# EdgeGallery R0.9 安全渗透测试结果

## EG-TST-SEC-001

登入EdgeGallery容器，使用LinEnum.sh脚本对容器中的用户/文件权限进行检查，检查结果如下：

### 测试结果：通过

## EG-TST-SEC-002

使用OWASP ZAP对EdgeGallery平台进行扫描，扫描结果如下：

### Summary of Alerts

|  |  |
| --- | --- |
| **Risk Level** | **Number of Alerts** |
| [High](C:/Users/Administrator/Desktop/owasp%20zap.html#high) | 0 |
| [Medium](C:/Users/Administrator/Desktop/owasp%20zap.html#medium) | 1 |
| [Low](C:/Users/Administrator/Desktop/owasp%20zap.html#low) | 4 |
| [Informational](C:/Users/Administrator/Desktop/owasp%20zap.html#info) | 5 |

### Alert Detail

|  |  |
| --- | --- |
| **Medium (Medium)** | **Proxy Disclosure** |
| Description | 1 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine  - A list of targets for an attack against the application.  - Potential vulnerabilities on the proxy servers that service the application.  - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Attack | TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. |
| URL | https://{host}:30091/login |
| Method | GET |
| Attack | TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method. |
| Instances | 2 |
| Solution | Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server.  Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing).  Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages.  Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers. |
| Other information | Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server:  - Unknown  The following web/application server has been identified:  - Unknown |
|  | |
| Reference | https://tools.ietf.org/html/rfc7231#section-5.1.2 |
| CWE Id | 200 |
| WASC Id | 45 |
| Source ID | 1 |

|  |  |
| --- | --- |
| **Low (Medium)** | **Cookie Without SameSite Attribute** |
| Description | A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks. |
|  | |
| URL | https://{host}:30067/oauth/authorize?client\_id=appstore-fe&redirect\_uri=https://{host}:30091/login&response\_type=code&state=oezF94 |
| Method | GET |
| Parameter | AUTHSERVERSESSIONID |
| Evidence | Set-Cookie: AUTHSERVERSESSIONID |
| Instances | 1 |
| Solution | Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies. |
| Reference | https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site |
| CWE Id | 16 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Low (Medium)** | **Cookie Without SameSite Attribute** |
| Description | A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | XSRF-TOKEN |
| Evidence | Set-Cookie: XSRF-TOKEN |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | APPSTORESESSIONID |
| Evidence | Set-Cookie: APPSTORESESSIONID |
| Instances | 2 |
| Solution | Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies. |
| Reference | https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site |
| CWE Id | 16 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Low (Medium)** | **Cookie No HttpOnly Flag** |
| Description | A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | XSRF-TOKEN |
| Evidence | Set-Cookie: XSRF-TOKEN |
| Instances | 1 |
| Solution | Ensure that the HttpOnly flag is set for all cookies. |
| Reference | http://www.owasp.org/index.php/HttpOnly |
| CWE Id | 16 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Low (Low)** | **Cookie Slack Detector** |
| Description | Repeated GET requests: drop a different cookie each time, followed by normal request with all cookies to stabilize session, compare responses against original baseline GET. This can reveal areas where cookie based authentication/attributes are not actually enforced. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| URL | https://{host}:30091/login |
| Method | GET |
| Instances | 2 |
| Solution |  |
| Other information | NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [APPSTORESESSIONID]  NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [AUTHSERVERSESSIONID]  Cookies that don't have expected effects can reveal flaws in application logic. In the worst case, this can reveal where authentication via cookie token(s) is not actually enforced.  These cookies affected the response:  These cookies did NOT affect the response: AUTHSERVERSESSIONID,XSRF-TOKEN,APPSTORESESSIONID |
|  | |
| Reference | http://projects.webappsec.org/Fingerprinting |
| CWE Id | 200 |
| WASC Id | 45 |
| Source ID | 1 |

|  |  |
| --- | --- |
| **Informational (Medium)** | **User Agent Fuzzer** |
| Description | Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3\_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| URL | https://{host}:30091/ |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3\_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| URL | https://{host}:30091/login |
| Method | GET |
| Parameter | Header User-Agent |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Instances | 14 |
| Solution |  |
| Reference | https://owasp.org/wstg |
| Source ID | 1 |

|  |  |
| --- | --- |
| **Informational (Low)** | **Timestamp Disclosure - Unix** |
| Description | A timestamp was disclosed by the application/web server - Unix |
|  | |
| URL | https://{host}:30067/js/chunk-35bc1722.02683615.js |
| Method | GET |
| Evidence | 02683615 |
| URL | https://{host}:30067/ |
| Method | GET |
| Evidence | 02683615 |
| URL | https://{host}:30067/js/app.b5aadec0.js |
| Method | GET |
| Evidence | 02683615 |
| URL | https://{host}:30067/js/chunk-vendors.36705334.js |
| Method | GET |
| Evidence | 36705334 |
| URL | https://{host}:30067/ |
| Method | GET |
| Evidence | 36705334 |
| URL | https://{host}:30067/js/chunk-vendors.36705334.js |
| Method | GET |
| Evidence | 2147483647 |
| Instances | 6 |
| Solution | Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns. |
| Other information | 02683615, which evaluates to: 1970-02-01 09:26:55 |
|  | |
| Reference | http://projects.webappsec.org/w/page/13246936/Information%20Leakage |
| CWE Id | 200 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Informational (Low)** | **Information Disclosure - Suspicious Comments** |
| Description | The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments. |
|  | |
| URL | https://{host}:30067/js/chunk-2712a8fd.fa76c025.js |
| Method | GET |
| URL | https://{host}:30067/js/chunk-35bc1722.02683615.js |
| Method | GET |
| URL | https://{host}:30067/js/chunk-vendors.36705334.js |
| Method | GET |
| URL | https://{host}:30067/js/app.b5aadec0.js |
| Method | GET |
| URL | https://{host}:30067/js/chunk-3e369268.9a2fbb0b.js |
| Method | GET |
| Instances | 5 |
| Solution | Remove all comments that return information that may help an attacker and fix any underlying problems they refer to. |
| Other information | The following comment/snippet was identified via the pattern: \bUSERNAME\b  (window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-2712a8fd"],{1276:function(t,e,n){"use strict";var r=n("d784"),i=n("44e7"),s=n("825a"),a=n("1d80"),o=n("4840"),u=n("8aa5"),c=n("50c4"),l=n("14c3"),f=n("9263"),d=n("d039"),p=[].push,g=Math.min,v=4294967295,h=!d((function(){return!RegExp(v,"y")}));r("split",2,(function(t,e,n){var r;return r="c"=="abbc".split(/(b)\*/)[1]||4!="test".split(/(?:)/,-1).length||2!="ab".split(/(?:ab)\*/).length||4!=".".split(/(.?)(.?)/).length||".".split(/()()/).length>1||"".split(/.?/).length?function(t,n){var r=String(a(this)),s=void 0===n?v:n>>>0;if(0===s)return[];if(void 0===t)return[r];if(!i(t))return e.call(r,t,s);var o,u,c,l=[],d=(t.ignoreCase?"i":"")+(t.multiline?"m":"")+(t.unicode?"u":"")+(t.sticky?"y":""),g=0,h=new RegExp(t.source,d+"g");while(o=f.call(h,r)){if(u=h.lastIndex,u>g&&(l.push(r.slice(g,o.index)),o.length>1&&o.index<r.length&&p.apply(l,o.slice(1)),c=o[0].length,g=u,l.length>=s))break;h.lastIndex===o.index&&h.lastIndex++}return g===r.length?!c&&h.test("")||l.push(""):l.push(r.slice(g)),l.length>s?l.slice(0,s):l}:"0".split(void 0,0).length?function(t,n){return void 0===t&&0===n?[]:e.call(this,t,n)}:e,[function(e,n){var i=a(this),s=void 0==e?void 0:e[t];return void 0!==s?s.call(e,i,n):r.call(String(i),e,n)},function(t,i){var a=n(r,t,this,i,r!==e);if(a.done)return a.value;var f=s(t),d=String(this),p=o(f,RegExp),m=f.unicode,x=(f.ignoreCase?"i":"")+(f.multiline?"m":"")+(f.unicode?"u":"")+(h?"y":"g"),y=new p(h?f:"^(?:"+f.source+")",x),b=void 0===i?v:i>>>0;if(0===b)return[];if(0===d.length)return null===l(y,d)?[d]:[];var S=0,w=0,E=[];while(w<d.length){y.lastIndex=h?w:0;var R,\_=l(y,h?d:d.slice(w));if(null===\_||(R=g(c(y.lastIndex+(h?0:w)),d.length))===S)w=u(d,w,m);else{if(E.push(d.slice(S,w)),E.length===b)return E;for(var I=1;I<=\_.length-1;I++)if(E.push(\_[I]),E.length===b)return E;w=S=R}}return E.push(d.slice(S)),E}]}),!h)},"14c3":function(t,e,n){var r=n("c6b6"),i=n("9263");t.exports=function(t,e){var n=t.exec;if("function"===typeof n){var s=n.call(t,e);if("object"!==typeof s)throw TypeError("RegExp exec method returned something other than an Object or null");return s}if("RegExp"!==r(t))throw TypeError("RegExp#exec called on incompatible receiver");return i.call(t,e)}},"25f0":function(t,e,n){"use strict";var r=n("6eeb"),i=n("825a"),s=n("d039"),a=n("ad6d"),o="toString",u=RegExp.prototype,c=u[o],l=s((function(){return"/a/b"!=c.call({source:"a",flags:"b"})})),f=c.name!=o;(l||f)&&r(RegExp.prototype,o,(function(){var t=i(this),e=String(t.source),n=t.flags,r=String(void 0===n&&t instanceof RegExp&&!("flags"in u)?a.call(t):n);return"/"+e+"/"+r}),{unsafe:!0})},"2a22":function(t,e,n){"use strict";n.r(e);var r=function(){var t=this,e=t.$createElement,n=t.\_self.\_c||e;return n("div",{staticClass:"login"},[n("div",{staticClass:"loginBox"},[n("div",{staticClass:"login-area"},[n("p",{staticClass:"login-top"},[t.\_v(" "+t.\_s(t.$t("login.loginWithUser"))+" ")]),n("el-input",{attrs:{id:"uname",type:"text",placeholder:t.$t("login.namePla")},model:{value:t.userData.username,callback:function(e){t.$set(t.userData,"username",e)},expression:"userData.username"}}),n("el-input",{attrs:{id:"upass",type:"password",placeholder:t.$t("login.pwdPla")},model:{value:t.userData.password,callback:function(e){t.$set(t.userData,"password",e)},expression:"userData.password"}})],1),n("div",{staticClass:"login-btn"},[n("verify",{attrs:{"success-fun":t.success,"error-fun":t.error,"verify-status":t.verifyStatus}})],1),n("div",{staticClass:"login-btn"},[n("el-button",{attrs:{id:"loginBtn",type:"primary",size:"medium",loading:t.loginBtnLoading},on:{click:function(e){return t.submitForm()}}},[t.\_v(" "+t.\_s(t.$t("login.login"))+" ")])],1),n("div",{staticClass:"login-tips rt"},[n("el-button",{attrs:{type:"text"},on:{click:function(e){return t.jumpTo("/mecm/register")}}},[t.\_v(" "+t.\_s(t.$t("login.freeSign"))+" ")]),this.enableSms?n("el-divider",{attrs:{direction:"vertical"}}):t.\_e(),this.enableSms?n("el-button",{attrs:{type:"text"},on:{click:function(e){return t.jumpTo("/mecm/getPwd")}}},[t.\_v(" "+t.\_s(t.$t("login.forgotPwd"))+" ")]):t.\_e()],1)])])},i=[],s=(n("4160"),n("c975"),n("b64b"),n("4d63"),n("ac1f"),n("25f0"),n("466d"),n("1276"),n("159b"),function(){var t=this,e=t.$createElement,n=t.\_self.\_c||e;return n("div",{staticClass:"verifyCom"},[n("div",{staticClass:"verify-box",class:t.sliderStatus?"success":""},[n("em",{ref:"btn",class:t.sliderStatus?t.successIcon:t.startIcon,on:{mousedown:t.moveSlider}}),n("span",{directives:[{name:"show",rawName:"v-show",value:t.sliderStatus,expression:"sliderStatus"}]},[t.\_v(t.\_s(t.$t("login.finishVerify")))]),n("span",{directives:[{name:"show",rawName:"v-show",value:!t.sliderStatus,expression:"!sliderStatus"}]},[t.\_v(t.\_s(t.$t("login.verify")))])])])}),a=[],o={props:{successFun:{type:Function,default:function(){}},successIcon:{type:String,default:"el-icon-success"},startIcon:{type:String,default:"el-icon-d-arrow-right"},errorFun:{type:Function,default:function(){}},verifyStatus:{type:Boolean,default:!1}},data:function(){return{disX:0,sliderStatus:!1}},watch:{verifyStatus:function(t){t||(this.$refs.btn.style.transition=".5s all",this.$refs.btn.style.transform="translateX(0)",this.sliderStatus=!1,this.errorFun&&this.errorFun())}},methods:{moveSlider:function(t){var e=this,n=t.target,r=t.clientX,i=n.offsetWidth,s=n.parentElement.offsetWidth,a=s-i;if(this.sliderStatus)return!1;document.onmousemove=function(t){var s=t.clientX;e.disX=s-r,e.disX<=0&&(e.disX=0),e.disX>=a-i&&(e.disX=a),n.style.transition=".1s all",n.style.transform="translateX("+e.disX+"px)",t.preventDefault()},document.onmouseup=function(){e.disX!==a?(n.style.transition=".5s all",n.style.transform="translateX(0)",e.errorFun&&e.errorFun()):(e.sliderStatus=!0,e.successFun&&e.successFun()),document.onmousemove=null,document.onmouseup=null}}}},u=o,c=(n("4374"),n("2877")),l=Object(c["a"])(u,s,a,!1,null,"706e775a",null),f=l.exports,d=n("af47"),p={name:"",components:{Verify:f},data:function(){return{userData:{username:"",password:""},loginBtnLoading:!1,verifyStatus:!1,returnUrl:"",enableSms:""}},created:function(){this.keyupSubmit()},mounted:function(){if(window.location.href.indexOf("return\_to=")>-1){this.returnUrl=this.getQueryString("return\_to"),this.enableSms=this.getQueryString("enable\_sms"),this.enableSms.indexOf("true")>-1?this.enableSms=!0:this.enableSms=!1;var t={return\_url:this.returnUrl,enable\_sms:this.enableSms,login\_url:window.location.href.split("#")[1]};sessionStorage.setItem("obj",JSON.stringify(t))}},methods:{success:function(){this.verifyStatus=!0},error:function(){this.verifyStatus=!1},getQueryString:function(t){var e=new RegExp("(^|&)"+t+"=([^&]\*)(&|$)","i"),n=window.location.href.split("?")[1].substr(0).match(e);return null!=n?decodeURIComponent(n[2]):null},submitForm:function(){var t=this;if(this.verifyStatus){this.loginBtnLoading=!0;var e=new FormData;Object.keys(this.userData).forEach((function(n){e.append(n,t.userData[n])}));var n={"Content-Type":"multipart/form-data","X-XSRF-TOKEN":this.$cookies.get("XSRF-TOKEN")};d["a"].login(e,n).then((function(t){window.location.href=decodeURIComponent(JSON.parse(sessionStorage.getItem("obj")).return\_url)})).catch((function(e){if(t.verifyStatus=!1,t.loginBtnLoading=!1,e&&e.response){switch(e.response.status){case 400:e.message="Bad request";break;case 401:e.message=t.$t("login.loginFail");break}t.$message.error(e.message)}}))}else this.$message.error(this.$t("tip.wrongCaptcha"))},keyupSubmit:function(){var t=this;document.onkeydown=function(e){var n=window.event.keyCode;13===n&&t.submitForm()}},jumpTo:function(t){this.$router.push(t)}}},g=p,v=(n("eb4e"),Object(c["a"])(g,r,i,!1,null,null,null));e["default"]=v.exports},"3fc9":function(t,e,n){},4374:function(t,e,n){"use strict";var r=n("3fc9"),i=n.n(r);i.a},"44e7":function(t,e,n){var r=n("861d"),i=n("c6b6"),s=n("b622"),a=s("match");t.exports=function(t){var e;return r(t)&&(void 0!==(e=t[a])?!!e:"RegExp"==i(t))}},"466d":function(t,e,n){"use strict";var r=n("d784"),i=n("825a"),s=n("50c4"),a=n("1d80"),o=n("8aa5"),u=n("14c3");r("match",1,(function(t,e,n){return[function(e){var n=a(this),r=void 0==e?void 0:e[t];return void 0!==r?r.call(e,n):new RegExp(e)[t](String(n))},function(t){var r=n(e,t,this);if(r.done)return r.value;var a=i(t),c=String(this);if(!a.global)return u(a,c);var l=a.unicode;a.lastIndex=0;var f,d=[],p=0;while(null!==(f=u(a,c))){var g=String(f[0]);d[p]=g,""===g&&(a.lastIndex=o(c,s(a.lastIndex),l)),p++}return 0===p?null:d}]}))},"4d63":function(t,e,n){var r=n("83ab"),i=n("da84"),s=n("94ca"),a=n("7156"),o=n("9bf2").f,u=n("241c").f,c=n("44e7"),l=n("ad6d"),f=n("9f7f"),d=n("6eeb"),p=n("d039"),g=n("69f3").set,v=n("2626"),h=n("b622"),m=h("match"),x=i.RegExp,y=x.prototype,b=/a/g,S=/a/g,w=new x(b)!==b,E=f.UNSUPPORTED\_Y,R=r&&s("RegExp",!w||E||p((function(){return S[m]=!1,x(b)!=b||x(S)==S||"/a/i"!=x(b,"i")})));if(R){var \_=function(t,e){var n,r=this instanceof \_,i=c(t),s=void 0===e;if(!r&&i&&t.constructor===\_&&s)return t;w?i&&!s&&(t=t.source):t instanceof \_&&(s&&(e=l.call(t)),t=t.source),E&&(n=!!e&&e.indexOf("y")>-1,n&&(e=e.replace(/y/g,"")));var o=a(w?new x(t,e):x(t,e),r?this:y,\_);return E&&n&&g(o,{sticky:n}),o},I=function(t){t in \_||o(\_,t,{configurable:!0,get:function(){return x[t]},set:function(e){x[t]=e}})},C=u(x),$=0;while(C.length>$)I(C[$++]);y.constructor=\_,\_.prototype=y,d(i,"RegExp",\_)}v("RegExp")},6547:function(t,e,n){var r=n("a691"),i=n("1d80"),s=function(t){return function(e,n){var s,a,o=String(i(e)),u=r(n),c=o.length;return u<0||u>=c?t?"":void 0:(s=o.charCodeAt(u),s<55296||s>56319||u+1===c||(a=o.charCodeAt(u+1))<56320||a>57343?t?o.charAt(u):s:t?o.slice(u,u+2):a-56320+(s-55296<<10)+65536)}};t.exports={codeAt:s(!1),charAt:s(!0)}},7156:function(t,e,n){var r=n("861d"),i=n("d2bb");t.exports=function(t,e,n){var s,a;return i&&"function"==typeof(s=e.constructor)&&s!==n&&r(a=s.prototype)&&a!==n.prototype&&i(t,a),t}},"8aa5":function(t,e,n){"use strict";var r=n("6547").charAt;t.exports=function(t,e,n){return e+(n?r(t,e).length:1)}},"8c5c":function(t,e,n){},9263:function(t,e,n){"use strict";var r=n("ad6d"),i=n("9f7f"),s=RegExp.prototype.exec,a=String.prototype.replace,o=s,u=function(){var t=/a/,e=/b\*/g;return s.call(t,"a"),s.call(e,"a"),0!==t.lastIndex||0!==e.lastIndex}(),c=i.UNSUPPORTED\_Y||i.BROKEN\_CARET,l=void 0!==/()??/.exec("")[1],f=u||l||c;f&&(o=function(t){var e,n,i,o,f=this,d=c&&f.sticky,p=r.call(f),g=f.source,v=0,h=t;return d&&(p=p.replace("y",""),-1===p.indexOf("g")&&(p+="g"),h=String(t).slice(f.lastIndex),f.lastIndex>0&&(!f.multiline||f.multiline&&"\n"!==t[f.lastIndex-1])&&(g="(?: "+g+")",h=" "+h,v++),n=new RegExp("^(?:"+g+")",p)),l&&(n=new RegExp("^"+g+"$(?!\\s)",p)),u&&(e=f.lastIndex),i=s.call(d?n:f,h),d?i?(i.input=i.input.slice(v),i[0]=i[0].slice(v),i.index=f.lastIndex,f.lastIndex+=i[0].length):f.lastIndex=0:u&&i&&(f.lastIndex=f.global?i.index+i[0].length:e),l&&i&&i.length>1&&a.call(i[0],n,(function(){for(o=1;o<arguments.length-2;o++)void 0===arguments[o]&&(i[o]=void 0)})),i}),t.exports=o},"9f7f":function(t,e,n){"use strict";var r=n("d039");function i(t,e){return RegExp(t,e)}e.UNSUPPORTED\_Y=r((function(){var t=i("a","y");return t.lastIndex=2,null!=t.exec("abcd")})),e.BROKEN\_CARET=r((function(){var t=i("^r","gy");return t.lastIndex=2,null!=t.exec("str")}))},ac1f:function(t,e,n){"use strict";var r=n("23e7"),i=n("9263");r({target:"RegExp",proto:!0,forced:/./.exec!==i},{exec:i})},ad6d:function(t,e,n){"use strict";var r=n("825a");t.exports=function(){var t=r(this),e="";return t.global&&(e+="g"),t.ignoreCase&&(e+="i"),t.multiline&&(e+="m"),t.dotAll&&(e+="s"),t.unicode&&(e+="u"),t.sticky&&(e+="y"),e}},af47:function(t,e,n){"use strict";n.d(e,"a",(function(){return o}));var r=n("bc3a"),i=n.n(r);function s(t,e,n){return i.a.post(t,e,{headers:n})}function a(t,e,n){return i.a.put(t,e,{headers:n})}var o={login:function(t,e){return i()({method:"POST",url:"/login",withCredentials:!0,headers:e,data:t})},getCaptcha:function(t,e){return s("/v1/identity/sms",t,e)},getPwd:function(t,e){return a("/v1/users/password",t,e)},register:function(t,e){return s("/v1/users",t,e)},uniqueness:function(t,e){return s("/v1/users/action/uniqueness",t,e)}}},c975:function(t,e,n){"use strict";var r=n("23e7"),i=n("4d64").indexOf,s=n("a640"),a=n("ae40"),o=[].indexOf,u=!!o&&1/[1].indexOf(1,-0)<0,c=s("indexOf"),l=a("indexOf",{ACCESSORS:!0,1:0});r({target:"Array",proto:!0,forced:u||!c||!l},{indexOf:function(t){return u?o.apply(this,arguments)||0:i(this,t,arguments.length>1?arguments[1]:void 0)}})},d784:function(t,e,n){"use strict";n("ac1f");var r=n("6eeb"),i=n("d039"),s=n("b622"),a=n("9263"),o=n("9112"),u=s("species"),c=!i((function(){var t=/./;return t.exec=function(){var t=[];return t.groups={a:"7"},t},"7"!=="".replace(t,"$<a>")})),l=function(){return"$0"==="a".replace(/./,"$0")}(),f=s("replace"),d=function(){return!!/./[f]&&""===/./[f]("a","$0")}(),p=!i((function(){var t=/(?:)/,e=t.exec;t.exec=function(){return e.apply(this,arguments)};var n="ab".split(t);return 2!==n.length||"a"!==n[0]||"b"!==n[1]}));t.exports=function(t,e,n,f){var g=s(t),v=!i((function(){var e={};return e[g]=function(){return 7},7!=""[t](e)})),h=v&&!i((function(){var e=!1,n=/a/;return"split"===t&&(n={},n.constructor={},n.constructor[u]=function(){return n},n.flags="",n[g]=/./[g]),n.exec=function(){return e=!0,null},n[g](""),!e}));if(!v||!h||"replace"===t&&(!c||!l||d)||"split"===t&&!p){var m=/./[g],x=n(g,""[t],(function(t,e,n,r,i){return e.exec===a?v&&!i?{done:!0,value:m.call(e,n,r)}:{done:!0,value:t.call(n,e,r)}:{done:!1}}),{REPLACE\_KEEPS\_$0:l,REGEXP\_REPLACE\_SUBSTITUTES\_UNDEFINED\_CAPTURE:d}),y=x[0],b=x[1];r(String.prototype,t,y),r(RegExp.prototype,g,2==e?function(t,e){return b.call(t,this,e)}:function(t){return b.call(t,this)})}f&&o(RegExp.prototype[g],"sham",!0)}},eb4e:function(t,e,n){"use strict";var r=n("8c5c"),i=n.n(r);i.a}}]); |
|  | |
| Reference |  |
| CWE Id | 200 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Informational (Low)** | **Timestamp Disclosure - Unix** |
| Description | A timestamp was disclosed by the application/web server - Unix |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Evidence | 36705334 |
| URL | https://{host}:30091/ |
| Method | GET |
| Evidence | 02683615 |
| Instances | 2 |
| Solution | Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns. |
| Other information | 36705334, which evaluates to: 1971-03-02 03:55:34 |
|  | |
| Reference | http://projects.webappsec.org/w/page/13246936/Information%20Leakage |
| CWE Id | 200 |
| WASC Id | 13 |
| Source ID | 3 |

|  |  |
| --- | --- |
| **Informational (Low)** | **Cookie Slack Detector** |
| Description | Repeated GET requests: drop a different cookie each time, followed by normal request with all cookies to stabilize session, compare responses against original baseline GET. This can reveal areas where cookie based authentication/attributes are not actually enforced. |
|  | |
| URL | https://{host}:30091/ |
| Method | GET |
| Instances | 1 |
| Solution |  |
| Other information | Dropping this cookie appears to have invalidated the session: [XSRF-TOKEN] A follow-on request with all original cookies still had a different response than the original request. |
|  | |
| Reference | http://projects.webappsec.org/Fingerprinting |
| CWE Id | 200 |
| WASC Id | 45 |
| Source ID | 1 |

### 测试结果：无高风险漏洞问题，通过

## EG-TST-SEC-003

使用uniofuzz对EdgeGallery容器服务端口进行fuzz测试。每个端口测试迭代数量为150，000。

### Appstore-fe

### 

### Appstore-be

### 

### Developer-fe

### 

### Mecm-apm

### 

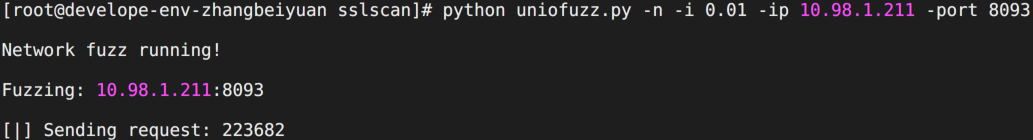
### Mecm-appo

### 

### Mecm-fe

### 

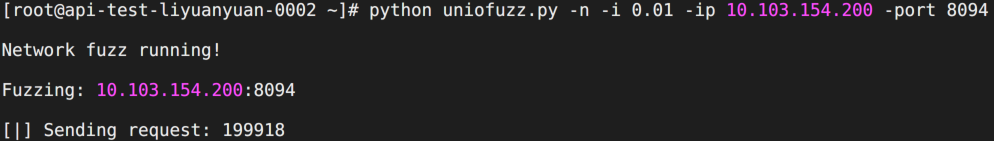
### Mecm-inventory



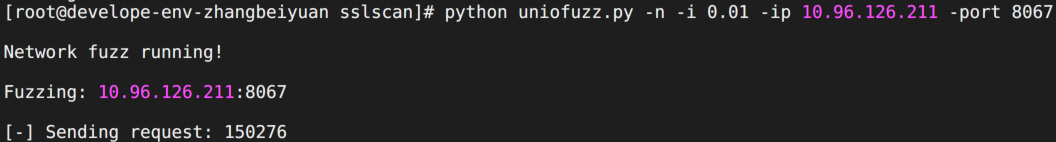
### Mecm-mepm-k8splugin

### 

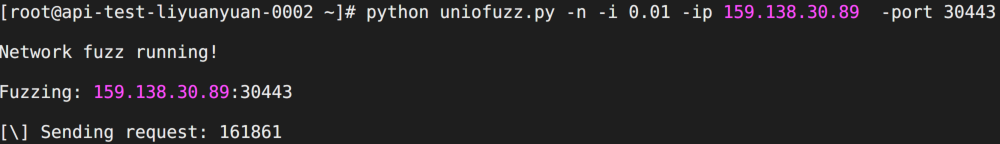
### Mecm-mepm-lcmcontroller



### User-mgmt



### Mep-api-gw



### 测试结果：在15万次迭代中各端口均无异常，通过