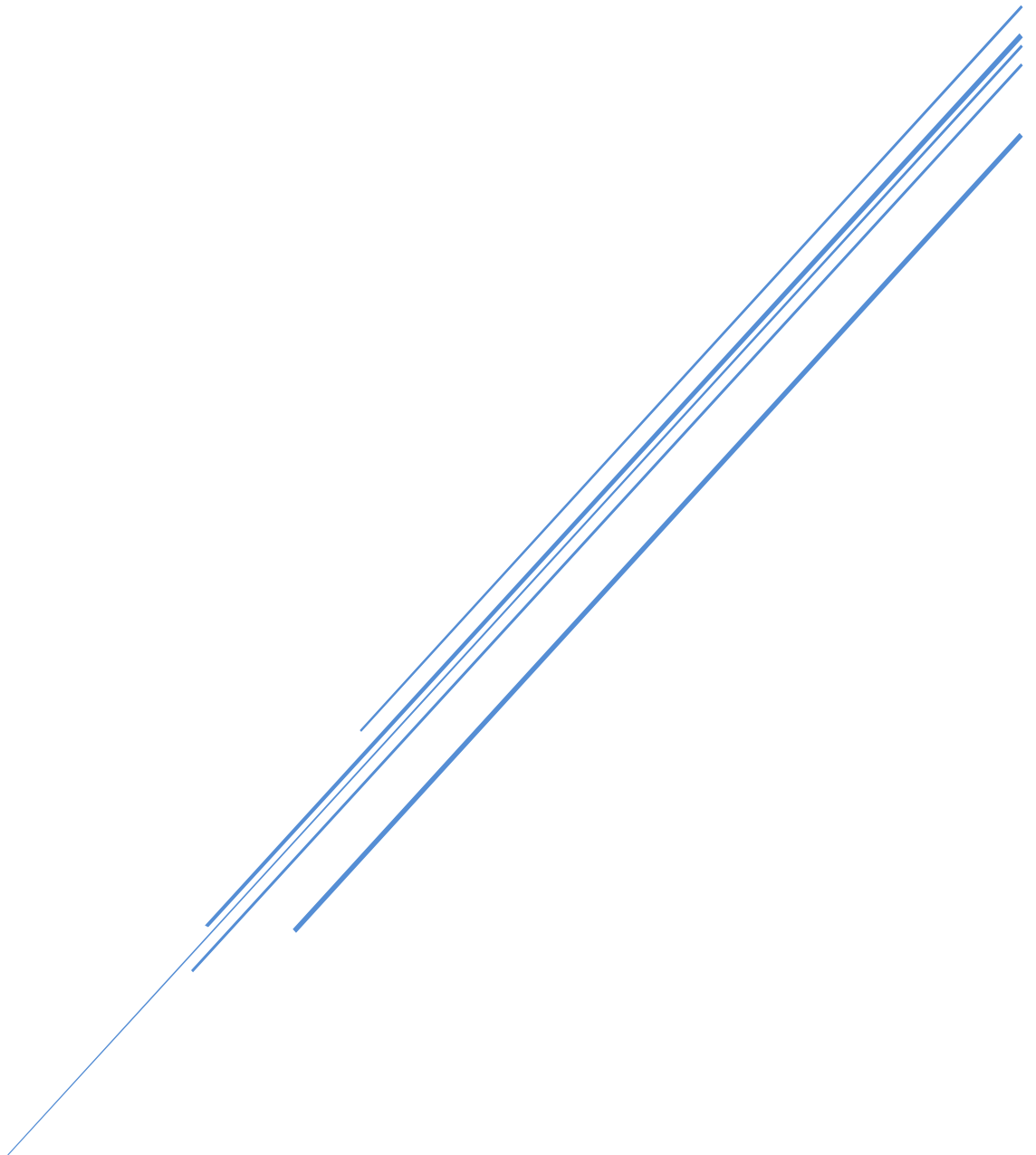


# PENETRATION TEST

JUGGYSHOP



NUR SYAIRAH BINTI ABD SALAM  
RCCE JULY 2022

---

## Table of Contents

Executive Summary .....	2
1. Introduction .....	3
2. Context and Scope.....	4
3. Statement of Methodology .....	5
4. Statement of Limitation.....	5
Findings .....	6
1. Footprinting .....	7
2. Threats and Vulnerabilities.....	9
3. Testing Narrative .....	17
Denial of Service Attack (DOS).....	17
Countermeasures .....	19
References .....	21
Appendix A: FinalRecon Results .....	22
Appendix B: Sucuri Scan.....	28
Appendix C: Virustotal.....	28
Appendix D: Nessus Scan .....	28

---

## Executive Summary

This report describes the results of vulnerability assessment and penetration testing for the website Juggyshop.com. Founded by the New York based company Ogami, the website offers online purchases of their in-house grown organic vegan groceries.

From the initial foot-printing report there is no high risk or critical vulnerabilities discovered within the website. Some errors that are low to medium risk that were identified from the Nessus and OWASP Zaproxy scan can be addressed quickly and sufficiently. DDos attack was performed on the server, which demonstrate its effectiveness in mitigating such attacks.

In summary, a penetration test was performed as specified in the published documentation and found that its security and privacy features are intact and effective.

## 1. Introduction

Juggyshop.com is an online platform launched under the New York based company, Ogami, where clients may buy natural organic and vegan groceries produced by the company's in-house farmers in their own integrated agro-forestry farms. Their produce is claimed to be healthy, fresh and grown through modern farming techniques and processes. Currently, they have over 16 farms and 142 active engineers working under Ogami. Juggyshop's product line ranges from fruits, vegetables, nuts, ocean foods, butter and eggs, cakes and biscuits, butter and eggs and fast foods such as banana salted chips, frozen samosa, masala papad and potato wafers. The website guarantees secure payment, free shipping and on-time delivery.

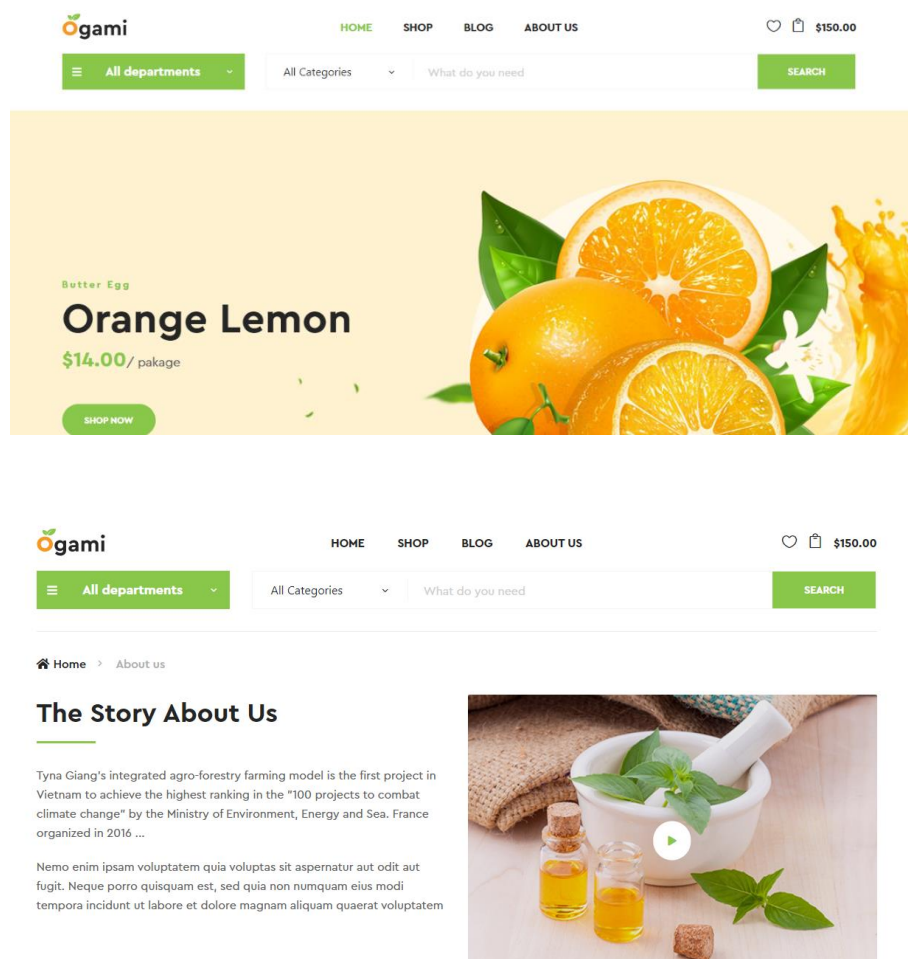


Figure 1: Juggyshop homepage

---

## 2. Context and Scope

The goal of this pentest was a thorough third-party, grey-box assessment of the security and soundness of the Juggyshop online platform, divulging a thorough picture of vulnerabilities associated to its server and application-based layer. The objective is to evaluate the validity of Juggyshop's security. Furthermore, the penetration test will determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental confidentiality, integrity and accessibility of the website. The test was performed during the period from May 2022 to July 2022, using the Rose and Kali Linux operating system when needed. Any live testing was done using platform provided (juggyshop.com).

---

### 3. Statement of Methodology

Information gathered from the website was collected from various sources such as sucuri, ipinfo.io, domaintools, shodan.io, whois, and HTTP3check. Additionally, information from the CVE list and Nessus scan was used to outline the weaknesses of the target. The DDos attack methodology was through the use of the popular Hammer tool, whereas Wireshark was used for the monitoring of the outgoing streams. Details on the methodologies used to complete the testing can be found in the Findings section on page 6.

### 4. Statement of Limitation

The testing was majorly dependent on the soundness of the Rose operating system. During testing, it was found that the OS cannot be accessed after 12AM MYT, and are prone to network disruptions, in which case Kali was used as a backup. Grey box testing means that very few information regarding the website was provided before the test which may hinder accurate testing. Furthermore, the website provided has many links that cannot be clicked to a legit page, eg. the login page and also the search bar page. This is found to hinder certain attacks such as SQL injections.

---

## Findings

The initial information gathering, and vulnerability assessment of this penetration test reports from various foot printing tools/sites. The results of the test reveal no high risk or critical vulnerabilities. The fact that most findings were low to medium risk issues or informational notes is a sign for the overall good quality and security of the website. The vulnerability list from CVE are on the server used (Cloudflare), however the choice of server is already secured enough against various web server attacks.

The audit revealed two low risk vulnerabilities: Incomplete or No Cache-control and Pragma HTTP Header Set and Cross-Domain JavaScript Source File Inclusion. The former relates to an application misconfiguration, whereas the latter are a vulnerability on information leakage. Another application misconfiguration found more on the medium risk scale, relates to the X-Frame-Options settings. All vulnerability can be mitigated by checking the settings on the application and ensuring all third-party scripts used are from trusted sources.



The identified low to medium risk vulnerabilities do not pose a directly exploitable risk to users but should be fixed nevertheless to leave a good overall impression of the code. While no audit can prove the complete absence of any vulnerabilities in a software/application, this audit left the impression that Juggyshop takes the security of the website seriously. The detailed findings revealed by this audit are outlined in the section below and in Appendix A, B, C and D.

---

## 1. Footprinting

Using various footprinting services such as sucuri, ipinfo.io, domaintools, shodan.io, whois and HTTP3check, various information regarding the website was found. Finalrecon analyses shows that the site's associated IP address are 172.67.156.205 and 104.21.8.41 with ASN AS13335. The IP address is geolocated to California, US. The website is created on November 2018 and is hosted on CloudFlare. Details of the Finalrecon report can be seen in Appendix A.

### (i) Details from domaintools.com

<i>Registrant</i>	Perfect Privacy, LLC
<i>Registrant Country</i>	US
<i>Registrar</i>	Network Solutions, LLC IANA ID: 2 URL: <a href="http://networksolutions.com">http://networksolutions.com</a>
<i>Registrar Status</i>	clientTransferProhibited
<i>Dates</i>	1,365 days old Created on 2018-11-05 Expires on 2022-11-05 Updated on 2021-09-06
<i>Name Servers</i>	Clark.ns.cloudflare.com (has 25,137,989 domains) Kristin.ns.cloudflare.com (has 25,137,989 domains)
<i>Tech Contact</i>	Perfect Privacy, LLC 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, US uh6dn7e53r8@networksolutionsprivateregistration.com (p) 15707088622
<i>IP Address</i>	104.21.8.41 - 471 other sites hosted on this server
<i>IP Location</i>	 - California - San Jose - Cloudflare Inc.
<i>ASN</i>	 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
<i>Domain Status</i>	Registered And Active Website
<i>IP History</i>	3 changes on 3 unique IP addresses over 4 years
<i>Registrar History</i>	2 registrars
<i>Hosting History</i>	2 changes on 3 unique name servers over 4 years

### (ii) Geolocation details from ipinfo.io

<i>State</i>	California
<i>Country</i>	United States
<i>Postal</i>	33101
<i>Timezone</i>	America/New_York
<i>Coordinates</i>	25.7743,-80.1937



---

(iii) Ports found from FinalRecon

80	http
9418	git
10000	webmin
10082	amandaidx
13722	bpjava-msvc
13782	bpcd
13783	# Local services
135	loc-srv
21	ftp
554	rtsp

(iv) HTTP3 and QUIC details of Juggyshop

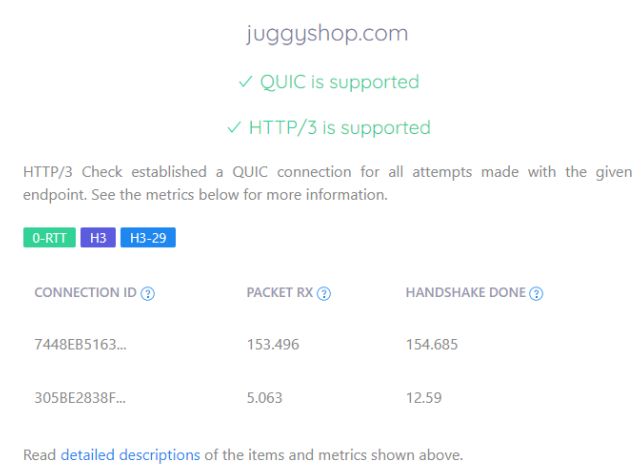


Figure 2: HTTP3 and QUIC details

## 2. Threats and Vulnerabilities

### (i) Sucuri, Virustotal and Nessus scanning results

A simple site check using the Sucuri website (Appendix B) monitoring tool and Virustotal (Appendix C) reveals no critical malwares associated with the target. Nessus scanning shows that there is no risk factor for the website (Appendix D), below shows more information on the HTTP and Web Server No 404 Error Code Check.

The screenshot displays the Nessus interface for a specific plugin. The title bar indicates 'INFO Web Server No 404 Error Code Check'. The 'Description' section explains that the remote web server is configured to not return '404 Not Found' error codes for non-existent files, instead returning a site map, search page, or authentication page. It also notes that Nessus has enabled counter measures, but they might be insufficient. The 'Output' section shows a message: 'CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : http://www.juggysshop.com/ruDZktLpvSN7.html'. The 'Port' is 80 / tcp / http\_proxy and the 'Hosts' are www.juggysshop.com. The 'Plugin Details' sidebar on the right lists: Severity: Info, ID: 10386, Version: \$Revision: 1.98 \$, Type: remote, Family: Web Servers, Published: April 28, 2000, Modified: October 13, 2015. The 'Risk Information' section shows 'Risk Factor: None'.

Figure 3: Web Server No 404 Error Code Check

This block contains two screenshots of Nessus scan results. The top screenshot is for the 'HTTP Methods Allowed (per directory)' plugin. The 'Description' states that by calling the OPTIONS method, it's possible to determine which HTTP methods are allowed on each directory. It also mentions that the plugin tests if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'. The 'Output' shows a list of allowed HTTP methods: ACL, BASELINE-CONTROL, BCOPY, BDELETE, BMOVE, BPROPFIND, BPROPPATCH, CHECKIN, CHECKOUT, CONNECT, COPY, DEBUG, DELETE, GET, HEAD, INDEX, LABEL, LOCK, MERGE, MKACTIVITY, MKCOL, MKWORKSPACE, MOVE, NOTIFY, OPTIONS, ORDERPATCH, PATCH, POLL, POST, PROPFIND, PROPPATCH, PUT, REPORT, RPC\_IN\_DATA, RPC\_OUT\_DATA, SEARCH, SUBSCRIBE, UNCHECKOUT, UNLOCK, UNSUBSCRIBE, UPDATE, VERSION-CONTROL, X-MS-ENUMATTS. The 'Plugin Details' sidebar lists: Severity: Info, ID: 43111, Version: 1.9, Type: remote, Family: Web Servers, Published: December 10, 2009, Modified: June 11, 2018. The 'Risk Information' section shows 'Risk Factor: None'. The bottom screenshot is for the 'HTTP Reverse Proxy Detection' plugin. The 'Description' states that this web server is reachable through a reverse HTTP proxy. The 'Output' shows: 'The GET method revealed those proxies on the way to this web server : HTTP/1.1 VENUS'. The 'Plugin Details' sidebar lists: Severity: Info, ID: 11040, Version: 1.31, Type: remote, Family: Web Servers, Published: July 2, 2002, Modified: August 10, 2018. The 'Risk Information' section shows 'Risk Factor: None'.

INFO

HTTP Server Type and Version

< >

Description

This plugin attempts to determine the type and the version of the remote web server.

Output

The remote web server type is :  
cloudflare

Port ▲

Hosts

80 / tcp / http\_proxy    www.juggystop.com

Plugin Details

Severity: Info

ID: 10107

Version: 1.132

Type: remote

Family: Web Servers

Published: January 4, 2000

Modified: September 13, 2018

Risk Information

Risk Factor: None

INFO

HyperText Transfer Protocol (HTTP) Redirect Information

< >

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Output

```
Request      : http://www.juggystop.com/
HTTP response : HTTP/1.1 301 Moved Permanently
Redirect to   : https://www.juggystop.com/
Redirect type  : 30x redirect

Note that Nessus did not receive a 200 OK response from the
last examined redirect.
```

Plugin Details

Severity: Info

ID: 91634

Version: \$Revision: 1.2 \$

Type: remote

Family: Web Servers

Published: June 16, 2016

Modified: October 12, 2017

Risk Information

Risk Factor: None

INFO

HyperText Transfer Protocol (HTTP) Information

< >

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Output

```
Response Code : HTTP/1.1 301 Moved Permanently
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :
Via: 1.1 VENUS
Connection: Keep-Alive ...
more...
```

Plugin Details

Severity: Info

ID: 24260

Version: \$Revision: 1.13 \$

Type: remote

Family: Web Servers

Published: January 30, 2007

Modified: November 13, 2017

Risk Information

Risk Factor: None

Figure 4: HTTP check

## (ii) CVE records of Cloudflare

The site is found to be running on CloudFlare; a global network designed to secure websites, APIs, and Internet applications connected to the Internet. A database search from the CVE lists shows that there is a total of 16 disclosed cybersecurity vulnerability associated with Cloudflare. The table documents a list of the CVE records and a description of its vulnerability.

---

CVE ID	Description of vulnerability
CVE-2022-2225	By using warp-cli subcommands (disable-ethernet, disable-wifi), it was possible for a user without admin privileges to bypass configured Zero Trust security policies (e.g. Secure Web Gateway policies) and features such as 'Lock WARP switch'.
CVE-2022-2147	Cloudflare Warp for Windows from version 2022.2.95.0 contained an unquoted service path which enables arbitrary code execution leading to privilege escalation. The fix was released in version 2022.3.186.0.
CVE-2022-2145	Cloudflare WARP client for Windows (up to v. 2022.5.309.0) allowed creation of mount points from its ProgramData folder. During installation of the WARP client, it was possible to escalate privileges and overwrite SYSTEM protected files.
CVE-2021-43800	Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git).

---

---

CVE-2021-3912	OctoRPKI tries to load the entire contents of a repository in memory, and in the case of a GZIP bomb, unzip it in memory, making it possible to create a repository that makes OctoRPKI run out of memory (and thus crash).
CVE-2021-3911	If the ROA that a repository returns contains too many bits for the IP address then OctoRPKI will crash.
CVE-2021-3910	OctoRPKI crashes when encountering a repository that returns an invalid ROA (just an encoded NUL (\0) character).
CVE-2021-3909	OctoRPKI does not limit the length of a connection, allowing for a slowloris DOS attack to take place which makes OctoRPKI wait forever. Specifically, the repository that OctoRPKI sends HTTP requests to will keep the connection open for a day before a response is returned, but does keep drip feeding new bytes to keep the connection alive.
CVE-2021-3908	OctoRPKI does not limit the depth of a certificate chain, allowing for a CA to create children in an ad-hoc fashion, thereby making tree traversal never end.
CVE-2021-3907	OctoRPKI does not escape a URI with a filename containing "..", this allows a repository to create a file, (ex. rsync://example.org/repo/../../etc/cron.daily/evil.roa), which would then be written to disk outside the base cache folder. This could allow for remote code execution on the host machine OctoRPKI is running on.
CVE-2021-3761	Any CA issuer in the RPKI can trick OctoRPKI prior to 1.3.0 into emitting an invalid VRP "MaxLength" value, causing RTR sessions to terminate. An attacker can use this to disable RPKI Origin Validation in a victim network (for example AS 13335 - Cloudflare) prior to launching a BGP hijack which during normal operations would be

---

---

rejected as "RPKI invalid". Additionally, in certain deployments RTR session flapping in and of itself also could cause BGP routing churn, causing availability issues.

CVE-2020-35152	Cloudflare WARP for Windows allows privilege escalation due to an unquoted service path. A malicious user or process running with non-administrative privileges can become an administrator by abusing the unquoted service path issue. Since version 1.2.2695.1, the vulnerability was fixed by adding quotes around the service's binary path. This issue affects Cloudflare WARP for Windows, versions prior to 1.2.2695.1.
----------------	--

CVE-2020-24356	`cloudflared` versions prior to 2020.8.1 contain a local privilege escalation vulnerability on Windows systems. When run on a Windows system, `cloudflared` searches for configuration files which could be abused by a malicious entity to execute commands as a privileged user. Version 2020.8.1 fixes this issue.
----------------	---

CVE-2020-15236	In Wiki.js before version 2.5.151, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit 084dcd69d1591586ee4752101e675d5f0ac6dcdc fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any directory traversal (e.g. `..` and `.`) sequences as well as invalid filesystem characters from the path. As a workaround, disable any storage module with local asset caching capabilities such as Local File System and Git.
----------------	---

---

CVE-2019-10842      Arbitrary code execution (via backdoor code) was discovered in bootstrap-sass 3.2.0.3, when downloaded from rubygems.org. An unauthenticated attacker can craft the `__cfduid` cookie value with base64 arbitrary code to be executed via `eval()`, which can be leveraged to execute arbitrary code on the target system. Note that there are three underscore characters in the cookie name. This is unrelated to the `_cfduid` cookie that is legitimately used by Cloudflare.

---

CVE-2017-7235      An issue was discovered in cloudflare-scrape 1.6.6 through 1.7.1. A malicious website owner could craft a page that executes arbitrary Python code against any cfscrape user who scrapes that website. This is fixed in 1.8.0.

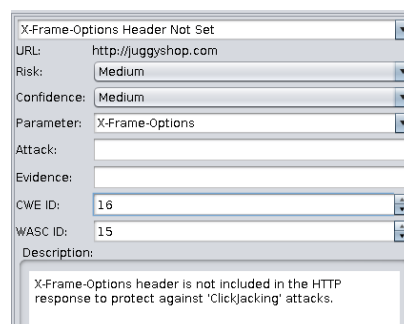
---

(iii)    OWASP Zed Attack Proxy (Zaproxy tool)

The website was run under the Zaproxy tool to determine any security vulnerabilities within the web application. This section below details the results of the scan.

- Application misconfiguration: X-Frame-Options Header Not Set

The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in `<frame>`, `<iframe>` or `<object>`. This feature is important in protecting against Clickjacking attacks.



*Figure 5: X-Frame Option vulnerability*

- Application misconfiguration: Cross-Domain JavaScript Source File Inclusion

The page includes one or more script files from a third-party domain. According to the CWE, when including third-party functionality, such as a web widget, library, or other source of functionality, the software must effectively trust that functionality. Without sufficient protection mechanisms, the functionality could be malicious in nature (either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source). An attacker could insert malicious functionality into the program by causing the program to download code that the attacker has placed into the untrusted control sphere, such as a malicious web site. The functionality might also contain its own weaknesses or grant access to additional functionality and state information that should be kept private to the base system, such as system state information, sensitive application data, or the DOM of a web application. This might lead to many different consequences depending on the included functionality, but some examples include injection of malware, information exposure by granting excessive privileges or permissions to the untrusted functionality, DOM-based XSS vulnerabilities, stealing user's cookies, or open redirect to malware

Cross-Domain JavaScript Source File Inclusion	
URL:	http://juggysshop.com
Risk:	Low
Confidence:	Medium
Parameter:	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Attack:	
Evidence:	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
CWE ID:	829
WASC ID:	15
Description:	The page includes one or more script files from a third-party domain.

*Figure 6: Third party script file vulnerability*



- 
- Information leakage: Incomplete or No Cache-control and Pragma HTTP Header Set

The web application does not use an appropriate caching policy that specifies the extent to which each web page and associated form fields should be cached. Browsers often store information in a client-side cache, which can leave behind sensitive information for other users to find and exploit, such as passwords or credit card numbers. The locations at most risk include public terminals, such as those in libraries and Internet cafes.

The screenshot shows a vulnerability scanner result for the issue 'Incomplete or No Cache-control and Pragma HTTP Header Set'. The URL is 'https://juggysshop.com/'. The risk is 'Low' and the confidence is 'Medium'. The parameter is 'Cache-Control'. The attack and evidence fields are empty. The CWE ID is '525' and the WASC ID is '13'. The description states: 'The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.'

Incomplete or No Cache-control and Pragma HTTP Header Set	
URL:	https://juggysshop.com/
Risk:	Low
Confidence:	Medium
Parameter:	Cache-Control
Attack:	
Evidence:	
CWE ID:	525
WASC ID:	13
Description:	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

*Figure 7: Cache control vulnerability*

### 3. Testing Narrative

#### Denial of Service Attack (DOS)

A DOS attack has the capability to render a computer/website unavailable to its intended user. Its main attack point is to flood the target with mindless requests until it is unable to process. An attack such as this is a particularly big inconvenience to an online commercial business such as Juggysshop, whereby it could block potential customers from accessing the site until the DOS attack is subdued. The potential financial loss to the company may be a critical point to consider when dealing with such attacks. To protect against this outcome, the website Juggysshop is firstly tested against the DOS attack to determine its efficiency in mitigating such attacks.

##### (i) Tools used

To perform the DOS attack, the Hammer tool was used.

```
Rocheston:~$ cd rcce
Rocheston:~/rcce$ cd hammer
Rocheston:~/rcce/hammer$ ./hammer.py
Hammer Dos Script v.1 http://www.canyalcin.com/
It is the end user's responsibility to obey all applicable laws.
It is just for server testing script. Your ip is visible.

usage : python3 hammer.py [-s] [-p] [-t]
-h : help
-s : server ip
-p : port default 80
-t : turbo default 135
Rocheston:~/rcce/hammer$ python3 hammer.py -s 104.21.8.41
```

Figure 8: DDoS attack methodology using Hammer

The outgoing streams were captured using the monitoring tool WireShark.

No.	Time	Source	Destination	Protocol	Length	Info
361825	471.9842506	10.61.50.40	157.240.10.35	TCP	54	55280 → 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0
361826	471.9845075	10.61.50.40	157.240.10.35	TLSv1	571	Client Hello
361827	471.9856687	157.240.10.35	10.61.50.40	TCP	60	443 → 55276 [ACK] Seq=3893 Ack=833 Win=65535 Len=0
361828	471.9102135	157.240.10.35	10.61.50.40	TCP	60	[TCP Retransmission] 443 → 55280 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1392
361829	471.9102240	10.61.50.40	157.240.10.35	TCP	54	[TCP Dup ACK 361825#1] 55280 → 443 [ACK] Seq=518 Ack=1 Win=29200 Len=0
361830	471.9239866	10.61.50.40	61.6.169.161	TCP	54	80 → 54260 [ACK] Seq=304414 Ack=38636 Win=108800 Len=0
361831	471.9458744	104.21.8.41	10.61.50.40	HTTP	512	HTTP/1.1 403 Forbidden (text/plain)
361832	471.9458919	10.61.50.40	104.21.8.41	TCP	54	32950 → 80 [RST] Seq=379 Win=0 Len=0
361833	471.9478960	104.21.8.41	10.61.50.40	HTTP	512	HTTP/1.1 403 Forbidden (text/plain)
361834	471.9479089	10.61.50.40	104.21.8.41	TCP	54	32936 → 80 [RST] Seq=352 Win=0 Len=0
361835	471.9492908	104.21.8.41	10.61.50.40	HTTP	512	HTTP/1.1 403 Forbidden (text/plain)
361836	471.9493012	10.61.50.40	104.21.8.41	TCP	54	32864 → 80 [RST] Seq=376 Win=0 Len=0
361837	471.9494540	104.21.8.41	10.61.50.40	HTTP	512	HTTP/1.1 403 Forbidden (text/plain)
361838	471.9494616	10.61.50.40	104.21.8.41	TCP	54	32970 → 80 [RST] Seq=379 Win=0 Len=0
361839	471.9651612	104.21.8.41	10.61.50.40	HTTP	512	HTTP/1.1 403 Forbidden (text/plain)
361840	471.9651747	10.61.50.40	104.21.8.41	TCP	54	32902 → 80 [RST] Seq=376 Win=0 Len=0
361841	472.0972048	10.61.50.40	61.6.169.161	HTTP	97	HTTP/1.1 200
361842	472.0988117	61.6.169.161	10.61.50.40	HTTP	1042	POST /tunnel?write:f6b34d70-22d8-488e-9c4b-5478df2386a1 HTTP/1.1 (application/x
361843	472.0994505	10.61.50.40	61.6.169.161	HTTP	279	HTTP/1.1 200
361844	472.1079881	10.61.50.40	157.240.10.35	TCP	571	[TCP Retransmission] 55280 → 443 [PSH, ACK] Seq=1 Ack=1 Win=29200 Len=517
361845	472.1136348	157.240.10.35	10.61.50.40	TCP	60	443 → 55280 [ACK] Seq=1 Ack=518 Win=65535 Len=0
361846	472.1157518	157.240.10.35	10.61.50.40	TLSv1.3	590	Server Hello, Change Cipher Spec
361847	472.1157793	10.61.50.40	157.240.10.35	TCP	54	55280 → 443 [ACK] Seq=518 Ack=537 Win=30016 Len=0

Figure 9: Packet analyzer from Wireshark

---



```
Stream Content
Host: 104.21.8.41
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
HTTP/1.1 403 Forbidden
Via: 1.1 VENU
Connection: Keep-Alive
Proxy-Connection: Keep-Alive
Content-Length: 16
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Date: Sun, 04 Sep 2022 13:45:36 GMT
Content-Type: text/plain; charset=UTF-8
Server: cloudflare
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
CF-RAY: 74572a9fffc39f85-SIN
error code: 1003
```

*Figure 10: Stream content of packets*

## *(ii) Targets affected*

The DOS attack targets the server of the website, pulverising several requests against the server until its limit. This will cause the server unable to entertain legitimate requests from real clients, rendering the server useless or making its request time very slow. From the Wireshark interface, we can see that the Hammer tool does its job by starting the false requests, however, it was stopped with an error message “HTTP/1.1 403 Forbidden”. According to the RFC 7231, the 403 (Forbidden) status code indicates that the server understood the request but refuses to authorize it. This error may be caused by unauthorized credentials; if authentication credentials were provided in the request, the server considers them insufficient to grant access. The process can be repeated with new or different credentials; however, a request might be forbidden for reasons unrelated to the credentials. From this, it is concluded that the server itself may be immune to DOS attack of this nature.

---

## Countermeasures

### (i) DDOS countermeasures

The use of Cloudflare as a server establishes secure connections to the global network and securely forward requests to the network. With this, there will be no hole in the firewall and all ports are ensured to be closed. Cloudflare uses Anycast, a network routing and addressing method which is able to route incoming connection requests across multiple data centres. When requests come into a single IP address associated with the Anycast network, the network distributes the data based on a prioritization methodology, which is optimized to reduce latency by selecting the data centre with the shortest distance from the requester. This helps in speed, redundancy, DDOS mitigation and load balancing. To further enhance speed, the HTTP/3 and TLS1.3 function in Cloudflare can be enabled to reduce latency, optimize performance and harden security.

### (ii) X-Frame-Options HTTP header risk countermeasures

Most modern web browsers support the X-Frame-Options HTTP header and can be set on all web pages returned by the site. If it is expected that the page to be framed only by pages on the server (e.g. it's part of a FRAMESET) then use SAMEORIGIN, otherwise it is not expected that the page to be framed, use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

### (iii) Cross-Domain JavaScript Source File Inclusion countermeasures

Ensure JavaScript source files are only loaded from trusted sources and can't be controlled by end users of the web application.

### (iv) Cache-control vulnerability countermeasures

Ensure that the cache control HTTP header is set with no-cache, no store, must revalidate and that the pragma HTTP header is set with no-cache.

---

(v) End user security

Devising an appropriate password policy for end users can safeguard against security breaches, especially if the website allows financial credentials to be stored within the website. An insufficient password policy greatly increases the risk of compromise in an environment. Informing users on password construction to avoid things like "L33t 5p34K" IE: replacing A's with 4;s and E's with 3's or using single dictionary words. Phrases and or multiple words are much harder to crack. The following guideline can be used to construct passwords that are up to standards:

- At least 12 alpha-numeric characters
- Uppercase/Lowercase
- At least 1 number
- At least 1 Special Character

---

## References

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=cloudflare>

<https://www.cloudflare.com/en-ca/>

<https://www.rfc-editor.org/rfc/rfc7231#section-6.5.3>

<https://cwe.mitre.org/data/definitions/829.html>

[https://cheatsheetseries.owasp.org/cheatsheets/Session Management Cheat Sheet.  
html#Web Content Caching](https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#Web_Content_Caching)

---

## Appendix A: FinalRecon Results

Version : 1.1.0

Date : 2022-08-02

Target : http://juggysshop.com

IP Address : 172.67.156.205

Start Time : 10:47:26 AM

End Time : 10:52:53 AM

Completion Time : 0:05:27.453732

#####

Headers

#####

Date : Tue, 02 Aug 2022 14:47:27 GMT

Content-Type : text/html

Transfer-Encoding : chunked

Connection : keep-alive

Last-Modified : Thu, 24 Feb 2022 23:53:30 GMT

Vary : Accept-Encoding

Access-Control-Allow-Origin : \*

CF-Cache-Status : DYNAMIC

Expect-CT : max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Report-To :  
{ "endpoints": [ { "url": "https://a.nel.cloudflare.com/report/v3?s=GXSldiHBk9K0I08Uv32kSfLh2ctu2pE7YCoWn572VBjHJYHqtEtUH6i0SyW47fnW2%2BNuonF998UQ4doJ8EFIZPpF4AL0C8IKgWlbqvXslCrSY%2B62JJJhgPBtul0pVQpn" } ], "group": "cf-nel", "max\_age": 604800 }

NEL : { "success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800 }

---

Server : cloudflare

CF-RAY : 73479bd9cd3a91ab-SIN

Content-Encoding : gzip

alt-svc : h3=":443"; ma=86400, h3-29=":443"; ma=86400

#####

SSL Certificate Information

#####

countryName : US

stateOrProvinceName : California

localityName : San Francisco

organizationName : Cloudflare, Inc.

commonName : Cloudflare Inc ECC CA-3

version : 3

serialNumber : 02A61C940B7F237CB8AEE38A753183A0

notBefore : Jun 19 00:00:00 2022 GMT

notAfter : Jun 19 23:59:59 2023 GMT

subjectAltName : (('DNS', 'sni.cloudflaressl.com'), ('DNS', '\*.juggyshop.com'), ('DNS', 'juggyshop.com'))

OCSP : ('http://ocsp.digicert.com',)

calssuers : ('http://cacerts.digicert.com/CloudflareIncECCCA-3.crt',)

crlDistributionPoints : ('http://crl3.digicert.com/CloudflareIncECCCA-3.crl',  
'http://crl4.digicert.com/CloudflareIncECCCA-3.crl')

#####

DNS Enumeration

#####

Dns

---



---

```
juggyshop.com.      300  IN  AAAA  2606:4700:3030::ac43:9ccd

juggyshop.com.      1800  IN  SOA   clark.ns.cloudflare.com. dns.cloudflare.com. 2281086073
10000 2400 604800 3600

juggyshop.com.      21600 IN  NS   clark.ns.cloudflare.com.

juggyshop.com.      21600 IN  NS   kristin.ns.cloudflare.com.

juggyshop.com.      3789  IN  HINFO 075246433834383200

juggyshop.com.      300  IN  AAAA  2606:4700:3031::6815:829

juggyshop.com.      300  IN  A     104.21.8.41

juggyshop.com.      300  IN  A     172.67.156.205
```

```
#####
```

#### Subdomain Enumeration

```
#####
```

Total Unique Sub Domains Found : 0

```
#####
```

#### Traceroute

```
#####
```

#### Result

```
=====
```

1	10.61.50.3	Unknown
2	192.168.61.20	Unknown
3	192.168.19.18	Unknown
4	219.93.16.129	Unknown
5	203.121.27.29	Unknown
6	10.55.100.124	Unknown
7	58.27.38.246	Unknown
8	223.28.43.54	Unknown

---

---

9	202.84.249.162	Unknown
10	202.84.224.190	i-93.istt04.telstraglobal.net
11	172.67.156.205	Unknown

Protocol : UDP

Port : 33434

Timeout : 1.0

#####

Port Scan

#####

80 : http

9418 : git

10000 : webmin

10082 : amandaidx

13722 : bpjava-msvc

13782 : bpcd

13783 : # Local services

135 : loc-srv

21 : ftp

554 : rtsp

#####

Crawler

#####

Total Unique Links Extracted : 85

Title : Juggyshop

Count ( Robots ) : 0

---

---

Count ( Sitemap ) : 0

Count ( CSS ) : 10

Count ( JS ) : 13

Count ( Links in JS ) : 8

Count ( Links in Sitemaps ) : 0

Count ( Internal ) : 0

Count ( External ) : 0

Count ( Images ) : 31

count ( Wayback Machine ) : 54

Count ( Total ) : 85

CSS

===

<http://juggyshop.com/assets/css/jquery.fancybox.min.css>

<http://juggyshop.com/assets/css/elegant.css>

[http://juggyshop.com/assets/css/custom\\_bootstrap.css](http://juggyshop.com/assets/css/custom_bootstrap.css)

<http://juggyshop.com/assets/css/scroll.css>

<http://juggyshop.com/assets/css/normalize.css>

<http://juggyshop.com/assets/css/animate.css>

<http://juggyshop.com/assets/css/style.css>

<http://juggyshop.com/assets/css/fontawesome.css>

<http://juggyshop.com/assets/css/slick.css>

<http://juggyshop.com/assets/css/icomoon.css>

Javascripts

=====

---

<http://juggysshop.com/assets/js/slick.min.js>

<http://juggysshop.com/assets/js/jquery.fancybox.js>

<http://juggysshop.com/assets/js/numscroller-1.0.js>

<http://juggysshop.com/assets/js/main.js>

<http://juggysshop.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js>

<http://juggysshop.com/assets/js/vanilla-tilt.min.js>

<http://juggysshop.com/assets/js/jquery-ui.min.js>

<http://juggysshop.com/assets/js/jquery.scrollUp.min.js>

<http://juggysshop.com/assets/js/jquery.zoom.min.js>

<https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js>

<http://juggysshop.com/assets/js/jquery.easing.js>

<http://juggysshop.com/assets/js/jquery.countdown.min.js>

<http://juggysshop.com/assets/js/parallax.js>

Links inside Javascripts

=====

[https://img.youtube.com/vi/\\$4/hqdefault.jpg](https://img.youtube.com/vi/$4/hqdefault.jpg)

[https://www.youtube.com/iframe\\_api](https://www.youtube.com/iframe_api)

<https://twitter.com/intent/tweet?url={{url}}&text={{descr}}>

<https://www.pinterest.com/pin/create/button/?url={{url}}&description={{descr}}&media={{media}}>

[https://www.youtube-nocookie.com/embed/\\$4](https://www.youtube-nocookie.com/embed/$4)

<https://www.facebook.com/sharer/sharer.php?u={{url}}>

<http://www.w3.org/2000/svg>

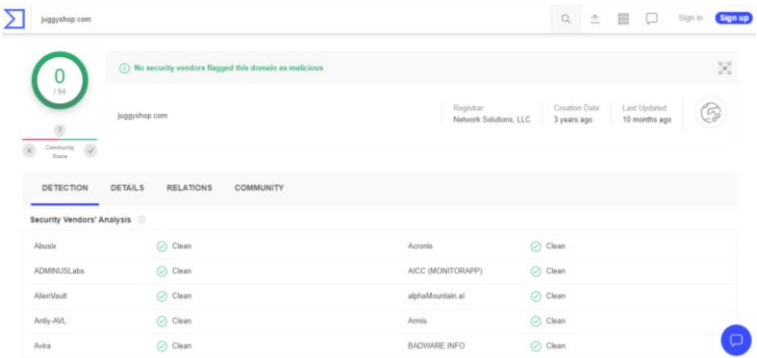
<https://player.vimeo.com/api/player.js>

# Appendix B: Sucuri Scan

## Website Malware & Security

- ✔ No malware detected by scan (Low Risk)
- ✔ No injected spam detected (Low Risk)
- ✔ No defacements detected (Low Risk)
- ✔ No internal server errors detected (Low Risk)

# Appendix C: Virustotal



# Appendix D: Nessus Scan

