Spoof an Authentication Cookie

Monday, November 6, 2017 9:41 PM

- Many applications will automatically log a user into their site if the right authentication cookie is specified
- Sometimes the cookie values can be guessed if the algorithm for generating the cookie can be obtained
- Sometimes the cookies are left on the client machine and can be stolen by exploiting another system vulnerability
- Sometimes the cookies may be intercepted using XSS

Solution:

- Upon inspection of the cookies, we find that the first part of the cookies are the same
- The last part is just the username reversed and the letters shifted ahead by one letter in the alphabet

- Login as alice
- Intercept your login request using Webscarab
- Inject into the cookie value in the header

; AuthCookie=65432fdjmb