Shihani Tharuka | Web Security | October 15, 2020

Bug Report

Snapchat



* Abstract
* Introduction

1. Domain
   1. Sub Domains
2. Security Policy (Copied from Original Source)
3. Summary of Findings

3.1. Nikto

3.1.1. Found Bug – www.bitmoji.com

3.2. Wapiti

3.3. Whatweb

4. Attacks (Previous Versions)

4.1. Network Attacks

4.1.1. Web Application

4.1.2. Mobile Application

1. Conclusion
2. Acknowledgement
3. References

**Abstract**

Snapchat is a popular social media application that allows users to share photos and videos for a limited time only.

As such, I have searched previous web-based attacks on Snapchat's web and mobile applications, as well as their third - party integration.

Mainly, I scanned web domain and its subdomains. Using web hacking tools, and SSL bypass mechanisms.

I have also discovered a bug from ‘www.bitmoji.com’ subdomain in snapchat.

After auditing many, finally I found a bug.

|  |  |
| --- | --- |
| Domain | www.snapchat.com |

**Introduction**

Snapchat is a popular multimedia messaging mobile application that allows instant photo and video messaging. The feature that differentiates Snapchat from Facebook Messenger, Viber, WhatsApp, and other messaging applications is the temporary nature of the recorded messages. The photos or videos of up to 10 seconds sent to Snapchat friends are automatically deleted after they are received and viewed.

Due to its fun use, the popularity of Snapchat is growing at a rapid pace among the younger generation of app consumers. Almost half of Snapchat users (45%) are in the 18-24 age group. More than one-third of U.S. teens (16-19) and more than half of Irish youngsters have installed and use Snapchat for daily communication with their friends.

However, from the beginning of its development in 2011, the app has gone through major cybersecurity challenges. In the end of 2013, Gibson Security published and later updated Snapchat Security Disclosure that contained details of the security vulnerabilities in Snapchat’s architecture. The disclosure stressed that the indicated vulnerabilities could lead to a data breach.

A few months later, personal credentials of 4.6 million U.S. Snapchat users, such as usernames and phone numbers, were made public on the Internet. *The responsibility for this incident was taken by the website SnapchatDB.info.*

This attack was claimed to be a response to the previously identified weaknesses in the app’s security.

Finally, in 2014, the U.S. Federal Trade Commission announced a suit against the app that included six complaints regarding Snapchat’s data security and privacy issues. The app was accused of misrepresenting its privacy policies and deceiving about its use of service, data collection, and security measures. In the end of 2014, the final order settling charges against Snapchat were approved. After the suit, Snapchat made an agreement with the Federal Trade Commission and took reasonable measures for improving app’s data security.

1. Domain

A domain name is the address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses. Domain names serve to identify Internet resources, such as computers, networks, and services, with a text-based label that is easier to memorize than the numerical addresses used in the Internet protocols. A domain name may represent entire collections of such resources or individual instances.

[*www.snapchat.com*](http://www.snapchat.com)

*Icon

Description automatically generated*

WHOIS is a database containing contact and registration information for domain names. By searching it you can discover a number of things about the domain's ownership and registration. For example,

***www.snapchat.com***

*Logo, company name

Description automatically generated*

|  |  |
| --- | --- |
|  |  |
| Domain: | snapchat.com |
| Registrar: | MarkMonitor Inc. |
| Registered On: | 2012-02-28 |
| Expires On: | 2026-02-28 |
| Status: | clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited |
| Name Servers: | ns-1468.awsdns-55.org ns-1892.awsdns-44.co.uk ns-220.awsdns-27.com ns-530.awsdns-02.net |

### Raw Whois Data

Domain Name: snapchat.com

Registry Domain ID: 1704543145\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2016-03-16T09:19:37-0700

Creation Date: 2012-02-28T11:29:26-0800

Registrar Registration Expiration Date: 2026-02-28T11:29:26-0800

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: email@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895770

Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)

Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)

Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)

Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)

Registry Registrant ID:

Registrant Name: Domain Administrator

Registrant Organization: DNStination Inc.

Registrant Street: 3450 Sacramento Street, Suite 405

Registrant City: San Francisco

Registrant State/Province: CA

Registrant Postal Code: 94118

Registrant Country: US

Registrant Phone: +1.4155319335

Registrant Phone Ext:

Registrant Fax: +1.4155319336

Registrant Fax Ext:

Registrant Email: email@dnstinations.com

Registry Admin ID:

Admin Name: Domain Administrator

Admin Organization: DNStination Inc.

Admin Street: 3450 Sacramento Street, Suite 405

Admin City: San Francisco

Admin State/Province: CA

Admin Postal Code: 94118

Admin Country: US

Admin Phone: +1.4155319335

Admin Phone Ext:

Admin Fax: +1.4155319336

Admin Fax Ext:

Admin Email: email@dnstinations.com

Registry Tech ID:

Tech Name: Domain Administrator

Tech Organization: DNStination Inc.

Tech Street: 3450 Sacramento Street, Suite 405

Tech City: San Francisco

Tech State/Province: CA

Tech Postal Code: 94118

Tech Country: US

Tech Phone: +1.4155319335

Tech Phone Ext:

Tech Fax: +1.4155319336

Tech Fax Ext:

Tech Email: email@dnstinations.com

Name Server: ns-530.awsdns-02.net

Name Server: ns-1892.awsdns-44.co.uk

Name Server: ns-1468.awsdns-55.org

Name Server: ns-220.awsdns-27.com

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2020-10-19T15:46:38-0700 <<<

* 1. Sub Domains

Subdomains are created to organize and navigate to different sections of your website. You can create multiple subdomains or child domains on your main domain. In this example, 'support' is the subdomain, 'snapchat' is the primary domain and '.com' is the top-level domain.

A subdomain is, as the name would suggest, an additional section of your main domain name. You create subdomains to help organize and navigate to different sections of your main website. Within your main domain, you can have as many subdomains as necessary to get to all the different pages of your website.

Each domain name can have up to 500 subdomains. You can also add multiple levels of subdomains, such as info.blog.snapchat.com. A subdomain can be up to 255 characters long, but if you have multiple levels in your subdomain, each level can only be 63 characters long.

These are the subdomains and hosting providers in “*www.snapchat.com*”

|  |  |
| --- | --- |
| Subdomains | Hosting Provider |
| [support.lensstudio.snapchat.com](https://securitytrails.com/domain/support.lensstudio.snapchat.com/dns) | Cloudflare, Inc. |
| [accounts.snapchat.com](https://securitytrails.com/domain/accounts.snapchat.com/dns) | Google LLC |
| [support.snapchat.com](https://securitytrails.com/domain/support.snapchat.com/dns) | Google LLC |
| [snapcamera.snapchat.com](https://securitytrails.com/domain/snapcamera.snapchat.com/dns) | Google LLC |
| [blog.snapchat.com](https://securitytrails.com/domain/blog.snapchat.com/dns) | ‐ |
| [forbusiness.snapchat.com](https://securitytrails.com/domain/forbusiness.snapchat.com/dns) | Google LLC |
| [kit.snapchat.com](https://securitytrails.com/domain/kit.snapchat.com/dns) | Google LLC |
| [create.snapchat.com](https://securitytrails.com/domain/create.snapchat.com/dns) | Google LLC |
| [play.snapchat.com](https://securitytrails.com/domain/play.snapchat.com/dns) | Google LLC |
| [geofilters.snapchat.com](https://securitytrails.com/domain/geofilters.snapchat.com/dns) | Google LLC |
| [snaporiginals.snapchat.com](https://securitytrails.com/domain/snaporiginals.snapchat.com/dns) | Google LLC |
| [story.snapchat.com](https://securitytrails.com/domain/story.snapchat.com/dns) | Amazon.com, Inc. |
| [go.snapchat.com](https://securitytrails.com/domain/go.snapchat.com/dns) | Google LLC |
| [whatis.snapchat.com](https://securitytrails.com/domain/whatis.snapchat.com/dns) | Google LLC |
| [ads.snapchat.com](https://securitytrails.com/domain/ads.snapchat.com/dns) | Google LLC |
| [snappublisher.snapchat.com](https://securitytrails.com/domain/snappublisher.snapchat.com/dns) | Google LLC |
| [docs.snapchat.com](https://securitytrails.com/domain/docs.snapchat.com/dns) | Google LLC |
| [app.snapchat.com](https://securitytrails.com/domain/app.snapchat.com/dns) | Google LLC |
| [iosbeta.snapchat.com](https://securitytrails.com/domain/iosbeta.snapchat.com/dns) | Amazon.com, Inc. |
| [business.snapchat.com](https://securitytrails.com/domain/business.snapchat.com/dns) | Google LLC |
| [tr.snapchat.com](https://securitytrails.com/domain/tr.snapchat.com/dns) | Google LLC |
| [auth.snapchat.com](https://securitytrails.com/domain/auth.snapchat.com/dns) | Google LLC |
| [intg.snapchat.com](https://securitytrails.com/domain/intg.snapchat.com/dns) | Amazon.com, Inc. |
| [chat-gateway336-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway336-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway363-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway363-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway033-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway033-prod.chat.snapchat.com/dns) | ‐ |
| [us-west1-gcp.api.snapchat.com](https://securitytrails.com/domain/us-west1-gcp.api.snapchat.com/dns) | Google LLC |
| [bitmoji.api.snapchat.com](https://securitytrails.com/domain/bitmoji.api.snapchat.com/dns) | Amazon.com, Inc. |
| [antivirus-testing.snappublisher.snapchat.com](https://securitytrails.com/domain/antivirus-testing.snappublisher.snapchat.com/dns) | Google LLC |
| [chat-gateway287-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway287-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway257-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway257-prod.chat.snapchat.com/dns) | ‐ |
| [app-analyticsv2.snapchat.com](https://securitytrails.com/domain/app-analyticsv2.snapchat.com/dns) | ‐ |
| [chat-gateway005-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway005-prod.chat.snapchat.com/dns) | ‐ |
| [staging-gcp.api.snapchat.com](https://securitytrails.com/domain/staging-gcp.api.snapchat.com/dns) | Google LLC |
| [perception.snapchat.com](https://securitytrails.com/domain/perception.snapchat.com/dns) | Google LLC |
| [chat-gateway066-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway066-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway230-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway230-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway242-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway242-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway172-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway172-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway355-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway355-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway300-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway300-prod.chat.snapchat.com/dns) | ‐ |
| [gcp-api.sc-gw-dev.snapchat.com](https://securitytrails.com/domain/gcp-api.sc-gw-dev.snapchat.com/dns) | Google LLC |
| [snapchat-compat-discover-us-east-1.snapchat.com](https://securitytrails.com/domain/snapchat-compat-discover-us-east-1.snapchat.com/dns) | Amazon.com, Inc. |
| [18.antivirus.snappublisher.snapchat.com](https://securitytrails.com/domain/18.antivirus.snappublisher.snapchat.com/dns) | Google LLC |
| [chat-gateway117-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway117-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway245-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway245-prod.chat.snapchat.com/dns) | ‐ |
| [chat-gateway116-prod.chat.snapchat.com](https://securitytrails.com/domain/chat-gateway116-prod.chat.snapchat.com/dns) | ‐ |
| [mail2.support.snapchat.com](https://securitytrails.com/domain/mail2.support.snapchat.com/dns) | Google LLC |
| [perception-dev.snapchat.com](https://securitytrails.com/domain/perception-dev.snapchat.com/dns) | Google LLC |

1. Security Policy

*“When you use these services, you’ll share some information with us. So, we want to be upfront about the information we collect, how we use it, whom we share it with, and the controls we give you to access, update, and delete your information.”*

“

## **Information We Collect**

There are three basic categories of information we collect:

* **Information you provide.**
* **Information we get when you use our services.**
* **Information we get from third parties.**

Here’s a little more detail on each of these categories.

### **Information You Provide**

When you interact with our services, we collect information that you provide to us. For example, most of our services require you to set up a Snapchat account, so we need to collect a few important details about you, such as your name, username, password, email address, phone number, and date of birth. We may also ask you to provide us with some additional information that will be publicly visible on our services, such as a profile picture or Bitmoji avatar. Other services, such as commerce products, may require you to provide us with a debit or credit card number and its associated account information.

Of course, you’ll also provide us whatever information you send through our services, such as Snaps and Chats. Keep in mind that the users who view your Snaps, Chats, and any other content can always save that content or copy it outside the app. So, the same common sense that applies to the internet at large applies to Snapchat as well: Don’t send messages or share content that you wouldn’t want someone to save or share.

When you contact customer support or communicate with us in any other way, we’ll collect whatever information you volunteer or that we need to resolve your question.

### **Information We Get When You Use Our Services**

When you use our services, we collect information about which of those services you’ve used and how you’ve used them. We might know, for instance, that you watched a particular Story, saw a specific ad for a certain period of time, and sent a few Snaps. Here’s a fuller explanation of the types of information we collect when you use our services:

* **Usage Information.** We collect information about your activity through our services. For example, we may collect information about:
  + how you interact with our services, such as which filters you view or apply to Snaps, which Stories you watch on Discover, whether you are using Spectacles, or which search queries you submit.
  + how you communicate with other Snap chatters, such as their names, the time and date of your communications, the number of messages you exchange with your friends, which friends you exchange messages with the most, and your interactions with messages (such as when you open a message or capture a screenshot).
* **Content Information.** We collect content you create on our services, such as custom stickers, and information about the content you create or provide, such as if the recipient has viewed the content and the metadata that is provided with the content.
* **Device Information.** We collect information from and about the devices you use. For example, we collect:
  + information about your hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone;
  + information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether you have headphones connected; and
  + information about your wireless and mobile network connections, such as mobile phone number, service provider, IP address, and signal strength.
* **Device Phonebook.** Because Snapchat is all about communicating with friends, we may—with your permission—collect information from your device’s phonebook.
* **Camera and Photos.** Many of our services require us to collect images and other information from your device’s camera and photos. For example, you won’t be able to send Snaps or upload photos from your camera roll unless we can access your camera or photos.
* **Location Information.** When you use our services we may collect information about your location. With your permission, we may also collect information about your precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses.
* **Information Collected by Cookies and Other Technologies.** Like most online services and mobile applications, we may use cookies and other technologies, such as web beacons, web storage, and unique advertising identifiers, to collect information about your activity, browser, and device. We may also use these technologies to collect information when you interact with services, we offer through one of our partners, such as advertising and commerce features. For example, we may use information collected on other websites to show you more relevant ads. Most web browsers are set to accept cookies by default. If you prefer, you can usually remove or reject browser cookies through the settings on your browser or device. Keep in mind, though, that removing or rejecting cookies could affect the availability and functionality of our services. To learn more about how we and our partners use cookies on our services and your choices, please check out our [Cookie Policy](https://www.snap.com/en-US/cookie-policy/).
* **Log Information.** We also collect log information when you use our website, such as:
  + details about how you have used our services.
  + device information, such as your web browser type and language.
  + access times.
  + pages viewed.
  + IP address.
  + identifiers associated with cookies or other technologies that may uniquely identify your device or browser; and
  + pages you visited before or after navigating to our website.

### **Information We Collect from Third Parties**

We may collect information about you from other users, our [affiliates](https://support.snapchat.com/a/snap-affiliates), and third parties. Here are a few examples:

* If you link your Snapchat account to another service (like Bitmoji or a third-party app), we may receive information from the other service, like how you use that service.
* Advertisers, app developers, publishers, and other third parties may share information with us as well. We may use this information, among other ways, to help target or measure the performance of ads. You can learn more about our use of this kind of third-party data in our [Support Center](https://support.snapchat.com/a/advertising-preferences).
* If another user uploads their contact list, we may combine information from that user’s contact list with other information we have collected about you.

## **How We Use Information**

What do we do with the information we collect? For the detailed answer, go [here](https://www.snap.com/privacy/your-information). The short answer is: Provide you with an amazing set of products and services that we relentlessly improve. Here are the ways we do that:

* develop, operate, improve, deliver, maintain, and protect our products and services.
* send you communications, including by email. For example, we may use email to respond to support inquiries or to share information about our products, services, and promotional offers that we think may interest you.
* monitor and analyze trends and usage.
* [personalize our services](https://www.snap.com/privacy/privacy-by-product#personalization) by, among other things, suggesting friends, profile information, or Bitmoji stickers, or customizing the content we show you, including ads.
* contextualize your experience by, among other things, tagging your Memories content using your precise location information (if, of course, you have given us permission to collect that information) and applying other labels based on the content.
* provide and improve our advertising services, ad targeting, and ad measurement, including by your precise location information (again, if you’ve given us permission to collect that information), both on and off our services.
* enhance the safety and security of our products and services.
* verify your identity and prevent fraud or other unauthorized or illegal activity.
* use information we have collected from cookies and other technology to enhance our services and your experience with them.
* enforce our Terms of Service and other usage policies and comply with legal requirements.

We may also use information from Apple’s TrueDepth camera to improve the quality of Lenses. Information from the TrueDepth camera is used in real time—we do not store this information on our servers or share it with third parties.

## **How We Share Information**

We may share information about you in the following ways:

* **With other Snap chatters.** We may share the following information with other Snap chatters:
  + information about you, such as your username, name, and Bitmoji.
  + information about how you have interacted with our services, such as your Snapchat “score,” the names of Snap chatters you are friends with, and other information that will help Snap chatters understand your connections with others using our services. For example, because it may not be clear whether a new friend request comes from someone you actually know, we may share whether you and the requestor have Snapchat friends in common.
  + any additional information you have directed us to share. For example, Snap will share your information when you connect your Snapchat account to a third-party app, and if you share information or content from Snapchat to the third-party app.
  + content you post or send. How widely your content is shared depends on your personal settings and the type of service you are using. For example, a Snap may be sent to just a single friend you select, but your My Story content may be seen by any Snap chatter whom you allow to see your My Story.
* **With all Snap chatters, our business partners, and the general public.** We may share the following information with all Snap chatters as well as with our business partners and the general public:
  + public information like your name, username, Snap code and profile pictures.
  + Story submissions that are set to be viewable by Everyone and any content that you submit to an inherently public service, like Our Story and other crowd-sourced services. This content may be viewed and shared by the public at large both on and off our services, including through search results, on websites, in apps, and in online and offline broadcasts.
* **With third parties.** We may share information about you with service providers who perform services on our behalf, including to measure and optimize the performance of ads and deliver more relevant ads, including on third-party websites and apps.
  + We may share information about you with business partners that provide services and functionality on our services.
  + We may share information about you, such as device and usage information, to help us and others prevent fraud.
  + We may share information about you for legal, safety, and security reasons. We may share information about you if we reasonably believe that disclosing the information is needed to:
    - comply with any valid legal process, governmental request, or applicable law, rule, or regulation.
    - investigate, remedy, or enforce potential Terms of Service violations.
    - protect the rights, property, or safety of us, our users, or others.
    - detect and resolve any fraud or security concerns.
  + We may share information about you as part of a merger or acquisition. If Snap Inc. gets involved in a merger, asset sale, financing, liquidation or bankruptcy, or acquisition of all or some portion of our business to another company, we may share your information with that company before and after the transaction closes.

We may also share with third parties that provide services to us or perform business purposes for us aggregated, non-personally identifiable, or de-identified information.

## **Third-Party Content and Integrations**

Our services may contain third-party content and integrations. Examples include third-party integrations in camera search, third-party games in Chat, and third-party Snap Kit integrations. Through these integrations, you may be providing information to the third party as well as to Snap. We are not responsible for how those third parties collect or use your information. As always, we encourage you to review the privacy policies of every third-party service that you visit or use, including those third parties you interact with through our services.

## **How Long We Keep Your Information**

Snapchat lets you capture what it’s like to live in the moment. On our end, that means most messages—like Snaps and Chats—sent in Snapchat will be automatically deleted by default from our servers after we detect they’ve been opened by all recipients or have expired. Other content, like Story posts, are stored for longer.

We store other information for longer periods of time. For example:

* We store your basic account information—like your name, phone number, and email address—and list of friends until you ask us to delete them.
* We store location information for different lengths of time based on how precise it is and which services you use. For example, if you use the Map, we store information about your favorite places for up to 40 days so we can personalize and improve your experience. If location information is associated with a Snap—like those saved to Memories or posted to Our Story—we’ll retain that location as long as we store the Snap.
* We’re constantly collecting and updating information about the things you might like and dislike, so we can provide you with more relevant content and advertisements.
* If you ever decide to stop using Snapchat, you can just [ask us to delete your account](https://support.snapchat.com/a/delete-my-account1). We will also delete most of the information we’ve collected about you after you’ve been inactive for a while—but don’t worry, we’ll try to contact you first!

Keep in mind that, while our systems are designed to carry out our deletion practices automatically, we cannot promise that deletion will occur within a specific timeframe. There may be legal requirements to store your data and we may need to suspend those deletion practices if we receive valid legal process asking us to preserve content, if we receive reports of abuse or other Terms of Service violations, or if your account or content created by you is flagged by our automated systems for abuse or other Terms of Service violations. Finally, we may also retain certain information in backup for a limited period of time or as required by law.

## **Control Over Your Information**

We want you to be in control of your information, so we provide you with the following tools.

* **Access, Correction, and Portability.** You can access and edit most of your basic account information right in our apps. You can also use [Download My Data](https://accounts.snapchat.com/accounts/downloadmydata) to obtain a copy of information that isn’t available in our apps in a portable format, so you can move it or store it wherever you want. Because your privacy is important to us, we will ask you to verify your identity or provide additional information before we let you access or update your personal information. We may also reject your request to access or update your personal information for a number of reasons, including, for example, if the request risks the privacy of other users or is unlawful.
* **Revoking permissions.** In most cases, if you let us use your information, you can simply revoke your permission by changing the settings in the app or on your device if your device offers those options. Of course, if you do that, certain services may lose full functionality.
* **Deletion.** While we hope you’ll remain a lifelong Snapchatter, if for some reason you ever want to delete your account, You can also delete some information in the app, like photos you’ve saved to Memories, Our Story submissions, and search history.
* **Advertising Preferences.** We try to show you ads that we think will be relevant to your interests. If you would like to modify the information, we and our advertising partners use to select these ads, you can do so in the app and through your device preferences.
* **Communicating with other Snapchatters.** It’s important to us that you stay in control over whom you communicate with. That’s why we’ve built a number of tools in Settings that let you indicate, among other things, who you want to see your Stories, whether you’d like to receive Snaps from just your friends or all Snapchatters, and whether you’d like to block another Snapchatter from contacting you again.

## **Revisions to the Privacy Policy**

We may change this Privacy Policy from time to time. But when we do, we’ll let you know one way or another. Sometimes, we’ll let you know by revising the date at the top of the Privacy Policy that’s available on our website and mobile application. Other times, we may provide you with additional notice (such as adding a statement to our websites’ homepages or providing you with an in-app notification).

**”**

These are the principals and features of Snapchat, and the associated security policies.

Snap, Inc.

* Deletes Snaps from servers once all Snapchat users it was sent to have viewed it, unless legally required to do otherwise
* Can keep data that was posted to a user’s Story, Live, Local, and other crowd-sourced services for a longer period

Snapchat Users

* Can add friends by username, from contacts list, by Snap code, using Nearby, and using Quick Add which uses mutual friends
* Can view, send, and save Snaps and Chats only sent to them and those in My Story of Snap chatters they have added
* Can see username, name, Bitmoji, Snapchat score, and mutual friends of other users
* Can view any additional information that a user has consented to share, including whether someone has a Snapchat account based on phone numbers from a user’s phonebook
* Cannot view deleted accounts, even if account information is still in server (for 30 days after deletion)
* Cannot send Snaps and Chats and view the Story of users who have blocked them

Everyone

* Public information of any user such as names, username, Snap code, and profile pictures
* Any content submitted to crowd-sourced features like Live and Local

Third-Party Advertisers

* Can include attachments to ads, which include articles, app installations, long-form videos, and website all within the Snapchat app
* Can use cookies, web beacons, and similar tracking technologies
* Can target Snap chatters by age, gender, geographical location, mobile device, operating system (Android or iOS), mobile carrier, interests, Snapchat's first-party audiences, lookalikes, and purchase intent with Datalogic segments

Features

* Memories - has access to phone camera roll photos
* Snapcash - uses debit card information and sent by using a $ in Chat
* Geofilters - have access to location, can be available only to a certain Geofence (bounded area) for a certain period
* Groups - can send Snaps and Chats to up to 16 users at a time
* Unlockables - can analyze Snaps taken (even if they are not yet sent) for any Snapcodes
* Shazam - can detect and analyze background audio
* Other Third-Party Integrations - can get any information (including personal information) based on the Terms and Services that they provide

1. Summary of Findings

I am going to Use these subdomains which covered all the priority levels, as my example:

|  |  |  |
| --- | --- | --- |
| Type | Identifier | Max. Severity |
| Domain | **accounts.snapchat.com** | Critical |
| Domain | **Ads.snapchat.com** | High |
| Domain | **www.bitmoji.com** | Medium |
| Domain | **story.snapchat.com** | Low |

* 1. Nikto

Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.

***nikto -h snapchat.com***

***Graphical user interface, text, application, email

Description automatically generated***

***Low – nikto -h story.snapchat.com***

***Graphical user interface, text

Description automatically generated***

***Medium – nikto -h bitmoji.com***

***Graphical user interface, text

Description automatically generated***

***High – nikto -h Ads.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

***Critical – nikto -h accounts.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

* ***Checking DATABASE***

***nikto -dbcheck snapchat.com***

***Graphical user interface, text

Description automatically generated***

***Low – nikto -dbcheck story.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

***Medium – nikto -dbcheck bitmoji.com***

***Graphical user interface, text, application

Description automatically generated***

***High – nikto -dbcheck Ads.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

***Critical – nikto -dbcheck accounts.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

* + 1. Found Bug – www.bitmoji.com

***nikto -h*** [***www.bitmoji.com***](http://www.bitmoji.com)

***Graphical user interface, text

Description automatically generated***

[www.bitmoji.com](http://www.bitmoji.com) is a subdomain of [www.snapchat.com](http://www.snapchat.com) and it has medium priority. I have scanned it through the nikto and I got some sensitive information, but it happens only once.

+Server banner has changed from ‘CloudFront’ to ‘AmazonS3’ which may suggest a WAF, load balancer or proxy is in place

+/SiteServer/admin/:Site Server components admin. Default account may be ‘LDAP\_Anonymous’ , pass is ‘LdapPassword\_1’ see http://www.fp/p/doc.asp/i1/d69.html

* 1. Wapiti

Wapiti allows you to audit the security of your websites or web applications. It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data. Once it gets the list of URLs, forms and their inputs, Wapiti acts like a [fuzzer](http://en.wikipedia.org/wiki/Fuzzing), injecting payloads to see if a script is vulnerable.

***wapiti -u*** [***https://snapchat.com***](https://snapchat.com)

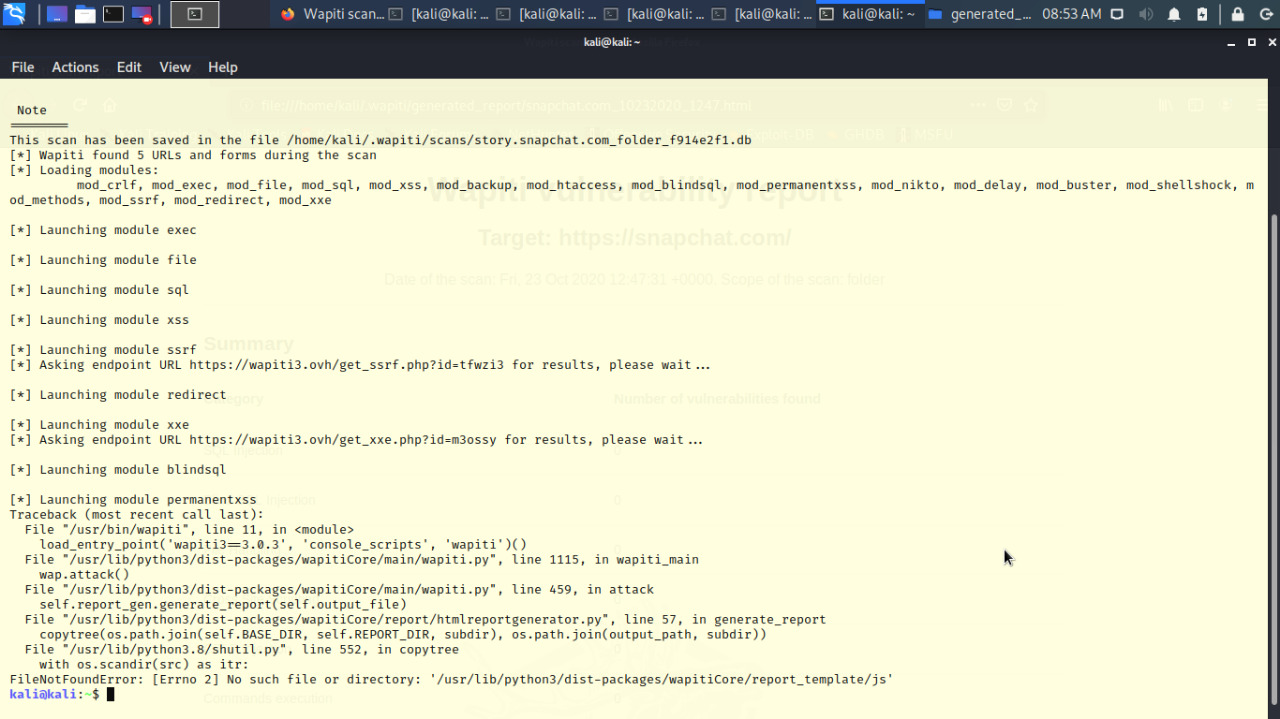
******

***Report :***

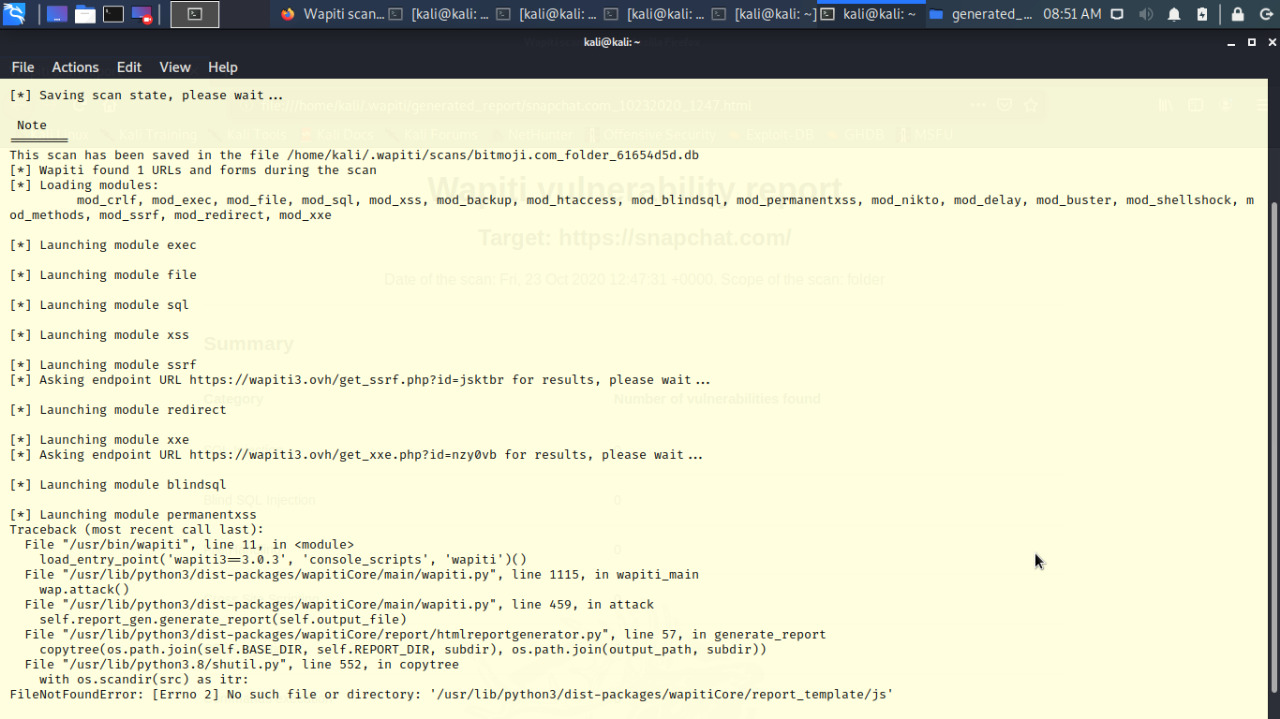
***Graphical user interface

Description automatically generated***

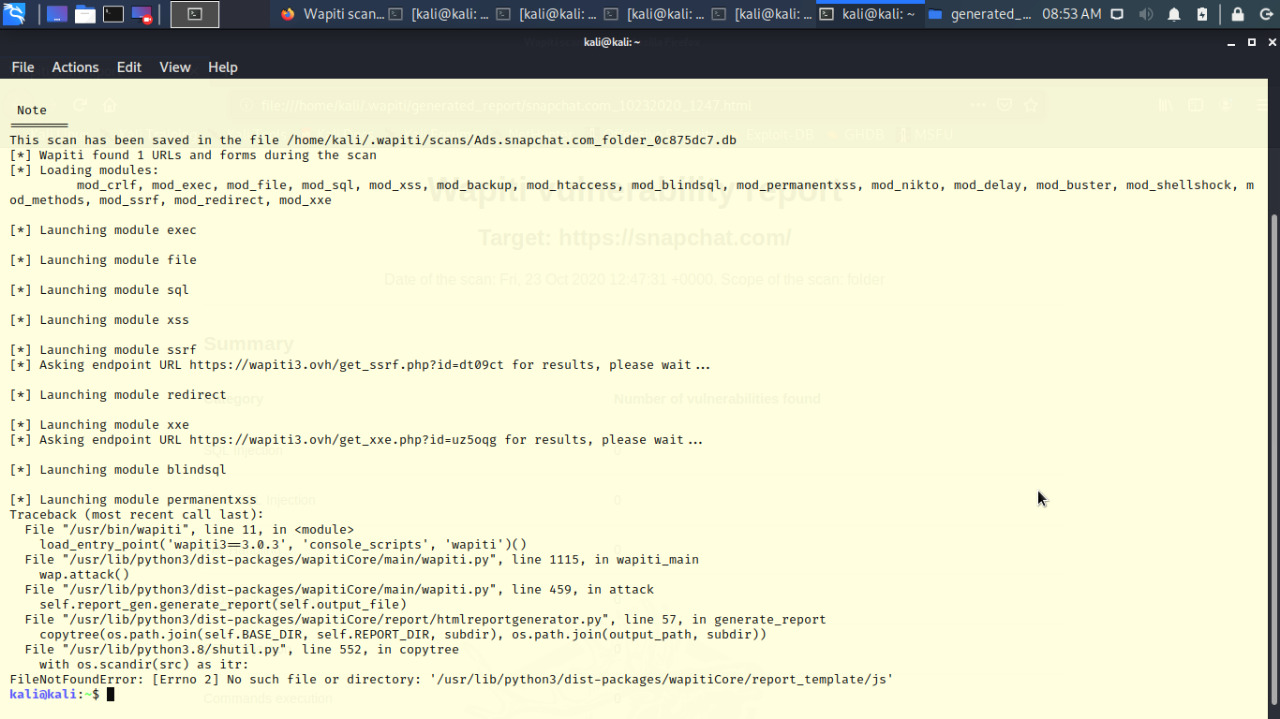
***Low - wapiti -u*** [***https://story.snapchat.com***](https://story.snapchat.com)

******

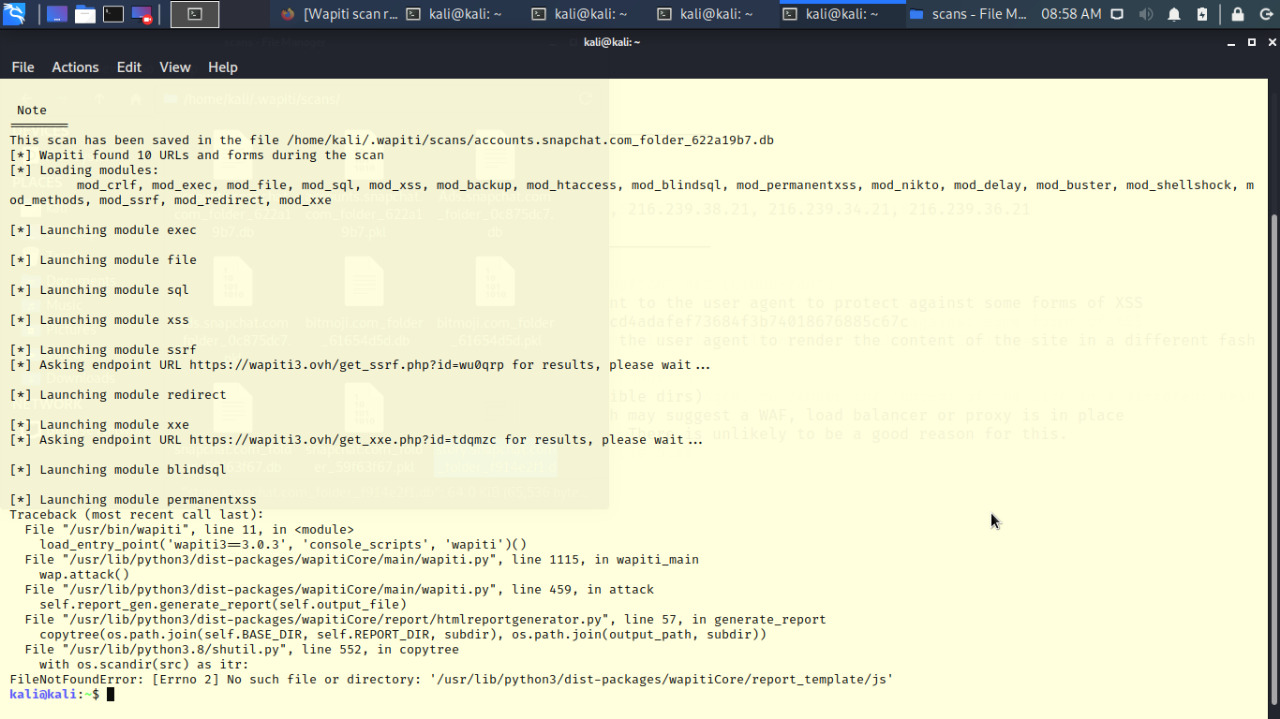
***Medium - wapiti -u*** [***https://bitmoji.com***](https://bitmoji.com)

******

***High – wapiti -u*** [***https://Ads.snapchat.com***](https://Ads.snapchat.com)

******

***Critical – wapiti -u*** [***https://accounts.snapchat.com***](https://accounts.snapchat.com)

******

* 1. whatweb

WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

***whatweb -V -a 1 snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

***Low – whatweb -V -a 1 story.snapchat.com***



***Medium - whatweb -V -a 1 bitmoji.com***

***Graphical user interface, text, application

Description automatically generated***

***High – whatweb -V -a 1 Ads.snapchat.com***

***Graphical user interface, text, application

Description automatically generated***

***Critical – whatweb -V -a accounts.snapchat.com***

***Graphical user interface, text, application, email

Description automatically generated***

4. Attacks (Previous versions)

To test the security measures used by Snapchat, I attempted a variety of network-based attacks against Snapchat’s mobile applications as well as its web application. In addition, I examined applications that were recently integrated into Snapchat. I also examined the application’s code and the generated databases for confidential data.

4.1 Network Attacks

Snapchat uses SSL (Secure Sockets Layer) / TSL (Transport Security Layer) to provide privacy and data integrity for its data communication. All data transmitted over the internet are encrypted using symmetric key encryption and ensured integrity with message authentication codes.

Graphical user interface, text, application

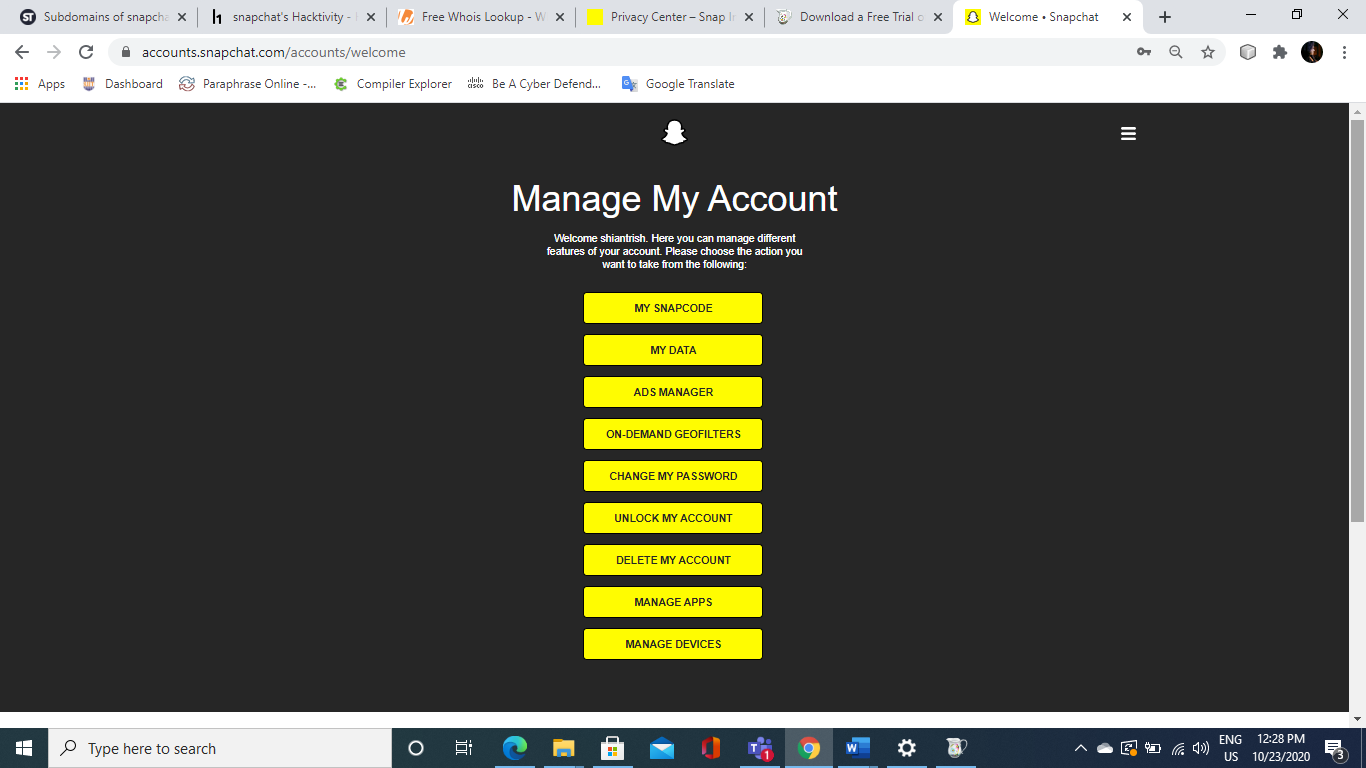
Description automatically generatedIn addition, the identity of the communicating parties is authenticated using public key encryption. The protocols rely on trusted third-party certificate authorities to establish the authenticity of digital certificates, which are typically used as a proof for ownership of the public key. This reliance on certificates authorities, however, is known to leave TSL/SSL susceptible to the man-in-the-middle attacks by attackers who have certificates signed by an authority the client trusts.

Under the consideration that users might get tricked to trust malicious certificate authorities and that all security guarantees are only valid when HTTPS is used, we installed a couple of HTTPS proxies on a number of machines and devices to simulate attacks that adversaries could perform. The HTTPS proxies used are Charles and mitmproxy. If configured correctly as described in detail below, the proxies can capture the traffic between the user and the Snapchat web servers and provide plaintext view of the traffic. One also has the option to modify, replay and abort packets. However, by using an SSL proxy, discovered that in some cases, Snapchat uses SSL pinning or HTTP Strict Transport Security (HSTS) as another layer of protection to prevent man-in-the-middle attacks.

This layer ensures that trusted certificates are correct according to the browser or OS itself, and that the users are always on HTTPS. Therefore, many attacks are not feasible without further efforts.

4.1.1 Web Application

Snapchat provides a web interface (accounts.snapchat.com) solely for account management purposes. Users may login to download or generate new Snapcodes, download in-depth account history, change one’s password, and unlock or delete one’s account. Some people examined the vulnerabilities against cross-site scripting attacks, SQL injection, cross-site request forgery, brute force login and source inspection, and concluded that it was secure.



Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**Exploiting Google Storage Files**

Many of the responses to the requests that the Snapchat app makes return JSON data containing information such as links to Google Storage data

* Stickers, Filters, Lenses, Logos, and Thumbnails: We were successful in downloading all these files. Stickers and lenses came in ZIP files, while the filters, logos, Story thumbnails, and lens thumbnails came as PNG files.
* Stories: We were able to download Story binary files, but we were unable to open/decrypt them.
* Memories: We were unsuccessful in downloading anything from the URLs found and got the error message that Google Storage needed a valid signature.

Graphical user interface, application

Description automatically generated4.1.2 Mobile Applications

Graphical user interface, text, application, email

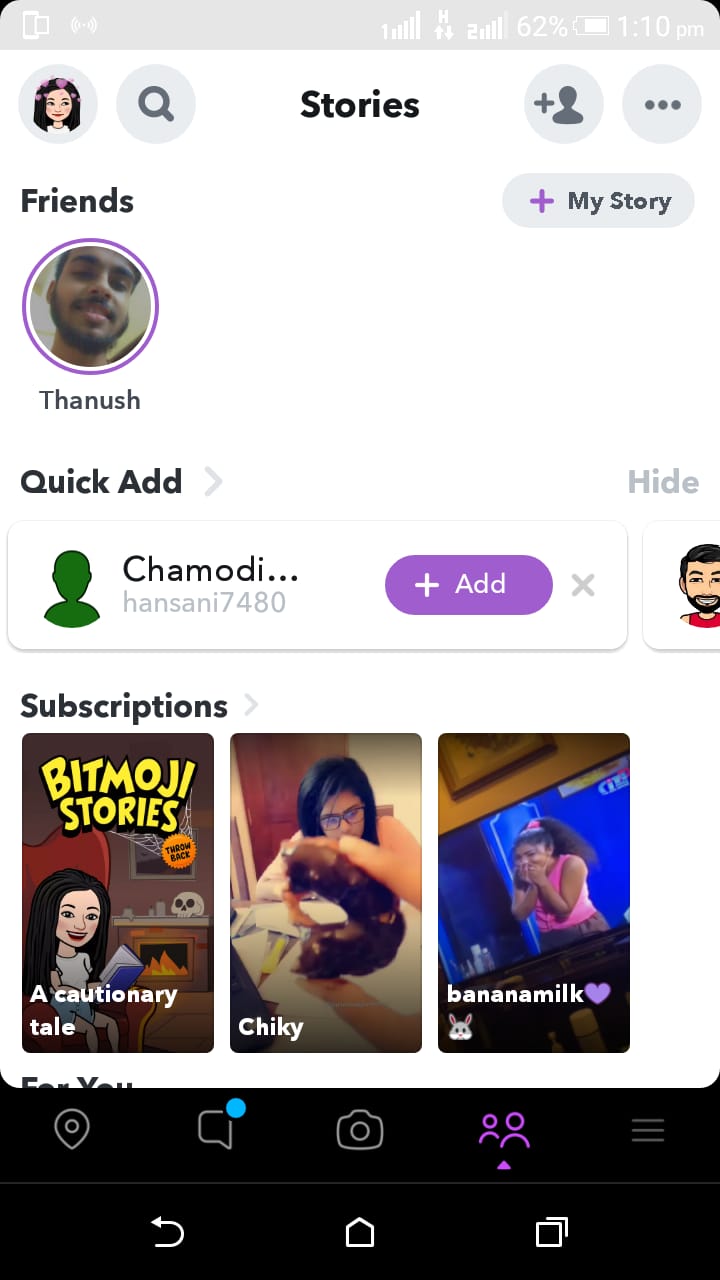
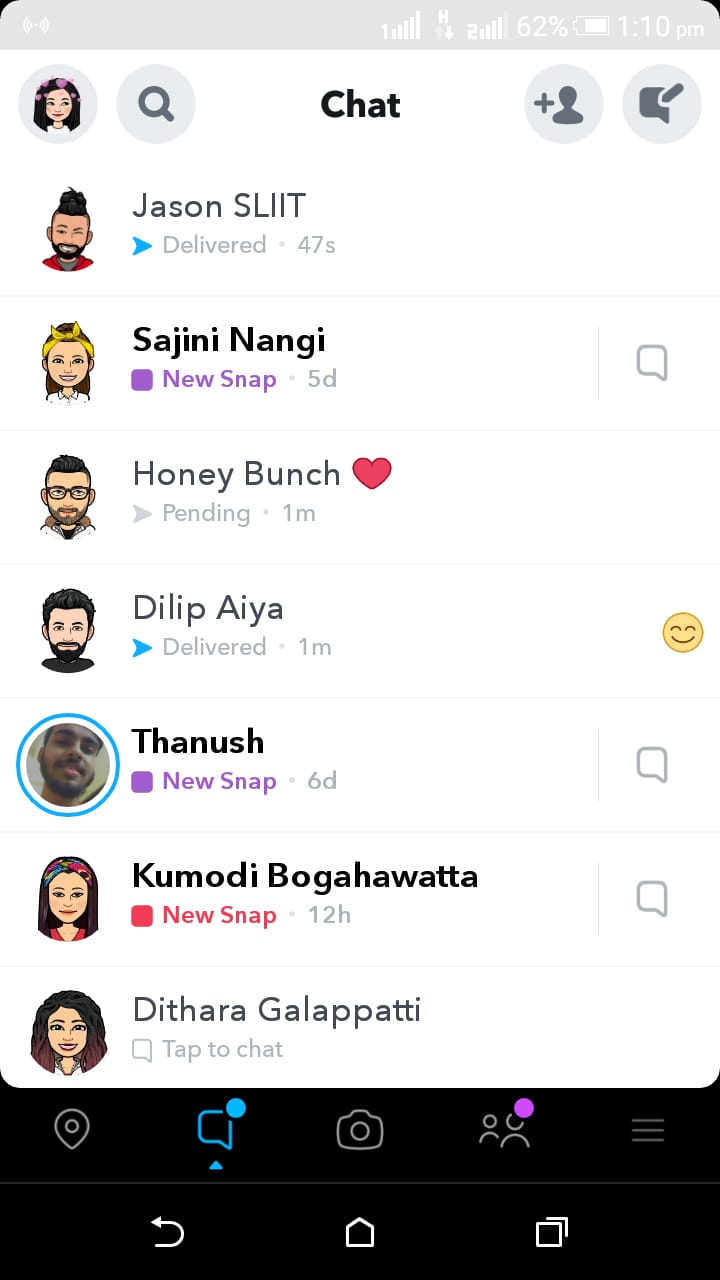
Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface

Description automatically generatedGraphical user interface, application

Description automatically generated

Snapchat transfers and keeps track of a lot of user information such as geolocations, chats, images and videos. To this end, confidentiality and data integrity are no doubt crucial. Over the last few years, Snapchat had integrated numerous features of partner apps into the app. Those include the peer-to-peer payment and in-app purchases supported by Square, video chat service provided by AddLive, personal emoji stickers in messages provided by Bitmoji and music recognition by Shazam. Hence, the security of its mobile application has inevitably become dependent on the security of those partner apps.



5. Conclusion

This report covered audit of web application. And also, a bug from subdomain www.bitmoji.com.

Snapchat is an extremely popular instant messaging platform that allows its users to interact via chat and self-destructing video and photo messages. However, since its creation in 2011, the app developers have gone through a sequence of incidents associated with Snapchat’s security vulnerabilities.

The security lessons learn by Snapchat could be a great source of inspiration for future application developers. Moreover, such incidents can help to change current privacy norms and raise security awareness among mobile app consumers.

6. Acknowledgements

I would like to thank

***Dr. Lakmal Rupasinghe, Ms. Chethana Liyanapathirana, Ms. Laneesha Rukgahakotuwa, Ms. Chathu Udagedara***

and

the rest of the 6.857 staff for obtaining permission from Snapchat to perform this security analysis.

7. References

[1] Akshay Gangwar. How to Sideload Apps on iPhone in iOS 10 (Without Jailbreak). Feb 28, 2017. URL: https://beebom.com/how-to-sideload-apps-iphone-ios-10-without-jailbreak/ 22

[2] Alban Diquet. SSL Kill Switch 2. Feb 6, 2017. URL: <https://github.com/nabla-c0d3/ssl-kill-switch2/>

[3] Apktool: a tool for reverse engineering Android apk files. URL: <http://ibotpeaches.github.io/Apktool>

[4] Charles. SSL Proxying. URL: <https://www.charlesproxy.com/documentation/proxying/ssl-proxying/>

[5] Digicert. What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?. URL: <https://www.digicert.com/ssl.htm>

[6] Gibson Security. Snapchat - GibSec Full Disclosure. Dec 23, 2013. URL: http://gibsonsec.org/snapchat/fulldisclosure/

[7] HTTP Strict Transport Security. URL: <https://https.cio.gov/hsts/>

[8] ios9cydia. Jailbreak iOS 9. URL: <http://www.ios9cydia.com/ios-9-jailbreak.html>

[9] Kingoroot. URL: <https://www.kingoapp.com/>

[10] Lewis Painter. How to screenshot on Snapchat without them knowing. Apr 7, 2017. URL: [http://www.pcadvisor.co.uk/how-to/social-networks/how-screenshot-on-snapchat-without -them-knowing-2017-3634217/](http://www.pcadvisor.co.uk/how-to/social-networks/how-screenshot-on-snapchat-without%20-them-knowing-2017-3634217/)

[11] Madeleine Dawson, Heeyoon Kim, Wei-En Lee, Kelly Shen. Security Analysis of Snapchat. May 2016. URL: <http://courses.csail.mit.edu/6.857/2016/files/11.pdf>

[12] mitmproxy. URL: <https://mitmproxy.org>

[13] Mozilla Developer Network. HTTP Request Methods: CONNECT. Feb 6, 2017. URL: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/CONNECT>

[14] Online Android decompiling tool. URL: <http://www.decompileandroid.com>

[15] OWASP. Certificate and Public Key Pinning. Jul 5, 2016. URL: <https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning>

[16] OWASP. HTTP Strict Transport Security Cheat Sheet. Jan 6, 2017. URL: [https://www.owasp.org/index.php/HTTP\_Strict\_Transport\_Security\_Cheat\_Sheet 23](https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet%2023)

[17] Pangu. URL: <http://en.9.pangu.io/>

[18] Recode. Snap’s IPO numbers look a lot more like Twitter’s than Facebook’s. URL: <https://www.recode.net/2017/2/2/14492932/snapchat-ipo-twitter-facebook-comparison>

[19] Scott Ogrin. Why HTTPS and SSL are not as secure as you think. URL: https://www.sott.net/article/275524-Why-HTTPS-and-SSL-are-not-as-secure-as-you-think

[20] Security StackExchange: How Safe is SSL. URL: https://security.stackexchange.com/questions/53596/how-safe-is-ssl

[21] Snap Inc. For Snapchatters with Jailbroken iPhones. URL: <https://support.snapchat.com/en-US/article/jailbroken-iphone>

[22] Snap Inc. I Can’t Create An Account Or Access My Account. URL: <https://support.snapchat.com/en-US/a/account-questions>

[23] Snap Inc. Privacy Policy. Jan 10, 2017. URL: <https://www.snap.com/en-US/privacy/privacy-policy/>

[24] Snap Inc. Third-Party Applications and Plugins. Apr 20, 2017. URL: <https://support.snapchat.com/en-US/a/third-party>

[25] Snap Inc. What Can Snapcash Be Used For? URL: <https://support.snapchat.com/en-US/a/snapcash-guidelines>

[26] Stackoverflow: How does the RSA private key passphrase work under the hood. URL: http://stackoverflow.com/questions/1774469/how-does-the-rsa-private-key-passphrase-w ork-under-the-hood

[27] Symantec. What is SSL, TLS and HTTPS?. URL: <https://www.symantec.com/page.jsp?id=ssl-information-center>

[28] Telegraph. 10 of the best hidden Snapchat features. Oct 12, 2016. URL: http://www.telegraph.co.uk/technology/0/the-best-hidden-snapchat-features/ 24