FamilyLaw DivorceHELP123

DivorceHelp123 Security

Data Protection and Confidential Computing

Abstract

In today's cloud data centers and edge computing, attack surfaces have significantly increased, hacking has become industrialized, and most security control implementations are not coherent or consistent. The principle of any computing security strategy should be securing the platform on which data and workloads will be executed and accessed.

This white paper explains our software and hardware based techniques and technologies that are applied in our platform for security and data protection for our cloud data centers.

Web Vulnerabilities Mitigation

123 utilizes the most up-to-date Angular framework to mitigate all of the following vulnerabilities:

- **Injection**. Injection flaws -- such as SQL, NoSQL, OS, and LDAP injection -- occurs when untrusted data is sent to an interpreter as part of a command or query.
- **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to exploit those flaws to compromise passwords, keys, or session tokens by assuming other users' identities temporarily or permanently.
- **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data such as financial, healthcare, and personally identifiable information (PII). Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection such as encryption at rest or in transit and requires special precautions when exchanged with the browser.
- **XML External Entities**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
- **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access to other users' accounts,

to view sensitive files, to modify other users' data, to change access rights, etc.

- **Security Misconfiguration**. Security misconfiguration is the most commonly seen issue. This is often a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
- **Cross-Site Scripting XSS**. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **Insecure Deserialization**. Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
- **Using Components with Known Vulnerabilities**. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

In addition we take several other measures -- described below -- to provide redundant mitigation of these vulnerabilities.

API Security

In addition to conforming to client side validation best practices, we secure all requests for information on the server side. By validating all of our queries using an ORM we prevent malicious code from being executed on the server side. With the use of personal session tokens we make it harder for any type of identity theft attack, making sure that only the logged in user is the one accessing his information. We authenticate every request to get or update data that the user is authorized to access this data.

Plugins, Wordpress, and Static HTML Websites

All of our website pages are updated with the latest plugins for the best functionality and security. We make sure that all our pages that ask for any kind of information are protected and secured by all the aforementioned steps. We convert our

FamilyLaw.DivorceHelp123 Wordpress website into static HTML before publishing which ensures no vulnerabilities of plugins.

Credit Card Information

DivorceHelp123 does not store your payment information in any of our own databases. We use the services provided by Authorize.net, storing your payment information with them and processing your payments through them, which is the most secure method possible. The following links provide a more detailed description of Authorize.net's security measures: https://www.authorize.net/our-features/secure-customer-data.html https://www.authorize.net/our-features/advanced-fraud-detection.html.

As part of our merchant agreement our payment processor utilizes a service called Trustwave. Trustwave ensures our Payment Card Industry (PCI) compliance is met and remains up-to-date. They provide full audits annually on all of our websites and web applications as well as scans every month. *These scans go much deeper than auditing payment method security.*

Data Transfer

DivorceHelp123 uses HTTPS which combines the Hypertext Transfer Protocol with the Secure SSL/TLS encryption protocol to provide encryption and secure identification of the server, which is a secure process of sending information. We block connections that are not using TLS 1.2 or higher protocol because prior connection protocols have been deemed insecure.

Passwords are passed encrypted between DivorceHelp123 pages via CGI.

Do you use secure transfer protocols for client information and documents via email, or across your company's network?

Work Environment Separation

We use three servers, all AWS RDS, separating environments to reduce risk.

1. One hosts our development environment for our web app.
2. Another hosts our staging & production environments for our web app.
3. The third hosts our websites.

Data Backups

We do backups of our production database every 5 minutes and keep a history of these backups for 15 days. These backups are located at AWS data centers in a low risk

zone.

This helps us in case of emergency and we need to use a recent backup to restore the data, providing:

- Protection from natural disaster and system failure
- Protection from data corruption

How often does your IT department do backups?

What is your plan for disaster or system failure?

Encryption of Data in Database

We utilized the encrypting RDS resources of our MySQL engine. With RDS-encrypted resources, all information that goes through the API is encrypted at the moment of insertion/update in the database, i.e. at rest. This includes the underlying storage for a database (DB) instance, its automated backups, read replicas, and snapshots.

In addition to the RDS encryption we add a second layer of encryption to passwords. We use mcrypt to encrypt user credentials which uses several modern algorithms such as AES. This means that even our technical employees cannot access your credentials to login to the application as you, and therefore cannot access your Firm's or Clients' confidential data.

Workloads

With the increase in adoption of consumer-based cloud services, virtualization has become a necessity in cloud data center infrastructure. Virtualization simulates the hardware that would be needed to resolve the workloads of data by using resources from the cloud. Each workload is isolated from the others so that it has access to only its own resources. Each workload can also be completely encapsulated for portability.

DivorceHelp123 uses Virtual Machines (VMs) that are located in Amazon Web Services (AWS). We may use one or more VMs to accommodate the volume of the data traffic and computing for that day.

Access & Network Security of Our Servers

- Built-in firewalls & other boundary devices:

    - By employing rule sets for server access we minimize the risk of an unauthorized person having access to our servers.
    - 123 utilizes access control lists (ACL) which contain entries that specify an individual user or group rights to specific system objects such as programs, processes, or files.
    - Configuration are applied to enforce the flow of information to specific information system services
- AWS Identity and Access Management (IAM) for AWS Admin Access
    - AWS IAM enables you to implement security best practices, such as least privilege, by granting unique credentials to every user within your AWS Account and only granting permission to access the AWS services and resources required for the users to perform their jobs. AWS IAM is secure by default; new users have no access to AWS until permissions are explicitly granted.
- Virtual Private Cloud (VPC)
    - provides a private subnet within the AWS cloud

How does your IT department secure your access and network?

Is your firm's IT department "up to the task" of providing the security required for your clients' confidential data?

Physical Security

- World-class, highly secure data centers hosted on Amazon Web Services (AWS) servers located in West North Virginia
- Multi-factor access control systems
- Staffed 24x7 by trained security guards
- Access is authorized strictly on a least privileged basis
- Located in low risk zones for natural disaster

How does your firm secure machines that store confidential client data in your office?

Do you permit laptops and phones with client data to leave the office?

Do all of your clients have physical privacy from their spouses for storing confidential paper documents and matter information on their computers?

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by DivorceHelp123.