HONING YOUR CRAFT

IN 2019

7MS USER GROUP

JANUARY 14TH, 2019

7 MINUTE SECURITY

www.7ms.us

SOFT SKILLS FOR THE COMMON SECURITY PRO

- WHY DO SOFT SKILLS MATTER? I JUST WANT TO HACK!
  - YOUR WORK MEANS NOTHING IF YOU CAN'T CONVEY WHY IT MATTERS
  - NOT EVERYONE IS AS SMART AS YOU (MOST LIKELY…)
  - FIX IT OR WE ALL DIE
    - NOT AN EFFECTIVE ARGUMENT
    - NOT THE ANSWER (AT LEAST 97.5% OF THE TIME)

KNOW YOUR SURROUNDINGS

Ask the right questions

Understand the Risk

Collaborate for success

- Understand risks within business context
  - Will this affect our product?
  - Will this affect our ability to deliver our product?
  - Will this affect our customers?
  - Will this affect our employees?
- Same questions apply for consultants and their clients

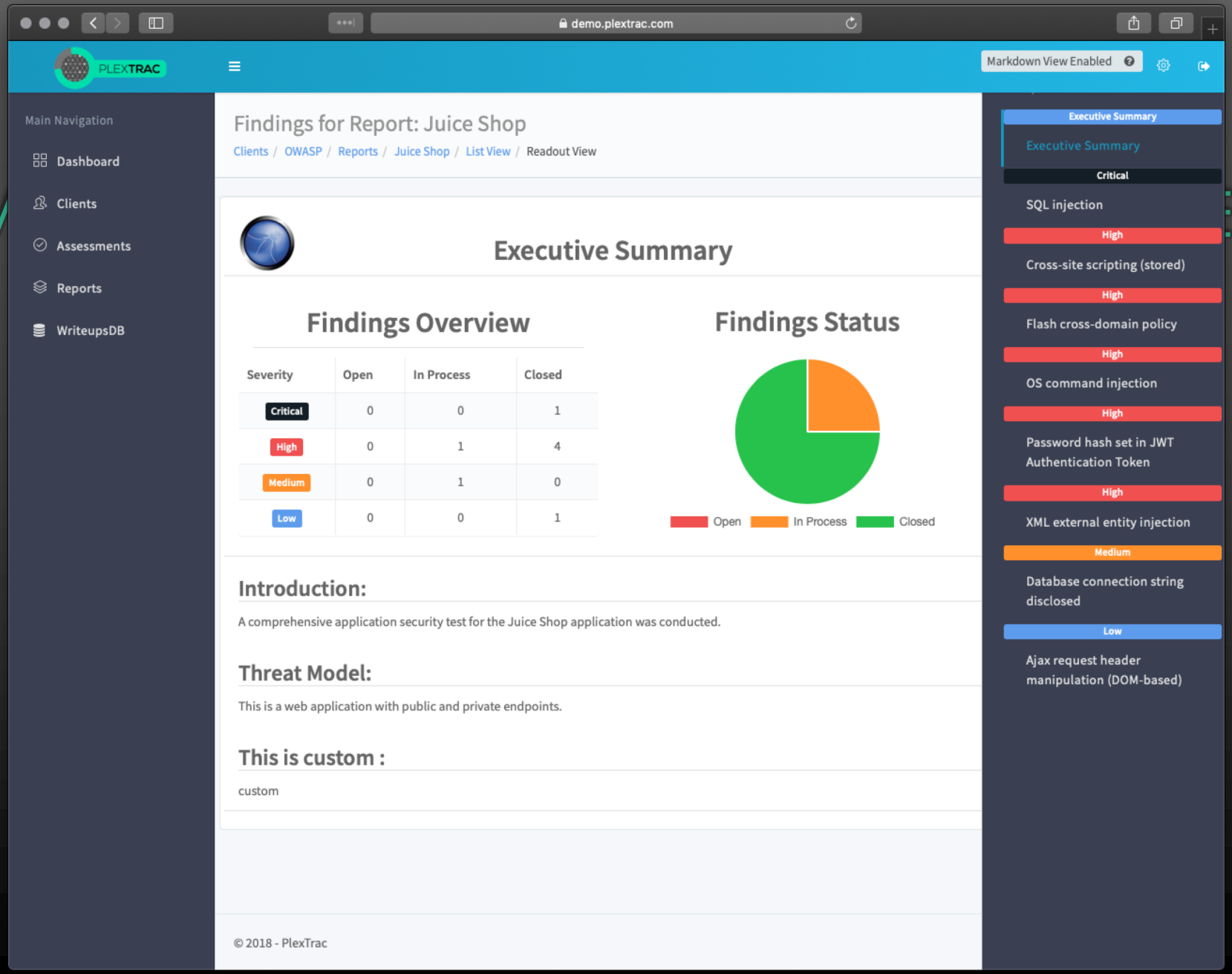
EXECUTE AND DELIVER

REPORTS == DELIVERABLE

MUST HAVE GOOD WRITING SKILLS

PRESENT WELL

BUT W EY?


demo.plextrac.com
PLEXTRAC
Markdown View Enabled
Main Navigation
Dashboard
Clients
Assessments
Reports
WriteupsDB
Findings for Report: Juice Shop
Clients / OWASP / Reports / Juice Shop / List View / Readout View
Executive Summary
Findings Overview
Severity | Open | In Process | Closed
Critical | 0 | 0 | 1
High | 0 | 1 | 4
Medium | 0 | 1 | 0
Low | 0 | 0 | 1
Findings Status
Open
In Process
Closed
Introduction:
A comprehensive application security test for the Juice Shop application was conducted.
Threat Model:
This is a web application with public and private endpoints.
This is custom :
custom
© 2018 - PlexTrac
Executive Summary
Executive Summary
Critical
SQL injection
High
Cross-site scripting (stored)
High
Flash cross-domain policy
High
OS command injection
High
Password hash set in JWT Authentication Token
High
XML external entity injection
Medium
Database connection string disclosed
Low
Ajax request header manipulation (DOM-based)

QUESTIONS

- DAN@PLEXTRAC.COM
- @PLEXTRACFTW
- HTTPS://PLEXTRAC.COM