Acunetix
by Invicti

Comprehensive Report

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	job.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 14, 2024, 10:13:54 PM GMT+8
Scan Duration	1 minute
Requests	3229
Average Response Time	33ms
Maximum Response Time	311ms
Application Build	v23.7.230728157

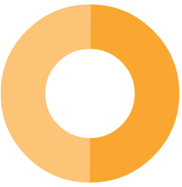
1	2	0	3
High	Medium	Low	Informational

Severity	Vulnerabilities	Instances
High	1	1
Medium	2	2
Low	0	0
Informational	3	3
Total	6	6

Informational

		Instances
🟩	Content type is not specified	1
🟩	No HTTP Redirection	1
🟩	Reverse proxy detected	1

Medium Severity



		Instances
🟧	Development configuration files	1
🟧	Unencrypted connection	1

High Severity

		Instances
🟥	Dotenv .env file	1

Impacts

SEVERITY	IMPACT	
High	1	Dotenv .env file
Medium	1	Development configuration files
Medium	1	Unencrypted connection
Informational	1	Content type is not specified
Informational	1	No HTTP Redirection
Informational	1	Reverse proxy detected

Dotenv .env file

A dotenv file (**.env**) was found in this directory. Dotenv files are used to load environment variables from a .env file into the running process.

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

http://job.ssbmultiservices.com/ Verified

File: **.env**

Pattern found:

```
APP_ENV=
```

Request

```
GET /.env HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

http://job.ssbmultiservices.com/

Development configuration files:

- http://job.ssbmultiservices.com/**package.json**

  ```
  package.json => Grunt configuration file. Grunt is a JavaScript task runner.
  ```

- http://job.ssbmultiservices.com/**composer.json**

  ```
  composer.json => Composer configuration file. Composer is a dependency manager
  for PHP.
  ```

- http://job.ssbmultiservices.com/**composer.lock**

  ```
  composer.lock => Composer lock file. Composer is a dependency manager for PHP.
  ```

- http://job.ssbmultiservices.com/**package-lock.json**

  ```
  package-lock.json => npm file. This file keeps track of the exact version of
  every package that is installed.
  ```

Request

```
GET /package.json HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

http://job.ssbmultiservices.com/ Verified

Request

```
GET / HTTP/1.1
Referer: http://job.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

http://job.ssbmultiservices.com/ Verified

Pages where the content-type header is not specified:

- http://job.ssbmultiservices.com/composer.lock
- http://job.ssbmultiservices.com/.env

Request

```
GET /composer.lock HTTP/1.1
Referer: http://job.ssbmultiservices.com/
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://job.ssbmultiservices.com/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

http://job.ssbmultiservices.com/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: job.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

None

Coverage

- http://job.ssbmultiservices.com
  - .env
  - composer.json
  - composer.lock
  - package-lock.json
  - package.json