1 Kit, 8 Steps, 30 Days. How we Raised Application Security Awareness.

Andrew Thompson
Solution Architect

CHECKMARX

Agenda

- Top AppSec Challenges
- The Secure Dev Kit
- Case Study
- AppSec Quiz Time
- Final Notes

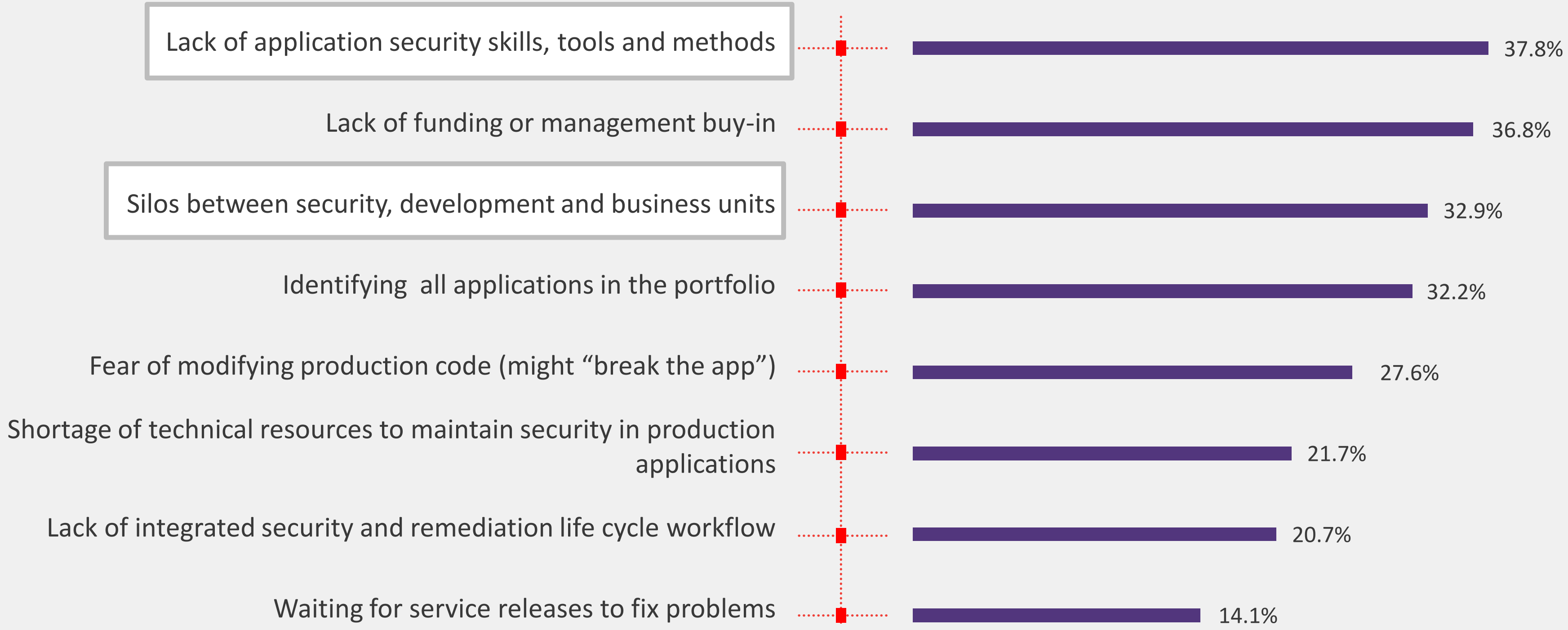
The Case for AppSec Education

Quick Sync Survey

What is your top challenge in implementing application security?

- A: Developer Education and Skills
- B: Silos between security and development
- C: Lack of Budget
- D: We have no challenges!

What Are Your Top Challenges In Implementing Application Security.



CHALLENGES: OUTNUMBERED, SILOED & INEXPERIENCED

Developers

Security Manager

Frost & Sullivan: “By 2020 we will have a shortage of 1.5M cyber experts”

Websense: “Takes 11 years to become an expert in modern cyber attacks”

The Result

Here's our 8 bit plan

For raising secure development awareness

Step 00000001

Order the Secure Development Kit

It's a physical kit that includes everything you need in order to raise awareness within your organization for application security and have some fun while doing so.

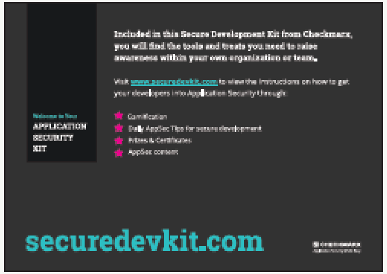
Order a Free Kit

The Kit

Secure Development Kit

www.securedevkit.com

package box



Welcome to Your
APPLICATION
SECURITY
KIT

Included in this Secure Development Kit from Checkmarx, you will find the tools and treats you need to raise awareness within your own organization or team.

Visit www.securedevkit.com to view the instructions on how to get your developers into Application Security through:

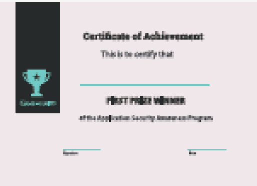
- Gamification
- Daily AppSec Tips for secure development
- Prizes & Certificates
- AppSec content

securedevkit.com

teaser business cards *50 units

welcome- A5

certificates- 1st, 2nd, 3rd place



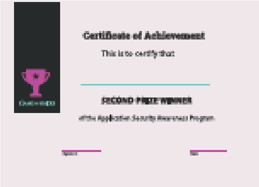
Certificate of Achievement

This is to certify that

FIRST PRIZE WINNER

of the Application Security Awareness Program

Signature Date



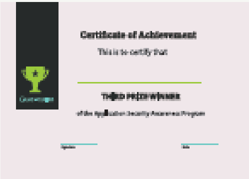
Certificate of Achievement

This is to certify that

SECOND PRIZE WINNER

of the Application Security Awareness Program

Signature Date



Certificate of Achievement

This is to certify that

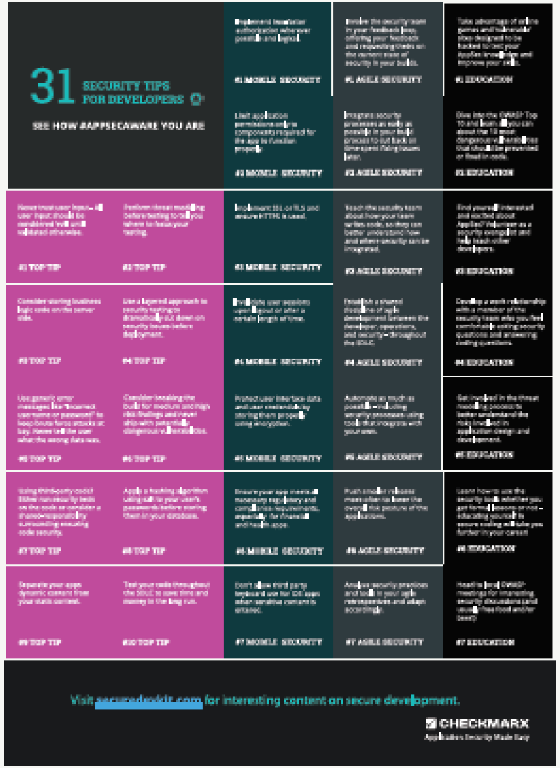
THIRD PRIZE WINNER

of the Application Security Awareness Program

Signature Date

3 GoH shirts

The Kit



31 SECURITY TIPS FOR DEVELOPERS

SEE HOW #APPSECAWARE YOU ARE

Implement two-factor authentication wherever possible and logical.
#1 MOBILE SECURITY

Limit application permissions only to components required for the app to function properly.
#2 MOBILE SECURITY

Implement SSL or TLS and ensure HTTPS is used.
#3 MOBILE SECURITY

Invalidate user sessions upon logout or after a certain length of time.
#4 MOBILE SECURITY

Protect user interface data and user credentials by storing them properly using encryption.
#5 MOBILE SECURITY

Ensure your app meets all necessary regulatory and compliance requirements, especially for financial and health apps.
#6 MOBILE SECURITY

Don't allow third party keyboard use for iOS apps when sensitive content is entered.
#7 MOBILE SECURITY

Involve the security team in your feedback loop, offering your feedback and requesting theirs on the current state of security in your builds.
#1 AGILE SECURITY

Integrate security processes as early as possible in your build process to cut back on time spent fixing issues later.
#2 AGILE SECURITY

Teach the security team about how your team writes code, so they can better understand how and where security can be integrated.
#3 AGILE SECURITY

Establish a shared discipline of agile development between the developer, operations, and security – throughout the SDLC.
#4 AGILE SECURITY

Automate as much as possible – including security processes using tools that integrate with your own.
#5 AGILE SECURITY

Push smaller releases more often to lower the overall risk posture of the applications.
#6 AGILE SECURITY

Analyze security practices and tools in your agile retrospectives and adapt accordingly.
#7 AGILE SECURITY

Take advantage of online games and vulnerable sites designed to be hacked to test your AppSec knowledge and improve your skills.
#1 EDUCATION

Dive into the OWASP Top 10 and learn all you can about the 10 most dangerous vulnerabilities that should be prevented or fixed in code.
#2 EDUCATION

Find yourself interested and excited about AppSec? Volunteer as a security evangelist and help teach other developers.
#3 EDUCATION

Develop a work relationship with a member of the security team who you feel comfortable asking security questions and answering coding questions.
#4 EDUCATION

Get involved in the threat modeling process to better understand the risks involved in application design and development.
#5 EDUCATION

Learn how to use the security tools whether you get formal lessons or not – educating yourself in secure coding will take you further in your career.
#6 EDUCATION

Head to local OWASP meetings for interesting security discussions and usually free food and/or beer!
#7 EDUCATION

Never trust user input – all user input should be considered 'evil' until validated otherwise.
#1 TOP TIP

Perform threat modeling before testing to tell you where to focus your testing.
#2 TOP TIP

Consider storing business logic code on the server side.
#3 TOP TIP

Use a layered approach to security testing to dramatically cut down on security issues before deployment.
#4 TOP TIP

Use generic error messages like "Incorrect username or password" to keep brute force attacks at bay. Never tell the user what the wrong data was.
#5 TOP TIP

Consider breaking the build for medium and high risk findings and never ship with potentially dangerous vulnerabilities.
#6 TOP TIP

Using third-party code? Either run security tests on the code or consider a shared-responsibility surrounding ensuring code security.
#7 TOP TIP

Apply a hashing algorithm using salt to your user's passwords before storing them in your database.
#8 TOP TIP

Separate your app's dynamic content from your static content.
#9 TOP TIP

Test your code throughout the SDLC to save time and money in the long run.
#10 TOP TIP

Visit securedevkit.com for interesting content on secure development.

CHECKMARX
Application Security Made Easy

31 security tips for developers

3 bag pins

20 stickers of each (120 in tot)

Case Study

Application Security Education Program

Organization Details

- Publicly held American technology company
- Develops products for online messaging, marketing, and analytics
- Multiple development teams globally distributed
- Group of 200 Developers were selected for the pilot

The Challenges

Challenges

Management Buy-In

- Explain the long term benefits
  - Top Notch Secure Coding standards
  - Employees with a goal are motivated employees

Engagement

- Don’t force it
- Make it interesting
- Make it Fun
- Make it worthwhile

Budget

- It isn’t expensive if you execute properly

Execution

- Execute locally and run a pilot before you go full scale

The 31 Day Program

Preparations

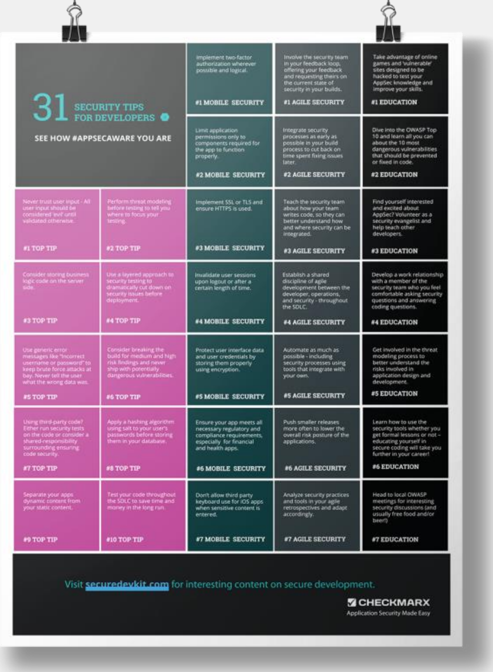
- Champions were assigned
  - Involve champions from the start
  - Invest in your champion's education
- Kickoff with champions
  - Engage champions
- Materials were created and plan was se

Week 1 - Engagement

- Teasers + Quiz + Prizes = Curiosity
- Provide reference and explain what's going on
- Make the program "viral" across the offices
  - Relevant materials were seen everywhere

DDOS?
ANSWER CORRECTLY TO WIN A $10 AMAZON GIFT CARD
DDOS?
ANSWER CORRECTLY TO WIN A $10 AMAZON GIFT CARD

We mean everywhere!



31 SECURITY TIPS FOR DEVELOPERS

SEE HOW #APPSECAWARE YOU ARE

Implement two-factor authorization wherever possible and logical.

#1 MOBILE SECURITY

Involve the security team in your feedback loop, offering your feedback and requesting theirs on the current state of security in your builds.

#1 AGILE SECURITY

Take advantage of online games and 'vulnerable' sites designed to be hacked to test your AppSec knowledge and improve your skills.

#1 EDUCATION

Limit application permissions only to components required for the app to function properly.

#2 MOBILE SECURITY

Integrate security processes as early as possible in your build process to cut back on time spent fixing issues later.

#2 AGILE SECURITY

Dive into the OWASP Top 10 and learn all you can about the 10 most dangerous vulnerabilities that should be prevented or fixed in code.

#2 EDUCATION

Never trust user input - All user input should be considered 'evil' until validated otherwise.

#1 TOP TIP

Perform threat modeling before testing to tell you where to focus your testing.

#2 TOP TIP

Implement SSL or TLS and ensure HTTPS is used.

#3 MOBILE SECURITY

Teach the security team about how your team writes code, so they can better understand how and where security can be integrated.

#3 AGILE SECURITY

Find yourself interested and excited about AppSec? Volunteer as a security evangelist and help teach other developers.

#3 EDUCATION

Consider storing business logic code on the server side.

#3 TOP TIP

Use a layered approach to security testing to dramatically cut down on security issues before deployment.

#4 TOP TIP

Invalidate user sessions upon logout or after a certain length of time.

#4 MOBILE SECURITY

Establish a shared discipline of agile development between the developer, operations, and security - throughout the SDLC.

#4 AGILE SECURITY

Develop a work relationship with a member of the security team who you feel comfortable asking security questions and answering coding questions.

#4 EDUCATION

Use generic error messages like "Incorrect username or password" to keep brute force attacks at bay. Never tell the user what the wrong data was.

#5 TOP TIP

Consider breaking the build for medium and high risk findings and never ship with potentially dangerous vulnerabilities.

#6 TOP TIP

Protect user interface data and user credentials by storing them properly using encryption.

#5 MOBILE SECURITY

Automate as much as possible - including security processes using tools that integrate with your own.

#5 AGILE SECURITY

Get involved in the threat modeling process to better understand the risks involved in application design and development.

#5 EDUCATION

Using third-party code? Either run security tests on the code or consider a shared-responsibility surrounding ensuring code security.

#7 TOP TIP

Apply a hashing algorithm using salt to your user's passwords before storing them in your database.

#8 TOP TIP

Ensure your app meets all necessary regulatory and compliance requirements, especially for financial and health apps.

#6 MOBILE SECURITY

Push smaller releases more often to lower the overall risk posture of the applications.

#6 AGILE SECURITY

Learn how to use the security tools whether you get formal lessons or not – educating yourself in secure coding will take you further in your career!

#6 EDUCATION

Separate your apps dynamic content from your static content.

#9 TOP TIP

Test your code throughout the SDLC to save time and money in the long run.

#10 TOP TIP

Don't allow third party keyboard use for iOS apps when sensitive content is entered.

#7 MOBILE SECURITY

Analyze security practices and tools in your agile retrospectives and adapt accordingly.

#7 AGILE SECURITY

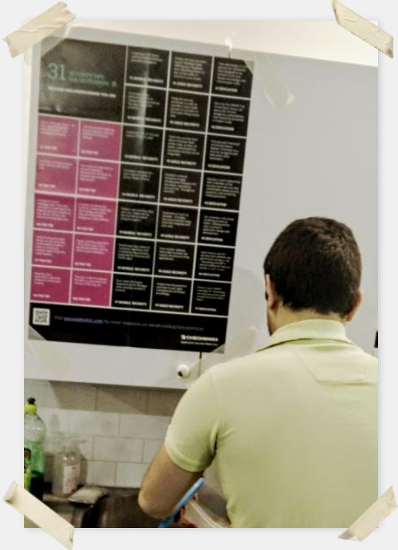
Head to local OWASP meetings for interesting security discussions (and usually free food and/or beer!)

#7 EDUCATION

Visit securedevkit.com for interesting content on secure development.

CHECKMARX

Application Security Made Easy

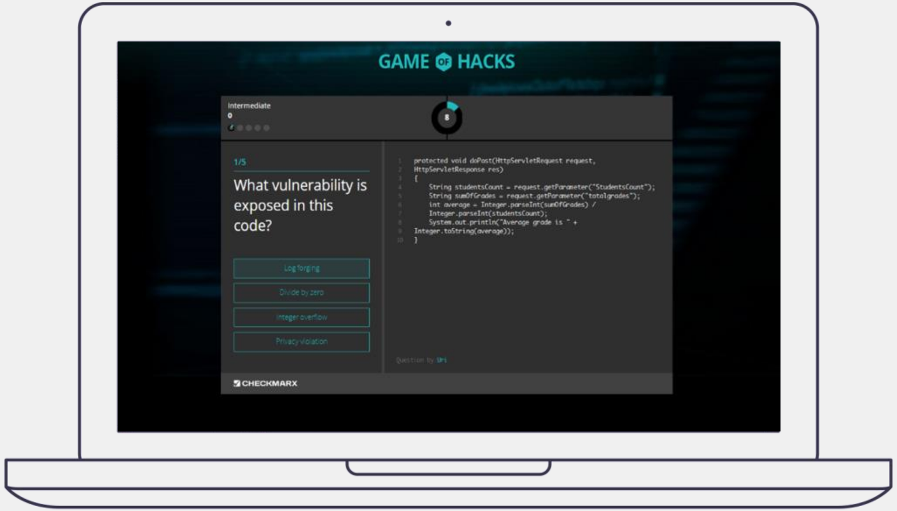


Office Kitchen

Everywhere!

Week 2 Education & Traction

- We started pushing relevant education materials
  - Introduction to secure coding Standards
  - Webinars
  - Reading materials
- Gamify the education to keep it interesting



GAME OF HACKS

Intermediate
0

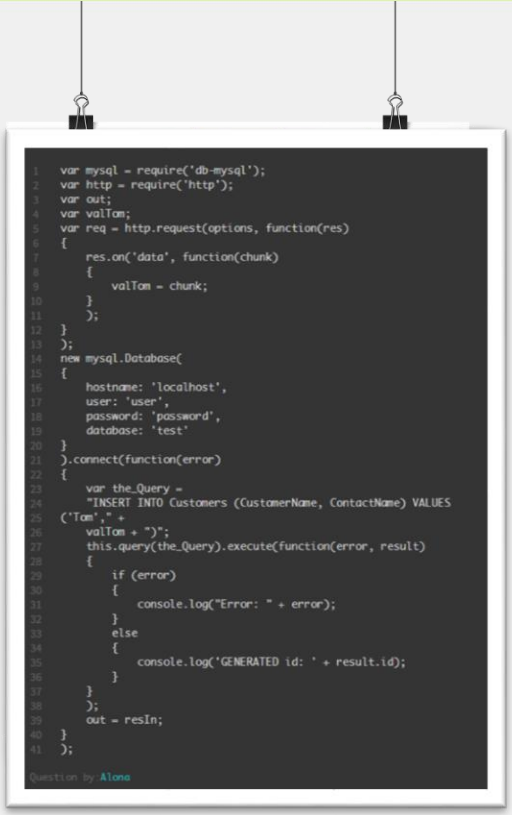
8

1/5

What vulnerability is exposed in this code?

```
protected void doPost(HttpServletRequest request,
HttpServletResponse res)
{
    String studentsCount = request.getParameter("StudentsCount");
    String sumOfGrades = request.getParameter("totalgrades");
    int average = Integer.parseInt(sumOfGrades) /
    Integer.parseInt(studentsCount);
    System.out.println("Average grade is " +
Integer.toString(average));
}
```

Week 3 Practice, Practice and more Practice



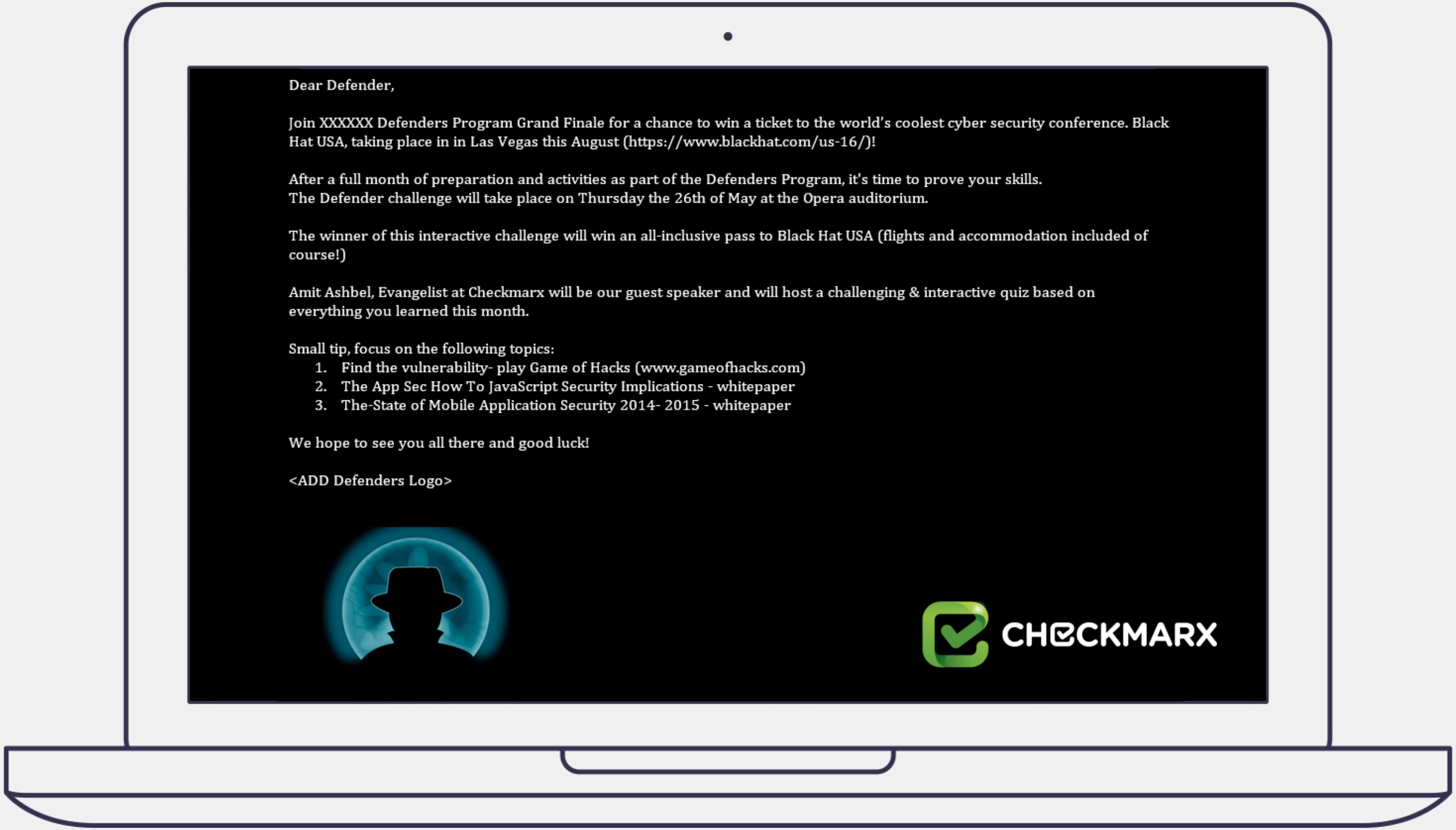
```
var mysql = require('db-mysql');
var http = require('http');
var out;
var valTom;
var req = http.request(options, function(res)
{
    res.on('data', function(chunk)
    {
        valTom = chunk;
    }
    );
}
);
new mysql.Database(
{
    hostname: 'localhost',
    user: 'user',
    password: 'password',
    database: 'test'
}
).connect(function(error)
{
    var the_Query =
    "INSERT INTO Customers (CustomerName, ContactName) VALUES
('Tom'," +
    valTom + ")";
    this.query(the_Query).execute(function(error, result)
    {
        if (error)
        {
            console.log("Error: " + error);
        }
        else
        {
            console.log('GENERATED id: ' + result.id);
        }
    }
    );
    out = resIn;
}
);
```

Question by: Alona

Spot the vulnerability!

- Public study materials
- Create healthy jealousy if there is such a thing
  - Give out something cool for competition winners!
- Announce the Grande Finale!
- Provide learning materials for preparations

Week 4 - The Grand Finale Challenge



Dear Defender,

Join XXXXXX Defenders Program Grand Finale for a chance to win a ticket to the world's coolest cyber security conference. Black Hat USA, taking place in in Las Vegas this August (https://www.blackhat.com/us-16/)!

After a full month of preparation and activities as part of the Defenders Program, it's time to prove your skills.
The Defender challenge will take place on Thursday the 26th of May at the Opera auditorium.

The winner of this interactive challenge will win an all-inclusive pass to Black Hat USA (flights and accommodation included of course!)

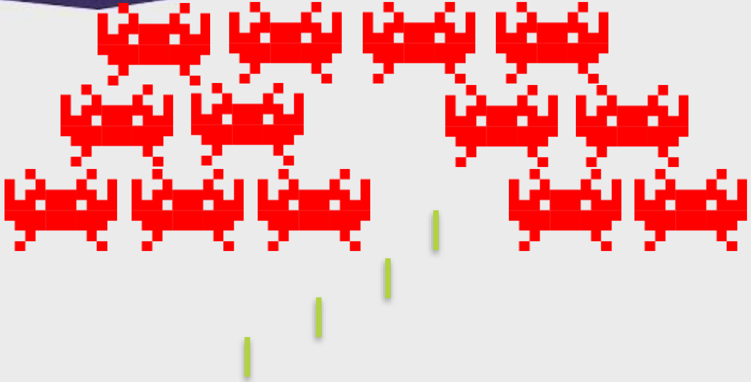
Amit Ashbel, Evangelist at Checkmarx will be our guest speaker and will host a challenging & interactive quiz based on everything you learned this month.

Small tip, focus on the following topics:

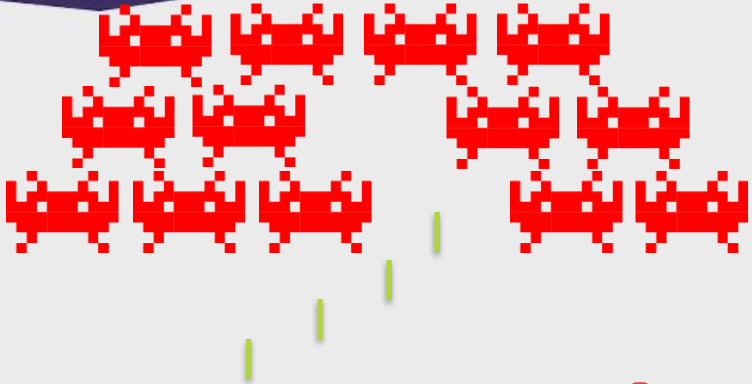
1. Find the vulnerability- play Game of Hacks (www.gameofhacks.com)
2. The App Sec How To JavaScript Security Implications - whitepaper
3. The-State of Mobile Application Security 2014- 2015 - whitepaper

We hope to see you all there and good luck!

<ADD Defenders Logo>



Let's try it out!



kahoot.it

Final Notes

Final Notes

- The Secure Dev kit is a kick start education tool
- This was an example how to implement an AppSec education program
- 400 organizations already kicked off their education program
- Gamification is key for success of any education program
- Checkmarx does not do this for a living, we Provide AppSec Solutions

Order a kit today

- https://www.securedevkit.com/

31 SECURITY TIPS FOR DEVELOPERS

Never trust user input - All user input should be considered 'evil' until validated otherwise.

#1 TOP TIP

Consider storing business logic code on the server side.

#3 TOP TIP

Perform threat modeling before testing to tell you where to focus your testing.

#2 TOP TIP

Use a layered approach to security testing to dramatically cut down on security issues before deployment.

#4 TOP TIP

Implement two-factor authentication wherever possible and logical.

#1 MOBILE SECURITY

Limit application permissions only to components required for the app to function properly.

#2 MOBILE SECURITY

Implement TLS and ensure HTTPS is used.

#3 MOBILE SECURITY

Invalidate user sessions upon logout or after a certain length of time.

#4 MOBILE SECURITY

Involve your scrum defender in your feedback loop, offering your feedback and requesting theirs on the current state of security in your builds.

#1 AGILE SECURITY

Integrate security processes as early as possible in your build process to cut back on time spent fixing issues later.

#2 AGILE SECURITY

Teach the security team about how your team writes code, so they can better understand how and where security can be integrated.

#3 AGILE SECURITY

Establish a shared discipline of agile development between the developer, operations, and security - throughout the SDLC.

#4 AGILE SECURITY

Take advantage of online games and 'vulnerable' sites designed to be hacked to test your AppSec knowledge and improve your skills.

#1 EDUCATION

Dive into the OWASP Top 10 and learn all you can about the 10 most dangerous vulnerabilities that should be prevented or fixed in code.

#2 EDUCATION

Find yourself interested and excited about AppSec? Volunteer as a security scrum defender and help teach other developers.

#3 EDUCATION

Develop a work relationship with a member of the security team who you feel comfortable asking security questions and answering coding questions.

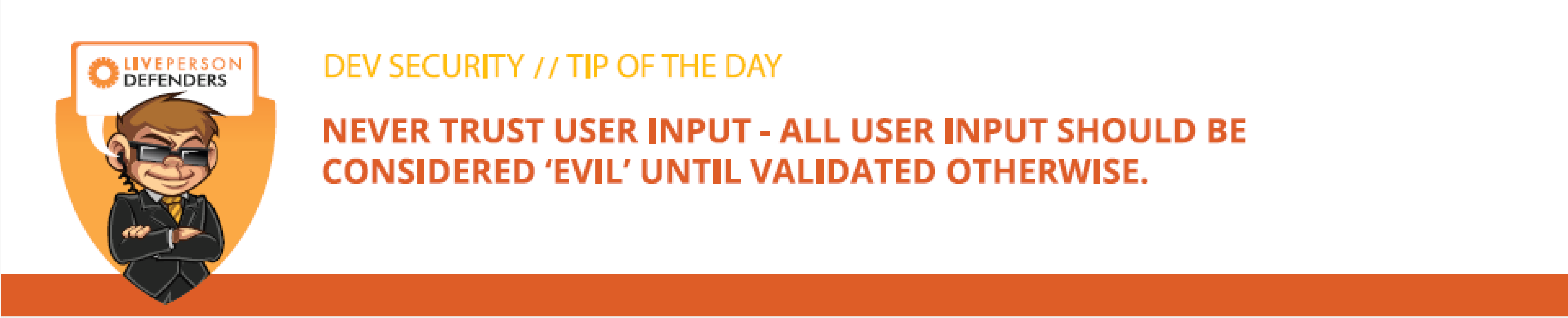
#4 EDUCATION

Tips

LIVEPERSON
DEFENDERS

AGILE DEV SECURITY // TIP OF THE DAY

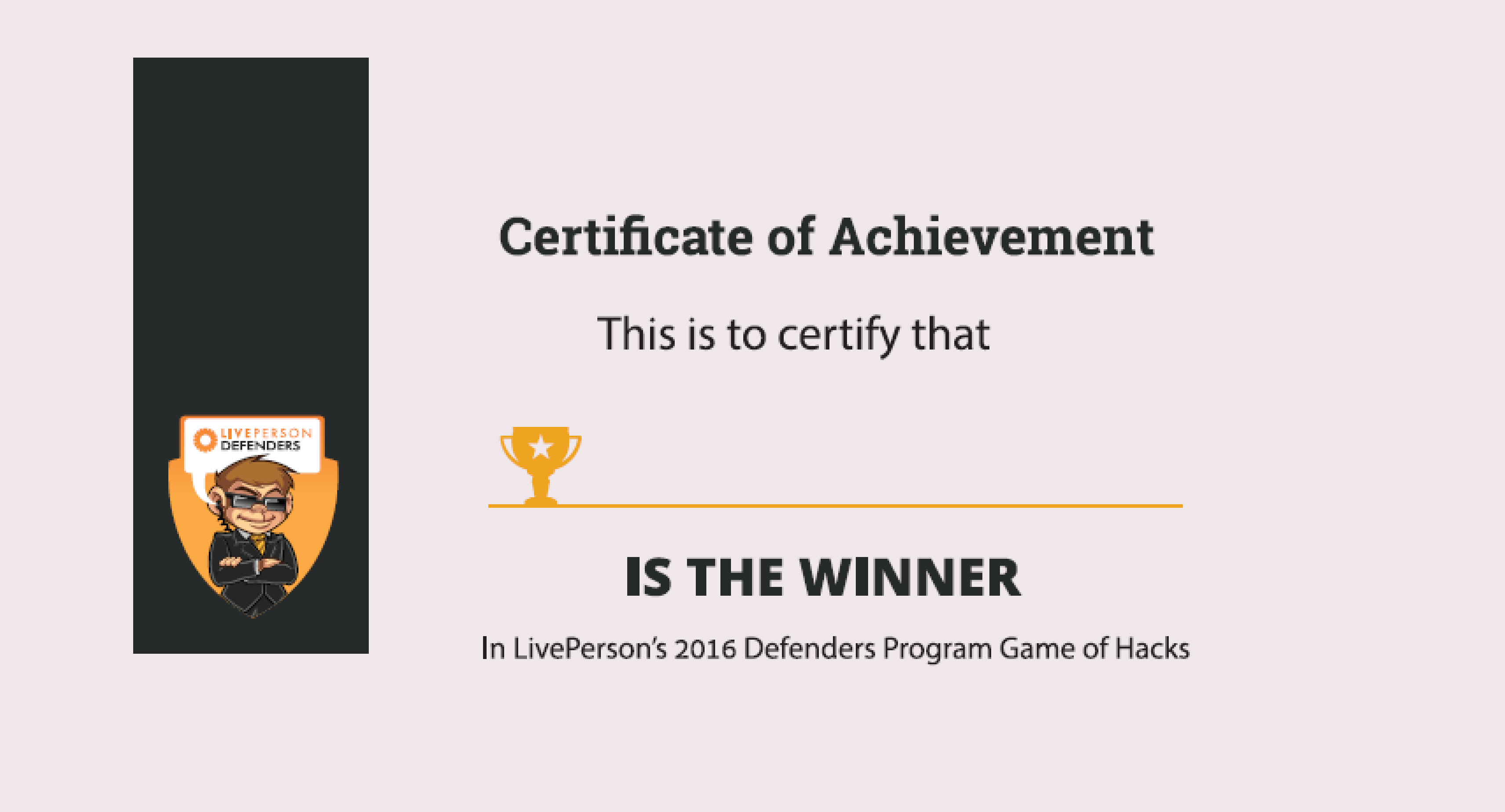
PUSH SMALLER RELEASES MORE OFTEN TO LOWER THE OVERALL RISK POSTURE OF THE APPLICATIONS.



DEV SECURITY // TIP OF THE DAY

NEVER TRUST USER INPUT - ALL USER INPUT SHOULD BE CONSIDERED ‘EVIL’ UNTIL VALIDATED OTHERWISE.

Certificates



LIVEPERSON
DEFENDERS

Certificate of Achievement

This is to certify that

IS THE WINNER

In LivePerson's 2016 Defenders Program Game of Hacks

Prizes !

THANK YOU

Andrew.thompson@Checkmarx.com