Discovering Components with Known Vulnerabilities in Web Applications

Author: Cristian Cornea

https://github.com/corneacristian/

https://www.linkedin.com/in/cristian-cornea-b37005178/

https://medium.com/@corneacristian

https://hackerone.com/droop3r

1. Purpose **2**

2. Extract Used Components and Versions **2**

3. Check Versions for Security Issues **3**

4. Payloads for Developer Console **3**

4.1.1. jQuery 3
4.1.2. jQuery UI 3
4.1.3. Angular 3
4.1.4. Bootstrap 3
4.1.5. Lodash 4
4.1.6. MomentJS 4
4.1.7. ExtJS 4
4.1.8. CKEditor 4
4.1.9. Vue 4
4.1.10. Highcharts 4
4.1.11. Froala Editor 5
4.1.12. DataTablesJS 5
4.1.13. Dojo 5
4.1.14. Meteor 5
4.1.15. React 5
4.1.16. Socket.IO 5
4.1.17. TinyMCE 6
4.1.18. EmberJS 6

1. Purpose

This paper serves as a cheat sheet for security researchers and penetration testers to identify and validate components of tested web applications which are subject to known vulnerabilities and security issues.

2. Extract Used Components and Versions

For this action, we will be using the Web Browser's Developer Console in correlation with the input payloads provided through this document, which will help us to extract different names of web-based libraries and their versions.

3. Check Versions for Security Issues

For this purpose we will be searching the versions of the used components within one of the listed platforms below:

- https://www.exploit-db.com/
- https://snyk.io/vuln/
- https://stack.watch
- https://www.cvedetails.com

4. Payloads for Developer Console

4.1.1. jQuery

```
jQuery().jquery
```

4.1.2. jQuery UI

```
$.ui.version
```

```
$.ui
```

4.1.3. Angular

```
angular.version
```

4.1.4. Bootstrap

```
$.fn.tooltip.Constructor.VERSION
```

4.1.5. Lodash

```
_.VERSION
```

4.1.6. MomentJS

```
moment.version
```

4.1.7. ExtJS

```
Ext.version
```

```
Ext.getVersion('extjs')
```

```
Ext.getVersion().version
```

4.1.8. CKEditor

```
CKEDITOR.version
```

4.1.9. Vue

```
Vue.version
```

4.1.10. Highcharts

```
Highcharts.version
```

4.1.11. Froala Editor

```
$.FE.VERSION
```

```
FroalaEditor.VERSION
```

4.1.12. DataTablesJS

```
$.fn.dataTable.version
```

```
$.fn.dataTable.versionCheck()
```

4.1.13. Dojo

```
dojo.version.toString()
```

4.1.14. Meteor

```
Meteor.release
```

4.1.15. React

```
React.version
```

4.1.16. Socket.IO

```
io.version
```

4.1.17. TinyMCE

```
tinyMCE
```

4.1.18. EmberJS

```
Ember.VERSION
```