

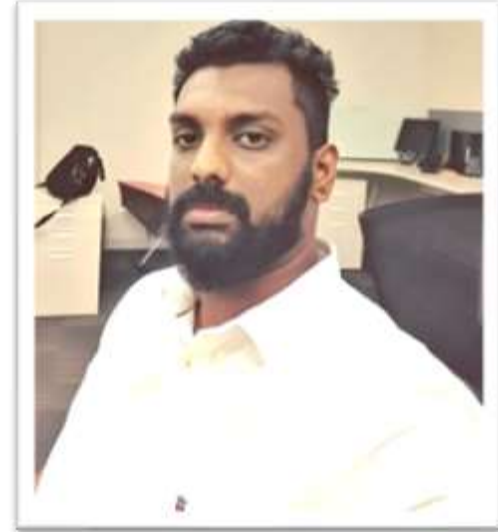
Automating Web Application Security Testing Using Hubot Artificial Intelligence Chat Bot

Abhijith B R / @abhijithbr
Thoufeeque N S / @thoufeequens

#BsidesDelhi2017

:~\$ whoami

- Abhijith B R
- **Sr. Security analyst at EY**
- **Traveller and Blogger**



I do blog : <https://abhijith.live>

Twitter : **@abhijithbr**

:~\$ whoami

- Thoufeeque N S
- Security analyst at EY
- Breaking applications for a living
- Love to play with radio devices
- Licensed ham radio operator



Twitter : **@thoufeequens**

groot@hubot:~\$ Significance of Automation and AI

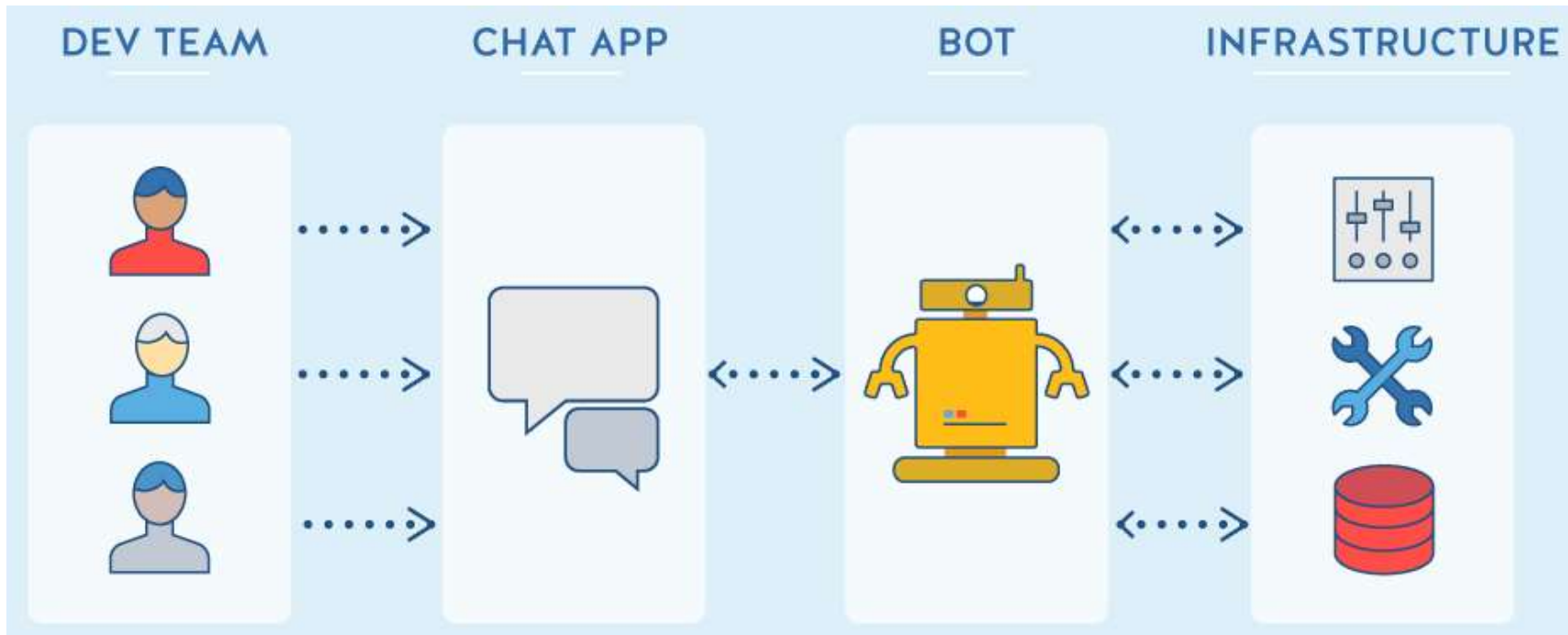
- **This is the age of Automation, Artificial Intelligence and Machine learning.**
- **Even the most sophisticated tasks are being automated.**
- **Robotic process automation and NLP / AI based technologies are emerging in the technology world**
- **Corporates finds it as a solution to cost cutting and as a smart way of working**
- **AI is an area of interest all the time! We can say that Cognitive Artificial Intelligence is very far from reality**
- **Big corporations are all behind AI technologies, to make the world a better place**
- **Lets hope so!**

groot@hubot:~\$ Chat Bots? The history!

- **ELIZA bot**
- **Created on 1966 at MIT AI laboratory**
- **Used pattern matching and substitution methodology**
- **A.L.I.C.E bot**
- **Artificial Linguistic Internet Computer Entity**
- **Uses AIML (Artificial Intelligence Markup Language)**
- **New generation chat bots**
- **Quite powerful, uses machine learning and powerful AI algorithms**

groot@hubot:~\$ ChatOps, DevOps and SecOps

Essentially it can be defined as,
Including tools and services within the conversation itself!



groot@hubot:~\$ ChatOps, DevOps and SecOps

Some popular names in the ChatOps industry



Why can't we use ChatOps for Security testing?

- **Command vs Natural language**
- **Project team/Dev team does not need to know the complex testing scenarios**
- **More productivity**
- **Use Multiple API services (Scanners, other security services) from different vendors**
- **A virtual assistant only for security or penetration testing;**
- **We can treat this bot as a person with huge amount of knowledge about information security;**

groot@hubot:~\$ Benefits

- **The same infosec chat bot can be helpful for both security testers and project/development teams**
- **Helps the security testers to save time and concentrate more on other important stuff**
- **It helps the Project/developer teams with the security policies, remediation plans etc**

Automation of web application security testing:

Mostly the boring tasks!

What to automate?

How to automate?

Why do we have to automate?

groot@hubot:~\$ What to automate?

- **Pen-testing as a profession, we will have to repeat a lot of boring tasks in daily basis.**
- **Automation of complex corporate security policies and rules**
- **So just automate the most boring and repetitive tasks**
- **Sometimes it takes a lot of time to answer the queries of Project teams and developers**
- **Most of the queries will be about the secure development policies or how to fix previously found vulnerabilities**
- **Why can't be automate this?**
- **Automation of pen-testing and other manual tasks**

groot@hubot:~\$ How to automate?

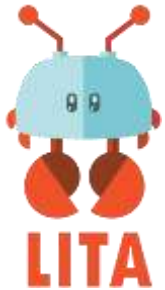
- **Automation scripts or methodologies in various languages**
- **API for cyber security services**
- **Write custom automation scripts for manual testing**
- **Finally link all of these to the NLP/AI chat bot**

groot@hubot:~\$ Why do we have to automate?

- **It saves time and improves productivity.**
- **If we can automate something, why should we waste time to do it manually every time?**

groot@hubot:~\$ Finding the best bot for our purpose

- We've looked for a few bots which can actually do “stuff”
- Some of them are as follows



COG bot



`groot@hubot:~$` What exactly is Hubot?

- After the comparison we decided to go with Hubot
- An open source Chat bot made by GitHub
- It was used in GitHub company chat room to automate things
- Hubot comes with a small set of core scripts
- Written using CoffeeScript on Nodejs
- Easily deployable to wide set of platforms such as Slack, Heroku etc



HUBOT

Commissioned by [GitHub](#)

groot@hubot:~\$ Advantages of using Hubot with Rocket chat

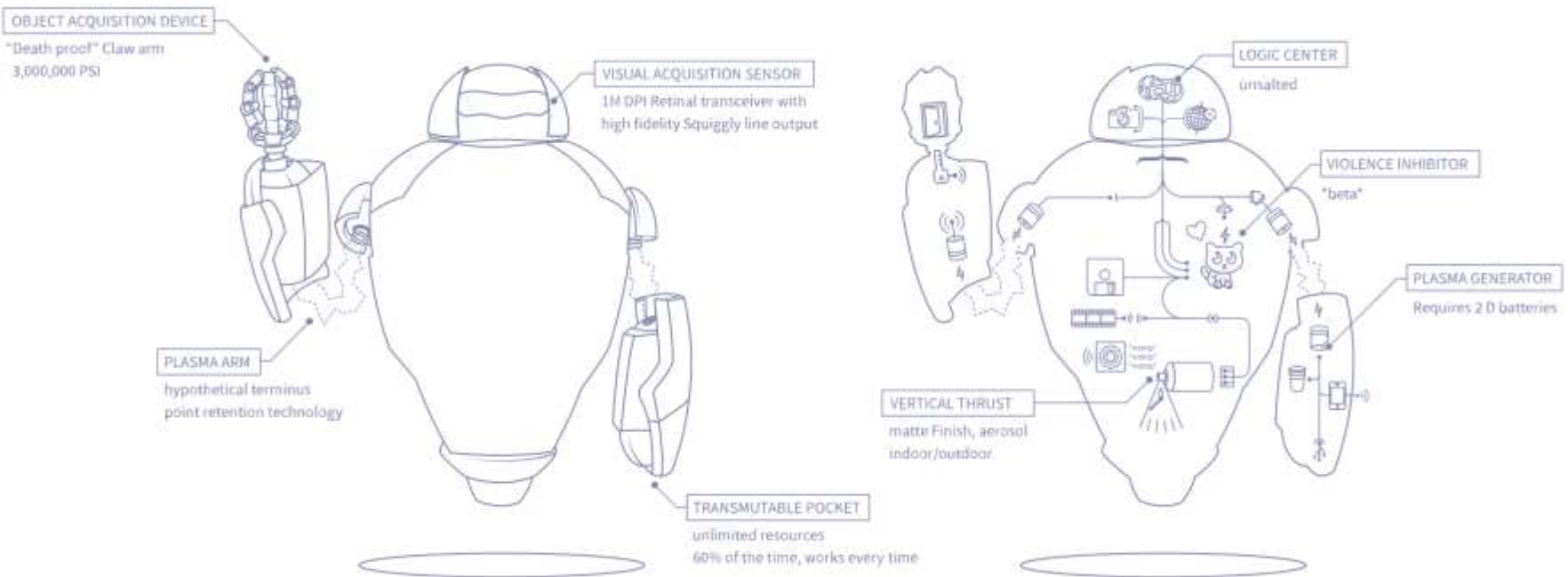
- **Open source and ultimately free**
- **User permissions and roles can be set for both Hubot and Rocket chat**
- **Sensitive command execution privileges can be limited based on users and roles**
- **Rocket chat web interface is lean and responsive**
- **Rocket chat supports AD authentication**
- **Which makes it perfect for internal use**
- **Highly Extensible**
- **We can access internal chat servers using VPN**



`groot@hubot:~$` Recipe for the perfect bot



groot@hubot:~\$ Let's start building our bot



`groot@hubot:~$` Scraping the existing Hubot scripts

- Where to look :
- [Github.com/hubot-scripts](https://github.com/hubot-scripts)
- NPM – `hubot-scripts`
- Digg deep enough – Because, we are damn lazy to write all required scripts from the scratch
- A great collection of hubot-scripts are already out there for information security
- We can just use it or modify it as per our requirements



Keep digging till you find it

groot@hubot:~\$ Creating new scripts for security testing

- **CoffeeScript can be used to create new scripts to increase the functionality of our bot**
- **We wrote a few; rented a few**
- **Created a bunch of scripts to automate manual testing scenarios**

groot@hubot:~\$ Using Python and Bash scripts

- **Yes, we can integrate Python and Bash scripts into our chat bot**
- **Which means a wide variety of web security testing or automation scripts can be invoked using simple human like interaction**
- **Just imagine the possibilities**

We named our chat bot, Sheru!

Sheru is a dumb tiger in Malayalam comics, who obeys the commands of his friend – a tricky fox!

Let's hope our bot – 'Sheru' is much intelligent than the tiger!

It's Demo time!!

groot@hubot:~\$ What's next?

- **We tried to make our bot, talk Human!**
- **But, Integrating with Artificial Intelligence API services will make it much powerful**
- **Hubot will send every query to these API services before executing them**
- **Its not something which we need in a security testing bot**
- **Solution is to create an exception and send the unsolved queries by Hubot to online AI libraries**
- **It will not send sensitive queries to API services and helps the bot to obtain more Human like behaviour**

groot@hubot:~\$ What's next?

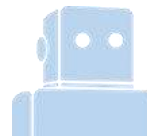
- AI / NLP API services

Natural Language API

4



Google Cloud Platform



wit.ai



api.ai

pandorabots API

groot@hubot:~\$ Security concerns

- **The chat bot server (Kali Linux) must use less privileged user accounts**
- **Please make sure, only a limited number of users have access to execute shell and other external scripts**
- **For internal use its better to use AD/LDAP authentication for chat room users**
- **If we are targeting developer teams as well, make sure they have only execute commands regarding policies; and cannot invoke any pentesting automation scripts**
- **Authentication, Authorization, Accounting**

SKY'S THE LIMIT!



Shoot your queries!



Thank you all!
Thank you #BsidesDelhi

References:

<https://hubot.github.com/>

<https://abhijith.live>

<https://nodejs.org>

<https://npmjs.com>

<https://rocket.chat>

<https://abhijith.live/infosec-bot-using-hubot/>

Thanks to our friend @boney for giving a hand with internal automation scripts

All image rights goes to respective owners