



# Extending Kibana

Pete Hampton, Senior Data Engineer

---

11 February, 2022

# Yo!



Pete Hampton 🙌

@pjhampton

- Live in Belfast, N. Ireland
- Engineer @ Elastic Security
- I build data feeds and pipelines

# Who are you?



(In lieu of your photograph above,  
Winnie Barker pictured)

- Basic understanding of Kibana & Elasticsearch
- Comfortable with TypeScript
- Comfortable with Git and Github

# ⚡ This lightning talk

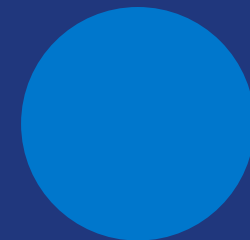
- Developed a Kibana plugin in 2017
- Been maintaining it since for various companies
- Lessons and resources about developing / maintaining plugins

# Extending Kibana

1. Starting
2. Testing
3. Security
4. Shipping

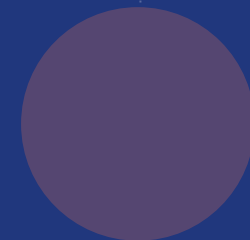


# Content



## Starting

Start building a Kibana plugin.



## Testing

Testing your Kibana Plugin



## Security

Keeping user security in mind



## Shipping

Package and ship your plugin



# Starting

- Download the Kibana Repo and run a local Elasticsearch node

```
kibana on □ main [$!] is 📦 v8.1.0 via 🟢 v16.13.0
→ nvm use
Found '/Users/ph/workspace/kibana/.nvmrc' with version <16.13.2>
Now using node v16.13.2 (npm v8.1.2)

kibana on □ main [$!] is 📦 v8.1.0 via 🟢 v16.13.2 took 2s
→ yarn kbn bootstrap
yarn run v1.22.5
$ node scripts/kbn bootstrap
succ [bazel_tools] all bazel tools are correctly installed
```

```
kibana on □ main [$!] is 📦 v8.1.0 via 🟢 v16.13.2 took 5s
→ yarn es snapshot --license trial -E xpack.security.authc.api_key.enabled=true
yarn run v1.22.5
$ node scripts/es snapshot --license trial -E xpack.security.authc.api_key.enabled=true
info Installing from snapshot
  info version: 8.1.0
  info install path: /Users/ph/workspace/kibana/.es/8.1.0
  info license: trial
  info Downloading snapshot manifest from https://storage.googleapis.com/kibana-ci-es-snapshots-daily/8.1.0/manifest-latest-verified.json
```

# Starting

```
kibana on □ main [$!] is 📦 v8.1.0 via 📌 v16.13.2
→ node scripts/generate_plugin.js demo_plugin
? Plugin name (use camelCase) demoPlugin
? Provide a description for your plugin. This is a demo plugin
? Will this plugin be part of the Kibana repository? No
? Who is developing and maintaining this plugin? Pete Hampton
? Should an UI plugin be generated? Yes
? Should a server plugin be generated? Yes
SUCC 🎉
```

Your plugin has been created in plugins/demo\_plugin



# Starting

kibana/plugins on `main` [\$!]

→ tree demo\_plugin

```
demo_plugin
├── README.md
├── common
│   └── index.ts
├── kibana.json
├── package.json
├── public
│   ├── application.tsx
│   ├── components
│   │   └── app.tsx
│   ├── index.scss
│   ├── index.ts
│   ├── plugin.ts
│   └── types.ts
├── server
│   ├── index.ts
│   ├── plugin.ts
│   ├── routes
│   │   └── index.ts
│   └── types.ts
├── translations
│   └── ja-JP.json
└── tsconfig.json
```

6 directories, 16 files

# Starting



WORK-WITH-ME AND AMA

## Extending Kibana with Plugins

Tue, Jan 18, 11:00 AM (PDT)

RSVP today

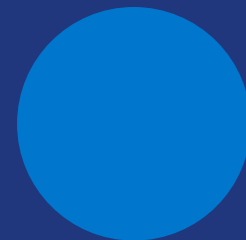
Special Guest:

Luke Elmers



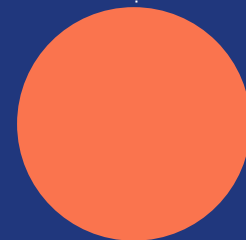
<https://www.youtube.com/watch?v=kzLmswbFQho>

# Content



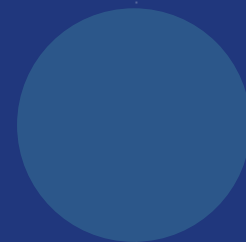
## Starting

Start building a Kibana plugin.



## Testing

Testing your Kibana Plugin



## Security

Keeping user security in mind



## Shipping

Package and ship your plugin

# Testing

- Unit tests
- I like Jest  
(<https://www.npmjs.com/package/jest>)
- Keeping tests in a similar named file: `index.ts` → `index.test.ts`

```
kibana/plugins on main [$!]
```

```
→ tree demo_plugin
```

```
demo_plugin
```

```
├── README.md
```

```
├── common
```

```
│   └── index.ts
```

```
├── kibana.json
```

```
├── package.json
```

```
├── public
```

```
│   ├── application.tsx
```

```
│   ├── components
```

```
│       └── app.tsx
```

```
│   ├── index.scss
```

```
│   ├── index.ts
```

```
│   ├── plugin.ts
```

```
│   └── types.ts
```

```
├── server
```

```
│   ├── index.ts
```

```
│   ├── plugin.ts
```

```
│   ├── routes
```

```
│       └── index.ts
```

```
│   └── types.ts
```

```
├── translations
```

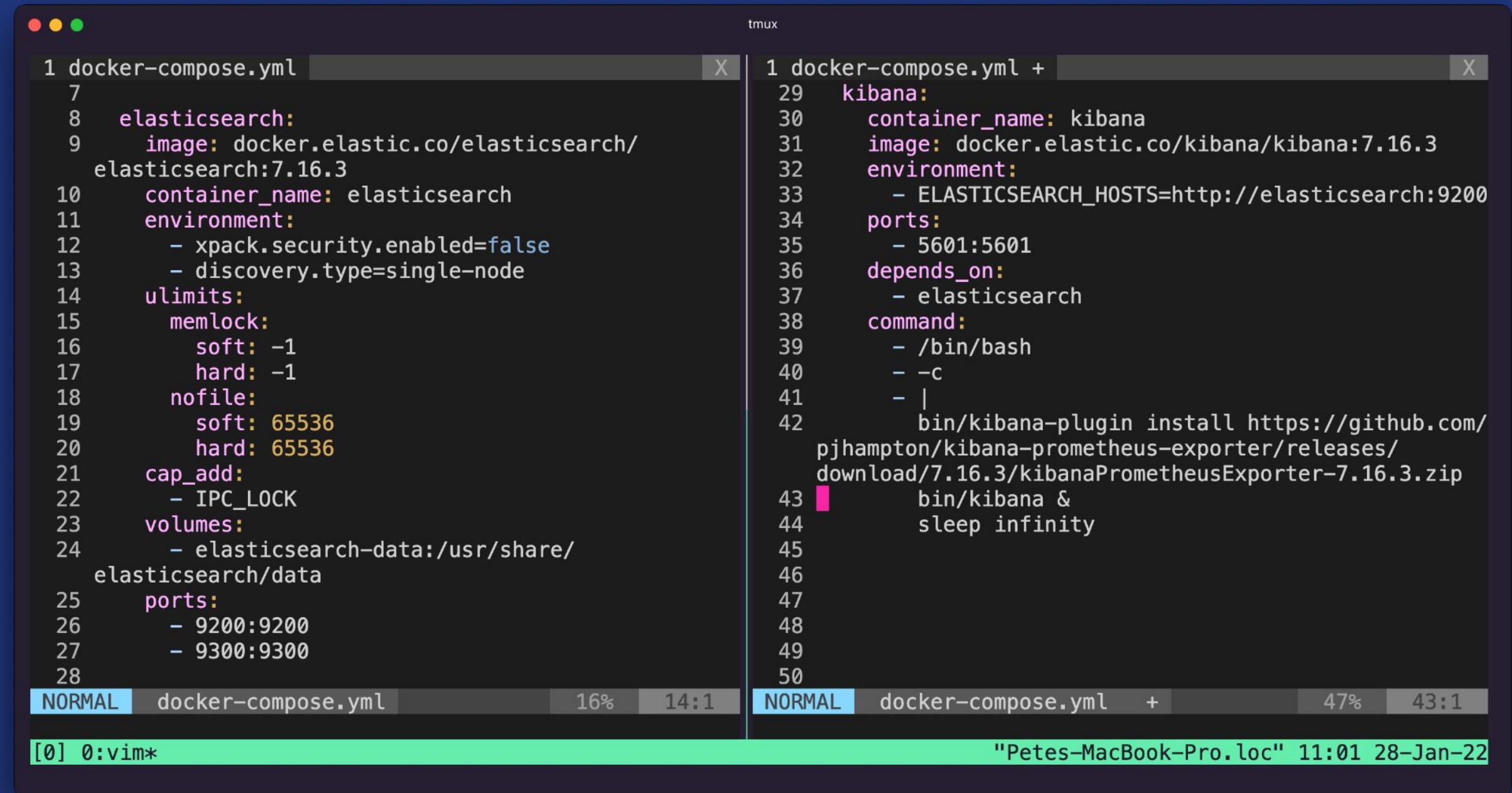
```
│   └── ja-JP.json
```

```
└── tsconfig.json
```

```
6 directories, 16 files
```

# Testing

- e2e tests
- A separate docker container that runs synthetic tests
- A good place to test security



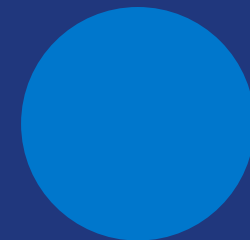
```
1 docker-compose.yml X
7
8   elasticsearch:
9     image: docker.elastic.co/elasticsearch/
    elasticsearch:7.16.3
10    container_name: elasticsearch
11    environment:
12      - xpack.security.enabled=false
13      - discovery.type=single-node
14    ulimits:
15      memlock:
16        soft: -1
17        hard: -1
18      nofile:
19        soft: 65536
20        hard: 65536
21    cap_add:
22      - IPC_LOCK
23    volumes:
24      - elasticsearch-data:/usr/share/
        elasticsearch/data
25    ports:
26      - 9200:9200
27      - 9300:9300
28
NORMAL docker-compose.yml 16% 14:1

1 docker-compose.yml + X
29   kibana:
30     container_name: kibana
31     image: docker.elastic.co/kibana/kibana:7.16.3
32     environment:
33       - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
34     ports:
35       - 5601:5601
36     depends_on:
37       - elasticsearch
38     command:
39       - /bin/bash
40       - -c
41       - |
42         bin/kibana-plugin install https://github.com/
        pjhampton/kibana-prometheus-exporter/releases/
        download/7.16.3/kibanaPrometheusExporter-7.16.3.zip
43       bin/kibana &
44       sleep infinity
45
46
47
48
49
50
NORMAL docker-compose.yml + 47% 43:1

[0] 0:vim* "Petes-MacBook-Pro.loc" 11:01 28-Jan-22
```

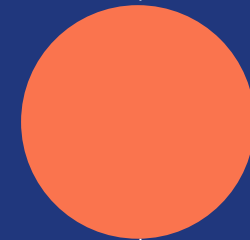


# Content



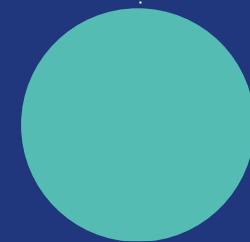
## Starting

Start building a Kibana plugin.



## Testing

Testing your Kibana Plugin



## Security

Keeping user security in mind



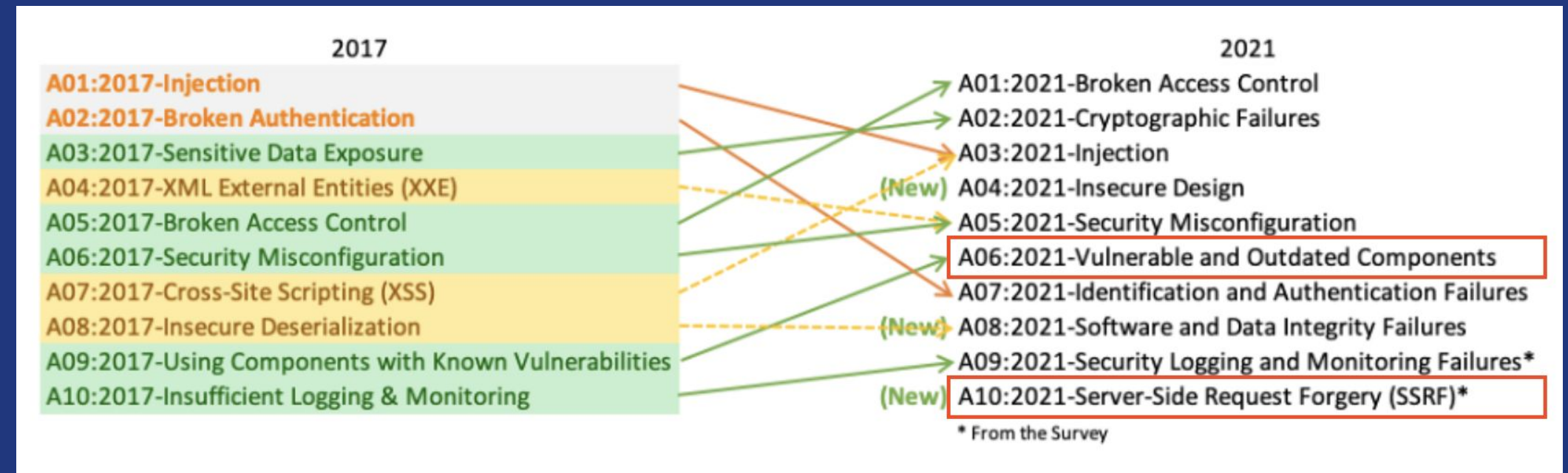
## Shipping

Package and ship your plugin



# Security

- Keep in mind that your plugin introduces a security risk into a users environment
- Keep OWASP Top 10 in mind



Source: <https://owasp.org/Top10/>

# Security

- Consider using a dependency updater service

The screenshot shows a GitHub pull request interface. At the top, the title is "Bump axios from 0.24.0 to 0.25.0 #251". Below the title, it says "Merged" and "pjhampton merged 1 commit into main from dependabot/npm\_and\_yarn/axios-0.25.0 10 days ago". The interface includes tabs for "Conversation" (1), "Commits" (1), "Checks" (0), and "Files changed" (3). A comment from "dependabot" (bot) is visible, stating "Bumps axios from 0.24.0 to 0.25.0." and listing expandable sections for "Release notes", "Changelog", and "Commits". A "compatibility 93%" badge is shown. Below the comment, it says "Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting @dependabot rebase .". At the bottom of the comment section, it says "Dependabot commands and options". The right sidebar contains sections for "Reviewers" (pjhampton with a green checkmark), "Assignees" (No one—assign yourself), "Labels" (dependencies), "Projects" (None yet), "Milestone" (No milestone), and "Linked issues" (Successfully merging this pull request may close these issues. None yet). The bottom of the pull request shows a commit "Bump axios from 0.24.0 to 0.25.0" with a "Verified" badge and a commit hash "7fd1f2b". A note at the bottom says "dependabot (bot) added the dependencies label 10 days ago".

# Security

- Consider using static analysis
- Finds common CVEs & CWEs

The screenshot displays the Snyk Code Analysis interface for a project named 'kibana-prometheus-exporter'. The top navigation bar includes links for Dashboard, Reports, Projects, Integrations, and Members. The main header shows the project name and a 'Code Analysis' section with tabs for Overview, History, and Settings. Below the header, it indicates the project was created on Thu 27th Jan 2022 and the snapshot was taken by snyk.io a few seconds ago. The interface is divided into two main sections: 'PROJECT OWNER' and 'SCAN COVERAGE'. The 'PROJECT OWNER' section has a button to 'Add a project owner'. The 'SCAN COVERAGE' section shows '8 Files (32% coverage)' and a 'View breakdown' link. The 'Issues' section is active, showing a list of issues. On the left, there are filters for SEVERITY (High, Medium, Low), PRIORITY SCORE (Scored between 0 - 1000), STATUS (Open, Ignored), and LANGUAGES (TypeScript). The main issue displayed is a 'Server-Side Request Forgery (SSRF)' with a score of 850. The issue is associated with the SNYK CODE CWE-918. The code snippet shows a request header being set to 'Authorization' and then used in an axios.get call. The description states: 'Unsanitized input from the request URL flows into axios.#default.get, where it is used as an URL to perform a request. This may result in a Server-Side Request Forgery vulnerability.' The file path is 'server/routes/index.ts' and it is '9 steps in 1 file'. A 'Full details' button is available at the bottom right of the issue details.

snyk pjhampton

Dashboard Reports Projects Integrations Members

kibana-prometheus-exporter main

Code Analysis Overview History Settings

Created Thu 27th Jan 2022 | Snapshot taken by snyk.io a few seconds ago

PROJECT OWNER

+ Add a project owner

SCAN COVERAGE

8 Files (32% coverage) View breakdown

Issues 1

SEVERITY

☐ High 1

☐ Medium 0

☐ Low 0

PRIORITY SCORE

Scored between 0 - 1000

STATUS

☒ Open 1

☐ Ignored 0

LANGUAGES

☐ TypeScript 1

1 of 1 issues

Group by none Sort by highest severity

**H** Server-Side Request Forgery (SSRF) SCORE 850

SNYK CODE | CWE-918

```
20 && request.headers.authorization !== undefined) {
21   reqHeaders = { 'Authorization': request.headers.authorization };
22 }
23
24 const kibanaInternalStatus = await axios.get(
```

Unsanitized input from the request URL flows into axios.#default.get, where it is used as an URL to perform a request. This may result in a Server-Side Request Forgery vulnerability.

server/routes/index.ts 9 steps in 1 file

Full details


Share your feedback!

# Security

- Can advise on remediation action within your code

Snyk

Free (current plan) ▾



For individuals and small organisations to stay secure.

✓ Unlimited tests on open-source projects, 200 tests/month on private projects


✓ Single click remediation

✓ CI/CD pipeline integration

✓ Continuous monitoring

\$0 / month

Cancel this plan

 **Server-Side Request Forgery (SSRF)**

SNYK CODE | [CWE-918](#)

[Data flow](#) [Fix analysis](#) ✕

**Details**

In a server-side request forgery attack, a malicious user supplies a URL (an external URL or a network IP address such as 127.0.0.1) to the application's back end. The server then accesses the URL and shares its results, which may include sensitive information such as AWS metadata, internal configuration information, or database contents with the attacker. Because the request comes from the back end, it bypasses access controls, potentially exposing information the user does not have sufficient privileges to receive. The attacker can then exploit this information to gain access, modify the web application, or demand a ransom payment.

**Best practices for prevention**

- Blacklists are problematic and attackers have numerous ways to bypass them; ideally, use a whitelist of all permitted domains and IP addresses.
- Use authentication even within your own network to prevent exploitation of server-side requests.
- Implement zero trust and sanitize and validate all URL and header data returning to the server from the user. Strip invalid or suspect characters, then inspect to be certain it contains a valid and expected value.
- Ideally, avoid sending server requests based on user-provided data altogether.
- Ensure that you are not sending raw response bodies from the server directly to the client. Only deliver expected responses.
- Disable suspect and exploitable URL schemas. Common culprits include obscure and little-used schemas such as `file://`, `dict://`, `ftp://`, and `gopher://`.

**Example fixes**

StirFry-js/stirfry

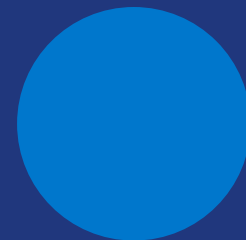
1 / 3

```
2 2 var StirFry = require('../stirfry.js');
3 3 var server = new StirFry(8080, '0.0.0.0');
4 4 server.request((req, res) => res.send(req.url));
4 server.request(/.*/, (req, res) => res.send(req.url));
```

# Security

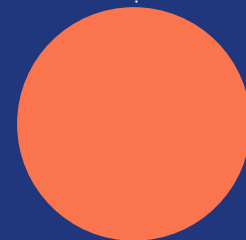
- If you are exposing routes you should research and advise on correct privilege
- Also consider how you handle errors not to bubble up to client.

# Content



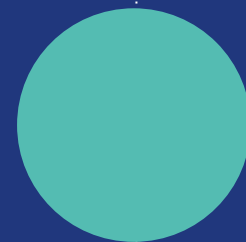
## Starting

Start building a Kibana plugin.



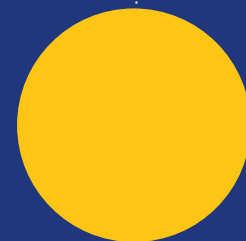
## Testing

Testing your Kibana Plugin



## Security

Keeping user security in mind



## Shipping

Package and ship your plugin



# Shipping

<input type="checkbox"/> <input checked="" type="radio"/> 0 Open <input checked="" type="radio"/> 82 Closed		Author ▾	Label ▾	Projects ▾	Milestones ▾	Assignee ▾	Sort ▾
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Release of new version kibana-prometheus-exporter 7.16.3</b>						2
	#252 by arjunav123 was closed 6 days ago						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Release 6.8.22</b> <b>RELEASE</b>						1
	#250 by andrewpollack was closed 11 days ago						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>RELEASE 7.16.1</b> <b>RELEASE</b>						3
	#247 by dropdeadfu was closed on 14 Dec 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Kibana 7.10.2 - Backport bugfix</b> <b>RELEASE</b> <b>todo</b>						11
	#235 by rursprung was closed on 20 Sep 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Internal Server Error with basePath and rewriteBasePath</b> <b>bug</b>						3
	#233 by MaxenceAdnot was closed on 19 Jul 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Plugin Returning 500</b>						2
	#226 by KnechtionsCoding was closed on 19 Jul 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>404 when hitting /_prometheus/metrics</b>						6
	#223 by KnechtionsCoding was closed on 29 May 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>metric kibana_heap_max_in_bytes not the max heap from configuration</b> <b>bug</b> <b>investigation</b>						10
	#219 by perkons was closed on 26 Apr 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Release 6.8.15</b> <b>RELEASE</b>						1
	#218 by branden was closed on 10 Nov 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Internal Server Error when Installing 7.10.0 in ECK Kibana</b> <b>bug</b>						3
	#217 by KnechtionsCoding was closed on 28 Apr 2021						
<input type="checkbox"/>	<input checked="" type="radio"/> <b>Release 7.12</b> <b>RELEASE</b>						2
	#216 by sasah was closed on 24 Mar 2021						

# Shipping

- Stack uses semantic versioning
- GH RSS feed:  
<https://github.com/elastic/kibana/releases.atom>
- Consider extended semantic versioning:  
**Major.Minor.Patch.<Iterator>**



# Shipping

```
kibana on □ main [$!] is 📦 v8.1.0 via 📌 v16.13.2  
→ curl \  
  -H "Accept: application/vnd.github.v3+json" \  
  https://api.github.com/repos/pjhampton/kibana-prometheus-exporter/releases \  
  | jq . -C \  
  | less -r
```

# Final Thoughts: Encourage Collaboration

- Users often request support older versions of Kibana (Elastic supports very old clusters: <https://www.elastic.co/support/matrix>)
- Ask to fork or clone project into environment
- Encourage contributions back to your project
- Share it! Promote your plugin via Elastic's official documentation

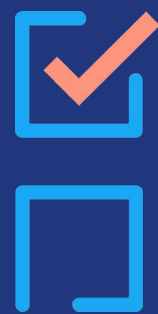
# Final Thoughts: What I'm focusing on (Non paid Open Source)

- Kibana can also be augmented via browser extensions - *not just Kibana Extensions*
- Building an automated release pipeline to test and build release

# References

- Kibana Prometheus Exporter Reference:  
<https://github.com/pjhampton/kibana-prometheus-exporter>
- Extending Kibana with Plugins (**Video: Host - Jay Miller / Speaker - Luke Elmers**):  
<https://www.youtube.com/watch?v=kzLmswbFQho>
- Kibana Development Guide:  
<https://www.elastic.co/guide/en/kibana/current/development-getting-started.html>
- Kibana Plugin Development Guide  
<https://www.elastic.co/guide/en/kibana/current/external-plugin-development.html>





**Thank you!**  
@pjhampton 🦄

