



# SH#FT Happens!! How to deploy DevSecOps principles in the development lifecycle.

Joylynn Kirui – Senior Cloud Security Advocate, Microsoft

[https://twitter.com/joylynn\\_kirui](https://twitter.com/joylynn_kirui) 

52% of companies  
sacrifice cybersecurity for speed

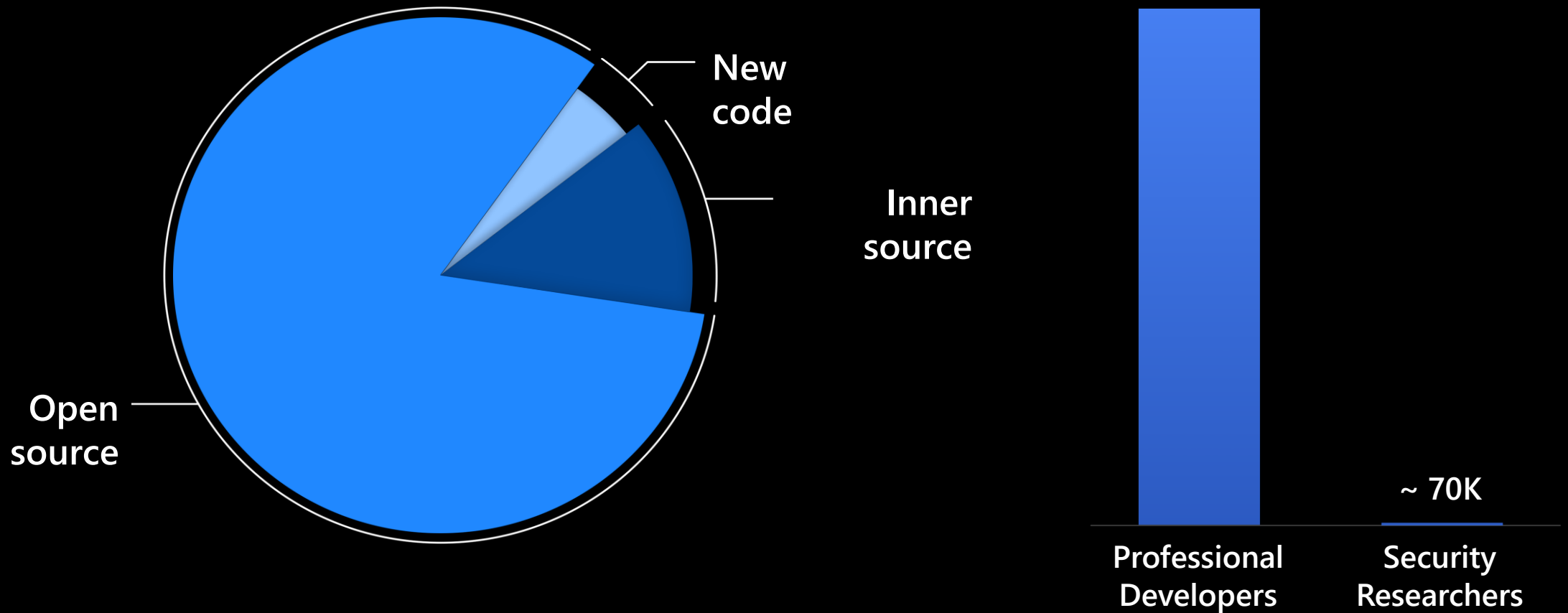
---

57% of ops teams  
push back on security best practices

---

44% of developers  
are not trained to code securely

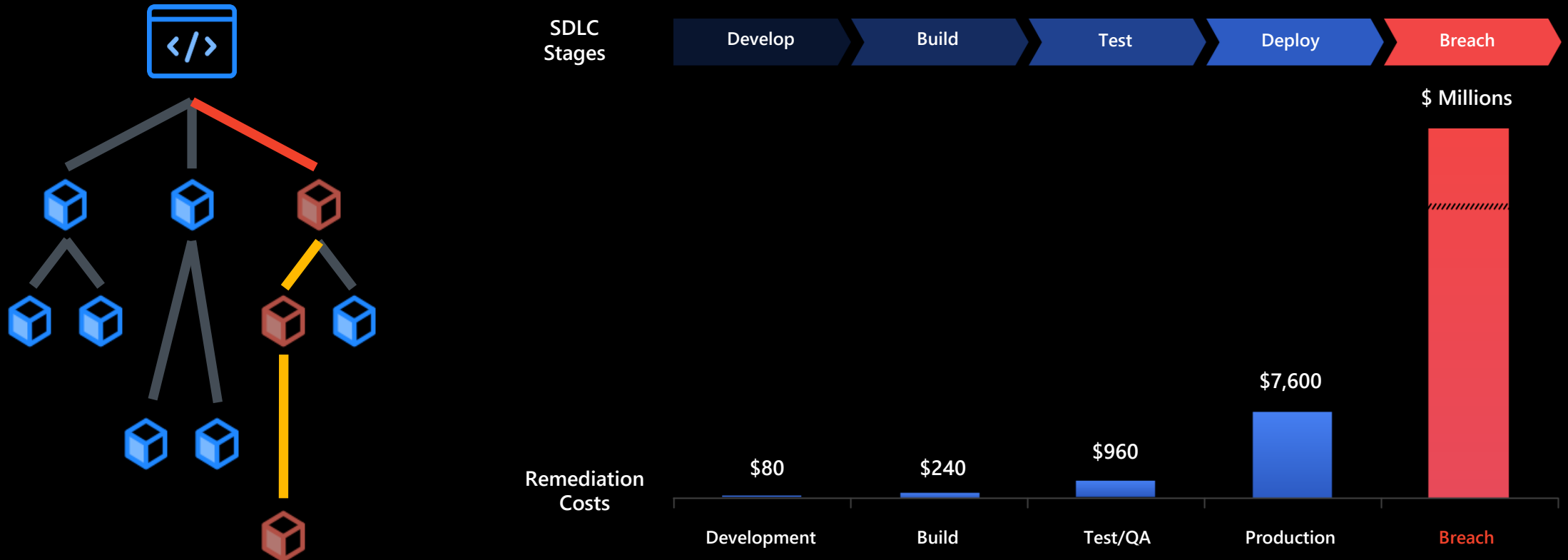
80-90% of the code in new applications  
comes from open source.



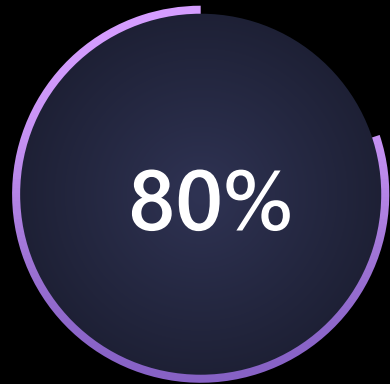
There 570x more developers than security researchers

## Other sources of vulnerabilities

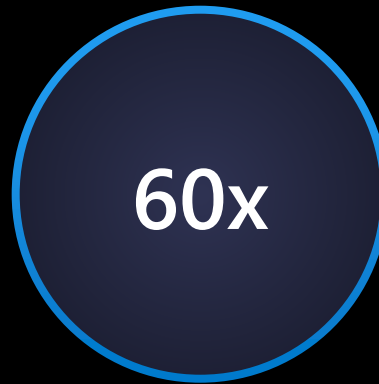
- Unchecked dependencies (80-90% of your code)
- Employee error (exposed access tokens, unsafe code patterns)
- 570x more developers than security researchers
- Damage is exponentially greater if it reaches production



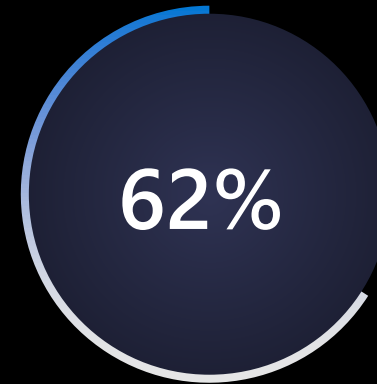
# Importance of shifting security left



reduction in security incidents by extending security to development<sup>2</sup>



Security cost to fix a security defect in production versus in development<sup>1</sup>



of enterprises do not integrate security in the development phase<sup>3</sup>

<sup>1</sup>National Institute of Standards and Technology

<sup>2</sup><https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/>

<sup>3</sup>Sources: McKinsey Developer Velocity, Microsoft Enterprise DevOps Report, GitHub Octoverse Report 2020

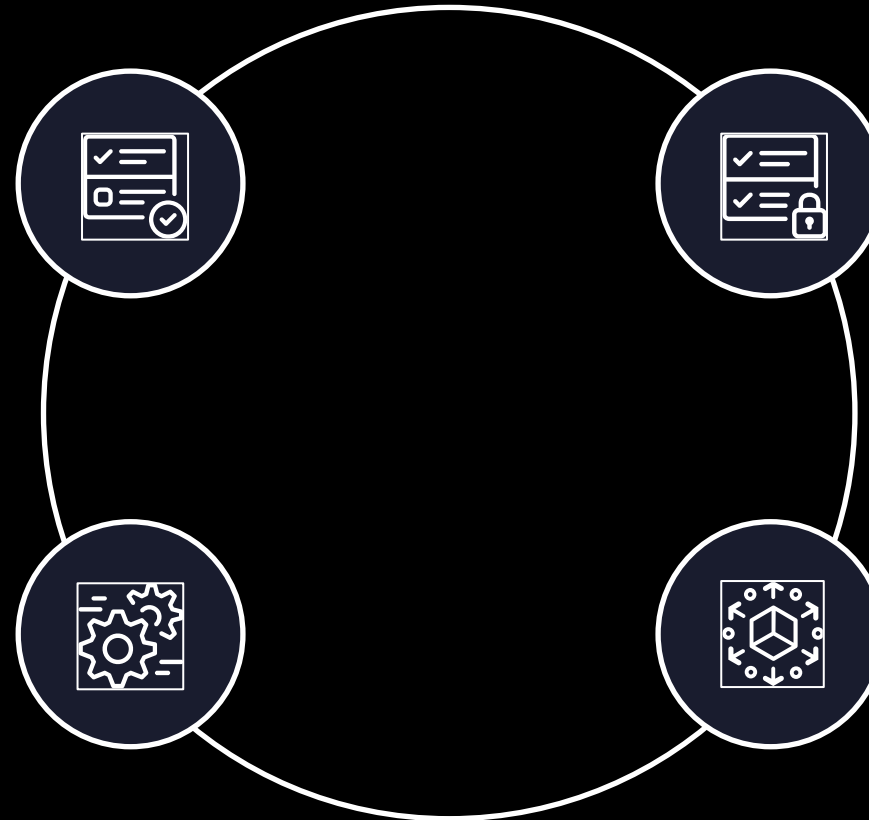
# How security fits in the development lifecycle

## PRE-COMMIT

- Threat modeling
- IDE security plug-in
- Pre-commit hooks
- Secure coding standards
- Peer review

## OPERATE & MONITOR

- Continuous monitoring
- Threat intelligence
- Blameless post-mortems



## COMMIT (CI)

- Static Application Security Testing (SAST)
- Security unit tests
- Dependency management / Software Composition Analysis (SCA)
- Credential scanning

## DEPLOY (CD)

- Infra as code (IaC)
- Dynamic security scanning
- Cloud configuration checks
- Security acceptance tests

# Run static & dynamic analysis

## AUTOMATED SECURITY REVIEW AND TESTING THROUGHOUT THE DEVOPS LIFECYCLE

### Automations:



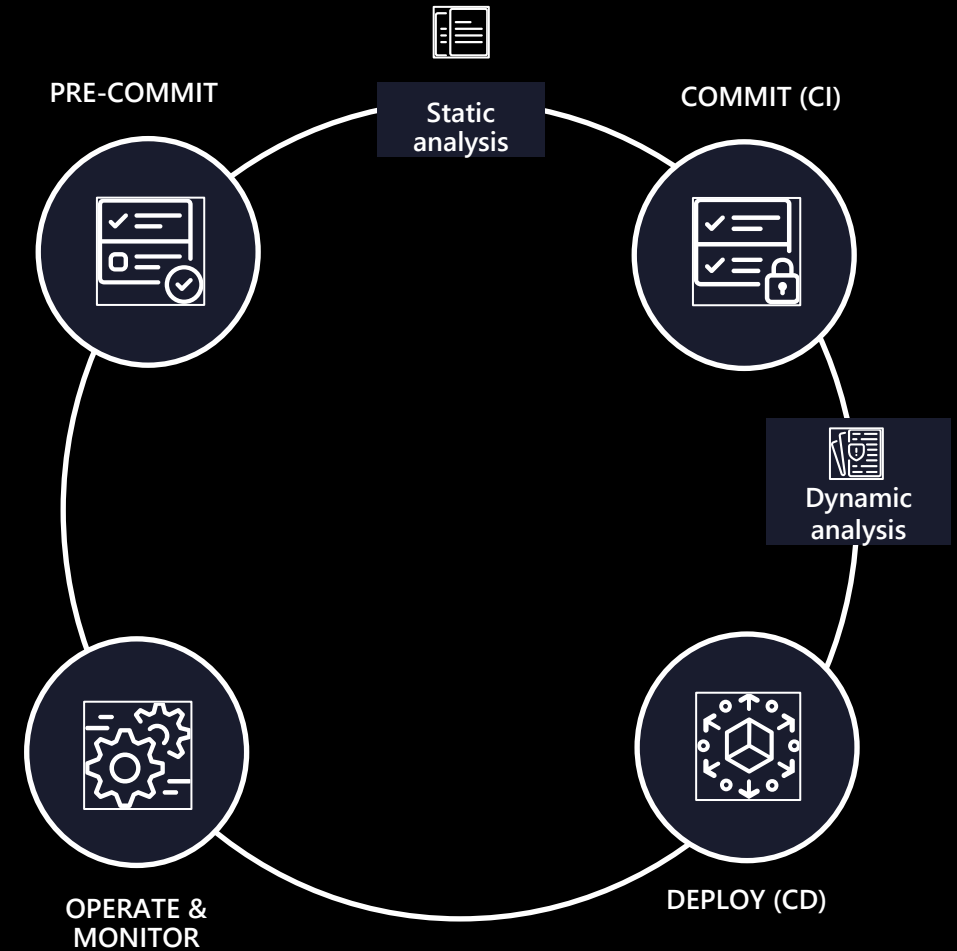
Automated  
security review  
of code



Automated  
simulated  
attacks  
targeting  
running  
application

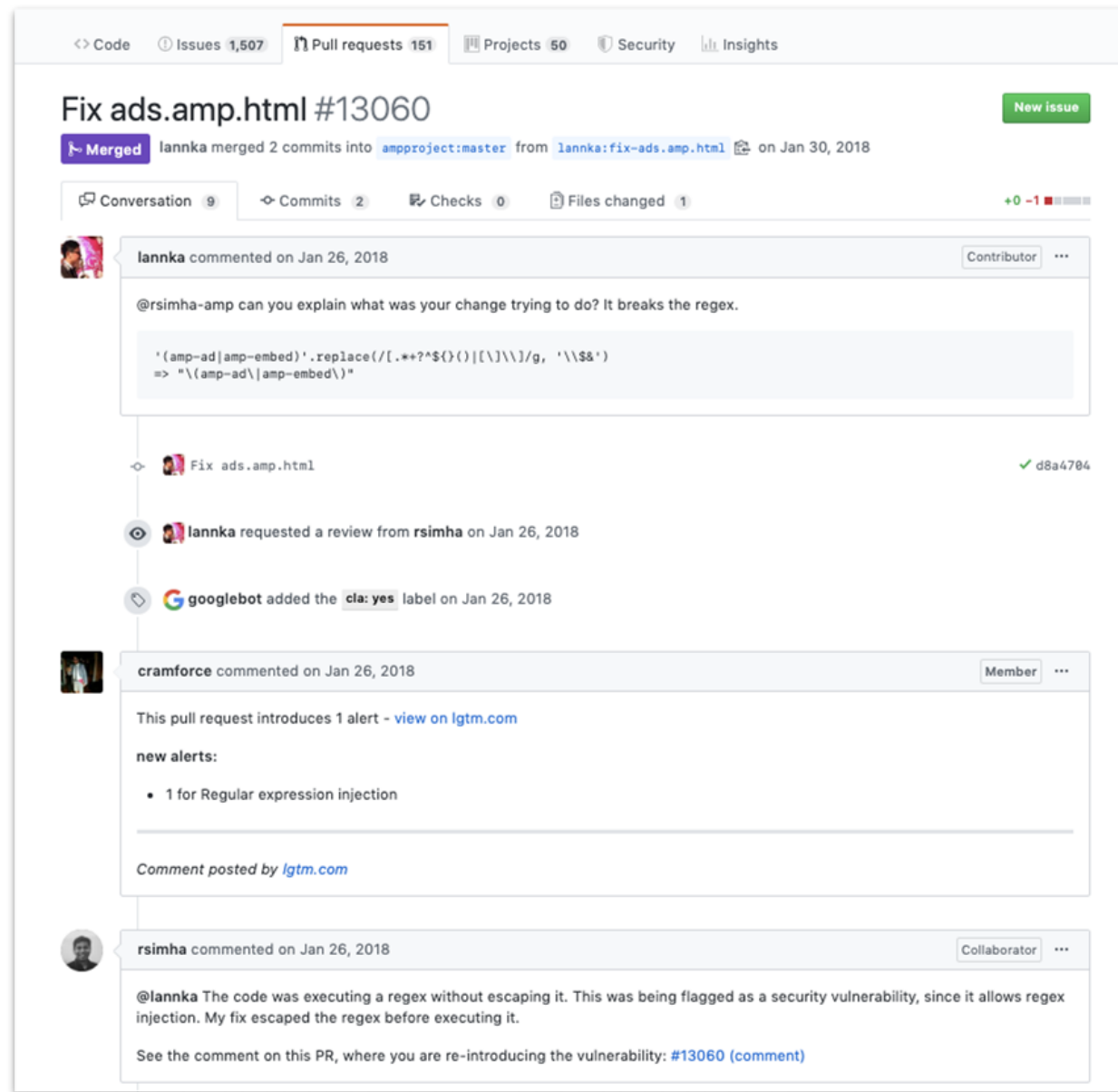
### PREVENT THESE TYPES OF ATTACKS:

- Common technical application security attacks

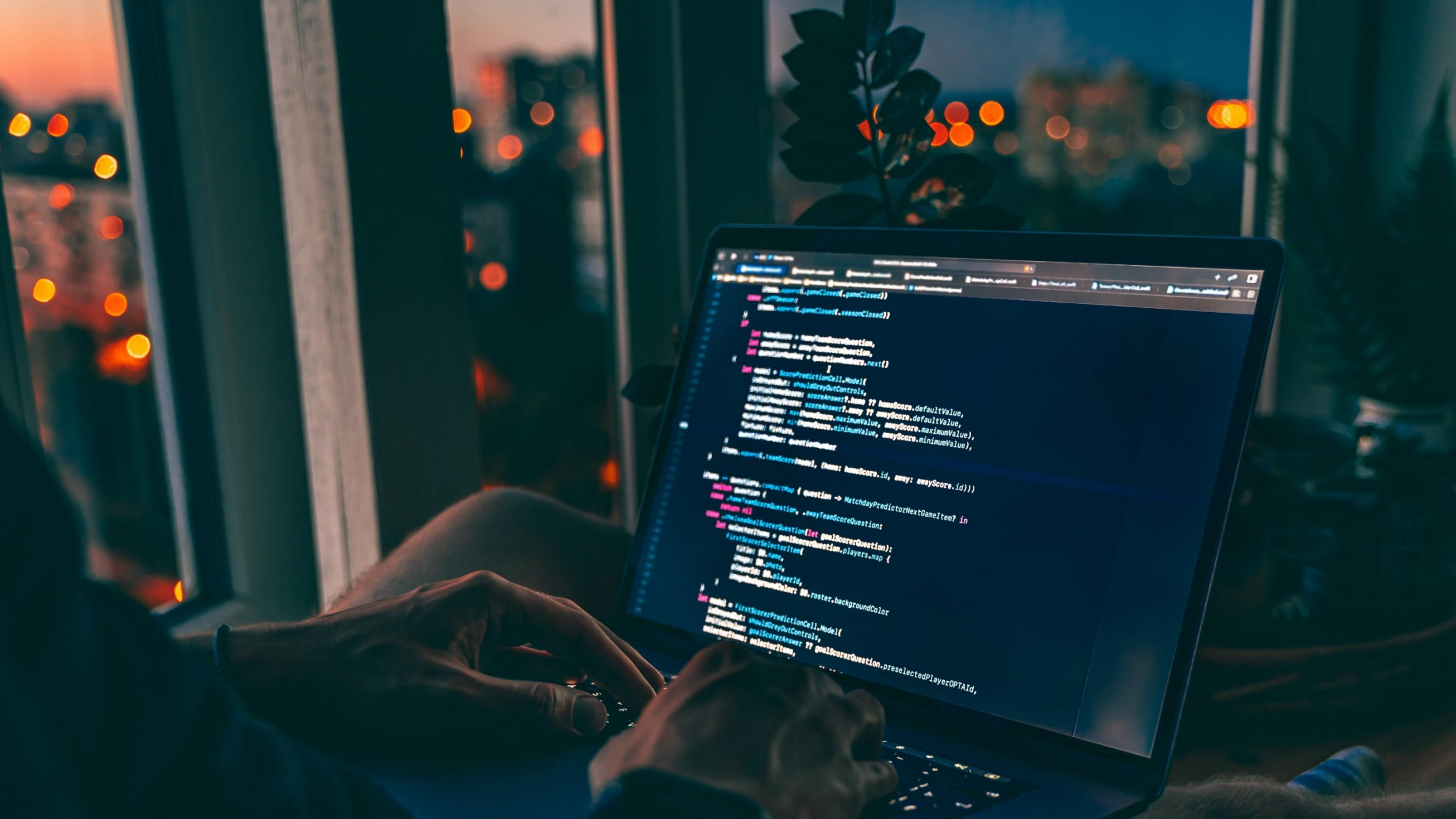


# Code Scanning

- CodeQL: The world's most advanced semantic code engine
- Community-driven query set brings top experts to your team
- Customize & build new queries to adapt to your specific threat topology and to find variants
- Extensible, with support for DAST and other SAST tools







```
if (homeScore?.gameClosed?.gameClosed) {
    // ...
}
if (homeScore?.gameClosed?.seasonClosed) {
    // ...
}

fun homeScore = homeScoreQuestion,
awayScore = awayScoreQuestion,
questionNumber = questionNumber.next()

fun homeScore = ScorePredictionCell.Model {
    shouldGreyOutControls: scoreAnswer?.home ?? homeScore.defaultValue,
    goalScorerAnswer: scoreAnswer?.away ?? awayScore.defaultValue,
    minScore: min(homeScore.minimumValue, awayScore.minimumValue),
    maxScore: max(homeScore.minimumValue, awayScore.minimumValue),
    questionNumber: questionNumber
}

fun homeScoreModel, (home: homeScore.id, away: awayScore.id)))

fun homeScoreModel {
    // ...
}

fun homeScoreQuestion, .awayTeamScoreQuestions:
    // ...
}

fun homeScoreQuestion {
    // ...
}

fun homeScoreQuestion {
    // ...
}

fun homeScoreQuestion {
    // ...
}
```

[aka.ms/DevSecOpsSolution](https://aka.ms/DevSecOpsSolution)



[https://codeql.github.com/docs/  
codeql-for-visual-studio-code/](https://codeql.github.com/docs/codeql-for-visual-studio-code/)

Code Issues 1,507 Pull requests 151 Projects 50 Security Insights

## Fix ads.amp.html #13060 New issue

Merged lannka merged 2 commits into `ampproject:master` from `lannka:fix-ads.amp.html` on Jan 30, 2018

Conversation 9 Commits 2 Checks 0 Files changed 1 +0 -1

**lannka** commented on Jan 26, 2018 Contributor

@rsimha-amp can you explain what was your change trying to do? It breaks the regex.

```
'(amp-ad|amp-embed)'.replace(/[\.\*\?^\$\{\}\|\[\]\$\{\}/g, '\\$&')  
=> "\\(amp-ad|amp-embed\\)"
```

Fix ads.amp.html d8a4784

**lannka** requested a review from **rsimha** on Jan 26, 2018

Googlebot added the `cla: yes` label on Jan 26, 2018

**cramforce** commented on Jan 26, 2018 Member

This pull request introduces 1 alert - [view on lgtm.com](#)

**new alerts:**

- 1 for Regular expression injection

*Comment posted by lgtm.com*

**rsimha** commented on Jan 26, 2018 Collaborator

@lannka The code was executing a regex without escaping it. This was being flagged as a security vulnerability, since it allows regex injection. My fix escaped the regex before executing it.

See the comment on this PR, where you are re-introducing the vulnerability: [#13060 \(comment\)](#)

## Resources

1. Configure Microsoft Security DevOps GitHub Actions – <https://learn.microsoft.com/en-us/azure/defender-for-cloud/github-action>
2. Connect your GitHub repositories to Microsoft Defender for Cloud - <https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-github>
3. DevOps Security Workbook - <https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/devops-security-workbook/ba-p/3637662>

# Thank you

[https://twitter.com/joylynn\\_kirui](https://twitter.com/joylynn_kirui)

