

## Project Part 2

### Part 1: Black Box Test Cases

#### Section 1: Client Side Bypassing

1. Upon addition of new patient, patient can be assigned any gender

**Unique ID:** 5.1-1

**ASVS:**

5.1.4 Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern

**CWE:** CWE-20

**URL:** [http://localhost/interface/new/new\\_comprehensive\\_save.php](http://localhost/interface/new/new_comprehensive_save.php)

**Input Field:** Sex

**Initial User Input:** Male

**Malicious Input:** Unassigned

**Steps:**

- Login to OpenEMR using valid credentials
- Navigate to Patients tab and then New Patient
- Create a valid patient using by entering the mandatory inputs in the valid format, a valid sex in this case
- Submit the form
- Navigate to OWASP ZAP and look for the post request containing the details of the form. It can be found at POST request for the given URL.
- Right click on the POST request and create a breakpoint
- Navigate to Patients tab and create a new patient again
- This time on submitting valid inputs, OWASP ZAP will intercept and request.
- Navigate to breakpoint and modify the value of 'form\_sex' to any custom value, 'Unassigned' in this case
- Forward the request to the server

**Expected Inputs:**

- 500 Internal Server Error
- Server Side sanitization of input

2. A new patient can be created with a blank first name and last name fields

**Unique ID:** 5.1-2

**ASVS:**

5.2.7 Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.

**CWE:** CWE-159

**URL:** [http://localhost/interface/new/new\\_comprehensive\\_save.php](http://localhost/interface/new/new_comprehensive_save.php)

**Input Field:** First Name, Last Name

**Initial User Input:** 'John', 'Doe'

**Malicious Input:** ", "

**Steps:**

- Login to OpenEMR using valid credentials
- Navigate to Patients tab and then New Patient
- Create a valid patient using by entering the mandatory inputs in the valid format, a first and last name in this case
- Submit the form
- Navigate to OWASP ZAP and look for the post request containing the details of the form. It can be found at POST request for the given URL.
- Right click on the POST request and create a breakpoint
- Navigate to Patients tab and create a new patient again
- This time on submitting valid inputs, OWASP ZAP will intercept and request.
- Navigate to breakpoint and modify the value of 'form\_fname' and 'form\_lname' to empty fields
- Forward the request to the server

**Expected Inputs:**

- 500 Internal Server Error
- Server Side sanitization of input

3. Date of Birth of the patient is accepting alphanumeric values

**Unique ID:** 5.1-3**ASVS:**

5.1.3 Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation

**CWE:** CWE-20: Improper Input Validation

**URL:** [http://localhost/interface/new/new\\_comprehensive\\_save.php](http://localhost/interface/new/new_comprehensive_save.php)

**Input Field:** Date of Birth

**Initial User Input:** Current/Past Date

**Malicious Input:** Any date in future

**Steps:**

- Login to OpenEMR using valid credentials

- Navigate to Patients tab and then New Patient
- Create a valid patient using by entering the mandatory inputs in the valid format, a valid date of birth in this case
- Submit the form
- Navigate to OWASP ZAP and look for the post request containing the details of the form. It can be found at POST request for the given URL.
- Right click on the POST request and create a breakpoint
- Navigate to Patients tab and create a new patient again
- This time on submitting valid inputs, OWASP ZAP will intercept and request.
- Navigate to breakpoint and modify the value of 'form\_DOB' to any alphanumeric value of date
- Forward the request to the server

**Expected Inputs:**

- 500 Internal Server Error
- Server Side sanitization of input.

4. Message length not validated in the POST request

**Unique ID:** 5.1-6

**ASVS:**

5.2.2 Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.

**CWE:** CWE-138

**URL:** <http://localhost/interface/main/messages/messages.php>

**Input Field:** Check or Reference Number

**Initial User Input:** Valid reference number

**Malicious Input:** Any alphanumeric input of unspecified length

**Steps:**

- Login to OpenEMR using valid credentials
- Navigate to patients tab
- Search for a patient using the details provided and select the patient
- Go to Visits->Create new visit and create a valid visit for the patient (if none is created)
- Go to Fees -> Payments
- Enter the payment details with valid inputs
- Submit the form.
- Navigate to OWASP ZAP and look for the post request containing the details of the form. It can be found at POST request for the given URL.
- Right click on the POST request and create a breakpoint
- Navigate to Patients tab and create a new patient visit again
- This time on submitting valid inputs, OWASP ZAP will intercept and request.

- Navigate to breakpoint and modify the value of ‘form\_source’ to any alphanumeric value of any length.
- Forward the request to the server

**Expected Inputs:**

- 500 Internal Server Error
- Error message specifying maximum input length

5. SQL Injection in login form

**Unique ID:** 5.1-6

**ASVS:**

5.3.4 Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks

**CWE:** CWE-89

**URL:** [http://localhost/interface/main/main\\_screen.php?auth=login&site=default](http://localhost/interface/main/main_screen.php?auth=login&site=default)

**Input Field:** admin

**Initial User Input:** valid admin input

**Malicious Input:** SQL Injection statement

**Steps:**

- Login to OpenEMR using valid credentials
- Navigate to patients tab
- Search for a patient using the details provided and select the patient
- Go to Fees -> Payments
- Enter the payment details with valid inputs
- Submit the form.
- Navigate to OWASP ZAP and look for the post request containing the details of the form. It can be found at POST request for the given URL.
- Right click on the POST request and create a breakpoint
- Navigate to Patients tab and create a new patient visit again
- This time on submitting valid inputs, OWASP ZAP will intercept and request.
- Navigate to breakpoint and modify the value of ‘form\_source’ to any alphanumeric value of any length.
- Forward the request to the server

**Expected Inputs:**

- 500 Internal Server Error
- Error message specifying maximum input length

## Section 2: Automated Fuzzing

**Total ZAP Automated Scan Time:** 1 hour 30 mins

**Total Time for finding True Positive:** 5 hours

**Total Time for planning the black box test cases:** 2 hours

**Time taken per true positive:** 1 hour 20 minutes

The actual screenshots of results as well as fuzzing as included in the second document

The screenshot shows the ZAP Attack Mode interface. The top bar has tabs for ATTACK Mode, SITES, CONTEXTS, and SITES. The left sidebar shows 'Contexts' with 'Default Context' selected. The main area is titled 'Automated Scan' with a sub-instruction: 'This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack''. It includes fields for 'URL to attack' (http://localhost:80), 'Use traditional spider' (checked), 'Use ajax spider' (checked, with 'Firefox Headless' selected), and buttons for 'Attack' and 'Stop'. Below this is a progress bar: 'Actively scanning (attacking) the URLs discovered by the spider(s)'. The bottom section is titled 'AJAX Spider' and contains a table of results. The table has columns: Processed, ID, Req. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, Size Resp. Body, Highest Alert, Note, and Tags. The table lists many entries, mostly with status 403 Forbidden and 130 bytes transferred. The bottom status bar shows 'Current Scans' with various icons.

Processed	ID	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Note	Tags
Out of Scope	13.007	3/8/24, 4:21:48 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.008	3/8/24, 4:21:48 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.009	3/8/24, 4:21:48 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.010	3/8/24, 4:21:50 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.011	3/8/24, 4:21:50 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.012	3/8/24, 4:21:50 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.013	3/8/24, 4:21:50 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.014	3/8/24, 4:21:50 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.015	3/8/24, 4:21:50 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.016	3/8/24, 4:21:51 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.017	3/8/24, 4:21:52 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.018	3/8/24, 4:21:53 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.019	3/8/24, 4:21:53 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.020	3/8/24, 4:21:53 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.021	3/8/24, 4:21:54 AM	GET	https://shaver.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.022	3/8/24, 4:21:54 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.023	3/8/24, 4:21:54 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.024	3/8/24, 4:21:54 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.025	3/8/24, 4:21:55 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.026	3/8/24, 4:21:55 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.027	3/8/24, 4:21:55 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.028	3/8/24, 4:21:56 AM	GET	https://shaver.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.029	3/8/24, 4:21:56 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.030	3/8/24, 4:21:56 AM	GET	https://firefox.settings.services.mozilla.com/v1/bu...	403	Forbidden	0 ms	130 bytes	40 bytes			
Out of Scope	13.031	3/8/24, 4:21:56 AM	POST	https://shaver.services.mozilla.com/downloads/cle...	403	Forbidden	0 ms	130 bytes	40 bytes			

## 2. Vulnerable dependencies

Github Checker total vulnerable dependencies: 25

Dependency name	CVE	Nature	Safer version
mongoose	CVE-2023-3696	Transitive	v5.13.20
xmldom	CVE-2022-39353	Transitive	N/A
	CVE-2021-32796		
angular	CVE-2024-21490	Direct	N/A
	CVE-2023-26116		
	CVE-2023-26117		
	CVE-2023-26118		
	CVE-2022-25844		
	CVE-2022-25869		
jszip	CVE-2022-48285	Transitive	v3.8.0
	CVE-2021-23413		v3.7.0
ckeditor4	CVE-2023-4771	Direct	v4.24.0-LTS
	CVE-2024-24816		
	CVE-2024-24815		
qs	CVE-2022-24999	Transitive	v6.5.3
xml2js	CVE-2023-0842	Transitive	v0.5.0
tar	CVE-2021-37713	Transitive	v4.4.18
	CVE-2021-32804		v3.2.2
postcss	CVE-2023-44270	Transitive	v8.4.31
got	CVE-2022-33987	Transitive	v11.8.5

**Snyk total vulnerable dependencies:** 6,486

Dependency name	CVE	Nature	Safer Version
xmldom	CVE-2022-39353	Transitive	N/A
	CVE-2022-37616		
	CVE-2021-32796		
mongoose	CVE-2023-3696	Transitive	v5.13.20
qs	CVE-2022-24999	Transitive	v6.2.4
xml2js	CVE-2023-0842	Transitive	v0.5.0
inflight	N/A	Transitive	N/A
jszip	CVE-2021-23413	Transitive	v3.7.0
	CVE-2022-48285		v3.8.0
ckeditor4	CVE-2024-24816	Direct	v4.24.0
	CVE-2024-24815		v4.24.0
	CVE-2023-4771		N/A
angular	CVE-2024-21490	Direct	N/A
	CVE-2022-25844		
	CVE-2023-26116		
	CVE-2023-26117		
	CVE-2023-26118		
	CVE-2022-25869		
i18next	N/A	Transitive	v19.8.5 v19.8.3 v19.5.5
dompdf	CVE-2024-25117	Direct	v2.0.4

- **Explain why you think the results differ among the two tools and write a comparison report. What do you think are the strengths and weaknesses of each tool from both technical and usability standpoints.)**

GitHub Dependabot offers a seamless integration with GitHub's version control system, providing a user-friendly interface for managing dependencies within GitHub repositories. This tight coupling streamlines the workflow for developers using GitHub's platform. However, Dependabot's major limitation is its exclusivity to GitHub repositories, which makes it non-compatible to alternative version control systems such as BitBucket, GitLab.

In contrast, Synk distinguishes itself by supporting multiple version control systems, including BitBucket and GitLab. Synk's strength lies in its extensive vulnerability database, enabling a more comprehensive scan that may uncover potential security vulnerabilities that GitHub Dependabot might overlook. Synk also provides detailed dependency paths, which is particularly useful for comprehending and mitigating vulnerabilities, especially in the case of transitive dependencies.

While Synk's is versatile, its broad integration options and extensive feature set may introduce some complexity and a learning curve for new users. The choice between GitHub Dependabot and Synk ultimately hinges upon the development team's specific requirements, including the version control system in use, the desired level of security coverage, and the team's familiarity with each tool's user interface.

The results differ due to the specific focus and integrations of each tool, the size and scope of their vulnerability databases, and the extent to which they address both direct and transitive dependencies. Github checker tool could have improved their design to provide a dependency path to better understand and mitigate the vulnerabilities. Moreover, there are some vulnerabilities that were found by Synk but not github checker, we believe that is because of the vulnerability database.

- **Compare the output of these two tools with that of the Bomber tool you ran during a classroom exercise.**

The comparison between GitHub Checks, Snyk, and the Bomber tool reveals distinct approaches to vulnerability management and reporting within the software development lifecycle (SDLC). GitHub Checks and Snyk provide integrated solutions that enable seamless identification and remediation of security vulnerabilities within the developers' workflow. Both tools leverage industry-standard vulnerability data, including Common Vulnerabilities and Exposures (CVE) identifiers, vulnerability titles, descriptions, Common Weakness Enumeration (CWE) classifications, and severity ratings, facilitating consistent vulnerability assessment across platforms.

The Bomber tool's output is detailed and structured, often in JSON format, providing a comprehensive breakdown of each vulnerability, which is ideal for automated processing and in-depth analysis. This contrasts with GitHub Checks and Snyk, which present more streamlined and user-friendly information, focusing on summarizing key details and remediation advice directly within their interfaces for quick decision-making by developers. While the Bomber tool caters to technical users requiring detailed data for extensive analysis or integration into complex workflows, GitHub Checks and Snyk are designed to provide accessible, actionable insights, optimizing ease of use and immediacy for developers in their daily work.

### 3. Secret Detection

#### Tool 1: Gitleaks

- 1) Secret type: API Key

Exposed Secret:

ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=

##### Screenshot of code:

```
49     XDEBUG_PROFILER_ON: 1
50     # setting xdebug client host for cases where xdebug.discover_client_host fails
51     XDEBUG_CLIENT_HOST: host.docker.internal
52     GITHUB_COMPOSER_TOKEN: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0
53     GITHUB_COMPOSER_TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=
54     OPENEMR_DOCKER_ENV_TAG: easy-dev-docker
55     OPENEMR_SETTING_site_addr_oauth: 'https://localhost:9300'
56     OPENEMR_SETTING_oauth_password_grant: 3
57     OPENEMR_SETTING_system_scopes_api: 1
```

##### Tool generated output:

```
{
  "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive operations.",
  "StartLine": 52,
  "EndLine": 52,
  "StartColumn": 23,
  "EndColumn": 0,
  "Match": "TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
  "Secret": "ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
  "File": "docker/development-easy-arm32/docker-compose.yml",
  "SymlinkFile": "",
  "Commit": "fe61175c8f0cc33552004ddc122b0722043f0d29",
  "Entropy": 4.4834447,
  "Author": "Brady Miller",
  "Email": "brady.g.miller@gmail.com",
  "Date": "2021-03-20T23:16:32Z",
  "Message": "docker dev fix (#4294)",
  "Tags": [],
  "RuleID": "generic-api-key",
  "Fingerprint": "fe61175c8f0cc33552004ddc122b0722043f0d29:docker/development-easy-arm32/docker-compose.yml:generic-api-key:52"
},
```

## 2) Secret type: API key

### Exposed Secret:

```
ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=
```

#### Screenshot of code:

```
docker > development-easy-light > docker-compose.yml > version
  2   services:
  16     openemr:
  32       environment:
  45         XDEBUG_ON: 1
  46         XDEBUG_PROFILER_ON: 1
  47         # setting xdebug client host for cases where xdebug.discover_client_host fails
  48         XDEBUG_CLIENT_HOST: host.docker.internal
  49         GITHUB_COMPOSER_TOKEN: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0
  50         GITHUB_COMPOSER_TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=
  51         OPENEMR_DOCKER_ENV_TAG: easy-dev-docker
  52         OPENEMR_SETTING_site_addr_oath: 'https://localhost:9300'
  53         OPENEMR_SETTING_oath_ca_bundle: /etc/ssl/certs/ca-certificates.crt
```

#### Tool generated output:

```
382 {
  383   "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive operations.",
  384   "StartLine": 49,
  385   "EndLine": 49,
  386   "StartColumn": 23,
  387   "EndColumn": 0,
  388   "Match": "TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
  389   "Secret": "ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
  390   "File": "docker/development-easy-light/docker-compose.yml",
  391   "SymlinkFile": "",
  392   "Commit": "fe61175c8f0cc33552004ddc122b0722043f0d29",
  393   "Entropy": 4.4834447,
  394   "Author": "Brady Miller",
  395   "Email": "brady.g.miller@gmail.com",
  396   "Date": "2021-03-20T23:16:32Z",
  397   "Message": "docker dev fix (#4294)",
  398   "Tags": [],
  399   "RuleID": "generic-api-key",
  400   "Fingerprint": "fe61175c8f0cc33552004ddc122b0722043f0d29:docker/development-easy-light/docker-compose.yml:generic-api-key:49"
  401 }
```

### 3) Secret type: API key

#### Exposed Secret:

```
ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=
```

#### Screenshot of code:

```
docker > development-easy > 🚀 docker-compose.yml > ⚒ version
  2   services:
 16     openemr:
 33       environment:
 47         XDEBUG_PROFILER_ON: 1
 48           # setting xdebug client host for cases where xdebug.discover_client_host fails
 49           XDEBUG_CLIENT_HOST: host.docker.internal
 50           GITHUB_COMPOSER_TOKEN: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0
 51           GITHUB_COMPOSER_TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=
 52           OPENEMR_DOCKER_ENV_TAG: easy-dev-docker
 53           OPENEMR_SETTING_site_addr_oauth: 'https://localhost:9300'
 54           OPENEMR_SETTING_oauth_password_grant: 3
```

#### Tool generated output:

```
422  {
423    "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive operations.",
424    "StartLine": 50,
425    "EndLine": 50,
426    "StartColumn": 23,
427    "EndColumn": 0,
428    "Match": "TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
429    "Secret": "ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",
430    "File": "docker/development-easy/docker-compose.yml",
431    "SymlinkFile": "",
432    "Commit": "fe61175c8f0cc33552004ddc122b0722043f0d29",
433    "Entropy": 4.4834447,
434    "Author": "Brady Miller",
435    "Email": "brady.g.miller@gmail.com",
436    "Date": "2021-03-20T23:16:32Z",
437    "Message": "docker dev fix (#4294)",
438    "Tags": [],
439    "RuleID": "generic-api-key",
440    "Fingerprint": "fe61175c8f0cc33552004ddc122b0722043f0d29:docker/development-easy/docker-compose.yml:generic-api-key:50"
441  },
442}
```

4) **Secret type:** API key

**Exposed Secret:**

ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=

**Screenshot of code:**

```
> development-insane > docker-compose.yml > {} services > {} openemr-8-3 > {} environment > GITHUB_COMPOSER_TOKEN  
services:  
  openemr-8-3:  
    environment:  
      - # setting xdebug client host for cases where xdebug.discover_client_host fails  
      XDEBUG_CLIENT_HOST: host.docker.internal  
      GITHUB_COMPOSER_TOKEN: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0      Brady Miller, 4 years ago  
      GITHUB_COMPOSER_TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=  
      OPENEMR_SETTING_site_addr_oath: 'https://localhost:9085'
```

**Tool generated output:**

```
442 {  
443   "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive operations.",  
444   "StartLine": 169,  
445   "EndLine": 169,  
446   "StartColumn": 23,  
447   "EndColumn": 0,  
448   "Match": "TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",  
449   "Secret": "ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2OQo=",  
450   "File": "docker/development-insane/docker-compose.yml",  
451   "SymlinkFile": "",  
452   "Commit": "fe61175c8f0cc33552004ddc122b0722043f0d29",  
453   "Entropy": 4.4834447,  
454   "Author": "Brady Miller",  
455   "Email": "brady.g.miller@gmail.com",  
456   "Date": "2021-03-20T23:16:32Z",  
457   "Message": "docker dev fix (#4294)",  
458   "Tags": [],  
459   "RuleID": "generic-api-key",  
460   "Fingerprint": "fe61175c8f0cc33552004ddc122b0722043f0d29:docker/development-insane/docker-compose.yml:generic-api-key:169"  
461 }
```

5) **Secret type:** Authentication Token  
**Exposed Secret:**

QkJENjI5MzUtRjc2Ri00RUM4LTg4MzQtQkRBQTc1REFEOEFCOjIBMzVEMzEzLUU3QkMtNDFDOS04OTMzLTNBMOQ3Mzk1M0Y3Mw==

**Screenshot of code:**

```
class Easipro
{
    public function __construct()
    {
        // direct to easipro dev server
        $this->server = "https://www.assessmentcenter.net/ac_api/2014-01/";

        // credential token for easipro dev server
        $this->devAuth = "QkJENjI5MzUtRjc2Ri00RUM4LTg4MzQtQkRBQTc1REFEOEFCOjIBMzVEMzEzLUU3QkMtNDFDOS04OTMzLTNBMOQ3Mzk1M0Y3Mw==";

    }

    // Collect list of forms (returns json)
    public function listForms()
    {
        $response = oeHttp::usingHeaders(['Authorization' => 'Basic ' . $this->devAuth])->get($this->server . 'Forms/.json');
        $data = $response->body();
    }
}
```

**Tool generated output:**

```
{
  "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive data.",
  "StartLine": 27,
  "EndLine": 27,
  "StartColumn": 20,
  "EndColumn": 128,
  "Match": "Auth = \"QkJENjI5MzUtRjc2Ri00RUM4LTg4MzQtQkRBQTc1REFEOEFCOjIBMzVEMzEzLUU3QkMtNDFDOS04OTMzLTNBMOQ3Mzk1M0Y3Mw==\"",
  "Secret": "QkJENjI5MzUtRjc2Ri00RUM4LTg4MzQtQkRBQTc1REFEOEFCOjIBMzVEMzEzLUU3QkMtNDFDOS04OTMzLTNBMOQ3Mzk1M0Y3Mw==",
  "File": "src/Easipro/Easipro.php",
  "SymlinkFile": "",
  "Commit": "9c5de9ce761c44061927f22a75f641749841db1c",
  "Entropy": 4.7440248,
  "Author": "StrongTSQ",
  "Email": "StrongTSQ@gmail.com",
  "Date": "2020-02-04T19:41:09Z",
  "Message": "easipro feature, 1st commit\n\nSee following PR for details:\nhttps://github.com/openTSQ/easipro/pull/1",
  "Tags": [],
  "RuleID": "generic-api-key",
  "Fingerprint": "9c5de9ce761c44061927f22a75f641749841db1c:src/Easipro/Easipro.php:generic-api-key"
}
```

6) **Secret type:**Token

**Exposed Secret:** SHBhCq4BL0pxJww3DG6g7dtKcuhG62zcK

**Screenshot of code:**

```
public > assets > i18next-9-0-1 > ! .coveralls.yml > repo_token
Brady Miller, 6 years ago | 1 author (Brady Miller)
1 | repo_token: SHBhCq4BL0pxJww3DG6g7dtKcuhG62zcK Brady Miller
2
```

**Tool generated output:**

```
{
  "Description": "Detected a Generic API Key, potentially exposing access to various services and sensitive operations.",
  "Startline": 1,
  "EndLine": 1,
  "StartColumn": 6,
  "EndColumn": 0,
  "Match": "token: SHBhCq4BL0pxJww3DG6g7dtKcuhG62zcK",
  "Secret": "SHBhCq4BL0pxJww3DG6g7dtKcuhG62zcK",
  "File": "public/assets/i18next-9-0-1/.coveralls.yml",
  "SymlinkFile": "",
  "Commit": "215c131cfccf749a5456ecaf4c493cedb647272c3",
  "Entropy": 4.6201515,
  "Author": "Brady Miller",
  "Email": "brady.g.miller@gmail.com",
  "Date": "2017-11-13T17:21:47Z",
  "Message": "added dwv package and dependencies (#1216)",
  "Tags": [],
  "RuleID": "generic-api-key",
  "Fingerprint": "215c131cfccf749a5456ecaf4c493cedb647272c3:public/assets/i18next-9-0-1/.coveralls.yml:generic-api-key:1"
},
```

7) **Secret type:** Private key

**Exposed Secret:**

----BEGIN RSA PRIVATE KEY----

```
MIIEpAIBAAKCAQEArmjyxQOgKQ17D4IEG0XvDP3Q58oq+6bqRkDCgFIrj6GkSbbt
9NKRwgA+ewjKO5uef8JuFSWGzOTCE9E5k1ZnjzdRKCXDackDWo52DfbxgDmVRp3
g95BjEUzoVkJ717TZ6nxZxLNqQHmcckmPFBZI3lWX3nFYflaSgosL4ODbuCr1o/i7R
2ofMkz86Q23kAmXCRfiugmObhXrNZbNjOrGUdiAx9DN5N0dX+ywIJ6UbWnHuqbXE
+Vbhy6hEfur3AzWDQOdPy/2lezTba2KLauKJbteGnt0wJ/ar311fqTdJ8r1HJ8Qq
6MNjuMBC+k4ku7F2HY60axG9RP7jfUqbL5N/bwIDAQABAoIBAAWlrEaoYWTK5PMP
mlxhxT38cekvaJjhXLCPnP6Xpp3t8+3XGHIW4BVSALPnlvJvlsCsdaucQYf4USHx
uJ9kAIRZICj6sillAgvVJq5TkLAmk06qHriMV7789qEAzKk9V9j50cZGsOgJiAJN
bLGzfE1AEfZj63ohZHogqfzX+nkqfy62tuQkrw5mHCHAxuHzIXKe5D/3ugOJAjt7/
K7pcsbFjj0N43lNm5ffn4JXX7Ko/y8asBSFEmmWIKp39wlcd6A/us18eYjFCIP
6GowncGruFxQSQoZK+603nWqw1CdrZIQlaCdD1AtDkP8YZUzJWDQjdr2o35Ef/lb
UGnCxmECgYEAE1LC8QY09n4Qjkovyvf+t8tlbM1e5DD0wsDAQRFXiORLeOJsETIG
BYrehIYsTDjSGtl/SqHnprmMo/mczfvjVbcxNAq518b1KQiwb61uiXCLj1IAlc+
WKyPVCgjlajQowjYRo7guy6XGWWprZK7RaU+Sqz3JYt2vQ3KIPyISSkCgYE0ey0
uQMdwY7YwYzn48/OUnhU0MF15YEJfbwblMKQMDfK8yUQ796F44L53F9+Uxf05+o4
89vSUugOGYg6+znpDhBM9w2SzAxL54PtM+YZCw7EXJswWHYrK+JcgHYS1SWZAtMx
BsO5pjgUmaapGhNmUM51uxzeN5XSrjQ8X4dZXtcCgYEAxRswq8pqLe1ohgQaJohP
bVKFMOmk2fagreexg9uliwZ/Bv1WxyzDtdk3VDt/y/eQhv9vXvcun60vMDtAXQX
lz3fhKmiSR+0DAE8knkkikx5mZROLUAjgEwS3BwCSsZA0oZ84A7DJ9UKhkfZcpkb
4nQ74Tqgl/Q2Swf/fUhrCNkCgYEAn9PRkN8vg5Pnsg0+7HLmCml1aS8SQu1otYNH
ml49y4hfc5pX99j7JUouRDusaUVfEdzDy95RcgKHCRdi7L+nselYbzC3HosPFt0
eMQiowmeNUeumlt16RaSCPhcxE243q6+sADK0yP1gzqhmwnUJ4fZmRmUksuOOTXq
FW1ufMcCgYBTqhDgLjj2kM5ZCL6TGZ63zQ0lxBgYGwUPsa3JwecDkQOPftc37zte
cZ9K9WuMJccMfbIgJl7K2YL9Jp91KeHRvural2kWwl4VynuVAnJVKxxNEsnZn27
YWDo52SqT/WajC99HKjnW3aD2PCZ5tma/VQejrZv8XVZMbPlkUipCg==
```

----END RSA PRIVATE KEY----

## Screenshot of code:

```
contrib > util > docker > ldap-ssl-certs-keys > easy > ca-key.pem
Brady Miller, 4 years ago | 1 author (Brady Miller)
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEpAIBAAKCAQEArmjyxQ0gKQ17D4IEG0XvDP3Q58oq+6bqRkDCgFlrj6GkSbbt
3 9NKRwgA+ewjKO5uef8jJuFSWGsOTCE9E5kIZnjzdrKCXDackDW52DfbxgDmVRp3
4 g95BjEuZoVkJ717TZ6nXzLnqQHmcKmPFBZI3lwX3nFYfIaSgosL40DbuCr1o/i7R
5 2ofMkz86Q23kAmXCrFiuigmObhXrNZbNjOrGUdiiAx9DN5N0dx+ywIJ6ublnHuqbXE
6 +Vbhy6hEfur3AzWDQdPy/2IezTba2LAUkjBteGnt0wJ/ar311fqTdj8r1HJ8Qq
7 6MNjuMBC+k4ku7F2HY60axG9RP7jfUqlb5N/bwIDAQABoIBAAWlrEaojWTK5PMp
8 mIxhT38cekaVjJhXLCNpD6Xpp3t8+3XGHl4W4BVSALPnIVuVisCsdaucQYf4UShx
9 uJ9kAIRZICj6sillAgvVJq5TkLAmk06qHriMV7789qEAzKk9V9j50cZGs0gJiAJN
10 blGzfE1AEFzJ63ohZhogqfzX+nkqfy62tUqkrw5mHCHAxuHzIXKe5D/3ugOJat7/
11 K7rpccsbfjj0N43INm5ffn4jJXX7Ko/y8asBSFEmmWiKp39wlcd6A/us18eYjFCIP
12 6GownGruFxQSQoZK+603nWqw1Cdr2lQtaCdD1AtDkP8YZUzJWDQjdr2o35Ef/Ib
13 UGnxCxeCgYEAE1LC8QY09n4Qjkoovyvf+t8lsBmle5DD0wsDAQRfxiORLeOJ+ETIG
14 BYrehIYsTDjSGt1/SqHhnprMo/mczfjvBvcxNAq518b1KQiwl61uiXCLj1lAlcc+
15 WKyPVCgjIaJQowjYRo7guy6XGwNprZ7RaU+Sqz3JYt2vQ3KIPyISSkCgYEAE0ey0
16 uQMdvY7wYzn48/OUnhUOMFL5YEJfbwb1MKQMDfK8yUQ796f44L53F9+Uxf05+o4
17 89vSuugOGYg6+znpDhBM9w2SzAxL54PtM+YZCw7EXJswWHYrK+JcgjHYS1SWZAtMx
18 Bs05pjglmaapGhMmlJM51uxzeNSXsrj08X4dZXtcCgYEAxRswq8pqle1ohgQaJohP
19 bVKfM0mk2fagreexg9uliwZ/Bv1WxyztDdk3VDT/y/eQhv9Xvcunc60vMDExAXQX
20 Iz3fhKmiSR+0DAE8knkkikx5mZROLUAjgEwS3BwCSsZA0oZ84A7DJ9UKhKfZcpkb
21 4nQ74TqgT/Q2Swf/fuhrCNkCgYEAn9PRkN8vg5Pnsq0+7HlmCml1aS8SQu1otYNH
22 mI49y4hfC5px99j7JUouRDusaUVfIEdzDy95RcgKHCRdi7L+nsEIYbzC3HosPFT0
23 eMQiowmeNUeumlt16RaSCPhcxE243q6+sADK0yP1gzqhmwnUJ4fZmrRmUksuOOTxq
24 Fw1ufmcCgYBTqhDglij2kM5ZCL6TGZ63zQ0lxBgYGwUPsa3JweeDkQOPFTc37zte
25 cZ9K9WuMjccMfb1gJl7k2YL9jP91KeHRvuraI2kWwII4VynuVAnJKoxNEsnZn27
26 YWDo52SqT/Wajc99HKjnW3aD2PCZ5tma/VQejrjzv8XVZMbPlkUiipCg==
27 -----END RSA PRIVATE KEY-----
28
```

## Tool generated output:

```
{
  "Description": "Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.",
  "StartLine": 1,
  "EndLine": 27,
  "StartColumn": 1,
  "EndColumn": 29,
  "Match": "-----BEGIN RSA PRIVATE KEY-----\nMIIEpAIBAAKCAQEArmjyxQ0gKQ17D4IEG0XvDP3Q58oq+6bqRkDCgFlrj6GkSbbt\n9NKRwgA+ewjKO5uef8jJuFSWGsOTCE9E5kIZnjzdrKCXDackDW52DfbxgDmVRp3\nFile": "contrib/util/docker/ldap-ssl-certs-keys/easy/ca-key.pem",
  "SymlinkFile": "",
  "Commit": "62c506acb492c087671a965d304c856afb6c8f59",
  "Entropy": 6.0210257,
  "Author": "Brady Miller",
  "Email": "brady.g.miller@gmail.com",
  "Date": "2020-08-19T19:32:39Z",
  "Message": "Ldap tls support (#3870)\n\\* ldap tls support\n\\* updates",
  "Tags": [],
  "RuleID": "private-key",
  "Fingerprint": "62c506acb492c087671a965d304c856afb6c8f59:contrib/util/docker/ldap-ssl-certs-keys/easy/ca-key.pem:private-key:1"
},
```

**8) Secret type:** Private Key

**Exposed Secret:**

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEAxitr10bBdY7zHhrXE8u9tFXJk71wSII63tBo0insHMonDYhc  
XXZte2DPRnTB/k+j6AkjkMxtTUbF6tkbhZIKcfWSBv7onfqSLsc9BkIlfDLDgy  
6NEMNmKCQwqfgvo5V8FiDPIBeVINevf3Nzk/JLzPewUN1neghKg1GUTXt835JDSY  
HILLBk4HLrCVR9lnuy9Lm4IDQ4EJm9KN1+04ofzBQ2W3p25DpAzqaL3QTVHfK/rQ  
tvPQR09ds1KeYfb7/rpzE1cPf8AcsW2AsBWDZROFEdtJ7eWga9LX4s/r28f5MdDC  
L6IWwcGblcOj6LSn4DZJ6IEVQMvxBifQAkanwlDAQABAoiBAQC3umA0aiRl8uzS  
d336m4XZYUQPPlq44gkYJuF3GpBmFo6LLeCZyfK8KmXnyz6NgPcQwB/EUWnwWjhL9  
QeIN65iiK+WuW0tUmSr8nYY9hcvA85s/Lyd8FPzmmzQ8Jeg3zfhGNUPLzr+xFHLt  
FGL+rzOswuT2IHxw393yz2aw89OwU0LzegmlKm4tNPIBDVwYqrbluaf5wUubO1J  
XK1ytWuJcx5+QIHhkWKebjjoW5xdH+iKF5Ppd9dX8Ct+6SzzxLR2HVnMPN1UT34  
wwUI5rajq02l0osl1WFL9qgHBG5ZAUn85sMMyK/sXAbQVtzSPIYwifMvn9TOWCmU  
dPNfZy/BAoGBAPPzY0TzBVHcQRW1TCsVBw4NGKrae5RNO6ifxlh5wF1Y5KxKCq  
5zXpP9HUKiOhHwdlXgDa8H9a/Kwm+L4gUZ7Z0z9O9EEEds08M2nIUnh8wKrQGdEQV  
ETflk+Xf0WcZ64Lncks9QIR2IktdSdtiS1id1AhssmhXqoh4oqoO/AoGBAM/1  
K10mxllSfcSQ6KWlKgOWxUbktYaG6swDTALnrZP/0SlbLJ96drz8sLATw67WGys  
O8eBKHoLD+9IKmLEgnoHPacEa9ykxrPORWHV84OhqjPzFmpcQ20kAZekvgrAwkOl  
jYFrLj5PXECetPaSNsBzrsNUtKW6rSKGJisLjaEhAoGBAKn6DFEa3/hvRq426cxF  
XAeQn5Vha15SWQKuFzcmBzdPWV2r+xV3/2lxA6bQjgwFV/lvR/CQnMlgQ64v+WGA  
Y16rp+WUvdwhNa7+5bZXZ1WT2i1V0e0eQMER1dt1+BI+nTq4yYpjRJLdduMeUOC0  
gxih/2++t5j3muVqd0tMSoNBAoGAOKczOvD6zeZZOPm5R5Ziy8OBTwTzpwIOYrH  
rPUcdcdFtW4BHDFc+jdHRWMaporHViO9zWYUXtswpiFk2q9qVFAwrZV4xQ1mzllb  
lrGwu4WJVsm8q5EjfVKf1G4fD9LfmYo6eK14VaVNhpWd+yZuiBPj4nbrF9M5Y5Rk  
RYnKNcECgYEAnAoATpLcHa5OH5bDtO8PxftsoUHr+W6pSeYPeZLIRWsFNZnl6cnA  
qyJh6YNrlDJabFcFq9HmYgVVaYa15P5vB7KpweepgJJZ7Vdws+78ZA7fmyR+cKDj  
PG++Yr9Lj8sJILQzuqcTA/XvX0cJb6f4oK/YbmXwEa8DFxnG8R6TcN8=

-----END RSA PRIVATE KEY-----

## Screenshot of code:

```
contrib > util > docker > ldap-ssl-certs-keys > easy > 🔒 client-key.pem
Brady Miller, 4 years ago | 1 author (Brady Miller)
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEpQIBAAKCAQEAxitr10bBdY7zHhrXE8u9tFXJk71wSI163tBo0insHMonDYhc
3 XXZte2DPRnTB/k+j6AkjktMxtTUbF6tkbhZIKcfWSBv7onfqSLsc9BkILLfLDgy
4 6NEMNmKCQwqfgvo5V8FiDPIBeVINevf3Nzk/JLzPewUN1negHkG1GUTXt835JDSY
5 HILLBk4HLrCVR9lnuy9Lm4lDQ4EJm9KN1+04ofzBQ2W3p25DpAzqaL3QTVhfK/rQ
6 tvPQR09ds1KeYfB7/rpzE1cPf8AcsW2AsBWDZROFEdtJ7eWga9LX4s/r28f5MdDC
7 L6lWwcGb1c016LSn4DZJ6IEVQMVxvBIfQAKanwIDAQABAoIBAQCB3umA0aiRI8uzS
8 d336m4XZYUQP1q44gkYJuF3GpBmFo6LLeCZyfK8KmXnyz6NgPcQwB/EUwnwWjhL9
9 QelN65iiK+WuW0tUmSr8nYY9hcvA85s/Lyd8FPzmmzQ8Jeg3zfGNUPLzr+xFHlt
10 FGL+rzOswuT2IHxw393yz2aw890wU0LzegmIKm4tNPiBDWvYqrbluaf5wUub01J
11 Xk1ytWu1Jcx5+Q1HHkWKebjjoW5xdh+iKF5Ppd9dX8Ct+65zzxLR2HvnMPN1UT34
12 wwUI5rjaq02I0os11WF9qgHBG5ZAUn85sMMyK/sXAbQVtzSP1YwifMvn9TOwCmU
13 dPNfZy/BAoGBAPPzY0TtzBVBHcQRW1TCsVBw4NGKrae5RNO6ifx1h5wF1Y5KxKCq
14 5zXpP9HUKi0hHwd1XgDa8H9a/Kwm+L4gUZ7Z0z909EEds08M2nIUhn8wKrQGdEQV
15 ETf1k+Xf0WcZ64Lncks9QiRt2IktrdSdti1S1id1AhssmhXoh4oqo0/AoGBAM/1
16 KI0mxIl5fcSQ6KWi0xUbktYaG6swDTALnrZP/0SiBLJ96drz8sLATw67WGys
17 08eBKHoLD+9IKmLEgnoHPacEa9ykxrP0rWHV840hqjPzFmpcQ20kAZekvgrAwk01
18 jYFrLj5PXECetPaSNsBzrsNUTKW6rSKGJisLjaEhAoGBAkN6DFEa3/hvRq426cxF
19 XAcQn5Vha15SWQKuFzcmBzdPWV2r+xV3/2IxA6bQjgwFV/lvR/CQnMIgQ64v+wGA
20 Y16rp+wUvdwhNa7+5bzXZ1WT2i1V0e0eQMER1dt1+BI+nTq4yYpjRJLdduMeUOC0
21 gxiH/2++t5j3muVqd0tMSoNBAoGAOKcz0vD6zeZZOPm5R5Zziy80BTwTzpwiOYrH
22 rPUdcdfTw4BHDIFc+jdHRWMaporHVi09zWYUXtswpiFk2q9qVFawrZV4xQ1mzIlb
23 1rGwu4WJVsm8q5EjFVKf1G4fD9Lfmy06eK14VaVNhpWd+yZuIBPj4nbrF9M5Y5Rk
24 RYnKnCgYEAnoATpLcHa50H5bDt08PxfsoUHr+W6pSeYPeZl1RWsFNZnI6cnA
25 qyJh6YNrLDJaBFcFq9HmYgVVaYa15P5vB7KpweepgJJZ7Vdws+78ZA7fmyR+cKDj
26 PG++Yr9Lj8sJILQzuqcTA/XvX0cJb6f4oK/YpmXwEa8DFxnG8R6TcN8= Brady
27 -----END RSA PRIVATE KEY-----
28
```

## Tool generated output:

```
{"Description": "Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.", "StartLine": 1, "EndLine": 27, "StartColumn": 1, "EndColumn": 29, "Match": "-----BEGIN RSA PRIVATE KEY-----\\nMIIEpQIBAAKCAQEAxitr10bBdY7zHhrXE8u9tFXJk71wSI163tBo0insHMonDYhc\\nXXZte2DPRnTB/k+j6AkjktMxtTUbF6tkbhZIKcfWSBv7onfqSLsc9BkILLfLDgy\\n6NEMNmKCQwqfgvo5V8FiDPIBeVINevf3Nzk/JLzPewUN1negHkG1GUTXt835JDSY\\nHILLBk4HLrCVR9lnuy9Lm4lDQ4EJm9KN1+04ofzBQ2W3p25DpAzqaL3QTVhfK/rQ\\ntvPQR09ds1KeYfB7/rpzE1cPf8AcsW2AsBWDZROFEdtJ7eWga9LX4s/r28f5MdDC\\nL6lWwcGb1c016LSn4DZJ6IEVQMVxvBIfQAKanwIDAQABAoIBAQCB3umA0aiRI8uzS\\nd336m4XZYUQP1q44gkYJuF3GpBmFo6LLeCZyfK8KmXnyz6NgPcQwB/EUwnwWjhL9\\nQelN65iiK+WuW0tUmSr8nYY9hcvA85s/Lyd8FPzmmzQ8Jeg3zfGNUPLzr+xFHlt\\nFGL+rzOswuT2IHxw393yz2aw890wU0LzegmIKm4tNPiBDWvYqrbluaf5wUub01J\\nXk1ytWu1Jcx5+Q1HHkWKebjjoW5xdh+iKF5Ppd9dX8Ct+65zzxLR2HvnMPN1UT34\\nwwUI5rjaq02I0os11WF9qgHBG5ZAUn85sMMyK/sXAbQVtzSP1YwifMvn9TOwCmU\\ndPNfZy/BAoGBAPPzY0TtzBVBHcQRW1TCsVBw4NGKrae5RNO6ifx1h5wF1Y5KxKCq\\n5zXpP9HUKi0hHwd1XgDa8H9a/Kwm+L4gUZ7Z0z909EEds08M2nIUhn8wKrQGdEQV\\nETf1k+Xf0WcZ64Lncks9QiRt2IktrdSdti1S1id1AhssmhXoh4oqo0/AoGBAM/1\\nKI0mxIl5fcSQ6KWi0xUbktYaG6swDTALnrZP/0SiBLJ96drz8sLATw67WGys\\n08eBKHoLD+9IKmLEgnoHPacEa9ykxrP0rWHV840hqjPzFmpcQ20kAZekvgrAwk01\\njYFrLj5PXECetPaSNsBzrsNUTKW6rSKGJisLjaEhAoGBAkN6DFEa3/hvRq426cxF\\nXAcQn5Vha15SWQKuFzcmBzdPWV2r+xV3/2IxA6bQjgwFV/lvR/CQnMIgQ64v+wGA\\nY16rp+wUvdwhNa7+5bzXZ1WT2i1V0e0eQMER1dt1+BI+nTq4yYpjRJLdduMeUOC0\\ngxiH/2++t5j3muVqd0tMSoNBAoGAOKcz0vD6zeZZOPm5R5Zziy80BTwTzpwiOYrH\\nrPUdcdfTw4BHDIFc+jdHRWMaporHVi09zWYUXtswpiFk2q9qVFawrZV4xQ1mzIlb\\n1rGwu4WJVsm8q5EjFVKf1G4fD9Lfmy06eK14VaVNhpWd+yZuIBPj4nbrF9M5Y5Rk\\nRYnKnCgYEAnoATpLcHa50H5bDt08PxfsoUHr+W6pSeYPeZl1RWsFNZnI6cnA\\nqyJh6YNrLDJaBFcFq9HmYgVVaYa15P5vB7KpweepgJJZ7Vdws+78ZA7fmyR+cKDj\\nPG++Yr9Lj8sJILQzuqcTA/XvX0cJb6f4oK/YpmXwEa8DFxnG8R6TcN8=\\nBrady\\n-----END RSA PRIVATE KEY-----", "Secret": "-----BEGIN RSA PRIVATE KEY-----\\nMIIEpQIBAAKCAQEAxitr10bBdY7zHhrXE8u9tFXJk71wSI163tBo0insHMonDYhc\\nXXZte2DPRnTB/k+j6AkjktMxtTUbF6tkbhZIKcfWSBv7onfqSLsc9BkILLfLDgy\\n6NEMNmKCQwqfgvo5V8FiDPIBeVINevf3Nzk/JLzPewUN1negHkG1GUTXt835JDSY\\nHILLBk4HLrCVR9lnuy9Lm4lDQ4EJm9KN1+04ofzBQ2W3p25DpAzqaL3QTVhfK/rQ\\ntvPQR09ds1KeYfB7/rpzE1cPf8AcsW2AsBWDZROFEdtJ7eWga9LX4s/r28f5MdDC\\nL6lWwcGb1c016LSn4DZJ6IEVQMVxvBIfQAKanwIDAQABAoIBAQCB3umA0aiRI8uzS\\nd336m4XZYUQP1q44gkYJuF3GpBmFo6LLeCZyfK8KmXnyz6NgPcQwB/EUwnwWjhL9\\nQelN65iiK+WuW0tUmSr8nYY9hcvA85s/Lyd8FPzmmzQ8Jeg3zfGNUPLzr+xFHlt\\nFGL+rzOswuT2IHxw393yz2aw890wU0LzegmIKm4tNPiBDWvYqrbluaf5wUub01J\\nXk1ytWu1Jcx5+Q1HHkWKebjjoW5xdh+iKF5Ppd9dX8Ct+65zzxLR2HvnMPN1UT34\\nwwUI5rjaq02I0os11WF9qgHBG5ZAUn85sMMyK/sXAbQVtzSP1YwifMvn9TOwCmU\\ndPNfZy/BAoGBAPPzY0TtzBVBHcQRW1TCsVBw4NGKrae5RNO6ifx1h5wF1Y5KxKCq\\n5zXpP9HUKi0hHwd1XgDa8H9a/Kwm+L4gUZ7Z0z909EEds08M2nIUhn8wKrQGdEQV\\nETf1k+Xf0WcZ64Lncks9QiRt2IktrdSdti1S1id1AhssmhXoh4oqo0/AoGBAM/1\\nKI0mxIl5fcSQ6KWi0xUbktYaG6swDTALnrZP/0SiBLJ96drz8sLATw67WGys\\n08eBKHoLD+9IKmLEgnoHPacEa9ykxrP0rWHV840hqjPzFmpcQ20kAZekvgrAwk01\\njYFrLj5PXECetPaSNsBzrsNUTKW6rSKGJisLjaEhAoGBAkN6DFEa3/hvRq426cxF\\nXAcQn5Vha15SWQKuFzcmBzdPWV2r+xV3/2IxA6bQjgwFV/lvR/CQnMIgQ64v+wGA\\nY16rp+wUvdwhNa7+5bzXZ1WT2i1V0e0eQMER1dt1+BI+nTq4yYpjRJLdduMeUOC0\\ngxiH/2++t5j3muVqd0tMSoNBAoGAOKcz0vD6zeZZOPm5R5Zziy80BTwTzpwiOYrH\\nrPUdcdfTw4BHDIFc+jdHRWMaporHVi09zWYUXtswpiFk2q9qVFawrZV4xQ1mzIlb\\n1rGwu4WJVsm8q5EjFVKf1G4fD9Lfmy06eK14VaVNhpWd+yZuIBPj4nbrF9M5Y5Rk\\nRYnKnCgYEAnoATpLcHa50H5bDt08PxfsoUHr+W6pSeYPeZl1RWsFNZnI6cnA\\nqyJh6YNrLDJaBFcFq9HmYgVVaYa15P5vB7KpweepgJJZ7Vdws+78ZA7fmyR+cKDj\\nPG++Yr9Lj8sJILQzuqcTA/XvX0cJb6f4oK/YpmXwEa8DFxnG8R6TcN8=\\nBrady\\n-----END RSA PRIVATE KEY-----", "File": "contrib/util/docker/ldap-ssl-certs-keys/easy/client-key.pem", "SymlinkFile": "", "Commit": "62c506acb492c087671a965d304c856afb6c8f59", "Entropy": "6.01207", "Author": "Brady Miller", "Email": "brady.g.miller@gmail.com", "Date": "2020-08-19T19:32:39Z", "Message": "Ldap tls support (#3870)\\n\\n* ldap tls support\\n\\n* updates", "Tags": [], "RuleID": "private-key", "Fingerprint": "62c506acb492c087671a965d304c856afb6c8f59:contrib/util/docker/ldap-ssl-certs-keys/easy/client-key.pem:private-key:1"}]
```

**9) Secret type: Private Key**

**Exposed Secret:**

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEA1O3a0T78PopUxuBRsARC7gnONEwgtkoDyu0vt5j2p1ydhMAP  
VNsZ5sSwaECgiZ8uzjDgMiQFCUj+IxTn9W9nMQPc7g/o25lrgtQQqQTkGovJXnac  
y1ToSe5QYrDRya8WMRDzMPFVNl9esuwoGgbzZWixfq2coJx9u25V0uqPvvPS0Xh  
DOo01t/Urc/Gt9TAXaDHDHovSAtWUv7c3POmGQf01Ogydwa047yYMu1U0CH3Xrtq  
fPv19D6BVs4U4XHsbyrCP/9s+P6uBKeNNRrcBRIhKvcVLGGTZ5l1s1O8T4fYJx  
yYXZczJSWMBK2l6Dw708IAFEfUUlfWeXVuEQIDAQABaoIBAQDHS93crkRw0Q8q  
mjK7M7HII73xCzQvCrXkEP7xrHVpDrHM1+tBtFXY/k5TNfJM/bZUfcDKjZY9K5pH  
IOTLf7spUIFQPYnpSP7LvKPfx1mUn35aMVDurAIDcZDB3thtGrj9sey96ZSj617a  
v1mFlu30A/rml9+PIQo6Dbq80JIAmLSRjpq0LGYz/hezXK4iuvkE1nKD7rLPtkHB  
llhFbQ5d0yhvlMw7YA+tiTeAAF+x+UPsp5fMZ9cfBU31jPYkc2YorgRKLwp3qcbv  
yPvrD0fzln9xvojjRc6GyKA2qPISiLjYLIdpcDV/+RXFPZzfgfzBs0ensfdwZJyf  
uTjmqfHV AoGBAPdsZ5u7/VG3RXbfpfrlhGPvir4YRHd8kkFyQ4Cv9t9vElV6ciln  
9j4u9eurk5pimG71a4gt5Ju00FAf5RoWWQeNzrdWm66ZRjS8YluTwP/1W4eSP51  
ReDWw34AZZJkmK3KiNRB2U0PIPpxW0af1GlaMhVFBotTkxPGgPxmhAoGBAnxP  
Wlpa4dCWn2nPf6/JgwO5sgpXYeP6lHC7DdfzT4CykzroJo71MAms6W1Xvrlx777  
pDnzPqayUFPZnICWIMI4GglDRWqcbah2nqZ5ekpP1dOCyUkpVPfPDMsmZwCv0kQ  
RyvUioqPuW5WNOOKsn89FTXabe5XPP9DWjjgy8GnAoGBAlxjpD5HYqs1NGMjgORI  
ysLxrmXCW0N17KvZ69dfANMyr8ss+Q3pgV0zRDKevjfBbgC3nHY+pBJ9fB2am217  
//Q7UGnS6K8fJSdQfGCgiJEaXr4GzSAk5qt28KHUE84G6mLiItVdL69wFs46dAeP  
gPxHCNsJFamqNZPxDuKTLhQNAoGAaTVX/6hBCHy1ujEGWCtSbregCitE3xUiFOGv  
Nb6ow7FPbLZlpulFspGl3wyjQ/4YLam8hRQdijvDUpetG+0dNq0tOd/D8OHJlh7r  
F/tgqR0yi33QordCYLBNr6RKMjDEqA8blj+RDdopUFz1mol3eyMsYATWWu9zGUc  
s+beRycCgYEAs0L8+OuoUsp7z9wB9vfTMZopEt7DJ4eG9owoo0xOL/RxWNLMvKrB  
+fajHq/nY5ByLojTuQCm6RpkyEkJjB+buS6e11omJHEJw9KynYDgOcL+B35QyMzE  
oSGrVrKxjm0UKsJ6UWF86Dlo8vkr/IUK/6C8KkliPa0MMSUHiudLz0M=

-----END RSA PRIVATE KEY-----

## Screenshot of code:

```
contrib > util > docker > ldap-ssl-certs-keys > easy >  server-key.pem
Brady Miller, 4 years ago | 1 author (Brady Miller)
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEpQIBAAKCAQEAI03a0T78PopUxuBRsARC7gnONEwgtkoDyu0vt5j2p1ydhMAP
3 VNz5ssSwaECgiZ8uzjDgMiQFCUj+lxTn9W9nMQPc7g/o25lrGtQQqQTkGcvJXnac
4 y1ToSe5QYrDRya8WMRDzMPFVNL9esuwoGgbzZwixfq2coJx9u25V0uqPvvvPS0Xh
5 D00o1t/Urc/Gt9TAXaHDHovSATwJv7c3POmQf010gydwa047yYMu1U0CH3Xrtq
6 fPv19D6BVs4U4XHsbyrCP/9s+P6uBKeNNRrcBRIHkvcFVLGGTZ5l1sI108T4FYJx
7 yYXZczJSWMBK216Dw708iAEFfUIILfdWeXVuEQIDAQABoIBAQDHS93crkRw0Q8q
8 mjk7M7H11T3xCzQvCrXkEP7xrHvpDrHM1+tBtFXY/k5TNfJM/bZUfcDKjZY9K5pH
9 lOTLf7spUIFPYnpSP7LvKPfX1mUn35aMDurAlDcZDB3thtGrj9sey96Szj617a
10 v1mFiu30A/rmI9+PIQo6Dbq8J1AmLSRjpq0LGyZ/hezXK4iuvkE1nKD7rLPtckHB
11 llhFbQ5d0yhvIMw7YA+tTeAAF+x+UPsp5fMz9cfBU31jPYkc2YorgRKLwp3qcby
12 yPvrD0fzln9xvojjRc6GyKA2qP1s1jYLIdpcDV/+RXFPZzfgfzBs0ensfdwZJyf
13 uTjmqqfhVAoGBAPdsZ5u7/VG3RXBgpfrl1hGPvir4YRHd8kkFyQ4Cv9t9vEV6c1ln
14 9j4u9eurn5pimG71a4gt5Ju00FAf5RoWQeNzrdWm66ZRjIS8YluTwP/1W4eSP51
15 ReDw34AZZJkmK3K1NRB2U10PIPpxW0af1GiaMhVrFB0TtKxPGgPxmHAoGBAnxP
16 Wlpa4dCwn2nPf6/Jgw05spgXYeP61HC7DdfzT4CykzroJo71MAms6W1XvrIx777
17 pDnzPqayUFPZnlCW1M14G1lRDRWqcbah2nqZekpP1d0CyUkpVPfPDMSmZwCv0kQ
18 RyvUiopuW5WNOOKsn89FTXabe5XPP9Dwjgjy8GnAoGBAIxjpD5HYqs1NGMJgOR1
19 yslxrmXCW0NI7Kvz69dFANMyr8ss+Q3pgV0zRDKevjfBbgC3nHY+pB19fB2am217
20 //Q7UGnS6K8fJ5d0fGCgiJEaxr4GzSAk5qt28KHUE84G6mLiItVdL69wFs46dAeP
21 gPxHCNsJFamqNZPxDuKTLHqNAoGAaTVX/6hBChy1ujEGWCtSbrgCitE3xuiIFOgv
22 Nb6ow7FPbLZlpufFspGI3wyjQ/4YLam8hRQdijvDUpetG+0dNq0t0d/D80HJlh7r
23 F/tgqrOy133QordCYLBNr16RKmjDEqA8bLj+RDdopUFz1moI3eyMsYATWu9zGUc
24 s+beRycCgYEAs0L8+OuoUsp7z9wB9vfTMZopEt7DJ4eG9owoo0x0L/RxWNLMvKrB
25 +fajHq/nY5ByLojTuQCm6RpkyEkjJB+buS6e11omJHEJw9KynYDg0cL+B35QyMzE
26 oSGrVrKxjm0UKsJ6WF86DIo8vkr/IUK/6C8KkIIpa0MMSSUHiudLz0M=
27 -----END RSA PRIVATE KEY-----
```

## Tool generated output:

```
{
  "Description": "Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.",
  "Startline": 1,
  "EndLine": 27,
  "StartColumn": 1,
  "EndColumn": 29,
  "Match": "-----BEGIN RSA PRIVATE KEY-----\nMIIEpQIBAAKCAQEAI03a0T78PopUxuBRsARC7gnONEwgtkoDyu0vt5j2p1ydhMAP\nVNz5ssSwaECgiZ8uzjDgMiQF",
  "Secret": "-----BEGIN RSA PRIVATE KEY-----\nMIIEpQIBAAKCAQEAI03a0T78PopUxuBRsARC7gnONEwgtkoDyu0vt5j2p1ydhMAP\nVNz5ssSwaECgiZ8uzjDgMiQF",
  "File": "contrib/util/docker/ldap-ssl-certs-keys/easy/server-key.pem",
  "SymlinkFile": "",
  "Commit": "62c506acb492c087671a965d304c856afb6c8f59",
  "Entropy": 6.0220375,
  "Author": "Brady Miller",
  "Email": "brady.g.miller@gmail.com",
  "Date": "2020-08-19T19:32:39Z",
  "Message": "Ldap tls support (#3870)\n\n* ldap tls support\n\n* updates",
  "Tags": [],
  "RuleID": "private-key",
  "Fingerprint": "62c506acb492c087671a965d304c856afb6c8f59:contrib/util/docker/ldap-ssl-certs-keys/easy/server-key.pem:private-key:1"
}
```

## 10) Secret type: Private Key

### Exposed Secret:

----BEGIN RSA PRIVATE KEY----

```
MIIEowIBAAKCAQEAxedVAO6KsklNwKpRXT9wFByBXHYKvgoXKi1tBAdlKslChy4m
0K3Mq5rAXBy27j2O+mrgRHQHTFlrzrZYINrdf8ZO2xGJgwMjiRITc5cNR7zFb+
JqjeMDzU+/DjLEmsDclobGSF9XTtmFwodfu8Kg4BUv7AO/EFBNoLev/165Ab7inx
LmSO0yphGxV8oqtEIO7820RyZ0HtLHknXLu9iR3VJNxgWey8P336gZ3syUs6J14
r2acNpyrWhjiuLYrwSdKPASAEFVRYWOvH0atdjql4wyig4VbsjcLZKazP/5Wt+H
PKjykEEfbHbzYKA4EU2u3/v+BxqM8ZFMFE5CnwIDAQABAoBABWH122khh5ipVBi
tzn3W+ysjg293A5dM+35XZcv5rpRJEkakClx/Cbg3YCAbzloZqj6iFIZIYugeSQ
iHnBkn1h5i561ZuRYxznpMXUP5/f4B5rmjSUmn5FEtKUiNTxSoHPG99f0AXaEH
1bcQTiZdI7O913gt/pfKiRk2o7Ce6gbcN5uSDVeQ57qn3SZesDDxjakxsWQMrHPS
gBqF/yTFyzWHDSf/e0M6HPM2ZnzogSngVemtYXG+Mq6h16dzjYQGwwWBeiQL8zcW
BdaNhfkDxs47EiDuqjky5l8kltzFau022Y5CH2iVm9XnGmfMaTjwyqTJfF6kXi3
IGvUrkECgYEAA6ldD10YKPMmLJ7/3K0K0ob1aSnEgbaPe+Hb/7sd2vzZNhBgODPQ0
HnzqKy6pnDtV5TmlbmxBKdL8ycdlw9K/3HMJePppnjfxhPwqV80eYELy2uhpkLS8
gmaL4mfCtSgZk4Ef+6u14iAPT+BEy45PxQfno8ZXOQwFa291LVZ4308CgYEAE2DHT
HyhGdkuP6wcdwBipou1ZJTX1VcXpOJ9k1HG4ZyMrqJwaPP237LmNRNQE13Fx/IMO
+pbmt5KsJTAgo0vMPViRipRV/CGyHcTt1VygZojQB7c6HvFSuBfUP7I7x7y6xIEI
ecqNUoyYOKRw7Pcqodp05+bKmCY4ttNN/JkHE7ECgYACj2mCVJWQEOzyRjqhEl1+
1t7BqXK9P+kTtdkd9rfpZuJ56vlcUt6u5pZ4Wk4oEs3hbzvLdQtRNajlw3QED61g
7zDPTY0R2XKeDVM5GliWnKSi59voUnd8saudou+Bu4gmmyLB1k5WzhPmxelUay1
blytgWE6klMM1W7mS+eOKQKBgF2SNkwO9XhLug2CNfknc3x9/hoAzhNgWSVcGGW
mrZg/YtrjNurAlj/wknb7euFWU4iRBnIZKAc+tgikRjGNcyxIMnG6U8u95hWqcP
XxDaK5+OjScRC4TejTbYo5PFBC1EdMMvN/mpBeX7JxTWetVjtW0CSmTGWbfy9gx
L2PxAoGBAMA83lhO3+omsh+MfW5HEC2t06hRB9HTdiFsJWLQlePYCpaINJeg5VV
dXj/+mxNBO//vZlr+5jGv3S8R0tWq61QLicDId/xB68e5ORuz+GM+rP5CP/An0RD
uDze2Z9woka08FeDYcfCDLAtS3xVXToycW0wn/gge1AxKeARXXqa
```

----END RSA PRIVATE KEY----

## Screenshot of code:

```
contrib > util > docker > ldap-ssl-certs-keys > insane > ca-key.pem
Brady Miller, 4 years ago | 1 author (Brady Miller)
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEAxedVA06KskINwKpRXT9wFBByBXHYKvgoXKi1tBAdlKsIChy4m
3 n0K3Mq5rAXBy27j20+mrgRHQHtFflrzrZYINrdf8fZ02xGJgwMjiR1Tc5cNR7zFb+
4 JqjeMDzU/+DjLEmsDcIobGSF9XTtmFwodfu8Kg4BUv7AO/EFBNolev/165Ab7inx
5 LmS00yphGxV8oqtEl07820RyZ0HtLhnXLu9iR3VJNXgWeyP336gZ3syts6JI4
6 r2acNpyrWhjiuLYrwSdKPASAEFVRYW0vH0atdjql4wyig4VbsjcLZKazP/5Wt+H
7 PKjykEEfbHbzYKA4EU2u3/v+BxqM8ZFMFE5CnwIDAQABoIBABWH122khh5ipVBi
8 tztn3W+ysjg293A5dM+35XZcv5rpRJEkakClx/Cbg3YCAbzloZqI6iFIZlYuge5Q
9 iHnBkn1h5i561ZuRYxznpMXUP5/f4B5rmjSUmns5FETKUizNTxSoHPG99f0Axah
10 1bcQTiZdI70913gt/pfKiRk2o7Ce6gbcN5uSDVeQ57qn35ZesDDxjakxswQMrHPS
11 gBqF/yTFyzWHDsf/e0M6HMPM2ZnzogSngVemtYXG+Mq6h16dzjYQGwwNBeiQL8zcW
12 BdaNhfkDxs47EiDuqjky5I8lktzFa02zY5CH2ivmx9XnGmfMaTjwyqTJff6kXi3
13 IGvUrkECgYEAlld10YKpmMLJ7/3K0K0ob1aSnEgbap+Hb/7sd2vzNhBg0DPQ0
14 HnzqKy6pnDtV5TmlbmxBKdL8ycdIw9K/3HMjePppnjfxhPwqV80eYELy2uhpkLS8
15 gmAL4mfCtSgZk4Ef+6u14iAPT+BEy45PxQfno8ZXQwFa291LVZ4308CgYEADht
16 HyhGdkuP6wcdwBipou1ZJT1VcXp0J9k1HG4ZyMrqJwaPP237LmNRNQE13Fx/iMO
17 +pbmt5KsJTAg0vMPViRipRV/CgyHcTt1VygZojQB7c6HvFSuBFUP7I7x7y6xIFEI
18 ecqNUoyYOKRw7Pcqodp05+bKmCY4ttNN/JkHE7EcGYZcj2mCVJWQE0zyRjqhE11+
19 1t7BqXK9P+kTdkd9rfpZuJ56vlcUt6u5pZ4Wk4oEs3hbzvLdQtRNaj1W3QED61g
20 7zDPTY0R2XKeDVM5GliWnKs159voUnd8saudou+Bu4gmmlyLB1k5WzhPmxelUay1
21 blytgWE6k1MM1W7mS+eOKQKBgF2SNkw09XhLug2CNfknc3x19/hoAzhNgWSVcGGW
22 mrZg/YtrjNurAIj/wknw7euFWU4iRGBnIZKAc+tgikRjGNcyx1MnG6U8u95hWqcP
23 XxDK5+OjScRC4TejTbYo5PfBKC1EdMMvN/mpBeX7JxTwetVjtW0CSmTGwbfy9gx
24 L2PxAoGBAMA83Ih03+omsh+Mfw5HEC2to6hRB9HTdiFsJWLaqlePYCpa1NJeg5W
25 dXj/+mxNBO//vZIr+5jGv3S8R0tWq61QLicDId/xB68e50Ruz+GM+rP5CP/An0RD
26 uDZe2Z9woka08FeDYcfCDLAtS3xVXToycW0wn/gge1AxKeARXXqa
27 -----
28 |
```

## Tool generated output:

```
{
  "Description": "Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.",
  "StartLine": 1,
  "Endline": 27,
  "StartColumn": 1,
  "EndColumn": 29,
  "Match": "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAxedVA06KskINwKpRXT9wFBByBXHYKvgoXKi1tBAdlKsIChy4m\nn0K3Mq5rAXBy27j20+mrgRHQ",
  "Secret": "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAxedVA06KskINwKpRXT9wFBByBXHYKvgoXKi1tBAdlKsIChy4m\nn0K3Mq5rAXBy27j20+mrgRHQ",
  "File": "contrib/util/docker/ldap-ssl-certs-keys/insane/ca-key.pem",
  "SymlinkFile": "",
  "Commit": "62c506acb492c087671a965d304c856afb6c8f59",
  "Entropy": 6.027987,
  "Author": "Brady Miller",
  "Email": "brady.g.miller@gmail.com",
  "Date": "2020-08-19T19:32:39Z",
  "Message": "Ldap tls support (#3870)\n\n* ldap tls support\n\n* updates",
  "Tags": [],
  "RuleID": "private-key",
  "Fingerprint": "62c506acb492c087671a965d304c856afb6c8f59:contrib/util/docker/ldap-ssl-certs-keys/insane/ca-key.pem:private-key:1"
},
```

**Gitleaks false positive pattern:**

Gitleaks often produces false positives primarily in documentation, readme files, and test code. This issue arises because Gitleaks employs a keyword-matching approach within the codebase, identifying terms like "password" or "token." However, the tool tends to interpret any such match as a potential hardcoded password, even when these instances are benign, such as in testing code or documentation. Notably, Gitleaks may flag variables named "password" or "token" as if they were actual hardcoded credentials, leading to a substantial number of inaccuracies. This behavior can be attributed to the tool's keyword-centric analysis, causing a significant volume of false positives that may not impact the production code but can create challenges in accurately identifying genuine security vulnerabilities.

## **Tool 2: SpectralOps**

### **1) Secret type: Private Key**

#### **Exposed Secret:**

-----BEGIN RSA PRIVATE KEY-----

```
MIIEogIBAAKCAQEA0LBNHVcD+lgc0o8IWsZ7NqVc891Qma4jG2/WrnR/TZyiCa18
/z6r/y32FT1/qg8kHEqvko8oK5Dv1Ju5kqomPUF7fs3sF1TBMbocaYYhIlnub/
7pis3eCEk60Uhq4KRlseCashCJavAqK9C2OFrld3tpklceNDAv/6ArsOPK02L55E
LMEVJfHPcoacxicG5y/WDA38V60qZcFFXnmf1f7L5TEOkZzStG2Sqh16xbt0s++
QyG814t8/INVRaGt+35eZg4RxP3l6kfgajBeayt1xfSqrG+g4nB10kWPeJ30QCrS
+fGbdMRLM81/CW9RCZeQY/BYmHSb4AXt2QdF0wIDAQABaoIBAEjCz4BFUIu+oP4B
BMaxoVAiQ9B6/5k1j+QHEHDvCVvEGvMI3CYacdmc6snpEVp3x31dxPyx4YWcfN5+
HVCKA1KhS5oYaewYw47sspurJlI9C2hr3hwQe2U43MCofhmfINH6/vQcCH54Gzju
CL+pyXhHnra5kk0tK6dFUxSb9pTYPbYXubf37zVsp7dkDG5O711Luuta7hLZYmu
xyiafrgXYRicutGdlvxx/DXIxx5RjSbk+pdkP2UAKsDpHFzsyz3cNvoTTpEtS5S8J
E9F3I8Hlf59eOkj8qWF7gEUSz9GdHUYcomeQRwlISmxIDsGeds18SNIdDzPKs/x
EY+JrdECgYE61ozyXnvCfGOr8ZGPEizt4K9QAVjBL22cH0eKQ+6jtJxXclIOBU
90rEV/EAQd3+O3g1UJyeox9VFgxqZaz2UblrKeOmOnlYbBQx1cJ3TwcwIFOVKrta
4JiCi0BxAEWudw5TlZZqeJGcp1toqhOS1NTJWEgsUP7KvVuxpj1dc0CgYE4v9B
27T2fjv3oloBDM8L8kNc8Sp1EWXpJTd9buT3adoWTs3KliDeOuKTfVFqe6rbTrR5
6+jICfzRuu3+H3US90s51u5tklu3kzlGRoCoYoxrRffciQEzznEMD8JH33UID8
r4DC+mmpyFXZFN2pB+qFNizXOp+4795Pyv2dECh8CgYAeEY8uPYLZvV/g0RNuyVgO
H/Y8aP9XvxCEr7ABPdK/8EUzkqpYqPYWFgPeD31LFyP0oLVQr1Nz/H5+CobxWZO
+KaFWo1hSSGP5WCck9TUZvGyH5ueMwOgUDvILzKAu2ZX1Z/CQm5l6wydoSMVH5R
zgHPYqEu0+6pFK70ssjJPQKBgA/gmtKrTbJ2r1NjU795m/ROEeosdhPJdQ1NXFCt
Y0DcKENK0ai+k8y6nGZfk3si8EQJC54cpCh5lZHlo6/n5v8fwcxlihOHYEGuqGm
2BhEekUJLm/ti+ZMIDzvwrMqvGndkE8WSo0JdQFbTGwb2pGVRr89/D5yw28Fwizx
JCkxAoGADLGduclOCVk1lwOZJCcdVwkKO8/y3R4ENcrVJQpqRhPCI1u3lphwCayR
YuydpjuWNTasvaVzXxi+CabWNLJrgyGYbFZ+rUXJ6ZmWsc3Eg8glp8GSzf4XKRx
jeCDD+VX10fL3P/n2hdpkCMI60FuM6q5UpPzqE3AYFuvaXenXeo=
-----END RSA PRIVATE KEY-----
```

## Screenshot of code:

A screenshot of a GitHub code review interface. At the top, it shows a commit from bradmiller titled "Support for ssl couchdb added" (openemr#4338). The code tab is selected, showing 27 lines of code (27 loc) and a file size of 1.64 KB. A GitHub Copilot badge indicates a 55% faster performance. The code itself is a large block of RSA PRIVATE KEY data, starting with "-----BEGIN RSA PRIVATE KEY-----". The code is numbered from 1 to 27.

```
-----BEGIN RSA PRIVATE KEY-----
1 MIIEogIBAAQCAQEAg0LBnVcd+Igc0o8IWsZ7NqVC891m+4jG2/WrnR/TzyiCa18
2 /z6r/y32FT1/qg8kHEqvvk0s0k5Dv1Ju5kqomPUF71fs3sF1TBMbocaYYhIIinub/
3 7pis3ecK60Uhq4KRIsecashcJavaQk9c20FrID3tpkiceNDAv/6ArsoPK02L55E
4 LMEVJfWfcpoacxicc5y/MDA38V6dqZFxmfif1fL5TEOKzzt62sqh16xbt0s+++
5 QyGB81atb/INVRaGt+35eZp4Rx7316kfgaJBeayt1xfSqrG+GanB10kWepe30QCrs
6 +fGbdMRLM81/CW9RCZeqY/BymIS4AX1zQdF9wIDAQABaoJBAEJCz4BFUtu+oP4B
7 BMaxoV1Q986/5k1j+QHEDvCVVEGvMI3Yacdmc6snpEVp3x31dxPxY4Wcfn5+
8 HVCKA1KhS5oYaeWYw47spurJI19C2hr3huQe2U43Mc0fhf1N16/vQcCH54Gzju
9 CL+pyXhInra5kko0tK6dFuxsb9pTPbYXubf37zVsp7dkDG50711Luuta7hLYmu
10 xy1afryXy1rcutgd1vxx/dX1XX5rSbjkpdkP2uAKsDpHrzsy3NvoTTpEt558J
11 E9f318H1f59eoekj8qf7geUSz9GdHUvcomeIQRWlTSmxIDSgeds18SNIdbzPKs/x
12 EY+3rdEcgyEA61o2zyXnvFc60or8ZGPEizt4K9AVjbL22Ch0eoK+6Ittxcc1l0BU
13 9OrEV/EQd3+03g1UJyeox9VfgxqZaz2Ub1rKe0mOnlyYbBQx1c3TwcwIFOVKrtA
14 4jic10BxAEMudw5TtZZqeJGcpitoqh0sINTjWegsUP7kvuxpjnidc0cgYEAv9B
15 2772fjv3oIoBDM8L8kNc8Sp1EWxpJ7d9but3ad0wts3k1ideouktFvFge6rbTr5
16 6+j1CfzRu3tH3US90651u5tkiu3kz1kgrocoyoxrRfcpiQezznEM8JH33U1d8
17 r4DC+mpyFXZFN2pB+qFnizXOp+4795Pyv2dEch8CgyAeEy8uPYLzv/g0RNuyVg0
18 H/YBaP9XvxCer7ABPdk/8EuzzkkqpVqPMFgPeD31LfyP0oLVR1Nz/H5+cobxNzO
19 +KaFW01hSSGP5Wcck9TUZvGYHsueMwg0gtUDV1LKau2ZX1Z/C0m516wydoSMVH50R
20 zgHPYqEu0+6pfK70ssjJPQkBgA/gwtKr1bJ2r1Nju795m/ROEeosdhP1dQ1NXFCt
21 Y0dcKENK0ai1+k8y6GZfk3s18EQjC54pcph51zHl061/nsv8fwcxlihOHYEGugQm
22 2BheekU1m/ti+zMLdzwrMgvGndKE8ws0oJdqbtGtgb2pGVrR89/D5yw28Fwizx
23 JckxAoGADLGduc1OCVK11w0ZJccdwkK08/y3R4ENcrV3OpqthPC11u3lpwhCayR
24 YuydpjuNNTasvaVxx1+cabWNLJrgyYbfZ+rUXJ6zmWsc3Eg8Ip8Gszf4XKR
25 JeCD0+VX10fL3P/n2hdpkCM160FuM6q5UpPzqE3AYFuvaXenXeo=
26 -----END RSA PRIVATE KEY-----
```

## Tool generated output:

A screenshot of a tool-generated output interface. It shows a single result entry for a visible OpenSSH Key. The entry includes a checkbox, a "HIGH" severity indicator, and a "Visible Private Key" label. The file path is listed as "docker/library/couchdb-config-ssl-cert-keys/easy/ca-key.pem" and is categorized under "code/infra". There is a "Show more info" link, a "Detector description" section stating "Found a visible OpenSSH Key", and a timestamp indicating the result is from 1 day ago. There are also refresh and checkmark icons.

HIGH Visible Private Key

docker/library/couchdb-config-ssl-cert-keys/easy/ca-key.pem (code/infra)

Show more info ▾

**Detector description:**  
Found a visible OpenSSH Key

⌚ 1 day

2) **Secret type:** SQL Credentials

**Exposed Secret:** MYSQL\_ROOT\_PASSWORD: root

**Screenshot of code:**

```
1      # docker-compose.yml for travis ci testing
2      version: '3.1'
3      services:
4          mysql:
5              restart: always
6              image: mariadb:10.11
7              command: ['mysqld','--character-set-server=utf8mb4']
8              environment:
9                  MYSQL_ROOT_PASSWORD: root
10             openemr:
11                 restart: always
12                 image: openemr/openemr:flex-3.19
13                 ports:
14                     - 80:80
15                     - 443:443
16                 volumes:
17                     - ../../:/var/www/localhost/htdocs/openemr
18                 environment:
19                     FORCE_NO_BUILD_MODE: "yes"
20                     EMPTY: "yes"
21                 depends_on:
22                     - mysql
```

**Tool generated output:**

HIGH ▾ [Visible MySQL Credentials details](#)

[ci/apache\\_83\\_1011/docker-compose.yml](#) (code/infra)

[Show more info](#)

**Detector description:**  
Found visible MySQL credentials details

### 3) Secret type: API

Exposed Secret: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0

#### Screenshot of code:

```
# Setting Xdebug client host for cases where xdebug.discover_client_host fails
XDEBUG_CLIENT_HOST: host.docker.internal
GITHUB_COMPOSER_TOKEN: c313de1ed5a00eb6ff9309559ec9ad01fcc553f0
GITHUB_COMPOSER_TOKEN_ENCODED: ZWU5YWIwZWNiM2ZlN2I4YThlNGQ0ZWZiNjMyNDQ5MjFkZTJhMTY2Qo=
OPENEMR_DOCKER_ENV_TAG: easy-dev-docker
OPENEMR_SETTING_site_addr_oauth: 'https://localhost:9300'
OPENEMR_SETTING_oauth_password_grant: 3
OPENEMR_SETTING_rest_system_scopes_api: 1
OPENEMR_SETTING_rest_api: 1
OPENEMR_SETTING_rest_fhir_api: 1
OPENEMR_SETTING_rest_portal_api: 1
OPENEMR_SETTING_portal_onsite_two_enable: 1
OPENEMR_SETTING_ccda_alt_service_enable: 3
OPENEMR_SETTING_couchdb_host: couchdb
OPENEMR_SETTING_couchdb_port: 6984
OPENEMR_SETTING_couchdb_user: admin
OPENEMR_SETTING_couchdb_pass: password
OPENEMR_SETTING_couchdb_dbname: example
OPENEMR_SETTING_couchdb_ssl_allow_selfsigned: 1
OPENEMR_SETTING_gbl_ldap_host: 'ldap://openldap:389'
OPENEMR_SETTING_gbl_ldap_dn: 'cn={login},dc=example,dc=org'
```

#### Tool generated output:

HIGH ▾ **Token Audit**  
docker/development-easy/docker-compose.yml (code/infra) ⌚ 1 day 🔗 ✓ 👤

Show more info ▾

**Detector description:**  
Possible sensitive machine generated token

**4) Secret type:** Certificate

**Exposed Secret:**

-----BEGIN CERTIFICATE-----

```
MIIDKzCCAhMCAQEWdQYJKoZIhvcNAQELBQAwWzELMAkGA1UEBhMCVVMxEzARBgNV
BAgMCldhc2hpmd0b24xEDAOBgNVBAcMB1NIYXR0bGUxEDAOBgNVBAoMB09wZW5F
TVIxExARBgNVBAMMCm9wZW5lbXItY2EwHhcNMjAwNzI4MDkxMTEwWhcNMzAwNjA2
MDkxMTEwJjBcMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGluZ3RvbjEQMA4G
A1UEBwwHU2VhdHRsZTEQMA4GA1UECgwHT3BlbKVNUjEUMBIGA1UEAwLbWFyaWFk
Yi1zc2wwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC134e9cUELhjVI
olNd8z/A+fY4WnQsrpmC24exK0ZWoliULWpBr7D2ruMHZp/R3oUh04Pch1jfXbl2
V4abwyfEiF2wHGKw+patTyk7xT6n+XETHTQToWLKMToOoIIT/+KBu3ABtXKgk4le
/18+JMgNryXRp1yEBQnBEjdRrxu7D/AZtlhWBZimUYLjDjiKGn+QrdslglfG0zVF
snnwmnHWRTctNACUtcIz4t6OvSjHlkNKkSsmKY2/Cr+YDVPvMLQ3HMdncoDoKy6
g7aN1FWLtcJM8d8sxcOpMe++ac+ShzjQtejBEQDH6gJAN16IYKADrx867IxmduH4
iyPaEJaAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIqPl/B9J53elamI15TuMQLZ
49kBdqM1LZwiAftsfR+yEFZY0n8p1stR1q5mofaljD4Ut8cy7/KaDHz2hzsYteK
9t2qltV83RjB+/kColldKAKfqhVuIF370E2rH5D1EL9gT5wn4RFrZ3D81P/Umult
Un37xTxbh2J+cw62QgfY2BBPXjCU50HKgHKoFA+ReO30+l04cclvOihN+SEwh0X0
bi2qTcaNDp3AYL3or+qB+yje0tkZ1cogoLqfR7RF1UJxnvqLxpNAZE0YH4iDhxyw
ap2EXdlR2o+nZVwlEQCl3Yqq0cb2nX/B5CSjJgqw3KzP8cXqoqumXt/ydAthXMk=
```

-----END CERTIFICATE-----

**Screenshot of code:**

```
1      -----BEGIN CERTIFICATE-----
2      MIIDKzCCAhMCAQEWdQYJKoZIhvcNAQELBQAwWzELMAkGA1UEBhMCVVMxEzARBgNV
3      BAgMCldhc2hpmd0b24xEDAOBgNVBAcMB1NIYXR0bGUxEDAOBgNVBAoMB09wZW5F
4      TVIxExARBgNVBAMMCm9wZW5lbXItY2EwHhcNMjAwNzI4MDkxMTEwWhcNMzAwNjA2
5      MDkxMTEwJjBcMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGluZ3RvbjEQMA4G
6      A1UEBwwHU2VhdHRsZTEQMA4GA1UECgwHT3BlbKVNUjEUMBIGA1UEAwLbWFyaWFk
7      Yi1zc2wwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC134e9cUELhjVI
8      olNd8z/A+fY4WnQsrpmC24exK0ZWoliULWpBr7D2ruMHZp/R3oUh04Pch1jfXbl2
9      V4abwyfEiF2wHGKw+patTyk7xT6n+XETHTQToWLKMToOoIIT/+KBu3ABtXKgk4le
10     /18+JMgNryXRp1yEBQnBEjdRrxu7D/AZtlhWBZimUYLjDjiKGn+QrdslglfG0zVF
11     snnwmnHWRTctNACUtcIz4t6OvSjHlkNKkSsmKY2/Cr+YDVPvMLQ3HMdncoDoKy6
12     g7aN1FWLtcJM8d8sxcOpMe++ac+ShzjQtejBEQDH6gJAN16IYKADrx867IxmduH4
13     iyPaEJaAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIqPl/B9J53elamI15TuMQLZ
14     49kBdqM1LZwiAftsfR+yEFZY0n8p1stR1q5mofaljD4Ut8cy7/KaDHz2hzsYteK
15     9t2qltV83RjB+/kColldKAKfqhVuIF370E2rH5D1EL9gT5wn4RFrZ3D81P/Umult
16     Un37xTxbh2J+cw62QgfY2BBPXjCU50HKgHKoFA+ReO30+l04cclvOihN+SEwh0X0
17     bi2qTcaNDp3AYL3or+qB+yje0tkZ1cogoLqfR7RF1UJxnvqLxpNAZE0YH4iDhxyw
18     ap2EXdlR2o+nZVwlEQCl3Yqq0cb2nX/B5CSjJgqw3KzP8cXqoqumXt/ydAthXMk=
19      -----END CERTIFICATE-----
```

## Tool generated output:

MEDIUM ▾ Potential cryptographic key bundle file

 docker/library/sql-ssl-certs-keys/insane/server-cert.pem (code/infra)

⌚ 1 day   

Show more info ▾

### 5) Secret type: Private Key

#### Exposed Secret:

----BEGIN RSA PRIVATE KEY----

```
MIIEpAIBAAKCAQEA0/GRIWU0TyhSTfvb8zKchRdKSBDaH1jqceiPfTLJlwcc9sTv
WxMlmiCYOfxdBHVPc1Z9YB18ujFSR3q7p42mFx4k2kvB69C2SesHISfzSk90CnmB
bcupRjkYlumpy1NI/iOjLkXutL7K7HNipNjHrv41ffk/kk5uXTFmtrRgldOL1er
K/n+Ma5RNmoxfiL4retmsabWwAAzPcJ/1iOCTy9CXJT0TQ2EfJ0IPWaV9KLYjD45
I3LUBKF1pEWktG93Xcmw9ognxnJGfPVhFloMFPkQaqCaWXAeHXtEsDmkt0BzGq+
9Q+wT8aHt5R9ySlEBp17PyRDVDI7DM67UKLGwIDAQABAoIBAAZBJLix6d9El1ml
yxHcNn4+97Q0uxsdtp1x7XoWW5UrCpHFsgKQCBYKTDO53Mza4WBGRyDk/d9lwVLW
rl79cR9Rhmvjv3BEEn0P8H/r++P/gD8m4sjor7AUjIM3lgkoBglp59Dfw3GlvD/H
2XbzboNjrK4zyJAwfQGaDpLJTF4UE7Tuls4ODtDChsYxEHWuDXW/ByQePGoAmod
0HkXpTQVW9UzA159IUU77OnTRGF52PG1OnJcXf6LOWnQ4pWZgEI+sbl3stdxC1r
EK5MDd9f15IE8Vzcl5t/ICqFFVjR5GINYzS/6bM9IG9We0whHi3OifR1x1V2aLs
BKBe2nECgYE+AzhJU5AWSBZo8r6bzewRW6AtXqFNdx4IlxxpabQfhFFznPi3UGQ
UfiKyR2SdWwYn4s9jhoUSw5OPCtcnO6zZzrMd3LAa+VAMOKmaD6gVW4VezymQ9WJ
60NJOS1MY11SpjkhEzyImV9A/QUmwlwksQuzoedAF2yUnKawySYIIGCcCgYEAl/n2
22723x0TxwopsHuTVE6QH9Tuo0Z7u/DZ7Lh78NzjpLPIsJLuSiUU2vlt1WuK9Nx
9OBF3hYyZyJNT/szNZjugLJtaemXzbPSzC35C7U4964K1Vmbevxvm3SDGDWkJIR+
L85aSiVcBXkf/BzUOeevnoXMwjGhzAgwp8Uxue0CgYEAYxrZpx9JxQTzIAoR6QMT
/z50zsRMmJwzftUtOKkiXRon3t8wZoOQY8VWp3zCIS8QxUR0ssOA7qGVPO4txS7z
Wp1eG6Bp05GYES3dLeCcDhWfRnBIV+h3xf4zYAewfsJGhN8hT4UcRyuMxkN4zJi8
8GrLFVjKsz9ZZ0axrV6MEPcCgYB/OcKPdQh8WhZIMAiq5zvzKXKVN+xMwn36YMcN
OTUbFlnmLNIUMnyE8ECf+6hbR1+4dXB1vf+qWg0K8Av3B5UdB5/HtFP7xh0kkb+l
g5dnrdOIw7+h+o06u+xq+PGYu1CcKmhjJP3PG77fgocY9RCXo8GyckMySiZzmleA
7Qrj6QKBgQCeflv4PONqU50LMguBskNEU2HJOEn4yVW26ym8KPjwtAtR7c6dA0eH
mhNNY8rllycZuBYPzeiTxxmkZWGULAhEDDeRMnQw680DhcDX2T3Y6cXsf02l7S32
5hKOYyZgfKd1wZHJgh49LvPQN4xT6vOnQu8Qsly/ucgA1dyhcLCsg==
```

----END RSA PRIVATE KEY----

## Screenshot of code:

```
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEpaIBAAKCAQEa0/gRlWu0TyhSTfvb8zKchRdKSBDaH1jqceiPfTLJIwcc9sTv
3 WxMlmicYOfxdBHvPC1Z9YB18ujFSR3q7p42mFx4k2kvB69C2SesHSfzSk90Cnmb
4 bcupRJkyLumpy1NI/i0jLkuttL7K7HNipNjhrv41ffk/kk5uXTFmtrRgld0L1er
5 K/n+Ma5RNmoxfiL4retmsabWwAAzPcJ/1ioCtY9CXJT0TQ2EfJ0lPWaV9KLYjd45
6 l3LUBKF1pEWktG93Xcmw9ognxnJGfPVhFIoMFpkQaqCalXAeHXxtEsDmkT0BzGq+
7 9Q+wT8aHt5R9ySiEBp17PyRDVDl7DM67UKLGwIDAQABoIBAAZBJLix6d9EI1ml
8 yxHcNn4+97Q0uxsdtp1x7x0wW5UrCpHFsgKQCByKTD053Mza4WBGRyDk/d9IwVLW
9 r179cR9Rhmjiv3BEEn0P8H/r++P/gD8m4sjor7AUjIM3lgkoBglp59dfw3Glvb/H
10 2xbzboNjrK4zyJAwfQGaDpLJt1F4UE7TuIs40DtDChsYxEHWuDXW/ByQePGoAmod
11 0HkXpTQVW9UzA159lUU770nTRGF52PG10nJcXf6L0WnQ4pWZgEl+sbl3stdxC1r
12 EK5Md9f15IE8VzcI5t/ICqFFVjR5GINYzs/6bM9IG9We0whHFi3oifR1x1V2aLs
13 BKBe2nECgYEa+zJVV5AWSBzo8r6bzewRW6AtxqFNdx4IIxxpabQfhFFznPi3UGQ
14 UfiKyR2SdwYn4s9jhoUsW50PCtn06zzrMd3LAA+VAMOKmaD6gVW4VezymQ9WJ
15 60NJOS1MYl1SpjkhEzyImV9A/QUmwlwksQuzoedAF2yUnKawySYIlGCcCgYEAI/n2
16 22723x0TxwopsHUtVTE6QH9Tuo0Z7u/DZ7Lh78NzjplPIsJLuSiUU2vIt1WuK9Nx
17 90BF3hYyZyJNT/szNZjugLJtaemXzbPSzC35C7U4964K1Vmbevxm3SDGDWkJIR+
18 L85aSiVCBXkf/BzU0eevnoXMwjGhzAgwp8Uxue0CgYEAYxrZpx9JxQTz1AoR6QMT
19 /z50zsRMmJwzftUtOKkiXRon3t8wZo0QY8VWp3zCIS8QxUR0ssOA7qGVPO4txs7z
20 Wp1eG6Bp05GYES3dLeCcdhWfRnBlV+h3xf4zYAewfsJGhN8hT4UcRyuMxkN4zJl8
21 8GrLFVjkSz9ZZ0axrV6MEPcCgYB/OcKPdQh8Whz1MA1q5zvzKXKVN+xMwn36YMcN
22 OTUbFlnmLNlUMnyE8EcF+6hbR1+4dXB1vf+qWg0K8Av3B5UdB5/HtFP7xh0kkb+l
23 g5dnrdOIw7+h+o06u+xq+PGYu1CcKmhjJP3PG77fgocy9RCxo8GyckMySiZzmIeA
24 7Qrj6QKBgQCefIv4PONqu50LMguBskNEU2HJOEn4yVW26ym8KPjwtaTr7c6dA0eH
25 mhNNY8rlylcZuBYPzejTxmxkZWGULAhEDDeRMnQw680DhcDX2T3Y6cXsf02l7S32
26 5hKO0Y2ZgfKd1wZHJgh49LvPQN4xT6vOnQu8QsIy/ucgA1dyhLCsg==
27 -----END RSA PRIVATE KEY-----
```

## Tool generated output:

**HIGH**  **Visible Private Key**

 docker/library/sql-ssl-certs-keys/easy/client-key.pem (code/infra)

Show more info ▾

**Detector description:**  
Found a visible OpenSSH Key

 1 day   

Rest of the leaks were identified as false positives like dummy files, tests file, readme and documentation files etc.

**Comparison report reflecting on the similarities and differences between the results of the two tools. Include a discussion of whether the true positive secrets you found are found by both tools.**

SpectralOps' secret detection tool identified a total of 176 vulnerabilities within OpenEMR, featuring an intuitive dashboard with severity labels for each vulnerability, enhancing accessibility for users of varying technical levels, from developers to non-technical personnel. The tool also offers comprehensive metric-based reporting for secret detection, with each issue linked for easy review and guidance on mitigation steps. In contrast to Gitleaks, SpectralOps includes an "information" leak label, detected MYSQL credential leaks absent in Gitleaks, and provides convenient links to the GitHub repository files, pinpointing the problematic code lines.

On the other hand, Gitleaks detected 109 secret exposures in OpenEMR, lacking a user interface like SpectralOps but allowing results exportation into a detailed JSON format, which includes information such as the description, file location, and entropy values to gauge severity. Notably, Gitleaks offers an entropy value for each exposure, aiding in severity assessment, but it has generated some false positives, particularly with AWS credentials, which SpectralOps did not encounter.

**Comment on how OpenEMR handles secrets. What OpenEmr should do to protect the secrets you found? Do these secrets appear to protect valuable resources/assets? What good design principles does it seem OpenEMR has used to protect other types of secrets (hint: gitignore, config files, contributor documentation, etc)? Refer to the class sides and the resources linked from the course website.**

Considering the huge scale of the project, the number of true positives found by the above tools is really small, however, cannot be considered negligible. Although some of the secrets have been removed from the latest version of master branch, they are still found in the previous commit history.

To enhance secret protection, OpenEMR can adopt cloud-native secret stores like AWS Secrets Manager or dedicated vaults, alongside leveraging secret-loading libraries such as .env. Access to configuration files should be restricted, with the removal of sensitive files from public repositories and avoidance of distribution among multiple sources. Implementing strict access controls and utilizing password managers or secure storage alternatives are vital measures, categorizing data and managing access rights based on sensitivity.

OpenEMR employs robust design principles to safeguard various types of secrets. The effective use of .gitignore files prevents accidental commits of sensitive information to version control repositories. Clear contributor documentation, including a code of conduct and guidelines on secure coding practices, ensures contributors handle secrets securely. However, secret management can be improved by use of environment variables files. In the current version of OpenEMR, environment variables are not being used effectively and efficiently. Specifically, all the hardcoded private keys can be added to environment variables and avoided to be uploaded to public repositories.

## Actual Results

### 1. Test Case 1 (True Positive):

**Ruleset:** Injection

**Actual Result:** The details were submitted successfully and a patient was created with an unassigned gender

**Mitigation:** Firstly, server-side validation should always be enforced, ensuring that all data submitted by the client is thoroughly validated and sanitized on the server before being processed or stored. Additionally, implementing strict access controls and authentication mechanisms can restrict users' abilities to modify sensitive data unless they have appropriate permissions. Furthermore, employing client-side integrity checks, such as checksums or digital signatures, can detect and reject unauthorized modifications made by clients.

### 2. Test Case 2 (True Positive)

**Ruleset:** XSS Attack

**Actual Result:** The details were submitted successfully and a patient was created with a blank first and last name

**Mitigation:**

Implement strong server-side validation to enforce mandatory fields. Require both first and last names with checks that prevent submission if these fields are empty or contain only whitespace. Consider setting minimum character lengths for the names as an added layer of protection.

### 3. Test Case 3 (True Positive)

**Ruleset:** Injection

**Actual Result:** The details were submitted successfully and a patient was created with a date of birth as 00-00-0000 and the form accepts alphanumeric string

**Mitigation:** Firstly, server-side validation should be enforced to verify the format and validity of all submitted data, including the date of birth field. This validation should ensure that the date conforms to a specific format (e.g., YYYY-MM-DD) and falls within a reasonable range. Additionally, client-side validation can be employed to provide immediate feedback to users and prevent invalid submissions before they are sent to the server. Input masks or date picker controls in the user interface can guide users to enter dates in the correct format and reduce the likelihood of alphanumeric inputs. Furthermore, enforcing strict data validation rules on the server side, such as checking for the presence of valid digits in the date fields, can help prevent invalid or nonsensical submissions.

### 4. Test Case 4 (True Positive)

**Ruleset:** Buffer Overflow

**Actual Result:** POST Request successfully accepts an alphanumeric string of any length

**Mitigation:** Implement strict server-side validation to enforce a specific format and length limit for the payment reference number. This could involve regular expressions to ensure correct alphanumeric patterns and a defined maximum character count. Additionally, we can consider using field types specifically designed for reference numbers, if available in server-side framework. It often makes sense to include client-side validation (e.g., with HTML5 input patterns) for immediate user feedback, but it shouldn't replace the essential server-side checks.

## **5. Test Case 5 (False Positive)**

**Ruleset:** SQL Injection

**Actual Result:** The login page does not accept any SQL injection statements

**Reasoning:** The developers may have taken protective measures such as input validation (filtering out special characters), sanitization (removing dangerous code elements), prepared statements (separating code and data), or stored procedures (pre-compiled code on the database). Alternatively, attacks might have incorrect syntax, or the specific login functionality might not be vulnerable to broad SQL injections. The database user account used by the application may have limited privileges, preventing it from executing certain types of SQL commands. A WAF can be configured to block requests that contain suspicious SQL injection patterns.

# Screenshots corresponding to the actual test cases

## Test Case 1

### Break at URL

The screenshot shows a browser window for the OpenEMR interface. The main page is a 'Search or Add Patient' form. A modal window titled 'HTTP Message' is overlaid, displaying the raw HTTP request sent to the server. The request is a POST to 'http://localhost/interface/new/new\_comprehensive\_save.php'. The payload is extremely long and contains many form fields, indicating a complex data structure being submitted. The response tab of the modal shows a JSON object with some fields like 'status': 'signed'.

### Bypass using malicious input

The screenshot shows the ZAP (Zed Attack Proxy) interface. A session named 'Untitled Session - 20240308-044836 - ZAP 2.14.0' is active. The 'Request' tab is selected, showing a POST request to 'http://localhost/interface/new/new\_comprehensive\_save.php'. The request body is filled with a large amount of malicious input, which appears to be a dump of the raw data from the previous screenshot. The ZAP interface has a toolbar at the top with icons for quick start, request, response, requester, break, and other functions. Below the toolbar is a header and body dropdown for selecting the request and response respectively. The main pane displays the raw request data.

### Result

Untitled Session - 20240308-044858 - ZAP 2.14.0

Quick Start Request Response Requester Break +

Header: Text Body: Text

```
HTTP/1.1 200 OK
Date: Fri, 08 Mar 2024 10:01:06 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OpenEMR=eCi9KdAmYZcaG58rpxVW3LvyvlUkXsExwFEWgkm3bZnvs4C; expires=Fri, 08 Mar 2024 17:47:47 GMT; Max-Age=28000; path=/;
SameSite=Strict
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 138
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
<html>
<body>
<script>
window.location='/interface/patient_file/summary/demographics.php?set_pid=2&is_new=1';
</script>
```

min Reports Miscella... [Help] 1 - 2 of 2

Name	Sex	Phone	SS	DOB	ID	PID	[Number Of Encounters]	[Days Since Last Encounter]	[Date of Last Encounter]	[90 Days From Last Encounter]
Asd, Asd	Male					2024-03-06 1	1	0		,
Qwe, Qwe						2024-03-07 2	2	0		,

Add Patient

Sex: Unassigned

Fuzzing:

The screenshot shows the OpenEMR web application interface. At the top, there's a navigation bar with links for Calendar, Finder, Flow, Recalls, and Message Center. Below the navigation is a search bar with placeholder text "Search by any demographics". On the left, there's a sidebar titled "Search or Add" with sections for Who (listing names like Qwe, Qwe; Rty, Rty; Dfds, Asddf; etc.), Contact, Choices, Employer, Stats, Misc, Guardian, and Insurance. A "Create New" button is also present in the sidebar. The main content area displays a table titled "[Help]" with the subtitle "1 - 100 of 537". The table has columns: Name, Sex, Phone, SS, DOB, ID, PID, [Number Of Encounters], [Days Since Last Encounter], [Date of Last Encounter], and [90 Days From Last Encounter]. The table lists numerous entries for "Rty, Rty", with the entry "Rty, Rty t" highlighted in blue. To the right of the table, there's a vertical sidebar with icons for various system functions, such as Sites, Start, Off, and Create.

Name	Sex	Phone	SS	DOB	ID	PID	[Number Of Encounters]	[Days Since Last Encounter]	[Date of Last Encounter]	[90 Days From Last Encounter]
Rty, Rty	Male			2024-03-06 3	3	0				
Asd, Asd	Male			2024-03-06 1	1	0				
Dfds, Asddf	Male			0000-00-00 4	4	1		0	2024-03-08 Thursday, 2024-06-06	
Qwe, Qwe	Unassigned			2024-03-07 2	2	0				
Rty, Rty	j			2024-03-06 256	256	0				
Rty, Rty	c			2024-03-06 512	512	0				
Rty, Rty	i			2024-03-06 257	257	0				
<b>Rty, Rty</b>	<b>t</b>			<b>2024-03-06 513</b>	<b>513</b>	<b>0</b>				
Rty, Rty	h			No other phone numbers listed						
Rty, Rty	i			2024-03-06 514	514	0				
Rty, Rty	g			2024-03-06 259	259	0				
Rty, Rty	h			2024-03-06 515	515	0				
Rty, Rty	f			2024-03-06 260	260	0				
Rty, Rty	g			2024-03-06 516	516	0				
Rty, Rty	Male			2024-03-06 5	5	0				
Rty, Rty	q			2024-03-06 261	261	0				
Rty, Rty	f			2024-03-06 517	517	0				
Rty, Rty	o			2024-03-06 6	6	0				
Rty, Rty	p			2024-03-06 262	262	0				
Rty, Rty	e			2024-03-06 518	518	0				
Rty, Rty	F			2024-03-06 7	7	0				
Rty, Rty	o			2024-03-06 263	263	0				
Rty, Rty	d			2024-03-06 519	519	0				
Rty, Rty	E			2024-03-06 8	8	0				
Rty, Rty	n			2024-03-06 264	264	0				

## Test Case 2:

## Break at the URL

The screenshot shows the OpenEMR web application running in a browser. The main page is titled "Search or Add Patient". On the left, there's a sidebar with tabs for "Who", "Contact", "Choices", "Employer", "Stats", "Misc", "Guardian", and "Insurance". Below the sidebar is a search bar with the placeholder "Search or Add Patient" and a "Create New Patient" button.

A modal window titled "HTTP Message" is open in the center. It has two tabs: "Request" and "Response". The "Request" tab displays a POST request to the URL `https://localhost/interface/new_comprehensive_save.php`. The "Response" tab is currently empty. At the bottom of the modal are three buttons: "Step", "Continue", and "Drop".

The browser's address bar shows the URL `https://localhost/interface/main/tabs/main.php?token_main=SgdpkkWf40dSjrfc7hc2bKzalp/RaaAWKx9kdh`. The top right corner of the browser window shows a battery icon at 80% and a zoom level of 80%.

Bypass using malicious input:

```
POST http://localhost/interface/new/_new_comprehensive_save.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://localhost/interface/new/_new.php
Content-Type: application/x-www-form-urlencoded

: csrf_token_form=a464a71d51569dfa6804733fc67042390ea854c&form_title=&form_fname=&form_mname=&form_lname=&form_suffix=&
form_preferred_name=&form_birth_fname=&form_birth_mname=&form_birth_lname=&form_DOB=2024-03-06&form_sex=Male&form_gender_identity=&
form_text_gender_identity=&form_sexual_orientation=&form_text_sexual_orientation=&form_pubpid=&form_ss=&form_drivers_license=&
form_status=&form_genericname1=&form_genericval1=&form_genericname2=&form_genericval2=&form_billing_note=&form_street=&
form_street_line_2=&form_city=&form_state=&form_postal_code=&form_country_code=&form_county=&form_mothersname=&
form_contact_relationship=&form_phone_contact=&form_phone_home=&form_phone_biz=&form_phone_cell=&form_email=&form_email_direct=&
form_providerID=&form_provider_since_date=&form_ref_providerID=&form_pharmacy_id=0&form_hipaa_notice=&form_hipaa_voice=&
form_hipaa_message=&form_hipaa_mail=&form_hipaa_allowsms=&form_hipaa_allownail=&form_allow_inn_reg_use=&form_allow_inn_info_share=&
form_allow_health_info_ex=&form_allow_patient_portal=&form_cmsportal_login=&form_inn_reg_status=&form_inn_reg_stat_effdate=&
form_publicity_code=&form_publ_code_eff_date=&form_protect_indicator=&form_prot_indi_effdate=&form_care_team_status=active&
form_patient_groups%5B%5D=&form_occupation=&form_industry=&form_em_name=&form_em_street=&form_em_street_line_2=&form_em_city=&
```

## Result:

HTTP/1.1 200 OK  
Date: Fri, 08 Mar 2024 10:05:59 GMT  
Server: Apache  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Set-Cookie: OpenEMR=eCi9KdAmTYZcaG58rpxVW3LvyvlUkXsExwFEWgkm3bZnvs4C; expires=Fri, 08 Mar 2024 17:52:39 GMT; Max-Age=28000; path=/;  
SameSite=Strict  
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload  
X-XSS-Protection: 1; mode=block  
Content-Length: 138  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
  
<html>  
<body>  
<script>  
window.location='/interface/patient\_file/summary/demographics.php?set\_pid=3&is\_new=1';  
</script>  
\*\*\*

The screenshot shows the OpenEMR interface with the title bar "OpenEMR". The top navigation bar includes links for Calendar, Finder, Flow, Recalls, Messages, Patient, Fees, Modules, Procedures, Admin, Reports, Miscellaneous, and Popups. A search bar on the right says "Search by an". Below the navigation is a patient summary box showing a profile picture, "(3) x", and the text "DOB: 2024-03-06 Age: 0 month". To the right is a button "Select Encounter (0) +". The main menu bar has tabs for Calendar, Message Center, Dashboard, Visit History, and others. The "Visit History" tab is active and highlighted with a blue border. On the left, there's a sidebar with icons for Out (0), Off (0), In (0), Off (3), Off (2), Off (3), and a plus sign. The main content area displays a table header with columns: Issue, Reason/Form, Provider, Billing, and Insurance. At the bottom, there are links for History (188) and WebSockets.

## Fuzzing:

### Test Case 3:

## Break the URL

The screenshot shows the OpenEMR web application running at [https://localhost/interface/main/tabs/main.php?token\\_main=SgdpkkWf4Dsjrfc7hcc2bKzalpVraaVAKx9kd](https://localhost/interface/main/tabs/main.php?token_main=SgdpkkWf4Dsjrfc7hcc2bKzalpVraaVAKx9kd). The main page displays a search form for 'Search or Add Patient' with fields for 'Who' (Title, Name, Preferred Name, Birth Name), 'When' (DOB, Gender Identity, External ID, License ID, User Defined), 'How' (Billing Note, Previous Names), and 'Contact' (Phone, Email, Address). A modal window titled 'HTTP Message' is open, showing the 'Request' and 'Response' tabs. The 'Request' tab contains a large block of raw HTTP POST data, which includes patient details and form parameters. The 'Response' tab is currently empty. At the bottom of the modal are buttons for 'Step', 'Continue', and 'Drop'. The status bar at the bottom right shows '80%' and a search bar for 'Search by any demographic'.

Bypass using malicious Input:

## Result:

Untitled Session - 20240308-044838 - ZAP 2.14.0

Quick Start Request Response Requester Break +

Header: Text Body: Text

```
HTTP/1.1 200 OK
Date: Fri, 08 Mar 2024 10:10:52 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OpenEMR=eCi9KdAmTYZcaG58rpxVW3LvyvlUkXsExwFEWgkm3bZnvs4C; expires=Fri, 08 Mar 2024 17:57:32 GMT; Max-Age=28000; path=/;
SameSite=Strict
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 138
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<html>
<body>
<script>
window.location='/interface/patient_file/summary/demographics.php?set_pid=4&is_new=1';
</script>
```

OpenEMR

https://localhost/interface/main/tabs/main.php?token\_main=SgdppkkWf4OdSjrfc7Hcc2bKzalpVRaaVAW 80%

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups Search by any

Asddf Dfds (4) ×  
DOB: 0000-00-00 Age: 2024  
Select Encounter (0) +

Visit History To Billing View

Out 0	Issue	Reason/Form	Provider	Billing	Insurance
Off 0					
Off 0					
Off 0					
Off 3					
Off 2					
Off 3					
+ 0					

History 217 WebSockets

Fuzzing:

Screenshot of a browser-based application interface showing a search results page for patients named "Rty". The search bar contains "Rty (543) x". The results table has columns: Name, Sex, Phone, SS, DOB, ID, PID, [Number Of Encounters], [Days Since Last Encounter], [Date of Last Encounter], and [90 Days From Last Encounter]. The table shows numerous entries for "Rty, Rty" with various demographic details and encounter counts.

Name	Sex	Phone	SS	DOB	ID	PID	[Number Of Encounters]	[Days Since Last Encounter]	[Date of Last Encounter]	[90 Days From Last Encounter]
Rty, Rty	j			2024-03-06 256	256	0	1			
Rty, Rty	c			2024-03-06 512	512	0	1			
Rty, Rty	Male			0000-00-00 768	768	0	1			
Rty, Rty	Male			0000-00-00 1024	1024	0	1			
Rty, Rty	i			2024-03-06 257	257	0	1			
Rty, Rty	t			2024-03-06 513	513	0	1			
Rty, Rty	Male			0000-00-00 769	769	0	1			
Rty, Rty	Male			0000-00-00 1025	1025	0	1			
Rty, Rty	h			2024-03-06 258	258	0	1			
Rty, Rty	i			2024-03-06 514	514	0	1			
Rty, Rty	Male			0000-00-00 770	770	0	1			
Rty, Rty	Male			0000-00-00 1026	1026	0	1			
Rty, Rty	g			2024-03-06 259	259	0	1			
Rty, Rty	h			2024-03-06 515	515	0	1			
Rty, Rty	Male			0000-00-00 771	771	0	1			
Rty, Rty	Male			0000-00-00 1027	1027	0	1			
Rty, Rty	f			2024-03-06 260	260	0	1			
Rty, Rty	g			2024-03-06 516	516	0	1			
Rty, Rty	Male			0000-00-00 772	772	0	1			
Rty, Rty	Male			0000-00-00 1028	1028	0	1			
Rty, Rty	Male			2024-03-06 5	5	0	1			
Rty, Rty	q			2024-03-06 261	261	0	1			
Rty, Rty	f			2024-03-06 517	517	0	1			
Rty, Rty	Male			0000-00-00 773	773	0	1			
Rty, Rty	Male			0000-00-00 1029	1029	0	1			
Rty, Rty	o			2024-03-06 6	6	0	1			
Rty, Rty	p			2024-03-06 262	262	0	1			
Rty, Rty	e			2024-03-06 518	518	0	1			
Rty, Rty	Male			0000-00-00 774	774	0	1			
Rty, Rty	Male			0000-00-00 1030	1030	0	1			
Rty, Rty	F			2024-03-06 7	7	0	1			
Rty, Rty	o			2024-03-06 263	263	0	1			
Rty, Rty	d			2024-03-06 519	519	0	1			
Rty, Rty	Male			0000-00-00 775	775	0	1			
Rty, Rty	Male			0000-00-00 1031	1031	0	1			

Note: This includes results from previous fuzzings as well

## Test Case 4:

Break in the URL

Accept Payment - Asddf

Payment

Payment Method:

Check Payment

Check or Reference Number:

Patient Coverage:

Self  Insurance

Payment against:

Co Pay  Invoice Balance

Collect For

Co

History 86 WebSockets

## Bypass using malicious input

Method: POST http://localhost/interface/patient\_file/front\_payment.php HTTP/1.1

Header: Text

Body: Text

```
POST http://localhost/interface/patient_file/front_payment.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://localhost/interface/patient_file/front_payment.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 293
Origin: https://localhost

csrf_token_form=87142acf2763c01fa0c6265alea829778865112&form_pid=4&form_method=check_payment&form_source=7hNf68KpQr4J3m6t9u2iW5yH7nBg4VcX6zA8sRdf1gT2yH6uJ3iK4oLpS9jA6qE8wZ5rCdVfB3nM8Bh7gKpQ4rT6yN9u2iW5yH7nB&radio_type_of_coverage=insurance&radio_type_of_payment=copay&form_prepayment=&form_upay%5B2%5D=45&form_paytotal=45.00&form_save=Generate+Invoice&hidden_patient_code=4&ajax_mode=&mode=
```

Results:

Untitled Session - 20240308-044838 - ZAP 2.14.0

Quick Start Request Response Requester Break +

Header: Text Body: Text

```
HTTP/1.1 200 OK
Date: Fri, 08 Mar 2024 10:28:01 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
content-length: 12497
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
```

## Receipt for Payment

Your Clinic Name Here

Invoice No.	Date
	2024-03-08

How Paid: Check Payment  
Check or Reference Number:  
7hNfG8KpQr4J3m6t9u2iW5yH7nBg4VcX6zA8sRdF1gT2yH6uJ3iK4oLpS9jA6qE8wZ5rCdVfB3nM8bH7gKpQ4rT6yN9u2iW5yH7nB  
Amount for Past Balance: 0.00  
Amount for This Visit: 45.00  
Received By: admin

Description	Price	Qty	Total
		Total	45.00

WebSockets

Fuzzing:

Screenshot of a web application interface showing a POST request to `http://localhost/interface/patient_file/front_payment.php`. The request header includes:

```
POST http://localhost/interface/patient_file/front_payment.php HTTP/1.1
host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
```

The request body contains a long URL-encoded string with parameters like `csrf_token_form=abcd285bf7b5db70a95hb2c3ad264a9b9a041&form_pid=1&form_method=check_payment&form_source=123&radio_type_of_coverage=insurance&radio_type_of_payment=copay&form_prepayment=&form_upay%5B2%5D=%&form_paytotal=5.00&form_save=Generate+Invoice&hidden_patient_code=1&jquery_mode=5mode`.

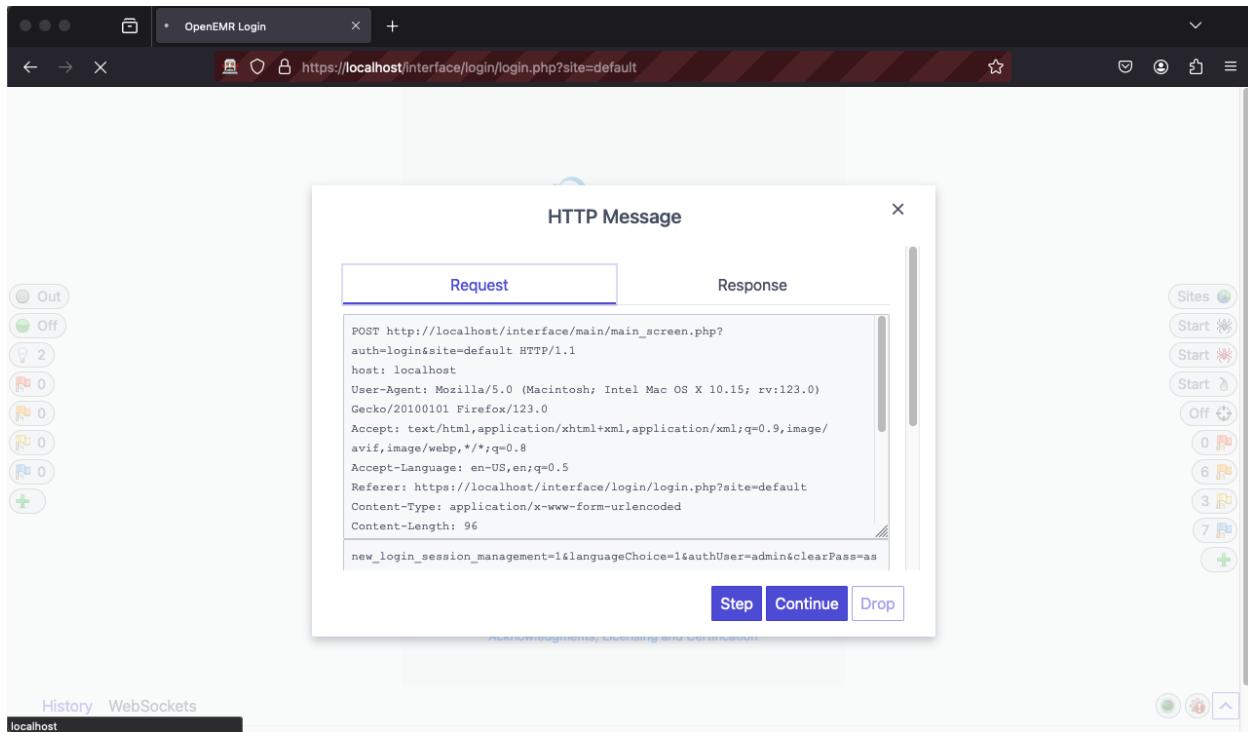
Below the request details, a table shows the results of 34 messages sent, all of which were successful (200 OK). The table includes columns for Task ID, Message Type, Code, Reason, RTT, Size Resp. Header, Size Resp. Body, Highest Alert, State, and Payloads.

Task ID ^	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
4 Fuzzed		200 OK		64 ms	407 bytes	12,650 bytes	Reflected	aaaaaaa	
5 Fuzzed		200 OK		64 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa	
6 Fuzzed		200 OK		65 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa...	
7 Fuzzed		200 OK		63 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa...	
8 Fuzzed		200 OK		65 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa...	
9 Fuzzed		200 OK		71 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa...	
10 Fuzzed		200 OK		76 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
11 Fuzzed		200 OK		66 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
12 Fuzzed		200 OK		62 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
13 Fuzzed		200 OK		74 ms	407 bytes	12,647 bytes	Reflected	aaaaaaaaaaaaaa...	
14 Fuzzed		200 OK		67 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
15 Fuzzed		200 OK		76 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
16 Fuzzed		200 OK		80 ms	407 bytes	12,649 bytes	Reflected	aaaaaaaaaaaaaa...	
17 Fuzzed		200 OK		99 ms	407 bytes	12,650 bytes	Reflected	aaaaaaaaaaaaaa...	

Below the table, a screenshot of a browser showing a "Receipt for Payment" page. The page title is "Receipt for Payment". The content area shows a table with columns "Date of Service" and "Description". The table lists numerous entries, each consisting of a date (e.g., 2024-03-08) followed by a long, repetitive string of characters (e.g., "Payment Pt 123", "Payment Pt a", etc.).

## Test Case 5:

Break in the URL



## Bypass using malicious input

The screenshot shows the ZAP interface with the title "Untitled Session - 20240308-044838 - ZAP 2.14.0". The "Request" tab is selected. The request details are as follows:

```
Method: POST  
Header: Text  
Body: Text  
POST http://localhost/interface/main/main_screen.php?auth=login&site=default HTTP/1.1  
Host: localhost  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Referer: https://localhost/interface/login/login.php?site=default  
Content-Type: application/x-www-form-urlencoded  
new_login_session_management=1&languageChoice=1&authUser='OR'1'=1'&clearPass=pass&languageChoice=1
```

The "Break" button is highlighted in red at the top of the Request pane.

Result:

Untitled Session - 20240308-044838 - ZAP 2.14.0

Header: Text Body: Text

```
Date: Fri, 08 Mar 2024 10:33:11 GMT
Server: Apache
Set-Cookie: OpenEMR=RXeUbEqDZzVXexSlW%2CLuWGFFJzlnEsSUGeXdJaoJvhCLC-82; expires=Fri, 08 Mar 2024 18:19:51 GMT; Max-Age=28000; path=/
SameSite=Strict
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 464
while (w.opener) { // in case we are in a dialog window
  var wtmp = w;
  w = w.opener;
  wtmp.close();
}
w.top.location.href = '/interface/login_screen.php?error=1&site=';
</script>
```

OpenEMR Login https://localhost/interface/login/login.php?site=default

The most popular open-source  
Electronic Health Record and Medical  
Practice Management solution.

**Invalid username or password**

Username

Password

Language Default - English (Standard)

Acknowledgments, Licensing and Certification

Fuzzing: