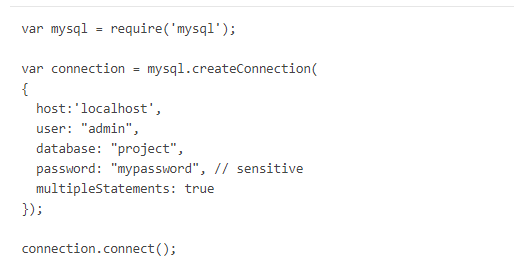
* **Authentication: 🡪Lucas**

[CWE-798](http://cwe.mitre.org/data/definitions/798) - Use of Hard-coded Credentials

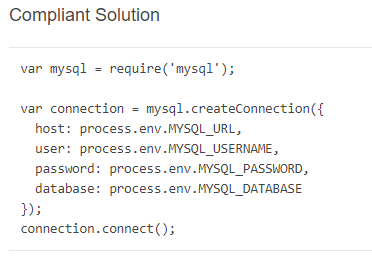
[CWE-259](http://cwe.mitre.org/data/definitions/259) - Use of Hard-coded Password

1. app/code/Magento/Customer/view/frontend/requirejs-config.js
2. app/code/Magento/Customer/view/frontend/requirejs-config.js
3. app/code/Magento/Customer/view/frontend/web/js/password-strength-indicator.js

**Bad example(exist in code):**



**Good example(remediation):**



* **Command injection**

[CWE-798](http://cwe.mitre.org/data/definitions/798) - Use of Hard-coded Credentials

[CWE-259](http://cwe.mitre.org/data/definitions/259) - Use of Hard-coded Password

app/code/Magento/Customer/view/frontend/web/js/password-strength-indicator.js

**[code, Good and bad examples are same as authentication]**

* **Cross-Site Scripting(XSS) 🡪 Shashank**

[CWE-79](http://cwe.mitre.org/data/definitions/79.html) - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

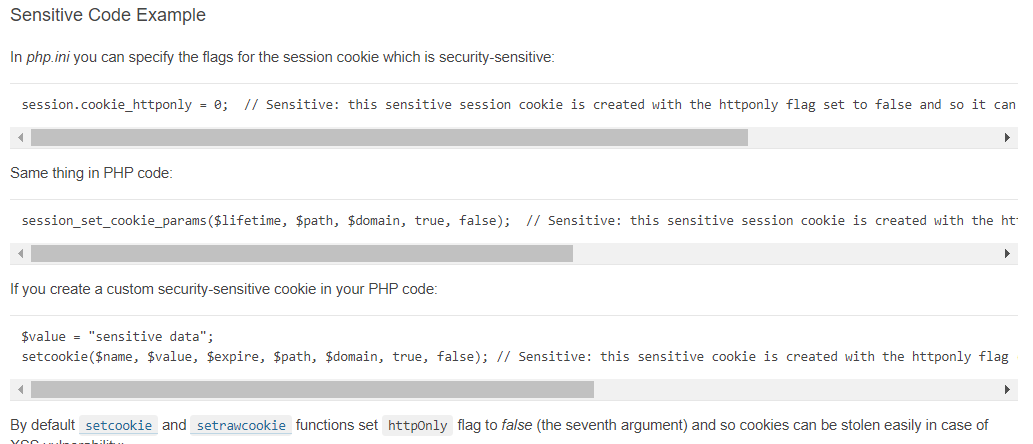
[CWE-1004](https://cwe.mitre.org/data/definitions/1004.html) - Sensitive Cookie Without 'HttpOnly' Flag

1) lib/web/jquery/fileUploader/cors/jquery.postmessage-transport.js

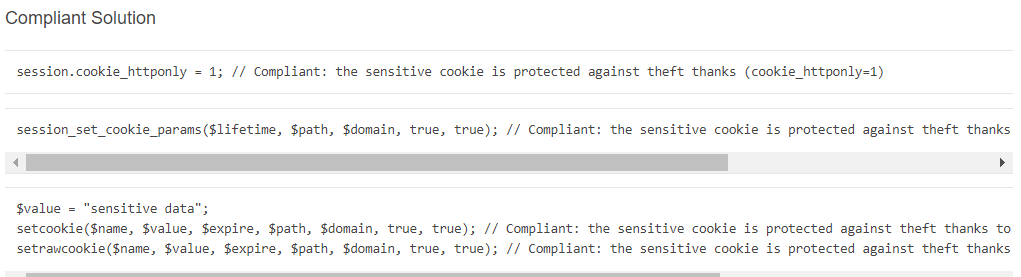
2)lib/web/MutationObserver.js



**Bad example(exist in code):**



**Good example(remediation):**



* **Denial of Service 🡪Pradeep**

[CWE-624](https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS) - Executable Regular Expression Error

1)app/code/Magento/Catalog/view/adminhtml/web/catalog/product/composite/configure.js

2)app/code/Magento/Catalog/view/adminhtml/web/component/image-size-field.js

3)app/code/Magento/Catalog/view/adminhtml/web/component/static-type-input.js

4) app/code/Magento/Catalog/view/adminhtml/web/js/components/import-handler.js

5)app/code/Magento/Catalog/view/frontend/web/js/product/breadcrumbs.js

6)app/code/Magento/Checkout/view/frontend/web/js/region-updater.js

7)app/code/Magento/Payment/view/base/web/js/model/credit-card-validation/expiration-date-validator/parse-date.js

8)app/code/Magento/ProductVideo/view/adminhtml/web/js/get-video-information.js

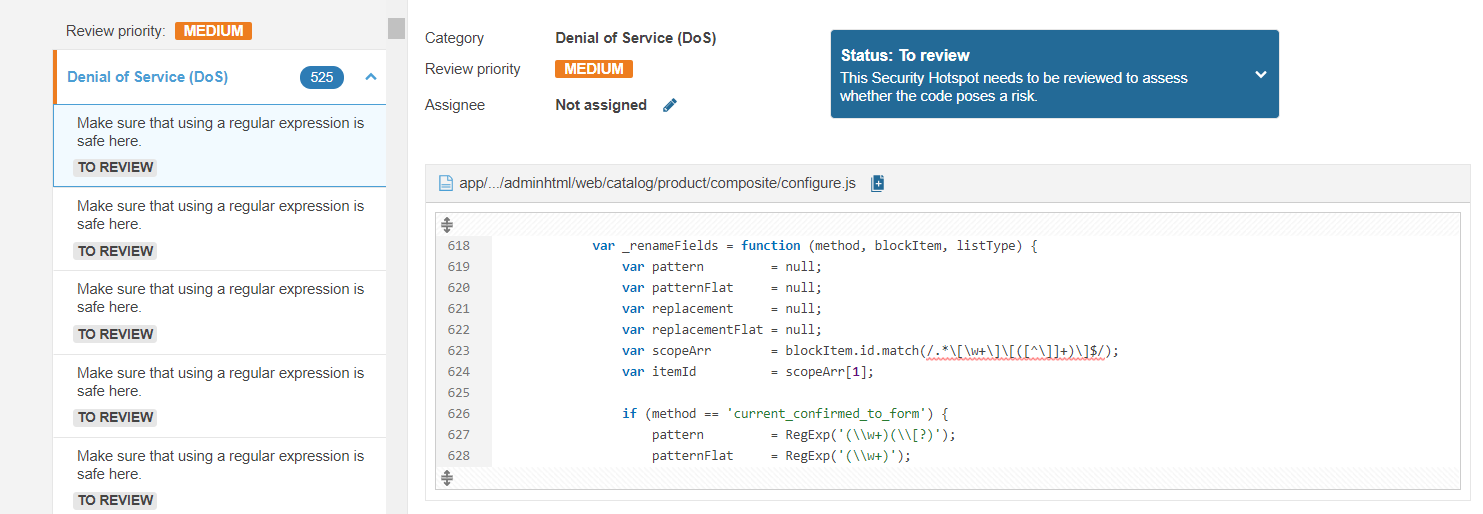
9)app/code/Magento/Rule/view/adminhtml/web/conditions-data-normalizer.js

10)app/code/Magento/Rule/view/adminhtml/web/rules.js

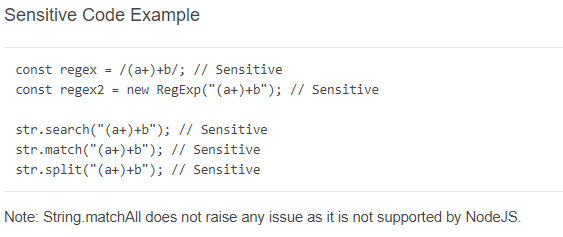
11)app/code/Magento/Sales/view/adminhtml/web/order/create/scripts.js

12) app/code/Magento/Tinymce3/view/base/web/tiny\_mce/plugins/media/js/media.js

13) setup/pub/bootstrap/js/bootstrap.js



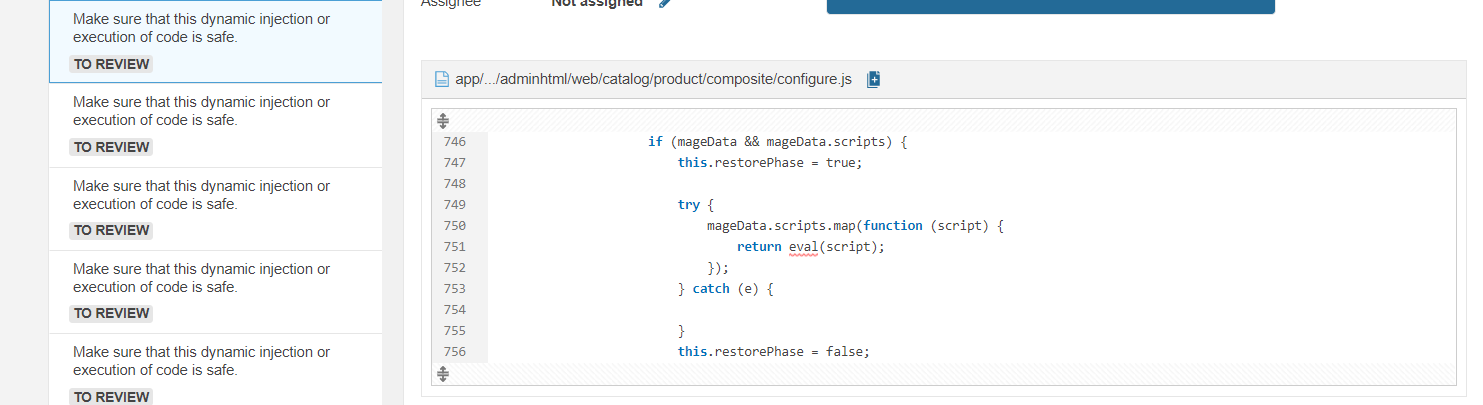
**Bad example(exist in code):**



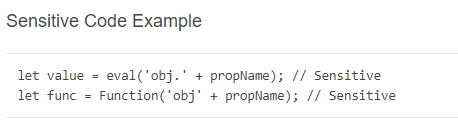
* **Code Injection: 🡪Pradeep**

[CWE-95](http://cwe.mitre.org/data/definitions/95.html) - Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

1. app/code/Magento/Catalog/view/adminhtml/web/catalog/product/composite/configure.js
2. app/code/Magento/Tinymce3/view/base/web/tiny\_mce/classes/Popup.js
3. app/code/Magento/Tinymce3/view/base/web/tiny\_mce/classes/firebug/firebug-lite.js
4. lib/web/extjs/ext-tree-checkbox.js
5. lib/web/jquery.js
6. lib/web/jquery/editableMultiselect/js/jquery.editable.js
7. lib/web/jquery/jquery.metadata.js
8. lib/web/mage/requirejs/static.js
9. lib/web/prototype/prototype.js



**Bad example(exist in code):**



* **Weak Cryptography 🡪Bhavana**

[CWE-330](https://cwe.mitre.org/data/definitions/330.html) - Use of Insufficiently Random Values

1)lib/internal/Magento/Framework/Session/SessionManager.php

2)app/code/Magento/Backend/Block/Widget/Grid/Extended.php

3)app/code/Magento/Backend/Helper/Dashboard/Data.php

4)app/code/Magento/Backend/view/adminhtml/templates/widget/grid/serializer.phtml

5)app/code/Magento/Catalog/Block/Navigation.php

6)app/code/Magento/Catalog/Controller/Adminhtml/Product/Attribute.php

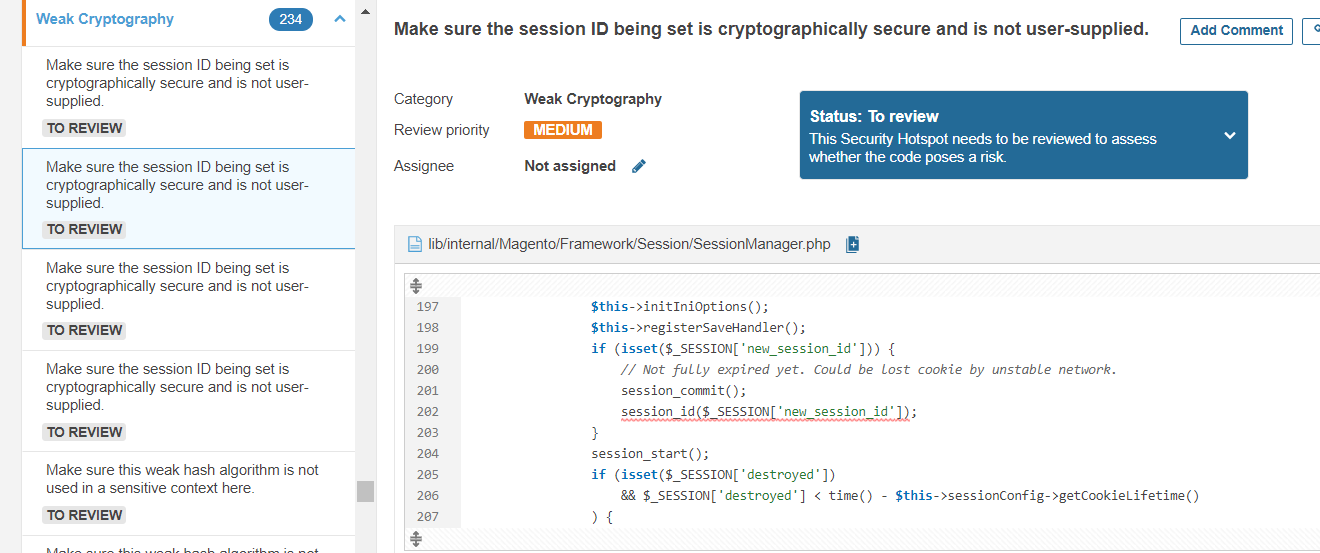
7)app/code/Magento/Cron/Observer/ProcessCronQueueObserver.php

8)app/code/Magento/Eav/Setup/EavSetup.php

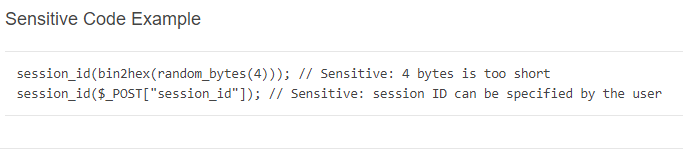
9)setup/src/Magento/Setup/Model/CryptKeyGenerator.php

10)lib/web/prototype/window.js

11)lib/web/scriptaculous/effects.js



**Bad example(exist in code):**



* **Insecure Configuration 🡪Bhavana**

[CWE-312](http://cwe.mitre.org/data/definitions/312.html) - Cleartext Storage of Sensitive Information

[CWE-315](http://cwe.mitre.org/data/definitions/315.html) - Cleartext Storage of Sensitive Information in a Cookie

1)app/code/Magento/Tinymce3/view/base/web/tiny\_mce/tiny\_mce\_jquery\_src.js

2)lib/web/mage/adminhtml/tools.js

3)lib/web/mage/cookies.js

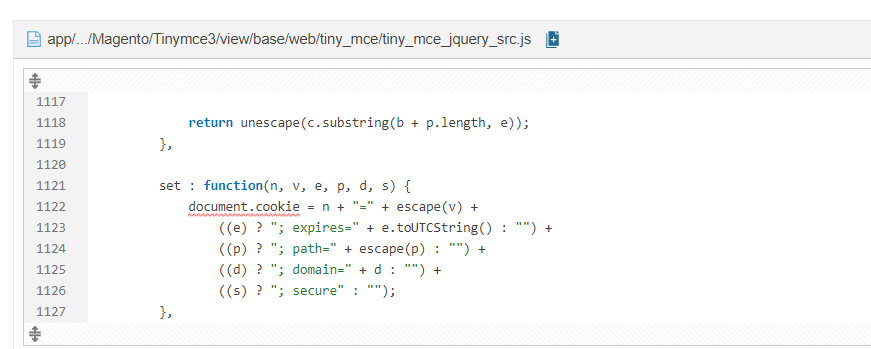
4)app/code/Magento/Rule/view/adminhtml/web/rules.js

5)app/code/Magento/Tinymce3/view/base/web/tiny\_mce/classes/WindowManager.js

6)app/code/Magento/Tinymce3/view/base/web/tiny\_mce/classes/firebug/firebug-lite.js

7)app/code/Magento/Tinymce3/view/base/web/tiny\_mce/plugins/advlink/js/advlink.js

8)app/code/Magento/Tinymce3/view/base/web/tiny\_mce/tiny\_mce\_src.js



**Bad example(exist in code):**



* **Log Injection🡪Reshma**

[CWE-532](https://cwe.mitre.org/data/definitions/532.html) - Information Exposure Through Log Files

[CWE-117](https://cwe.mitre.org/data/definitions/117.html) - Improper Output Neutralization for Logs

[CWE-778](https://cwe.mitre.org/data/definitions/778.html) - Insufficient Logging

1)app/code/Magento/Deploy/Console/ConsoleLogger.php

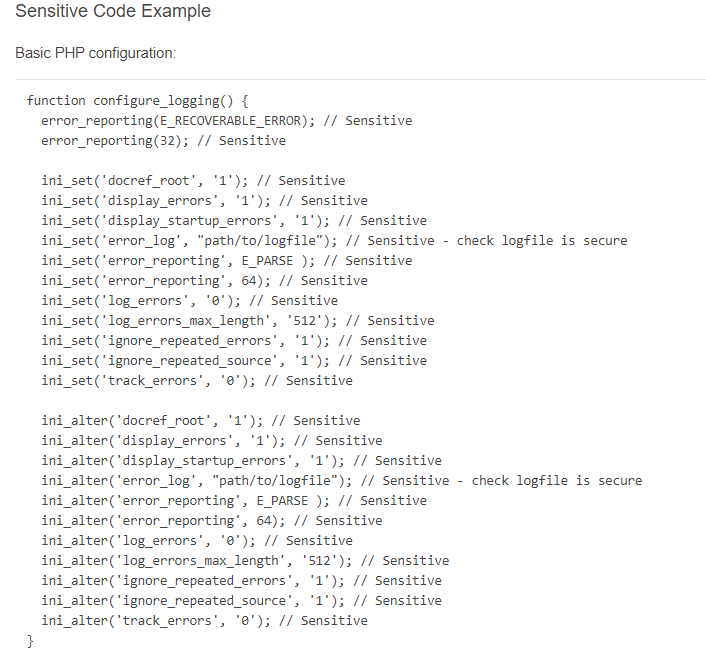
2)app/code/Magento/SampleData/Console/Command/SampleDataDeployCommand.php

3)lib/internal/Magento/Framework/DB/Statement/Pdo/Mysql.php

4)lib/internal/Magento/Framework/Logger/LoggerProxy.php



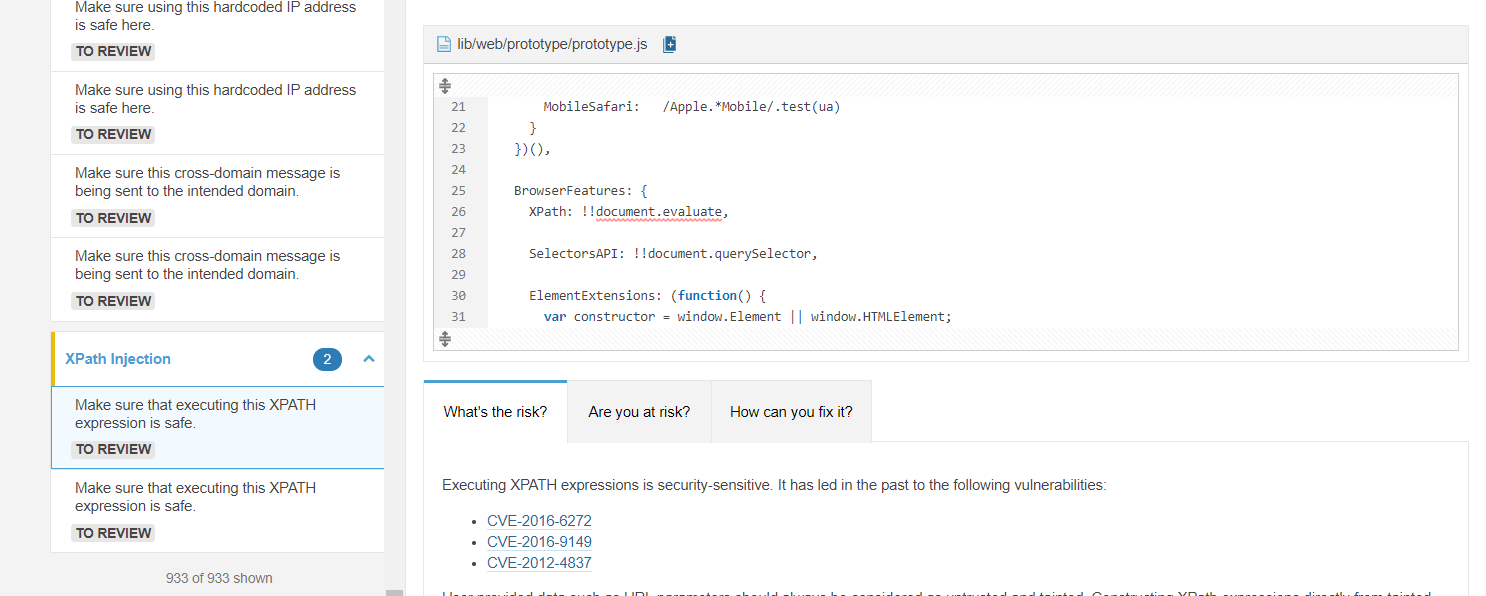
**Bad example(exist in code):**



* **XPath Injection**

[CWE-643](http://cwe.mitre.org/data/definitions/643) - Improper Neutralization of Data within XPath Expressions

1)lib/web/prototype/prototype.js



**Bad example(exist in code):**

