# X-Parent-Control
# 父页面控制协议

谢继雷

∞ 海宁小蜜蜂软件

November 6, 2010

**Abstract**

X-Parent-Control 协议用于在 AJAX 请求中，实现由内部页面向外部传递异常的机制。目前 X-Parent-Control 实现了两种控制：父页面重定向与父页面脚本调用。

## Contents



## 1 协议头

X-Parent-Control 协议向 HTTP 返回报文中添加了以下字段：（见 Table 1）

Table 1: X-Parent-Control 头列表

| 协议头 | 描述 | 格式 |
|---|---|---|
| X-Parent-Control | X-Parent-Control 版本 | 1.0 |
| X-Parent-Location | 父页面重定向 | 相对或绝对 URL |
| X-Parent-Invoke | 父页面脚本调用 | JavaScript 脚本 |
| X-Parent-Auth | 控制验证授权码 | URL 或 Javascript 的 HMAC 字符串 |

## 2 父页面重定向

| |
|---|
| X-Parent-Control: 1.0<br>X-Parent-Location: *URL-Spec*<br>X-Parent-Auth: HMAC( *URL-Spec* ) |

*URL-Spec* 可以是绝对 URL 或相对于当前父页面地址的相对 URL。当父页面收到 X-Parent-Control 控制时，应该使用 HTML4 DOM 模型的 location.href = *URL-Spec* 来解释。

安全措施： `X-Parent-Location` 必须验证。MITM 攻击中，入侵者篡改内部页面，插入 HTTP `Location` (301) 重定向头，可以使内部页面重定向到非法内容。但父页面决定如何解释内部页面的数据。如果入侵者插入非法 `X-Parent-Location` 值，则可能导致非法的跨站请求。

## 3 父页面脚本调用

| |
|---|
| X-Parent-Control: 1.0<br>X-Parent-Invoke: *JavaScript*<br>X-Parent-Auth: HMAC( *JavaScript*) |

其中 *JavaScript* 指定要执行的脚本。该脚本通过 JavaScript `eval` 的方法被求值。

安全措施： `X-Parent-Invoke` 必须验证。理由是显而易见的。

## 4 验证算法

为了防止恶意代码注入，在返回的控制信息中必须附加验证码。目前为了简化起见，只使用了随机数，并用下列方式实现密钥分享，在真正应用中这是不安全的。将来改变这一算法应不影响程序结构。

1. Parent 生成随機數 $secret$，计算 $E = 9 * secret^2 + 102 * secret + 57$，发送 $E$ 给远程.
2. 远程计算 $secret = \dfrac{\sqrt{E - 232} - 17}{3}$
3. 远程计算 $H = hmac(secret, message)$，作为 HMAC 验证码
4. 远程将 HMAC 附加到 X-Parent-Control HTTP 报文上
5. Parent 收到 $message$，重新计算 $H$ 并核对，如果 $H$ 错误则丢弃控制信息。

验证使用如下 HMAC 算法 [2]：

$$K = sha1(string(k))$$
$$hmac(K, m) = sha1((K \oplus opad) \parallel sha1((K \oplus ipad) \parallel m))$$
$$opad = 50_{16}$$
$$ipad = 36_{16}$$

## 5 使用

下图描述了 X-Parent-Control 的典型用法：（其中 *斜体* 部分为验证相关，目前可暂时缺省）

### 5.1 父页面

1. include jquery-min.js;
2. include jquery.sha1.js;

3. include jquery.ajaxex.js;
4. *sessionSecret = secret = RANDOM;*
5. *E = 9*secret*secret + 102*secret + 57;*
6. Xxx.load(AJAX-URL... *&e=E* );

### 5.2 AJAX 请求

1. import ParentControl;
2. *E = request.getParameter("e");*
3. *secret = (Math.sqrt(E - 232) - 17) / 3;*
4. ParentControl.sendParentRedirect(response, "new-location..." , *secret* );

## A 实现参考

引用 [1] 以启用父页面控制扩展。
Servlet 支持类参考 [3]。

## References


[1] Lenik. jquery ajax 父页面控制扩展, 2010. `http://track.secca-project.com/projects/stack/browser/sems/trunk/archetype/type-ublock-webapp/src/main/webapp/js/jquery.ajaxex.js`.

[2] Lenik. Parent-auth hmac 算法, 2010. `http://track.secca-project.com/projects/stack/browser/sems/trunk/modules/EBC/ebc-dev/src/main/java/com/seccaproject/sems/ajax/HMAC.java`.

[3] Lenik. X-Parent-Control 支持类, 2010. `http://track.secca-project.com/projects/stack/browser/sems/trunk/modules/EBC/ebc-dev/src/main/java/com/seccaproject/sems/ajax/ParentControl.java`.


## B 索引

## List of Tables