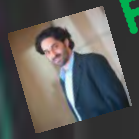
GAME OF HACKS

What vulnerability the following code contains?



Amit Ashbel
Product Marketing Manager

www.gameofhacks.com

About me

- What I am not?
  - Formally Educated
  - Developer
  - Hacker
- What I am?
  - Interested

CHECKMARX

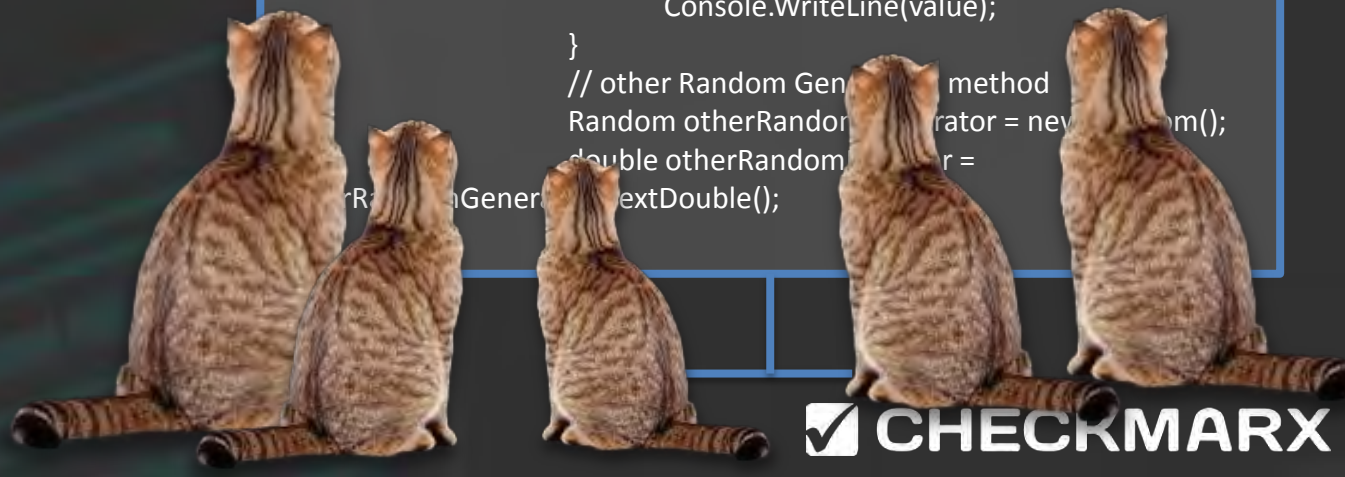
How I am about to spend your time?

- What is GoH?
- What's behind it?
- Not so wet T-Shirt contest
- Node.js potential risks
- Takeaways

Game of Hacks – An idea is born

```
using System;
using System.Security.Cryptography;
class Program
{
        static void Main()
        {
                using (RNGCryptoServiceProvider rng = new
RNGCryptoServiceProvider())
                {
                        // Buffer storage.
                        byte[] data = new byte[4];
                        // Ten iterations.
                        for (int i = 0; i < 10; i++)
                        {
                                // Fill buffer.
                                rng.GetBytes(data);
                                // Convert to int 32.
                                int value = BitConverter.ToInt32(data, 0);
                                Console.WriteLine(value);
                        }
                        // other Random Gen[illegible] method
                        Random otherRandom[illegible]rator = new[illegible]m();
                        double otherRandom[illegible]r =
[illegible]rRa[illegible]nGener[illegible]extDouble();
```

Spot The Vulnerability



CHECKMARX

CISO Concerns – Education and Awareness

Top 5 CISO Priorities

1. Security awareness and training for developers
2. Secure development lifecycle processes (e.g., secure coding, QA process)
3. Security testing of applications (dynamic analysis, runtime observation)
4. Application layer vulnerability management technologies and processes
5. Code review (static analysis of source code to find security defects)



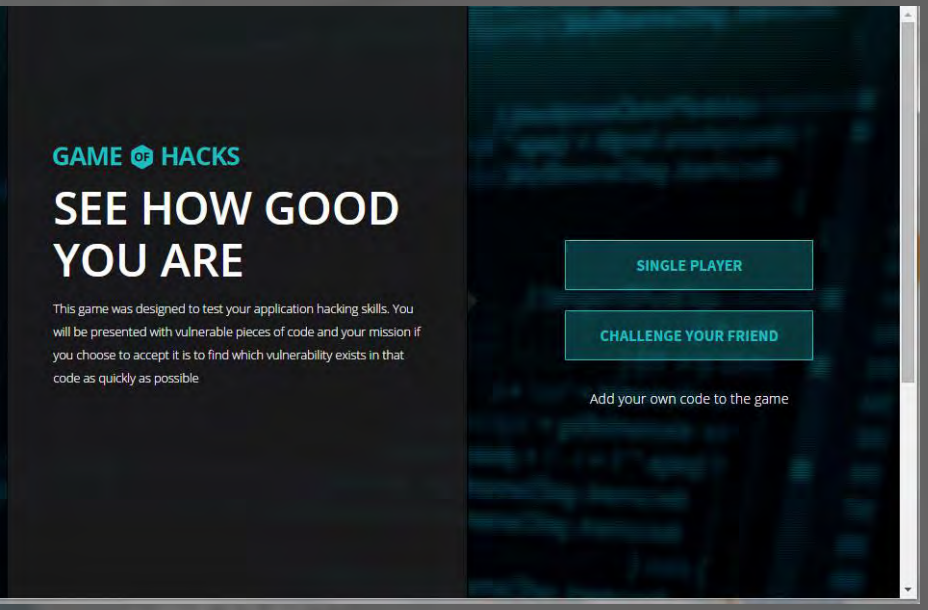
Top 5 CISO Challenges to effectively delivering your organization's application security initiatives

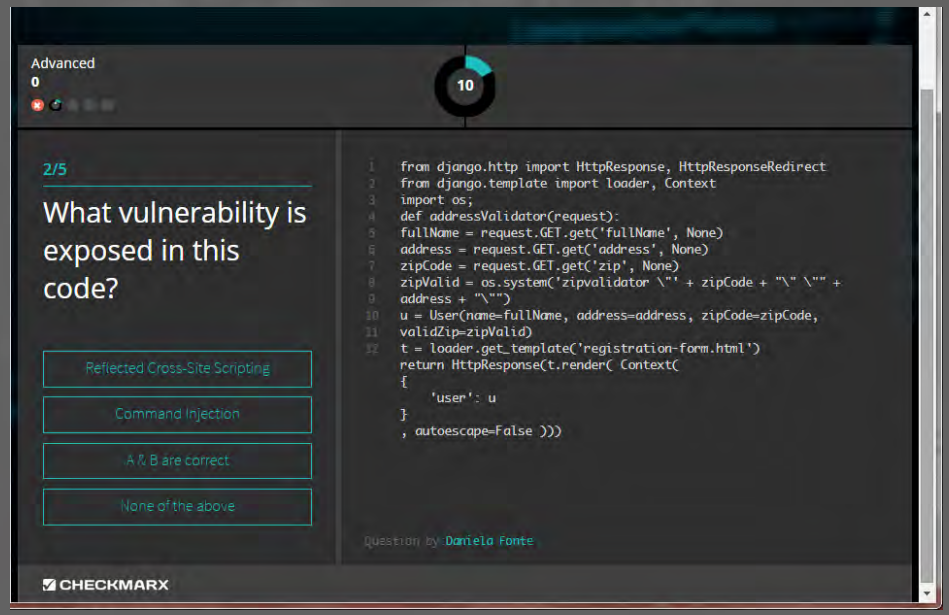
1. Availability of skilled resources
2. Level of security awareness by the developers
3. Management awareness and sponsorship
4. Adequate budget
5. Organizational change

(https://www.owasp.org/images/2/28/Owasp-ciso-report-2013-1.0.pdf



1+1=?





Launched on August

More than 100,000 games were played since

GAME OF HACKS

CHECKMARX

What was behind GoH?



CHECKMARX

Honeypot

▲ ZirconCode 203 days ago

The best part of this game is the leaderboard:

7e+177 - maplesyrupguy

1e+73 - Game itself was harder than to hack it

1.3999999999999998e+26 - I learned at least one thing...

1.555555682012021e+24 - Tries to teach security, fails at security.

1.4e+22 - jon

1e+22 - idiots

123456789212345710000 - Ironically it's easy to hack a game about finding security bugs!

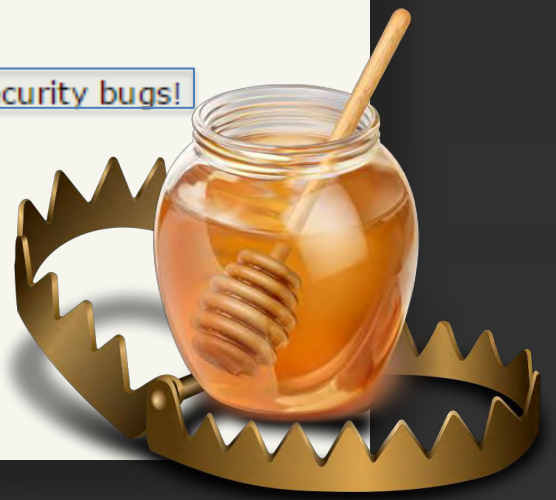
100100000000000000000 - did i do

70000000000000130000 - alex

28000000000000251000 - frankwins

▲ kybernetyk 202 days ago

Maybe that was the meta game.



- We assumed the game would be attacked
- We might as well learn from it
- Vulnerabilities were left exposed and patched along the way

CHECKMARX

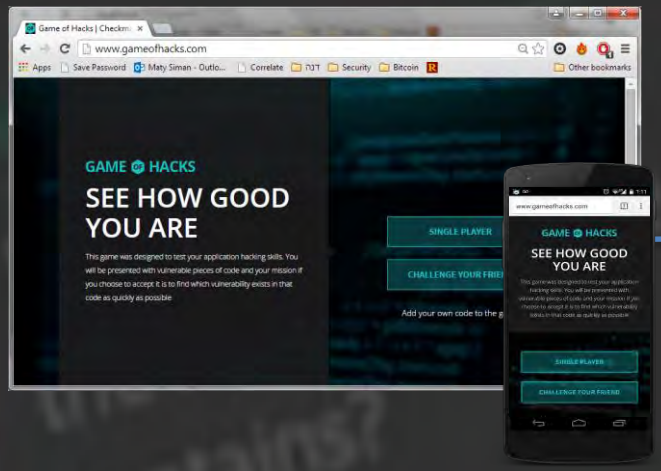
Let’s take a look at the game



CHECKMARX

GoH Architecture

Client



Server

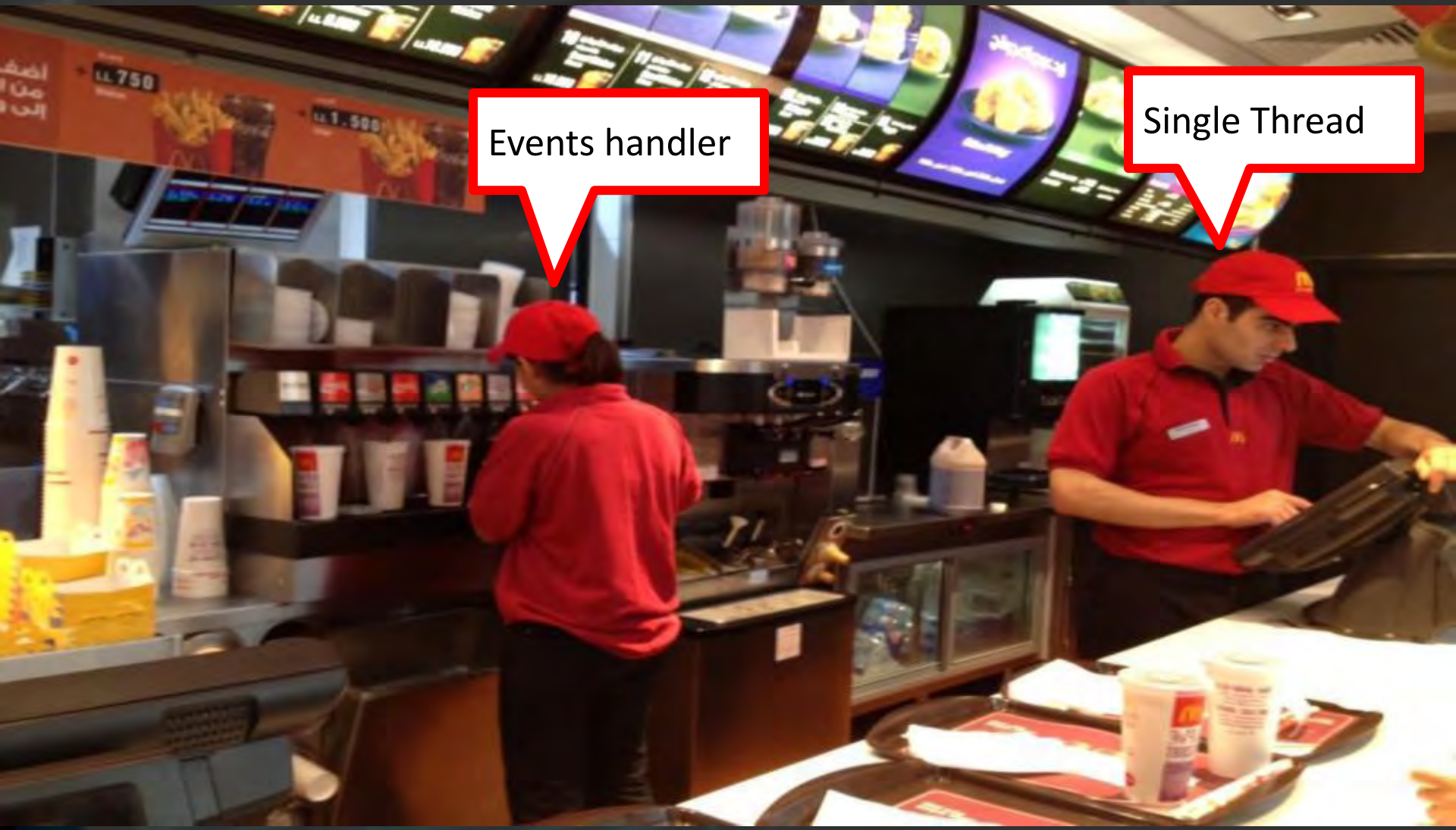
heroku

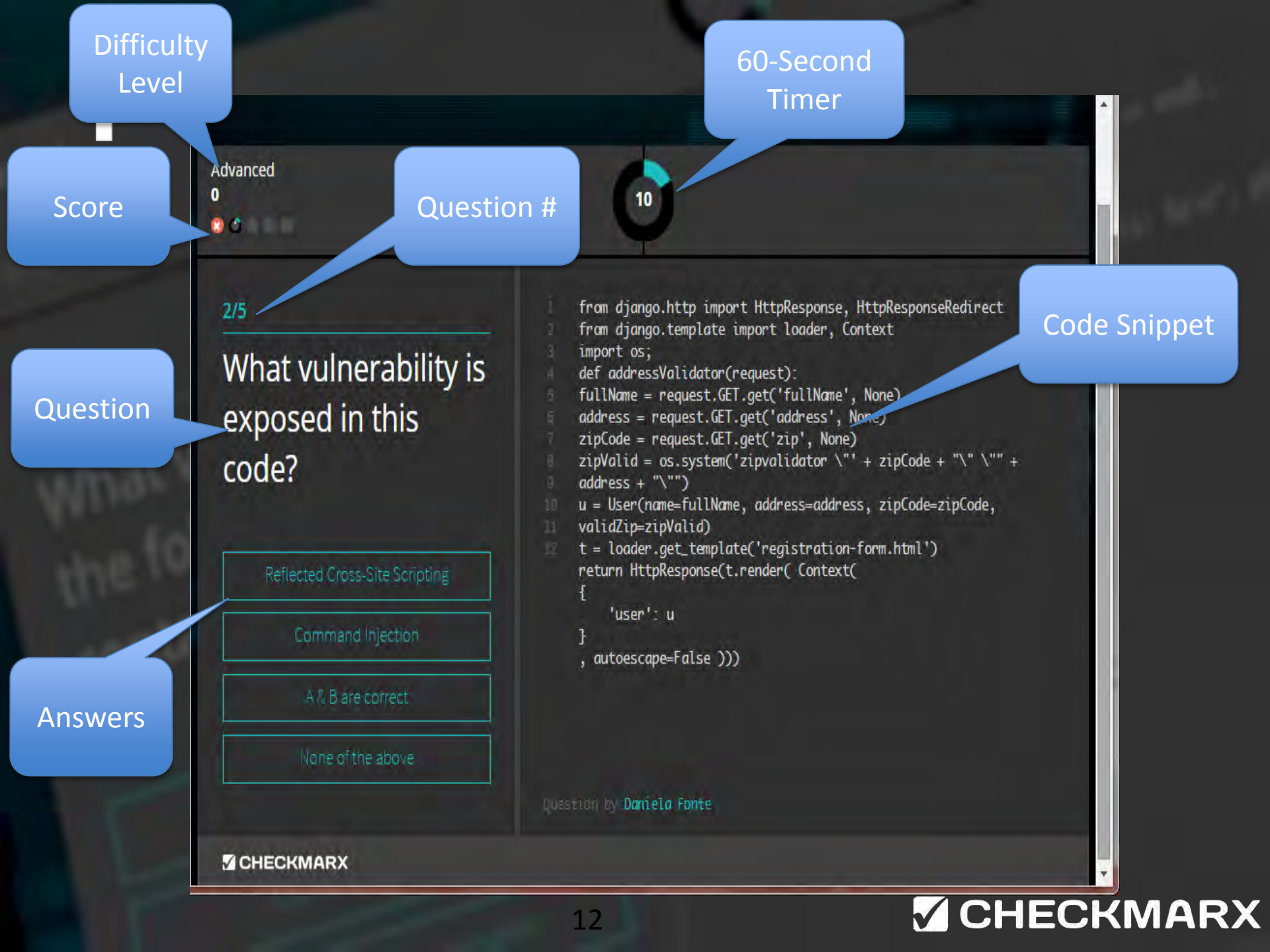
node.js

GAME OF HACKS

mongoDB.

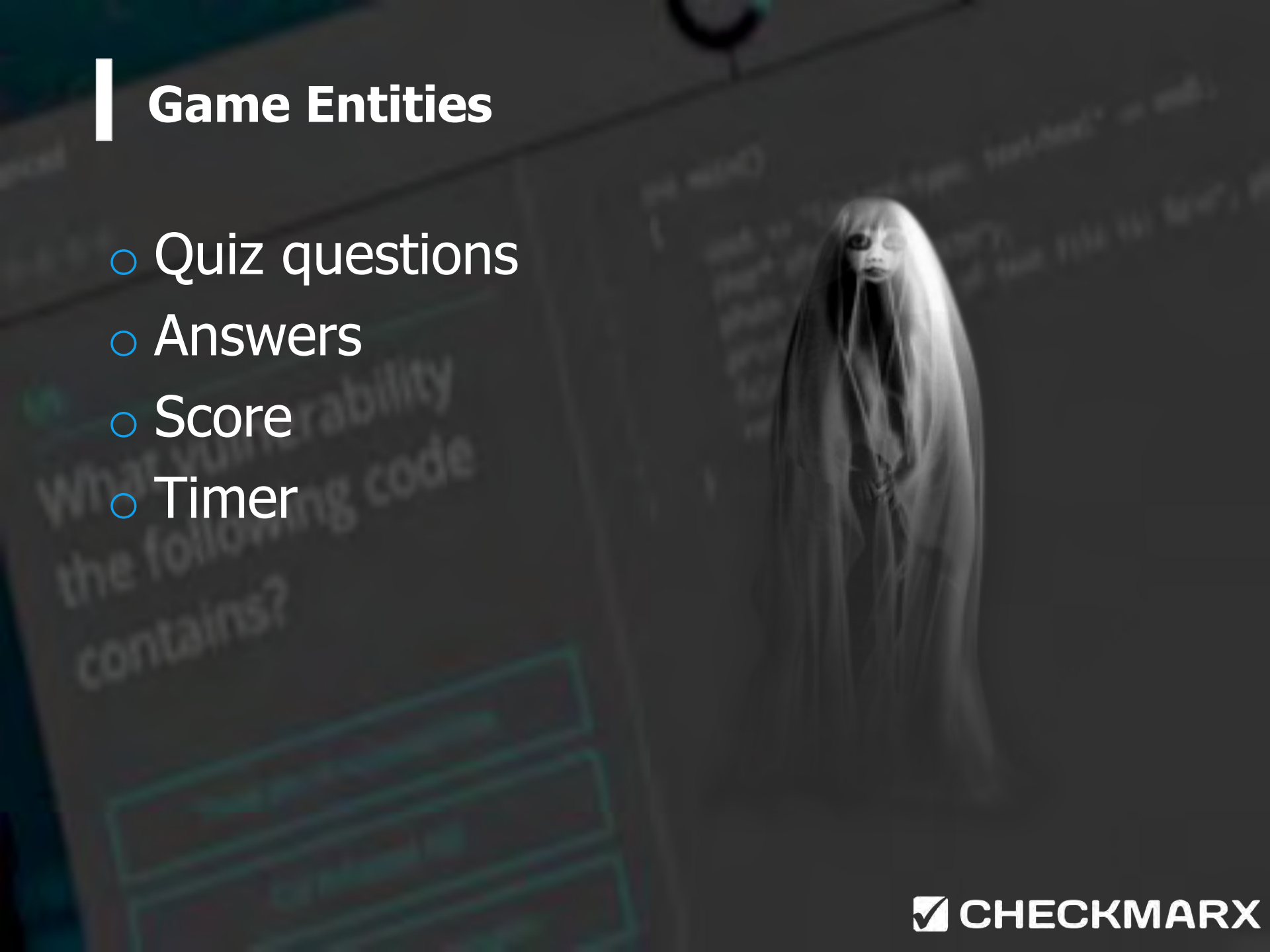
Event Driven




Difficulty Level
Score
Question #
60-Second Timer
Code Snippet
Question
Answers
Advanced
0
10
2/5
What vulnerability is exposed in this code?
Reflected Cross-Site Scripting
Command Injection
A & B are correct
None of the above
from django.http import HttpResponse, HttpResponseRedirect
from django.template import loader, Context
import os;
def addressValidator(request):
fullName = request.GET.get('fullName', None)
address = request.GET.get('address', None)
zipCode = request.GET.get('zip', None)
zipValid = os.system('zipvalidator \"' + zipCode + "\" \"" +
address + "\"")
u = User(name=fullName, address=address, zipCode=zipCode,
validZip=zipValid)
t = loader.get_template('registration-form.html')
return HttpResponse(t.render(Context(
{
'user': u
}
, autoescape=False)))
Question by Daniela Fonte
CHECKMARX

Game Entities

- Quiz questions
- Answers
- Score
- Timer



CHECKMARX

Get your Browsers ready!

Checkmarx@Defcon 23
Turn your mobile devices ON!

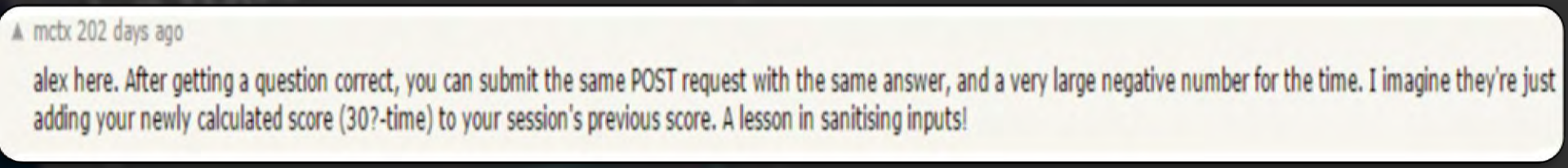
Go to: www.kahoot.it



CHECKMARX

Answered Question

- Initially users initiated app.sendAnswers multiple times, until they got "Correct answer" response.
- This allowed malicious users to systematically locate the correct answer – and to gain points over and over for the same question.



- Solutions
  - "Question Already Answered" flag added

CHECKMARX

Timer

- GoH Version 1
  - Timer handled by client
  - User forced to go to next question when time ends
  - Client sends to server Answer + Time spent
- So what?
  - Players stopped timer by modifying JS code

▲ granttimmerman 203 days ago

Here's how to hack the hacking game. Pretty simple (in your console):

app.sendAnswer({answer: 1,time: -999999999999})

(I added the instructions on the leaderboard itself)

▲ byerley 203 days ago

Somewhat ironic that the high scores have already been hacked, though a little inevitable since the game is client side I guess.



- GoH 2
  - Time is now computed at the server with minor traffic influence

Timer

- What else?

▲ Sonicmouse 203 days ago

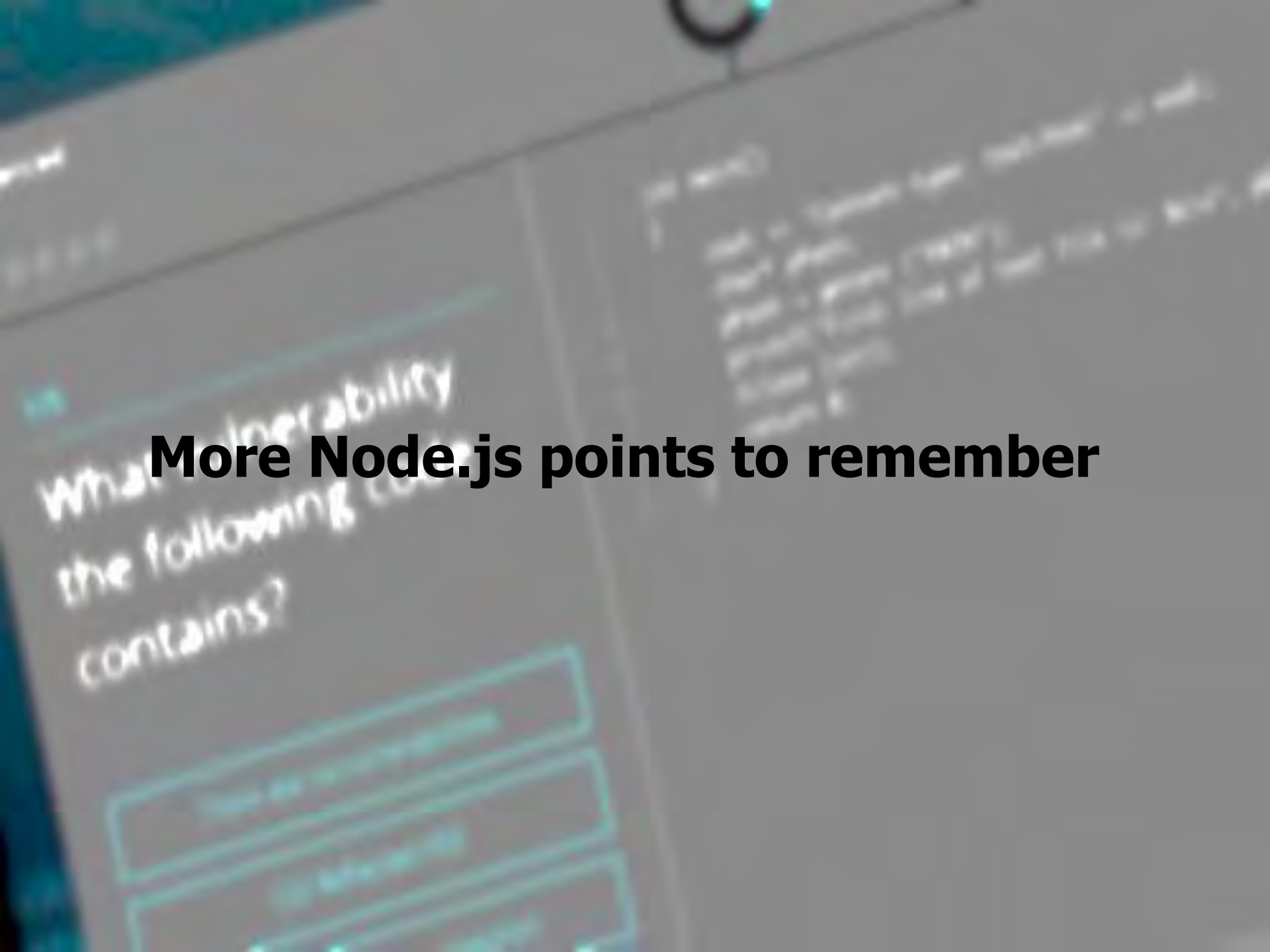
Play it on an iPhone. You can pause the timer by holding your finger on the iPhone's screen.

Yeah, it's cheating, but isn't that what it's all about?

▲ CaRDiaK 203 days ago

Hacking the hack!





More Node.js points to remember

Architecture and MongoDB

db.products.insert

Data is inserted and stored as JSON

```
db.products.insert( { item: "card", qty : 15 } )
db.products.insert( { name: “elephant", size: 1700 } )
```

db.products.find

```
db.products.find()                - Find all of them
db.products.find( { qty: 15 })      - Find based on equality
db.products.find( { qty: { $gt: 25 } } ) - Find based on criteria
```

Queries as described using JSON

```
var obj;
obj.qty=15;
db.products.find(obj)
```

Security – User Supplied Data

- Can you spot the vulnerabilities in the code?

```
SELECT * FROM users WHERE username = '$username' AND password = '$password'
```

- Fix:

```
name = req.query.username;
pass = req.query.password;
db.users.find({username: name, password: pass});
…
If exists ….
```

WRONG!

Security – User Supplied Data

```
name = req.query.username;
pass = req.query.password;
db.users.find({username: name, password: pass});
```

- What if we use the following query:

```
db.users.find({username: {$gt, “a”},
               password : {$gt, “a”}});
```

JSON-base SQL Injection

- Node.JS, being a JSON based language, can accept JSON values for the .find method:

```
db.users.find({username: username, password: password});
```

- A user can bypass it by sending

```
http:///server/page?user[$gt]=a&pass[$gt]=a
```

http://blog.websecurify.com/2014/08/hacking-nodejs-and-mongodb.html

DEMO

http://localhost:49090/?user=hi&pass=bye

JSON Based SQL Injection

- You can use the following:

```
db.users.find({username: username});
```

- Then

```
bcrypt.compare(candidatePassword, password, cb);
```

WRONG!

JSON Based SQLi

```
db.users.find({username: username});
```

- This can lead to Regular Expression Denial of Service through the {“username”: {“$regex”: “……..}}

Re-Dos Demo

*http://localhost:49090/?user=admin&pass[$regex]=^(a|a|a|

Some Key Takeaways

Gamification of education

- Knowledge is key to deliver secure code
- Students (of all ages) absorb and retain information better
- Anytime you have a chance to make learning a fun experience you should do it

Using code

- Always validate the input length, structure and permitted characters
- Each coding language has its own pitfalls
- Research and learn a language before you use it publicly.
- Remember - Node.js is highly sensitive to CPU-intensive tasks

Thank You

Questions?


amit.ashbel@checkmarx.com


Amit Ashbel


@aashbel

GAME OF HACKS

CHECKMARX