



Securing the Modern Web

Andrei Sabelfeld

X@asabelfeld



CHALMERS



Web security today –
it's rough out there



Coop ransomware attacks July 2021 and Dec 2023



Swedish universities were dropped again because of their burning of the Quran

- <https://www.gu.se/>
<https://check-host.net/check-report/ea83dffk80f>
- <https://www.kth.se/>
<https://check-host.net/check-report/ea83df6kf01>
- <https://www.chalmers.se/>
<https://check-host.net/check-report/ea83de4k4b>
- <https://www.su.se/>
<https://check-host.net/check-report/ea83de0kfb6>
- <https://www.lunduniversity.lu.se/>
<https://check-host.net/check-report/ea83e64k1>

Anonymous Sudan attacks in Feb 2023

**Tillfälligt
stängt!**

**Vi har råkat ut för
en stor IT-störning
och våra system
fungerar inte.**

Problemet drabbar tyvärr även andra
tjänster i butiken, eftersom vi måste
hålla helt stängd.

**Vi beklagar att du som
kund drabbas.**

NEWS

Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Entertainment & Arts

Tech

Fitness app Strava lights up staff at military bases

© 29 January 2018



STRAVA

The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan

Security concerns have been raised after a fitness tracking firm showed the exercise routes of military personnel in bases around the world.

Misconfigured Amazon S3 Buckets Exposed US Military's Social Media Spying Campaign

BY WAQAS · NOVEMBER 18, 2017 · 3 MINUTE READ





Web security: Demo time!

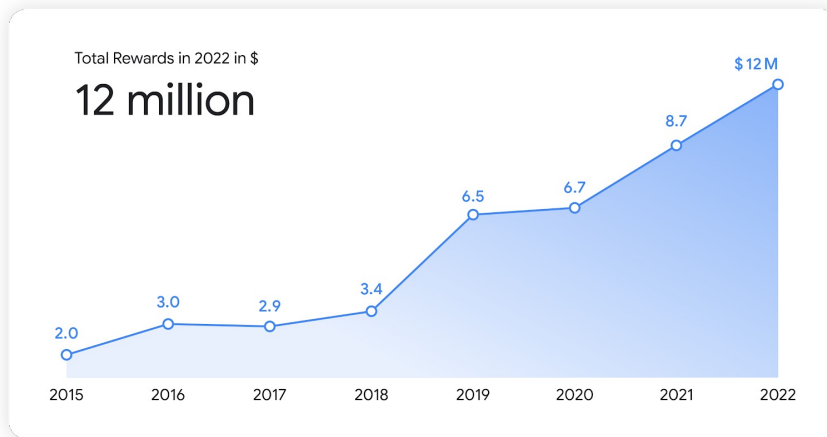
- Have I been pwned?
 - <https://haveibeenpwned.com/>
- Tracking everywhere
 - Your favorite news or commercial web site
- Am I unique?
 - <https://amiunique.org/>
- Leaky cloud database
 - <https://s3.amazonaws.com>
- Google dorking

Attackers

- No longer “hobby hackers”
- Cybercriminals
 - Ransomware: from individuals to industries
 - Aided by cryptocurrencies
- Governments
 - Stuxnet (2010, check out “Zero Days”)
 - Election meddling (DNC attack 2016)
 - Critical infrastructures (Colonial Pipeline 2021)
- Hacktivists
- All weaponized by tools, rootkits, exposed credentials, Darknet,... and AI!



Securing web applications is hard & costly



 Meta \$2 million in bounty awards in 2022



Cross-site scripting (XSS) prevailing web insecurity (20 years on OWASP Top 10)!



[Home](#) » [Enforcement](#) » [Cases and Proceedings](#) » [Refunds](#) » [Equifax Data Breach Settlement](#)

Equifax Data Breach Settlement

SHARE THIS PAGE   

January 2020

In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to \$425 million to help people affected by the data breach.

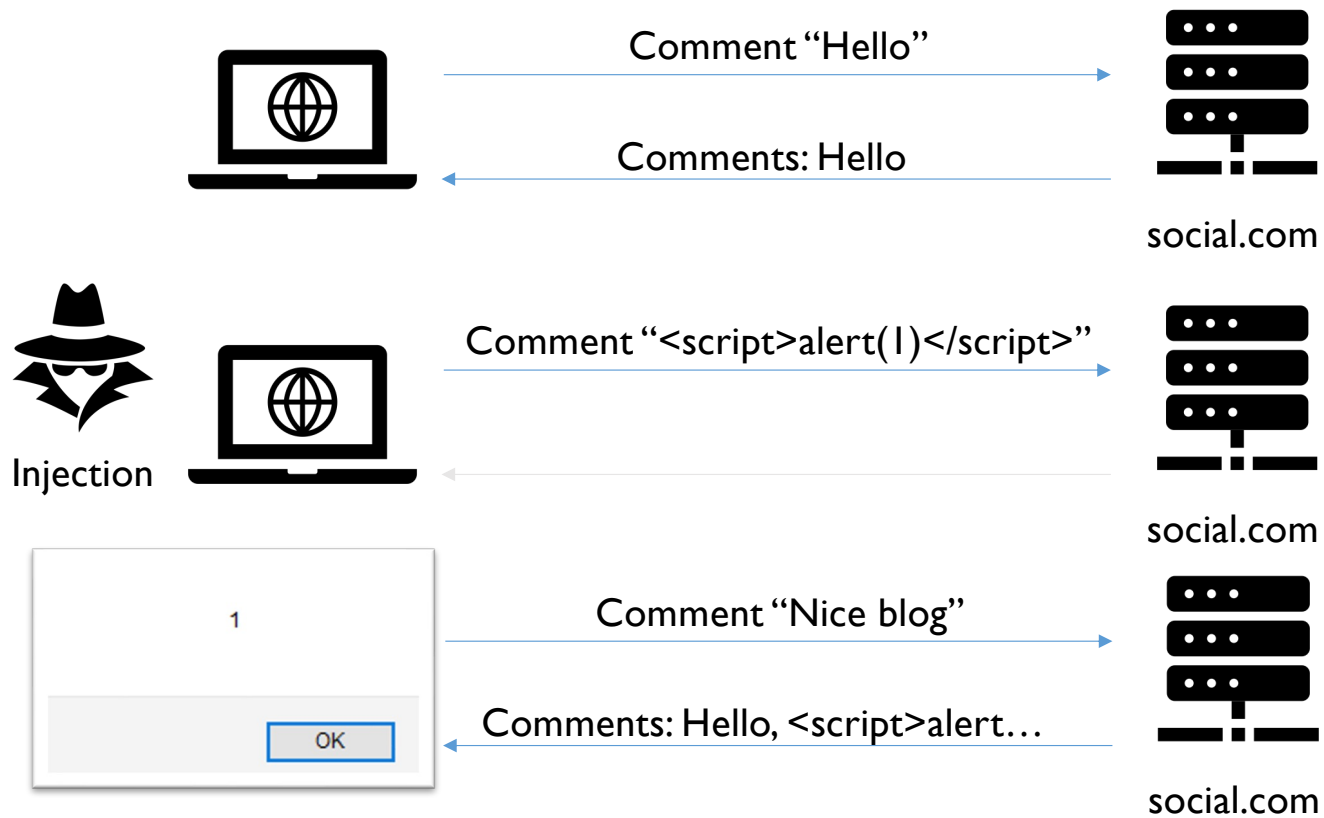
People whose Facebook data was improperly shared by Cambridge Analytica

United States	70,632,350 (81.6%)
Philippines	1,175,870 (1.4%)
Indonesia	1,096,666 (1.3%)
United Kingdom	1,079,031 (1.2%)
Mexico	789,880 (0.9%)
Canada	622,161 (0.7%)
India	562,455 (0.6%)
Brazil	443,117 (0.5%)
Vietnam	427,446 (0.5%)
Australia	311,127 (0.4%)

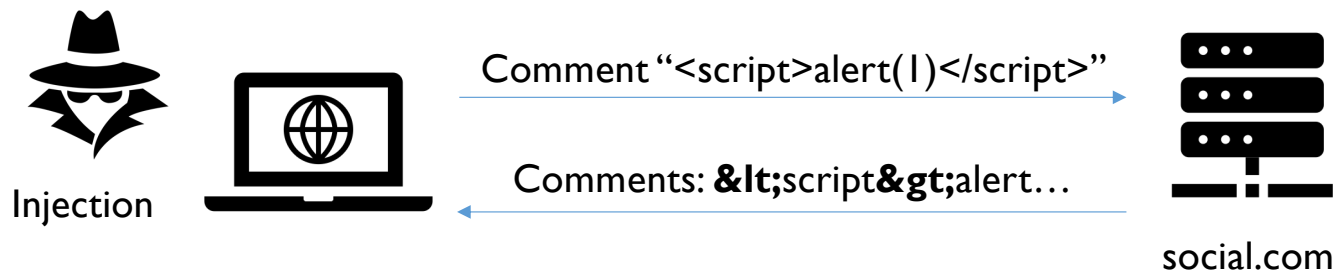
Source: Facebook

© DW

XSS attacks by code injection



Fix: input validation and output sanitization/encoding



Hard to find!

- Comment section
- Admin panel
- Newsletter email
- Feedback forms
- Product reviews
- ...

Security Researcher Earns \$10,000 After Finding Critical Google Maps Bug

[Home](#) > [News](#) > [Technology](#)

9 Sep 2020, 6:04 UTC · by [Bogdan Popa](#) 



Black Widow



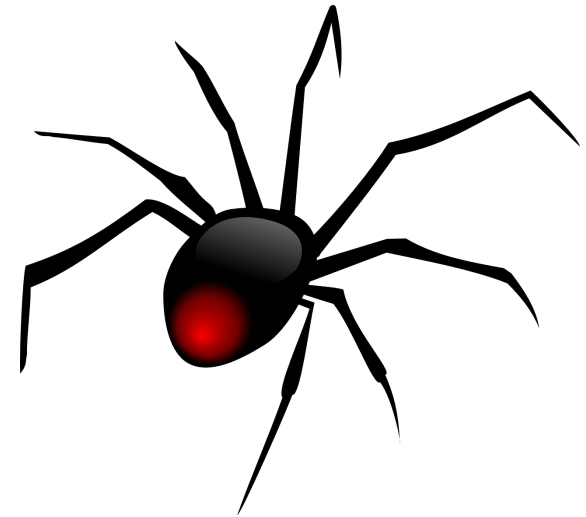
Black Ostrich



Spider-Scents

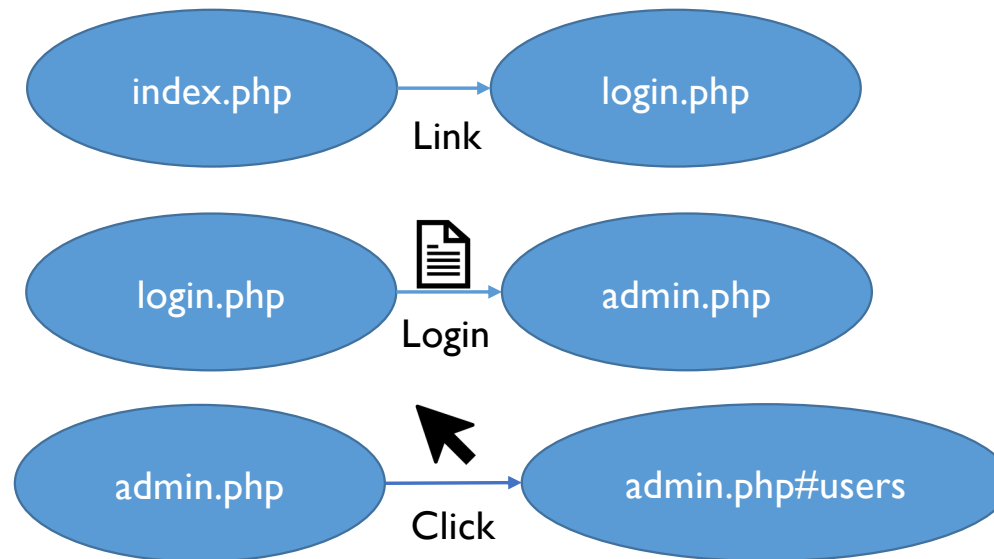
Black Widow

- Securing web applications is hard
- Blackbox web security scanners play an important role
- Practitioner scanners: Arachni, ZAP,...
- Research scanners: jÄk, CrawlJAX, LigRE, KameleonFuzz, Enemy of the State
- Black Widow combines the advantages
 - Traverse by clicking links and and submit forms
 - Model the navigation graph
 - Track injection tokens throughout web app



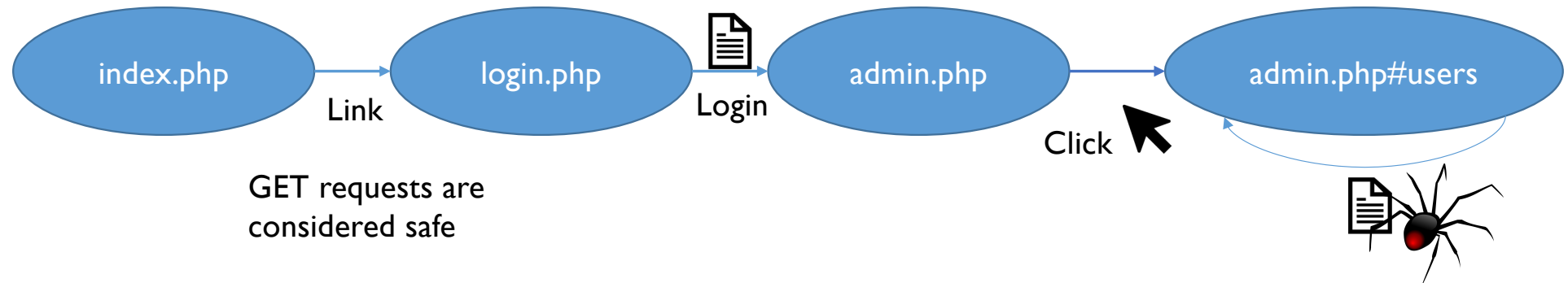
Navigation

- Nodes as client-side states
- Edges as actions moving between these states



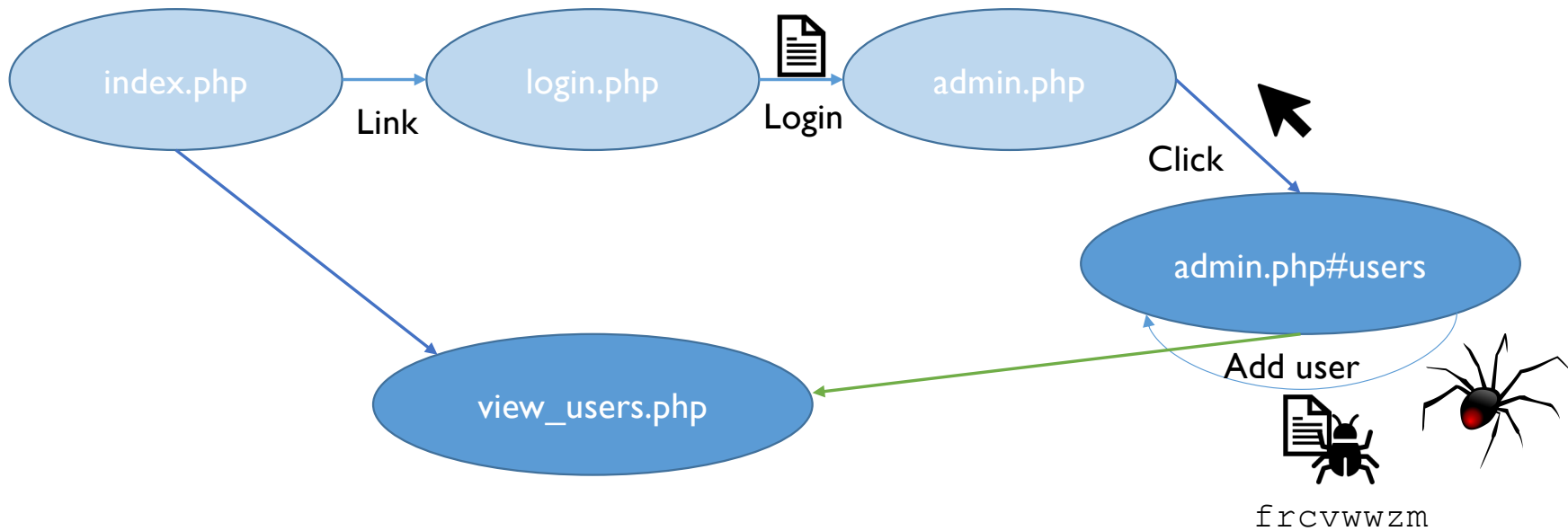
Traversing

- Pick unvisited edges from the navigation graph
- Re-execute workflows if needed



Inter-state dependencies

- Where the data is inserted can differ from where it is reflected
- We insert random tokens to infer sources and sinks

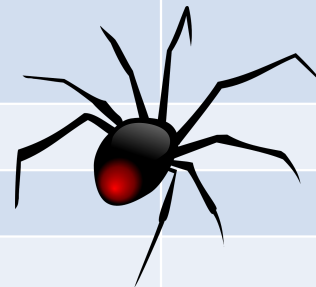


Evaluation

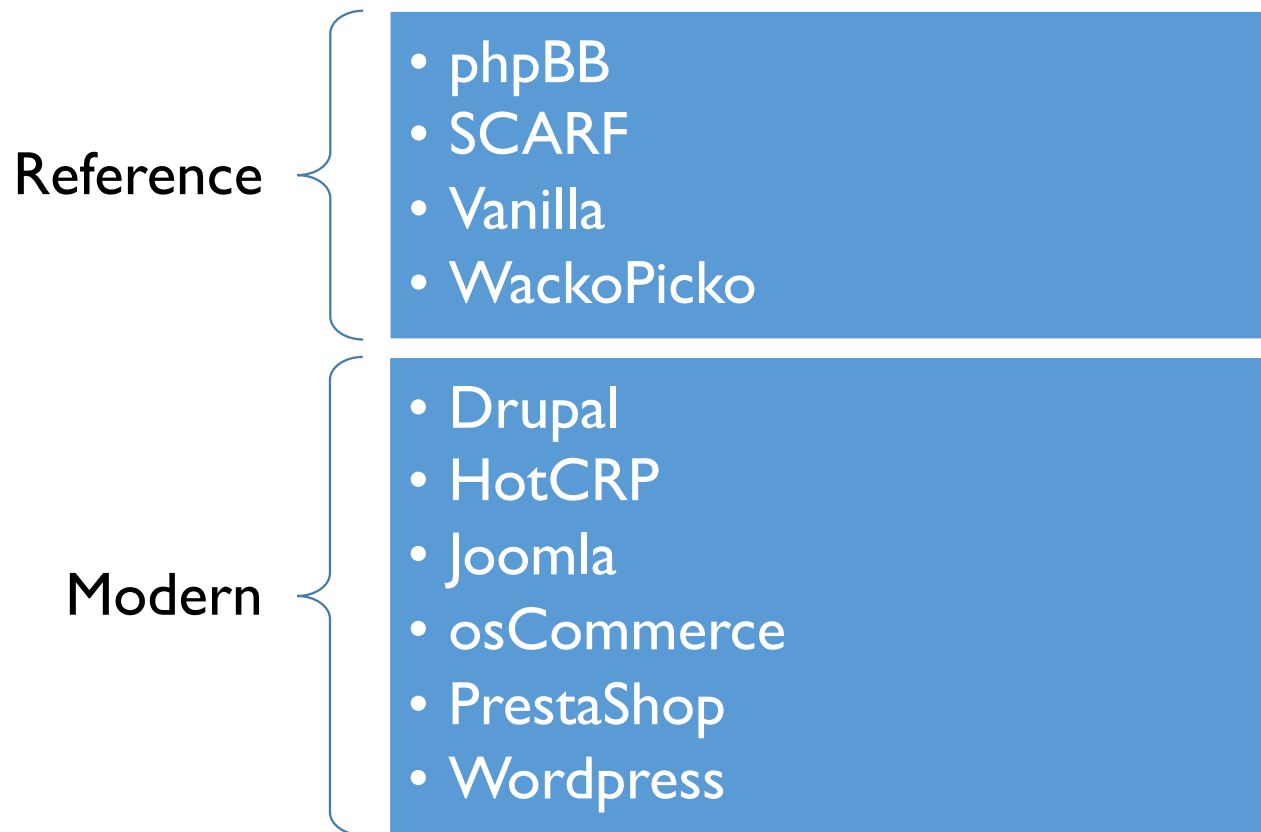
- Server-side code coverage
- Number of found vulnerabilities

Evaluation

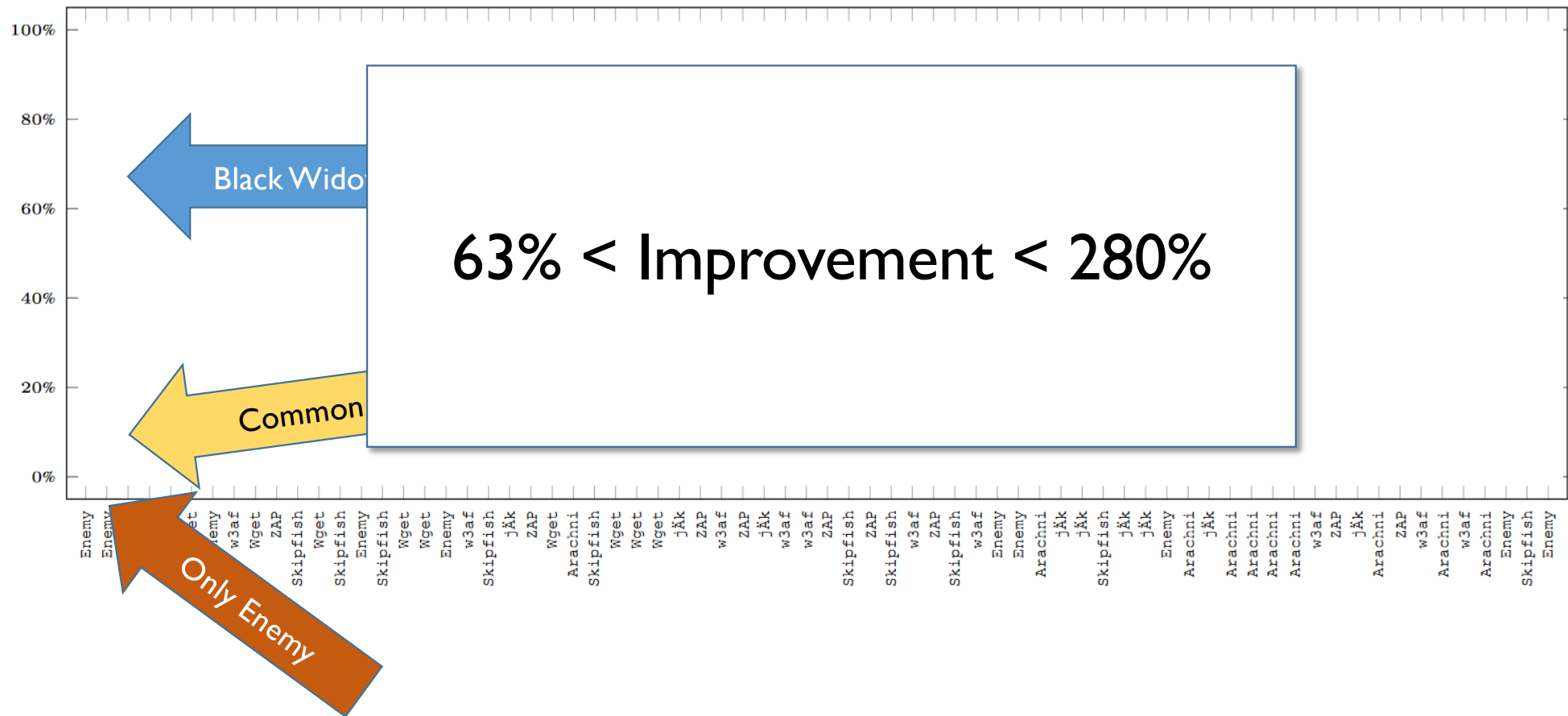
	Arachni	Enemy	jÄk	Skipfish	W3af	Wget	ZAP
Drupal							
HotCRP							
Joomla							
osCommerce							
phpBB							
PrestaShop							
SCARF							
Vanilla							
WackoPicko							
Wordpress							



Evaluation - Applications



Results – Coverage (Lines of Code)



Results – Vulnerabilities

Crawler	Reference (Reflected XSS)	Reference (Stored XSS)	Modern (Reflected XSS)	Modern (Stored XSS)	Total
Black Widow	8	13	3	1	25
Arachni	6	1			7
Enemy	2	1			3
jÄk	1				1
Skipfish	1				1
W3af	2				2
ZAP					0

Results – Vulnerabilities

Crawler	Reference (Reflected XSS)	Reference (Stored XSS)	Modern (Reflected XSS)	Modern (Stored XSS)	Total
Black Widow	8	13	3	1	25
Arachni	6	1			7
Enemy	2	1			3
jÄk	1				1
Skipfish	1				1
W3af	2				2
ZAP					0

Results – Vulnerabilities

Crawler	Reference (Reflected XSS)	Reference (Stored XSS)	Modern (Reflected XSS)	Modern (Stored XSS)	Total
Black Widow	8	13	3	1	25
Arachni	6	1			7
Enemy	2	1			3
					1

✓ **Corrected** master kohle

Reflected XSS with dashboard calendar

PierreRambaud published GHSA-m2x6-c2c6-pjrx on Apr 20

Severity	Affected versions	Patched versions	CVE identifier
moderate	> 1.6.0.0	1.7.6.5	CVE-2020-5271

Conclusion

- Securing web applications is hard
- Blackbox web security scanners play an important role
- Practitioner scanners: Arachni, ZAP,...
- Research scanners: jÄk, CrawlJAX, LigRE, KameleonFuzz, Enemy of the State
- Black Widow combines the advantages
 - Traverse by clicking links and and submit forms
 - Model the navigation graph
 - Track injection tokens throughout web app

