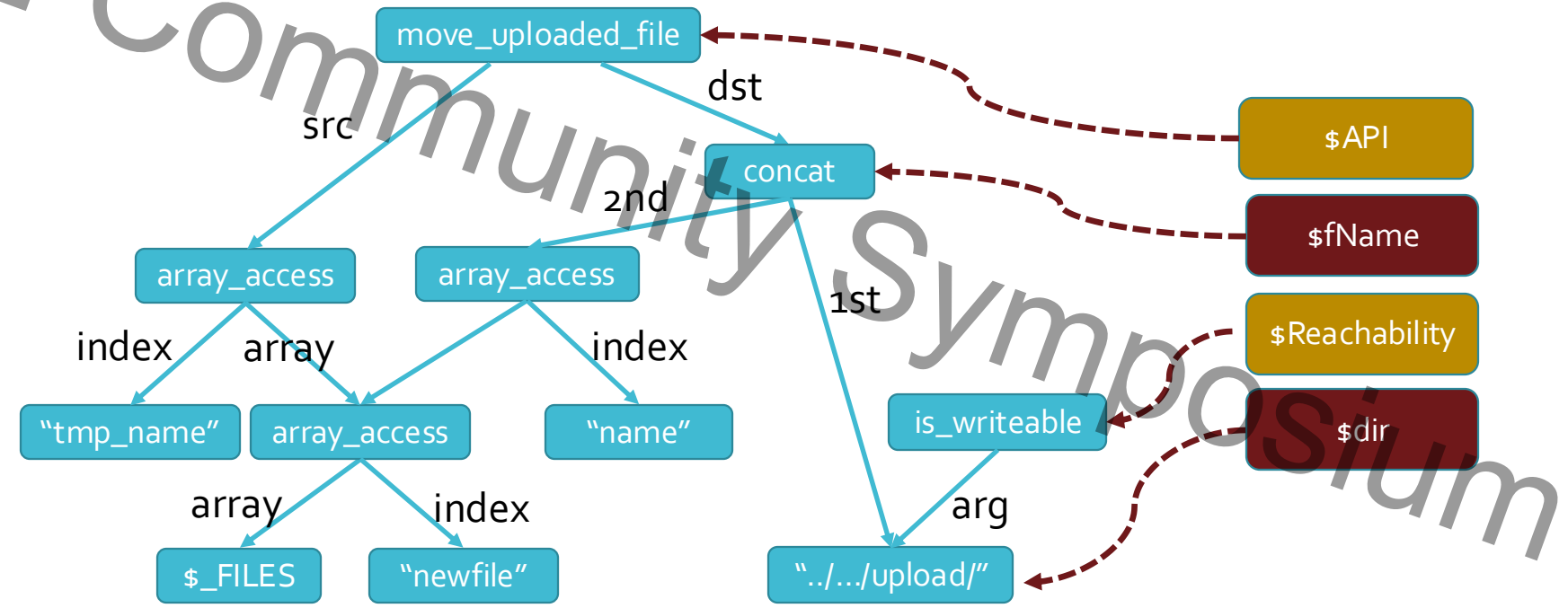


Generating The Graph Model

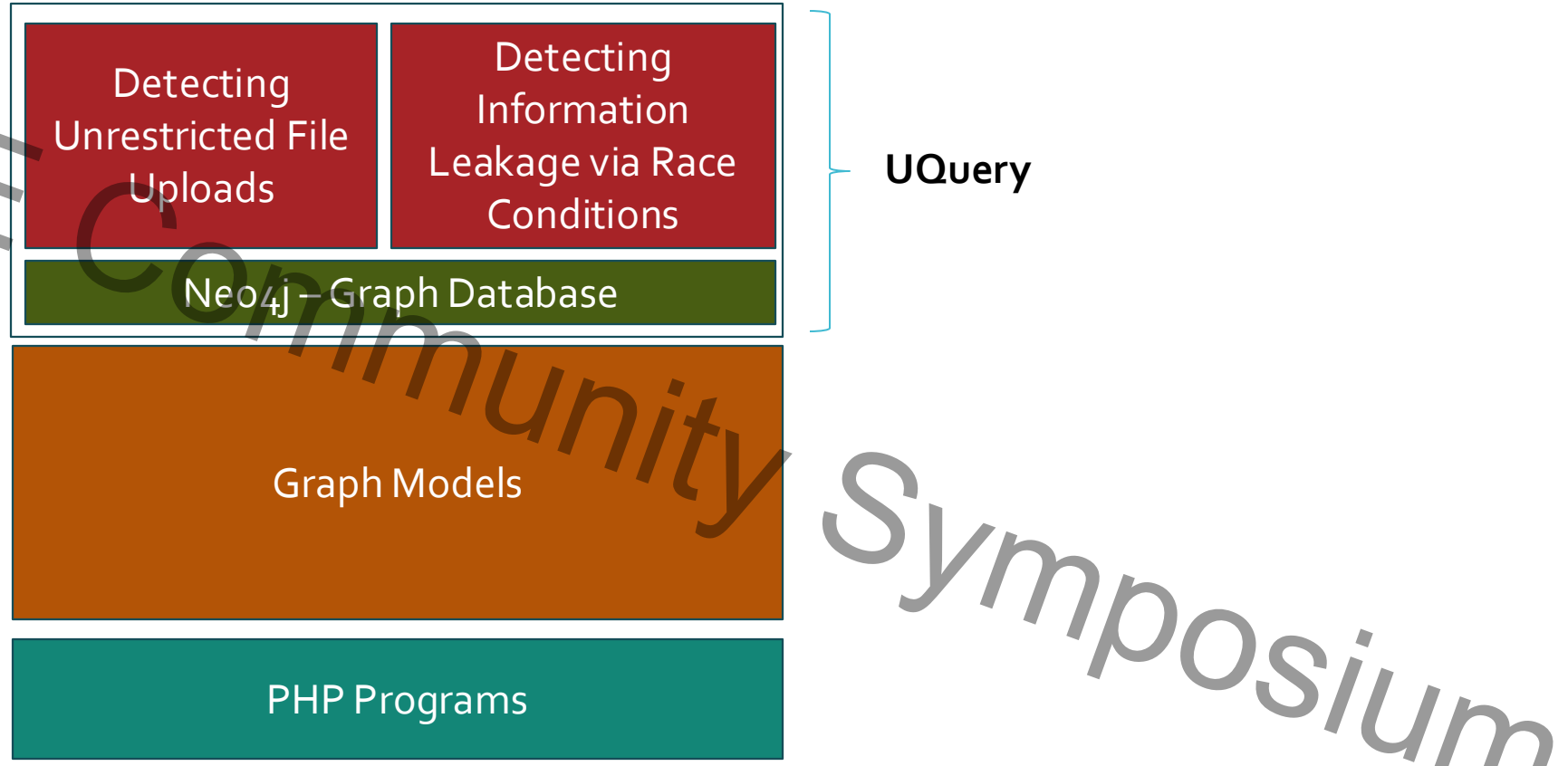


An Example

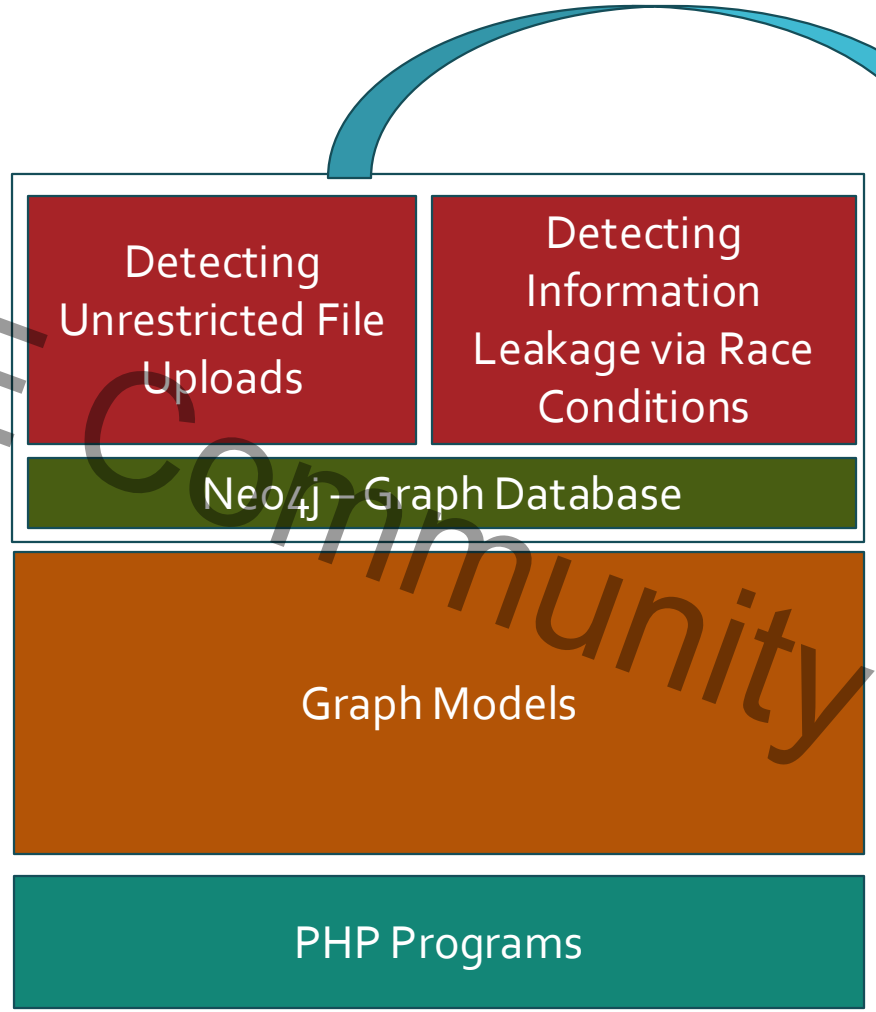
```php
<?php
$dir = "../wp-content/plugins/upload/";
if(is_writeable($dir)){
    $fName = $dir.$_FILES['newfile']['name'];
    move_uploaded_file($_FILES['newfile']['tmp_name'], $fName);
}
?>
```



UQuery (CNS'24)



UQuery (CNS'24)



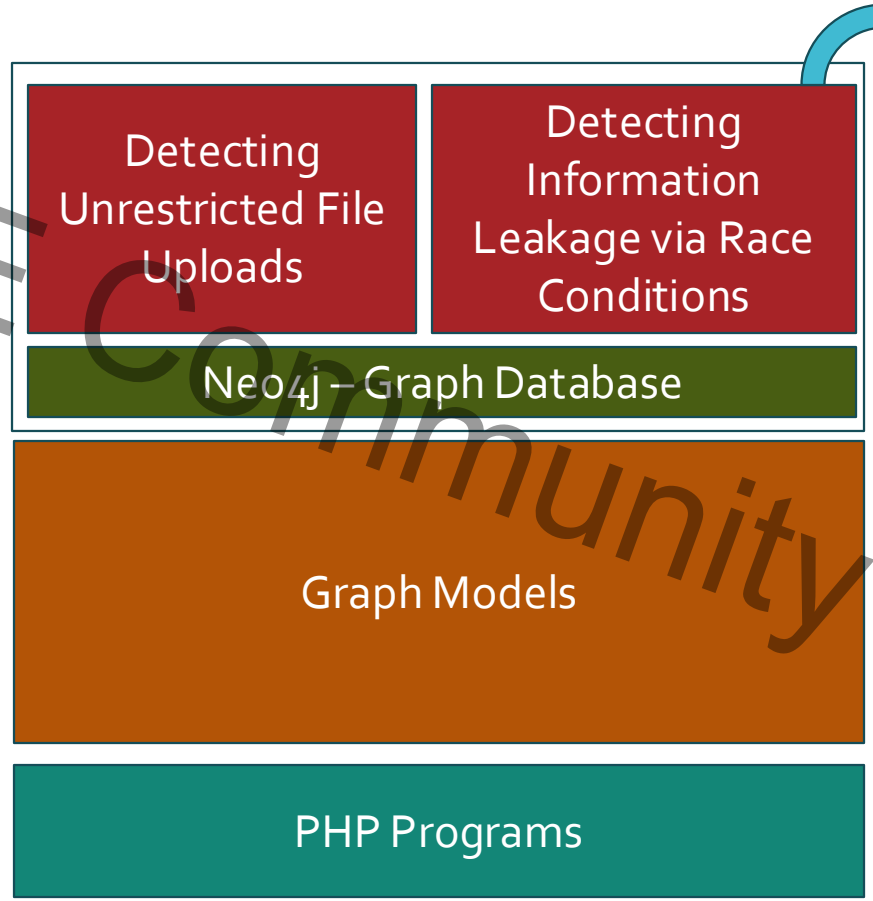

```
1 MATCH ({name:'move_uploaded_file'})-[{type:'ctrl'}]
2       ->(root)
3 MATCH ({name:'_FILES'})<--({name:'array'})<--
4       ({name:'array_access'})<--(t{name:'array_access'})
5       -->({name:'name'})
6 WITH id(root) AS start, [id(t)] AS ends, t AS target
7 CALL gds.alpha.dfs.stream('myGraph', {startNode:start,
8                           targetNodes:ends})
9 YIELD path
10 UNWIND [n IN nodes(path)
11       WHERE n.name IN ['pathinfo', 'explode', 'strripos'
              ,
12                       'preg_match']
13       AND (n)-[*]->(target) | n ] as sanitizationAPIs
14 RETURN sanitizationAPIs.id
```

Listing 4: The Rule to Identify The Control-Flow-Based UFU Vulnerability Prevention Methods

```
1 MATCH ({name:'move_uploaded_file'})-[{type:'arg2'}]->
2       ({name:'Concat'})-[{type:'right'}]->
3       (res{Data_type:'string'})
4 WHERE NOT res.name =~ '.*php|.*exe'
5 RETURN res.name
```

Listing 5: The Rule to Identify The Data-Flow-Based UFU Vulnerability Prevention Methods

UQuery (CNS'24)




```
1 MATCH (c1{name:'file_put_contents'})-[{type:'arg1'}]->
2       (file_name)<--(c2{name:'unlink'})
3 WHERE c1.line_num < c2.line_num AND
4       NOT (file_name)-[*]->({name:'random_bytes'}) AND
5       NOT (file_name)-[*]->({name:'random_int'}) AND
6       NOT (file_name)-[*]->
7           ({name:'openssl_random_pseudo_bytes'})
8 RETURN file_name.id
```

Listing 6: The Rule to Detect The Information Leakage through The Exploitable Race Condition

UQuery Detection Results

No.	PHP Application	*UQuery*	*UFuzzer*	*UChecker*	*WAP*	Comment	CVE
1	Ads EZ Lite 3.20	✔	✖	✖	✖	New	
2	classyfrieds 3.8	✔	✖	✖	✖	New	(CVE-2021-24252)
3	College Publisher Import 0.1	✔	✔	✖	✖	New	(CVE-2021-24253)
4	Email Artillery 4.1	✔	✖	✖	✖	New	(CVE-2021-24490)
5	Fileviewer 2.2	✔	✖	✖	✖	New	(CVE-2021-24491)
6	Formi Form Builder 1.0	✔	✔	✔	✔	New	
7	Google Analytics Client 1.0.2	✔	✔	✖	✔	New	
8	Image Twinning 1.0.0	✔	✔	✖	✖	New	
9	Advert Manager 1.0	✔	✔	✔	✔	New	
10	RAD Dropbox Uploader 1.1.3	✔	✔	✖	✖	New	
11	RAD Text Highlighter 1.0.0	✔	✔	✖	✖	New	
12	Scroll Baner 1.0	✔	✖	✖	✖	New	(CVE-2021-24642)
13	Simple Schools Staff Directory 1.1	✔	✔	✖	✖	New	(CVE-2021-24663)
14	Daily Different Corner Band 1.0	✔	✔	✖	✖	New	
15	Testimonials King Light 0.1	✔	✔	✖	✖	Known	
16	WP-Curriculo Vitae Free 6.1	✔	✔	✖	✖	Known	(CVE-2021-24222)
17	Easy Form Builder 1.0	✔	✔	✔	✖	Known	(CVE-2021-24224)
18	imagements 1.2.5	✔	✔	✔	✖	Known	(CVE-2021-24236)
19	Event Banner 1.3	✔	✔	✖	✖	Known	(CVE-2021-24251)
20	Quick Image Transform 1.0.1	✔	✔	✖	✖	Known	
21	BSK Files Manager 1.0.0	✔	✔	✖	✖	Known	
22	Gallerio 1.0.1	✔	✖	✔	✖	Known	
23	Banner Cycler 1.4	✔	✔	✖	✖	Known	
24	N5 Upload Form 1.0	✖	✔	✖	✖	Known	(CVS-2021-24223)
25	Adicon Server	✖	✖	✖	✔	FP	
26	Alchemyst Forms 1.1.8	✖	✖	✖	✔	FP	

TABLE II: Detecting PHP Applications with UFU Vulnerabilities. *UQuery* detected 14 new vulnerable applications, contributing 6 CVEs and introducing 0 false positive.

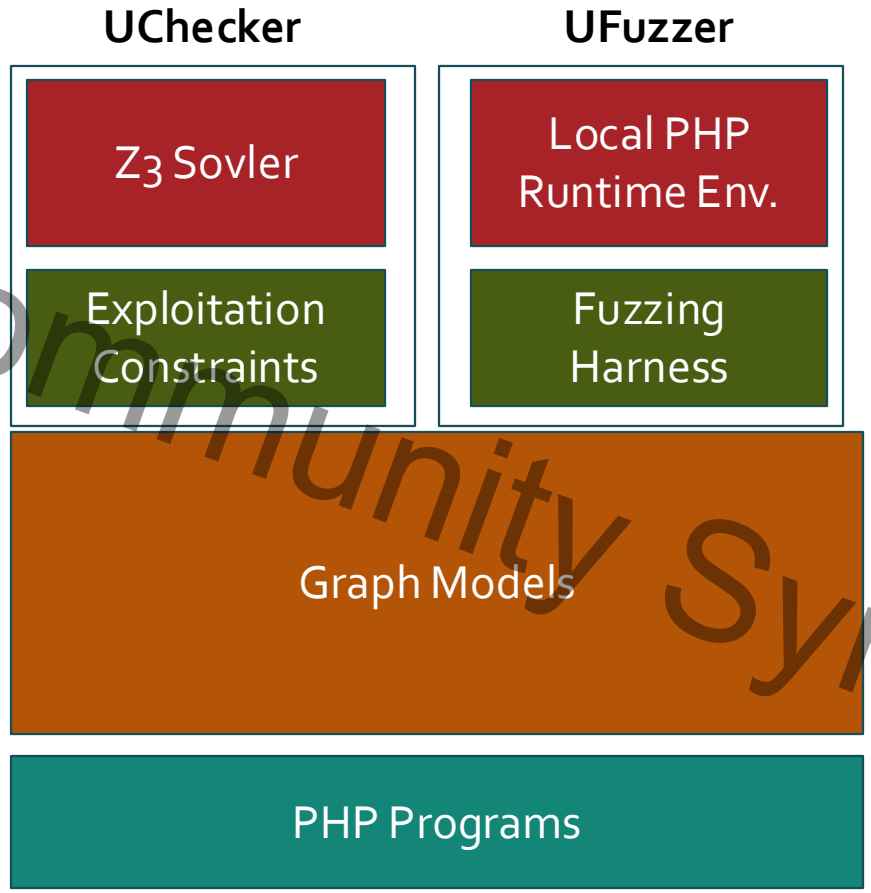
UQuery Detection Results

WP Demo Buddy

Uvdesk

Two Vulnerable PHP Applications With Potential Information Leakage via Race Conditions

UChecker (DSN'19) & UFuzzer (RAID'21)



UChecker (DSN'19) & UFuzzer (RAID'21)

No.	Application	UFuzzer	Vuln Source File : Line No.	UChecker	Verification Method	Root Cause	Admin Required?	CVE
1	Basic-Laravel-CMS - PHP Framework For Web Artisans	✔	uploader.php:31	✔	Code Review	LS	No	
2	BloggerCMS - Easiest Static Blog Generator	✔	Image.php:77	✖	Code Review	SInS	No	
3	Lapin_CMS - Slim 3 RAD Skeleton	✔	upload.php:36	✖	Code Review	SInS	No	
4	Learningphp-CMS	✔	upload.php:41	✔	Code Review	LS	No	
5	Mini_CMS - PHP Based Mini Blog	✔	zamiesc-post.php:40	✔	Exploiting	SInS	No	
6	laravelCMS - PHP Framework For Web Artisans	✔	ProfileController.php:29	✔	Code Review	SInS	No	
7	WikiDocs - Databaseless Markdown Wiki Engine	✔	submit.php:264	✖	Code Review	SInS	No	
8	Buffalo-Webpage-CMS	✔	actionProductoCtrl.php:81	✖	Code Review	SInS	No	
9	LCMS - College Website with CMS	✔	student_avatar.php:13	✔	Code Review	LS	No	
10	Palette - PHP Based Site Builder	✔	upload.php:27	✖	Code Review	LS	No	
11	Progress_Business - CMS for Company Profile Web	✔	adding_news.php:12	✔	Exploiting	LS	No	
12	publisher.mod - FlatCore CMS Module	✔	upload.php:29	✖	Code Review	SInS	No	
13	User-Management-PHP-MYSQL	✔	edit-user.php:32	✔	Exploiting	SC	No	
14	MicroCMS1 - CMS Based On Model-View-Controller	✔	uploads.php:31	✖	Code Review	LS	No	
15	BlogStop - Simple Content Management System	✔	admin_edit_post.php:22	✖	Exploiting	LS	Yes	
16	CMS-Blogging-System - Blog Made with PHP and MySQL	✔	add_post.php:15	✔	Code Review	LS	Yes	
17	Cmsphp - Simple PHP based CMS System	✔	add_post.php:21	✔	Code Review	LS	Yes	
18	CMSPortfolio - PHP based Portfolio Template	✔	func.php:464	✖	Code Review	SInS	Yes	
19	CMSProjectPHP	✔	add_post.php:16	✔	Code Review	LS	Yes	
20	CMSsite - Simple CMS Site	✔	profile.php:27	✖	Exploiting	LS	Yes	
21	CmsV1 - CMS Based on PHP	✔	add_user.php:21	✔	Code Review	LS	Yes	
22	N5 Upload Form 1.0	✔	n5uploadform.php:156	✖	Exploiting	LS	No	CVE-2021-24223
23	Testimonials King Light 0.1	✔	testimonial-king-form.php:38	✖	Code Review	MisAPI	No	
24	WP-Curriculo Vitae Free 6.1	✔	enviarCadastro.php:86	✖	Exploiting	LS	No	CVE-2021-24222
25	Easy Form Builder 1.0	✔	newForm.php:49	✔	Exploiting	LS	No	CVE-2021-24224
26	imagements 1.2.5	✔	imagements.php:127	✔	Exploiting	SInS	No	CVE-2021-24236
27	Event Banner 1.3	✔	admin_events.php:29	✖	Exploiting	LS	Yes	CVE-2021-24251
28	Quick Image Transform 1.0.1	✔	file-upload.php:79	✖	Exploiting	SC	Yes	
29	College Publisher Import 0.1	✔	college-publisher-import.php:144	✖	Exploiting	LS	Yes	
30	BSK Files Manager 1.0.0	✔	bsk-files-manager.php:269	✖	Exploiting	MisAPI	Yes	
31	Banner Cycler 1.4	✔	admin.php:167	✖	Exploiting	LS	Yes	
32	Gallerio 1.0.1	✖	gallerio.php:610	✔	Exploiting	LS	Yes	

Potential Impacts on Cybersecurity Education

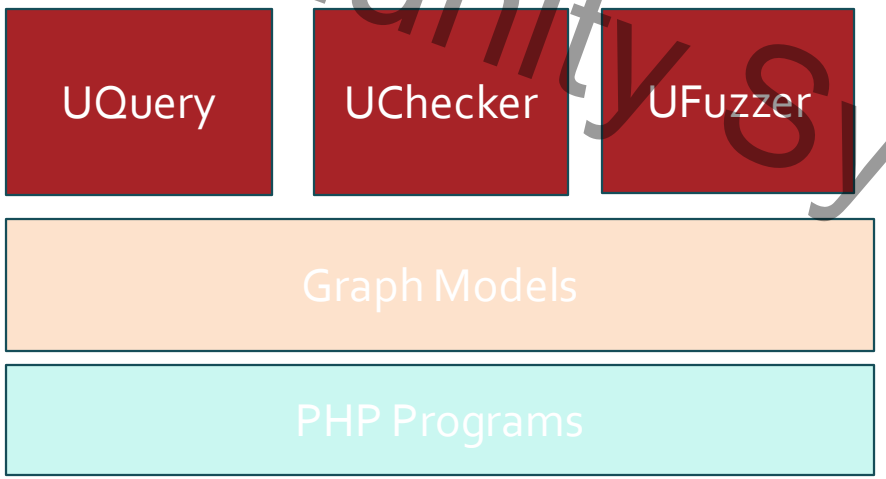
- Education Modules - Foundation Level
  - AST-Based Program Interpretation
  - AST-Based Symbolic Program Interpretation

Potential Impacts on Cybersecurity Education

- Education Modules – Program Modeling
  - Graph-Based Program Modeling
    - Abstracting away syntactical variances
    - Model control and data flows

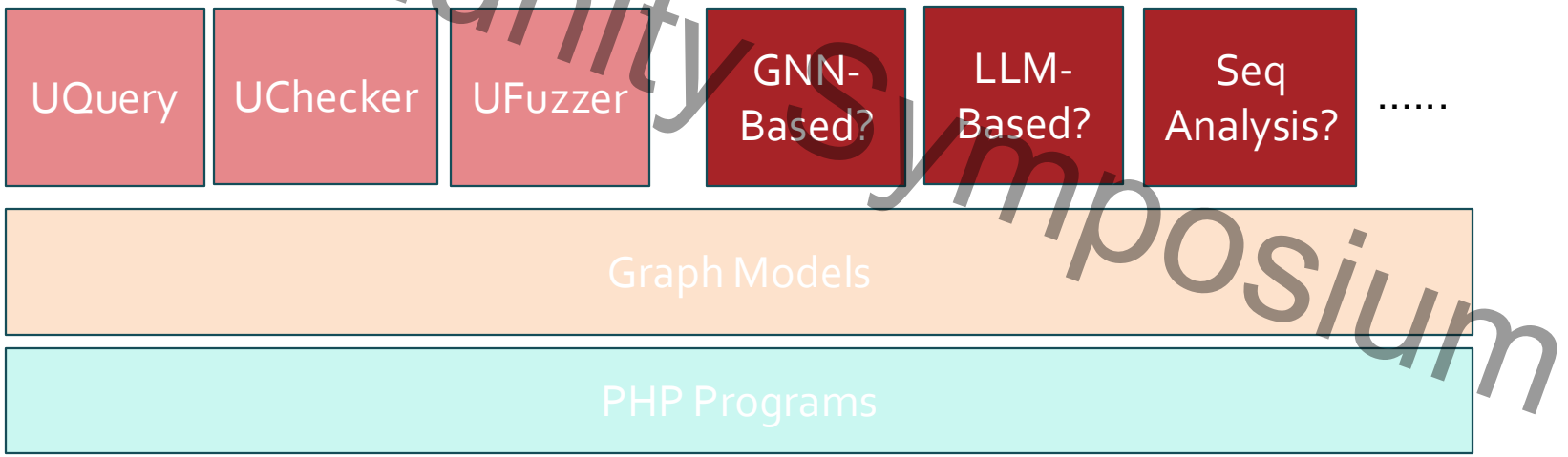
Potential Impacts on Cybersecurity Education

- Education Modules – Security Applications
  - Taint Analysis Using Graph Queries
  - Generating Exploitation Constraints
  - Regenerate PHP Code from Graph Models for Light-weight Fuzzing



Potential Impacts on Cybersecurity Education

- Education Modules – New Applications
  - AI-Enabled, Security-Oriented Graph Analysis



END

2025 CAE Community Symposium

Thank you!

Junjie Zhang
PoC, CAE-CD, Wright State University
junjie.zhang@wright.edu