

OWASP Juice Box

Vulnerability Assessment

**Pauline Finlay**

**B00107945**

***Department of Informatics***

***School of Informatics & Engineering***

***Technological University Dublin, Blanchardstown***

***Dublin 15.***

**Word Limit for Assignment: 3000 Actual Word Count: 3246**

**BSc (Hons) in Computing in Digital Forensics & Cyber Security**

**DFCS H4013 Application Security**

**11th December 2020**

**Plagiarism Declaration**

I hereby certify that this material, which I am submitting for assessment for the course title of BSc. (Hons) In Computing in Digital Forensics and Cyber Security is my own work and that I have:

* Clearly referenced/listed all sources as appropriate
* Given the sources of all pictures, data etc. that is not our own
* Any work of any other student(s) either past or present is clearly referenced
* Not submitted for assessment work previously submitted for any other course, degree or qualification
* Not incorporated any text acquired from external agencies other than extracts from attributed sources (including online facilities)
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* My work may be electronically checked for plagiarism, including, but not exclusively, by the use of plagiarism detection software and stored for future comparison
* Any false claim for this work will be penalised in accordance with the College’s regulations

**Signed:** Pauline Finlay **Date:** 11/12/2020

**Executive Summary**

***Overview***

***Summary of Findings***

Contents

[1. Introduction 1](#_Toc56854123)

[1.1. Overview 1](#_Toc56854124)

[1.2. Scope 1](#_Toc56854125)

[1.3. Out of Scope 1](#_Toc56854126)

[1.4. Project Team 1](#_Toc56854127)

[2. Assessment Methods 1](#_Toc56854128)

[2.1. Functionality Testing 1](#_Toc56854129)

[2.2. Usability testing 1](#_Toc56854130)

[2.3. Interface testing 1](#_Toc56854131)

[2.4. Compatibility testing 1](#_Toc56854132)

[2.5. Performance testing 2](#_Toc56854133)

[2.5.1. Load testing 2](#_Toc56854134)

[2.5.2. Stress testing 2](#_Toc56854135)

[2.5.3. Soak testing 2](#_Toc56854136)

[2.5.4. Spike testing 2](#_Toc56854137)

[2.6. Security testing 2](#_Toc56854138)

[3. Control Areas 3](#_Toc56854139)

[3.1. Architecture and design 3](#_Toc56854140)

[3.2. Access Control 3](#_Toc56854141)

[3.3. Authentication 3](#_Toc56854142)

[3.4. Configuration Management 3](#_Toc56854143)

[3.5. Cryptography 3](#_Toc56854144)

[3.6. Patch Management 3](#_Toc56854145)

[3.7. Protective monitoring 3](#_Toc56854146)

[4. Findings & Recommendations 3](#_Toc56854147)

[4.1. Web Application Security Assessment 3](#_Toc56854148)

[4.1.1. Information Gathering 3](#_Toc56854149)

[4.1.2. Reconnaissance 3](#_Toc56854150)

[4.1.3. Communications Security and Cryptography 3](#_Toc56854151)

[4.1.4. Authentication Mechanisms 3](#_Toc56854152)

[4.1.5. Session Management 3](#_Toc56854153)

[4.1.6. Authorisation Access Controls 3](#_Toc56854154)

[4.1.7. Data Validation 3](#_Toc56854155)

[4.2. Technical Summary 3](#_Toc56854156)

[4.3. Vulnerability Table 3](#_Toc56854157)

[5. Conclusion 4](#_Toc56854158)

[6. References 4](#_Toc56854159)

[7. Appendix 5](#_Toc56854160)

[7.1. Impact and Exploitation Definitions 5](#_Toc56854161)

[7.2. Port Scan Details 6](#_Toc56854162)

[7.3. Tools List 7](#_Toc56854163)

**Table of Tables**

[Table 1: Asset Table 2](#_Toc55469824)

[Table 2: Threat Table 11](#_Toc55469825)

[Table 3: DREAD Scoring 22](#_Toc55469826)

[Table 4: Mitigation Plan 23](#_Toc55469827)

**Table of Figures**

[Figure 1: Overall DFD for Money Management Web Application 4](#_Toc55469828)

[Figure 2: User Login 7](#_Toc55469829)

[Figure 3: Authorised user request transaction history 8](#_Toc55469830)

[Figure 4: Authorised user logs into banking server to request current information 8](#_Toc55469831)

[Figure 5: Authorised user logs into baking server to issue bill payment instruction 9](#_Toc55469832)

[Figure 6: New bill sent from biller to application 9](#_Toc55469833)

[Figure 7: Administrator login direct to application 10](#_Toc55469834)

# Introduction

## Overview

This report was prepared to document the findings of the vulnerability assessment for OWASP Juice Box an internet facing application. This assessment was carried out to identify potential vulnerabilities within the system.

## Scope

OWASP Juice Box defined the following URL as in scope:

* http://localhost:3000/

## Out of Scope

OWASP Juice Box defined the following URL’s as out of scope:

* https://github.com/bkimminich/juice-shop

## External Tools

VEGA

OWASP ZAP

Nikto

## Project Team

The assessment began on the 21st November 2020 and was carried out by the following team members:

|  |  |
| --- | --- |
| **Role** | **Name** |
| Customer Project Manager | Stephen O’Shaughnessy |
| Vulnerability Assessor | Pauline Finlay |

# Assessment Methods

## ***Functionality Testing***

The below are some of the checks that are performed but not limited to the below list:

* Verify there is no dead page or invalid redirects.
* First check all the validations on each field.
* Wrong inputs to perform negative testing.
* Verify the workflow of the system.
* Verify the data integrity.

## Usability testing

To verify how the application is easy to use with.

* Test the navigation and controls.
* Content checking.
* Check for user intuition.

## Interface testing

Performed to verify the interface and the dataflow from one system to other.

## Compatibility testing

Compatibility testing is performed based on the context of the application.

* Browser compatibility
* Operating system compatibility
* Compatible to various devices like notebook, mobile, etc.

## Performance testing

Performed to verify the server response time and throughput under various load conditions.

### Load testing

It is the simplest form of testing conducted to understand the behaviour of the system under a specific load. Load testing will result in measuring important business critical transactions and load on the database, application server, etc. are also monitored.

### Stress testing

It is performed to find the upper limit capacity of the system and also to determine how the system performs if the current load goes well above the expected maximum.

### Soak testing

Soak Testing also known as endurance testing, is performed to determine the system parameters under continuous expected load. During soak tests the parameters such as memory utilization is monitored to detect memory leaks or other performance issues. The main aim is to discover the system's performance under sustained use.

### Spike testing

Spike testing is performed by increasing the number of users suddenly by a very large amount and measuring the performance of the system. The main aim is to determine whether the system will be able to sustain the work load.

## Security testing

### Injection

### Broken Authentication and Session Management

### Sensitive Data Exposure

### XML External Entities (XXE)

### Broken Access Control

### Security Misconfiguration

### Cross-Site Scripting (XSS)

### Insecure Deserialization

### Using Components with Known Vulnerabilities

### Insufficient Logging & Monitoring

### Unvalidated Redirects and Forwards

### Cross-Site Request Forgery (CSRF)

## Automated Vulnerability Scanning Tools

The web application was tested using automated vulnerability scanning tools, OWASP ZAP and VEGA. The results from the scans are detailed in the tables below.

### OWASP ZAP

Scan Alert Summary

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cross-Domain Misconfiguration**  **Risk: Medium**  **Count: 30**  **CWE ID: 264**  **WASC ID: 14** | | | | | | | | | | | | | | |
| **Resource** | | | | | **Discussion** | | | | **Impact** | | | | | **Remediation** |
| GET:http://localhost:3000  GET:http://localhost:3000/  GET:http://localhost:3000/assets/public/favicon\_js.ico  GET:http://localhost:3000/ftp  GET:http://localhost:3000/ftp/  GET:http://localhost:3000/ftp/acquisitions.md  GET:http://localhost:3000/ftp/announcement\_encrypted  GET:http://localhost:3000/ftp/coupons\_2013.md.bak  GET:http://localhost:3000/ftp/eastere.gg  GET:http://localhost:3000/ftp/encrypt.pyc  GET:http://localhost:3000/ftp/incident-support.kdbx  GET:http://localhost:3000/ftp/legal.md  GET:http://localhost:3000/ftp/package.json.bak  GET:http://localhost:3000/ftp/quarantine  GET:http://localhost:3000/ftp/quarantine/juicy\_malware\_linux\_amd\_64.url  GET:http://localhost:3000/ftp/quarantine/juicy\_malware\_linux\_arm\_64.url  GET:http://localhost:3000/ftp/quarantine/juicy\_malware\_macos\_64.url  GET:http://localhost:3000/ftp/quarantine/juicy\_malware\_windows\_.64.exe.url  GET:http://localhost:3000/ftp/suspicious\_errors.yml  GET:http://localhost:3000/main-es2018.js  GET:http://localhost:3000/main-es5.js  GET:http://localhost:3000/polyfills-es2018.js  GET:http://localhost:3000/polyfills-es5.js  GET:http://localhost:3000/robots.txt  GET:http://localhost:3000/runtime-es2018.js  GET:http://localhost:3000/main-es5.js  GET:http://localhost:3000/sitemap.xml  GET:http://localhost:3000/styles.css  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es5.js | | | | | Resource has set an insecure Cross-Origin Resource Sharing (CORS) access control | | | | Any site can issue requests to access resources irrespective of origin | | | | | Set ‘Access-Control-Allow-Origin’ to allow access from trusted domains only |
| **Cross-Domain JavaScript Source File Inclusion**  **Risk: Low**  **Count: 6**  **CWE ID: 829**  **WASC ID: 15** | | | | | | | | | | | | | | |
| **Resource** | | | | **Discussion** | | | **Impact** | | | | | | **Remediation** | |
| GET:http://localhost:3000  GET:http://localhost:3000  GET:http://localhost:3000/  GET:http://localhost:3000/  GET:http://localhost:3000/sitemap.xml  GET:http://localhost:3000/sitemap.xml | | | | This page includes one or more script files from a 3rd party domain | | | JavaScript files could be loaded allowing end users to control the application | | | | | | Ensure JavaScript source files are loaded from only trusted sources | |
| **Web Browser XSS Protection Not Enabled**  **Risk: Low**  **Count: 11**  **CWE ID: 933**  **WASC ID: 14** | | | | | | | | | | | | | | |
| **Resource** | | | **Discussion** | | | | | **Impact** | | | **Remediation** | | | |
| GET:http://localhost:3000  GET:http://localhost:3000/  GET:http://localhost:3000/ftp  GET:http://localhost:3000/ftp/  GET:http://localhost:3000/ftp/coupons\_2013.md.bak  GET:http://localhost:3000/ftp/eastere.gg  GET:http://localhost:3000/ftp/encrypt.pyc  GET:http://localhost:3000/ftp/package.json.bak  GET:http://localhost:3000/ftp/quarantine  GET:http://localhost:3000/ftp/suspicious\_errors.yml  GET:http://localhost:3000/sitemap.xml | | | Web Browser XSS Protection is not enabled or is disabled by the configuration of the ‘X-XSS-Protection’ HTTP response header on the web server | | | | |  | | | Ensure that the XSS filter is enabled by setting the X-XSS Protection HTTP response header to ‘1’ | | | |
| **Information Disclosure – Suspicious Comments**  **Risk: Informational**  **Count: 6**  **CWE ID: 200**  **WASC ID: 13** | | | | | | | | | | | | | | |
| **Resource** | **Discussion** | | | | | **Impact** | | | | **Remediation** | | | | |
| GET:http://localhost:3000/main-es2018.js  GET:http://localhost:3000/main-es5.js  GET:http://localhost:3000/polyfills-es2018.js  GET:http://localhost:3000/polyfills-es5.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es5.js | Response appears to contain suspicious comments which may help attacker | | | | |  | | | | Remove all comment that return information that my help an attacker  And fix any underlying problems they refer to | | | | |
| **Timestamp Disclosure - UNIX**  **Risk: Informational**  **Count: 23**  **CWE ID: 200**  **WASC ID: 13** | | | | | | | | | | | | | | |
| **Resource** | | **Discussion** | | | | | | **Impact** | | | | **Remediation** | | |
| GET:http://localhost:3000/polyfills-es5.js  GET:http://localhost:3000/polyfills-es5.js  GET:http://localhost:3000/styles.css  GET:http://localhost:3000/styles.css  GET:http://localhost:3000/styles.css  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es2018.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js  GET:http://localhost:3000/vendor-es5.js | | A timestamp was disclosed by the application/web server - UNIX | | | | | | Sensitive data could be disclosed to an attacker | | | | Confirm timestamp data is not sensitive | | |

### VEGA

Scan Alert Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Insecure Cross-Origin Resource Access Control**  **Classification: Information**  **Risk: High**  **Count: 36** | | | | | |
| **Resource** | | **Discussion** | **Impact** | | **Remediation** |
| /  /assets/  /assets/public/  /assets/public/assets/  /assets/public/assets/assets  /assets/public/assets/assets/public  /assets/public/assets/assets/public/favicon\_js.ico  /assets/public/assets/main-es2018.js  /assets/public/assets/main-es5.js  /assets/public/assets/polyfills-es2018.js  /assets/public/assets/polyfills-es5.js  /assets/public/assets/public/  /assets/public/assets/public/favicon\_js.ico  /assets/public/assets/runtime-es2018.js  /assets/public/assets/runtime-es5.js  /assets/public/assets/styles.css  /assets/public/assets/vendor-es2018.js  /assets/public/assets/vendor-es5.js  /assets/public/main-es2018.js  /assets/public/main-es5.js  /assets/public/polyfills-es2018.js  /assets/public/polyfills-es5.js  /assets/public/runtime-es2018.js  /assets/public/runtime-es5.js  /assets/public/styles.css  /assets/public/vendor-es2018.js  /assets/public/vendor-es5.js  /main-es2018.js  /main-es5.js  /polyfills-es2018.js  /polyfills-es5.js  /runtime-es2018.js  /rumtime-es5.js  /styles.css  /vendor-es2018.js  /vendor-es5.js | | Resource has set an insecure Cross-Origin Resource Sharing (CORS) access control | Any site can issue requests to access resources irrespective of origin | | Set ‘Access-Control-Allow-Origin’ to allow access from trusted domains only |
| **Blank Body Detected**  **Classification: Information**  **Risk: High**  **Count: 2** | | | | | |
| **Resource** | **Discussion** | **Impact** | | **Remediation** | |
| /vendor-es2018.js  /vendor-es5.js | Requesting URI returned blank response body | May indicate error condition manual investigation needed | | Investigate occurrence and any security implications | |

### Nikto

|  |  |  |  |
| --- | --- | --- | --- |
| **Blank Body Detected**  **Classification: Information**  **Risk: High**  **Count: 2** | | | |
| **Resource** | **Discussion** | **Impact** | **Remediation** |
|  |  |  |  |

# Control Areas

## Architecture and design

## Access Control

## Authentication

## Configuration Management

## Cryptography

## Patch Management

## Protective monitoring

# Findings & Recommendations

## Web Application Security Assessment

### Information Gathering

### Reconnaissance

### Communications Security and Cryptography

### Authentication Mechanisms

### Session Management

### Authorisation Access Controls

### Data Validation

## Technical Summary

## Vulnerability Table

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Vulnerability/Impact** | **Ease of Exploit** | **Recommendation** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Key Issues

# Conclusion

# References

[1]"Web Application Testing - Tutorialspoint", *Tutorialspoint.com*, 2020. [Online]. Available: https://www.tutorialspoint.com/software\_testing\_dictionary/web\_application\_testing.htm. [Accessed: 19- Nov- 2020].

[2]*Cstl.com*, 2020. [Online]. Available: https://www.cstl.com/CST/Penetration-Test/CST-Web-Application-Testing-Report.pdf. [Accessed: 19- Nov- 2020].

# Appendix

## Impact and Exploitation Definitions

A qualitative impact factor (High, Medium, or Low) has been associated with each vulnerability as well as an arbitrary assignment of the degree of skill that an attacker would require to exploit the vulnerability (Trivial, Moderate, Difficult). This should assist Acme Inc in their risk management efforts through the prioritisation of any remedial activity.

Activity’s impact and ease of exploitation categorisation can be illustrated in the tables below:

|  |  |
| --- | --- |
| **Impact** | **Definition** |
| Low | Minimal impact on the business if exploited. Information disclosed is of no significant detrimental value, no repudiation or legal consequence, minimal to no impact in regards to regulatory or standards compliance. |
| Medium | Moderate financial impact, possible legal consequences and reputational ramifications. |
| High | Significant financial loss, damage to brand and business identity through potential media involvement, exposure and compromise of data. |

|  |  |
| --- | --- |
| **Ease of Exploit** | **Definition** |
| Trivial | Publicly available exploit code or easily available tools to automate discovery and exploitation. Vulnerability is exploitable with the aid of minimal knowledge and or research. |
| Moderate | Requires some level of skill in basic programming or scripting and or a degree of knowledge and understanding of the target platform/software/application etc. |
| Difficult | Exploitation requires a highly skilled, motivated and apt attacker. |

## Port Scan Details

TCP and UDP port scans were conducted on all hosts within the scope of testing to establish running services on the hosts the results of which are detailed in the tables below.

|  |  |
| --- | --- |
| **IP Address** | **TCP Ports** |
|  |  |

## Nikto Scan

kali@kali:~$ nikto -h 127.0.0.1:3000

- Nikto v2.1.6

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

+ Target IP: 127.0.0.1

+ Target Hostname: 127.0.0.1

+ Target Port: 3000

+ Start Time: 2020-11-22 11:28:31 (GMT-5)

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

+ Server: No banner retrieved

+ Retrieved access-control-allow-origin header: \*

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'feature-policy' found, with contents: payment 'self'

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Entry '/ftp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

+ "robots.txt" contains 1 entry which should be manually viewed.

+ /0.tgz: Potentially interesting archive/cert file found.

+ /0.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.pem: Potentially interesting archive/cert file found.

+ /site.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.alz: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.egg: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.war: Potentially interesting archive/cert file found.

+ /backup.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.tar.bz2: Potentially interesting archive/cert file found.

+ /1270.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.cer: Potentially interesting archive/cert file found.

+ /0.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.cer: Potentially interesting archive/cert file found.

+ /12700.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.tgz: Potentially interesting archive/cert file found.

+ /1270.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.tar: Potentially interesting archive/cert file found.

+ /127001.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.pem: Potentially interesting archive/cert file found.

+ /127.0.0.1.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.pem: Potentially interesting archive/cert file found.

+ /0.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.tar.lzma: Potentially interesting archive/cert file found.

+ /127.0.0.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.pem: Potentially interesting archive/cert file found.

+ /12700.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.alz: Potentially interesting archive/cert file found.

+ /1.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.jks: Potentially interesting archive/cert file found.

+ /127.0.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.war: Potentially interesting archive/cert file found.

+ /127.0.0.1.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.alz: Potentially interesting archive/cert file found.

+ /site.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.tar: Potentially interesting archive/cert file found.

+ /backup.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.jks: Potentially interesting archive/cert file found.

+ /127.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.egg: Potentially interesting archive/cert file found.

+ /127.0.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.tar.bz2: Potentially interesting archive/cert file found.

+ /1.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.cer: Potentially interesting archive/cert file found.

+ /127.0.0.1.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.cer: Potentially interesting archive/cert file found.

+ /127.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.tar.lzma: Potentially interesting archive/cert file found.

+ /1.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.alz: Potentially interesting archive/cert file found.

+ /127.0.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.jks: Potentially interesting archive/cert file found.

+ /1.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.war: Potentially interesting archive/cert file found.

+ /127001.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.alz: Potentially interesting archive/cert file found.

+ /127001.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.alz: Potentially interesting archive/cert file found.

+ /0.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.pem: Potentially interesting archive/cert file found.

+ /127001.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.tar: Potentially interesting archive/cert file found.

+ /1270.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.pem: Potentially interesting archive/cert file found.

+ /1.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.tar.bz2: Potentially interesting archive/cert file found.

+ /127.0.0.1.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.cer: Potentially interesting archive/cert file found.

+ /site.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.jks: Potentially interesting archive/cert file found.

+ /0.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.war: Potentially interesting archive/cert file found.

+ /site.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.tar.lzma: Potentially interesting archive/cert file found.

+ /0.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.tar.lzma: Potentially interesting archive/cert file found.

+ /12700.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.tar.bz2: Potentially interesting archive/cert file found.

+ /0.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.tar: Potentially interesting archive/cert file found.

+ /127.0.0.1.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.jks: Potentially interesting archive/cert file found.

+ /1270.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.tar.bz2: Potentially interesting archive/cert file found.

+ /12700.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.tgz: Potentially interesting archive/cert file found.

+ /127.0.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.war: Potentially interesting archive/cert file found.

+ /127.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.tar: Potentially interesting archive/cert file found.

+ /127.0.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.tar.lzma: Potentially interesting archive/cert file found.

+ /1270.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.war: Potentially interesting archive/cert file found.

+ /12700.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.alz: Potentially interesting archive/cert file found.

+ /backup.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.egg: Potentially interesting archive/cert file found.

+ /1270.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.jks: Potentially interesting archive/cert file found.

+ /127.0.0.1.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.pem: Potentially interesting archive/cert file found.

+ /backup.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.tgz: Potentially interesting archive/cert file found.

+ /1.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.alz: Potentially interesting archive/cert file found.

+ /127.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.tar.lzma: Potentially interesting archive/cert file found.

+ /127.0.0.1.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.tgz: Potentially interesting archive/cert file found.

+ /127.0.0.1.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.egg: Potentially interesting archive/cert file found.

+ /127.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.cer: Potentially interesting archive/cert file found.

+ /1.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.alz: Potentially interesting archive/cert file found.

+ /1270.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.jks: Potentially interesting archive/cert file found.

+ /127.0.0.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.jks: Potentially interesting archive/cert file found.

+ /127001.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.tgz: Potentially interesting archive/cert file found.

+ /127.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.cer: Potentially interesting archive/cert file found.

+ /127.0.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.tgz: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.tar.lzma: Potentially interesting archive/cert file found.

+ /backup.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.tar.lzma: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.cer: Potentially interesting archive/cert file found.

+ /127.0.0.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.tar: Potentially interesting archive/cert file found.

+ /1.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.jks: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.cer: Potentially interesting archive/cert file found.

+ /127001.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.tar: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.jks: Potentially interesting archive/cert file found.

+ /backup.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.tar.lzma: Potentially interesting archive/cert file found.

+ /127001.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.tar.bz2: Potentially interesting archive/cert file found.

+ /site.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.egg: Potentially interesting archive/cert file found.

+ /12700.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.alz: Potentially interesting archive/cert file found.

+ /12700.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.tgz: Potentially interesting archive/cert file found.

+ /site.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.tgz: Potentially interesting archive/cert file found.

+ /127.0.0.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.tar.bz2: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.pem: Potentially interesting archive/cert file found.

+ /1270.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.pem: Potentially interesting archive/cert file found.

+ /127.0.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.jks: Potentially interesting archive/cert file found.

+ /12700.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.cer: Potentially interesting archive/cert file found.

+ /backup.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.egg: Potentially interesting archive/cert file found.

+ /0.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.war: Potentially interesting archive/cert file found.

+ /0.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.tar.lzma: Potentially interesting archive/cert file found.

+ /127.0.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.cer: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.tgz: Potentially interesting archive/cert file found.

+ /backup.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.egg: Potentially interesting archive/cert file found.

+ /127.0.0.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.tar.bz2: Potentially interesting archive/cert file found.

+ /127.0.0.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.tar.bz2: Potentially interesting archive/cert file found.

+ /127001.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.alz: Potentially interesting archive/cert file found.

+ /127.0.0.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.egg: Potentially interesting archive/cert file found.

+ /127001.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.tar.bz2: Potentially interesting archive/cert file found.

+ /127.0.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.tar.lzma: Potentially interesting archive/cert file found.

+ /127.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.tar: Potentially interesting archive/cert file found.

+ /127.0.0.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.war: Potentially interesting archive/cert file found.

+ /127.0.0.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.tgz: Potentially interesting archive/cert file found.

+ /12700.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.pem: Potentially interesting archive/cert file found.

+ /127.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.tar.bz2: Potentially interesting archive/cert file found.

+ /127.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.war: Potentially interesting archive/cert file found.

+ /1.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1.egg: Potentially interesting archive/cert file found.

+ /1.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.pem: Potentially interesting archive/cert file found.

+ /127.0.0.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.tar: Potentially interesting archive/cert file found.

+ /127.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.war: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.tar.lzma: Potentially interesting archive/cert file found.

+ /site.tar.lzma: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127\_0\_0\_1.pem: Potentially interesting archive/cert file found.

+ /127\_0\_0\_1.pem: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.egg: Potentially interesting archive/cert file found.

+ /site.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.egg: Potentially interesting archive/cert file found.

+ /backup.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.war: Potentially interesting archive/cert file found.

+ /1270.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127001.tgz: Potentially interesting archive/cert file found.

+ /127001.tgz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.jks: Potentially interesting archive/cert file found.

+ /site.jks: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.egg: Potentially interesting archive/cert file found.

+ /127.0.0.1.egg: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /backup.tar.bz2: Potentially interesting archive/cert file found.

+ /backup.tar.bz2: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /12700.tar: Potentially interesting archive/cert file found.

+ /12700.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /site.tar: Potentially interesting archive/cert file found.

+ /site.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /1270.cer: Potentially interesting archive/cert file found.

+ /1270.cer: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.war: Potentially interesting archive/cert file found.

+ /127.0.war: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /0.tar: Potentially interesting archive/cert file found.

+ /0.tar: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ /127.0.0.1.alz: Potentially interesting archive/cert file found.

+ /127.0.0.1.alz: Potentially interesting archive/cert file found. (NOTE: requested by IP address).

+ OSVDB-3092: /ftp/: This might be interesting...

+ OSVDB-3092: /public/: This might be interesting...

+ ERROR: Error limit (20) reached for host, giving up. Last error:

+ Scan terminated: 2 error(s) and 247 item(s) reported on remote host

+ End Time: 2020-11-22 11:30:36 (GMT-5) (125 seconds)

## Tools List

The table below is a list of commercial, open source and proprietary scripts, tools, applications and software suites that were used to perform the assessment.

|  |  |
| --- | --- |
| **Tool** | **Description** |
| Burp | Burp Suite is an integrated platform for attacking web applications.  http://portswigger.net/suite |
| Nessus | Nessus is an automated vulnerability scanner.  http://www.nessus.org/nessus/ |
| netcat | Netcat is a featured networking utility, which reads and writes data across.  http://netcat.sourceforge.net/ |
| Nikto |  |
| Nmap | Nmap ("Network Mapper") is a free and open source (license) utility for network exploration or security auditing.  http://nmap.org |
| ZAP | OWASP Zed Attack Proxy (ZAP) is a free, open source, web application scanner.  https://www.zaproxy.org/ |