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.

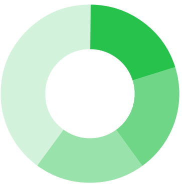
Scan Detail

Target	vhvshop.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 14, 2024, 9:58:50 PM GMT+8
Scan Duration	3 minutes
Requests	4408
Average Response Time	33ms
Maximum Response Time	306ms
Application Build	v23.7.230728157

1	3	1	5
High	Medium	Low	Informational

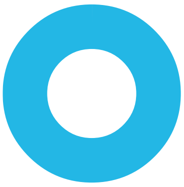
Severity	Vulnerabilities	Instances
High	1	1
Medium	3	3
Low	1	1
Informational	5	5
Total	10	10

Informational



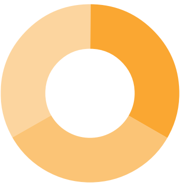
		Instances
🟩	Content Security Policy (CSP) not implement…	1
🟩	Content type is not specified	1
🟩	No HTTP Redirection	1
🟩	Others	2

Low Severity



		Instances
🟦	Clickjacking: X-Frame-Options header	1

Medium Severity



		Instances
🟧	Development configuration files	1
🟧	Unencrypted connection	1
🟧	Vulnerable package dependencies [medium]	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
Medium	1	Vulnerable package dependencies [medium]
Low	1	Clickjacking: X-Frame-Options header
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Content type is not specified
Informational	1	No HTTP Redirection
Informational	1	Permissions-Policy header not implemented
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://vhvshop.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: vhvshop.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://vhvshop.ssbmultiservices.com/

Development configuration files:

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

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

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

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

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

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

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

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

- http://vhvshop.ssbmultiservices.com/**.styleci.yml**

  ```
  .styleci.yml => StyleCI configuration file
  ```

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: vhvshop.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://vhvshop.ssbmultiservices.com/ Verified

Request

```
GET / HTTP/1.1
Referer: http://vhvshop.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: vhvshop.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

http://vhvshop.ssbmultiservices.com/

List of vulnerable **composer** packages:

Package: spatie/browsershot
Version: 3.60.0
CVE: CVE-2020-7790
Title: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Description: This affects the package spatie/browsershot from 0.0.0. By specifying a URL in the file:// protocol an attacker is able to include arbitrary files in the resultant PDF.

CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CWE: CWE-22

References:

- https://snyk.io/vuln/SNYK-PHP-SPATIEBROWSERSHOT-1037064
- https://github.com/spatie/browsershot/issues/441%23issue-735049731

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

http://vhvshop.ssbmultiservices.com/

Paths without secure XFO header:

- http://vhvshop.ssbmultiservices.com/
- http://vhvshop.ssbmultiservices.com/sitemap.xml
- http://vhvshop.ssbmultiservices.com/sitemap.xml.gz

- http://vhvshop.ssbmultiservices.com/clientaccesspolicy.xml
- http://vhvshop.ssbmultiservices.com/crossdomain.xml

Request

```
GET / HTTP/1.1
Referer: http://vhvshop.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: vhvshop.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://vhvshop.ssbmultiservices.com/

Paths without CSP header:

- http://vhvshop.ssbmultiservices.com/
- http://vhvshop.ssbmultiservices.com/sitemap.xml
- http://vhvshop.ssbmultiservices.com/sitemap.xml.gz
- http://vhvshop.ssbmultiservices.com/clientaccesspolicy.xml
- http://vhvshop.ssbmultiservices.com/crossdomain.xml

Request

```
GET / HTTP/1.1
Referer: http://vhvshop.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: vhvshop.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

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://vhvshop.ssbmultiservices.com/ Verified

Pages where the content-type header is not specified:

- http://vhvshop.ssbmultiservices.com/.styleci.yml
- http://vhvshop.ssbmultiservices.com/composer.lock
- http://vhvshop.ssbmultiservices.com/.env
- http://vhvshop.ssbmultiservices.com/.env.dev

Request

```
GET /.styleci.yml HTTP/1.1
Referer: http://vhvshop.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: vhvshop.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://vhvshop.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: vhvshop.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

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

http://vhvshop.ssbmultiservices.com/

Locations without Permissions-Policy header:

- http://vhvshop.ssbmultiservices.com/
- http://vhvshop.ssbmultiservices.com/sitemap.xml
- http://vhvshop.ssbmultiservices.com/sitemap.xml.gz
- http://vhvshop.ssbmultiservices.com/clientaccesspolicy.xml
- http://vhvshop.ssbmultiservices.com/crossdomain.xml

Request

```
GET / HTTP/1.1
Referer: http://vhvshop.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: vhvshop.ssbmultiservices.com
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)

https://www.w3.org/TR/permissions-policy-1/

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://vhvshop.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: vhvshop.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

None

Coverage

http://vhvshop.ssbmultiservices.com

- .env
- .env.dev
- .styleci.yml
- clientaccesspolicy.xml
- composer.json
- composer.lock
- crossdomain.xml
- package-lock.json
- package.json
- robots.txt
- sitemap.xml