github.com/WebGoat/WebGoat

Commit: `d4238ab406f2` License: `GPL-2.0` Scanned: Mon, 19 Jan 2026 11:35:15 UTC 628 files in 1m9s

SECURITY SCORE

41	141	0	0
CRITICAL	HIGH	MEDIUM	LOW

Findings (182)

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/it/java/org/owasp/webgoat/playwright/webwolf/JwtUITest.java:31

```
31          "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c";
```

java.spring.security.injection.tainted-sql-string.tainted-sql-string CRITICAL

User data flows into this manually-constructed SQL string. User data can be safely inserted into SQL strings using prepared statements or an object-relational mapper (ORM). Manually-constructed SQL strings is a possible indicator of SQL injection, which could let an attacker steal or manipulate data from the database. Instead, use prepared statements (`connection.PreparedStatement`) or a safe library.

src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java:45

```
45                "select password from challenge_users where userid = '"
                  + username_login
                  + "' and password = '"
                  + password_login
                  + "'");
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java:50

```
50        ResultSet resultSet = statement.executeQuery();
```

java.spring.security.injection.tainted-url-host.tainted-url-host CRITICAL

User data flows into the host portion of this manually-constructed URL. This could allow an attacker to send data to their own server, potentially exposing sensitive data such as cookies or authorization information sent with this request. They could also probe internal servers or other resources that the server running this code can access. (This is called server-side request forgery, or SSRF.) Do not allow arbitrary hosts. Instead, create an allowlist for approved hosts, hardcode the correct host, or ensure that the user data can only affect the path or parameters.

src/main/java/org/owasp/webgoat/lessons/jwt/claimmisuse/JWTHeaderJKUEndpoint.java:57

```
57          var jwkProvider = new JwkProviderBuilder(new URL(jku.asString())).build();
```

java.lang.security.httpservlet-path-traversal.httpservlet-path-traversal CRITICAL

Detected a potential path traversal. A malicious actor could control the location of this file, to include going backwards in the directory with '../'. To address this, ensure that user-controlled variables in file paths are sanitized. You may also consider using a utility method such as org.apache.commons.io.FilenameUtils.getName(...) to only retrieve the file name from the path.

src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadRetrieval.java:100

```
100         var catPicture =
          new File(catPicturesDirectory, (id == null ? RandomUtils.nextInt(1, 11) : id)
+ ".jpg");
```

java.spring.security.injection.tainted-sql-string.tainted-sql-string CRITICAL

User data flows into this manually-constructed SQL string. User data can be safely inserted into SQL strings using prepared statements or an object-relational mapper (ORM). Manually-constructed SQL strings is a possible indicator of SQL injection, which could let an attacker steal or manipulate data from the database. Instead, use prepared statements (`connection.PreparedStatement`) or a safe library.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java:55

```
55              "select userid from sql_challenge_users where userid = '" + username +
"'";
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java:57

```
57          ResultSet resultSet = statement.executeQuery(checkUserQuery);
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java

```
56          ResultSet results = statement.executeQuery(query);
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements

(java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java:

```
52          ResultSet results = statement.executeQuery(query);
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java:

```
69          ResultSet results = query.executeQuery();
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java:

```
62          ResultSet results = statement.executeQuery(query);
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java:

```
142         statement.executeUpdate(logQuery);
```

java.lang.security.audit.formatted-sql-string.formatted-sql-string CRITICAL

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java:(

```
65        statement.execute(queryInjection);
```

java.spring.security.injection.tainted-sql-string.tainted-sql-string CRITICAL

User data flows into this manually-constructed SQL string. User data can be safely inserted into SQL strings using prepared statements or an object-relational mapper (ORM). Manually-constructed SQL strings is a possible indicator of SQL injection, which could let an attacker steal or manipulate data from the database. Instead, use prepared statements (`connection.PreparedStatement`) or a safe library.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/mitigation/Servers.java:51

```
51                "select id, hostname, ip, mac, status, description from SERVERS where s
tatus <> 'out"
                  + " of order' order by "
                  + column)) {
```

java.spring.security.injection.tainted-file-path.tainted-file-path CRITICAL

Detected user input controlling a file path. An attacker could control the location of this file, to include going backwards in the directory with '../'. To address this, ensure that user-controlled variables in file paths are sanitized. You may also consider using a utility method such as org.apache.commons.io.FilenameUtils.getName(...) to only retrieve the file name from the path.

src/main/java/org/owasp/webgoat/webwolf/FileServer.java:79

```
79      log.debug("File saved to {}", new File(destinationDir, multipartFile.getOriginalF
ilename()));
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js:6

```
6      document.getElementById("employeeRecord").innerHTML = document.getElementById(newE
mployeeID).innerHTML;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js:38

```
38          newdiv.innerHTML = html;
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_decode.adoc:8

```
8  eyJhbGciOiJIUzI1NiJ9.ew0KICAiYXV0aG9yaXRpZXMiIDogWyAiUk9MRV9BRE1JTiIsICJST0xFX1VTRVIiI
F0sDQogICJjbGllbnRfaWQiIDogIm15LWNsaWVudC13aXRoLXNlY3JldCIsDQogICJleHAiIDogMTYwNzA5OTYwO
CwNCiAgImp0aSIgOiAiOWJjOTJhNDQtMGIxYS00YzVlLWJlNzAtZGE1MjA3NWI5YTg0IiwNCiAgInNjb3BlIiA6I
FsgInJlYWQiLCAid3JpdGUiF0sDQogICJ1c2VyX25hbWUiIDogInVzZXIiDQp9.9lYaULTuoIDJ86-zKDSntJQy
HPpJ2mZAbnWRfel99iI
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc:28

```
28  var token = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI
6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.NFvYpuwbF6YWbPyaNAGEPw9wbhiQSovvSrD89B8K7Ng";
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc:40

```
40  var token = " eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI
6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.NFvYpuwbF6YWbPyaNAGEPw9wbhiQSovvSrD89B8K7Ng";
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc:56

```
56  var token = "eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6
IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.";
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment.adoc:7

```
7  eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzdWIiOiIxMjM0NTY3ODkwIiwidXNlciI6IkpvaG4gRG9lIi
wiYWRtaW4iOnRydWUsImlhdCI6MTUxNjIzOTAyMn0.
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment2.adoc:7

```
7  eyJhbGciOiJIUzI1NiJ9.ew0KICAiYWRtaW4iIDogdHJ1ZSwNCiAgImlhdCIgOiAxNTE2MjM5MDIyLA0KICAic
3ViIiA6ICIxMjM0NTY3ODkwIiwNCiAgInVzZXIiIDogIkpvaG4gRG9lIg0KfQ.
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_libraries_solution.adoc:7

```
7  eyJhbGciOiJIUzI1NiJ9.ew0KICAiYWRtaW4iIDogdHJ1ZSwNCiAgImlhdCIgOiAxNTE2MjM5MDIyLA0KICAic
3ViIiA6ICIxMjM0NTY3ODkwIiwNCiAgInVzZXIiIDogIkpvaG4gRG9lIg0KfQ.
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc:35

```
35  access_token=eyJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE2MDgxMjg1NjYsImFkbWluIjoiZmFsc2UiLCJ1c2VyIjoiVG9tIn0.rTSX6PSXqUoGUvQQDBiqX0re2BSt7s2-X6FPf34Qly9SMpqIUSP8jykedJbjOBNlM3_CTjgk1SvUv48Pz8zIzA
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc:77

```
77  eyJhbGciOiJub25lIn0.ew0KICAiYWRtaW4iIDogInRydWUiLA0KICAiaWF0IiA6IDE2MDgxMjg1NjYsDQogICJ1c2VyIiA6ICJUb20iDQp9
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/html/JWT.html:323

```
323                 th:action="@{/JWT/jku/delete?token=eyJ0eXAiOiJKV1QiLCJqa3UiOiJodHRwczovL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5hbWF6b25hd3MuY29tL3dlYmdvYXQvLndlbGwta25vd24vandrcy5qc29uIiwiYWxnIjoiUlMyNTYifQ.ewogICJpc3MiOiAiV2ViR29hdCBUb2tlbiBCdWlsZGVyIiwKICAiaWF0IjogMTUyNDIxMDkwNCwKICAiZXhwIjogMTYxODkwNTMwNCwKICAiYXVkIjogIndlYmdvYXQub3JnIiwKICAic3ViIjogImplcnJ5QHdlYmdvYXQuY29tIiwKICAidXNlcm5hbWUiOiAiSmVycnkiLAogICJFbWFpbCI6ICJqZXJyeUB3ZWJnb2F0LmNvbSIsCiAgIlJvbGUiOiBbCiAgICAiQ2F0IgogIF0KfQ.SabvRaYSCW7xI0ueca19TL1e66cJIJaxRiydK2G5lgFMIbL5gQQjE6022HEha9HcprqFXyHbtXrQWRXAp6Gjaf5zs8LUMBMARWjEr8TS43ihguarmLLmvBCoqjiZY39o4EcEjEH9xAoyIYR_Trh7kXn6JVU-8MM76l9IOcYIJ9c8LqT1ERNmbCqtI4PP0tdqCy99nHhqlxSCVXaGDF0jMHV5kjCDSHNYib9riy9xZ63Sztify-bwPqRvxmaShPYtG4BBM_WOGlg-bYTTuws-6yISMfTB5U1WBDwLr6dLU123TGO26wCVBgTKbA0KKG94-ToOcneWLOTEacEfQQOlIQ}">
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/html/JWT.html:389

```
389                 th:action="@{/JWT/kid/delete?token=eyJ0eXAiOiJKV1QiLCJraWQiOiJ3ZWJnb2F0X2tleSIsImFsZyI6IkhTMjU2In0.ewogICJpc3MiOiAiV2ViR29hdCBUb2tlbiBCdWlsZGVyIiwKICAiaWF0IjogMTUyNDIxMDkwNCwKICAiZXhwIjogMTYxODkwNTMwNCwKICAiYXVkIjogIndlYmdvYXQub3JnIiwKICAic3ViIjogImplcnJ5QHdlYmdvYXQuY29tIiwKICAidXNlcm5hbWUiOiAiSmVycnkiLAogICJFbWFpbCI6ICJqZXJyeUB3ZWJnb2F0LmNvbSIsCiAgIlJvbGUiOiBbCiAgICAiQ2F0IgogIF0KfQ.CgZ27DzgVW8gzc0n6izOU638uUCi6UhiOJKYzoEZGE8}">
```

generic.secrets.security.detected-jwt-token.detected-jwt-token CRITICAL

JWT token detected

src/main/resources/lessons/jwt/images/logs.txt:2

```
2  194.201.170.15 - - [28/Jan/2016:21:28:01 +0100] "GET /JWT/refresh/checkout?token=eyJhb
GciOiJIUzUxMiJ9.eyJpYXQiOjE1MjYxMzE0MTEsImV4cCI6MTUyNjIxNzgxMSwiYWRtaW4iOiJmYWxzZSIsInVz
ZXIiOiJUb20ifQ.DCoaq9zQkyDH25EcVWKcdbyVfUL4c9D4jRvsqOqvi9iAd4QuqmKcchfbU8FNzeBNF9tLeFXHZ
LU4yRkq-bjm7Q HTTP/1.1" 401 242 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Ge
cko/20100101 Firefox/60.0" "-"
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/js/quiz.js:34

```
34              document.getElementById("q_container").innerHTML = html;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1189

```
1189              el.innerHTML = fragmentStr;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1206

```
1206              el.innerHTML = fragmentStr;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4011

```
4011      tempElement.innerHTML = "<span></span>" + _convertUrlsToLinks(textNode.data);
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4354

```
4354      try { tempElement.innerHTML = html; } catch(e) {}
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4391

```
4391        tempElement.innerHTML = html;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5999

```
5999          try { node.innerHTML = wysihtml5.INVISIBLE_SPACE; } catch(e) {}
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6202

```
6202              element.innerHTML = wysihtml5.INVISIBLE_SPACE;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6695

```
6695          try { node.innerHTML = wysihtml5.INVISIBLE_SPACE; } catch(e) {}
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7940

```
7940        this.element.innerHTML = browser.displaysCaretInEmptyContentEditableCorrectly
() ? "" : this.CARET_HACK;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7962

```
7962        this.element.innerHTML = html;
```

javascript.browser.security.insecure-document-method.insecure-document-method CRITICAL

User controlled data in methods like `innerHTML`, `outerHTML` or `document.write` is an anti-pattern that can lead to XSS vulnerabilities

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8056

```
8056        this.element.innerHTML  = this.textarea.getValue(true);
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson2.java:4

```
49        ResultSet results = statement.executeQuery(query);
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java:35

```
35    @RequestMapping(path = URL_DEBUG_LABELS_MVC, produces = MediaType.APPLICATION_JSON_
VALUE)
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java:37

```
37            HashingAssignment.SECRETS[new Random().nextInt(HashingAssignment.SECRETS.le
ngth)];
```

java.lang.security.audit.tainted-session-from-http-request.tainted-session-from-http-request HIGH

Detected input from a HTTPServletRequest going into a session command, like `setAttribute`. User input into such a command could lead to an attacker inputting malicious code into your session parameters, blurring the line between what's trusted and untrusted, and therefore leading to a trust boundary violation. This could lead to programmers trusting unvalidated data. Instead, thoroughly sanitize user input before passing it into such function calls.

src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java:39

```
39        request.getSession().setAttribute("basicAuth", basicAuth);
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java:(

```
62          ResultSet results = statement.executeQuery(query);
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java:30

```
30    @RequestMapping(path = "/crypto/hashing/md5", produces = MediaType.TEXT_HTML_VALUE)
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java:1

```
142         statement.executeUpdate(logQuery);
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java:37

```
37        String secret = SECRETS[new Random().nextInt(SECRETS.length)];
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java:6

```
65        statement.execute(queryInjection);
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java:9

```
94      ResultSet results = statement.executeQuery(query);
```

java.lang.security.audit.crypto.use-of-md5.use-of-md5 HIGH

Detected MD5 hash algorithm which is considered insecure. MD5 is not collision resistant and is therefore not suitable as a cryptographic signature. Use HMAC instead.

src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java:39

```
39        MessageDigest md = MessageDigest.getInstance("MD5");
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/lessons/xxe/SimpleXXE.java:77

```
77    @RequestMapping(
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/webwolf/FileServer.java:56

```
56    @RequestMapping(
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java:49

```
49    @RequestMapping(path = "/crypto/hashing/sha256", produces = MediaType.TEXT_HTML_VAL
UE)
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/authbypass/html/AuthBypass.html:23

```
23              <form class="attack-form" accept-charset="UNKNOWN" id="verify-account-for
m"
                  method="POST" name="form"
                  successCallback="onBypassResponse"
                  th:action="@{/auth-bypass/verify-account}">
                <p>Verify Your Account by answering the questions below:</p>

                <p>What is the name of your favorite teacher?</p>
                <input name="secQuestion0" value="" type="TEXT" /><br/>

                <p>What is the name of the street you grew up on?</p>
                <input name="secQuestion1" value="" type="TEXT" /><br/><br />

                <input type="hidden" name="jsEnabled" value="1" />
                <input type="hidden" name="verifyMethod" value="SEC_QUESTIONS" />
                <input type="hidden" name="userId" value="12309746" />

                <input name="submit" value="Submit" type="submit"/>

            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/authbypass/html/AuthBypass.html:43

```
43              <form class="attack-form" accept-charset="UNKNOWN" id="change-password-fo
rm"
                  method="POST" name="form"
                  successCallback="onBypassResponse"
                  th:action="@{/auth-bypass/verify-account}"
                  style="display:none"><!-- start off hidden -->
                <p>Please provide a new password for your account</p>

                <p>Password:</p>
```

```
                <input name="newPassword" value="" type="password" /><br/>

                <p>Confirm Password:</p>
                <input name="newPasswordConfirm" value="" type="password" /><br/><br />

                <input type="hidden" name="userId" value="12309746" />

                <input name="submit" value="Submit" type="submit"/>

            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge1.html:15

```
15                    <form class="attack-form" accept-charset="UNKNOWN"
                        method="POST" name="form"
                        th:action="@{/challenge/1}"
                        style="width: 200px;">

                    <div class="form-group">
                        <label for="exampleInputEmail1" th:text="#{username}">Userna
me</label>
                        <input autofocus="dummy_for_thymeleaf_parser" type="text" cl
ass="form-control"
                               id="exampleInputEmail1" placeholder="Username" name
='username' value="admin"/>
                    </div>
                    <div class="form-group">
                        <label for="exampleInputPassword1" th:text="#{password}">Pas
sword</label>
                        <input type="password" class="form-control" id="exampleInput
Password1"
                               placeholder="Password"
                               name='password'/>
                    </div>
                    <button class="btn btn-primary btn-block" type="submit" th:text
="#{sign.in}">Sign in</button>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge1.html:37

```
37          <form class="attack-form" method="POST" name="form" th:action="@{/challenge/f
lag/1}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="flag"
                           placeholder="a7179f89-906b-4fec-9d99-f15b796e7208"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit flag</button>
                </div>
            </div>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge5.html:69

```
69          <form class="attack-form" method="POST" name="form" th:action="@{/challenge/f
lag/5}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="flag"
                           placeholder="a7179f89-906b-4fec-9d99-f15b796e7208"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit flag</button>
                </div>
            </div>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge6.html:102

```
102          <form class="attack-form" method="POST" name="form" th:action="@{/challenge/
flag/6}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="flag"
                           placeholder="a7179f89-906b-4fec-9d99-f15b796e7208"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit flag</button>
                </div>
            </div>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge7.html:60

```
60          <form class="attack-form" method="POST" name="form" th:action="@{/challenge/f
lag/7}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="flag"
                           placeholder="a7179f89-906b-4fec-9d99-f15b796e7208"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit flag</button>
                </div>
            </div>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/challenges/html/Challenge8.html:234

```
234          <form class="attack-form" method="POST" name="form" th:action="@{/challenge/
flag/8}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="flag"
                           placeholder="a7179f89-906b-4fec-9d99-f15b796e7208"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit flag</button>
                </div>
            </div>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html:25

```
25          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="DOMFollowUp"
              th:action="@{/ChromeDevTools/dummy}">
            <input name="successMessage" value="" type="TEXT" />
            <input name="submitMessage" value="Submit" type="SUBMIT"/>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html:46

```
46          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/ChromeDevTools/network}">
            <script>
                // sample custom javascript in the recommended way ...
                // a namespace has been assigned for it, but you can roll your own if yo
u prefer
                document.getElementById("btn").addEventListener("click", function() {
                    document.getElementById("networkNum").value = Math.random() * 100;
                    document.getElementById("networkNumCopy").value = document.getElemen
tById("networkNum").value;
                });
            </script>
            <input type="hidden" name="networkNum" id="networkNum" value="foo" />
            <table>
                <tr>
                    <td>Click this button to make a request:</td>
                    <td><input id="btn" name="SUBMIT" value="Go!" type="SUBMIT" /></td>
                    <td></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html:67

```
67          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/ChromeDevTools/network}">
            <table>
                <tr>
                    <td>What is the number you found:   </td>
                    <td><input name="number" type="text"/></td>
                    <td><input type="submit" name="Submit" value="check"/></td>
                    <td></td>
                </tr>
            </table>
            <input type="hidden" name="network_num" id="networkNumCopy" value="foo" />
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cia/html/CIA.html:30

```
30              <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN"
                  method="POST" name="form"
                  th:action="@{/cia/quiz}" role="form">
                <div id="q_container"></div>
                <br />
                <input name="Quiz_solutions" value="Submit answers" type="SUBMIT"/>
            </form>
```

html.security.plaintext-http-link.plaintext-http-link HIGH

This link points to a plaintext HTTP URL. Prefer an encrypted HTTPS URL if possible.

src/main/resources/lessons/clientsidefiltering/html/ClientSideFiltering.html:96

```
96                          <h5 style="color:#337ab7"><a href="http://www.samsung.com">Sa
msung</a> ·
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java:55

```
55        String secret = SECRETS[new Random().nextInt(SECRETS.length)];
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/lessons/cryptography/SigningAssignment.java:37

```
37    @RequestMapping(path = "/crypto/signing/getprivate", produces = MediaType.TEXT_HTML
_VALUE)
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cryptography/html/Cryptography.html:31

```
31                      <form class="attack-form" method="POST" name="form"     th:actio
n="@{/crypto/encoding/basic-auth}">
                        Then what was the username
                        <input name="answer_user" value="" type="TEXT"/>
                        and what was the password:
                        <input name="answer_pwd" value="" type="TEXT"/>
                        <input name="SUBMIT" value="post the answer" type="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cryptography/html/Cryptography.html:48

```
48                      <form class="attack-form" method="POST" name="form"     th:actio
n="@{/crypto/encoding/xor}">
                        Suppose you found the database password encoded as {xor}Oz4rPj0+
LDovPiwsKDAtOw==<br/>
                        What would be the actual password
                        <input name="answer_pwd1" value="" type="TEXT"/><br/>
                        <input name="SUBMIT" value="post the answer" type="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cryptography/html/Cryptography.html:65

```
65                      <form class="attack-form" method="POST" name="form"     th:actio
n="@{/crypto/hashing}">
                        Which password belongs to this hash: <div id="md5token" ></div>
```

```
                        <input name="answer_pwd1" value="" type="TEXT"/><br/>
                        Which password belongs to this hash: <div id="sha256token" ></di
v>
                        <input name="answer_pwd2" value="" type="TEXT"/>
                        <input name="SUBMIT" value="post the answer" type="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cryptography/html/Cryptography.html:90

```
90                      <form class="attack-form" method="POST" name="form"     th:actio
n="@{/crypto/signing/verify}">
                        Then what was the modulus of the public key
                        <input name="modulus" value="" type="TEXT"/>
                        and now provide a signature for us based on that modulus
                        <input name="signature" value="" type="TEXT"/>
                        <input name="SUBMIT" value="post the answer" type="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/cryptography/html/Cryptography.html:113

```
113                     <form class="attack-form" method="POST" name="form"     th:actio
n="@{/crypto/secure/defaults}">
                        What is the unencrypted message<br/>
                        <input name="secretText" value="" type="TEXT"/><br/>
                        and what is the name of the file that stored the password <br/>
                        <input name="secretFileName" value="" type="TEXT"/>
                        <input name="SUBMIT" value="post the answer" type="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/csrf/html/CSRF.html:16

```
16      <form accept-charset="UNKNOWN" id="basic-csrf-get"
          method="POST" name="form1"
          target="_blank"
          successCallback=""
          th:action="@{/csrf/basic-get-flag}">
        <input name="csrf" type="hidden" value="false"/>
        <input type="submit" name="submit"/>

    </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/csrf/html/CSRF.html:35

```
35          <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-1"
              method="POST" name="form2"
              successCallback=""
              th:action="@{/csrf/confirm-flag-1}">

            Confirm Flag Value:
            <input type="text" length="6" name="confirmFlagVal" value=""/>

            <input name="submit" value="Submit" type="submit"/>
            <br/>
            <br/>
            <br/>
            <br/>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/csrf/html/CSRF.html:93

```
93                          <form class="attack-form" accept-charset="UNKNOWN" id="cs
rf-review"
                              method="POST" name="review-form"
                              successCallback=""
                              th:action="@{/csrf/review}">
                            <input class="form-control" id="reviewText" name="review
Text" placeholder="Add a Review"
                                   type="text"/>
```

```
                                <input class="form-control" id="reviewStars" name="star
s" type="text"/>

                                <input type="hidden" name="validateReq" value="2aa14227b
9a13d0bede0388a7fba9aa9"/>

                                <input type="submit" name="submit" value="Submit revie
w"/>
                            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/csrf/html/CSRF.html:213

```
213          <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-feedbac
k"
              method="POST" name="form2"
              th:action="@{/csrf/feedback}">

            Confirm Flag Value:
            <input type="text" length="6" name="confirmFlagVal" value=""/>

            <input name="submit" value="Submit" type="submit"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/csrf/html/CSRF.html:237

```
237          <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-login"
              method="POST" name="form2"
              th:action="@{/csrf/login}">

            Press the button below when your are logged in as the other user<br/>

            <input name="submit" value="Solved!" type="submit"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/deserialization/html/InsecureDeserialization.html:26

```
26              <form class="attack-form" accept-charset="UNKNOWN" name="task"
                  method="POST"
                  th:action="@{/InsecureDeserialization/task}">

                <input type="textarea" rows="4" cols="40" value="" name="token" placehol
der="token"/>
                <input type="submit" value="Submit" />

            </form>
```

html.security.audit.missing-integrity.missing-integrity HIGH

This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) you're telling the browser to fetch in the 'integrity' attribute for all externally hosted files.

src/main/resources/lessons/hijacksession/html/HijackSession.html:5

```
5  <link rel="stylesheet" type="text/css"
        href="http://code.jquery.com/ui/1.9.1/themes/base/jquery-ui.css" />
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/hijacksession/templates/hijackform.html:3

```
3               <form class="attack-form" accept-charset="UNKNOWN" method="POST"
                       th:action="@{/HijackSession/login}">
                       <div style="padding: 20px;" id="password-login">
                               <h4 style="border-bottom: 1px solid #c5c5c5;">Account Ac
cess</h4>
                               <fieldset>
                                       <div class="form-group input-group">
                                               <span class="input-group-addon"> <i
                                                       class="glyphicon glyphicon-use
r"></i>
```

```
                                                </span> <input class="form-control" plac
eholder="User name"
                                                       name="username" type="text"></in
put>
                                        </div>
                                        <div class="form-group input-group">
                                                <span class="input-group-addon"><i
                                                       class="glyphicon glyphicon-loc
k"></i></span> <input class="form-control"
                                                       placeholder="Password" name="pas
sword" type="password" />
                                        </div>
                                        <button type="submit" class="btn btn-primary btn
-block">Access</button>
                                </fieldset>
                        </div>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/httpbasics/html/HttpBasics.html:26

```
26                                      <form accept-charset="UNKNOWN" method="POST" nam
e="form"
                                                th:action="@{/#attack/307/100}">
                                                Enter your name: <input name="person" va
lue="" type="TEXT"/><input
                                                       name="SUBMIT" value="Go!" type
="SUBMIT" class="spacing"/>
                                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/httpproxies/html/HttpProxies.html:25

```
25              <form class="attack-form" accept-charset="UNKNOWN" name="intercept-reques
t"
                  method="POST"
                  th:action="@{/HttpProxies/intercept-request}">

                <input type="text" value="doesn't matter really" name="changeMe" />
```

```
            <input type="submit" value="Submit" />

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/idor/html/IDOR.html:23

```
23          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/IDOR/login}">
            <table>
                <tr>
                    <td>user/pass</td>
                    <td>user:<input name="username" value="" type="TEXT" /></td>
                    <td>pass:<input name="password" value="" type="password" /></td>
                    <td>
                        <input
                            name="submit" value="Submit" type="SUBMIT"/>
                    </td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/idor/html/IDOR.html:81

```
81          <form class="attack-form"
              method="POST" name="diff-form"
              th:action="@{/IDOR/diff-attributes}">
            <input name="attributes" type="text" />
            <input name="Submit Diffs" value="Submit Diffs" type="submit" />
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/idor/html/IDOR.html:108

```
108          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/IDOR/profile/alt-path}">
            <div class="adoc-content" th:replace="~{doc:lessons/idor/documentation/IDOR_
inputAltPath.adoc}"></div>
            <input name="url" value="WebGoat/" type="text"/>
            <input name="submit" value="Submit" type="SUBMIT"/>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/insecurelogin/html/InsecureLogin.html:18

```
18              <form class="attack-form" accept-charset="UNKNOWN" name="task"
                  method="POST"
                  th:action="@{/InsecureLogin/task}">

                <button onclick="javascript:submit_secret_credentials();return false;">L
og in</button>

            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/insecurelogin/html/InsecureLogin.html:26

```
26              <form class="attack-form" accept-charset="UNKNOWN" name="task"
                  method="POST"
                  th:action="@{/InsecureLogin/task}">

                <input type="text" value="" name="username" placeholder="username"/>
                <input type="password" value="" name="password" placeholder="password" /
>
                <input type="submit" value="Submit" />

            </form>
```

java.lang.security.audit.object-deserialization.object-deserialization HIGH

Found object deserialization using ObjectInputStream. Deserializing entire Java objects is dangerous because malicious actors can create Java object streams with unintended consequences. Ensure that the objects being deserialized are not user-controlled. If this must be done, consider using HMACs to sign the data stream to make sure it is not tampered with, or consider only transmitting object fields and populating a new object.

src/main/java/org/owasp/webgoat/lessons/deserialization/InsecureDeserializationTask.java:42

```
42      try (ObjectInputStream ois =
        new ObjectInputStream(new ByteArrayInputStream(Base64.getDecoder().decode(b64tok
en)))) {
```

java.lang.security.audit.object-deserialization.object-deserialization HIGH

Found object deserialization using ObjectInputStream. Deserializing entire Java objects is dangerous because malicious actors can create Java object streams with unintended consequences. Ensure that the objects being deserialized are not user-controlled. If this must be done, consider using HMACs to sign the data stream to make sure it is not tampered with, or consider only transmitting object fields and populating a new object.

src/main/java/org/owasp/webgoat/lessons/deserialization/SerializationHelper.java:22

```
22      ObjectInputStream ois = new ObjectInputStream(new ByteArrayInputStream(data));
```

java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly HIGH

A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'

src/main/java/org/owasp/webgoat/lessons/hijacksession/HijackSessionAssignment.java:70

```
70      response.addCookie(cookie);
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/hijacksession/cas/HijackSessionAuthenticationProvide

```
25    private static long id = new Random().nextLong() & Long.MAX_VALUE;
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java:38

```
38        TextCodec.BASE64.encode(SECRETS[new Random().nextInt(SECRETS.length)]);
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java:43

```
43    @RequestMapping(path = "/JWT/secret/gettoken", produces = MediaType.TEXT_HTML_VALU
E)
```

java.servlets.security.cookie-issecure-false.cookie-issecure-false HIGH

Default session middleware settings: `setSecure` not set to true. This ensures that the cookie is sent only over HTTPS to prevent cross-site scripting attacks.

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:114

```
114        Cookie cookie = new Cookie("access_token", token);
```

java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly HIGH

A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:115

```
115         response.addCookie(cookie);
```

java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag HIGH

A cookie was detected without setting the 'secure' flag. The 'secure' flag for cookies prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the 'secure' flag by calling 'cookie.setSecure(true);'

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:115

```
115         response.addCookie(cookie);
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/jwt/html/JWT.html:20

```
20          <form id="decode" class="attack-form" method="POST" name="form" th:action="@
{/JWT/decode}">
            <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidd
en="true"></i></div>
            <br>
            <div class="row">
                <div class="col-lg-10">
                        <span>
                            <span>
                                 Username:
                            </span>
                        <input type="text" name="jwt-encode-user">
                               <button type="SUBMIT">Submit</button>
                            </span>
                </div>
            </div>
            <br>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/jwt/html/JWT.html:125

```
125             <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN"
                 method="POST" name="form"
                 th:action="@{/JWT/quiz}"
                 role="form">
                <div id="q_container"></div>
                <br/>
                <input name="Quiz_solutions" value="Submit answers" type="SUBMIT"/>
            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/jwt/html/JWT.html:158

```
158          <form class="attack-form" method="POST" name="form" th:action="@{/JWT/secre
t}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
hidden="true"
                                                      style="font-size:20px"></i></div>
                    <input type="text" class="form-control" id="flag" name="token"
                           placeholder="XXX.YYY.ZZZ"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit token</button>
                </div>
            </div>

        </form>
```

java.servlets.security.cookie-issecure-false.cookie-issecure-false HIGH

Default session middleware settings: `setSecure` not set to true. This ensures that the cookie is sent only over HTTPS to prevent cross-site scripting attacks.

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:119

```
119        Cookie cookie = new Cookie("access_token", "");
```

java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly HIGH

A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:120

```
120         response.addCookie(cookie);
```

java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag HIGH

A cookie was detected without setting the 'secure' flag. The 'secure' flag for cookies prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the 'secure' flag by calling 'cookie.setSecure(true);'

src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java:120

```
120         response.addCookie(cookie);
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/lessontemplate/html/LessonTemplate.html:48

```
48              <form class="attack-form" accept-charset="UNKNOWN"
                  method="POST" name="form"
                  th:action="@{/lesson-template/sample-attack}">
                <table>
                    <tr>
                        <td>two random params</td>
                        <td>parameter 1:<input name="param1" value="" type="TEXT" /></td
>
                        <td>parameter 2:<input name="param2" value="" type="TEXT" /></td
>
                        <td>
                            <input name="submit" value="Submit" type="SUBMIT"/>
                        </td>
                    </tr>
                </table>
            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/logging/html/LogSpoofing.html:17

```
17          <form class="attack-form" accept-charset="UNKNOWN" name="task"
              method="POST"
              th:action="@{/LogSpoofing/log-spoofing}">

            <input type="text" value="" name="username" placeholder="username"/>
            <input type="password" value="" name="password" placeholder="password"/>
            <input type="submit" value="Submit"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/logging/html/LogSpoofing.html:39

```
39          <form class="attack-form" accept-charset="UNKNOWN" name="task"
              method="POST"
              th:action="@{/LogSpoofing/log-bleeding}">

            <input type="text" value="" name="username" placeholder="username"/>
            <input type="password" value="" name="password" placeholder="password"/>
            <input type="submit" value="Submit"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/missingac/html/MissingFunctionAC.html:53

```
53          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/access-control/hidden-menu}">

            <p>Hidden item 1 <input name="hiddenMenu1" value="" type="TEXT"/></p>
            <p>Hidden item 2 <input name="hiddenMenu2" value="" type="TEXT"/></p>
            <br/>
```

```
        <input name="submit" value="Submit" type="SUBMIT"/>

    </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/missingac/html/MissingFunctionAC.html:76

```
76          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/access-control/user-hash}">

            <p>Your Hash: <input name="userHash" value="" type="TEXT"/></p>
            <br/>
            <input name="submit" value="Submit" type="SUBMIT"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/missingac/html/MissingFunctionAC.html:98

```
98          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/access-control/user-hash-fix}">

            <p>Your Hash: <input name="userHash" value="" type="TEXT"/></p>
            <br/>
            <input name="submit" value="Submit" type="SUBMIT"/>

        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:18

```
18        <form class="attack-form" method="POST" th:action="@{/OpenRedirect/task1}">
        <label for="t1url">Return URL</label>
        <input id="t1url" name="url" placeholder="https://evil.test" value="/home" size
="60" />
        <button type="submit">Simulate Redirect</button>
        <div class="tiny-hint">Provide an absolute external URL using http or https.</di
v>
      </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:33

```
33        <form class="attack-form" method="POST" th:action="@{/OpenRedirect/task2}">
        <label for="t2url">Return URL (substring filter active)</label>
        <input id="t2url" name="url" placeholder="https://webgoat.org.evil.com" size="6
0" />
        <button type="submit">Simulate Redirect</button>
      </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:48

```
48        <form class="attack-form" method="POST" th:action="@{/OpenRedirect/task3}">
        <label for="t3target">Target URL</label>
        <input id="t3target" name="target" placeholder="https://webgoat.local@evil.com"
size="55" />
        <label for="t3token">Tracking Token</label>
        <input id="t3token" name="token" value="abc123" size="15" />
        <button type="submit">Simulate Redirect</button>
      </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:64

```
64        <form class="attack-form" method="POST" th:action="@{/OpenRedirect/task4}">
        <label for="t4target">Target URL (double-encoded)</label>
        <input
          id="t4target"
          name="target"
          placeholder="Double-encoded target URL (e.g. https://example%2540attacker.tes
t)"
          size="60"
        />
        <button id="task4-autofill" type="button" data-sample="https://webgoat.local%254
0evil.com">
          Autofill sample
        </button>
        <button type="submit">Simulate Redirect</button>
      </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:100

```
100         <form id="quiz-form" class="attack-form" method="POST" th:action="@{/OpenRed
irect/quiz}" role="form">
          <div id="q_container"></div>
          <br />
          <input name="Quiz_solutions" value="Submit answers" type="SUBMIT" />
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/openredirect/html/OpenRedirect.html:116

```
116        <form class="attack-form" method="POST" th:action="@{/OpenRedirect/mitigatio
n}">
        <label for="mitigationUrl">External URL to test mitigation</label>
        <input id="mitigationUrl" name="url" placeholder="https://evil.test" size="60" /
>
        <button type="submit">Test Mitigation</button>
        <div class="tiny-hint">Try an absolute external URL (http/https) that is NOT an
internal host.</div>
      </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/passwordreset/html/PasswordReset.html:144

```
144          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              action="PasswordReset/SecurityQuestions">
            <select name="question">
                <option>What is your favorite animal?</option>
                <option>In what year was your mother born?</option>
                <option>What was the time you were born?</option>
                <option>What is the name of the person you first kissed?</option>
                <option>What was the house number and street name you lived in as a chil
d?</option>
                <option>In what town or city was your first full time job?</option>
                <option>In what city were you born?</option>
                <option>On which wrist do you were your watch?</option>
                <option>What was the last name of your favorite teacher in grade three?
</option>
                <option>What is the name of a college/job you applied to but didn't atte
nd?</option>
                <option>What are the last 5 digits of your drivers license?</option>
                <option>What was your childhood nickname?</option>
                <option>Who was your childhood hero?</option>
                <option>What is your favorite color?</option>
            </select>
            <input name="Check Question" value="check" type="SUBMIT"/>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/passwordreset/templates/password_reset.html:12

```
12              <form role="form" method="POST" th:action="@{/PasswordReset/reset/change-
password}" th:object="${form}" novalidate="novalidate">
                <h2 class="sign_up_title">Reset your password</h2>
                    <div class="form-group" th:classappend="${#fields.hasErrors('passwor
d')}? 'has-error'">
                        <input type="hidden" name="resetLink" th:field="*{resetLink}" />
                        <label for="password" class="control-label" th:text="#{passwor
d}">Password</label>
                        <input type="password" class="form-control" id="password" placeh
```

```
older="Password"
                                name='password' th:value="*{password}"/>
                        <span th:if="${#fields.hasErrors('password')}" th:errors="*{pass
word}">Password error</span>
                    </div>
                <div class="row">
                    <div class="col-xs-12 col-md-12">
                        <button type="submit" class="btn btn-success btn-block btn-lg">S
ave</button>
                    </div>
                </div>
            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/pathtraversal/html/PathTraversal.html:192

```
192              <form class="attack-form" method="POST" name="form" action="PathTraversa
l/random">
                <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
                <div class="form-group">
                    <div class="input-group">
                        <div class="input-group-addon"><i class="fa fa-flag-checkered" a
ria-hidden="true"
                                                          style="font-size:20px"></i></d
iv>
                        <input type="text" class="form-control" id="pathTraversalSecret"
name="secret"/>
                    </div>
                    <div class="input-group" style="margin-top: 10px">
                        <button type="submit" class="btn btn-primary">Submit secret</but
ton>
                    </div>
                </div>

            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/securepasswords/html/SecurePasswords.html:21

```
21          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SecurePasswords/assignment}"
              autocomplete="off">

            <div class="input-group input-group">
                <input id="myInput" name="password" value="" type="password" class="form
-control"
                       placeholder="Enter a secure password..."
                       aria-describedby="password-label">
                <span class="input-group-addon"><input type="checkbox" onclick="javascri
pt:myFunction()"/> Show password</span>
            </div>
            <div class="input-group" style="margin-top: 10px">
                <button type="submit" class="btn btn-primary">Submit</button>
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/securitymisconfiguration/html/SecurityMisconfiguration.html:18

```
18          <form class="attack-form" method="POST" th:action="@{/SecurityMisconfiguratio
n/task1}">
          <div class="form-group">
            <label for="username">Username</label>
            <input class="form-control" id="username" name="username" placeholder="Try t
he default admin username" autocomplete="username" />
          </div>
          <div class="form-group">
            <label for="password">Password</label>
            <input class="form-control" id="password" name="password" type="password" pl
aceholder="And the matching default password" autocomplete="current-password" />
          </div>
          <button type="submit" class="btn btn-primary btn-block" style="margin-top:10p
x;">Attempt login</button>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/securitymisconfiguration/html/SecurityMisconfiguration.html:47

```
47          <form class="attack-form" method="POST" th:action="@{/SecurityMisconfiguratio
n/task2}" style="margin-top:15px;">
          <div class="form-group">
            <label for="token">Leaked token</label>
            <input class="form-control" id="token" name="token" placeholder="Paste the t
oken from the stack trace" autocomplete="off" />
          </div>
          <button type="submit" class="btn btn-primary btn-block" style="margin-top:10p
x;">Submit token</button>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/securitymisconfiguration/html/SecurityMisconfiguration.html:72

```
72          <form class="attack-form" method="POST" th:action="@{/SecurityMisconfiguratio
n/task3}" style="margin-top:15px;">
          <div class="form-group">
            <label for="apiKey">System API key</label>
            <input class="form-control" id="apiKey" name="apiKey" placeholder="Paste the
leaked key" autocomplete="off" />
          </div>
          <button type="submit" class="btn btn-primary btn-block" style="margin-top:10p
x;">Submit key</button>
        </form>
```

html.security.audit.missing-integrity.missing-integrity HIGH

This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) you're telling the browser to fetch in the 'integrity' attribute for all externally hosted files.

src/main/resources/lessons/spoofcookie/html/SpoofCookie.html:5

```
5  <link rel="stylesheet" type="text/css"
        href="http://code.jquery.com/ui/1.9.1/themes/base/jquery-ui.css" />
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:16

```
16          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack2}"
              autocomplete="off">
            <table>
                <tr>
                    <td><label>SQL query</label></td>
                    <td width="100%"><input class="form-control" name="query" value="" t
ype="TEXT" placeholder="SQL query"/></td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Submit</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:40

```
40          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack3}"
              autocomplete="off">
            <table>
                <tr>
                    <td><label>SQL query</label></td>
                    <td width="100%"><input class="form-control" name="query" value="" t
ype="TEXT" placeholder="SQL query"/></td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Submit</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:64

```
64          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack4}"
              autocomplete="off">
            <table>
                <tr>
                    <td><label>SQL query</label></td>
                    <td width="100%"><input class="form-control" name="query" value="" t
ype="TEXT" placeholder="SQL query"/></td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Submit</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:88

```
88          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack5}"
              autocomplete="off">
            <table>
                <tr>
                    <td><label>SQL query</label></td>
                    <td width="100%"><input class="form-control" name="query" value="" t
ype="TEXT" placeholder="SQL query"/></td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Submit</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:189

```
189          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/assignment5b}">
            <table>
                <tr>
                    <td>Login_Count:</td>
                    <td><input name="login_count" type="text" required="true"/></td>
                </tr>
                <tr>
                    <td>User_Id:</td>
                    <td><input name="userid" type="TEXT" required="true"/></td>
                </tr>
                <tr>
                    <td></td>
                    <td><input
                            name="Get Account Info" value="Get Account Info" type="SUBMI
T"/></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:217

```
217          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack8}"
              autocomplete="off">
            <table>
                <tr>
                    <td><label>Employee Name:</label></td>
                    <td><input name="name" value="" type="TEXT" placeholder="Lastname"/>
</td>
                </tr>
                <tr>
                    <td><label>Authentication TAN:</label></td>
                    <td><input name="auth_tan" value="" type="TEXT" placeholder="TAN"/>
```

```
</td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Get department</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:245

```
245          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack9}"
              autocomplete="off">
             <table>
                <tr>
                    <td><label>Employee Name:</label></td>
                    <td><input name="name" value="" type="TEXT" placeholder="Lastname"/>
</td>
                </tr>
                <tr>
                    <td><label>Authentication TAN:</label></td>
                    <td><input name="auth_tan" value="" type="TEXT" placeholder="TAN"/>
</td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Get department</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjection.html:274

```
274          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjection/attack10}"
              autocomplete="off">
```

```
            <table>
                <tr>
                    <td><label>Action contains:</label></td>
                    <td><input name="action_string" value="" type="TEXT" placeholder="En
ter search string"/></td>
                </tr>
                <tr>
                    <td><button type="SUBMIT">Search logs</button></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html:21

```
21          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjectionAdvanced/attack6a}">
            <table>
                <tr>
                    <td>Name:</td>
                    <td><input name="userid_6a" value="" type="TEXT"/></td>
                    <td><input
                            name="Get Account Info" value="Get Account Info" type="SUBMI
T"/></td>
                    <td></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html:34

```
34          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlInjectionAdvanced/attack6b}">
            <table>
                <tr>
                    <td>Password:</td>
```

```
                    <td><input name="userid_6b" value="" type="TEXT"/></td>
                    <td><input
                            name="Check Dave's Password:" value="Check Password" type="S
UBMIT"/></td>
                    <td></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html:169

```
169                 <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN"
                     method="POST" name="form"
                     th:action="@{/SqlInjectionAdvanced/quiz}"
                     role="form">
                    <div id="q_container"></div>
                    <br />
                <input name="Quiz_solutions" value="Submit answers" type="SUBMIT"/>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html:26

```
26          <form class="attack-form" accept-charset="UNKNOWN" method="POST" name="form"
th:action="@{/SqlInjectionMitigations/attack10a}">
            <div>
                <p>Connection conn = DriverManager.<input type="text" name="field1" id
="field1" />(DBURL, DBUSER, DBPW);</p>
                <p><input type="text" name="field2" id="field2" /> = conn.<input type="t
ext" name="field3" id="field3" />("SELECT status FROM users WHERE name=<input type="tex
t" name="field4" id="field4" /> AND mail=<input type="text" name="field5" id="field5" /
>");</p>
                <p><input type="text" name="field6" id="field6" />;</p>
                <p><input type="text" name="field7" id="field7" />;</p>
            </div>
            <div class="input-group" style="margin-top: 10px">
                <button type="submit" class="btn btn-primary">Submit</button>
```

```
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html:45

```
45          <form id="codesubmit" style="height: 100%; min-height: 300px;" class="attack-
form" accept-charset="UNKNOWN" method="POST" name="form" th:action="@{/SqlInjectionMitig
ations/attack10b}">
            <div>
                <div id="editor" style="position: absolute; top: 0; right: 0; bottom: 0;
left: 0; height: 300px;" name="editor"></div>
                <script th:src="@{/js/libs/ace.js}" type="text/javascript" charset="utf-
8"></script>
                <script th:src="@{/lesson_js/assignment10b.js}" type="text/javascript" c
harset="utf-8"></script>
            </div>
            <input type="hidden" name="editor"/>
            <div class="input-group" style="position: absolute; top: 310px;">
                <button class="btn btn-primary" type="submit">Submit</button>
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html:73

```
73          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlOnlyInputValidation/attack}"
              enctype="application/json;charset=UTF-8">
            <table>
                <tr>
                    <td>Name:</td>
                    <td><input name="userid_sql_only_input_validation" value="" type="TE
XT"/></td>
                    <td><input
                            name="Get Account Info" value="Get Account Info" type="SUBMI
T"/></td>
                    <td></td>
```

```
            </tr>
        </table>
    </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html:96

```
96          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              th:action="@{/SqlOnlyInputValidationOnKeywords/attack}"
              enctype="application/json;charset=UTF-8">
            <table>
                <tr>
                    <td>Name:</td>
                    <td><input name="userid_sql_only_input_validation_on_keywords" value
="" type="TEXT"/></td>
                    <td><input
                            name="Get Account Info" value="Get Account Info" type="SUBMI
T"/></td>
                    <td></td>
                </tr>
            </table>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html:176

```
176          <form class="attack-form" method="POST" name="form" th:action="@{/SqlInjecti
onMitigations/attack12a}">
            <div class="form-group">
                <div class="input-group">
                    <div class="input-group-addon">IP address webgoat-prd server:</div>
                    <input type="text" class="form-control" id="ip" name="ip"
                           placeholder="192.1.0.12"/>
                </div>
                <div class="input-group" style="margin-top: 10px">
                    <button type="submit" class="btn btn-primary">Submit</button>
                </div>
```

```
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/ssrf/html/SSRF.html:13

```
13              <form class="attack-form" accept-charset="UNKNOWN"
                  method="POST" name="form"
                  th:action="@{/SSRF/task1}">
                <table>
                    <tr>
                        <td><input type="hidden" id="url1" name="url" value="images/tom.
png"/></td>

                        <td><input
                                name="Steal the Cheese" value="Steal the Cheese" type="S
UBMIT"/></td>
                        <td></td>
                    </tr>
                </table>
            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/ssrf/html/SSRF.html:35

```
35              <form class="attack-form" accept-charset="UNKNOWN"
                  method="POST" name="form"
                  th:action="@{/SSRF/task2}">
                <table>
                    <tr>
                        <td><input type="hidden" id="url2" name="url" value="images/cat.
png"/></td>

                        <td><input
                                name="try this" value="try this" type="SUBMIT"/></td>
                        <td></td>
                    </tr>
                </table>
            </form>
```

html.security.audit.missing-integrity.missing-integrity HIGH

This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) you're telling the browser to fetch in the 'integrity' attribute for all externally hosted files.

src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html:5

```
5      <link rel="stylesheet" type="text/css" href="http://code.jquery.com/ui/1.9.1/theme
s/base/jquery-ui.css" />
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html:104

```
104                                 <form accept-charset="UNKNOWN" method="POST" nam
e="form"
                                            action="#attack/307/100">
                                            <table>
                                                    <tr>
                                                            <td>Enter the contact's
xml representation:</td>
                                                            <td><textarea name="payl
oad" value="" type="TEXT" rows="15" cols="60"/></td>
                                                            <td><input name="SUBMIT"
value="Go!" type="SUBMIT"/></td>
                                                    </tr>
                                            </table>
                                    </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html:19

```
19          <form class="attack-form" accept-charset="UNKNOWN"  style="position:relative;
top:150px"
              method="POST" name="form"
```

```
            th:action="@{/WebWolf/mail}">
        <div class="container-fluid">
            <div class="row">
                <div class="col-md-4">
                    <div class="input-group">
                        <input type="text" class="form-control"
                               placeholder="Type in your unique code"
                               name='uniqueCode'/>
                        <div class="input-group-btn">
                            <button class="btn btn-primary" type="submit">Go</button
>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html:40

```
40          <form class="attack-form" accept-charset="UNKNOWN"  style="position:relative;
top:-50px"
              method="POST" name="secondform"
              th:action="@{/WebWolf/mail/send}">
            <div class="container-fluid">
                <div class="row">
                    <div class="col-md-4">
                        <div class="form-group input-group">
          <span class="input-group-addon">
            @
          </span>
                            <input class="form-control" th:attr="placeholder=${username
+ '@webgoat.org'}" name="email" type="email"
                                   required=""/>
                        </div>
                        <button type="submit" class="btn btn-primary btn-block" id="btn-
login">
                            Send e-mail
                        </button>
                    </div>
                </div>
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html:77

```
77          <form class="attack-form" accept-charset="UNKNOWN"
              method="POST" name="form"
              action="WebWolf/landing">
            <div class="container-fluid">
                <div class="row">
                    <div class="col-md-4">
                        <div class="input-group">
                            <input type="text" class="form-control"
                                   placeholder="Type in your unique code"
                                   name='uniqueCode'/>
                            <div class="input-group-btn">
                                <button class="btn btn-primary" type="submit">Go</button
>
                            </div>
                        </div>
                    </div>
                </div>
            </div>
        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScripting.html:13

```
13                      <form class="attack-form" accept-charset="UNKNOWN"
                                method="POST" name="form"
                                th:action="@{/CrossSiteScripting/attack1}">
                              <table>
                                    <tr>
                                            <td><input type="checkbox" name="checkbo
xAttack1"> The cookies are the same on each tab </td>
                                            <td><input
                                                        name="answer" value="Sub
mit" type="SUBMIT"/></td>
                                            <td></td>
                                    </tr>
```

```
                    </table>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScripting.html:134

```
134             <form class="attack-form" accept-charset="UNKNOWN"
                      method="POST" name="DOMTestRoute"
                      th:action="@{/CrossSiteScripting/attack6a}">
                    <input name="DOMTestRoute" value="" type="TEXT" />
                    <input name="SubmitTestRoute" value="Submit" type="SUBMIT"/>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScripting.html:149

```
149             <form class="attack-form" accept-charset="UNKNOWN"
                      method="POST" name="DOMFollowUp"
                      th:action="@{/CrossSiteScripting/dom-follow-up}">
                    <input name="successMessage" value="" type="TEXT" />
                    <input name="submitMessage" value="Submit" type="SUBMIT"/>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScripting.html:169

```
169                 <form id="quiz-form" class="attack-form" accept-charset="UNKNOW
N"
                          method="POST" name="form"
                          th:action="@{/CrossSiteScripting/quiz}" role="form">
                        <div id="q_container"></div>
                        <br />
                        <input name="Quiz_solutions" value="Submit answers" type
```

```
="SUBMIT"/>
                        </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html:24

```
24              <form id="codesubmit" style="height: 100%; min-height: 350px;" class="at
tack-form" accept-charset="UNKNOWN" method="POST" name="form" th:action="@{/CrossSiteScr
ipting/attack3}">
                        <div>
                                <div id="editor" style="position: absolute; top: 0; righ
t: 0; bottom: 0; left: 0; height: 350px;" name="editor"></div>
                                <script th:src="@{/js/libs/ace.js}" type="text/javascrip
t" charset="utf-8"></script>
                                <script th:src="@{/lesson_js/assignment3.js}" type="tex
t/javascript" charset="utf-8"></script>
                        </div>
                        <input type="hidden" name="editor"/>
                        <div class="input-group" style="position: absolute; top: 365p
x;">
                                <button class="btn btn-primary" type="submit">Submit</bu
tton>
                        </div>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html:44

```
44              <form id="codesubmit2" style="height: 100%; min-height: 350px;" class="a
ttack-form" accept-charset="UNKNOWN" method="POST" name="form" th:action="@{/CrossSiteSc
ripting/attack4}">
                        <div>
                                <div id="editor2" style="position: absolute; top: 0; rig
ht: 0; bottom: 0; left: 0; height: 350px;" name="editor2"></div>
                                <script th:src="@{/js/libs/ace.js}" type="text/javascrip
t" charset="utf-8"></script>
                                <script th:src="@{/lesson_js/assignment4.js}" type="tex
t/javascript" charset="utf-8"></script>
                        </div>
```

```
                        <input type="hidden" name="editor2"/>
                        <div class="input-group" style="position: absolute; top: 365p
x;">
                                <button class="btn btn-primary" type="submit">Submit</bu
tton>
                        </div>
                </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/lessons/xss/html/CrossSiteScriptingStored.html:68

```
68              <form class="attack-form" accept-charset="UNKNOWN"
                        method="POST" name="DOMFollowUp"
                        th:action="@{/CrossSiteScriptingStored/stored-xss-follow-up}">
                      <input name="successMessage" value="" type="TEXT" />
                      <input name="submitMessage" value="Submit" type="SUBMIT"/>
                </form>
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `t` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/backbone-min.js:1

```
1  (function(t){var e=typeof self=="object"&&self.self===self&&self||typeof global=="obje
ct"&&global.global===global&&global;if(typeof define==="function"&&define.amd){define
(["underscore","jquery","exports"],function(i,n,r){e.Backbone=t(e,r,i,n)})}else if(typeo
f exports!=="undefined"){var i=require("underscore"),n;try{n=require("jquery")}catch(r)
{}t(e,exports,i,n)}else{e.Backbone=t(e,{},e._,e.jQuery||e.Zepto||e.ender||e.$)}})(functi
on(t,e,i,n){var r=t.Backbone;var s=Array.prototype.slice;e.VERSION="1.4.0";e.$=n;e.noCon
flict=function(){t.Backbone=r;return this};e.emulateHTTP=false;e.emulateJSON=false;var a
=e.Events={};var o=/\s+/;var h;var u=function(t,e,n,r,s){var a=0,h;if(n&&typeof n==="obj
ect"){if(r!==void 0&&"context"in s&&s.context===void 0)s.context=r;for(h=i.keys(n);a<h.l
ength;a++){e=u(t,e,h[a],n[h[a]],s)}}else if(n&&o.test(n)){for(h=n.split(o);a<h.length;a+
+){e=t(e,h[a],r,s)}}else{e=t(e,n,r,s)}return e};a.on=function(t,e,i){this._events=u(l,th
is._events||{},t,e,{context:i,ctx:this,listening:h});if(h){var n=this._listeners||(this.
_listeners={});n[h.id]=h;h.interop=false}return this};a.listenTo=function(t,e,n){if(!t)r
```

```
eturn this;var r=t._listenId||(t._listenId=i.uniqueId("l"));var s=this._listeningTo||(th
is._listeningTo={});var a=h=s[r];if(!a){this._listenId||(this._listenId=i.uniqueId
("l"));a=h=s[r]=new g(this,t)}var o=c(t,e,n,this);h=void 0;if(o)throw o;if(a.interop)a.o
n(e,n);return this};var l=function(t,e,i,n){if(i){var r=t[e]||(t[e]=[]);var s=n.context,
a=n.ctx,o=n.listening;if(o)o.count++;r.push({callback:i,context:s,ctx:s||a,listening:
o})}return t};var c=function(t,e,i,n){try{t.on(e,i,n)}catch(r){return r}};a.off=function
(t,e,i){if(!this._events)return this;this._events=u(f,this._events,t,e,{context:i,listen
ers:this._listeners});return this};a.stopListening=function(t,e,n){var r=this._listening
To;if(!r)return this;var s=t?[t._listenId]:i.keys(r);for(var a=0;a<s.length;a++){var o=r
[s[a]];if(!o)break;o.obj.off(e,n,this);if(o.interop)o.off(e,n)}if(i.isEmpty(r))this._lis
teningTo=void 0;return this};var f=function(t,e,n,r){if(!t)return;var s=r.context,a=r.li
steners;var o=0,h;if(!e&&!s&&!n){for(h=i.keys(a);o<h.length;o++){a[h[o]].cleanup()}retur
n}h=e?[e]:i.keys(t);for(;o<h.length;o++){e=h[o];var u=t[e];if(!u)break;var l=[];for(var
c=0;c<u.length;c++){var f=u[c];if(n&&n≠=f.callback&&n≠=f.callback._callback||s&&s≠=f.
context){l.push(f)}else{var d=f.listening;if(d)d.off(e,n)}}if(l.length){t[e]=l}else{dele
te t[e]}}return t};a.once=function(t,e,i){var n=u(d,{},t,e,this.off.bind(this));if(typeo
f t===="string"&&i==null)e=void 0;return this.on(n,e,i)};a.listenToOnce=function(t,e,i){v
ar n=u(d,{},e,i,this.stopListening.bind(this,t));return this.listenTo(t,n)};var d=functi
on(t,e,n,r){if(n){var s=t[e]=i.once(function(){r(e,s);n.apply(this,arguments)});s._callb
ack=n}return t};a.trigger=function(t){if(!this._events)return this;var e=Math.max(0,argu
ments.length-1);var i=Array(e);for(var n=0;n<e;n++)i[n]=arguments[n+1];u(v,this._events,
t,void 0,i);return this};var v=function(t,e,i,n){if(t){var r=t[e];var s=t.all;if(r&&s)s=
s.slice();if(r)p(r,n);if(s)p(s,[e].concat(n))}return t};var p=function(t,e){var i,n=-1,r
=t.length,s=e[0],a=e[1],o=e[2];switch(e.length){case 0:while(++n<r)(i=t[n]).callback.cal
l(i.ctx);return;case 1:while(++n<r)(i=t[n]).callback.call(i.ctx,s);return;case 2:while(+
+n<r)(i=t[n]).callback.call(i.ctx,s,a);return;case 3:while(++n<r)(i=t[n]).callback.call
(i.ctx,s,a,o);return;default:while(++n<r)(i=t[n]).callback.apply(i.ctx,e);return}};var g
=function(t,e){this.id=t._listenId;this.listener=t;this.obj=e;this.interop=true;this.cou
nt=0;this._events=void 0};g.prototype.on=a.on;g.prototype.off=function(t,e){var i;if(thi
s.interop){this._events=u(f,this._events,t,e,{context:void 0,listeners:void 0});i=!this.
_events}else{this.count--;i=this.count===0}if(i)this.cleanup()};g.prototype.cleanup=func
tion(){delete this.listener._listeningTo[this.obj._listenId];if(!this.interop)delete thi
s.obj._listeners[this.id]};a.bind=a.on;a.unbind=a.off;i.extend(e,a);var m=e.Model=functi
on(t,e){var n=t||{};e||(e={});this.preinitialize.apply(this,arguments);this.cid=i.unique
Id(this.cidPrefix);this.attributes={};if(e.collection)this.collection=e.collection;if(e.
parse)n=this.parse(n,e)||{};var r=i.result(this,"defaults");n=i.defaults(i.extend({},r,
n),r);this.set(n,e);this.changed={};this.initialize.apply(this,arguments)};i.extend(m.pr
ototype,a,{changed:null,validationError:null,idAttribute:"id",cidPrefix:"c",preinitializ
e:function(){},initialize:function(){},toJSON:function(t){return i.clone(this.attribute
s)},sync:function(){return e.sync.apply(this,arguments)},get:function(t){return this.att
ributes[t]},escape:function(t){return i.escape(this.get(t))},has:function(t){return thi
s.get(t)≠=null},matches:function(t){return!!i.iteratee(t,this)(this.attributes)},set:fun
ction(t,e,n){if(t==null)return this;var r;if(typeof t==="object"){r=t;n=e}else{(r={})[t]
=e}n||(n={});if(!this._validate(r,n))return false;var s=n.unset;var a=n.silent;var o=[];
var h=this._changing;this._changing=true;if(!h){this._previousAttributes=i.clone(this.at
tributes);this.changed={}}var u=this.attributes;var l=this.changed;var c=this._previousA
ttributes;for(var f in r){e=r[f];if(!i.isEqual(u[f],e))o.push(f);if(!i.isEqual(c[f],e))
{l[f]=e}else{delete l[f]}s?delete u[f]:u[f]=e}if(this.idAttribute in r)this.id=this.get
(this.idAttribute);if(!a){if(o.length)this._pending=n;for(var d=0;d<o.length;d++){this.t
rigger("change:"+o[d],this,u[o[d]],n)}}if(h)return this;if(!a){while(this._pending){n=th
is._pending;this._pending=false;this.trigger("change",this,n)}}this._pending=false;this.
```

_changing=false;return this},unset:function(t,e){return this.set(t,void 0,i.extend({},e,{unset:true}))},clear:function(t){var e={};for(var n in this.attributes)e[n]=void 0;return this.set(e,i.extend({},t,{unset:true}))},hasChanged:function(t){if(t==null)return!i.isEmpty(this.changed);return i.has(this.changed,t)},changedAttributes:function(t){if(!t)return this.hasChanged()?i.clone(this.changed):false;var e=this._changing?this._previousAttributes:this.attributes;var n={};var r;for(var s in t){var a=t[s];if(i.isEqual(e[s],a))continue;n[s]=a;r=true}return r?n:false},previous:function(t){if(t==null||!this._previousAttributes)return null;return this._previousAttributes[t]},previousAttributes:function(){return i.clone(this._previousAttributes)},fetch:function(t){t=i.extend({parse:true},t);var e=this;var n=t.success;t.success=function(i){var r=t.parse?e.parse(i,t):i;if(!e.set(r,t))return false;if(n)n.call(t.context,e,i,t);e.trigger("sync",e,i,t)};G(this,t);return this.sync("read",this,t)},save:function(t,e,n){var r;if(t==null||typeof t==="object"){r=t;n=e}else{(r={})[t]=e}n=i.extend({validate:true,parse:true},n);var s=n.wait;if(r&&!s){if(!this.set(r,n))return false}else if(!this._validate(r,n)){return false}var a=this;var o=n.success;var h=this.attributes;n.success=function(t){a.attributes=h;var e=n.parse?a.parse(t,n):t;if(s)e=i.extend({},r,e);if(e&&!a.set(e,n))return false;if(o)o.call(n.context,a,t,n);a.trigger("sync",a,t,n)};G(this,n);if(r&&s)this.attributes=i.extend({},h,r);var u=this.isNew()?"create":n.patch?"patch":"update";if(u==="patch"&&!n.attrs)n.attrs=r;var l=this.sync(u,this,n);this.attributes=h;return l},destroy:function(t){t=t?i.clone(t):{};var e=this;var n=t.success;var r=t.wait;var s=function(){e.stopListening();e.trigger("destroy",e,e.collection,t)};t.success=function(i){if(r)s();if(n)n.call(t.context,e,i,t);if(!e.isNew())e.trigger("sync",e,i,t)};var a=false;if(this.isNew()){i.defer(t.success)}else{G(this,t);a=this.sync("delete",this,t)}if(!r)s();return a},url:function(){var t=i.result(this,"urlRoot")||i.result(this.collection,"url")||V();if(this.isNew())return t;var e=this.get(this.idAttribute);return t.replace(/[^\/]$/,"$&/")+encodeURIComponent(e)},parse:function(t,e){return t},clone:function(){return new this.constructor(this.attributes)},isNew:function(){return!this.has(this.idAttribute)},isValid:function(t){return this._validate({},i.extend({},t,{validate:true}))},_validate:function(t,e){if(!e.validate||!this.validate)return true;t=i.extend({},this.attributes,t);var n=this.validationError=this.validate(t,e)||null;if(!n)return true;this.trigger("invalid",this,n,i.extend(e,{validationError:n}));return false}});var _=e.Collection=function(t,e){e||(e={});this.preinitialize.apply(this,arguments);if(e.model)this.model=e.model;if(e.comparator!==void 0)this.comparator=e.comparator;this._reset();this.initialize.apply(this,arguments);if(t)this.reset(t,i.extend({silent:true},e))};var y={add:true,remove:true,merge:true};var b={add:true,remove:false};var x=function(t,e,i){i=Math.min(Math.max(i,0),t.length);var n=Array(t.length-i);var r=e.length;var s;for(s=0;s<n.length;s++)n[s]=t[s+i];for(s=0;s<r;s++)t[s+i]=e[s];for(s=0;s<n.length;s++)t[s+r+i]=n[s]};i.extend(_.prototype,a,{model:m,preinitialize:function(){},initialize:function(){},toJSON:function(t){return this.map(function(e){return e.toJSON(t)})},sync:function(){return e.sync.apply(this,arguments)},add:function(t,e){return this.set(t,i.extend({merge:false},e,b))},remove:function(t,e){e=i.extend({},e);var n=!i.isArray(t);t=n?[t]:t.slice();var r=this._removeModels(t,e);if(!e.silent&&r.length){e.changes={added:[],merged:[],removed:r};this.trigger("update",this,e)}return n?r[0]:r},set:function(t,e){if(t==null)return;e=i.extend({},y,e);if(e.parse&&!this._isModel(t)){t=this.parse(t,e)||[]}var n=!i.isArray(t);t=n?[t]:t.slice();var r=e.at;if(r!=null)r=+r;if(r>this.length)r=this.length;if(r<0)r+=this.length+1;var s=[];var a=[];var o=[];var h=[];var u={};var l=e.add;var c=e.merge;var f=e.remove;var d=false;var v=this.comparator&&r==null&&e.sort!==false;var p=i.isString(this.comparator)?this.comparator:null;var g,m;for(m=0;m<t.length;m++){g=t[m];var _=this.get(g);if(_){if(c&&g!==_){var b=this._isModel(g)?g.attributes:g;if(e.parse)b=_.parse(b,e);_.set(b,e);o.push(_);if(v&&!d)d=_.hasChanged(p)}if(!u[_.cid]){u[_.cid]=true;s.push(_)}t[m]=_}else if(l){g=t[m]=this._prepareModel(g,e);if(g){a.push(g);this._addReference(g,e);u[g.cid]=true;s.push(g)}}}if(f){for(m

=0;m<this.length;m++){g=this.models[m];if(!u[g.cid])h.push(g)}if(h.length)this._removeMo
dels(h,e)}var w=false;var E=!v&&l&&f;if(s.length&&E){w=this.length!==s.length||i.some(th
is.models,function(t,e){return t!==s[e]});this.models.length=0;x(this.models,s,0);this.l
ength=this.models.length}else if(a.length){if(v)d=true;x(this.models,a,r==null?this.leng
th:r);this.length=this.models.length}if(d)this.sort({silent:true});if(!e.silent){for(m=
0;m<a.length;m++){if(r!=null)e.index=r+m;g=a[m];g.trigger("add",g,this,e)}if(d||w)this.t
rigger("sort",this,e);if(a.length||h.length||o.length){e.changes={added:a,removed:h,merg
ed:o};this.trigger("update",this,e)}}return n?t[0]:t},reset:function(t,e){e=e?i.clone
(e):{};for(var n=0;n<this.models.length;n++){this._removeReference(this.models[n],e)}e.p
reviousModels=this.models;this._reset();t=this.add(t,i.extend({silent:true},e));if(!e.si
lent)this.trigger("reset",this,e);return t},push:function(t,e){return this.add(t,i.exten
d({at:this.length},e))},pop:function(t){var e=this.at(this.length-1);return this.remove
(e,t)},unshift:function(t,e){return this.add(t,i.extend({at:0},e))},shift:function(t){va
r e=this.at(0);return this.remove(e,t)},slice:function(){return s.apply(this.models,argu
ments)},get:function(t){if(t==null)return void 0;return this._byId[t]||this._byId[this.m
odelId(this._isModel(t)?t.attributes:t)]||t.cid&&this._byId[t.cid]},has:function(t){retu
rn this.get(t)!=null},at:function(t){if(t<0)t+=this.length;return this.models[t]},where:
function(t,e){return this[e?"find":"filter"](t)},findWhere:function(t){return this.where
(t,true)},sort:function(t){var e=this.comparator;if(!e)throw new Error("Cannot sort a se
t without a comparator");t||(t={});var n=e.length;if(i.isFunction(e))e=e.bind(this);if(n
===1||i.isString(e)){this.models=this.sortBy(e)}else{this.models.sort(e)}if(!t.silent)th
is.trigger("sort",this,t);return this},pluck:function(t){return this.map(t+"")},fetch:fu
nction(t){t=i.extend({parse:true},t);var e=t.success;var n=this;t.success=function(i){va
r r=t.reset?"reset":"set";n[r](i,t);if(e)e.call(t.context,n,i,t);n.trigger("sync",n,i,
t)};G(this,t);return this.sync("read",this,t)},create:function(t,e){e=e?i.clone(e):{};va
r n=e.wait;t=this._prepareModel(t,e);if(!t)return false;if(!n)this.add(t,e);var r=this;v
ar s=e.success;e.success=function(t,e,i){if(n)r.add(t,i);if(s)s.call(i.context,t,e,i)};
t.save(null,e);return t},parse:function(t,e){return t},clone:function(){return new this.
constructor(this.models,{model:this.model,comparator:this.comparator})},modelId:function
(t){return t[this.model.prototype.idAttribute||"id"]},values:function(){return new E(thi
s,k)},keys:function(){return new E(this,I)},entries:function(){return new E(this,S)},_re
set:function(){this.length=0;this.models=[];this._byId={}},_prepareModel:function(t,e){i
f(this._isModel(t)){if(!t.collection)t.collection=this;return t}e=e?i.clone(e):{};e.coll
ection=this;var n=new this.model(t,e);if(!n.validationError)return n;this.trigger("inval
id",this,n.validationError,e);return false},_removeModels:function(t,e){var i=[];for(var
n=0;n<t.length;n++){var r=this.get(t[n]);if(!r)continue;var s=this.indexOf(r);this.model
s.splice(s,1);this.length--;delete this._byId[r.cid];var a=this.modelId(r.attributes);if
(a!=null)delete this._byId[a];if(!e.silent){e.index=s;r.trigger("remove",r,this,e)}i.pus
h(r);this._removeReference(r,e)}return i},_isModel:function(t){return t instanceof m},_a
ddReference:function(t,e){this._byId[t.cid]=t;var i=this.modelId(t.attributes);if(i!=nul
l)this._byId[i]=t;t.on("all",this._onModelEvent,this)},_removeReference:function(t,e){de
lete this._byId[t.cid];var i=this.modelId(t.attributes);if(i!=null)delete this._byId[i];
if(this===t.collection)delete t.collection;t.off("all",this._onModelEvent,this)},_onMode
lEvent:function(t,e,i,n){if(e){if((t==="add"||t==="remove")&&i!==this)return;if(t==="des
troy")this.remove(e,n);if(t==="change"){var r=this.modelId(e.previousAttributes());var s
=this.modelId(e.attributes);if(r!==s){if(r!=null)delete this._byId[r];if(s!=null)this._b
yId[s]=e}}}this.trigger.apply(this,arguments)}});var w=typeof Symbol==="function"&&Symbo
l.iterator;if(w){_.prototype[w]=_.prototype.values}var E=function(t,e){this._collection=
t;this._kind=e;this._index=0};var k=1;var I=2;var S=3;if(w){E.prototype[w]=function(){re
turn this}}E.prototype.next=function(){if(this._collection){if(this._index<this._collect
ion.length){var t=this._collection.at(this._index);this._index++;var e;if(this._kind===

k){e=t}else{var i=this._collection.modelId(t.attributes);if(this._kind===I){e=i}else{e=[i,t]}}return{value:e,done:false}}this._collection=void 0}return{value:void 0,done:true}};var T=e.View=function(t){this.cid=i.uniqueId("view");this.preinitialize.apply(this,arguments);i.extend(this,i.pick(t,H));this._ensureElement();this.initialize.apply(this,arguments)};var P=/^(\S+)\s*(.*)$/;var H=["model","collection","el","id","attributes","className","tagName","events"];i.extend(T.prototype,a,{tagName:"div",$:function(t){return this.$el.find(t)},preinitialize:function(){},initialize:function(){},render:function(){return this},remove:function(){this._removeElement();this.stopListening();return this},_removeElement:function(){this.$el.remove()},setElement:function(t){this.undelegateEvents();this._setElement(t);this.delegateEvents();return this},_setElement:function(t){this.$el=t instanceof e.$?t:e.$(t);this.el=this.$el[0]},delegateEvents:function(t){t||(t=i.result(this,"events"));if(!t)return this;this.undelegateEvents();for(var e in t){var n=t[e];if(!i.isFunction(n))n=this[n];if(!n)continue;var r=e.match(P);this.delegate(r[1],r[2],n.bind(this))}return this},delegate:function(t,e,i){this.$el.on(t+".delegateEvents"+this.cid,e,i);return this},undelegateEvents:function(){if(this.$el)this.$el.off(".delegateEvents"+this.cid);return this},undelegate:function(t,e,i){this.$el.off(t+".delegateEvents"+this.cid,e,i);return this},_createElement:function(t){return document.createElement(t)},_ensureElement:function(){if(!this.el){var t=i.extend({},i.result(this,"attributes"));if(this.id)t.id=i.result(this,"id");if(this.className)t["class"]=i.result(this,"className");this.setElement(this._createElement(i.result(this,"tagName")));this._setAttributes(t)}else{this.setElement(i.result(this,"el"))}},_setAttributes:function(t){this.$el.attr(t)}});var $=function(t,e,i,n){switch(e){case 1:return function(){return t[i](this[n])};case 2:return function(e){return t[i](this[n],e)};case 3:return function(e,r){return t[i](this[n],C(e,this),r)};case 4:return function(e,r,s){return t[i](this[n],C(e,this),r,s)};default:return function(){var e=s.call(arguments);e.unshift(this[n]);return t[i].apply(t,e)}}};var A=function(t,e,n,r){i.each(n,function(i,n){if(e[n])t.prototype[n]=$(e,i,n,r)})};var C=function(t,e){if(i.isFunction(t))return t;if(i.isObject(t)&&!e._isModel(t))return R(t);if(i.isString(t))return function(e){return e.get(t)};return t};var R=function(t){var e=i.matches(t);return function(t){return e(t.attributes)}};var M={forEach:3,each:3,map:3,collect:3,reduce:0,foldl:0,inject:0,reduceRight:0,foldr:0,find:3,detect:3,filter:3,select:3,reject:3,every:3,all:3,some:3,any:3,include:3,includes:3,contains:3,invoke:0,max:3,min:3,toArray:1,size:1,first:3,head:3,take:3,initial:3,rest:3,tail:3,drop:3,last:3,without:0,difference:0,indexOf:3,shuffle:1,lastIndexOf:3,isEmpty:1,chain:1,sample:3,partition:3,groupBy:3,countBy:3,sortBy:3,indexBy:3,findIndex:3,findLastIndex:3};var N={keys:1,values:1,pairs:1,invert:1,pick:0,omit:0,chain:1,isEmpty:1};i.each([[_,M,"models"],[m,N,"attributes"]],function(t){var e=t[0],n=t[1],r=t[2];e.mixin=function(t){var n=i.reduce(i.functions(t),function(t,e){t[e]=0;return t},{});A(e,t,n,r)};A(e,i,n,r)});e.sync=function(t,n,r){var s=j[t];i.defaults(r||(r={}),{emulateHTTP:e.emulateHTTP,emulateJSON:e.emulateJSON});var a={type:s,dataType:"json"};if(!r.url){a.url=i.result(n,"url")||V()}if(r.data==null&&n&&(t==="create"||t==="update"||t==="patch")){a.contentType="application/json";a.data=JSON.stringify(r.attrs||n.toJSON(r))}if(r.emulateJSON){a.contentType="application/x-www-form-urlencoded";a.data=a.data?{model:a.data}:{}}if(r.emulateHTTP&&(s==="PUT"||s==="DELETE"||s==="PATCH")){a.type="POST";if(r.emulateJSON)a.data._method=s;var o=r.beforeSend;r.beforeSend=function(t){t.setRequestHeader("X-HTTP-Method-Override",s);if(o)return o.apply(this,arguments)}}if(a.type!=="GET"&&!r.emulateJSON){a.processData=false}var h=r.error;r.error=function(t,e,i){r.textStatus=e;r.errorThrown=i;if(h)h.call(r.context,t,e,i)};var u=r.xhr=e.ajax(i.extend(a,r));n.trigger("request",n,u,r);return u};var j={create:"POST",update:"PUT",patch:"PATCH","delete":"DELETE",read:"GET"};e.ajax=function(){return e.$.ajax.apply(e.$,arguments)};var O=e.Router=function(t){t||(t={});this.preinitialize.apply(this,arguments);if(t.routes)this.routes=t.routes;this._bindRoutes();this.initialize.apply(this,arguments)};var U=/\((.*?)\)/g;var z=/(\(\?)?:\w+/g;var q

```
=/\*\w+/g;var F=/[\-{}\[\]+?.,\\\^$|#\s]/g;i.extend(O.prototype,a,{preinitialize:functio
n(){},initialize:function(){},route:function(t,n,r){if(!i.isRegExp(t))t=this._routeToReg
Exp(t);if(i.isFunction(n)){r=n;n=""}if(!r)r=this[n];var s=this;e.history.route(t,functio
n(i){var a=s._extractParameters(t,i);if(s.execute(r,a,n)!==false){s.trigger.apply(s,["ro
ute:"+n].concat(a));s.trigger("route",n,a);e.history.trigger("route",s,n,a)}});return th
is},execute:function(t,e,i){if(t)t.apply(this,e)},navigate:function(t,i){e.history.navig
ate(t,i);return this},_bindRoutes:function(){if(!this.routes)return;this.routes=i.result
(this,"routes");var t,e=i.keys(this.routes);while((t=e.pop())!=null){this.route(t,this.r
outes[t])}},_routeToRegExp:function(t){t=t.replace(F,"\\$&").replace(U,"(?:$1)?").replac
e(z,function(t,e){return e?t:"([^/?]+)"}).replace(q,"([^?]*?)");return new RegExp("^"+t
+"(?:\\?([\\s\\S]*))?$")},_extractParameters:function(t,e){var n=t.exec(e).slice(1);retu
rn i.map(n,function(t,e){if(e===n.length-1)return t||null;return t?decodeURIComponent
(t):null})}});var B=e.History=function(){this.handlers=[];this.checkUrl=this.checkUrl.bi
nd(this);if(typeof window!=="undefined"){this.location=window.location;this.history=wind
ow.history}};var J=/^[#\/]|\s+$/g;var L=/^\/+|\/+$/g;var W=/#.*$/;B.started=false;i.exte
nd(B.prototype,a,{interval:50,atRoot:function(){var t=this.location.pathname.replace(/[^
\/]$/,"$&/");return t===this.root&&!this.getSearch()},matchRoot:function(){var t=this.de
codeFragment(this.location.pathname);var e=t.slice(0,this.root.length-1)+"/";return e===
this.root},decodeFragment:function(t){return decodeURI(t.replace(/%25/g,"%2525"))},getSe
arch:function(){var t=this.location.href.replace(/#.*/,"").match(/\?.+/);return t?t
[0]:""},getHash:function(t){var e=(t||this).location.href.match(/#(.*)$/);return e?e
[1]:""},getPath:function(){var t=this.decodeFragment(this.location.pathname+this.getSear
ch()).slice(this.root.length-1);return t.charAt(0)==="/"?t.slice(1):t},getFragment:funct
ion(t){if(t==null){if(this._usePushState||!this._wantsHashChange){t=this.getPath()}else
{t=this.getHash()}}return t.replace(J,"")},start:function(t){if(B.started)throw new Erro
r("Backbone.history has already been started");B.started=true;this.options=i.extend({roo
t:"/"},this.options,t);this.root=this.options.root;this._wantsHashChange=this.options.ha
shChange!==false;this._hasHashChange="onhashchange"in window&&(document.documentMode===v
oid 0||document.documentMode>7);this._useHashChange=this._wantsHashChange&&this._hasHash
Change;this._wantsPushState=!!this.options.pushState;this._hasPushState=!!(this.history&
&this.history.pushState);this._usePushState=this._wantsPushState&&this._hasPushState;thi
s.fragment=this.getFragment();this.root=("/"+this.root+"/").replace(L,"/");if(this._want
sHashChange&&this._wantsPushState){if(!this._hasPushState&&!this.atRoot()){var e=this.ro
ot.slice(0,-1)||"/";this.location.replace(e+"#"+this.getPath());return true}else if(thi
s._hasPushState&&this.atRoot()){this.navigate(this.getHash(),{replace:true})}}if(!this._
hasHashChange&&this._wantsHashChange&&!this._usePushState){this.iframe=document.createEl
ement("iframe");this.iframe.src="javascript:0";this.iframe.style.display="none";this.ifr
ame.tabIndex=-1;var n=document.body;var r=n.insertBefore(this.iframe,n.firstChild).conte
ntWindow;r.document.open();r.document.close();r.location.hash="#"+this.fragment}var s=wi
ndow.addEventListener||function(t,e){return attachEvent("on"+t,e)};if(this._usePushStat
e){s("popstate",this.checkUrl,false)}else if(this._useHashChange&&!this.iframe){s("hashc
hange",this.checkUrl,false)}else if(this._wantsHashChange){this._checkUrlInterval=setInt
erval(this.checkUrl,this.interval)}if(!this.options.silent)return this.loadUrl()},stop:f
unction(){var t=window.removeEventListener||function(t,e){return detachEvent("on"+t,e)};
if(this._usePushState){t("popstate",this.checkUrl,false)}else if(this._useHashChange&&!t
his.iframe){t("hashchange",this.checkUrl,false)}if(this.iframe){document.body.removeChil
d(this.iframe);this.iframe=null}if(this._checkUrlInterval)clearInterval(this._checkUrlIn
terval);B.started=false},route:function(t,e){this.handlers.unshift({route:t,callback:
e})},checkUrl:function(t){var e=this.getFragment();if(e===this.fragment&&this.iframe){e=
this.getHash(this.iframe.contentWindow)}if(e===this.fragment)return false;if(this.ifram
e)this.navigate(e);this.loadUrl()},loadUrl:function(t){if(!this.matchRoot())return fals
```

e;t=this.fragment=this.getFragment(t);return i.some(this.handlers,function(e){if(e.rout
e.test(t)){e.callback(t);return true}})},navigate:function(t,e){if(!B.started)return fal
se;if(!e||e===true)e={trigger:!!e};t=this.getFragment(t||"");var i=this.root;if(t===""||
t.charAt(0)==="?"){i=i.slice(0,-1)||"/"}var n=i+t;t=t.replace(W,"");var r=this.decodeFra
gment(t);if(this.fragment===r)return;this.fragment=r;if(this._usePushState){this.history
[e.replace?"replaceState":"pushState"]({},document.title,n)}else if(this._wantsHashChang
e){this._updateHash(this.location,t,e.replace);if(this.iframe&&t!==this.getHash(this.ifr
ame.contentWindow)){var s=this.iframe.contentWindow;if(!e.replace){s.document.open();s.d
ocument.close()}this._updateHash(s.location,t,e.replace)}}else{return this.location.assi
gn(n)}if(e.trigger)return this.loadUrl(t)},_updateHash:function(t,e,i){if(i){var n=t.hre
f.replace(/(javascript:|#).*$/,"");t.replace(n+"#"+e)}else{t.hash="#"+e}}});e.history=ne
w B;var D=function(t,e){var n=this;var r;if(t&&i.has(t,"constructor")){r=t.constructor}e
lse{r=function(){return n.apply(this,arguments)}}i.extend(r,n,e);r.prototype=i.create(n.
prototype,t);r.prototype.constructor=r;r.__super__=n.prototype;return r};m.extend=_.exte
nd=O.extend=T.extend=B.extend=D;var V=function(){throw new Error('A "url" property or fu
nction must be specified')};var G=function(t,e){var i=e.error;e.error=function(n){if(i)
i.call(e.context,t,n,e);t.trigger("error",t,n,e)}};return e});

javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop HIGH

Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-existence of certain attributes, or uses pre-defined attributes of object prototype (such as hasOwnProperty, toString or valueOf). Possible mitigations might be: freezing the object prototype, using an object without prototypes (via Object.create(null)), blocking modifications of attributes that resolve to object prototype, using Map instead of object.

src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js:622

```
622                                 curOption = curOption[ parts[ i ] ];
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `commentRegex` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/mode-java.js:573

```
573          this.foldingStartMarker = new RegExp(
            this.foldingStartMarker.source.replace(/\|[^|]*?$/, "|" + commentRegex.star
t)
        );
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `commentRegex` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/mode-java.js:576

```
576          this.foldingStopMarker = new RegExp(
            this.foldingStopMarker.source.replace(/\|[^|]*?$/, "|" + commentRegex.end)
        );
```

javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop HIGH

Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-existence of certain attributes, or uses pre-defined attributes of object prototype (such as hasOwnProperty, toString or valueOf). Possible mitigations might be: freezing the object prototype, using an object without prototypes (via Object.create(null)), blocking modifications of attributes that resolve to object prototype, using Map instead of object.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6

```
6  var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!=m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
```

unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);case 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)return t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return function(n){return null==n?void 0:n[r]}}function x(n,r){return null≠n&&o.call(n,r)}function S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.iteratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==typeof r&&0⩽r&&r⩽A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}function N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++){var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3⩽arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o-1;for(e||(t=n[u?u[i]:i],i+=f);0⩽i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void 0≠=e&&-1≠=e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t){e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"≠typeof t||e)&&(t=0),0⩽ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)return;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"≠typeof n[0]&&null≠n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null≠(t=n[a])&&o<t&&(o=t);else e=b(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}function K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):On(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t){x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udfff]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.call(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z(n,r,t,e){er(r)||(e=t,t=r,r=!1),null≠t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i++){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(function(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0⩽u&&u<e;u+=o)if(r(n[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}function cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0⩽t?t:Math.max(t+u,e):u=0⩽t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-1;if(r≠r)return 0⩽(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0⩽t&&t<u;t+=o)if(n[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}v

```
ar vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a functio
n");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,
o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=
o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn
(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!
1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){va
r e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return
n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(thi
s,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arg
uments)),n<=1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toS
tring"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnPropert
y","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototy
pe||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]!==u[o]&&!D
(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t i
n n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];fo
r(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=
Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.l
ength;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&
r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if
(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f
(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0!==n[a]||(n[a]=e[a])}return n}}var kn=Nn
(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r
(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t=
{},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!
1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}ret
urn t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N
(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn
(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(n
ull==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]!==u[i]||!(i in u))re
turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0!==n||1/n==1/r;if(null==n||null==
r)return!1;if(n!=n)return r!=r;var u=typeof n;return("function"===u||"object"===u||"obje
ct"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._w
rapped);var u=s.call(n);if(u!==s.call(r))return!1;switch(u){case"[object RegExp]":case"
[object String]":return""+n==""+r;case"[object Number]":return+n!=+n?+r!=+r:0==+n?1/+n==
1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbo
l]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("o
bject"!=typeof n||"object"!=typeof r)return!1;var i=n.constructor,a=r.constructor;if(i!=
=a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in
r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.pus
h(n),e.push(r),o){if((f=n.length)!==r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))re
turn!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!==f)return!1;for(;f--;)if(c=l[f],!x
(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){re
turn function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln
(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn
("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Erro
r"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!functio
n(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.docume
nt.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[o
bject Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function
(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}fun
ction ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=
```

```
typeof/./&&"object"≠typeof Int8Array&&"function"≠typeof rr&&(Cn=function(n){return"fun
ction"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr=
{"&":"&amp;","<":"&lt;",">":"&gt;",'"':"&quot;","'":"&#x27;","`":"&#x60;"},lr=Mn(cr);fun
ction pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=Reg
Exp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var s
r=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interp
olate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr=
{"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|
\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).c
hain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=functi
on(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["po
p","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototyp
e[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"==r&&"splice"==
r||0!=n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r
=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.pr
ototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.
prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSIO
N:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:
I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return
R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,plu
ck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},m
ax:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"≠t
ypeof n[0]&&null≠n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null≠(t=n[a])&&t<o&&
(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});
return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;r
eturn e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort
(function(n,r){var t=n.criteria,e=r.criteria;if(t≠e){if(e<t||void 0===t)return 1;if(t<
e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,
toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},siz
e:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,ta
ke:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r
||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n)
{return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,
union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){va
r o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return
r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?
t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,i
ndexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for
(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chun
k:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call
(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function
(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,a
rguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,
i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i
=a=null)},n=function(){var n=fr();c||!1!=u.leading||(c=n);var r=e-(n-c);return i=this,a
=arguments,r<=0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!
1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=
i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,
r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(t
his,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=nu
ll},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e
```

```
=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call
(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,a
rguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b
(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return
o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r
[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findK
ey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},c
lone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,
r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn
(n).length)},isElement:function(n){return!(!n||1!==n.nodeType)},isArray:Kn,isObject:Ln,i
sArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isS
ymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&
l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUnd
efined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var
t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},i
dentity:ur,constant:function(n){return function(){return n}},noop:function(){},property:
or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r
[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);
for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:fu
nction(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u
<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return
n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:funct
ion(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).sou
rce,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+
='";o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,
r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':
__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a
+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arg
uments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n)
{throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";retur
n u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!
0,r},mixin:_r});return wr._=wr});
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `r` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6

```
6  var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
```

```
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!==m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments
[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);c
ase 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e
[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)re
turn t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return funct
ion(n){return null==n?void 0:n[r]}}function x(n,r){return null!=n&&o.call(n,r)}function
S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.i
teratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==
typeof r&&0<=r&&r<=A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e
++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}fu
nction N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++)
{var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3
<=arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o
-1;for(e||(t=n[u?u[i]:i],i+=f);0<=i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}
(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void
0!==e&&-1!==e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t)
{e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).leng
th,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b
(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))
return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"!=typeof t||e)&&(t
=0),0<=ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-
1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)re
turn;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function
P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"!=typeof n[0]&&nu
ll!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&o<t&&(o=t);else e=b
(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}fun
ction K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):O
n(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];
e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],
[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function
(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t)
{x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udff
f]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.l
ength<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.cal
l(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||
t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if
(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=
e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z
(n,r,t,e){er(r)||(e=t,t=r,r=!1),null!=t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i+
+){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push
(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(fun
ction(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var
r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function
un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0<=u&&u<e;u+=o)if(r(n
```

```
[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b
(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}func
tion cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0⩽t?t:
Math.max(t+u,e):u=0⩽t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-
1;if(r!=r)return 0⩽(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0⩽t&&t<u;t+=o)if(n
[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e
instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}v
ar vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a functio
n");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,
o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=
o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn
(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!
1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){va
r e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return
n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(this
s,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arg
uments)),n⩽1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toS
tring"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnPropert
y","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototy
pe||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]!=u[o]&&!D
(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t i
n n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];fo
r(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=
Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.l
ength;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&
r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if
(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f
(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0!=n[a]||(n[a]=e[a])}return n}}var kn=Nn
(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r
(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t=
{},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!
1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}ret
urn t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N
(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn
(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(n
ull==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]!=u[i]||!(i in u))re
turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0!=n||1/n==1/r;if(null==n||null==
r)return!1;if(n!=n)return r!=r;var u=typeof n;return("function"===u||"object"===u||"obje
ct"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._w
rapped);var u=s.call(n);if(u!=s.call(r))return!1;switch(u){case"[object RegExp]":case"
[object String]":return""+n==""+r;case"[object Number]":return+n!=+n?+r!=+r:0==+n?1/+n==
1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbo
l]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("o
bject"!=typeof n||"object"!=typeof r)return!1;var i=n.constructor,a=r.constructor;if(i!
=a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in
r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.pus
h(n),e.push(r),o){if((f=n.length)!=r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))re
turn!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!=f)return!1;for(;f--;)if(c=l[f],!x
(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){re
turn function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln
(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn
```

("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Erro
r"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!functio
n(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.docume
nt.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[o
bject Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function
(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}fun
ction ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=
typeof/./&&"object"!=typeof Int8Array&&"function"!=typeof rr&&(Cn=function(n){return"fun
ction"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr=
{"&":"&","<":"<",">":">",'"':""","'":"'","`":"`"},lr=Mn(cr);fun
ction pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=Reg
Exp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var s
r=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interp
olate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr=
{"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|
\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).c
hain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=functi
on(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["po
p","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototyp
e[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"!==r&&"splice"!==
r||0!==n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r
=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.pr
ototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.
prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSIO
N:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:
I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return
R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,plu
ck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},m
ax:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"!=t
ypeof n[0]&&null!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&t<o&&
(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});
return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;r
eturn e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort
(function(n,r){var t=n.criteria,e=r.criteria;if(t!==e){if(e<t||void 0===t)return 1;if(t<
e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,
toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},siz
e:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,ta
ke:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r
||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n)
{return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,
union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){va
r o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return
r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?
t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,i
ndexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for
(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chun
k:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call
(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function
(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,a
rguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,
i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i

```
=a=null)},n=function(){var n=fr();c||!1≠=u.leading||(c=n);var r=e-(n-c);return i=this,a
=arguments,r⩽0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!
1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=
i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,
r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(t
his,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=nu
ll},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e
=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call
(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,a
rguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b
(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return
o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r
[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findK
ey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},c
lone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,
r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn
(n).length)},isElement:function(n){return!(!n||1≠=n.nodeType)},isArray:Kn,isObject:Ln,i
sArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isS
ymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&
l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUnd
efined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var
t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},i
dentity:ur,constant:function(n){return function(){return n}},noop:function(){},property:
or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r
[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);
for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:fu
nction(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u
<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return
n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:funct
ion(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).sou
rce,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+
='";o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,
r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':
__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a
+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arg
uments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n)
{throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";retur
n u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!
0,r},mixin:_r});return wr._=wr});
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `r` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6

```
6  var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!==m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments
[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);c
ase 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e
[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)re
turn t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return funct
ion(n){return null==n?void 0:n[r]}}function x(n,r){return null!=n&&o.call(n,r)}function
S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.i
teratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==
typeof r&&0<=r&&r<=A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e
++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}fu
nction N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++)
{var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3
<=arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o
-1;for(e||(t=n[u?u[i]:i],i+=f);0<=i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}
(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void
0!==e&&-1!==e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t)
{e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).leng
th,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b
(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))
return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"!=typeof t||e)&&(t
=0),0<=ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-
1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)re
turn;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function
P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"!=typeof n[0]&&nu
ll!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&o<t&&(o=t);else e=b
(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}fun
ction K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):O
n(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];
e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],
[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function
(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t)
{x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udff
f]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.l
ength<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.cal
l(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||
t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if
(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=
```

```
e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z
(n,r,t,e){er(r)||(e=t,t=r,r=!1),null≠t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i+
+){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push
(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(fun
ction(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var
r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function
un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0⩽u&&u<e;u+=o)if(r(n
[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b
(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}func
tion cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0⩽t?t:
Math.max(t+u,e):u=0⩽t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-
1;if(r≠r)return 0⩽(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0⩽t&&t<u;t+=o)if(n
[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e
instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}v
ar vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a functio
n");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,
o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=
o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn
(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!
1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){va
r e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return
n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(thi
s,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arg
uments)),n⩽1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toS
tring"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnPropert
y","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototy
pe||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]≠u[o]&&!D
(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t i
n n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];fo
r(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=
Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.l
ength;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&
r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if
(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f
(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0≠n[a]||(n[a]=e[a])}return n}}var kn=Nn
(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r
(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t=
{},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!
1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}ret
urn t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N
(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn
(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(n
ull==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]≠u[i]||!(i in u))re
turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0≠n||1/n==1/r;if(null==n||null==
r)return!1;if(n≠n)return r≠r;var u=typeof n;return("function"===u||"object"===u||"obje
ct"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._w
rapped);var u=s.call(n);if(u≠s.call(r))return!1;switch(u){case"[object RegExp]":case"
[object String]":return""+n==""+r;case"[object Number]":return+n≠+n?+r≠+r:0==+n?1/+n==
1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbo
l]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("o
bject"≠typeof n||"object"≠typeof r)return!1;var i=n.constructor,a=r.constructor;if(i≠
```

```
=a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in
r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.pus
h(n),e.push(r),o){if((f=n.length)!=r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))re
turn!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!=f)return!1;for(;f--;)if(c=l[f],!x
(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){re
turn function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln
(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn
("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Erro
r"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!functio
n(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.docume
nt.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[o
bject Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function
(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}fun
ction ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=
typeof/./&&"object"!=typeof Int8Array&&"function"!=typeof rr&&(Cn=function(n){return"fun
ction"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr=
{"&":"&amp;","<":"&lt;",">":"&gt;",'"':"&quot;","'":"&#x27;","`":"&#x60;"},lr=Mn(cr);fun
ction pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=Reg
Exp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var s
r=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interp
olate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr=
{"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|
\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).c
hain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=functi
on(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["po
p","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototyp
e[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"!=r&&"splice"!=
r||0!=n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r
=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.pr
ototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.
prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSIO
N:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:
I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return
R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,plu
ck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},m
ax:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"!=t
ypeof n[0]&&null!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&t<o&&
(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});
return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;r
eturn e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort
(function(n,r){var t=n.criteria,e=r.criteria;if(t!=e){if(e<t||void 0===t)return 1;if(t<
e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,
toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},siz
e:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,ta
ke:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r
||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n)
{return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,
union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){va
r o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return
r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?
t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,i
```

ndexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chunk:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,arguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i=a=null)},n=function(){var n=fr();c||!1!==u.leading||(c=n);var r=e-(n-c);return i=this,a=arguments,r<=0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(this,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=null},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,arguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findKey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},clone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn(n).length)},isElement:function(n){return!(!n||1!==n.nodeType)},isArray:Kn,isObject:Ln,isArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isSymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUndefined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},identity:ur,constant:function(n){return function(){return n}},noop:function(){},property:or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:function(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:function(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).source,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+='";o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arguments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n){throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";return u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!0,r},mixin:_r});return wr._=wr});

javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop

HIGH

Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-existence of certain attributes, or uses pre-defined attributes of object prototype (such as hasOwnProperty, toString or valueOf). Possible mitigations might be: freezing the object prototype, using an object without prototypes (via Object.create(null)), blocking modifications of attributes that resolve to object prototype, using Map instead of object.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6


```
6  var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!=m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments
[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);c
ase 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e
[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)re
turn t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return funct
ion(n){return null==n?void 0:n[r]}}function x(n,r){return null!=n&&o.call(n,r)}function
S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.i
teratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==
typeof r&&0<=r&&r<=A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e
++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}fu
nction N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++)
{var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3
<=arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o
-1;for(e||(t=n[u?u[i]:i],i+=f);0<=i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}
(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void
0!==e&&-1!==e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t)
{e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).leng
th,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b
(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))
return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"!=typeof t||e)&&(t
=0),0<=ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-
1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)re
turn;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function
P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"!=typeof n[0]&&nu
ll!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&o<t&&(o=t);else e=b
(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}fun
ction K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):O
n(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];
e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],
```

[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t){x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udfff]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.call(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z(n,r,t,e){er(r)||(e=t,t=r,r=!1),null!=t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i++){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(function(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0<=u&&u<e;u+=o)if(r(n[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}function cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0<=t?t:Math.max(t+u,e):u=0<=t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-1;if(r!=r)return 0<=(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0<=t&&t<u;t+=o)if(n[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}var vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a function");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){var e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(this,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arguments)),n<=1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toString"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnProperty","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototype||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]!==u[o]&&!D(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t in n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];for(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.length;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0===n[a]||(n[a]=e[a])}return n}}var kn=Nn(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t={},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}return t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(null==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]!==u[i]||!(i in u))re

turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0!==n||1/n==1/r;if(null==n||null==r)return!1;if(n!=n)return r!=r;var u=typeof n;return("function"===u||"object"===u||"object"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._wrapped);var u=s.call(n);if(u!==s.call(r))return!1;switch(u){case"[object RegExp]":case"[object String]":return""+n==""+r;case"[object Number]":return+n!=+n?+r!=+r:0==+n?1/+n==1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbol]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("object"!=typeof n||"object"!=typeof r)return!1;var i=n.constructor,a=r.constructor;if(i!==a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.push(n),e.push(r),o){if((f=n.length)!==r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))return!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!==f)return!1;for(;f--;)if(c=l[f],!x(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){return function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Error"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!function(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.document.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[object Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}function ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=typeof/./&&"object"!=typeof Int8Array&&"function"!=typeof rr&&(Cn=function(n){return"function"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr={"&":"&","<":"<",">":">",'"':""","'":"'","`":"`"},lr=Mn(cr);function pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=RegExp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var sr=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interpolate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr={"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).chain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=function(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["pop","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototype[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"!==r&&"splice"!==r||0!==n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.prototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSION:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,pluck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},max:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"!=typeof n[0]&&null!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&t<o&&(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;return e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort(function(n,r){var t=n.criteria,e=r.criteria;if(t!==e){if(e<t||void 0===t)return 1;if(t<e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},siz

```
e:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,ta
ke:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r
||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n)
{return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,
union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){va
r o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return
r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?
t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,i
ndexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for
(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chun
k:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call
(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function
(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,a
rguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,
i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i
=a=null)},n=function(){var n=fr();c||!1!==u.leading||(c=n);var r=e-(n-c);return i=this,a
=arguments,r<=0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!
1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=
i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,
r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(t
his,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=nu
ll},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e
=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call
(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,a
rguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b
(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return
o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r
[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findK
ey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},c
lone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,
r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn
(n).length)},isElement:function(n){return!(!n||1!==n.nodeType)},isArray:Kn,isObject:Ln,i
sArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isS
ymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&
l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUnd
efined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var
t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},i
dentity:ur,constant:function(n){return function(){return n}},noop:function(){},property:
or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r
[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);
for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:fu
nction(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u
<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return
n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:funct
ion(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).sou
rce,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+
='';o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,
r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':
__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a
+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arg
uments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n)
```

```
{throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";retur
n u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!
0,r},mixin:_r});return wr._=wr});
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `n` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6

```
6  var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!=m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments
[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);c
ase 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e
[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)re
turn t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return funct
ion(n){return null==n?void 0:n[r]}}function x(n,r){return null!=n&&o.call(n,r)}function
S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.i
teratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==
typeof r&&0<=r&&r<=A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e
++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}fu
nction N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++)
{var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3
<=arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o
-1;for(e||(t=n[u?u[i]:i],i+=f);0<=i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}
(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void
0!==e&&-1!==e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t)
{e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).leng
th,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b
(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))
return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"!=typeof t||e)&&(t
=0),0<=ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-
1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)re
```

```
turn;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function
P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"≠typeof n[0]&&nu
ll≠n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null≠(t=n[a])&&o<t&&(o=t);else e=b
(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}fun
ction K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):O
n(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];
e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],
[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function
(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t)
{x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udff
f]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.l
ength<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.cal
l(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||
t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if
(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=
e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z
(n,r,t,e){er(r)||(e=t,t=r,r=!1),null≠t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i+
+){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push
(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(fun
ction(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var
r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function
un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0⩽u&&u<e;u+=o)if(r(n
[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b
(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}func
tion cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0⩽t?t:
Math.max(t+u,e):u=0⩽t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-
1;if(r≠r)return 0⩽(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0⩽t&&t<u;t+=o)if(n
[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e
instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}v
ar vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a functio
n");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,
o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=
o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn
(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!
1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){va
r e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return
n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(thi
s,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arg
uments)),n⩽1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toS
tring"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnPropert
y","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototy
pe||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]≠u[o]&&!D
(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t i
n n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];fo
r(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=
Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.l
ength;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&
r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if
(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f
(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0≠n[a]||(n[a]=e[a])}return n}}var kn=Nn
(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r
```

(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t=
{},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!
1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}ret
urn t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N
(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn
(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(n
ull==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]!==u[i]||!(i in u))re
turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0!==n||1/n==1/r;if(null==n||null==
r)return!1;if(n!=n)return r!=r;var u=typeof n;return("function"===u||"object"===u||"obje
ct"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._w
rapped);var u=s.call(n);if(u!==s.call(r))return!1;switch(u){case"[object RegExp]":case"
[object String]":return""+n==""+r;case"[object Number]":return+n!=+n?+r!=+r:0==+n?1/+n==
1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbo
l]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("o
bject"!=typeof n||"object"!=typeof r)return!1;var i=n.constructor,a=r.constructor;if(i!=
=a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in
r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.pus
h(n),e.push(r),o){if((f=n.length)!==r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))re
turn!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!==f)return!1;for(;f--;)if(c=l[f],!x
(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){re
turn function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln
(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn
("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Erro
r"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!functio
n(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.docume
nt.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[o
bject Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function
(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}fun
ction ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=
typeof/./&&"object"!=typeof Int8Array&&"function"!=typeof rr&&(Cn=function(n){return"fun
ction"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr=
{"&":"&","<":"<",">":">",'"':""","'":"'","`":"`"},lr=Mn(cr);fun
ction pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=Reg
Exp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var s
r=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interp
olate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr=
{"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|
\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).c
hain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=functi
on(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["po
p","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototyp
e[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"!==r&&"splice"!==
r||0!==n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r
=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.pr
ototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.
prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSIO
N:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:
I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return
R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,plu
ck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},m
ax:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"!=t

ypeof n[0]&&null≠n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null≠(t=n[a])&&t<o&&(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;return e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort(function(n,r){var t=n.criteria,e=r.criteria;if(t≠e){if(e<t||void 0===t)return 1;if(t<e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},size:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,take:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n){return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){var o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,indexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chunk:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,arguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i=a=null)},n=function(){var n=fr();c||!1≠u.leading||(c=n);var r=e-(n-c);return i=this,a=arguments,r⩽0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(this,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=null},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,arguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findKey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},clone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn(n).length)},isElement:function(n){return!(!n||1≠n.nodeType)},isArray:Kn,isObject:Ln,isArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isSymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUndefined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},identity:ur,constant:function(n){return function(){return n}},noop:function(){},property:or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:function(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:funct

ion(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).sou
rce,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+
='";o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,
r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':
__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a
+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arg
uments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n)
{throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";retur
n u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!
0,r},mixin:_r});return wr._=wr});

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `r` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/js/libs/underscore-min.js:6

6 var n="object"==typeof self&&self.self===self&&self||"object"==typeof global&&global.g
lobal===global&&global||Function("return this")()||{},e=Array.prototype,i=Object.prototy
pe,p="undefined"!=typeof Symbol?Symbol.prototype:null,u=e.push,f=e.slice,s=i.toString,o=
i.hasOwnProperty,r=Array.isArray,a=Object.keys,t=Object.create,c=n.isNaN,l=n.isFinite,v=
function(){};function h(n){return n instanceof h?n:this instanceof h?void(this._wrapped=
n):new h(n)}var g=h.VERSION="1.10.2";function y(u,o,n){if(void 0===o)return u;switch(nul
l==n?3:n){case 1:return function(n){return u.call(o,n)};case 3:return function(n,r,t){re
turn u.call(o,n,r,t)};case 4:return function(n,r,t,e){return u.call(o,n,r,t,e)}}return f
unction(){return u.apply(o,arguments)}}function d(n,r,t){return null==n?ur:Cn(n)?y(n,r,
t):Ln(n)&&!Kn(n)?ir(n):or(n)}function m(n,r){return d(n,r,1/0)}function b(n,r,t){return
h.iteratee!=m?h.iteratee(n,r):d(n,r,t)}function j(u,o){return o=null==o?u.length-1:+o,f
unction(){for(var n=Math.max(arguments.length-o,0),r=Array(n),t=0;t<n;t++)r[t]=arguments
[t+o];switch(o){case 0:return u.call(this,r);case 1:return u.call(this,arguments[0],r);c
ase 2:return u.call(this,arguments[0],arguments[1],r)}var e=Array(o+1);for(t=0;t<o;t++)e
[t]=arguments[t];return e[o]=r,u.apply(this,e)}}function _(n){if(!Ln(n))return{};if(t)re
turn t(n);v.prototype=n;var r=new v;return v.prototype=null,r}function w(r){return funct
ion(n){return null==n?void 0:n[r]}}function x(n,r){return null!=n&&o.call(n,r)}function
S(n,r){for(var t=r.length,e=0;e<t;e++){if(null==n)return;n=n[r[e]]}return t?n:void 0}h.i
teratee=m;var A=Math.pow(2,53)-1,O=w("length");function M(n){var r=O(n);return"number"==
typeof r&&0<=r&&r<=A}function E(n,r,t){var e,u;if(r=y(r,t),M(n))for(e=0,u=n.length;e<u;e
++)r(n[e],e,n);else{var o=Sn(n);for(e=0,u=o.length;e<u;e++)r(n[o[e]],o[e],n)}return n}fu
nction N(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=Array(u),i=0;i<u;i++)
{var a=e?e[i]:i;o[i]=r(n[a],a,n)}return o}function k(f){return function(n,r,t,e){var u=3
<=arguments.length;return function(n,r,t,e){var u=!M(n)&&Sn(n),o=(u||n).length,i=0<f?0:o
-1;for(e||(t=n[u?u[i]:i],i+=f);0<=i&&i<o;i+=f){var a=u?u[i]:i;t=r(t,n[a],a,n)}return t}
(n,y(r,e,4),t,u)}}var I=k(1),T=k(-1);function B(n,r,t){var e=(M(n)?on:Tn)(n,r,t);if(void

```
0≠=e&&-1≠=e)return n[e]}function R(n,e,r){var u=[];return e=b(e,r),E(n,function(n,r,t)
{e(n,r,t)&&u.push(n)}),u}function F(n,r,t){r=b(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).leng
th,o=0;o<u;o++){var i=e?e[o]:o;if(!r(n[i],i,n))return!1}return!0}function q(n,r,t){r=b
(r,t);for(var e=!M(n)&&Sn(n),u=(e||n).length,o=0;o<u;o++){var i=e?e[o]:o;if(r(n[i],i,n))
return!0}return!1}function D(n,r,t,e){return M(n)||(n=On(n)),("number"≠=typeof t||e)&&(t
=0),0⩽ln(n,r,t)}var W=j(function(n,t,e){var u,o;return Cn(t)?o=t:Kn(t)&&(u=t.slice(0,-
1),t=t[t.length-1]),N(n,function(n){var r=o;if(!r){if(u&&u.length&&(n=S(n,u)),null==n)re
turn;r=n[t]}return null==r?r:r.apply(n,e)})});function z(n,r){return N(n,or(r))}function
P(n,e,r){var t,u,o=-1/0,i=-1/0;if(null==e||"number"==typeof e&&"object"≠typeof n[0]&&nu
ll≠n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null≠(t=n[a])&&o<t&&(o=t);else e=b
(e,r),E(n,function(n,r,t){u=e(n,r,t),(i<u||u===-1/0&&o===-1/0)&&(o=n,i=u)});return o}fun
ction K(n,r,t){if(null==r||t)return M(n)||(n=On(n)),n[ar(n.length-1)];var e=M(n)?Dn(n):O
n(n),u=O(e);r=Math.max(Math.min(r,u),0);for(var o=u-1,i=0;i<r;i++){var a=ar(i,o),f=e[i];
e[i]=e[a],e[a]=f}return e.slice(0,r)}function L(i,r){return function(e,u,n){var o=r?[[],
[]]:{};return u=b(u,n),E(e,function(n,r){var t=u(n,r,e);i(o,n,t)}),o}}var V=L(function
(n,r,t){x(n,t)?n[t].push(r):n[t]=[r]}),C=L(function(n,r,t){n[t]=r}),J=L(function(n,r,t)
{x(n,t)?n[t]++:n[t]=1}),U=/[^\ud800-\udfff]|[\ud800-\udbff][\udc00-\udfff]|[\ud800-\udff
f]/g;var $=L(function(n,r,t){n[t?0:1].push(r)},!0);function G(n,r,t){return null==n||n.l
ength<1?null==r?void 0:[]:null==r||t?n[0]:H(n,n.length-r)}function H(n,r,t){return f.cal
l(n,0,Math.max(0,n.length-(null==r||t?1:r)))}function Q(n,r,t){return f.call(n,null==r||
t?1:r)}function X(n,r,t,e){for(var u=(e=e||[]).length,o=0,i=O(n);o<i;o++){var a=n[o];if
(M(a)&&(Kn(a)||Vn(a)))if(r)for(var f=0,c=a.length;f<c;)e[u++]=a[f++];else X(a,r,t,e),u=
e.length;else t||(e[u++]=a)}return e}var Y=j(function(n,r){return rn(n,r)});function Z
(n,r,t,e){er(r)||(e=t,t=r,r=!1),null≠t&&(t=b(t,e));for(var u=[],o=[],i=0,a=O(n);i<a;i+
+){var f=n[i],c=t?t(f,i,n):f;r&&!t?(i&&o===c||u.push(f),o=c):t?D(o,c)||(o.push(c),u.push
(f)):D(u,f)||u.push(f)}return u}var nn=j(function(n){return Z(X(n,!0,!0))});var rn=j(fun
ction(n,r){return r=X(r,!0,!0),R(n,function(n){return!D(r,n)})});function tn(n){for(var
r=n&&P(n,O).length||0,t=Array(r),e=0;e<r;e++)t[e]=z(n,e);return t}var en=j(tn);function
un(o){return function(n,r,t){r=b(r,t);for(var e=O(n),u=0<o?0:e-1;0⩽u&&u<e;u+=o)if(r(n
[u],u,n))return u;return-1}}var on=un(1),an=un(-1);function fn(n,r,t,e){for(var u=(t=b
(t,e,1))(r),o=0,i=O(n);o<i;){var a=Math.floor((o+i)/2);t(n[a])<u?o=a+1:i=a}return o}func
tion cn(o,i,a){return function(n,r,t){var e=0,u=O(n);if("number"==typeof t)0<o?e=0⩽t?t:
Math.max(t+u,e):u=0⩽t?Math.min(t+1,u):t+u+1;else if(a&&t&&u)return n[t=a(n,r)]===r?t:-
1;if(r≠r)return 0⩽(t=i(f.call(n,e,u),tr))?t+e:-1;for(t=0<o?e:u-1;0⩽t&&t<u;t+=o)if(n
[t]===r)return t;return-1}}var ln=cn(1,on,fn),pn=cn(-1,an);function sn(n,r,t,e,u){if(!(e
instanceof r))return n.apply(t,u);var o=_(n.prototype),i=n.apply(o,u);return Ln(i)?i:o}v
ar vn=j(function(r,t,e){if(!Cn(r))throw new TypeError("Bind must be called on a functio
n");var u=j(function(n){return sn(r,u,t,this,e.concat(n))});return u}),hn=j(function(u,
o){var i=hn.placeholder,a=function(){for(var n=0,r=o.length,t=Array(r),e=0;e<r;e++)t[e]=
o[e]===i?arguments[n++]:o[e];for(;n<arguments.length;)t.push(arguments[n++]);return sn
(u,a,this,this,t)};return a});hn.placeholder=h;var gn=j(function(n,r){var t=(r=X(r,!1,!
1)).length;if(t<1)throw new Error("bindAll must be passed function names");for(;t--;){va
r e=r[t];n[e]=vn(n[e],n)}});var yn=j(function(n,r,t){return setTimeout(function(){return
n.apply(null,t)},r)}),dn=hn(yn,h,1);function mn(n){return function(){return!n.apply(thi
s,arguments)}}function bn(n,r){var t;return function(){return 0<--n&&(t=r.apply(this,arg
uments)),n⩽1&&(r=null),t}}var jn=hn(bn,2),_n=!{toString:null}.propertyIsEnumerable("toS
tring"),wn=["valueOf","isPrototypeOf","toString","propertyIsEnumerable","hasOwnPropert
y","toLocaleString"];function xn(n,r){var t=wn.length,e=n.constructor,u=Cn(e)&&e.prototy
pe||i,o="constructor";for(x(n,o)&&!D(r,o)&&r.push(o);t--;)(o=wn[t])in n&&n[o]≠=u[o]&&!D
(r,o)&&r.push(o)}function Sn(n){if(!Ln(n))return[];if(a)return a(n);var r=[];for(var t i
n n)x(n,t)&&r.push(t);return _n&&xn(n,r),r}function An(n){if(!Ln(n))return[];var r=[];fo
```

```
r(var t in n)r.push(t);return _n&&xn(n,r),r}function On(n){for(var r=Sn(n),t=r.length,e=
Array(t),u=0;u<t;u++)e[u]=n[r[u]];return e}function Mn(n){for(var r={},t=Sn(n),e=0,u=t.l
ength;e<u;e++)r[n[t[e]]]=t[e];return r}function En(n){var r=[];for(var t in n)Cn(n[t])&&
r.push(t);return r.sort()}function Nn(f,c){return function(n){var r=arguments.length;if
(c&&(n=Object(n)),r<2||null==n)return n;for(var t=1;t<r;t++)for(var e=arguments[t],u=f
(e),o=u.length,i=0;i<o;i++){var a=u[i];c&&void 0===n[a]||(n[a]=e[a])}return n}}var kn=Nn
(An),In=Nn(Sn);function Tn(n,r,t){r=b(r,t);for(var e,u=Sn(n),o=0,i=u.length;o<i;o++)if(r
(n[e=u[o]],e,n))return e}function Bn(n,r,t){return r in t}var Rn=j(function(n,r){var t=
{},e=r[0];if(null==n)return t;Cn(e)?(1<r.length&&(e=y(e,r[1])),r=An(n)):(e=Bn,r=X(r,!1,!
1),n=Object(n));for(var u=0,o=r.length;u<o;u++){var i=r[u],a=n[i];e(a,i,n)&&(t[i]=a)}ret
urn t}),Fn=j(function(n,t){var r,e=t[0];return Cn(e)?(e=mn(e),1<t.length&&(r=t[1])):(t=N
(X(t,!1,!1),String),e=function(n,r){return!D(t,r)}),Rn(n,e,r)}),qn=Nn(An,!0);function Dn
(n){return Ln(n)?Kn(n)?n.slice():kn({},n):n}function Wn(n,r){var t=Sn(r),e=t.length;if(n
ull==n)return!e;for(var u=Object(n),o=0;o<e;o++){var i=t[o];if(r[i]!==u[i]||!(i in u))re
turn!1}return!0}function zn(n,r,t,e){if(n===r)return 0!==n||1/n==1/r;if(null==n||null==
r)return!1;if(n!=n)return r!=r;var u=typeof n;return("function"===u||"object"===u||"obje
ct"==typeof r)&&function(n,r,t,e){n instanceof h&&(n=n._wrapped);r instanceof h&&(r=r._w
rapped);var u=s.call(n);if(u!=s.call(r))return!1;switch(u){case"[object RegExp]":case"
[object String]":return""+n==""+r;case"[object Number]":return+n!=+n?+r!=+r:0==+n?1/+n==
1/r:+n==+r;case"[object Date]":case"[object Boolean]":return+n==+r;case"[object Symbo
l]":return p.valueOf.call(n)===p.valueOf.call(r)}var o="[object Array]"===u;if(!o){if("o
bject"!=typeof n||"object"!=typeof r)return!1;var i=n.constructor,a=r.constructor;if(i!=
=a&&!(Cn(i)&&i instanceof i&&Cn(a)&&a instanceof a)&&"constructor"in n&&"constructor"in
r)return!1}e=e||[];var f=(t=t||[]).length;for(;f--;)if(t[f]===n)return e[f]===r;if(t.pus
h(n),e.push(r),o){if((f=n.length)!=r.length)return!1;for(;f--;)if(!zn(n[f],r[f],t,e))re
turn!1}else{var c,l=Sn(n);if(f=l.length,Sn(r).length!=f)return!1;for(;f--;)if(c=l[f],!x
(r,c)||!zn(n[c],r[c],t,e))return!1}return t.pop(),e.pop(),!0}(n,r,t,e)}function Pn(r){re
turn function(n){return s.call(n)==="[object "+r+"]"}}var Kn=r||Pn("Array");function Ln
(n){var r=typeof n;return"function"===r||"object"===r&&!!n}var Vn=Pn("Arguments"),Cn=Pn
("Function"),Jn=Pn("String"),Un=Pn("Number"),$n=Pn("Date"),Gn=Pn("RegExp"),Hn=Pn("Erro
r"),Qn=Pn("Symbol"),Xn=Pn("Map"),Yn=Pn("WeakMap"),Zn=Pn("Set"),nr=Pn("WeakSet");!functio
n(){Vn(arguments)||(Vn=function(n){return x(n,"callee")})}();var rr=n.document&&n.docume
nt.childNodes;function tr(n){return Un(n)&&c(n)}function er(n){return!0===n||!1===n||"[o
bject Boolean]"===s.call(n)}function ur(n){return n}function or(r){return Kn(r)?function
(n){return S(n,r)}:w(r)}function ir(r){return r=In({},r),function(n){return Wn(n,r)}}fun
ction ar(n,r){return null==r&&(r=n,n=0),n+Math.floor(Math.random()*(r-n+1))}"function"!=
typeof/./&&"object"!=typeof Int8Array&&"function"!=typeof rr&&(Cn=function(n){return"fun
ction"==typeof n||!1});var fr=Date.now||function(){return(new Date).getTime()},cr=
{"&":"&amp;","<":"&lt;",">":"&gt;",'"':"&quot;","'":"&#x27;","`":"&#x60;"},lr=Mn(cr);fun
ction pr(r){var t=function(n){return r[n]},n="(?:"+Sn(r).join("|")+")",e=RegExp(n),u=Reg
Exp(n,"g");return function(n){return n=null==n?"":""+n,e.test(n)?n.replace(u,t):n}}var s
r=pr(cr),vr=pr(lr);var hr=0;var gr=h.templateSettings={evaluate:/<%([\s\S]+?)%>/g,interp
olate:/<%=([\s\S]+?)%>/g,escape:/<%-([\s\S]+?)%>/g},yr=/(.)^/,dr=
{"'":"'","\\":"\\","\r":"r","\n":"n","\u2028":"u2028","\u2029":"u2029"},mr=/\\|'|\r|\n|
\u2028|\u2029/g,br=function(n){return"\\"+dr[n]};function jr(n,r){return n._chain?h(r).c
hain():r}function _r(t){return E(En(t),function(n){var r=h[n]=t[n];h.prototype[n]=functi
on(){var n=[this._wrapped];return u.apply(n,arguments),jr(this,r.apply(h,n))}}),h}E(["po
p","push","reverse","shift","sort","splice","unshift"],function(r){var t=e[r];h.prototyp
e[r]=function(){var n=this._wrapped;return t.apply(n,arguments),"shift"!=r&&"splice"!=
r||0!==n.length||delete n[0],jr(this,n)}}),E(["concat","join","slice"],function(n){var r
=e[n];h.prototype[n]=function(){return jr(this,r.apply(this._wrapped,arguments))}}),h.pr
```

ototype.valueOf=h.prototype.toJSON=h.prototype.value=function(){return this._wrapped},h.prototype.toString=function(){return String(this._wrapped)};var wr=_r({default:h,VERSION:g,iteratee:m,restArguments:j,each:E,forEach:E,map:N,collect:N,reduce:I,foldl:I,inject:I,reduceRight:T,foldr:T,find:B,detect:B,filter:R,select:R,reject:function(n,r,t){return R(n,mn(b(r)),t)},every:F,all:F,some:q,any:q,contains:D,includes:D,include:D,invoke:W,pluck:z,where:function(n,r){return R(n,ir(r))},findWhere:function(n,r){return B(n,ir(r))},max:P,min:function(n,e,r){var t,u,o=1/0,i=1/0;if(null==e||"number"==typeof e&&"object"!=typeof n[0]&&null!=n)for(var a=0,f=(n=M(n)?n:On(n)).length;a<f;a++)null!=(t=n[a])&&t<o&&(o=t);else e=b(e,r),E(n,function(n,r,t){((u=e(n,r,t))<i||u===1/0&&o===1/0)&&(o=n,i=u)});return o},shuffle:function(n){return K(n,1/0)},sample:K,sortBy:function(n,e,r){var u=0;return e=b(e,r),z(N(n,function(n,r,t){return{value:n,index:u++,criteria:e(n,r,t)}}).sort(function(n,r){var t=n.criteria,e=r.criteria;if(t!=e){if(e<t||void 0===t)return 1;if(t<e||void 0===e)return-1}return n.index-r.index}),"value")},groupBy:V,indexBy:C,countBy:J,toArray:function(n){return n?Kn(n)?f.call(n):Jn(n)?n.match(U):M(n)?N(n,ur):On(n):[]},size:function(n){return null==n?0:M(n)?n.length:Sn(n).length},partition:$,first:G,head:G,take:G,initial:H,last:function(n,r,t){return null==n||n.length<1?null==r?void 0:[]:null==r||t?n[n.length-1]:Q(n,Math.max(0,n.length-r))},rest:Q,tail:Q,drop:Q,compact:function(n){return R(n,Boolean)},flatten:function(n,r){return X(n,r,!1)},without:Y,uniq:Z,unique:Z,union:nn,intersection:function(n){for(var r=[],t=arguments.length,e=0,u=O(n);e<u;e++){var o=n[e];if(!D(r,o)){var i;for(i=1;i<t&&D(arguments[i],o);i++);i===t&&r.push(o)}}return r},difference:rn,unzip:tn,zip:en,object:function(n,r){for(var t={},e=0,u=O(n);e<u;e++)r?t[n[e]]=r[e]:t[n[e][0]]=n[e][1];return t},findIndex:on,findLastIndex:an,sortedIndex:fn,indexOf:ln,lastIndexOf:pn,range:function(n,r,t){null==r&&(r=n||0,n=0),t||(t=r<n?-1:1);for(var e=Math.max(Math.ceil((r-n)/t),0),u=Array(e),o=0;o<e;o++,n+=t)u[o]=n;return u},chunk:function(n,r){if(null==r||r<1)return[];for(var t=[],e=0,u=n.length;e<u;)t.push(f.call(n,e,e+=r));return t},bind:vn,partial:hn,bindAll:gn,memoize:function(e,u){var o=function(n){var r=o.cache,t=""+(u?u.apply(this,arguments):n);return x(r,t)||(r[t]=e.apply(this,arguments)),r[t]};return o.cache={},o},delay:yn,defer:dn,throttle:function(t,e,u){var o,i,a,f,c=0;u||(u={});var l=function(){c=!1===u.leading?0:fr(),o=null,f=t.apply(i,a),o||(i=a=null)},n=function(){var n=fr();c||!1!==u.leading||(c=n);var r=e-(n-c);return i=this,a=arguments,r<=0||e<r?(o&&(clearTimeout(o),o=null),c=n,f=t.apply(i,a),o||(i=a=null)):o||!1===u.trailing||(o=setTimeout(l,r)),f};return n.cancel=function(){clearTimeout(o),c=0,o=i=a=null},n},debounce:function(t,e,u){var o,i,a=function(n,r){o=null,r&&(i=t.apply(n,r))},n=j(function(n){if(o&&clearTimeout(o),u){var r=!o;o=setTimeout(a,e),r&&(i=t.apply(this,n))}else o=yn(a,e,this,n);return i});return n.cancel=function(){clearTimeout(o),o=null},n},wrap:function(n,r){return hn(r,n)},negate:mn,compose:function(){var t=arguments,e=t.length-1;return function(){for(var n=e,r=t[e].apply(this,arguments);n--;)r=t[n].call(this,r);return r}},after:function(n,r){return function(){if(--n<1)return r.apply(this,arguments)}},before:bn,once:jn,keys:Sn,allKeys:An,values:On,mapObject:function(n,r,t){r=b(r,t);for(var e=Sn(n),u=e.length,o={},i=0;i<u;i++){var a=e[i];o[a]=r(n[a],a,n)}return o},pairs:function(n){for(var r=Sn(n),t=r.length,e=Array(t),u=0;u<t;u++)e[u]=[r[u],n[r[u]]];return e},invert:Mn,functions:En,methods:En,extend:kn,extendOwn:In,assign:In,findKey:Tn,pick:Rn,omit:Fn,defaults:qn,create:function(n,r){var t=_(n);return r&&In(t,r),t},clone:Dn,tap:function(n,r){return r(n),n},isMatch:Wn,isEqual:function(n,r){return zn(n,r)},isEmpty:function(n){return null==n||(M(n)&&(Kn(n)||Jn(n)||Vn(n))?0===n.length:0===Sn(n).length)},isElement:function(n){return!(!n||1!=n.nodeType)},isArray:Kn,isObject:Ln,isArguments:Vn,isFunction:Cn,isString:Jn,isNumber:Un,isDate:$n,isRegExp:Gn,isError:Hn,isSymbol:Qn,isMap:Xn,isWeakMap:Yn,isSet:Zn,isWeakSet:nr,isFinite:function(n){return!Qn(n)&&l(n)&&!c(parseFloat(n))},isNaN:tr,isBoolean:er,isNull:function(n){return null===n},isUndefined:function(n){return void 0===n},has:function(n,r){if(!Kn(r))return x(n,r);for(var t=r.length,e=0;e<t;e++){var u=r[e];if(null==n||!o.call(n,u))return!1;n=n[u]}return!!t},i

dentity:ur,constant:function(n){return function(){return n}},noop:function(){},property:or,propertyOf:function(r){return null==r?function(){}:function(n){return Kn(n)?S(r,n):r[n]}},matcher:ir,matches:ir,times:function(n,r,t){var e=Array(Math.max(0,n));r=y(r,t,1);for(var u=0;u<n;u++)e[u]=r(u);return e},random:ar,now:fr,escape:sr,unescape:vr,result:function(n,r,t){Kn(r)||(r=[r]);var e=r.length;if(!e)return Cn(t)?t.call(n):t;for(var u=0;u<e;u++){var o=null==n?void 0:n[r[u]];void 0===o&&(o=t,u=e),n=Cn(o)?o.call(n):o}return n},uniqueId:function(n){var r=++hr+"";return n?n+r:r},templateSettings:gr,template:function(o,n,r){!n&&r&&(n=r),n=qn({},n,h.templateSettings);var t,e=RegExp([(n.escape||yr).source,(n.interpolate||yr).source,(n.evaluate||yr).source].join("|")+"|$","g"),i=0,a="__p+='";o.replace(e,function(n,r,t,e,u){return a+=o.slice(i,u).replace(mr,br),i=u+n.length,r?a+="'+\n((__t=("+r+"))==null?'':_.escape(__t))+\n'":t?a+="'+\n((__t=("+t+"))==null?'':__t)+\n'":e&&(a+="';\n"+e+"\n__p+='"),n}),a+="';\n",n.variable||(a="with(obj||{}){\n"+a+"}\n"),a="var __t,__p='',__j=Array.prototype.join,"+"print=function(){__p+=__j.call(arguments,'');};\n"+a+"return __p;\n";try{t=new Function(n.variable||"obj","_",a)}catch(n){throw n.source=a,n}var u=function(n){return t.call(this,n,h)},f=n.variable||"obj";return u.source="function("+f+"){\n"+a+"}",u},chain:function(n){var r=h(n);return r._chain=!0,r},mixin:_r});return wr._=wr});

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java:48

```
48    @RequestMapping(
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `nodeTypes` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:843

```
843             regex = new RegExp("^(" + nodeTypes.join("|") + ")$");
```

java.spring.security.audit.spring-unvalidated-redirect.spring-unvalidated-redirect HIGH

Application redirects a user to a destination URL specified by a user supplied parameter that is not validated.

src/main/java/org/owasp/webgoat/lessons/openredirect/OpenRedirectRealRedirect.java:18

```
18    @GetMapping("/OpenRedirect/realRedirect")
  public ModelAndView real(@RequestParam("url") String url) {
    // Intentionally vulnerable: no validation
    return new ModelAndView("redirect:" + url);
  }
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/container/service/LessonMenuService.java:45

```
45    @RequestMapping(path = URL_LESSONMENU_MVC, produces = "application/json")
```

java.servlets.security.cookie-issecure-false.cookie-issecure-false HIGH

Default session middleware settings: `setSecure` not set to true. This ensures that the cookie is sent only over HTTPS to prevent cross-site scripting attacks.

src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java:58

```
58      Cookie cookie = new Cookie(COOKIE_NAME, "");
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `className` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex

checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4079

```
4079      element.className = element.className.replace(new RegExp("(^|\\s+)" + className + "(\\s+|$)"), " ");
```

javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp HIGH

RegExp() called with a `className` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled input, consider performing input validation or use a regex checking/sanitization library such as https://www.npmjs.com/package/recheck to verify that the regex does not appear vulnerable to ReDoS.

src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4088

```
4088      return (elementClassName.length > 0 && (elementClassName == className || new RegExp("(^|\\s)" + className + "(\\s|$)").test(elementClassName)));
```

java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly HIGH

A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'

src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java:60

```
60      response.addCookie(cookie);
```

java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag HIGH

A cookie was detected without setting the 'secure' flag. The 'secure' flag for cookies prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the 'secure' flag by calling 'cookie.setSecure(true);'

src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java:60

```
60      response.addCookie(cookie);
```

java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly HIGH

A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'

src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java:77

```
77        response.addCookie(newCookie);
```

java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping HIGH

Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').

src/main/java/org/owasp/webgoat/container/service/SessionService.java:22

```
22    @RequestMapping(path = "/service/enable-security.mvc", produces = "application/jso
n")
```

java.lang.security.audit.crypto.weak-random.weak-random HIGH

Detected use of the functions `Math.random()` or `java.util.Random()`. These are both not cryptographically strong random number generators (RNGs). If you are using these RNGs to create passwords or secret tokens, use `java.security.SecureRandom` instead.

src/main/java/org/owasp/webgoat/lessons/challenges/challenge1/ImageServlet.java:21

```
21    public static final int PINCODE = new Random().nextInt(10000);
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java:57

```
57          ResultSet resultSet = statement.executeQuery(checkUserQuery);
```

html.security.audit.missing-integrity.missing-integrity HIGH

This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) you're telling the browser to fetch in the 'integrity' attribute for all externally hosted files.

docs/index.html:7

```
7    <link rel="canonical" href="https://webgoat.org" />
```

java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli HIGH

Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.

src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java

```
56          ResultSet results = statement.executeQuery(query);
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/webgoat/templates/login.html:31

```
31              <form th:action="@{/login}" method='POST' style="width: 200px;">
                <div class="form-group">
                    <label for="exampleInputEmail1" th:text="#{username}">Username</labe
l>
                    <input autofocus="dummy_for_thymeleaf_parser" type="text" class="for
m-control"
                           id="exampleInputEmail1" th:placeholder="#{username}" name='us
ername' />
                </div>
                <div class="form-group">
                    <label for="exampleInputPassword1" th:text="#{password}">Password</l
```

```
abel>
                    <input type="password" class="form-control" id="exampleInputPassword
1" th:placeholder="#{password}"
                           name='password' />
                </div>
                <button class="btn btn-primary btn-block" type="submit" th:text="#{sign.
in}">Sign in</button>
                <div class="text-center"><a th:href="@{/registration}" th:text="#{regist
er.new}"></a></div>
            </form>
```

python.django.security.django-no-csrf-token.django-no-csrf-token HIGH

Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.

src/main/resources/webwolf/templates/files.html:32

```
32              <form th:action="@{/fileupload}" method="post" enctype="multipart/form-da
ta">
                <fieldset>
                    <div class="mb-3">
                        <input type="file" class="form-control" name="file"/>
                    </div>
                    <div class="mb-3">
                        <button type="submit" class="btn btn-md btn-primary">Upload file
s</button>
                    </div>
                </fieldset>
            </form>
```