How to Mask Sensitive Data in Logs

https://campus.barracuda.com/doc/4259965/

Data masking security of the Barracuda Web Application Firewall obscures sensitive data elements before logging them. Configured parameters like social security numbers, credit card information, or other proprietary data in the URL parameters of a request can be protected from unauthorized exposure in the logs. Data masking is configured for an application using parameter names to specify sensitive data. Logged data appears in **BASIC > Access Logs**, with the sensitive data overwritten by '*X*'es**.**

- Masking cannot be applied to sensitive data in custom parameters or custom headers.
- Once masked, the original data cannot be retrieved, recovered, or restored.

Configure Data Masking

---

1. Go to the **WEBSITES > Advanced Security** page, **Mask Sensitive Data In Logs** section.
2. Click **Edit** next to the service for which masking is necessary.
3. In the **Mask Sensitive Data** window, enter the names of sensitive parameters. You can provide multiple parameter names separated by commas with no spaces between. Example: cardId,securityNumber,password
   You can use the asterisk (*) wildcard character to mask all parameters in the URL.
4. Click **Save**.