Contrast Security Tech Workshop
Sales Engineering Exercise

Mordecai Kraushar
mkraushar@gmail.com

Agenda

A look at Pixi a MEAN stack intentionally vulnerable application (Web and API)

- http://34.227.100.241:8000
- A look at some Pixi vulnerabilities
- Starting and stopping Pixi without Contrast

A look at Contrast with Pixi

- A look at the Contrast console
- Getting the Contrast agent into Pixi
- Starting and stopping Pixi with Contrast

Contrast with Pixi in Assess Mode

Contrast with Pixi in Protect Mode

Remediation discussion for Pixi

Optional: Installed WebGoat with a Contrast agent and tested this in the Eval

http://34.230.24.194:8080/WebGoat/

Pixi (under the hood)

Running on an Ubuntu AWS instance

Original code is at :

> *git clone https://github.com/thedeadrobots/pixi.git*

Pulls down two docker images (app and Mongo database)

> *Docker-compose up*

App code was extracted to run on box

> *Mongo is running in a docker container*

A couple of shell windows and docker commands

A bit of look at Pixi

A bit of POSTMAN to see the API

-
-

Contrast and Pixi

Eval license of Contrast was provided for this demo

- *Downloaded and installed node-contrast-<version>.tgz agent for nodejs*
- *Downloaded and installed YAML config file*
- *Started pixi with contrast agent*

Contrast console then populated

- *Applications*
- *Servers*
- *Libraries*
- *Vulnerabilities*
- *Attacks*

Policy management and organization settings also reviewed

Contrast and Pixi Demo

Contrast in Assess Mode

Contrast in Protect Mode

Contrast in Protect mode blocking

Other Contrast actions (blacklist, virtual firewalls)

Other Contrast features (for developers,for devsecops, for admins)

Review of Pixi with Contrast (performance, functionality)

Fixing the XSS in Pixi

Contrast and Pixi Demo (cheat sheet)

Script tag in search form field after you login:

```
<script> alert("Hi") ; </script>
```

Addressed by @sce in pixi.html

```
Vi pixi.html and  change  $sceProvider.enabled(false)
```

Nosql injection on login

```
more curlpostnosql
user=bob%40bob.com&pass[$ne]=
curl -X POST   -d @curlpostnosql  http://34.227.100.241:8000/login
```

Attack with nikto (or burp or zap)

npm commands to update libraries

Node and nodemon commands to start the app

Contrast Security Tech Workshop
Questions ?

CONTRAST
SECURITY

Mordecai Kraushar
mkraushar@gmail.com