Security Report for 192.168.1.119:3000

Report generated on: 2024-06-04 22:22:13

Nmap Scan Results

```
# Nmap 7.94SVN scan initiated Tue Jun  4 22:13:29 2024 as: nmap -A -sV -p
Nmap scan report for 192.168.1.119
Host is up (0.0013s latency).

PORT     STATE SERVICE VERSION
3000/tcp open  ppp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: SAMEORIGIN
|     Feature-Policy: payment 'self'
|     X-Recruiting: /#/jobs
|     Accept-Ranges: bytes
|     Cache-Control: public, max-age=0
|     Last-Modified: Wed, 29 May 2024 21:57:32 GMT
|     ETag: W/"ea4-18fc65bc0ae"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 3748
|     Vary: Accept-Encoding
|     Date: Tue, 04 Jun 2024 22:13:40 GMT
|     Connection: close
|
|
|
|
|
|     \n\x20\x20\n\x20\x20\n\x20\x20\n\x20\x20\n\x20\x20
```

Nuclei Scan Results

```
[addeventlistener-detect] [http] [info] http://192.168.1.119:3000
[owasp-juice-shop-detect] [http] [info] http://192.168.1.119:3000
[fingerprinthub-web-fingerprints:qm-system] [http] [info] http://192.168.1
```

Wapiti Scan Results

```
*********************************************************************
                    Wapiti 3.0.4 - wapiti.sourceforge.io
                    Report for http://192.168.1.119:3000/
             Date of the scan : Tue, 04 Jun 2024 22:17:50 +0000
                         Scope of the scan : folder
*********************************************************************

Summary of vulnerabilities :
----------------------------
                                                          Backup file
                                                 Blind SQL Injection
                                                    Weak credentials
                                                      CRLF Injection
                                  Content Security Policy Configuration
                                             Cross Site Request Forgery
                                             Potentially dangerous file
                                                      Command execution
                                                         Path Traversal
                                                    Htaccess Bypass
                                                HTTP Secure Headers
                                               HttpOnly Flag cookie
                                                       Open Redirect
                                                 Secure Flag cookie
                                                       SQL Injection
                                           Server Side Request Forgery
                                                  Cross Site Scripting
                                                   XML External Entity
*********************************************************************

Content Security Policy Configuration
-------------------------------------
CSP is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                     *   *   *

CSP is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                     *   *   *

CSP is not set
Evil request:
```

```
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

**************************************************************************

HTTP Secure Headers
-------------------
X-XSS-Protection is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

Strict-Transport-Security is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

X-XSS-Protection is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

Strict-Transport-Security is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

X-XSS-Protection is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

Strict-Transport-Security is not set
Evil request:
```

```
    GET / HTTP/1.1
    Host: 192.168.1.119:3000
cURL command PoC : "curl "http://192.168.1.119:3000/""

                                    *   *   *

**************************************************************************

Summary of anomalies :
----------------------
                                                        Internal Server Error
                                                         Resource consumption
**************************************************************************
Summary of additionals :
------------------------
                                                    Fingerprint web technology
**************************************************************************
```

WhatWeb Scan Results

```
WhatWeb report for http://192.168.1.119:3000
Status    : 200 OK
Title     : OWASP Juice Shop
IP        : 192.168.1.119
Country   : RESERVED, ZZ

Summary   : HTML5, JQuery[2.2.4], Script[module], UncommonHeaders[access-c

Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Version      : 2.2.4
        Website     : http://jquery.com/

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : module

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
```

```
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : access-control-allow-origin,x-content-type-options,

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

HTTP Headers:
        HTTP/1.1 200 OK
        Access-Control-Allow-Origin: *
        X-Content-Type-Options: nosniff
        X-Frame-Options: SAMEORIGIN
        Feature-Policy: payment 'self'
        X-Recruiting: /#/jobs
        Accept-Ranges: bytes
        Cache-Control: public, max-age=0
        Last-Modified: Wed, 29 May 2024 21:57:32 GMT
        ETag: W/"ea4-18fc65bc0ae"
        Content-Type: text/html; charset=UTF-8
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Date: Tue, 04 Jun 2024 22:17:38 GMT
        Connection: close
        Transfer-Encoding: chunked
```

Nikto Scan Results

```
- Nikto v2.5.0/
+ Target Host: 192.168.1.119
+ Target Port: 3000
+ GET /: Retrieved access-control-allow-origin header: *.
+ GET /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ GET /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect H
+ GET /robots.txt: contains 1 entry which should be manually viewed. See:
+ GET .: The X-Content-Type-Options header is not set. This could allow th
+ HEAD /192.168.1.tar: Potentially interesting backup/cert file found. . S
+ HEAD /database.egg: Potentially interesting backup/cert file found. . Se
+ HEAD /archive.cer: Potentially interesting backup/cert file found. . See
+ HEAD /1.cer: Potentially interesting backup/cert file found. . See: http
+ HEAD /168.tar.lzma: Potentially interesting backup/cert file found. . Se
+ HEAD /1.tgz: Potentially interesting backup/cert file found. . See: http
+ HEAD /192.168.1.119.tar: Potentially interesting backup/cert file found.
+ HEAD /database.jks: Potentially interesting backup/cert file found. . Se
+ HEAD /192.168.1.119.pem: Potentially interesting backup/cert file found.
```

```
+ HEAD /archive.tar.bz2: Potentially interesting backup/cert file found. .
+ HEAD /192.jks: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.168.1.tar.lzma: Potentially interesting backup/cert file found
+ HEAD /119.jks: Potentially interesting backup/cert file found. . See: ht
+ HEAD /168.war: Potentially interesting backup/cert file found. . See: ht
+ HEAD /1921681.egg: Potentially interesting backup/cert file found. . See
+ HEAD /168.alz: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192_168_1_119.tar.lzma: Potentially interesting backup/cert file f
+ HEAD /192.168.tar.lzma: Potentially interesting backup/cert file found.
+ HEAD /dump.pem: Potentially interesting backup/cert file found. . See: h
+ HEAD /192.168.tar: Potentially interesting backup/cert file found. . See
+ HEAD /192168.cer: Potentially interesting backup/cert file found. . See:
+ HEAD /archive.tgz: Potentially interesting backup/cert file found. . See
+ HEAD /dump.tar.bz2: Potentially interesting backup/cert file found. . Se
+ HEAD /192_168_1_119.egg: Potentially interesting backup/cert file found.
+ HEAD /backup.cer: Potentially interesting backup/cert file found. . See:
+ HEAD /archive.war: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.1.119.tgz: Potentially interesting backup/cert file found.
+ HEAD /dump.war: Potentially interesting backup/cert file found. . See: h
+ HEAD /192.168.1.war: Potentially interesting backup/cert file found. . S
+ HEAD /site.cer: Potentially interesting backup/cert file found. . See: h
+ HEAD /192.168.1.119.cer: Potentially interesting backup/cert file found.
+ HEAD /192_168_1_119.war: Potentially interesting backup/cert file found.
+ HEAD /192.168.1.egg: Potentially interesting backup/cert file found. . S
+ HEAD /192.168.1.119.jks: Potentially interesting backup/cert file found.
+ HEAD /database.cer: Potentially interesting backup/cert file found. . Se
+ HEAD /1921681.jks: Potentially interesting backup/cert file found. . See
+ HEAD /1921681119.tar.lzma: Potentially interesting backup/cert file foun
+ HEAD /site.tar.lzma: Potentially interesting backup/cert file found. . S
+ HEAD /192.168.1.119.alz: Potentially interesting backup/cert file found.
+ HEAD /archive.alz: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.jks: Potentially interesting backup/cert file found. . See
+ HEAD /1921681119.tgz: Potentially interesting backup/cert file found. .
+ HEAD /119.tar.bz2: Potentially interesting backup/cert file found. . See
+ HEAD /192.tar.bz2: Potentially interesting backup/cert file found. . See
+ HEAD /192_168_1_119.tar.bz2: Potentially interesting backup/cert file fo
+ HEAD /1921681.tar.lzma: Potentially interesting backup/cert file found.
+ HEAD /backup.egg: Potentially interesting backup/cert file found. . See:
+ HEAD /1921681.tar: Potentially interesting backup/cert file found. . See
+ HEAD /database.alz: Potentially interesting backup/cert file found. . Se
+ HEAD /168.egg: Potentially interesting backup/cert file found. . See: ht
+ HEAD /backup.jks: Potentially interesting backup/cert file found. . See:
+ HEAD /192168.egg: Potentially interesting backup/cert file found. . See:
+ HEAD /1.tar.lzma: Potentially interesting backup/cert file found. . See:
+ HEAD /archive.pem: Potentially interesting backup/cert file found. . See
+ HEAD /168.pem: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192168.jks: Potentially interesting backup/cert file found. . See:
+ HEAD /database.pem: Potentially interesting backup/cert file found. . Se
+ HEAD /site.war: Potentially interesting backup/cert file found. . See: h
+ HEAD /1921681119.cer: Potentially interesting backup/cert file found. .
+ HEAD /dump.cer: Potentially interesting backup/cert file found. . See: h
+ HEAD /192.tgz: Potentially interesting backup/cert file found. . See: ht
```

```
+ HEAD /site.pem: Potentially interesting backup/cert file found. . See: h
+ HEAD /168.tar: Potentially interesting backup/cert file found. . See: ht
+ HEAD /119.tgz: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.168.egg: Potentially interesting backup/cert file found. . See
+ HEAD /1.war: Potentially interesting backup/cert file found. . See: http
+ HEAD /168.cer: Potentially interesting backup/cert file found. . See: ht
+ HEAD /site.tar.bz2: Potentially interesting backup/cert file found. . Se
+ HEAD /dump.tar.lzma: Potentially interesting backup/cert file found. . S
+ HEAD /192.168.1.tar.bz2: Potentially interesting backup/cert file found.
+ HEAD /192.168.1.alz: Potentially interesting backup/cert file found. . S
+ HEAD /site.alz: Potentially interesting backup/cert file found. . See: h
+ HEAD /archive.egg: Potentially interesting backup/cert file found. . See
+ HEAD /database.war: Potentially interesting backup/cert file found. . Se
+ HEAD /backup.tar.bz2: Potentially interesting backup/cert file found. .
+ HEAD /192168.tar.bz2: Potentially interesting backup/cert file found. .
+ HEAD /1.alz: Potentially interesting backup/cert file found. . See: http
+ HEAD /1921681.tar.bz2: Potentially interesting backup/cert file found. .
+ HEAD /site.tgz: Potentially interesting backup/cert file found. . See: h
+ HEAD /1.pem: Potentially interesting backup/cert file found. . See: http
+ HEAD /dump.tar: Potentially interesting backup/cert file found. . See: h
+ HEAD /1.jks: Potentially interesting backup/cert file found. . See: http
+ HEAD /192168.tar.lzma: Potentially interesting backup/cert file found. .
+ HEAD /119.cer: Potentially interesting backup/cert file found. . See: ht
+ HEAD /database.tar.lzma: Potentially interesting backup/cert file found.
+ HEAD /192168.tar: Potentially interesting backup/cert file found. . See:
+ HEAD /192.cer: Potentially interesting backup/cert file found. . See: ht
+ HEAD /1921681119.jks: Potentially interesting backup/cert file found. .
+ HEAD /database.tar: Potentially interesting backup/cert file found. . Se
+ HEAD /1921681119.war: Potentially interesting backup/cert file found. .
+ HEAD /119.tar: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.tar: Potentially interesting backup/cert file found. . See: ht
+ HEAD /168.tgz: Potentially interesting backup/cert file found. . See: ht
+ HEAD /backup.tar.lzma: Potentially interesting backup/cert file found. .
+ HEAD /192.168.1.119.tar.bz2: Potentially interesting backup/cert file fo
+ HEAD /1921681.cer: Potentially interesting backup/cert file found. . See
+ HEAD /backup.tar: Potentially interesting backup/cert file found. . See:
+ HEAD /dump.jks: Potentially interesting backup/cert file found. . See: h
+ HEAD /archive.jks: Potentially interesting backup/cert file found. . See
+ HEAD /database.tgz: Potentially interesting backup/cert file found. . Se
+ HEAD /192.pem: Potentially interesting backup/cert file found. . See: ht
+ HEAD /1921681.alz: Potentially interesting backup/cert file found. . See
+ HEAD /119.pem: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.egg: Potentially interesting backup/cert file found. . See: ht
+ HEAD /119.egg: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.168.1.jks: Potentially interesting backup/cert file found. . S
+ HEAD /dump.egg: Potentially interesting backup/cert file found. . See: h
+ HEAD /1921681119.tar: Potentially interesting backup/cert file found. .
+ HEAD /168.tar.bz2: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.pem: Potentially interesting backup/cert file found. . See
+ HEAD /1921681.war: Potentially interesting backup/cert file found. . See
+ HEAD /backup.war: Potentially interesting backup/cert file found. . See:
+ HEAD /192168.tgz: Potentially interesting backup/cert file found. . See:
```

```
+ HEAD /backup.tgz: Potentially interesting backup/cert file found. . See:
+ HEAD /database.tar.bz2: Potentially interesting backup/cert file found.
+ HEAD /192.168.1.pem: Potentially interesting backup/cert file found. . S
+ HEAD /1921681.tgz: Potentially interesting backup/cert file found. . See
+ HEAD /192168.war: Potentially interesting backup/cert file found. . See:
+ HEAD /1.egg: Potentially interesting backup/cert file found. . See: http
+ HEAD /1921681.pem: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.war: Potentially interesting backup/cert file found. . See
+ HEAD /site.tar: Potentially interesting backup/cert file found. . See: h
+ HEAD /backup.alz: Potentially interesting backup/cert file found. . See:
+ HEAD /dump.tgz: Potentially interesting backup/cert file found. . See: h
+ HEAD /192_168_1_119.pem: Potentially interesting backup/cert file found.
+ HEAD /192168.alz: Potentially interesting backup/cert file found. . See:
+ HEAD /archive.tar.lzma: Potentially interesting backup/cert file found.
+ HEAD /dump.alz: Potentially interesting backup/cert file found. . See: h
+ HEAD /1.tar.bz2: Potentially interesting backup/cert file found. . See:
+ HEAD /archive.tar: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.tgz: Potentially interesting backup/cert file found. . See
+ HEAD /1921681119.egg: Potentially interesting backup/cert file found. .
+ HEAD /site.jks: Potentially interesting backup/cert file found. . See: h
+ HEAD /1.tar: Potentially interesting backup/cert file found. . See: http
+ HEAD /192.168.alz: Potentially interesting backup/cert file found. . See
+ HEAD /192.168.1.tgz: Potentially interesting backup/cert file found. . S
+ HEAD /192.168.1.cer: Potentially interesting backup/cert file found. . S
+ HEAD /192_168_1_119.tar: Potentially interesting backup/cert file found.
+ HEAD /192.alz: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192.168.1.119.war: Potentially interesting backup/cert file found.
+ HEAD /192_168_1_119.jks: Potentially interesting backup/cert file found.
+ HEAD /119.alz: Potentially interesting backup/cert file found. . See: ht
+ HEAD /site.egg: Potentially interesting backup/cert file found. . See: h
+ HEAD /192.war: Potentially interesting backup/cert file found. . See: ht
+ HEAD /119.war: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192168.pem: Potentially interesting backup/cert file found. . See:
+ HEAD /1921681119.alz: Potentially interesting backup/cert file found. .
+ HEAD /backup.pem: Potentially interesting backup/cert file found. . See:
+ HEAD /168.jks: Potentially interesting backup/cert file found. . See: ht
+ HEAD /192_168_1_119.alz: Potentially interesting backup/cert file found.
+ HEAD /192.168.cer: Potentially interesting backup/cert file found. . See
+ HEAD /1921681119.pem: Potentially interesting backup/cert file found. .
+ HEAD /192.168.1.119.tar.lzma: Potentially interesting backup/cert file f
+ HEAD /192.tar.lzma: Potentially interesting backup/cert file found. . Se
+ HEAD /192_168_1_119.tgz: Potentially interesting backup/cert file found.
+ HEAD /192.168.1.119.egg: Potentially interesting backup/cert file found.
+ HEAD /119.tar.lzma: Potentially interesting backup/cert file found. . Se
+ HEAD /192.168.tar.bz2: Potentially interesting backup/cert file found. .
+ HEAD /1921681119.tar.bz2: Potentially interesting backup/cert file found
+ HEAD /192_168_1_119.cer: Potentially interesting backup/cert file found.
+ GET /ftp/: This might be interesting.
+ GET /public/: This might be interesting.
+ POST /wp-content/plugins/nextgen-gallery/products/photocrati_nextgen/mod
+ POST /wordpress/wp-content/plugins/nextgen-gallery/products/photocrati_n
```

Dirb Scan Results

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: results/192.168.1.119:3000_04-06-2024/dirb/192.168.1.119:3000
START_TIME: Tue Jun  4 22:21:32 2024
URL_BASE: http://192.168.1.119:3000/
WORDLIST_FILES: wordlists/big.txt

-----------------

GENERATED WORDS: 555

---- Scanning URL: http://192.168.1.119:3000/ ----
+ http://192.168.1.119:3000/profile (CODE:500|SIZE:1160)
+ http://192.168.1.119:3000/video (CODE:200|SIZE:10075518)
+ http://192.168.1.119:3000/assets (CODE:301|SIZE:179)
+ http://192.168.1.119:3000/redirect (CODE:500|SIZE:3119)
+ http://192.168.1.119:3000/ftp (CODE:200|SIZE:11062)

-----------------
END_TIME: Tue Jun  4 22:21:42 2024
DOWNLOADED: 555 - FOUND: 5
```

XSS Scan Results

```
 [91m
        XSStrike  [97mv3.1.5
 [0m
 [97m[~] [0m Crawling the target  [0m
 [97m[~] [0m Parsing ftp
  [0m
 [97m[~] [0m Parsing ftp/incident-support.kdbx
  [0m
 [97m[~] [0m Parsing ftp/eastere.gg
  [0m
 [97m[~] [0m Parsing ftp/quarantine
  [0m
 [97m[~] [0m Parsing ftp/announcement_encrypted.md
  [0m
 [97m[~] [0m Parsing ftp/package.json.bak
  [0m
 [97m[~] [0m Parsing ftp/legal.md
  [0m
 [97m[~] [0m Parsing ftp/acquisitions.md
  [0m
 [97m[~] [0m Parsing ftp/suspicious_errors.yml
```

```
 [0m
[97m[~] [0m Parsing ftp/coupons_2013.md.bak
 [0m
[97m[~] [0m Parsing ftp/encrypt.pyc
 [0m
[93m[!] [0m Progress: 10/11
 [0m
[93m[!] [0m Progress: 11/11
 [0m
```

SQLi Scan Results

File not found.