Microsoft

The Art of Defensive Programming

Joylynn Kirui – Senior Cloud Security Advocate, Microsoft

https://twitter.com/joylynn_kirui

52% of companies

sacrifice cybersecurity for speed

57% of ops teams

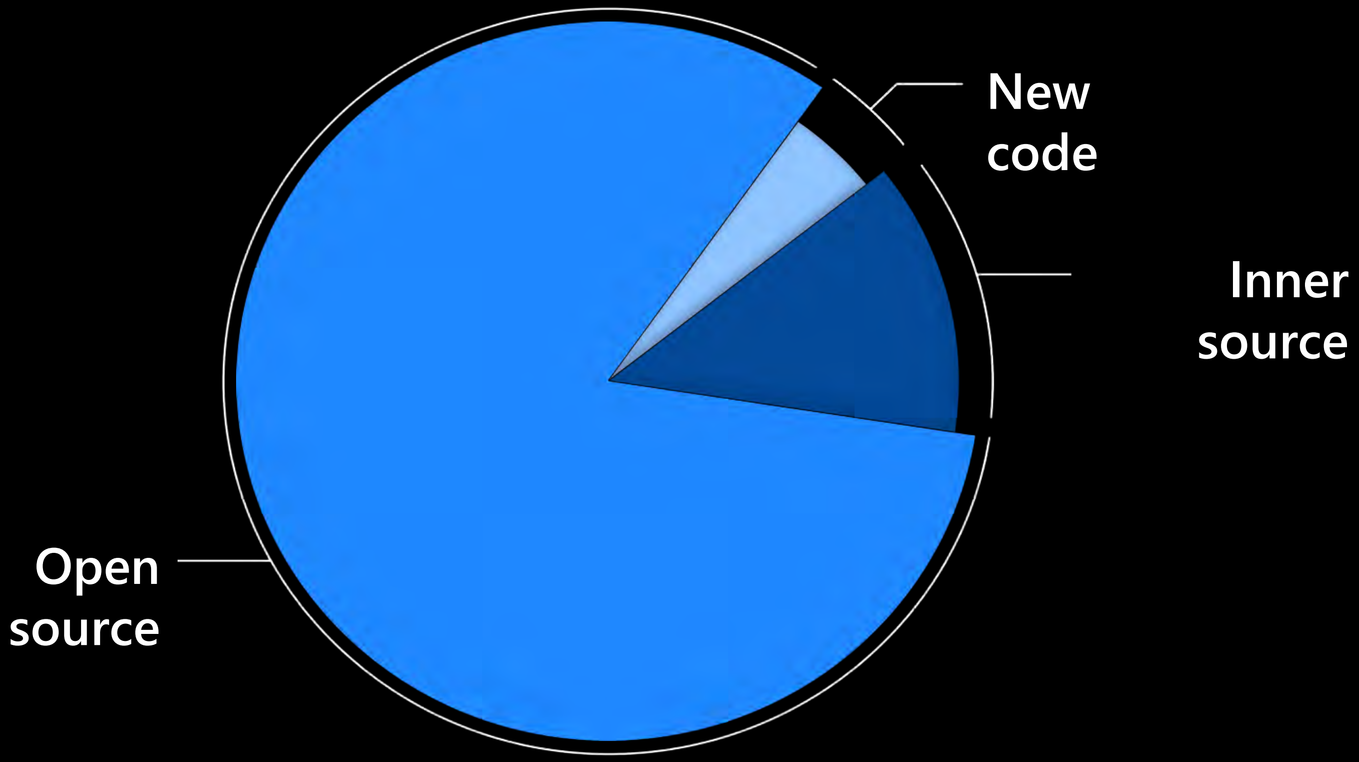
push back on security best practices

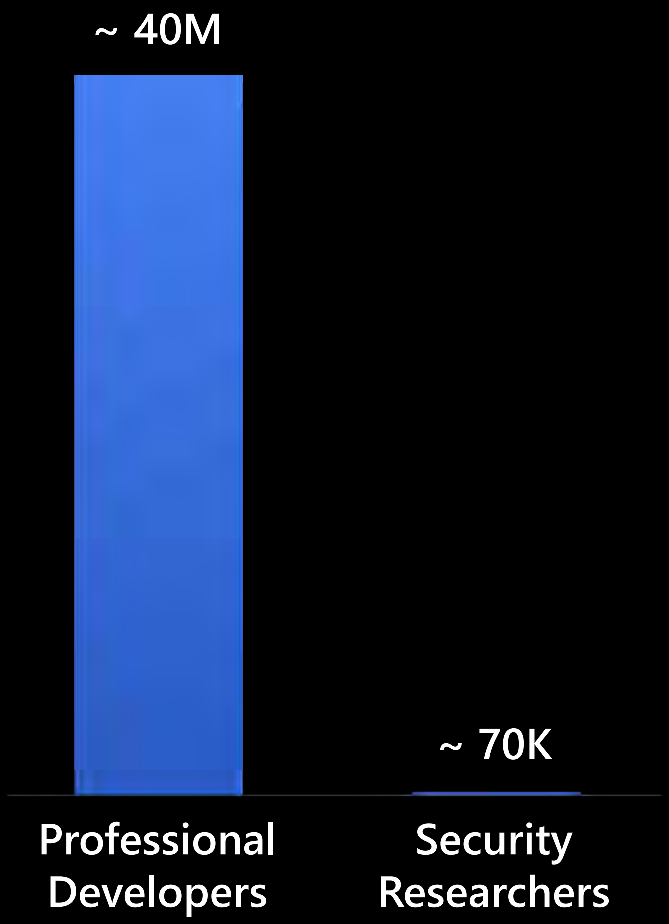
44% of developers

are not trained to code securely

Source: Threat Stack, 2018

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

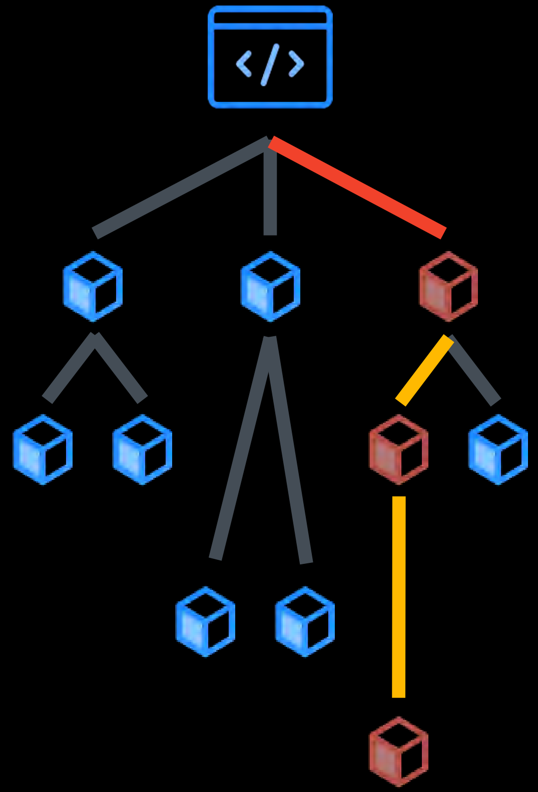


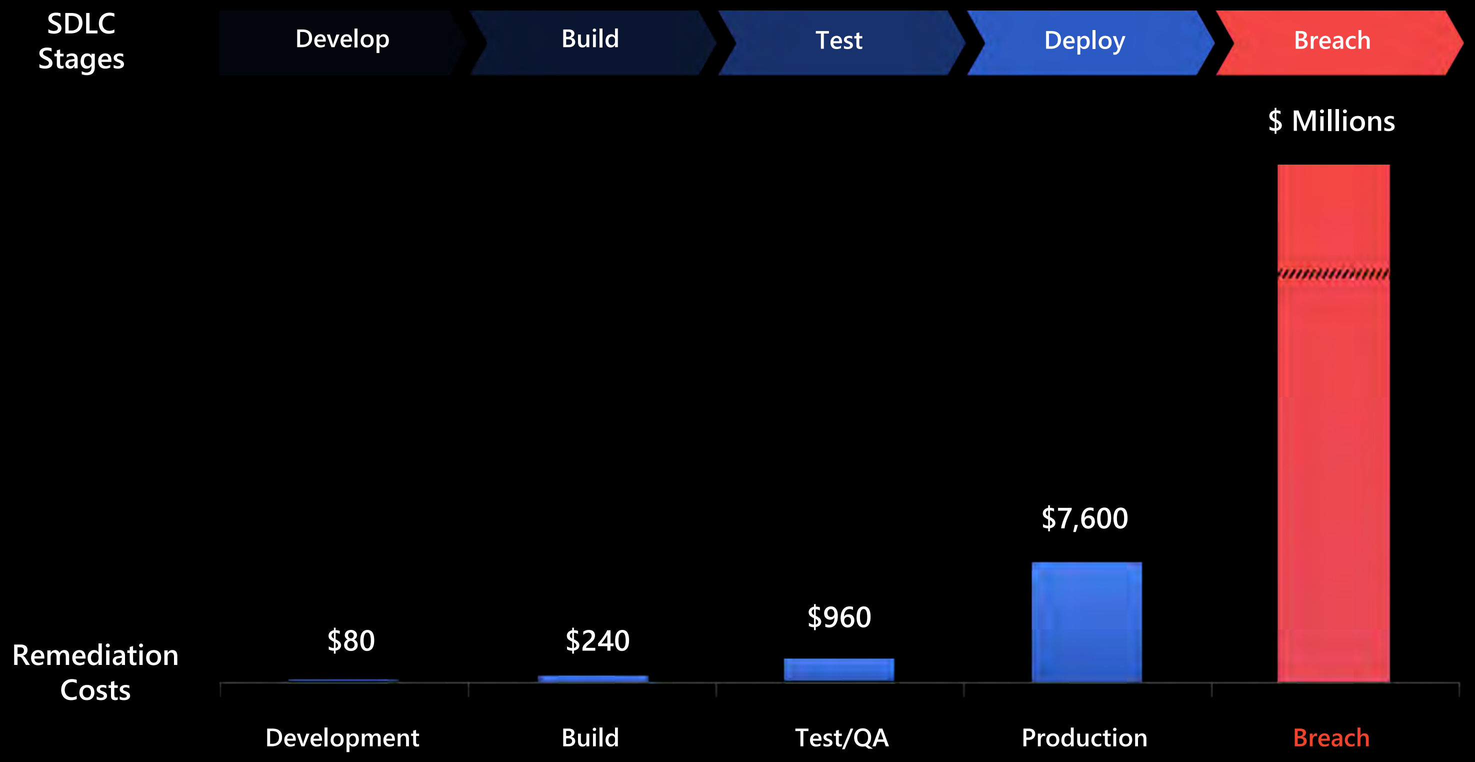


There 570x more developers than security researchers

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





Sources: NIST, Polemon Institute

Importance of shifting security left

80%

reduction in security incidents by extending security to development[2]

60x

Security cost to fix a security defect in production versus in development[1]

62%

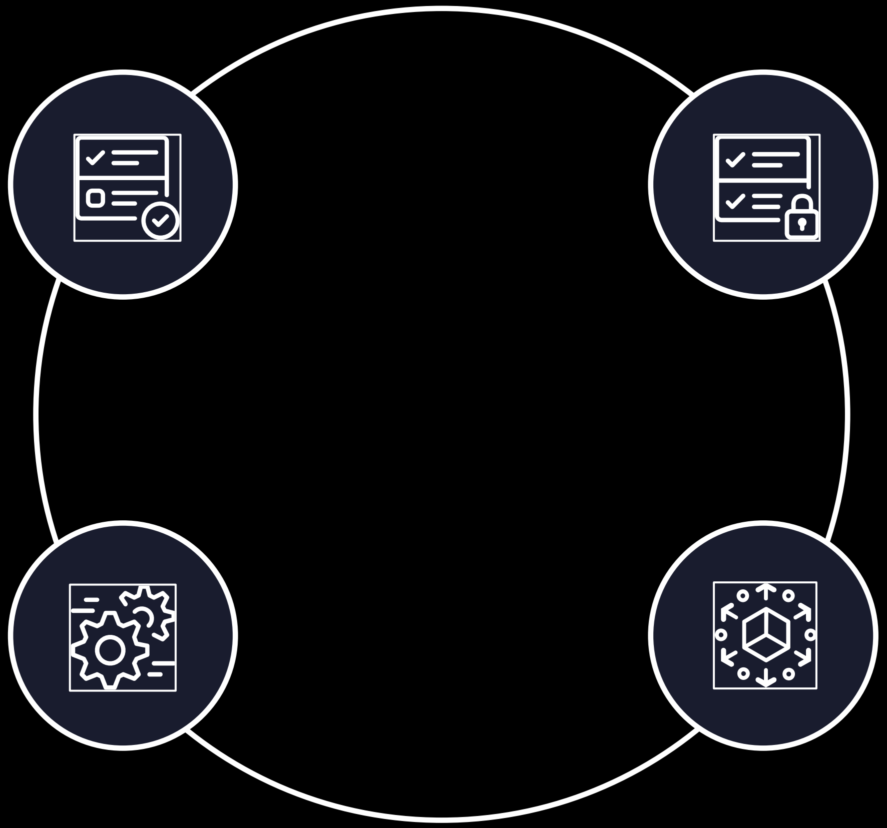
of enterprises do not integrate security in the development phase[3]

[1] National Institute of Standards and Technology

[2] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[3] 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

COMMIT (CI)

- Static code analysis
- Security unit tests
- Dependency management
- Credential scanning

DEPLOY (CD)

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

OPERATE & MONITOR

- Continuous monitoring
- Threat intelligence
- Blameless post-mortems

Run static & dynamic analysis

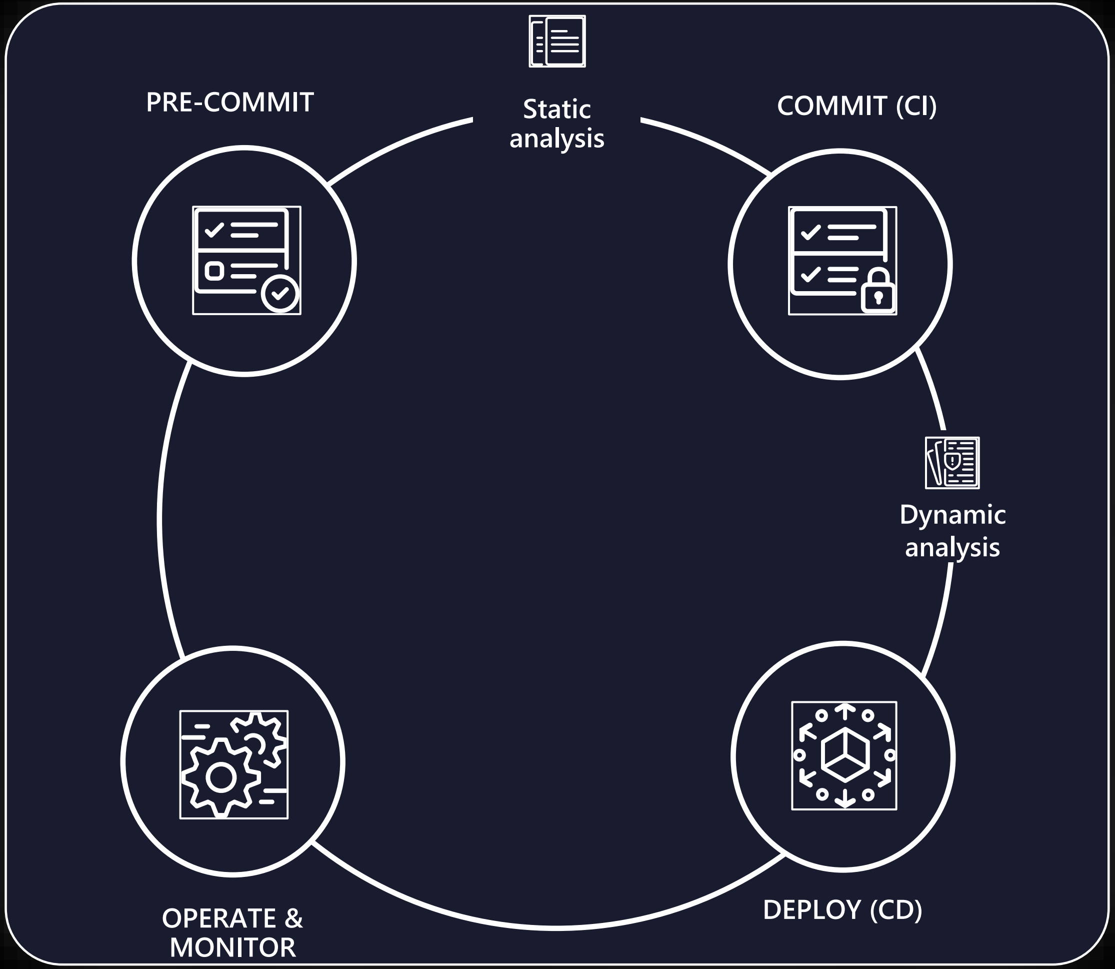
AUTOMATED SECURITY REVIEW AND TESTING THROUGHOUT THE DEVOPS LIFECYCLE

Automations:

- Automated security review of code
- Automated simulated attacks targeting running application

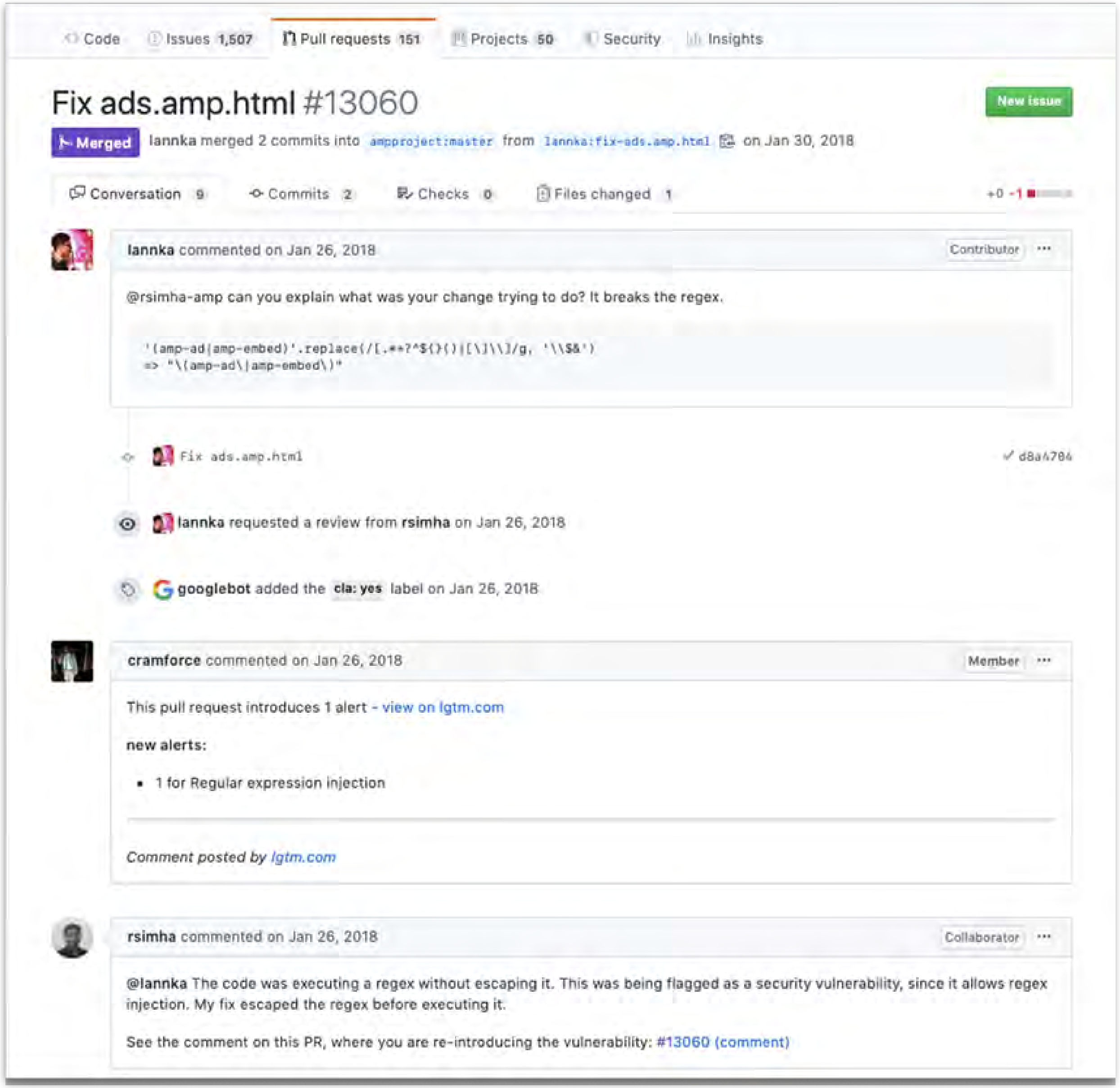
PREVENT THESE TYPES OF ATTACKS:

- 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



Fix ads.amp.html #13060

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

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.

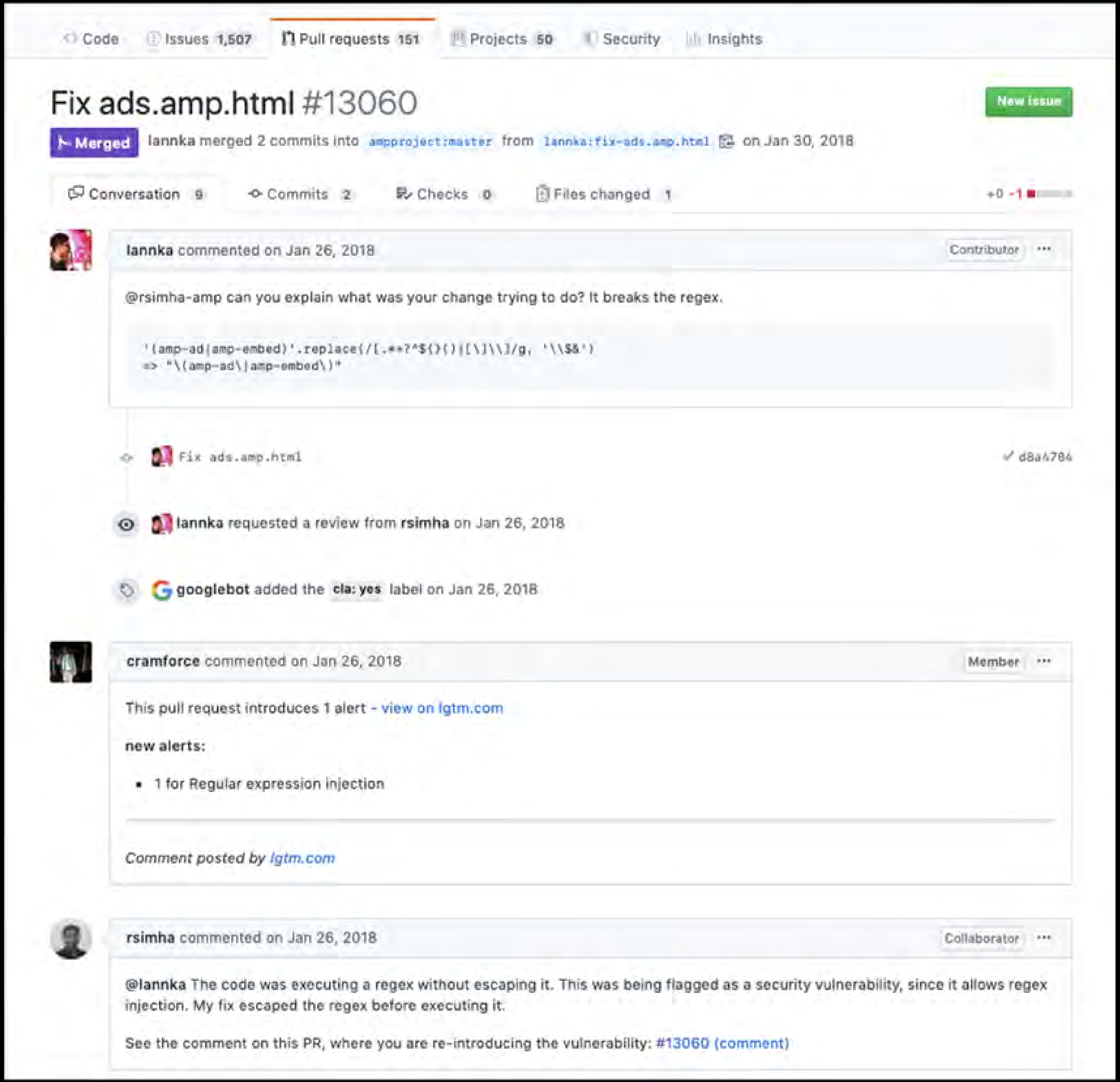
See the comment on this PR, where you are re-introducing the vulnerability: #13060 (comment)

```
[illegible].append(.gameClosed(.gameClosed))
case .[illegible]Season:
    [illegible].append(.gameClosed(.seasonClosed))
}
[illegible]
    let homeScore = homeTeamScoreQuestion,
    let awayScore = awayTeamScoreQuestion,
    let questionNumber = questionNumbers.next()
{
let model = ScorePredictionCell.Model(
    [illegible]: shouldGreyOutControls,
    [illegible]: scoreAnswer?.home ?? homeScore.defaultValue,
    [illegible]: scoreAnswer?.away ?? awayScore.defaultValue,
    [illegible]: max(homeScore.maximumValue, awayScore.maximumValue),
    [illegible]: min(homeScore.minimumValue, awayScore.minimumValue),
    [illegible]: [illegible],
    questionNumber: questionNumber
)
[illegible].append(.teamScore(model, (home: homeScore.id, away: awayScore.id)))
}

[illegible] += [illegible].compactMap { question -> MatchdayPredictorNextGameItem? in
    switch question {
    case .homeTeamScoreQuestion, .awayTeamScoreQuestion:
        return nil
    case .[illegible]GoalScorerQuestion(let goalScorerQuestion):
        let [illegible] = goalScorerQuestion.players.map {
            FirstScorerSelectorItem(
                [illegible]: $0.name,
                [illegible]: $0.photo,
                playerId: $0.playerId,
                [illegible]BackgroundColor: $0.roster.backgroundColor
            )
        }
        let model = FirstScorerPredictionCell.Model(
            [illegible]: shouldGreyOutControls,
            [illegible]: goalScorerAnswer ?? goalScorerQuestion.preselectedPlayerOPTAId,
            selectorItems: selectorItems,
```

aka.ms/DevSecOpsSolution

https://codeql.github.com/docs/codeql-for-visual-studio-code/



Fix ads.amp.html #13060

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

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)

Thank you

https://twitter.com/joylynn_kirui