ROMA
MMXVI

APPSEC
EUROPE

Leveling up your AppSec program

Agenda

- Intro
- Riot AppSec
- Bug Bounty
- Automation

Intro

- Senior Security Engineer at Riot Games
- Owner of application security and bug bounty
- 10 years of application security experience
- Gamer (not a good one)

Riot Games

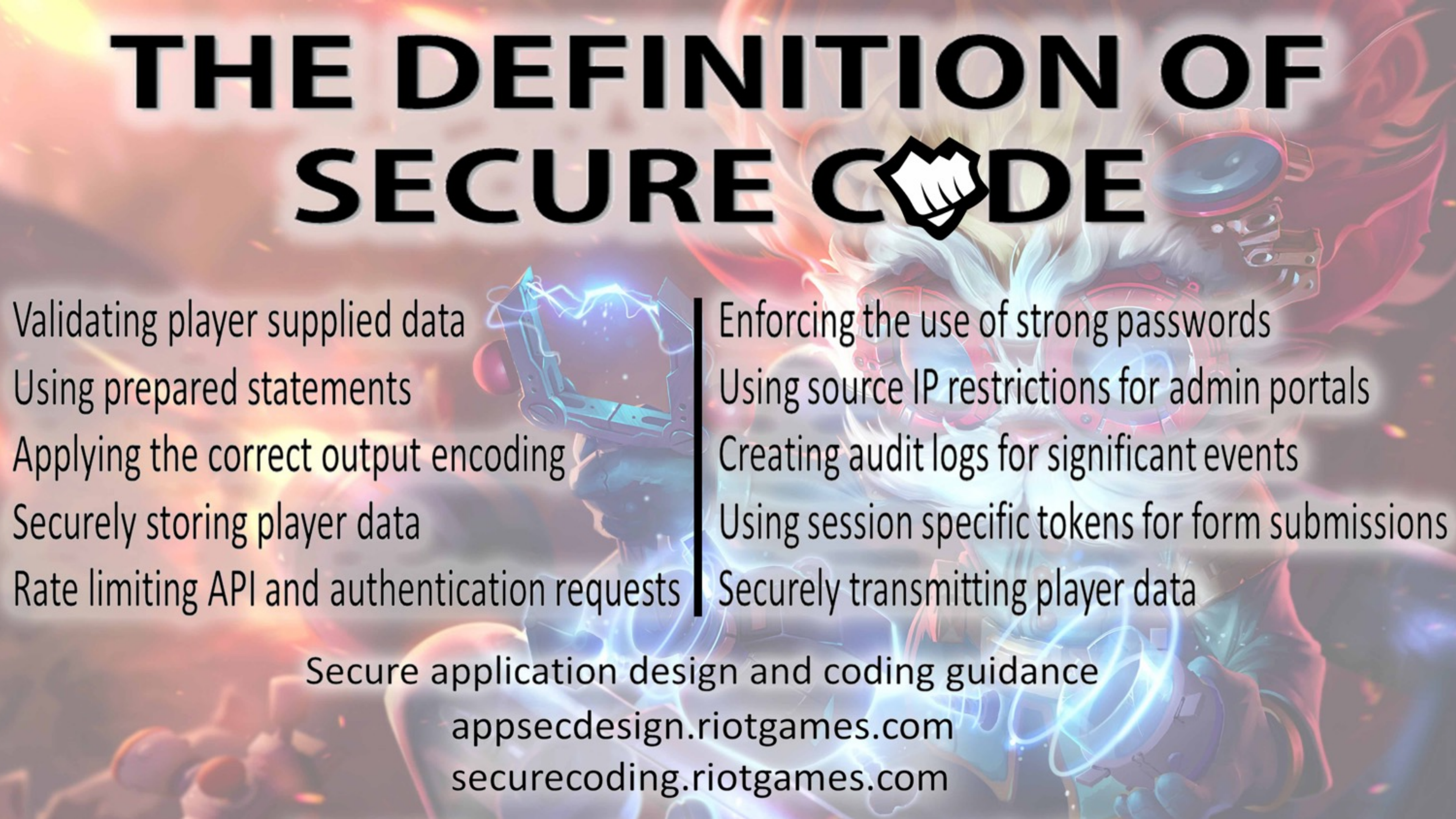
- Developer and publisher of League of Legends
- Focused on player experiences first
- Gamers who take play seriously

WORLDS 2015
LEGENDS TAKE ALL
SKT
KOO

Riot AppSec

We aim to arm every software engineer with the tools and knowledge they need to build safe and secure experiences for Players and Rioters

WORLDS 2015
LEGENDS TAKE ALL
BENGI
FAKER
BANG
WOLF
SMEB
HOJIN
KURO
PRAY



THE DEFINITION OF SECURE CODE

Validating player supplied data

Using prepared statements

Applying the correct output encoding

Securely storing player data

Rate limiting API and authentication requests

Enforcing the use of strong passwords

Using source IP restrictions for admin portals

Creating audit logs for significant events

Using session specific tokens for form submissions

Securely transmitting player data

Secure application design and coding guidance

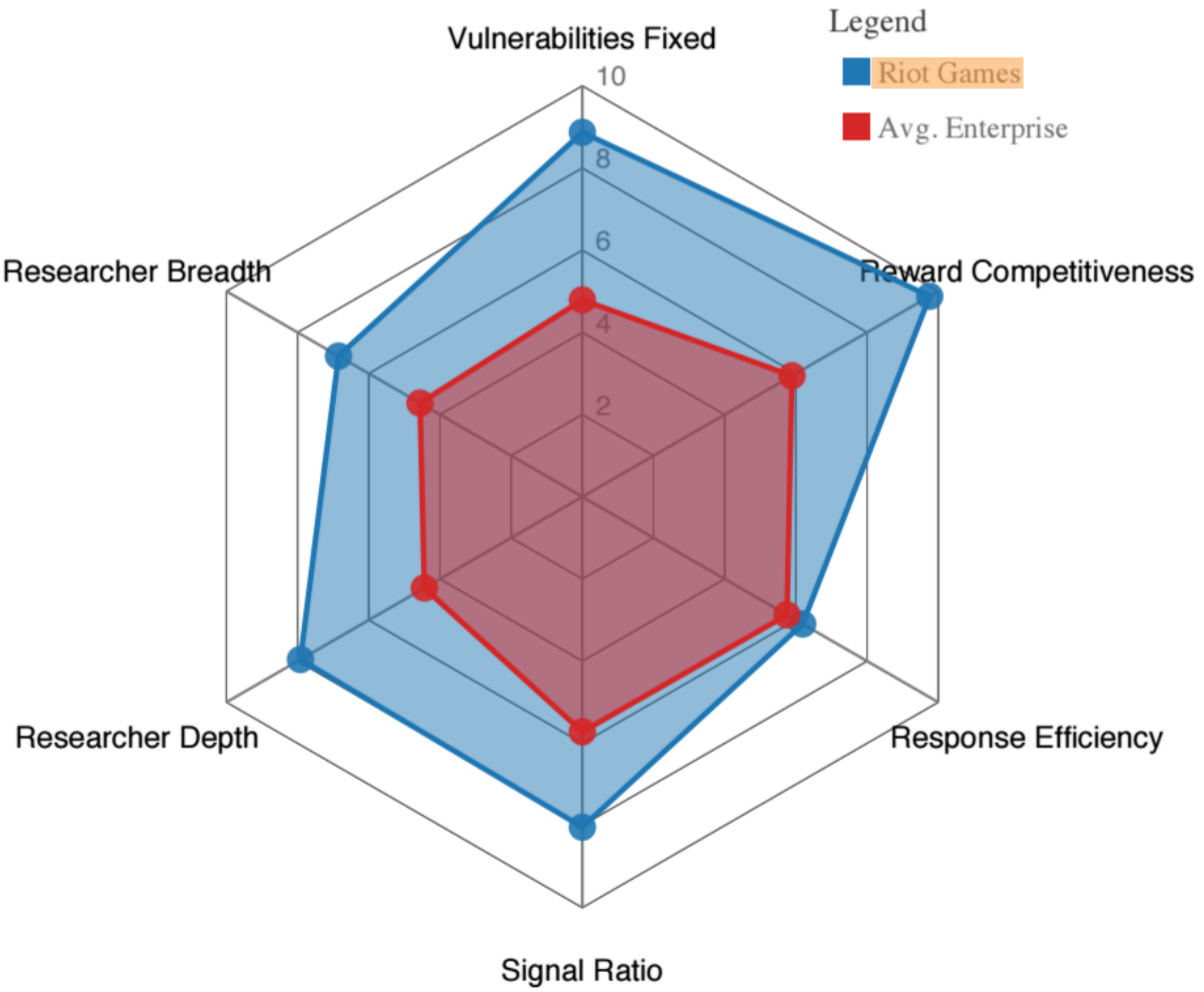
appsecdesign.riotgames.com

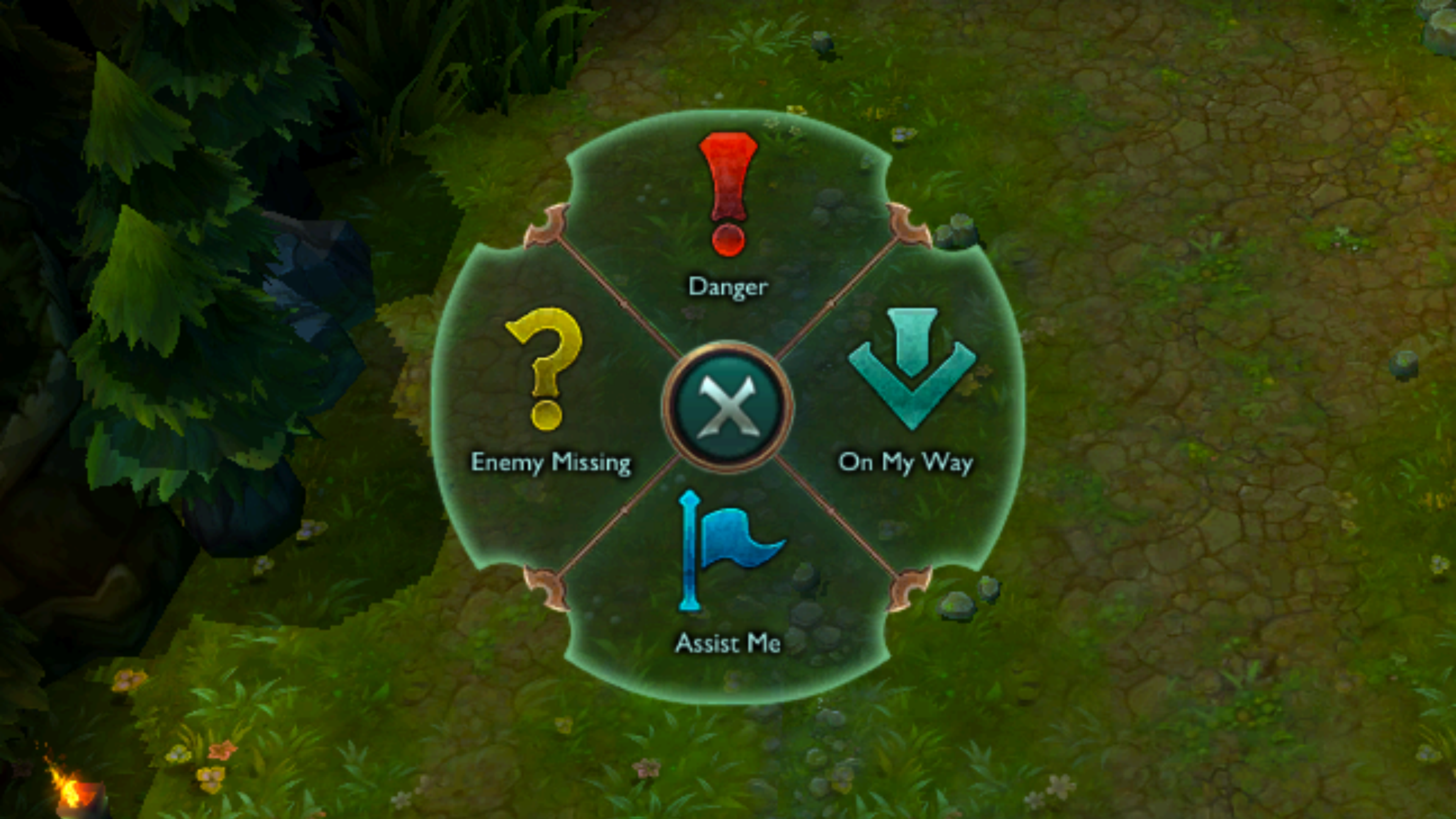
securecoding.riotgames.com

GG
GG

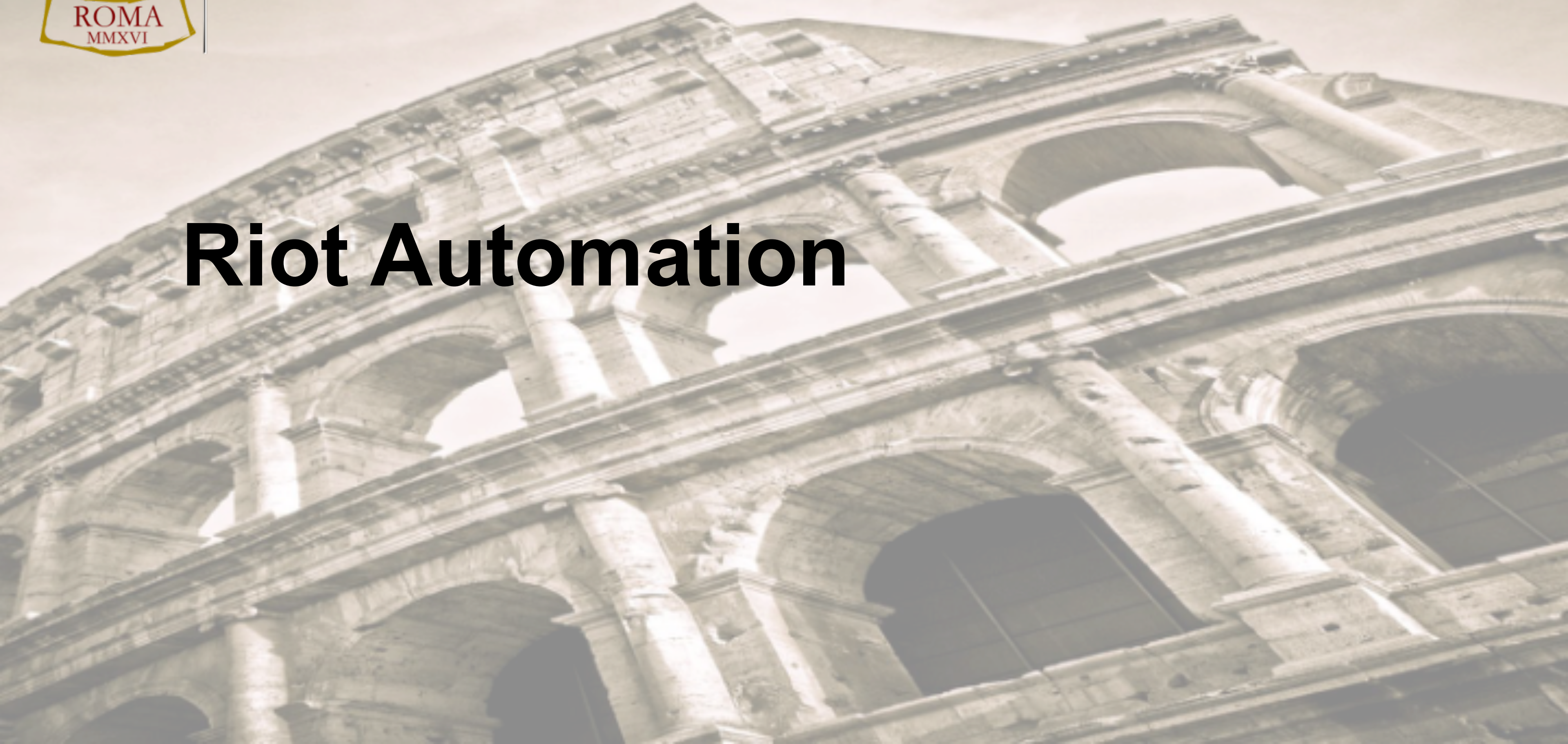
SHAN
龙珠直播
SK telecom
T1
宅米
FILA
KLEVV
F

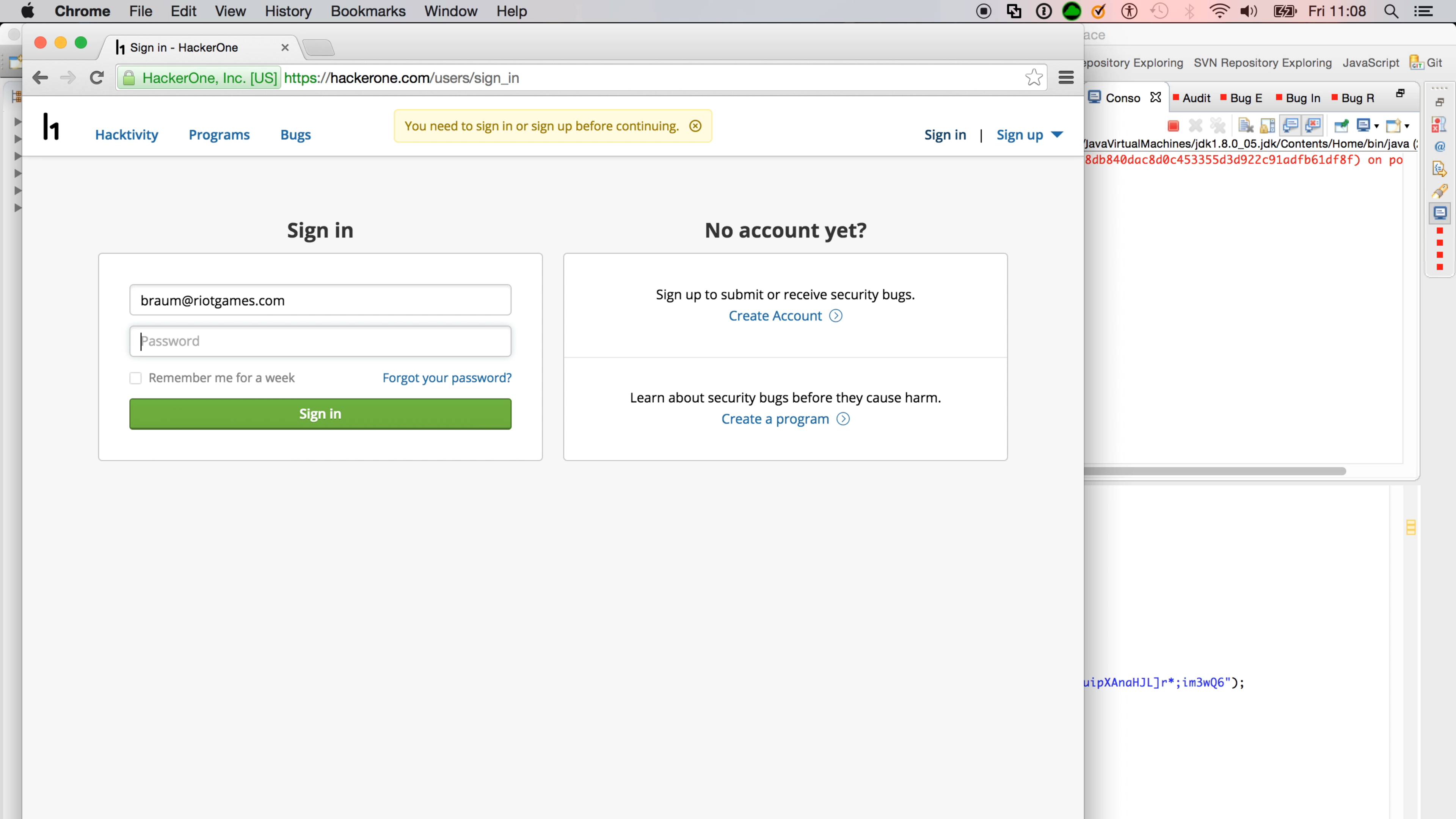
Riot Bug Bounty


Vulnerabilities Fixed
Reward Competitiveness
Response Efficiency
Signal Ratio
Researcher Depth
Researcher Breadth
10
8
6
4
2
Legend
🟦 Riot Games
🟥 Avg. Enterprise


Danger
Enemy Missing
On My Way
Assist Me

Riot Automation





https://hackerone.com/users/sign_in

You need to sign in or sign up before continuing.

Sign in

braum@riotgames.com

Password

□ Remember me for a week

Forgot your password?

No account yet?

Sign up to submit or receive security bugs.

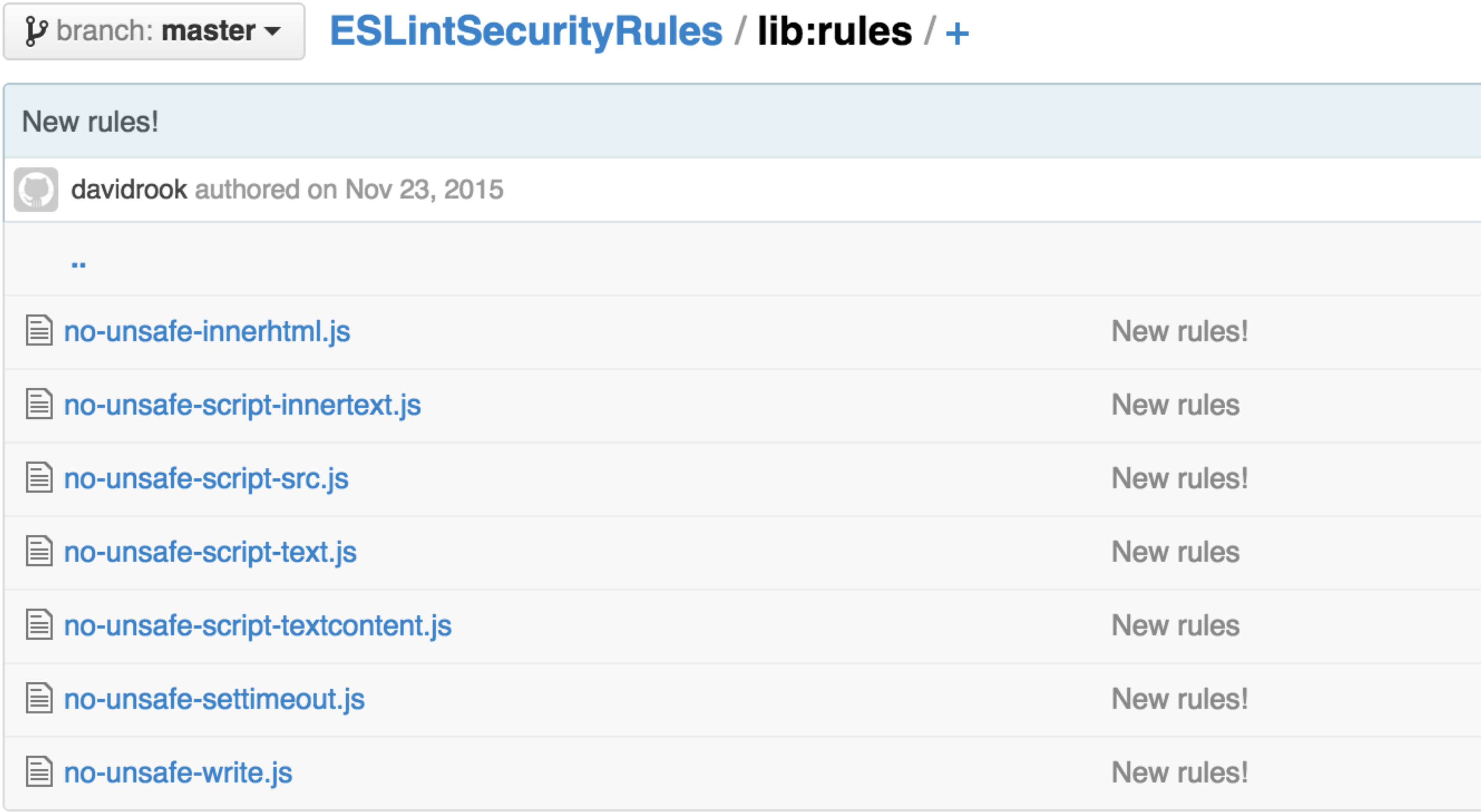
Create Account

Learn about security bugs before they cause harm.

Create a program

```
/JavaVirtualMachines/jdk1.8.0_05.jdk/Contents/Home/bin/java (
8db840dac8d0c453355d3d922c91adfb61df8f) on po
```

```
uipXAnaHJL]r*;im3wQ6");
```

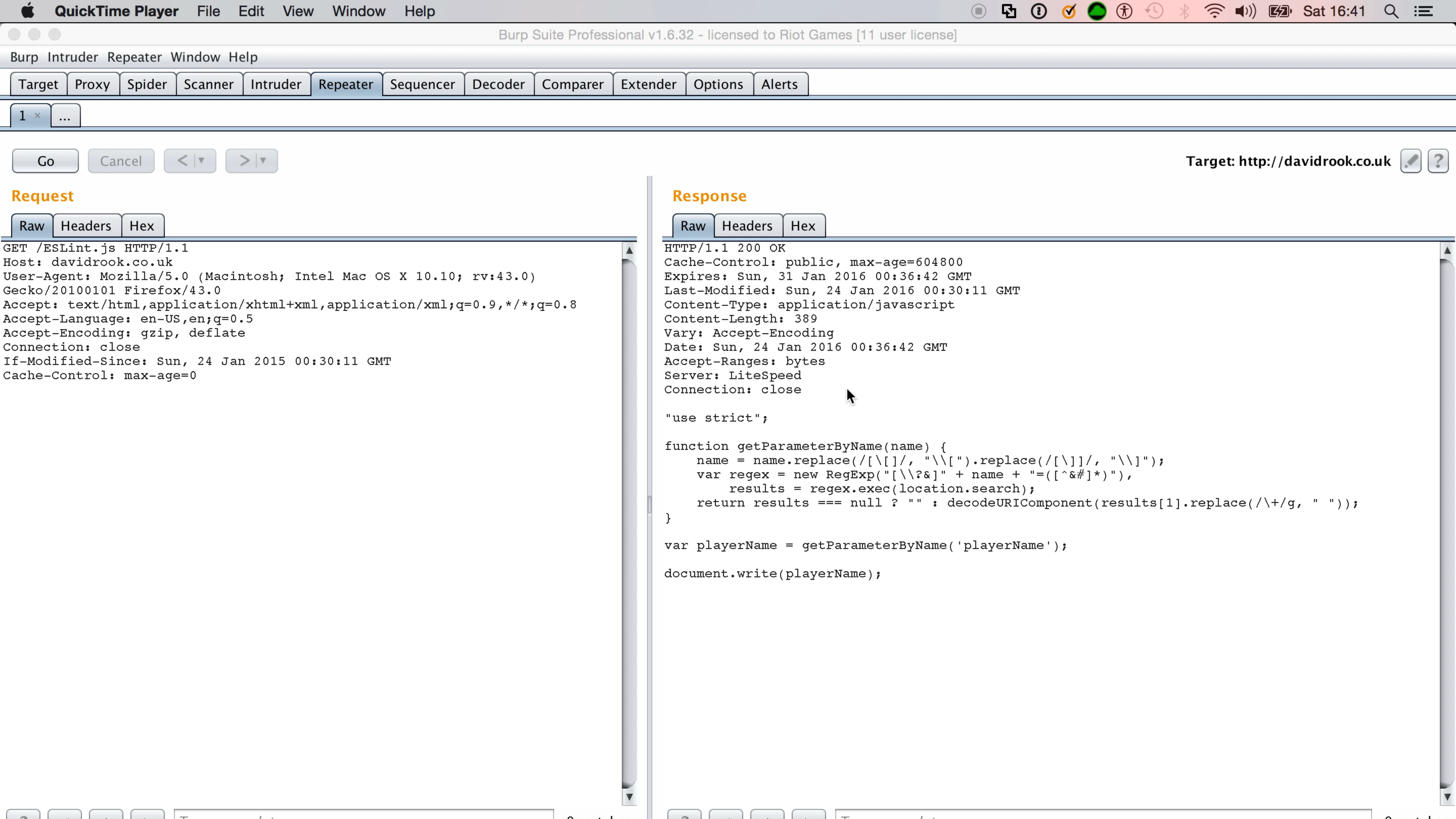


New rules!

davidrook authored on Nov 23, 2015

..

no-unsafe-innerhtml.js	New rules!
no-unsafe-script-innertext.js	New rules
no-unsafe-script-src.js	New rules!
no-unsafe-script-text.js	New rules
no-unsafe-script-textcontent.js	New rules
no-unsafe-settimeout.js	New rules!
no-unsafe-write.js	New rules!



Request

```
GET /ESLint.js HTTP/1.1
Host: davidrook.co.uk
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:43.0)
Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
If-Modified-Since: Sun, 24 Jan 2015 00:30:11 GMT
Cache-Control: max-age=0
```

Response

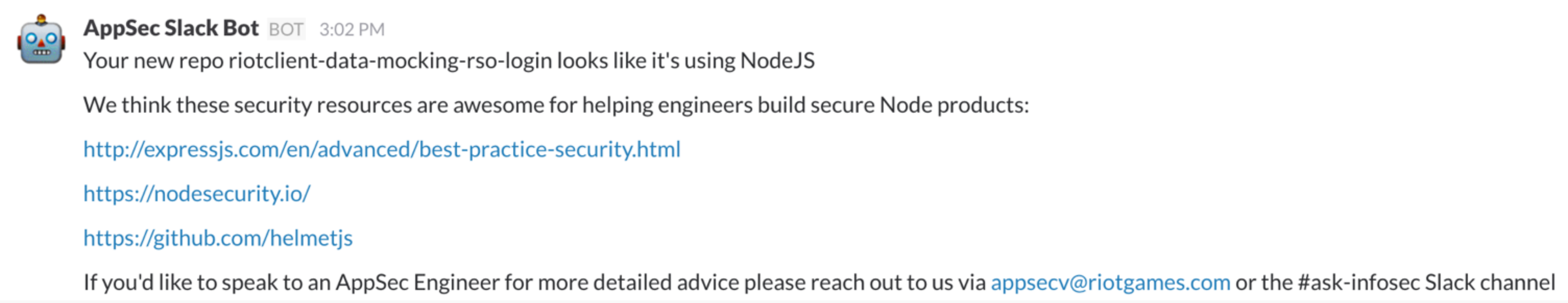
```
HTTP/1.1 200 OK
Cache-Control: public, max-age=604800
Expires: Sun, 31 Jan 2016 00:36:42 GMT
Last-Modified: Sun, 24 Jan 2016 00:30:11 GMT
Content-Type: application/javascript
Content-Length: 389
Vary: Accept-Encoding
Date: Sun, 24 Jan 2016 00:36:42 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

"use strict";

function getParameterByName(name) {
    name = name.replace(/[\[]/, "\\[").replace(/[\]]/, "\\]");
    var regex = new RegExp("[\\?&]" + name + "=([^&#]*)"),
        results = regex.exec(location.search);
    return results === null ? "" : decodeURIComponent(results[1].replace(/\+/g, " "));
}

var playerName = getParameterByName('playerName');

document.write(playerName);
```



AppSec Slack Bot BOT 3:02 PM

Your new repo riotclient-data-mocking-rso-login looks like it's using NodeJS

We think these security resources are awesome for helping engineers build secure Node products:

http://expressjs.com/en/advanced/best-practice-security.html

https://nodesecurity.io/

https://github.com/helmetjs

If you'd like to speak to an AppSec Engineer for more detailed advice please reach out to us via appsecv@riotgames.com or the #ask-infosec Slack channel

ROMA MMXVI | APPSEC EUROPE

Questions?

@davidrook