

DATA BREACH IN CASHAPP

A REPORT

Submitted by
SAI CHARITESH
[RA2111030010171]

Under the Guidance of
Dr. D. Deepika
Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of
BACHELOR OF TECHNOLOGY
in

COMPUTER SCIENCE ENGINEERING
with specialization in CYBER SECURITY



SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603203

APRIL 2024



SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **“DATA BREACH IN CASHAPP”** is the bonafide work of **“S. SAI CHARITESH”** of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE

Dr. D. Deepika

Assistant Professor

Networking and Communications

SIGNATURE

Dr. Annapurani Panaiyappan K

Professor and Head

Networking and Communications

CASE STUDY ON “INSIDER THREAT AT YAHOO”

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and
Vulnerability Assessment

Year & Semester : III/VI

Report Title : DATA BREACH IN CASHAPP

Course Faculty : Dr. D. Deepika

Student Name : SAI CHARITESH[RA2111030010171]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
7	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

S. No	Title	Page. No
1	Introduction	1
2	Scope and Objective	2-4
3	About the tool and the application chosen	5-6
4	Tool working procedure	7-9
5	Steps of ethical hacking that you have done on your application using the chosen tool	10-11
6	Screenshots of the implementation	12-15
7	Conclusion	16
8	References	17

INTRODUCTION

In our interconnected digital era, financial transactions have undergone a remarkable transformation, with mobile payment platforms emerging as convenient alternatives to traditional banking methods. Among these, Cash App has garnered significant popularity, offering users a seamless experience for sending, receiving, and managing money. However, the convenience of such platforms comes hand in hand with inherent risks, chief among them being the specter of data breaches. Data breaches, the unauthorized access or exposure of sensitive information, pose a substantial threat to the security and privacy of users on any online platform, including Cash App. The repercussions of such breaches extend far beyond mere financial losses, encompassing the erosion of trust, regulatory scrutiny, and potential legal liabilities. Understanding the nuances of data breaches in Cash App is essential for users, regulators, and the company alike, as they navigate the increasingly complex landscape of digital finance.

This introduction sets the stage for a comprehensive exploration of data breaches in Cash App, delving into their causes, consequences, and the measures necessary to mitigate their impact. By shedding light on this critical issue, we aim to empower users with the knowledge needed to safeguard their financial transactions and privacy in an ever-evolving digital ecosystem.

SCOPE

- Cash App allows users to send money to friends, family, or anyone else with a Cash App account. This can be for splitting bills, paying back loans, or simply sending gifts.
- Many businesses, especially smaller ones, now accept Cash App as a form of payment. This can be useful for transactions where cash or cards are not practical. Cash App offers a feature that allows users to invest in stocks and Bitcoin directly through the app. It's a simple way for beginners to start investing.
- Cash App provides users with a debit card, known as the Cash Card, which can be used to make purchases anywhere that accepts Visa. Users can set up direct deposit to receive paychecks, government benefits, and tax returns directly into their Cash App account.
- Cash App occasionally offers discounts or cashback rewards, known as Boosts, for using the Cash Card at certain retailers or services. Cash App allows users to donate to charitable organizations directly through the app. Cash App allows users to send and receive money quickly and easily to friends, family, or anyone else with a Cash App account. This is particularly useful for splitting bills, paying rent, or reimbursing friends
- Cash App provides users with a free debit card, known as the Cash Card, which is linked to their Cash App account. The Cash Card can be used to make purchases at retail stores, online shops, or to withdraw cash from ATMs. Cash App offers a feature that allows users to invest in stocks and Bitcoin directly from the app. Users can buy, sell, and track their investments conveniently through Cash App's interface.
- Cash App offers a feature that allows users to invest in stocks and Bitcoin directly from the app. Users can buy, sell, and track their investments conveniently through Cash App's interface. In addition to Bitcoin investing, Cash App allows users to buy, sell, and transfer Bitcoin to other Cash App users. This adds another dimension to the platform's financial services.
- Overall, Cash App provides a convenient and versatile platform for various financial activities, from everyday transactions to investing and charitable giving. However, users should always be mindful of security measures and potential scams when using any financial app or service.

OBJECTIVE

Investigate the Insider Threat:

- Determine the nature and scope of the data breach, including the type of information compromised and the extent of the unauthorized access. Conduct forensic analysis and internal investigations to identify any employees or insiders who may have been involved in the breach.
- This may involve examining access logs, monitoring suspicious activities, and interviewing employees. Understand the motives behind insider involvement, whether it was for financial gain, personal reasons, or unintentional actions due to negligence or lack of training.

Assess the Impact on Data Security:

- Cash App deals with sensitive financial information, including bank account details, debit card information, and transaction history. Any compromise of this data could lead to financial losses for users and erode trust in the platform.
- Therefore, Cash App must implement robust encryption protocols and access controls to safeguard this data from unauthorized access or breaches. In addition to financial data, Cash App also collects personal information from users, such as names, addresses, and contact details.
- Protecting this PII is crucial to prevent identity theft, fraud, and other malicious activities. Despite preventive measures, security incidents may still occur. Cash App should have a robust incident response plan in place to detect, contain, and mitigate breaches promptly.

Enhance Insider Threat Detection and Prevention Mechanisms:

- Implement user behavior analytics to monitor and analyze employees' actions within the system. This includes tracking login attempts, access to sensitive data, and unusual activity patterns that may indicate insider threats.
- Enforce the principle of least privilege by granting employees only the access necessary to perform their job functions. Implement strong access controls, such as multi-factor authentication and role-based access controls, to limit unauthorized access to sensitive information.

TOOL DISCRIPTION

BURPSUITE is a popular cybersecurity tool used for web application security testing. It's developed by PortSwigger, a UK-based cybersecurity company. Burp Suite provides a comprehensive set of tools for performing various security testing tasks.

KeyFeatures:

Security: Ensure that Burp Suite is configured to communicate securely with the target web application. This often involves configuring Burp Suite to use HTTPS when communicating with the target server.

Forensics:

Burp Suite's proxy feature allows capturing and analyzing web traffic between the client and the server. In forensic investigations, this feature can be used to reconstruct the sequence of events leading up to a security incident.

Parental Control:

With Burp Suite acting as a proxy, you can monitor the websites and online activities accessed by the child in real-time. Burp Suite captures HTTP requests and responses, which can give insights into the websites visited, content accessed, and interactions made.

Personal Use:

Many cybersecurity enthusiasts and students use Burp Suite to learn about web application security. They may experiment with different features of Burp Suite, such as its proxy, scanner, intruder, and repeater, to understand common vulnerabilities like SQL injection, cross-site scripting (XSS), and more.

Advantages of Using BURPSUITE TOOL:

Burp Suite offers several advantages for security professionals, researchers, and developers:

1. **Comprehensive Web Security Testing:** Burp Suite provides a wide range of tools and functionalities for testing web applications' security comprehensively. It includes features like a web vulnerability scanner, proxy, spider, intruder, repeater, sequencer, decoder, comparer, and more, covering various aspects of web security testing.
2. **User-Friendly Interface:** Despite its powerful capabilities, Burp Suite maintains a user-friendly interface that makes it accessible to both beginners and experienced security professionals. Its intuitive design allows users to navigate through different modules and perform complex security assessments with ease.
3. **Active Community Support:** Burp Suite has a large and active community of security professionals and researchers who contribute to its development, share knowledge, and provide support. This community-driven approach ensures that users have access to resources, tutorials, and plugins to enhance their Burp Suite experience.

INSTALLATION

The installation process for Burp Suite can vary slightly depending on your operating system. Here's a general guide for installing Burp Suite:

Download Burp Suite: Go to the official website of PortSwigger, the company behind Burp Suite, and navigate to the download page. Choose the edition of Burp Suite you want to install (Community Edition or Professional Edition) and download the appropriate installer for your operating system (Windows, macOS, or Linux).

Run the Installer: Once the download is complete, locate the installer file on your computer and run it. This will launch the Burp Suite installer.

Follow Installation Instructions: Follow the on-screen instructions provided by the installer to complete the installation process. You may be prompted to specify installation settings such as the installation directory and any additional components you want to install.

Launch Burp Suite: After the installation is complete, you can launch Burp Suite from the installation directory or using the shortcut created on your desktop (if applicable).

Configure Proxy Settings (Optional): If you plan to use Burp Suite's web proxy functionality for intercepting and modifying HTTP/S traffic, you may need to configure your web browser to use Burp Suite as a proxy. This typically involves specifying the proxy settings in your browser's network settings.

Activate License (Professional Edition Only): If you've installed the Professional Edition of Burp Suite, you'll need to activate your license. Follow the instructions provided by PortSwigger to activate your license using the license key you received.

Update Burp Suite (Optional): It's a good idea to check for updates regularly to ensure you have the latest version of Burp Suite with the newest features and security fixes. Burp Suite includes an update checker that can be accessed from the Help menu.

IMPLEMENTATION

BURPSUITE on cashapp application:

Burp Suite can be used to identify and investigate potential data breaches in web applications by analyzing network traffic and identifying sensitive information being transmitted. Here's how Burp Suite might be used in the context of a data breach investigation:

1.Traffic Analysis: Burp Suite's proxy functionality allows you to intercept and analyze HTTP/S traffic between the client and server. During a data breach investigation, you can monitor network traffic to identify any suspicious or unauthorized data transmissions.

2.Sensitive Data Detection: Burp Suite can be configured to detect and alert on the presence of sensitive information in HTTP requests and responses. This includes personally identifiable information (PII) such as usernames, passwords, credit card numbers, social security numbers, and other confidential data.

3.Customized Rules and Alerts: You can create custom rules within Burp Suite to search for specific patterns or keywords indicative of sensitive data. Burp Suite can then trigger alerts or notifications when such data is detected, helping you quickly identify potential data breaches.

4.Session Tracking: Burp Suite's session management capabilities allow you to track user sessions and interactions with the web application. During a data breach investigation, you can analyze session data to identify any unusual or unauthorized activities that may indicate a breach.

5.Replay and Reconstruction: Burp Suite's repeater tool enables you to replay captured requests and responses, facilitating the reconstruction of data breach scenarios. By replaying suspicious requests and analyzing server responses, you can gain insights into how the breach occurred and what data may have been

compromised.

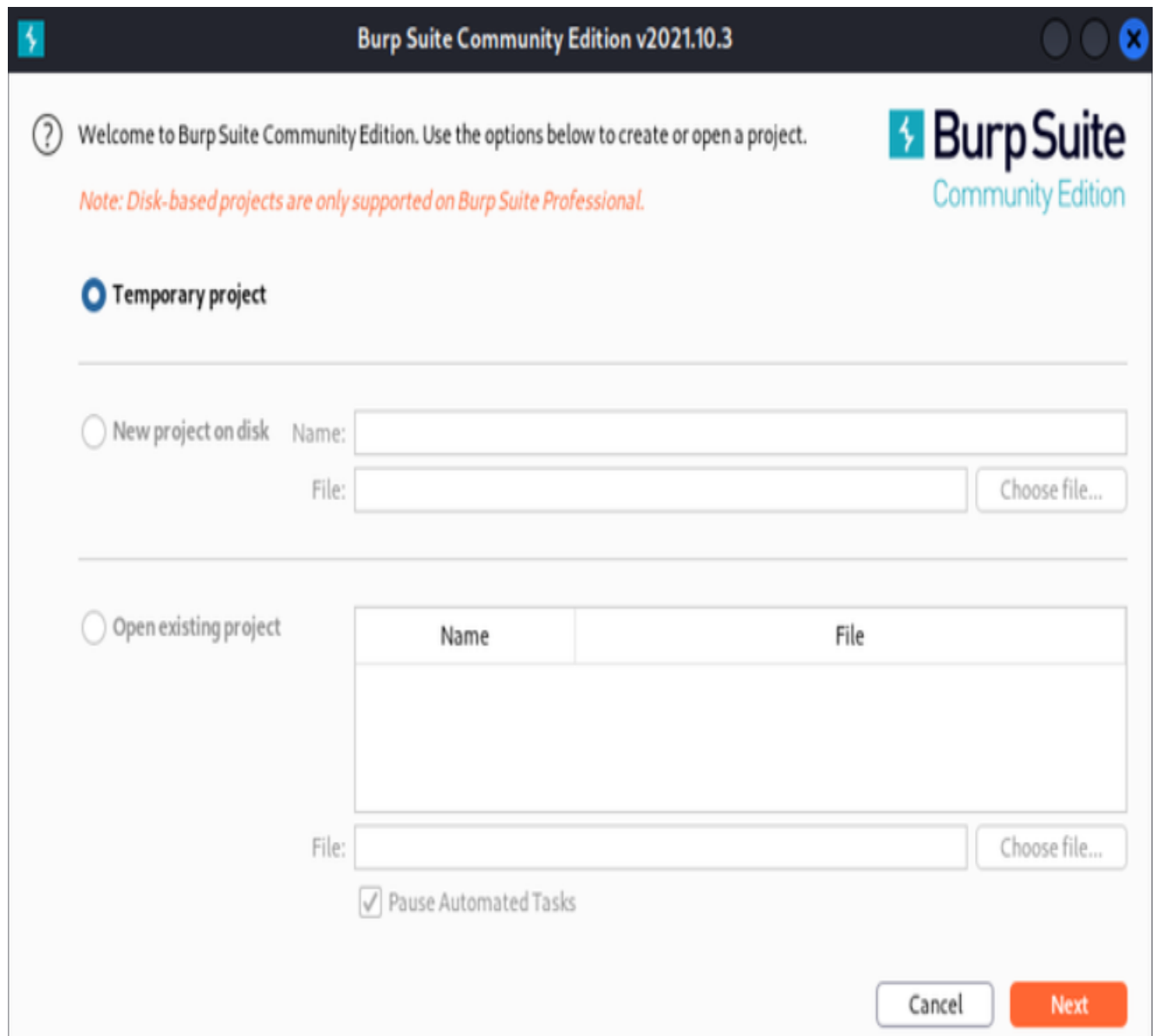
6.Vulnerability Assessment: In some cases, data breaches may occur due to security vulnerabilities in the web application. Burp Suite's web vulnerability scanner can help identify such vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR), which may have been exploited by attackers to gain unauthorized access to data.

7.Forensic Analysis: Burp Suite can assist in forensic analysis by providing detailed logs and reports of intercepted traffic, including timestamps, request/response headers, parameters, and payloads. This information can be invaluable in reconstructing the sequence of events leading up to the data breach and determining its scope and impact.

8.Documentation and Reporting: Burp Suite allows you to generate comprehensive reports documenting the findings of your investigation, including details of any detected data breaches, the methods used to identify them, and recommendations for remediation and mitigation.

Screenshots of the implementation

6.1: Selection of Project



The screenshot shows the 'Welcome to Burp Suite Community Edition' dialog box. It features a title bar with the application name and version. The main content area has a welcome message and a note about disk-based projects. There are three radio buttons for project selection: 'Temporary project' (selected), 'New project on disk', and 'Open existing project'. The 'New project on disk' option has input fields for 'Name' and 'File', with a 'Choose file...' button. The 'Open existing project' option has a table with 'Name' and 'File' columns, a 'File' input field, and a 'Choose file...' button. A 'Pause Automated Tasks' checkbox is also present. At the bottom right are 'Cancel' and 'Next' buttons.

Burp Suite Community Edition v2021.10.3

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

☒ Temporary project

☐ New project on disk

Name:

File:

☐ Open existing project

Name	File
------	------

File:

☒ Pause Automated Tasks

6.2: Configuring Proxy Settings

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Tasks

Filter Running Paused Finished

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing: ☒

3. Passive scans

Audit checks - passive

Audit finished.

Event log

Filter Critical Error Info Debug

Time	Type	Source
14:14:35 4 Apr 2021	Error	Proxy
14:14:32 4 Apr 2021	Error	Proxy
14:14:32 4 Apr 2021	Error	Proxy
14:14:31 4 Apr 2021	Error	Proxy
14:14:28 4 Apr 2021	Error	Proxy
14:14:24 4 Apr 2021	Error	Proxy
14:14:22 4 Apr 2021	Error	Proxy

New scan

Scan details

Scan configuration

Application login

Resource pool

Scan Type

☒ Crawl and audit

☐ Crawl

URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will i

https://hackthissite.org/

Protocol settings

☒ Scan using HTTP & HTTPS ☐ Scan using my specified protocols

> Detailed scope configuration

6.3: Finding the Required Data:

The screenshot displays the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar shows various tools like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, and User options. The HTTP history tab is active, showing a list of requests. The third request is highlighted, showing a GET request to a JavaScript file. The bottom pane shows the raw request and response details.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Size
1	https://www.comparitech.com	GET	/			200	224011	HTML		Comparitech - Tech ...		✓	95.168.178.100		22:34:43 6 ...	80
2	http://www.gitatic.com	GET	/generate_204			204	102						142.250.179.227		22:35:12 6 ...	80
3	https://www.comparitech.com	GET	/6uK9szCotqRV.js?ts=58403		✓	200	354	script	js			✓	95.168.178.100		22:59:52 6 ...	80
4	https://pro.ip-api.com	GET	/json/?key=koxg594M2RrKa3r		✓	200	476	JSON				✓	208.95.112.2		22:59:52 6 ...	80
5	https://www.googletagm...	GET	/gtm.js?id=GTM-TX6HUV		✓	200	151907	script	js			✓	142.250.187.200		22:59:52 6 ...	80
12	https://cdn.comparitech.c...	GET	/wp-content/plugins/autoptimi...		✓	200	10106	script	js			✓	95.168.178.100		22:59:53 6 ...	80
13	https://cdn.comparitech.c...	GET	/wp-includes/js/wp-embed.min...		✓	200	1798	script	js			✓	95.168.178.100		22:59:53 6 ...	80
41	https://www.google-anal...	GET	/analytics.js			200	50008	script	js			✓	172.217.169.14		22:59:54 6 ...	80
42	https://unpkg.com	GET	/web-vitals@0.2.2/dist/web-vital...			200	4104	script	js			✓	104.16.122.175		22:59:54 6 ...	80
43	https://www.google-anal...	POST	/j/collect?v=1&y=js&a=85544...		✓	200	647	text				✓	172.217.169.14		22:59:55 6 ...	80
44	https://stats.d.doubleclick...	POST	/j/collect?t=dc&aid=1&r=3&y...		✓	200	720	text				✓	66.102.1.156		22:59:55 6 ...	80

Request

```
1 GET /6uK9szCotqRV.js?ts=58403 HTTP/2
2 Host: www.comparitech.com
3 Cookie: _ga=GAI.2.1651019085.1625603398; _gid=GAI.2.389739200.1625603398
4 Sec-Ch-Ua: "Chromium";v="91", " Not:A Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
7 Accept: */*
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Dest: script
11 Referer: https://www.comparitech.com/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Connection: close
```

Response

```
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Tue, 06 Jul 2021 21:59:52 GMT
4 Content-Type: application/javascript
5 X-Request-Id: a0a0379f566a5b14aef9c3449571bf66
6 X-Presslabs-Stats: desktop
7 Vary: Accept-Encoding
8 Expires: Thu, 01 Jan 1970 00:00:01 GMT
9 Cache-Control: no-cache
10
11 // this beacon is used by Presslabs for metric computations on v
12
```

INSPECTOR

- Query Parameters (1)
- Request Cookies (2)
- Request Headers (13)
- Response Headers (8)

6.4: Extraction of Data:

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Showing all items

http://www.google.com

- /
- advanced_search
- client_204
- history
- images
- imghp
- intl
- language_tools
- preferences
- search
 - hl=en&gbv=1&ie=UTF-8&q=bipolar+test&
 - hl=en&gbv=1&ie=UTF-8&q=burp+suite&s
 - hl=en&gbv=1&ie=UTF-8&q=depression+t
 - hl=en&gbv=1&ie=UTF-8&q=fun+test&sa=
 - hl=en&gbv=1&ie=UTF-8&q=internet+spee
 - hl=en&gbv=1&ie=UTF-8&q=kali+linux+tu
 - hl=en&gbv=1&ie=UTF-8&q=learn+pentest
 - hl=en&gbv=1&ie=UTF-8&q=metasploit&s
 - hl=en&gbv=1&ie=UTF-8&q=pen+testing&
 - hl=en&gbv=1&ie=UTF-8&q=personality+t
 - hl=en&gbv=1&ie=UTF-8&q=phishing+fre
 - hl=en&gbv=1&ie=UTF-8&q=related:https:
 - hl=en&gbv=1&ie=UTF-8&q=related:https:

Contents Issues

Host	Method	URL	Params	Stat
http://www.google.c...	GET	/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...	✓	200
http://www.google.c...	GET	/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...	✓	200
http://www.google.c...	GET	/xjs/_/js/k=xjs.hp.en_US.JrX4RoZaeBk.O/m=sb_he,d/r...		200
http://www.google.c...	GET	/client_204?&atyp=i&biw=1649&bih=742&ei=nzvhV9iy...	✓	204
http://www.google.c...	GET	/advanced_search		
http://www.google.c...	GET	/advanced_search?hl=en&authuser=0	✓	
http://www.google.c...	GET	/advanced_search?q=pentestgeek&hl=en&gbv=1&ie=U...	✓	

Request Response

Raw Params Headers Hex

GET
/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgeek&gs_l=heirloom-serp.3..0j0i30.56132.57:
heirloom-serp..1.10.373.28pXafQweKk HTTP/1.1
Host: www.google.com
User-Agent: SNCAppSec2016
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
DNT: 1
Referer: http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=&q=test&gbv=1&oq=t
.26166.0.26302.4.4.0.0.0.127.253.2j1.3.0...0...lac.1.34.heirloom-hp..2.2.126.3rCfcg
Cookie:

CONCLUSION

In the event of a data breach, the immediate focus would be on mitigating the damage, securing affected accounts, and investigating the cause of the breach. Cash App would likely need to notify affected users, regulators, and possibly law enforcement agencies, depending on the severity and scope of the breach. This would involve providing details about the breach, steps taken to address it, and any measures users can take to protect themselves. Overall, a data breach on Cash App would be a serious matter with far-reaching implications. It underscores the importance of robust cybersecurity measures, proactive risk management, and effective incident response capabilities for financial service providers like Cash App.

REFERENCES

<https://www.geeksforgeeks.org/what-is-burp-suite/>

[https://portswigger.net/burp/releases/professional-community-](https://portswigger.net/burp/releases/professional-community-2023-6-2)

[2023-6-2](https://portswigger.net/burp/releases/professional-community-2023-6-2)