No salvation from trackers: Privacy analysis of religious websites and mobile apps

Nayanamana Samarasinghe, Pranay Kapoor, Mohammad Mannan, and Amr Youssef

Concordia University, Montreal, Canada
{n_samara,p_apoo,mmannan,youssef}@ciise.concordia.ca

Abstract. Many religious communities are going online to save costs and reach a large audience to spread their religious beliefs. Since the COVID-19 pandemic, such online transitions have accelerated, primarily to maintain the existence and continuity of religious communities. However, online religious services (e.g., websites and mobile apps) open the door to privacy and security issues that result from tracking and leakage of personal/sensitive information. While web privacy in popular sites (e.g., commercial and social media sites) is widely studied, privacy and security issues of religious online services have not been systematically studied. In this paper, we perform privacy and security measurements in religious websites and Android apps: 62,373 unique websites and 1454 Android apps, pertaining to major religions (e.g., Christianity, Buddhism, Islam, Hinduism). We identified the use of commercial trackers on religious websites — e.g., 32% of religious websites and 78% of religious Android apps host Google trackers. Session replay services (*FullStory*, *Yandex*, *Incpectlet*, *Lucky Orange*) on 198 religious sites sent sensitive information to third parties. Religious sites (14) and apps (7) sent sensitive information in clear text. Besides privacy issues, we also identify sites with potential security issues: 19 religious sites were vulnerable to various security issues; and 69 religious websites and 29 Android apps were flagged by VirusTotal as malicious. We hope our findings will raise awareness of privacy and security issues in online religious services.

1 Introduction

With the advancement of technology, significant changes are made as to how religious practices are conducted during the last couple of decades [1]. The early online churches simply used websites with static pages (e.g., scriptorium pages of religious texts) to share information with an increased audience. Gradually, these websites started to include dynamic content hosting various interactive services (e.g., chat and messaging services, podcasts, videos of sermons, interactive worship). Also, with the proliferation of mobile devices, religious services were offered through mobile apps [2]. The recent COVID-19 pandemic has also resulted in offering religious services through online social media platforms (e.g., Facebook Live, YouTube) [3], and religious faiths in the United States have

strengthened due to the pandemic [4]; 57% of the adults in the United States who attended religious services at least monthly, are now watching religious services online due to the pandemic [4]; churches supplement their revenue using virtual offering (e.g., donation) services. Unfortunately, various third parties included on religious online services to support various functionalities, are used to track users [5], and engage in privacy violations [6] leaking sensitive information; a prayer app (*Muslim Pro*) that eases the practicing of daily rituals prescribed in Islam, has leaked user location data to a broker (*X Mode*), which in turn had sold the same information to its contractors (including US military contractors) [7]; another prayer app (*pray.com*) sold the prayers of a grieving user who suffered a tragedy [8]. Also, while the possible influences from artificial intelligence (AI) technology on religious online services is still an under-studied area, potential exposures of highly confidential conversations relating to spiritual needs of users through chatbots (included on religious online services) will impact the privacy of users. In addition, security issues in religious online services can expose sensitive information of users; the Vatican site was hacked and compromised (in 2020) [9] with the aim of stealing sensitive information.

Past studies primarily discussed the evolution of digital religious communities from traditional religious institutions. Campbell [10] studied Internet trends and their implications on religious practices (including social and cultural shifts) and challenges related to online religious networks. The author observed that studying the religious practices of Internet users leads to a more refined understanding of the complex interactions with online services. Campbell et al. [2] provided a methodological approach to study religious-oriented mobile apps available on iTunes app store. The authors reviewed 451 religious app functions and their use, and group those apps into 11 categories.

In this work, we perform a large scale web privacy measurement of religious websites and Android apps. To the best of our knowledge, this is the first measurement study on privacy/security of religious online services, performed on a global scale. For the web privacy measurements, we use 62,373 websites collected from the *URL Classification* [11] source, after filtering out false positives (i.e, non-religious sites) using VirusTotal [12] website categorizations. Thereafter, we crawl the extracted religious websites using OpenWPM [13] web privacy measurement framework. We analyze the instrumented tracking metrics (third party scripts/cookies, fingerprinting APIs) using the instrumented data saved to the OpenWPM database. We identify religious websites that use session replay services, by inspecting the traffic sent by potential sites including session replay services with *HTTP Toolkit* [14]. In addition, we examine religious sites that send personal information to external parties using the chatbot functionality. We look for leaked personal/sensitive information (e.g., name, email address, address, prayer requests, confessions, user's location provided for searches) from religious websites that use HTTP or configured to use session replay. To find potential TLS vulnerabilities and weaknesses, we collect and analyze TLS certificates of 45,004 religious websites. In order to find other vulnerabilities in religious websites (e.g., Cross Site Scripting, SQL Injection, Path Traversal), we

scan 11,888 religious websites using the *Wapiti* scanner. We also collect religious Android apps, and leverage MobSF [15], LiteRadar [16], and mitmproxy (with Google UI/Application Exerciser Monkey), to perform static and dynamic analysis techniques (using a Pixel 6 phone). However, we limit the security evaluation of religious online services due to possible legal and ethical issues. We also use VirusTotal [12] to identify religious sites, Android APKs and included third party domains hosting scripts/cookies that are malicious.

Contributions and notable findings.

1. We develop a framework to collect religious websites and Android apps by eliminating false positives from given external source(s), and a test methodology to evaluate the privacy and security exposures from these religious websites.

2. 198/62,373 (0.3%) religious websites include session replay services — e.g., *FullStory* (*fullstory.com*), *Inspectlet* (*inspectlet.com*), *Luckyorange* (*luckyorange.com*), *Yandex* (*yandex.com*). We observed that users' personal/sensitive information is sent from the analyzed religious websites to session replay services (*FullStory*, *Yandex*, *Inspectlet*). Such shared sensitive information includes name, phone number, address, email address, message/comment, prayer request, location searches, login information, donation information, and keywords used in site searches.

3. 19/11,888 religious websites were found to be vulnerable — SQL Injection (9), Reflected Cross Site Scripting (7), Server Side Request Forgery (2), Path Traversal (1). The Path Traversal attack (on *christcc.org*) exposes several local files under /etc directory (e.g., /etc/password).

4. 7/1454 religious Android apps leaked sensitive information (e.g., user credentials, API key, phone number) from unprotected Firebase endpoints. In addition, 2 apps (*cdff.mobileapp*, *com.avrpt.teachingsofswamidayananda*) sent user credentials/device information over HTTP.

5. 17,418/62,373 (27.9%) and 3569/62,373 (5.7%) of religious sites include commercial tracking scripts and cookies, respectively. These trackers embed analytic and other third party services (e.g., social media plugins) on religious websites. Google dominates in tracking on both religious sites (32%) and apps (78%). There were tracking cookies that expire after a long period of time (including 4 tracking cookies by center.io on 4 religious sites that expire in year 9999). In addition, 1351/1454 (93%) of religious Android apps included tracking SDKs.

6. 69/62,373 religious websites were flagged as malicious at least by 5 security engines used by VirusTotal (e.g., *samenleesbijbel.nl*, *csiholytrinitychurch.com*). We also observed 12 malicious domains set tracking scripts/cookies on religious sites. Additionally, 29/1454 (2%) religious Android apps were flagged by VirusTotal by at least one security engine; *islamictech.slfgo* religious Android app was flagged by 10 security engines in VirusTotal.

7. 14/24 religious websites that use HTTP, sent personal/sensitive information (name, email address, phone number, address, message, prayer request, confession, date of birth, password).

We disclosed our findings on security vulnerabilities of the 10 websites and 9 Android apps to the corresponding admins/developers. We also notified Google about *islamictech.slfgo*.

2 Related work

Web privacy measurements. There are various privacy measurement studies that are performed in the past. Englehardt et al. [17] implemented OpenWPM, a fully automated web privacy measurement framework. Using OpenWPM, Englehardt et al. [17] performed a web privacy measurement of the top-1M Alexa popular sites (mostly commercial sites), and found Google and Facebook dominates in tracking. Samarasinghe et al. [18] measured tracking on 150,244 government websites and 1166 Android apps, and found commercial trackers on those online services (mostly Google trackers), although it was unexpected to have trackers on government sites that are funded by the taxpayers. Hoy et al. [19] studied 102 church websites in the United States and found that they collect personal identifying information. The confidential information that are entered to church guest books and prayer requests, were leaked from corresponding church websites. We studied tracking on religious websites and found a larger proportion of those sites with Google trackers (32%, 19,772 out of 62,373 websites). In addition, we found 22 websites leak sensitive information of users (e.g., name, address, email, donation amount, prayer requests) to session recording services.

Privacy analysis of mobile apps. Several past studies analyzed privacy and security issues in mobile apps. For example, Binns et al. [20] studied 959,000 apps from US and UK Google Play stores, and found that third party tracking follows a long tail distribution dominated by Google (87.75%). Nguyen et al. [21] performed a large-scale measurement on Android apps to understand violation of General Data Protection Regulation (GDPR) explicit consent. They found 28.8% (24,838/86,163) of apps sent data to ad-related domains without explicit user consent. Several recent studies (e.g., [22]) analyzed COVID-19 tracing apps, and highlighted privacy and surveillance risks in these apps. In contrast, we study privacy and security issues of 1454 religious Android apps and found Google specific tracking SDKs in a large proportion (78%, 1132 out of 1454) of them.

Analysis of SSL/TLS certificates used in online services. Felt et al., [23] measured the HTTPS adoption on the web, and found the number of top websites (from HTTPWatch Global, Alexa top-1M, Google top-100) that use HTTPS (by default) doubled between early 2016 and 2017. Alabduljabbar et al. [24] investigated the potential vulnerabilities (SSL/TLS) in free content websites (FCW) and premium websites. The authors found 17% and 12% of free websites have invalid and expired certificates, respectively. The authors also found more FCWs (38%) use ECDSA signature algorithm compared to premium websites (20%). We analyze TLS certificates of 45,004 religious websites and found 92.9% and 7.1% of HTTPS sites use RSA and ECDSA signature algorithms, respectively.

3 Methodology

In this section, we provide details of our website and apps collection methodology. Then, we elaborate our privacy analysis and measurement techniques; see Figure 1 for an overview of our methodology.

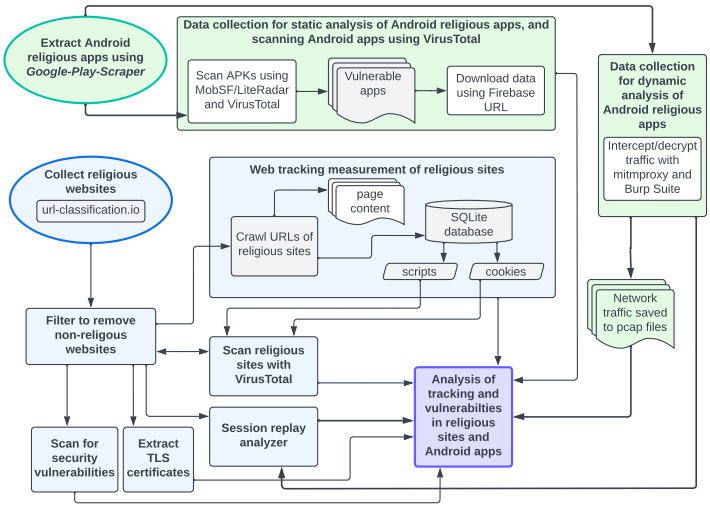

Fig. 1: Overview of our methodology.

3.1 Collecting religious websites and Android apps

Religious websites. We acquired a list of 583,784 websites (on April 26, 2022) from *URL Classification* [11] that are categorized as *Religion*; 448,646 (out of 583,784, 76.9%) are classified into multiple categories (including *Religion*). *URL Classification* provides a confidence rank for classified categories of each website, and with manual inspection, we find websites ranked 50 and above are likely religious sites; 202,968 (out of 583,784, 34.8%) websites are ranked 50 and above. To ensure, false positives are eliminated, we scan the the 202,968 websites with VirusTotal [12], and filter 62,373 (out of 583,784, 10.7%) websites that are flagged as *Religion* by at least one security engine included in VirusTotal.

Religious Android apps. We feed unique keywords related to major religions (i.e., Christianity, Islam, Hinduism, Buddhism) to *Google-Play-Scraper* [25], that crawls and extracts 2512 Android apps matching those search keywords from Google Play Store. We eliminate false positives by manual inspection, and finally select 1454 apps for our analysis.

3.2 Web privacy measurements

We configure OpenWPM [13] web privacy measurement framework to run with 10 parallel browser instances in headless mode. We configure OpenWPM instrumentations for HTTP requests/responses, JavaScript, cookies, DNS requests and

callbacks. JavaScipt instrumentation also collects passive fingerprinting APIs included in religious websites. To mimic a new request, and to avoid any influence from past browsing history, for each URL visit, we clear the browser profile after each visit to a website. We use a physical machine (connected to our university network) running Ubuntu server 20.4 LTS, 64GB RAM, 1TB SSD, AMD Ryzen Threadripper 2950X 16-Core Processor for our measurements between May 1, 2022 - May 7, 2022. A total of 62,373 religious sites were successfully crawled. We also configure OpenWPM to save the site content to a *LevelDB* [26] database. The instrumented tracking metrics extracted from OpenWPM are saved to an SQLite database for further analysis. The saved information in the database contains both stateful (i.e., scripts/cookies) and stateless (fingerprinting) forms of tracking metrics. We then extract scripts and cookies hosted on third-party domains (i.e., domains of scripts/cookies that do not match the domain of the religious site that they are included). We use *EasyPrivacy* [27] filtering rules that block third party trackers in religious sites to identify known third party tracking scripts/cookies.

3.3 Session replay scripts and chatbot services in religious websites

We identify a list of known session replay scripts offering session replay services [28] — *FullStory* (fs.js), *Inspectlet* (inspectlet.js), *Lucky Orange* (core/lo.js), *Yandex* (watch.js, tag.js). Then we extract the religious websites (198 out of 62,373, 0.32%) that include those scripts, from the *javascript* table of OpenWPM SQLite database. Thereafter, we inspect these 198 sites manually, to identify possible personal/sensitive information leaked during user interactions with the religious websites (e.g., while submitting messages and prayer requests, donating to religious institutions). During the interactions with these websites, we use crafted data (e.g., name, email, date of birth, messages, amount for donations), but do not submit the form, as input information is sent to remote servers, after each keystroke during user input. Personal information is also sent during interactions with chatbots in religious websites. We manually inspect the network traffic using *HTTP Toolkit* [14] to identify information sent over the network.

3.4 Security issues in religious websites

Potential security issues in religious websites can cause privacy issues. In this section, we discuss security issues in the analyzed religious websites.

Malicious religious websites. In order to determine if the religious websites and included third party domains (hosting scripts/cookies) are malicious, we scan all 62,373 religious websites, and included 1906 third party tracking domains using VirusTotal. Note that, at least in some cases, VirusTotal engines[1] may misclassify or delay in updating domain categorization labels [29]. We report domains that are flagged by at least 5 security engines as malicious.

[1] `https://tinyurl.com/2p8ynsfj` (we exclude CRDF and Quttera for their unreliable results as we observed).

HTTP/HTTPS traffic and TLS certificates used in religious websites. We use *PyOpenSSL* [30] to collect the TLS certificates (in X509 format) of the analyzed religious websites. Then we extract various information of the collected certificates — i.e., validity duration, common name, issuer information (e.g., issuer name, issuer country, issuer organization), signature algorithm, public key size (for RSA only). We identify the protocol used in each web request (i.e., HTTP, HTTPS). We also analyze the collected information, to determine whether any of the religious websites send personal/sensitive information over plain HTTP, or the associated certificates used in religious websites expose users to risks.

Other security issues in religious websites. We randomly selected 11,888 religious websites (out of 62,373), and scanned them using the *Wapiti* [31] scanner to find other security issues (e.g., Cross Site Scripting, Server Side Request Forgery, SQL Injection). *Wapiti* crawls the web pages of a given website, and looks for scripts and forms in web pages where it can inject payloads to identify vulnerabilities. We configured *Wapiti* to use 15 seconds as *max-attack-time* and *max-scan-time*, and scan up to a depth of 5 levels from the base URL.

3.5 Android app analysis

Tracking SDK detection. We perform static analysis, using LiteRadar [16] by feeding APK files of each of the religious Android apps. The output from this process includes the tracking SDKs included in religious Android apps, the use of tracking SDKs, and requested permissions (including dangerous permissions such as camera, contacts, microphone, SMS, storage, and location).

Misconfigured Firebase database. Many Android apps, including religious apps, use Google Firebase [32] (a widely used data store for mobile apps) to manage their backend infrastructure. However, due to possible misconfiguration, Android apps connected to Firebase database can be vulnerable. Exposed data from Firebase vulnerabilities includes personally identifiable information (PII) and plain text passwords. We leverage MobSF [15] to extract URLs of unprotected Firebase endpoints for each APK file, which contains potential vulnerabilities; we then download the exposed data from the Firebase datastore URL[2] and check for apparent sensitive and PII items, including: user identifiers, passwords, email addresses, and phone numbers. However, for ethical/legal considerations, we do not validate the leaked information (e.g., login to an app using the leaked user credentials). Then we remove the downloaded datastore.

Dynamic analysis. We use a rooted Pixel 6 mobile phone with Android 12, to proxy traffic from newly installed apps via mitmproxy [33]. To avoid collecting traffic from other apps, we uninstall all other apps, except those apps required for basic functionalities (e.g., Camera, Google Play Store). A mitmproxy root certificate is installed on the phone. We also install mitmproxy on a separate

[2] The URL is of the form *<Firebase project name>.firebaseio.com/.json* (e.g., `https://catholic-connect-213606.firebaseio.com/.json`).

desktop machine to collect and decrypt HTTPS traffic. Both the desktop machine and phone are connected to the same Wi-Fi network. We use adb [34] to automate the installation, launch, and uninstallation of the apps. We also use Monkey [35] with 5000 events (e.g., touch, slide, swipe, click) for each app; login to app UI is not supported (if prompted). The network traffic is captured and stored in pcap files. We use the captured network traffic to determine sensitive information (e.g., device identifiers sent to trackers, leaked hardcoded user/admin credentials and API keys) sent to external entities. We close mitmproxy and uninstall the installed religious app before moving to the next app.

Session replay from Android apps. We leverage the dynamic analysis to inspect third party domains included in apps, to identify those known session replay services (e.g., Yandex, Hotjar, MouseFlow, UXCam) to which apps send HTTP requests. For this exercise, we use Burp Suite [36] to identify apps that send sensitive information to corresponding session replay services.

Malicious domains and apps. We scan the APK files of 1454 religious Android apps with VirusTotal. We also scan 1539 domains included in apps (as found in the network traffic) with VirusTotal.

3.6 Ethical considerations and limitations

We do not use the sensitive information (e.g., user identifiers and passwords) extracted from static and dynamic analyses of Android apps for any intrusive validations that may have an impact to the privacy of users. In addition, we did not retain any data from exposed Firebase databases. The *Wapiti* black-box scanner we use to find vulnerabilities in religious websites, limits the scope of the scan only to the web page (e.g., add/remove query parameters).

EasyPrivacy [27] filtering rules that we use are not comprehensive enough to identify all possible tracking scripts/cookies set on religious sites (especially country specific trackers). We also resorted to use manual steps in verifying false positives/negatives of religious websites and Android apps, which are not trivial to automate (e.g., inspection of sensitive information relayed from session replay services to third parties). Android apps with obfuscated code may have impacted our static analysis, but not so on our dynamic analysis. Random clicks triggered from the UI automation that use monkeyrunner, may not precisely target the specific targeted areas on the UI.

4 Results: Religious websites

4.1 Session replay and chatbot services

With session replay services that are included in websites, a user's session is replayed through the browser and sent to a remote third party; information replayed includes user interactions on a website, such as typed inputs, mouse movements, clicks, page visits, tapping and scrolling events. During this process,

user's sensitive information can be exposed to third-party servers that host session replay scripts. We identified four session replay services on the analyzed religious sites (62,373): *FullStory* (4), *Inspectlet* (5), *Lucky Orange* (1), *Yandex* (187). The Lucky Orange session replay service was included only on one analyzed religious site (*discoverquran.com*), and we found session replaying on this site was disabled by the site owner. FullStory was used (e.g., in *fbckahoka.org*, *emmausdenver.com*) to replay requests for religious material and prayer requests by users. Inspectlet was used to replay meta-information (e.g., page title, browser information, dependent resources of websites requested) of religious sites (e.g., *gbcga.com*, *afci.com.au*) browsed by users, which can be leveraged for fingerprinting. We found personal information (e.g., name, email, phone, message, address, login ID), donation details (e.g., donation amount), prayer requests and keywords used during site searches being replayed to Yandex session replay services from 19 religious sites; see Table 1.

Furthermore, AI-based chatbots are being included in religious websites to emulate personal human conversations. Exposure of these conversations to adversaries may divulge personal information of users. We observed chatbots of two religious sites shared personal conversation to third parties: *chertzumc.com* transmitted user conversations in base64 format to an external domain (*chat.amy.us*), and *immersivehistory.com* sent user conversations as is, over a websocket to a third party domain (*socket.tidio.co*).

4.2 Religious sites with security issues

The *Wapiti* scanner identified security issues in 19 (out of 11,888) religious websites — SQL Injection (9), Reflected Cross Site Scripting (7), Server Side Request Forgery (2), Path Traversal (1); see Table 2 for examples of security issues in religious websites. *Christcc.org* is vulnerable to the Path Traversal attack that exposes the local /etc/passwd file. Although, user passwords are not revealed from the /etc/passwd file, the content (e.g., full names, list of system users indicating software installed on the host) of it can be used for reconnaissance and social engineering efforts, which may eventually lead to reverse shells and local privilege escalations. The potential Reflected Cross Site Scripting attacks that can be launched by some websites (e.g., *abccolumbia.org*, *christcc.org*, *cogsabbath.org*), are proof of the attacker's ability to execute much more harmful attacks (e.g., steal credentials, hijack user accounts, exfiltrate sensitive information) on users. The same applies to religious websites (e.g., *abccolumbia.org*, *aoffcc.com*, *welfarebc.com*) subjected to SQL Injection vulnerability, where the consequences from such attacks (e.g., unauthorized viewing of user data, removal of data from database tables, attacker gaining database administrative rights) are far reaching. We also scanned religious Android apps pertaining to these religious websites (for security issues) using *Wapiti*, and found *com.subsplashconsulting.s_R858KV* (CCC Camp Hill, PA App) app that corresponds to *christcc.org* religious website, contains 2 endpoints (`https://app.easytithe.com/AppAPI/api/account/churchInfo`, `https://app.easytithe.com/AppAPI/api/account/paymentList`) that are vulnerable to SQL Injection.

Leakage type	Religious site	SRS	Leaked information
Personal information	glorygod.ru, aglow.org.uk, novizavet.ru, standrews.ru, slovo-istini.com, zhslovo.ru, sda-spb.ru	Yandex	Name, phone number, email, address/city, message
	nehemiah.ru	Yandex	Location entered to search for the closest church
	mbs.ru, belchurch.org	Yandex	Login ID
	solba.ru	Yandex	Email address used to subscribe for a newsletter
Request for religious material	fbckahoka.org	FullStory	Email address, sermon notes
Request for prayer	fbckahoka.org	FullStory	Full name, email, phone, prayer request
	solba.ru	Yandex	Name, message, donation amount of the prayer request for a patient (Corona and other diseases), and to succeed in studies/exams
Meta information of site requests	lifeteen.com	FullStory	links clicked by users (relating to various religious missions)
	gbcga.com	Inspectlet	Page title, URL browsed, browser information (i.e., browser type, version, webkit, user-agent).
	afci.com.au	Inspectlet	URL and dependencies (CSS, JavaScript) of the site browsed
	bengalipdfbooks.info	Yandex	Links clicked by users
Donation details	novizavet.ru	Yandex	First name, last name, donation amount
	rpconline.ru	Yandex	Donation amount, mode of payment (e.g., bank card)
Keywords uses for searches	new-church.ru, wolrus.org, sda-spb.ru, kateheo.ru	Yandex	Keywords used in site searches that may include sensitive information

Table 1: Use cases for information leakage with session replay services (SRS) on religious sites.

4.3 Religious sites flagged as malicious

We found 69 (out of 62,373, 0.1%) religious sites were flagged as malicious by VirusTotal (at least by 5 engines). We only considered sites that apparently were used for malicious purposes according to VirusTotal category labels and community comments, containing keywords including malware, compromised, infection, spyware, fraud, weapons, command and control, bot network and callhome. We also observed 12 malicious domains host tracking scripts/cookies on religious sites, as per VirusTotal (at least by 5 engines): *freecontent.date* (modifies files in Chrome extension folder) and *iclickcdn.com* (website redirected to malicious pages) were flagged as malicious by more than 10 engines. With *Retire.js* [37], we found JavaScript sources (i.e., *bootstrap*, *jquery*, *swfobject*) included in 3 religious sites (*wierdapark-suid.co.za*, *divyabodhanam.org* and *divyabodhanam.org*) were using legacy script versions that are vulnerable to Cross Site Scripting.

Security issue	Website	Details of the security issue
Reflected Cross Site Scripting (XSS)	spiritofmedjugorje.org	This vulnerability is found via injection of parameter *ArticleSeq* (e.g., `https://spiritofmedjugorje.org/index.php?ArticleSeq=%3C%2Fscript%3E%3CScRiPt%3Ealert%28%27wfj7hux5b6%27%29%3C%2FsCrIpT%3E`)
SQL Injection	abccolumbia.org	Injection of parameter *media_id* (e.g., `https://abccolumbia.org/video.php?media_id=10%27%20AND%2092%3D92%20AND%20%2714%27%3D%2714`). The parameter value passed to *media_id* is decoded as *10' AND 92=92 AND '14'='14*
Path Traversal	christcc.org	Linux local files disclosure vulnerability via injection of parameter *path* — exposes /etc/passwd, /etc/group, /etc/hosts, /etc/host.conf, /etc/resolv.conf, /etc/profile, /etc/csh.login, /etc/fstab, /etc/networks, /etc/services files (e.g., `https://christcc.org/vcf_download.php?path=%2Fetc%2Fpasswd`)
Server Side Request Forgery (SSRF)	allsaintsphoenix.org	SSRF vulnerability via injection of parameter *url* (e.g., `https://allsaintsphoenix.org/s/cdn/v1.0/i/m?url=http%3A%2F%2Fexternal.url%2Fpage&methods=resize%2C500%2C5000`)

Table 2: Examples of security issues in religious websites.

4.4 Analysis HTTP/HTTPS traffic from religious websites

We analyze the HTTP/HTTPS traffic and characteristic of TLS certificates used in religious websites. We were able to extract 45,004 (72.2%, out of 62,349) websites that use HTTPS; 17,345 requests failed (e.g., because of timeout).

Use of HTTP in religious websites. We found 24 religious websites (out of 62,373, 0.04%) use plain HTTP for communication. HTTP is not secure, and allow adversaries to listen to the traffic sent from these websites, and capture sensitive personal information. We found 14 out of 24 of religious websites that use HTTP, sent personal/sensitive information (first/last names, email address, phone number, address, message/comment, prayer request/confession, date of birth/age, password) of users over the clear; see Table 3 for top-5 religious websites that leak personal/sensitive information over HTTP.

Website	Name	Email	Phone	Address	Message	DOB/Age	Password	PR/Confession
eliotchapel.org	✓	✓	✓	✓		✓	✓	
nbcog.net	✓	✓	✓	✓	✓			
therockchurchla.org	✓	✓	✓		✓			✓
walkatliberty.com	✓	✓			✓		✓	
catholicfamily.net	✓	✓				✓		✓

Table 3: Top-5 religious websites with most leakages of personal/sensitive information over HTTP — DOB = Date of Birth, PR = Prayer Request

Validity period of TLS certificates. Popular browsers (e.g., Google Chrome) have announced in 2020, SSL/TLS certificates cannot be issued for more than 13 months (397 days) [38]. Larger validity periods make it tedious to roll out changes to cryptographic primitives of certificates (e.g., update to a stronger encryption

algorithm) by certificate issuers, and to ensure the trust of an identity (i.e., website's domain). We found 590 (out of 45,004, 1.3%) of the religious websites that use HTTPS have a validity period between 24-28 months in the issued certificates; none of the certificate issuers of these certificates are free certificate authorities — e.g., *Sectigo Limited* (398), *GoDaddy.com, Inc.* (80), *Starfield Technologies, Inc.* (61), *DigiCert Inc* (27).

Analysis of certificate issuers. We observed that the top-5 certificate authorities that issue certificates for the analyzed religious websites are *Let's Encrypt* (29,357/45,004, 65.2%), *cPanel, Inc.* (4996, 11.1%), *Cloudflare, Inc.* (2945, 6.5%), *GoDaddy.com*, Inc. (2416, 5.4%), *DigiCert Inc* (1799, 4%). We also explored the country level distribution of TLS certificate issuing organizations, and found United States (42,618/45,004, 94.7%) and United Kingdom (1724, 3.8%) dominates in the distribution.

TLS certificate signature analysis. We found 41,804 (out of 45,004, 92.9%) of HTTPS religious sites use RSA signature algorithms — i.e., *sha256 with RSA* (41,697), *sha384 with RSA* (106), *sha512 with RSA* (1); all RSA signature algorithms use a pubic key of at least 2048 bits. In addition, 3200 (out of 45,004, 7.1%) HTTPS religious websites use ECDSA (Elliptic Curve Digital Signature Algorithm) signature algorithm — i.e., *ecdsa with SHA256* (2966), *ecdsa with SHA384* (234). The ECDSA signature algorithm uses shorter keys for the same security level as in RSA with larger keys. Although ECDSA is a more efficient signature algorithm, recent studies found it is more vulnerable to attacks [24].

4.5 Third-party tracking scripts

We found 27.9% (17,418/62,373) of religious websites had at least one known tracker on their landing pages, and a total of 359 unique known trackers. We observed popular non-commercial religious websites include commercial trackers on them — e.g., *churchofjesuschrist.org* (a top ranked religious website [39]) included third party scripts from 7 unique commercial tracking domains. The most common known commercial trackers on religious websites were *google-analytics.com* (12,653, 20.3% of websites), *googletagmanager.com* (7064, 11.3%) and *wp.com* (3713, 6%). Religious sites we analyzed, are often developed using WordPress and Squarespace website building services. The scripts included by the former are used for pixel tracking, while the latter use analytics to track users. In addition, the Facebook (*facebook.net*) social media plugin included in religious sites is used to

		Cookie expiry		
Tracker	**#Sites**	**1m-1y**	**1y-5y**	**> 5y**
bidswitch.net	1165	1	1	-
adsrvr.org	686	-	690	-
rlcdn.com	517	4	513	-
id5-sync.com	454	390	-	-
demdex.net	201	402	-	-
statcounter.com	379	-	-	379
casalemedia.com	342	2	343	-
crwdcntrl.net	298	298	-	-
tapad.com	298	296	-	-
eyeota.net	271	-	3	-

Table 4: The top-10 known tracking cookies and their expiry periods (m=month, y=year).

collect information on users' browsing behaviors (e.g., websites and other apps visited), and share this information with other third parties. Furthermore, the PayPal plugin included in religious websites (for online donations) can also be used to track users.

4.6 Third-party tracking cookies

We found 3569/62,373 (5.7%) websites set tracking cookies. The most number of cookies are set by *bidswitch.net* (1165/62,373, 1.9%), *adsrvr.org* (686/62,373, 1.1%) and *rlcdn.com* (514/62,373, 0.01). *Biblehub.com* and *biblegateway.com* are top ranked religious websites [39] that included cookies set by 42 and 16 tracking domains, respectively; a cookie set by *cpmstar.com* (an adware) on *biblehub.com* expires after 20 years. Cookies set by *statcounter.com* (used for web analytics) expires after 5 years; see Table 4. We also found tracking cookies set by center.io on 4 religious websites (*zionbaptistva.com*, *lavendervines.com*, *effect900.com*, *catholicfundraiser.net*) expire in year 9999.

5 Results: Religious Android apps

Static analysis results: Tracking SDKs and exposed Firebase databases. With LibRadar, we found a total of 7398 tracking SDKs (203 unique) on 1454 religious Android apps. We also used LibRadar to check the usage types of these SDKs (e.g., *Google Mobile Services* is used as a development aid, *Google Analytics* is used for mobile analytics). Similar to religious websites, most tracking SDKs in apps were also from Google (1132/1454, 78%) and Facebook (205/1454, 14.1%). Note that Google tracking SDKs are also used for ad and mobile analytics. Although the collection of analytics can help provide a better user experience and improve protection (e.g., fraud detection [40]), it can also be effectively used for tracking/profiling. A notable example is the *com.prayapp* app that embedded 10 tracking SDKs (including Google and Facebook). The app collects personal information (e.g., location, app usage), and apparently, the app owners also purchase data (e.g., gender, age, ethnicity, religious affiliation) from third parties for better profiling [41]; they may also share personal information to third parties (e.g., advertisers) for commercial purposes.

We found 55 (3.8%, 1454) religious Android apps exposed their Firebase databases due to unprotected endpoints; 7 of these apps leaked sensitive information—e.g., user name, password, phone number, email, profile picture, chat details, API key, device type. However, we did not verify/use/store this info (deleted immediately after checking the data types). Notable examples: Vedic Library (*com.hinbook.library*) — an app that supports individual spiritual enhancement (100K+ installs), and Catholic Connect (*com.catholicconnect*) — a social media platform to build and collaborate between Catholic communities (10K+ installs).

Dynamic analysis results. Examples from what we observed from our dynamic analysis include a Christian dating chat app (*cdff.mobileapp*, 1M+ installs), that sent login information via HTTP to a domain owned by the

same owner (*christiandatingforfree.com*). We also found *cdff.mobileapp* and *com.avrpt.teachingsofswamidayananda* sent device information (device ID, device model, device manufacturer, device operating system, screen resolution) over HTTP to *christiandatingforfree.com* and *avrpt.com* domains, respectively (both the apps and corresponding domains are owned by the same party). Such device data can be used to passively track users by fingerprinting their devices.

Session replaying from apps. We found that the UXCam session replay service collected users' location (i.e., GPS coordinates) from the *Tabella Catholic* app. Hotjar and MouseFlow collected fingerprinting information from *Muslim kids* (e.g., device model) and *Buddhist Sangam* (e.g., mouse events) apps, respectively.

Religious apps and 3rd-party domains flagged as malicious. 29/1454 religious apps were flagged as malicious by VirusTotal: one app by 10 engines, eight apps by two engines and 20 apps flagged by one engine. *islamictech.slfgo* (50K+ installations) is flagged as malicious by 10 security engines. 8 apps included the *Android.WIN32.MobiDash.bm* [42] stealthy adware that usually displays ads when the mobile device screen is unlocked. 8 apps contained the *AdLibrary:Generisk* [43] malware that steals information (e.g., Facebook credentials). We also observed calls to two malicious 3rd-party domains by religious apps — *jainpanchang.in* and *orthodoxfacts.org* third party domains were included in *com.mosync.app_Jain_Panchang* (Jain Panchang) and *com.orthodoxfacts* (Orthodox Sayings) religious Android apps, respectively. Jain Panchang requires the *WRITE_SECURE_SETTINGS*[3] Android permission, allowing the app to read/write secure systems settings, which is not supposed to be used by third-party apps.

6 Conclusion

Online religious services raise concerns about user privacy. Information with deeply personal content shared by faith-based communities over online religious services are accessed by various third parties (via tracking scripts/cookies, session replay) that include commercial entities, governments (for surveillance purposes) [7]. As such, adherence to best practices is imperative to safeguard the privacy/security of users; developers need to be vigilant in including third party scripts/libraries in religious websites, and should do proper scanning before using such dependencies. Privacy regulations require personal data used to interact with religious websites to be protected; according to GDPR [44], personal data relating to religious beliefs are deemed sensitive. However, we observed religious online services do not fully comply with these regulations. Proliferation of privacy regulations should drive faith based organization to partner with trusted service providers that comply with industry standards/best practices. In addition, routine risk assessments, audits and inspections of the policies/procedures of religious online services should be carried out by the owners of these services.

[3] `https://tinyurl.com/489ee9xu`

Finally, we note that there are several privacy measurement studies [45–48] that looked into tracking/exposure of sensitive information from online services of different types (e.g., business, government). However, these measurements were done using different tools, environments, techniques and time intervals. Therefore, a naive comparison between the reported findings in these studies and ours is not meaningful, and we leave it as a future work to find a better comparison approach.

References

1. H. Campbell, "Introduction: The rise of the study of digital religion," *Digital religion*, pp. 1–22, 2013.
2. H. A. Campbell, B. Altenhofen, W. Bellar, and K. J. Cho, "There's a religious app for that! A framework for studying religious mobile applications," *Mobile Media & Communication*, vol. 2, no. 2, pp. 154–172, 2014.
3. Pandemic Religion, "Social media use during COVID-19," 2020, https://tinyurl.com/bdfbw3pk.
4. Pew Research Center, "Few Americans say their house of worship is open," 2020, https://tinyurl.com/3ejcj7yr.
5. Forbes, "God is not the only one watching over your church's website," 2014, https://tinyurl.com/5xx5wa5d.
6. CNET, "Religious apps with sinful permissions requests are more common than you think," 2019, https://tinyurl.com/yckme9x3.
7. Los Angeles Times, "Muslims reel over a prayer app that sold user data," 2020, https://tinyurl.com/4edmn96n.
8. BuzzFeed News, "Nothing sacred: These apps reserve the right to sell your prayers," 2022, https://tinyurl.com/3z6jz7wh.
9. The Washington Post, "Chinese state-backed hackers infiltrated vatican," 2020, https://tinyurl.com/mpttxmc.
10. H. A. Campbell, "Religion and the internet: A microcosm for studying internet trends and implications," *New Media & Society*, vol. 15, no. 5, pp. 680–694, 2013.
11. Keywords Standings Ltd., "URL Classification," 2020, https://url-classification.io/.
12. VirusTotal, "VirusTotal," 2021, https://www.virustotal.com.
13. Princeton University, "OpenWPM," 2022, https://github.com/citp/OpenWPM.
14. HTTP Toolkit, "HTTP Toolkit," 2022, https://httptoolkit.tech/.
15. MobSF, "MobSF," 2022, https://tinyurl.com/mr2vwfr4.
16. LiteRadar, "LiteRadar," 2020, https://github.com/pkumza/LiteRadar.
17. S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *ACM CCS'16*, Vienna, Austria, Oct. 2016.
18. N. Samarasinghe, A. Adhikari, M. Mannan, and A. Youssef, "Et tu, brute? Privacy analysis of government websites and mobile apps," in *TheWebConf'22*, 2022.
19. M. G. Hoy and J. Phelps, "Consumer privacy and security protection on church web sites: Reasons for concern," *Journal of Public Policy & Marketing*, vol. 22, no. 1, pp. 58–70, 2003.
20. R. Binns, U. Lyngs, M. Van Kleek, J. Zhao, T. Libert, and N. Shadbolt, "Third party tracking in the mobile ecosystem," in *ACM Conference on Web Science (WebSci'18)*, May 2018.

21. T. T. Nguyen, M. Backes, N. Marnau, and B. Stock, "Share first, ask later (or never?)-studying violations of GDPR's explicit consent in Android apps," in *USENIX Security Symposium (USENIX Security'21)*, Online, Aug. 2021.
22. H. Cho, D. Ippolito, and Y. W. Yu, "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs," *preprint arXiv:2003.11511*, 2020.
23. A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz, "Measuring HTTPS adoption on the web," in *USENIX Security Symposium (USENIX Security'17)*, 2017.
24. A. Alabduljabbar, R. Ma, S. Choi, R. Jang, S. Chen, and D. Mohaisen, "Understanding the security of free content websites by analyzing their ssl certificates: A comparative study," in *Workshop on Cybersecurity and Social Sciences*, 2022.
25. Google-Play-Scraper, "Google-Play-Scraper," 2022, https://tinyurl.com/pm75cxy2.
26. LevelDB, "LevelDB," 2022, https://github.com/google/leveldb.
27. EasyList, "EasyList," 2022, https://easylist.to/.
28. G. Acar, "Script URL substrings used to detect the embeddings from the companies offering session replay services," 2017, https://tinyurl.com/2rhnfbwz.
29. P. Peng, L. Yang, L. Song, and G. Wang, "Opening the blackbox of VirusTotal: Analyzing online phishing scan engines," in *ACM Internet measurement conference (IMC'19)*, 2019.
30. PyOpenSSL, "PyOpenSSL," 2022, https://pypi.org/project/pyOpenSSL/.
31. Wapiti, "Wapiti," 2022, https://wapiti-scanner.github.io/.
32. Google, "Firebase," 2021, https://firebase.google.com/.
33. Mitmproxy, "mitmproxy," 2021, https://mitmproxy.org/.
34. Google, "Android Debug Bridge (adb)," 2020, https://tinyurl.com/2v2a28sc.
35. Monkeyrunner, "monkeyrunner," 2020, https://tinyurl.com/yckz2hyb.
36. PortSwigger, "Burp Suite," 2022, https://portswigger.net/burp.
37. Retire.js, "Retire.js," 2022, https://retirejs.github.io/retire.js/.
38. PKI Consortium, "One Year Certs," 2020, https://tinyurl.com/2p8y8eh4.
39. Similarweb, "Top Websites Ranking for Faith and Beliefs in the world," Online article (2022). https://tinyurl.com/2p9d43jk.
40. OneSpan, "Fraud Analytics," 2021, https://tinyurl.com/muwn78j2.
41. Foundation.mozilla.org, "Pray.com," 2022, https://tinyurl.com/2p8v5bep.
42. Malwarebytes Labs, "Android/Adware.MobiDash," 2022, https://tinyurl.com/2p8kbcpk.
43. 2-viruses.com, "FlyTrap," 2021, https://tinyurl.com/ma7hr3ma.
44. European Commission, "How is data on my religious beliefs/sexual orientation/health/political views protected," 2022, https://tinyurl.com/5cj2fmpt.
45. C. Han, I. Reyes, Á. Feal, J. Reardon, P. Wijesekera, N. Vallina-Rodriguez, A. E. B. On, K. A. Bamberger, and S. Egelman, "The price is (not) right: Comparing privacy in free and paid apps," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, pp. 222 – 242, 2020.
46. D. Cassel, S.-C. Lin, A. Buraggina, W. Wang, A. Zhang, L. Bauer, H.-C. Hsiao, L. Jia, and T. Libert, "OmniCrawl: Comprehensive measurement of web tracking with real desktop and mobile browsers." *Proc. Priv. Enhancing Technol.*, vol. 2022, no. 1, pp. 227–252, 2022.
47. S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *ACM Conference on Computer and Communications Security (CCS'16)*, Vienna, Austria, Oct. 2016.
48. N. Samarasinghe and M. Mannan, "Towards a global perspective on web tracking," *Computers & Security*, vol. 87, p. 101569, 2019.