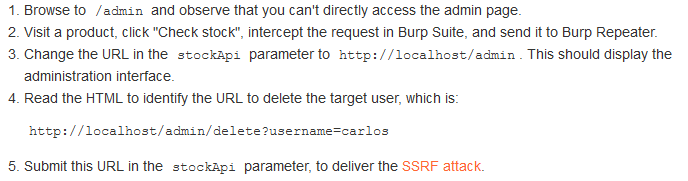
Server-Side Request Forgery

A picture containing diagram

Description automatically generated

This could bring us to the admin panel which we could then view and capture requests for various actions that require admin privs to perform. Once we capture the URLs for these actions, we can feed the new URL back into the stock api to execute it. See the example below.

Ex:

Display admin page, capture admin functionality, add the new functionality to the localhost URL to perform that action via localhost and win.

Text

Description automatically generated We can use a fuzzer to scan for IPs of backend machines related to the server were attacking. Capture the IPs using ASN or Dns lookups, figure out the subnet or a subnet and start to fuzz around looking for alive systems.

Often admin panels will allow unauthenticated users from within their local network to access admin functionality.

Graphical user interface, text, application, email

Description automatically generatedOne of the most important parts of this section right here. These are some obfuscation methods to find these vulnerabilities.

Again encoding payloads is also a necessary part of this. See the example below for a cool example.

To double encode lettersText

Description automatically generated use the hackvertor burp extension. Use 2 sets of the url encode tags for a double encoding.

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Example below:

Graphical user interface, text, application, email

Description automatically generatedLook for API calls and URLs referenced by the application.