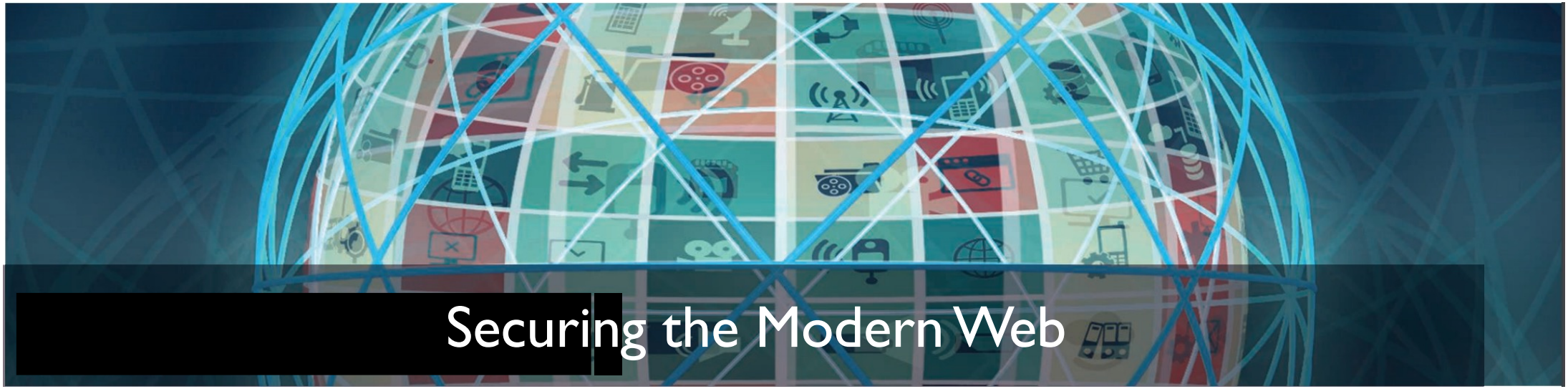


Securing the Modern Web

Andrei Sabelfeld
𝕏@asabelfeld

CHALMERS

KTH VETENSKAP OCH KONST

Web security today –
it's rough out there

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/

Anonymous Sudan attacks in Feb 2023

Coop ransomware attacks July 2021 and Dec 2023

Fitness app Strava lights up staff at military bases

29 January 2018

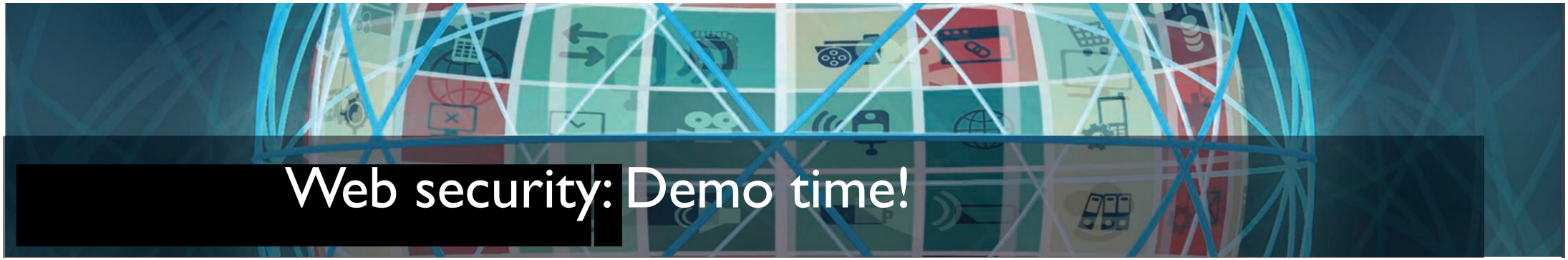
The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan

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

LEAKS SECURITY

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

Google

Meta $2 million in bounty awards in 2022

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

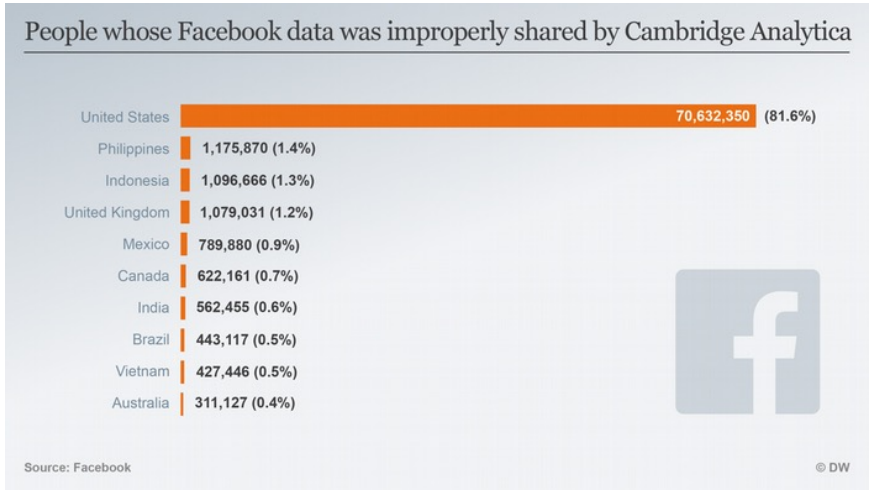
Home » Enforcement » Cases and Proceedings » Refunds » Equifax Data Breach Settlement

Equifax Data Breach Settlement

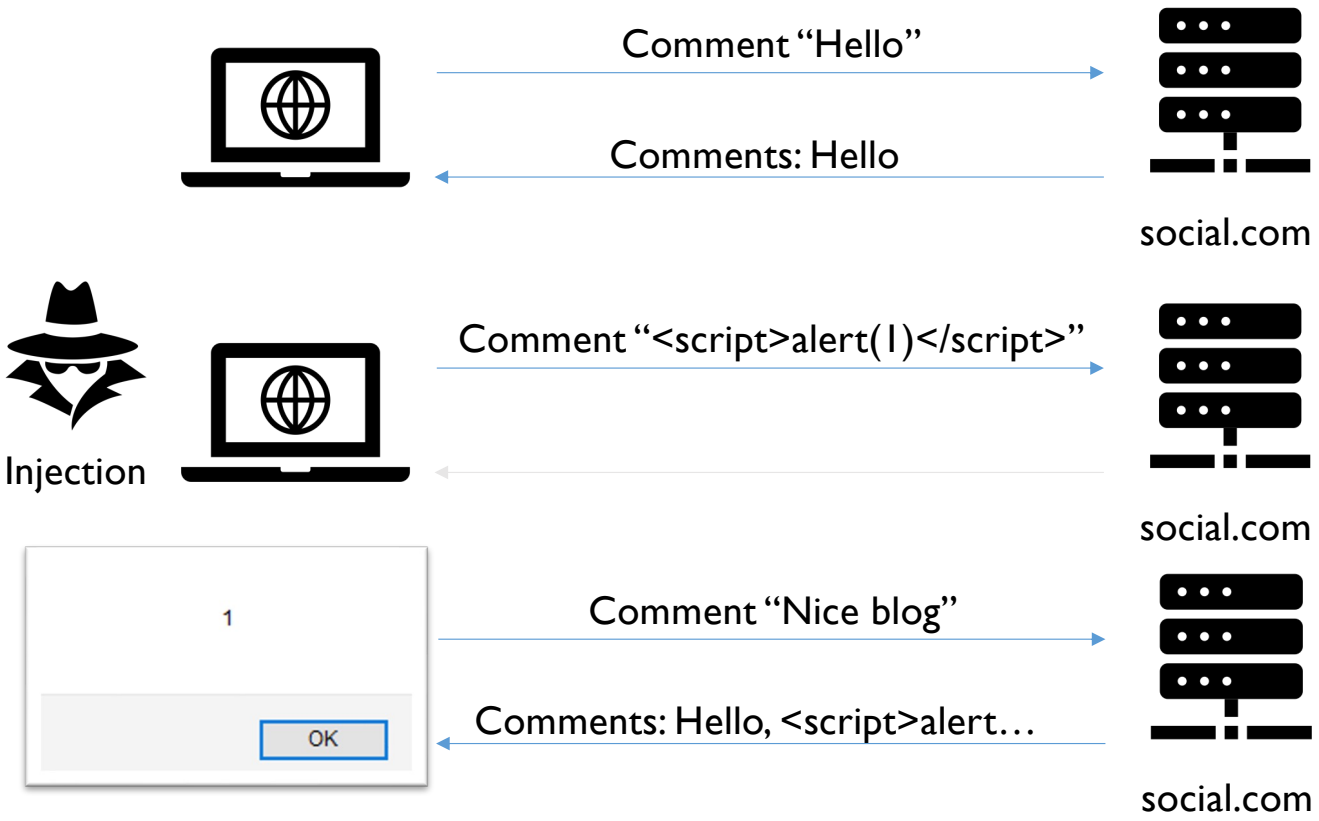
SHARE THIS PAGE

January 2020

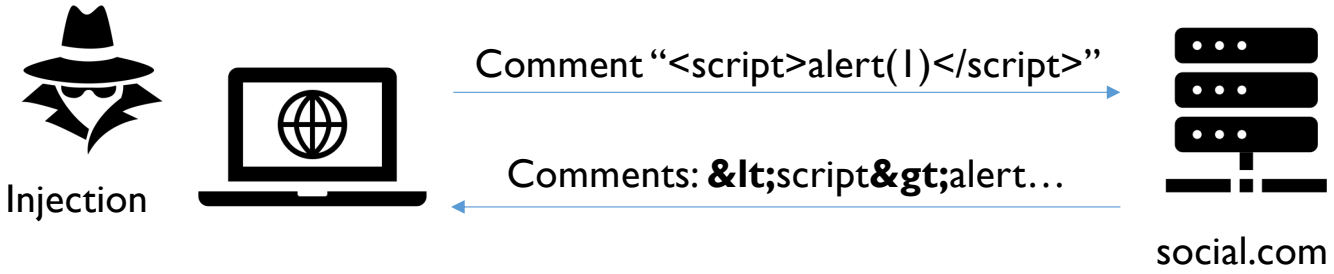
In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up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



XSS attacks by code injection

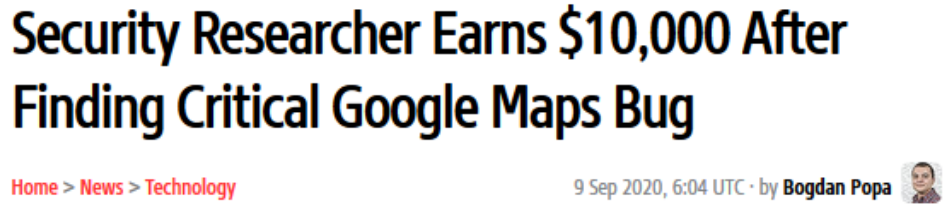


Fix: input validation and output sanitization/encoding



Hard to find!

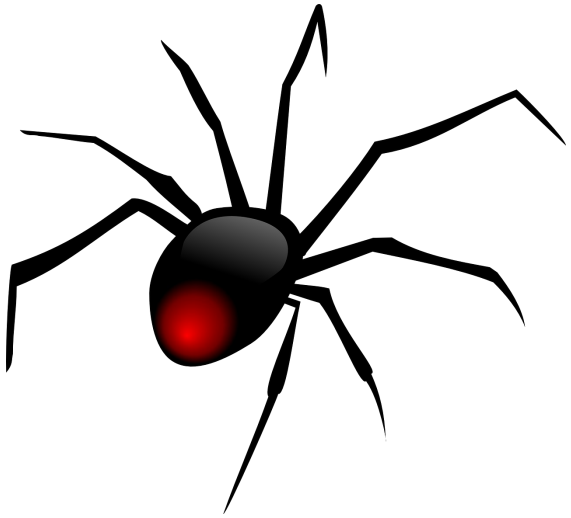
- Comment section
- Admin panel
- Newsletter email
- Feedback forms
- Product reviews
- …



Black Widow Black Ostrich Spider-Scents

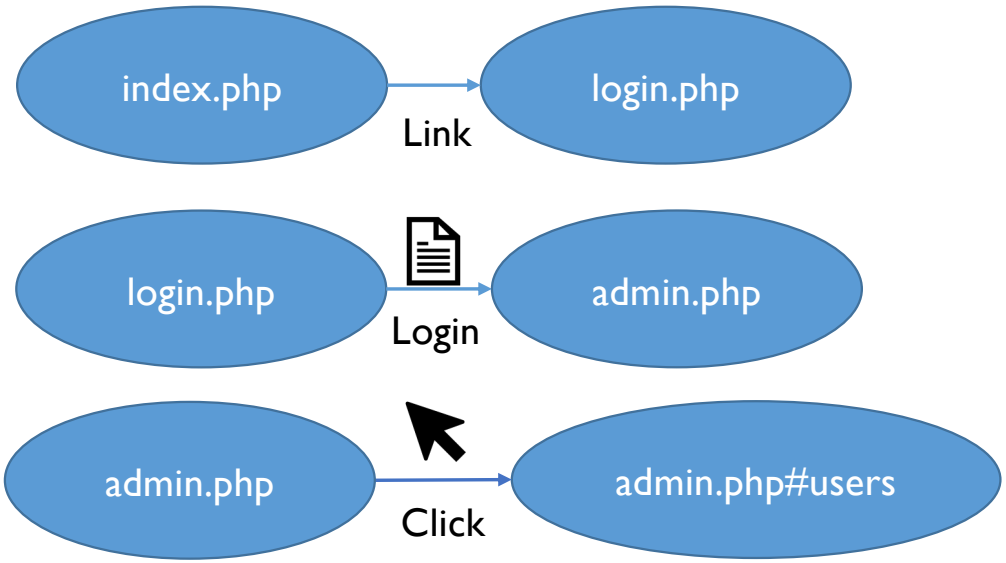
Black Widow

- 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



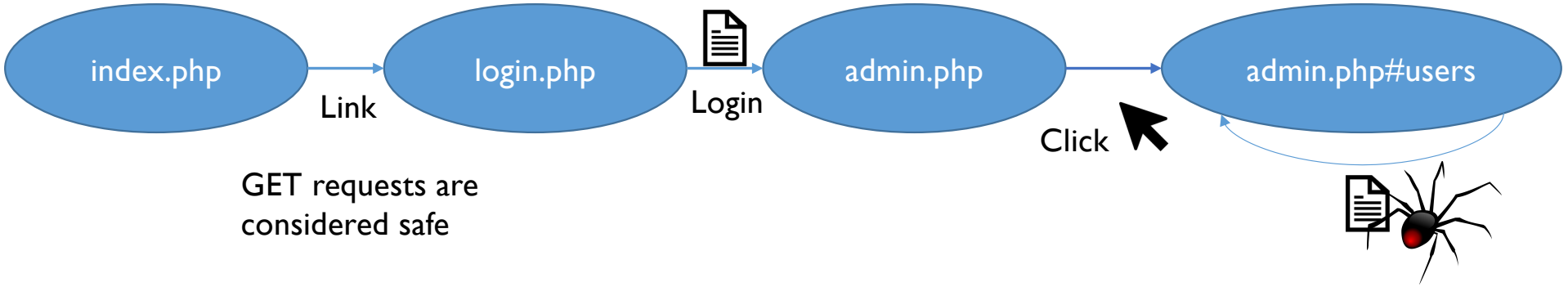
Navigation

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



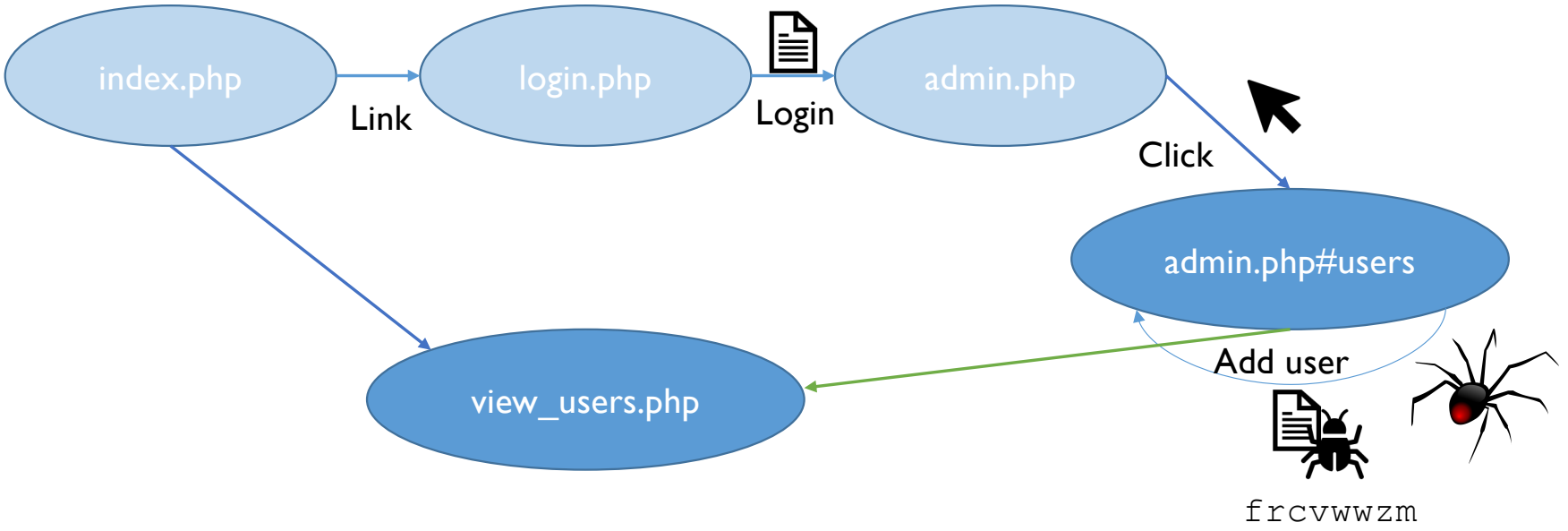
Traversing

- 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

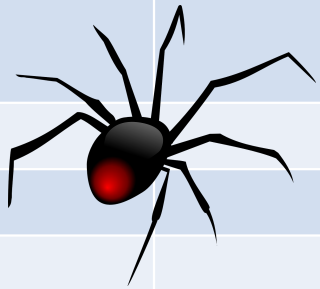


Evaluation

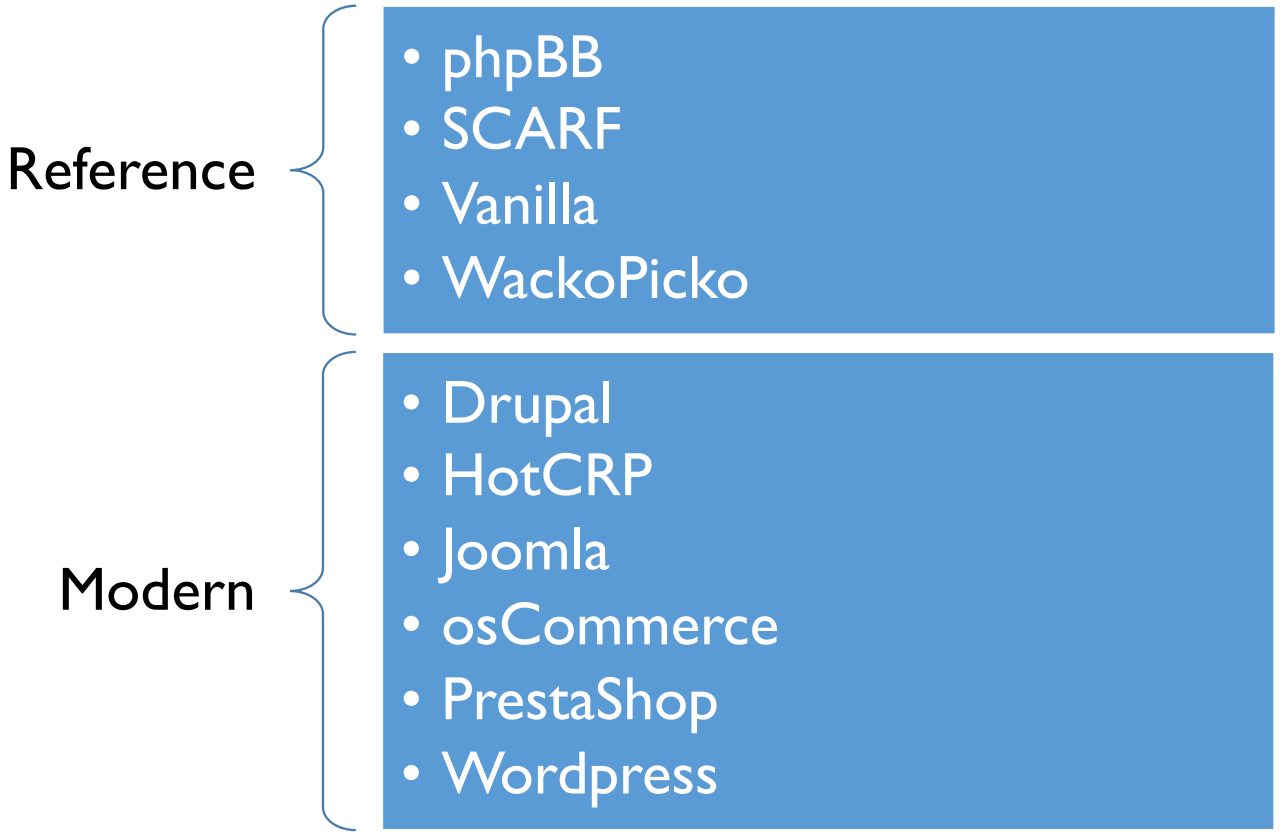
- Server-side code coverage
- Number of found vulnerabilities

Evaluation

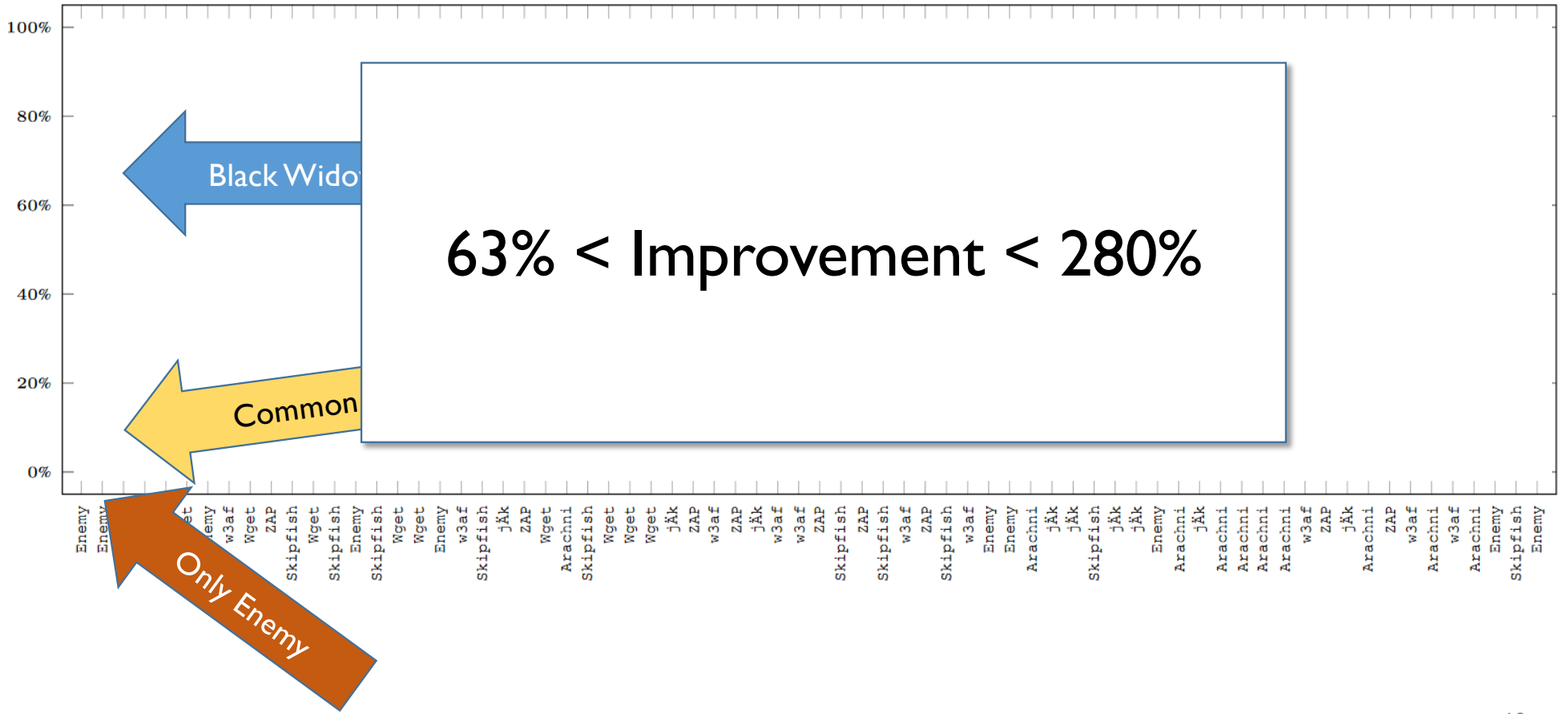
	Arachni	Enemy	jÄk	Skipfish	W3af	Wget	ZAP
Drupal							
HotCRP							
Joomla							
osCommerce							
phpBB							
PrestaShop							
SCARF							
Vanilla							
WackoPicko							
Wordpress							



Evaluation - Applications



Results – Coverage (Lines of Code)



Results – Vulnerabilities

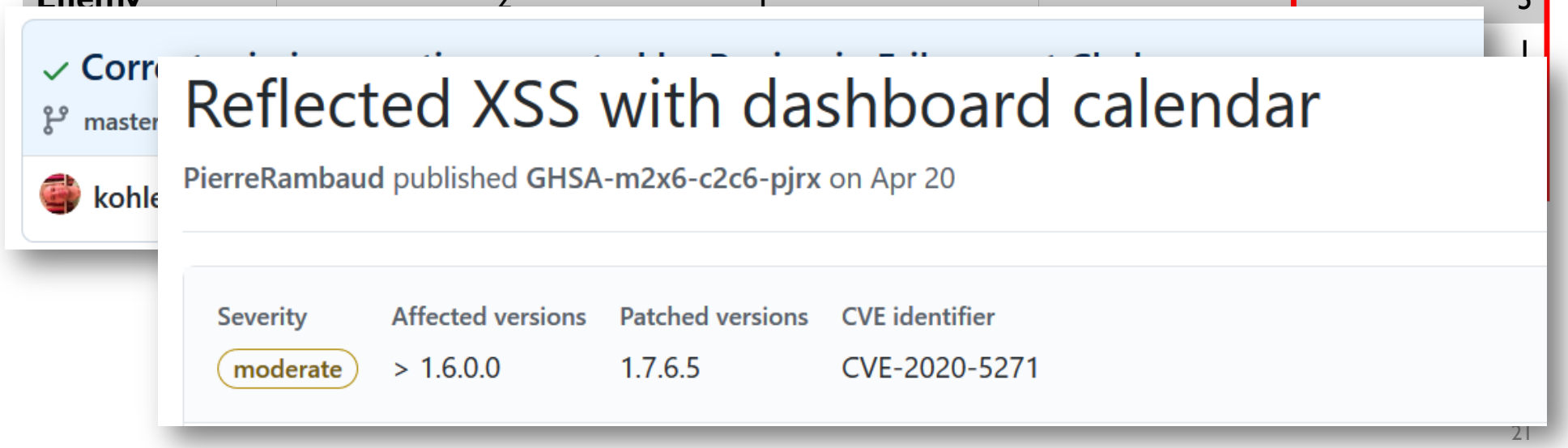
Crawler	Reference (Reflected XSS)	Reference (Stored XSS)	Modern (Reflected XSS)	Modern (Stored XSS)	Total
Black Widow	**8**	**13**	**3**	**1**	**25**
Arachni	6	1			7
Enemy	2	1			3
jÄk	1				1
Skipfish	1				1
W3af	2				2
ZAP					0

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



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