PrivateBin Testing & Evaluation

Testing & Evaluation Sheet	
PrivateBin	
1. Tool Overview	
Name:	PrivateBin
Category:	Pastebin
Purpose:	Minimalist, open source online pastebin where the server has zero knowledge of pasted data
Date	4/16/25
Status:	Deployed ☑ Operational - Actively running/maintained ☐ In Testing - Currently being evaluated or piloted ☐ Inactive/Deprecated - No longer maintained or functional
Deployment Architecture:	☐ A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server) ☑ A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud) ☑ A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.) **Self hostable but public instance available.** ☐ A service that is hosted by a third party but can also be self-hosted
Version:	1.7.6
2. Installation & Setup	
OS Compatibility	Linux, Windows, macOS, FreeBSD, OpenBSD (Android and iOS are accessible but not officially supported for hosting)

Installation Manual:	Yes
Installation Steps:	1. Open Public Instance: a. https://privatebin.net/ b. macOS/Linux: Open **Terminal**. 2. Self-Host/Deploy: a. Follow the extensive installation guide and configuration guide provided b. https://github.com/PrivateBin/PrivateBin/blob/master/doc/Installation.md#installation c. https://github.com/PrivateBin/PrivateBin/wiki/Configuration
Mention if command-line setup or special configurations are needed	**Public Instance:** ● No command-line setup needed ● No configuration required **Self Host:** ● Basic command-line skills are needed to install and configure PrivateBin on a server (Linux or Windows-based). ● A web server (e.g., Apache or Nginx) ● PHP (since PrivateBin is a PHP app) ● Adjusting settings in config.php (to define things like paste expiration, size limits, file uploads, etc.) ● Optionally configuring HTTPS (recommended)
Common Installation Issues & Fixes:	The FAQ page has extensive list of common errors/issues users face and how to troubleshoot them https://github.com/PrivateBin/PrivateBin/wiki/FAQ
User Documentation:	Yes https://github.com/PrivateBin/PrivateBin/tree/master/doc https://privatebin.info/codedoc/
Required Technical Knowledge	Beginner (If self-hosting, Advanced knowledge)

3. Testing & Evaluation

Category	Details	Score
Operational Functionality:	**Functionality** ● PrivateBin works well for its intended purpose, allowing users to securely store and share text data. There are no major known bugs or broken features reported currently.	4.3

	☐ The tool is mostly non-functional with many broken features and bugs. ☐ Several broken features or bugs ☐ Minor bugs or issues ☐ Mostly functional with few bugs or no bugs ☑ Fully functional with no bugs **Internet Dependence:** ● PrivateBin is a web-based application, so it doesn't function offline and requires an internet connection to interact with the platform. ● Slower 2G and 3G networks should be able to use the service, however depending on network speed and reliability, file uploads or processing may take longer. **Localization & Language Support** ● There are translations and language support for 181 languages including Chinese. ● PrivateBin provides extensive translation instructions. The community also regularly submits improvements via GitHub. **Mobile Accessibility** ● There is no official mobile app. ● PrivateBin is however fully functional in mobile browsers. ● Paste creation, encryption, decryption, and viewing all work via mobile Chrome/Safari/Firefox. ● UI is minimal and responsive, though not optimized like a native app. ● Drag-and-drop file upload may be limited on mobile but works via file picker.	
Usability for Non-Technical Users	**Ease of Installation & Deployment** ● No need to install or deploy as users can use a public instance (already deployed). ● To set up your own instance (deploy) it requires more technical skills and other tools like composer. ● Setup guides, manuals, and FAQ's are well maintained and encouraged to look at before opening issues in repo. ● No time to install as there is a public instance but deploying Private Bin yourself will take anywhere	4.0

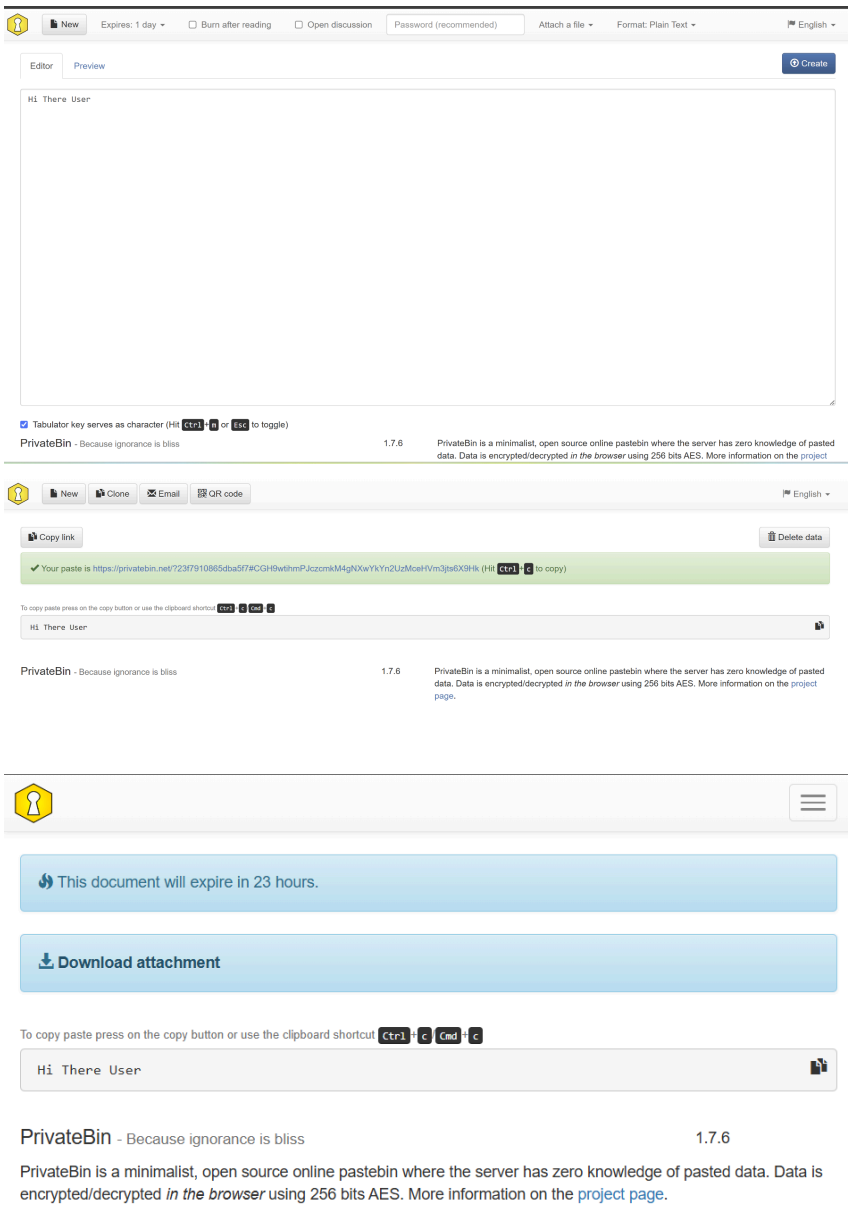
	from 1 hour to multiple hours depending on technical skills. **User Onboarding Experience** ● There are lots of instructions on how to self-host PrivateBin. However, these instructions are still difficult to understand for non-technical users and may require lots of time. ● There is a public instance which combats that issue, providing a public instance of the tool. **Technical Experience Level Required** ● Non-technical users can easily navigate the tool as the user interface for the public instance is intuitive. ● To self host Private Bin it will require more knowledge on PHP applications and hosting services.	
Security & Privacy Strength	**Encryption Standards** ● PrivateBin uses client-side encryption, meaning the data is encrypted in the user's browser before being uploaded to the server. This ensures that the server only stores encrypted data and has no access to the contents. ● Encryption Strength: PrivateBin uses strong encryption algorithms (AES-256) for the encryption of paste data. The encryption key is generated on the client side, and users can also choose to use their own password for additional security. ● Security Protocols: PrivateBin uses HTTPS (SSL/TLS) for secure transmission of data between the client and server, ensuring that data is encrypted in transit and protected against interception. ● Government Censorship: PrivateBin's primary feature—client-side encryption—does not rely on the server to decrypt data. This makes it harder for governments or other entities to access paste data, as they would need to compromise the user's local encryption key. It does not, however, automatically get over censorship or limitations imposed by the government. PrivateBin's accessibility is dependent on the domain's censorship; users might not be able to use the service if the government limits the domain or the server's internet connectivity. **Known Strength resilience**	4.0

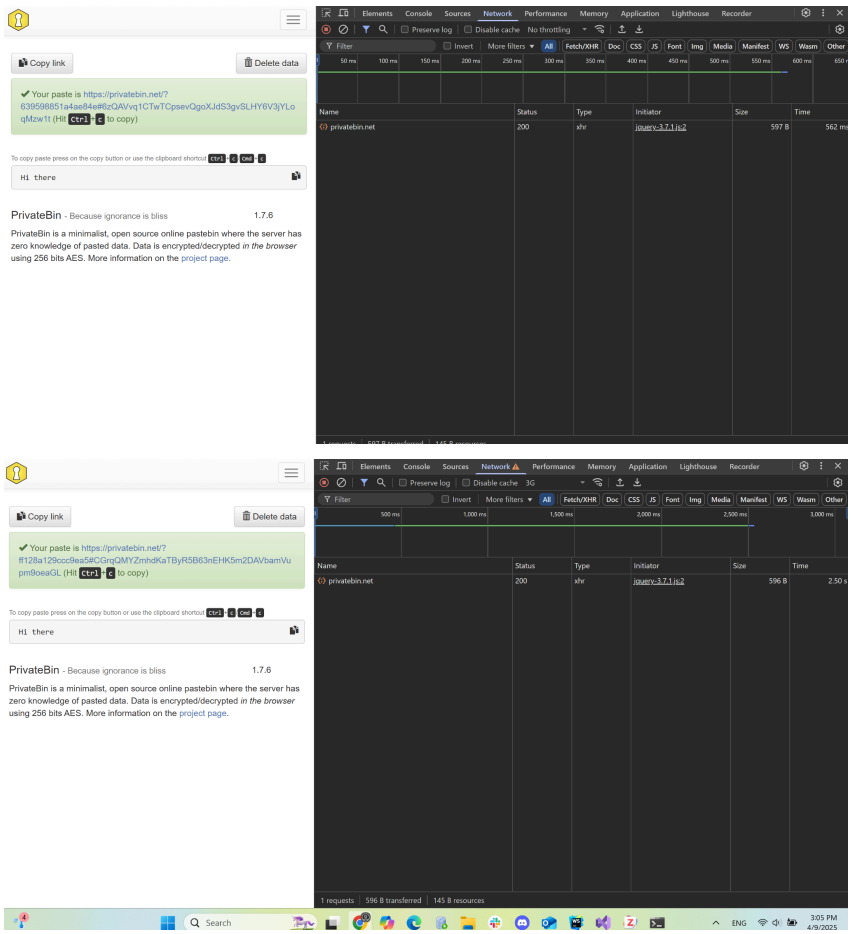
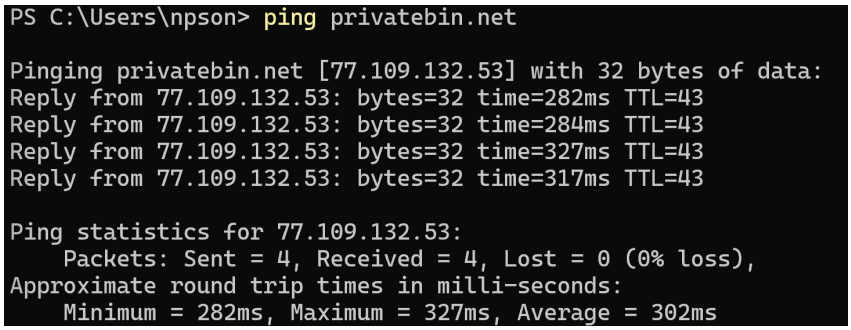
	• Is the tool usable in regions with heavy censorship or surveillance?
	• Partially usable in regions with heavy censorship and surveillance.
	  ○ Client-side encryption ensures content remains private, even if the server is monitored.
	  ○ Access to the server itself (e.g., privatebin.net or your self-hosted instance) can be blocked or monitored in countries with heavy internet controls.
	• Users in censored regions can host PrivateBin locally or access via a VPN/Tor.
	• No built-in circumvention but for higher resilience, instances can be self-hosted on .onion (Tor) services or behind CDNs that mask origin. Also, users can access the public instance https://privatebin.net/ on the Tor browser to make their connection anonymous.
	• There are not any current weaknesses known but there were some in the past.
	• Also the use of URL shorteners in private instances can cause vulnerabilities.
	• Since PrivateBin uses strong encryption and doesn't store data in a readable form, it's resilient against server-side attacks. However, the client-side encryption still depends on the strength of the encryption password and the security of the user's device.
	• There may be vulnerabilities in the web application itself, such as cross-site scripting (XSS) or other browser-based exploits. Regular updates and patches are made to address these issues.
	• Users can report any vulnerabilities they discover by completing a vulnerability report form. https://github.com/PrivateBin/PrivateBin/security
	Comparison with Known Standards
	• PrivateBin is far more secure than conventional pastebin services that don't employ encryption. PrivateBin delivers a comparable level of security to existing encrypted paste services (like PasteBin or ZeroBin), but it is more visible and open-source, which fosters better trust in it.
	• PrivateBin follows industry standards for security by using HTTPS and mainstream encryption standards	

	(AES-256). The complete dependence on client-side encryption is the primary distinction. **Data Minimization** ● Private Bin only collects necessary data and the paste (text/file) is encrypted before being uploaded. ● Users also do not need to create an account and this helps them avoid tracking or being profiled. **Privacy Policy Accessibility and Clarity** ● PrivateBin's privacy policy is straightforward, indicating that it does not store any personal data and does not track users. However, there is not a clearly written document detailing its policy as the responsibility for creating and displaying a privacy policy lies with the administrator of each individual PrivateBin instance.	
Maintenance/Sustainability	**Community support** ● PrivateBin has a community that is relatively active and large. The community mainly consists of privacy-conscious individuals, developers, and open-source advocates. The community engages via GitHub discussions, issue tracking, and other open-source forums. ● Users can seek help from the community through GitHub issues, open-source forums, submitting vulnerability form, or by reading documentation. **Development active status** ● PrivateBin is actively maintained, with regular contributions from its developers and the open-source community. The development status can be tracked via its GitHub repository, where contributors regularly add new features, fix bugs, and update the project to address security vulnerabilities. ● Updates happen often, although not always at the same time. The frequency of updates is determined by whether vulnerabilities, new features, or community-requested enhancements are found. Security updates and patches are often handled promptly. ● The development team is relatively responsive to issues and pull requests on GitHub. If a security vulnerability is discovered, it is typically addressed swiftly, and users can also report them as well.	4.3

	Funding and Sponsorship ● Limited information about the funding for Private Bin and have no known sponsorships. ● It is primarily supported by community contributors.	
Performance / Effectiveness & Reliability	**Testing Environment Setup:** ● **Device:** Dell XPS 15 ● **OS:** Windows ● **Network:** 4G **User Experience Observations** ● PrivateBin felt pretty smooth and easy to use. Installation was not required and the tool was intuitive to use. ● The tool was highly responsive during normal use with no lag observed. **Speed & Responsiveness:** ● It took about 560 ms to upload and encrypt minimal text + a large file in the pastebin at 4G. It took about 2.5 seconds on 3G for the same content. ● Does not work offline. **Resource Usage:** ● When measuring CPU and Memory usage for same content from speed & responsiveness, there was negligible CPU or Memory usage. **Network Performance:** ● Latency: PrivateBin has relatively low latency (time it takes a packet of data to travel from computer to the target server and back) at about <100 ms but even with lots of extensive programs running and memory usage, it averages ~300ms as seen in Figure 3. **Reliability** ● PrivateBin is open-source and has been peer-reviewed by the community. It is actively maintained on GitHub, and its encryption practices have been validated by security experts. ● Given its open-source nature and reliance on strong encryption algorithms like AES-256, it benefits from scrutiny by security researchers and privacy advocates as there are currently 130 contributors.	4.5
Deployment Considerations:	**Open Source & Transparency:** ● PrivateBin is fully open-source and the code is available on GitHub. This allows anyone to	

	independently verify and audit the code, ensuring transparency and trust. ● GitHub Repository: PrivateBin GitHub **Cloud vs. Local Deployment:** ● Although PrivateBin is not dependent on any one cloud service provider, it may be set up on cloud services like AWS or Azure. Any server can host the service on its own. ● PrivateBin can also be deployed locally on private servers, making it a great solution for CSOs with specific security requirements who wish to keep all data and infrastructure within their control. **Dependencies:** ● The deployment requires basic server software (such as Apache or Nginx) and PHP to run. It's designed to be easy to set up with minimal dependencies (instructions and guides provided). ● With extremely few dependencies, PrivateBin is a simple service. For server-side functions, PHP and Apache/Nginx are required. Since no database is needed, deployment and management are simple. **Post-Deployment Maintenance** ● Once deployed, PrivateBin is easy to maintain. ● Developers can freely fork the project, customize it (easy to modify), and deploy their version. **Merge/Sustainability:** ● Contributions to the main repository are encouraged. Users can submit pull requests for bug fixes, security patches, or feature additions.	
4. Testing Scenarios		

Sending Text/File using PrivateBin	 *Figure 1*: Above images show the process in which text and/or file can be sent through PrivateBin across devices.

Testing Speed & Responsiveness of PrivateBin	 *Figure 2*: Testing the speed and responsiveness of PrivateBin using the same payload/content using 4G(first image) and 3G(second image).
Testing Network Performance of PrivateBin	 *Figure 3*: Network performance of PrivateBin with extensive programs concurrently running on device. This is a measure of latency, which is the delay between sending a request and receiving a response.
5. Insights & Recommendations	
Key Findings	**Strengths:**

	● End-to-end encryption by default ensures that even the server cannot read the content of the pastes. ● No need to deploy as there is a public instance running. ● No IP logging or metadata storage, which reduces surveillance risk. ● Do not need an account which protects user identities. **Weaknesses:** ● Requires some familiarity with server configuration and web hosting to deploy. ● While functional, the interface may not be intuitive for all non-technical users.
Suggested Improvements	Add tooltips or help buttons to explain encryption options, expiration settings, and burn-after-read.
Alternative Tools:	● Paaster ● ProtectedText
License	Free and open-source (zlib/libpng license)
Cost/Resource Implications	**Total Cost of Ownership:** ● Time to Deploy: A few hours if technical staff is available; longer for first-timers. ● Hosting requires a server (e.g., VPS), which can range from $5–$20/month depending on traffic.
Why is this useful to civil societies in authoritarian environments?	Civil society organizations would find PrivateBin useful by offering a secure and anonymous method of communication. This can be valuable for those working in sensitive environments, particularly those advocating for human rights, privacy, and freedom of expression. Also it can protect whistleblowers and give them a safe way to share sensitive documents without revealing identity or location. Furthermore, PrivateBin can be integrated into a broader CSO digital security toolkit and be more adaptable. For example, a labor rights group in Tibet could use a self-hosted PrivateBin instance to safely exchange updates without fear of exposing names or locations, even if their server is seized. Similarly, a journalist in Hong Kong might use PrivateBin over Tor to publish links to sensitive leaked documents, ensuring both their sources' safety and their own anonymity. In regions with heavy censorship, access to public instances may be blocked by national firewalls such as the Great Firewall. However, PrivateBin remains usable via circumvention tools like Tor, or by

	self-hosting on internal networks or .onion services. Self hosting PrivateBin would give CSOs more control over their own security model and infrastructure.