Cookie Security

https://campus.barracuda.com/doc/76284727/

Cookies provide a mechanism to store session state information on client navigation platforms, such as browsers and other user agents. Cookies can store user preferences or shopping cart items and can include sensitive information like registration or login credentials. If a cookie is modified, the system can become vulnerable to attacks and sensitive information can be stolen.

How Cookie Security Works

Cookie Security in Barracuda WAF-as-a-Service is transparent to back-end servers. When a server inserts a cookie, Barracuda WAF as a Service intercepts the response and encrypts or signs the cookie before delivering it to the client. When a subsequent request from the client returns this cookie, the system intercepts the request and decrypts it or verifies its signature.

- If the cookie is *unaltered*, Barracuda WAF-as-a-Service forwards the original cookie to the server.
- If the cookie *has been altered*, Barracuda WAF-as-a-Service removes it before forwarding the request to the server.

Encryption prevents both viewing and tampering with cookies, so it prevents the client from accessing cookie values. If you have clients who need to access cookie values, use *signing* to allow this access. When signing cookies, Barracuda WAF-as-a-Service forwards *two* cookies to the client browser – one plain text cookie and one signed cookie. When a subsequent request from the client returns the cookies, if *either* cookie is altered, signature verification fails, and Barracuda WAF-as-a-Service removes both cookies before forwarding the request to the server.

Encrypting a cookie may change the length of the cookie, but the number of headers in the message remains unchanged. When a cookie is signed, the length of the cookie changes and one or more headers is appended to the forwarded message. If the Request Limits component specifies constraints on the number or length of HTTP headers, a signed or encrypted cookie may violate the request limits and result in unwanted rejection of messages. Messages rejected for this reason are logged as ***Cloak*** under **Action** on the **Firewall Logs** page.