



Web 应用程序报告

该报告包含有关 **web** 应用程序的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.3.11, 规则: 16342
扫描开始时间: 2019/4/18 14:27:06

目录

介绍

- 常规信息
- 登陆设置

摘要

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- 已解密的登录请求 ③
- 登录错误消息凭证枚举 ①
- 跨站点请求伪造 ③
- “Content-Security-Policy”头缺失或不安全 ④
- “X-Content-Type-Options”头缺失或不安全 ⑤
- “X-XSS-Protection”头缺失或不安全 ⑤
- Oracle 日志文件信息泄露 ⑥
- 查询中接受的主体参数 ①
- 检测到隐藏目录 ②
- 发现可能的服务器路径泄露模式 ①
- 检测到应用程序测试脚本 ②⑧

修订建议

- 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

- 向每个错误登录尝试发出相同的错误消息
- 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce
- 除去服务器中的测试脚本
- 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去
- 关闭跟踪，限制对日志文件的访问，或者将其除去
- 将服务器配置为使用安全策略的“Content-Security-Policy”头
- 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头
- 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头
- 请勿接受在查询字符串中发送的主体参数
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁

咨询

- 已解密的登录请求
- 登录错误消息凭证枚举
- 跨站点请求伪造
- “Content-Security-Policy”头缺失或不安全
- “X-Content-Type-Options”头缺失或不安全
- “X-XSS-Protection”报头缺失或不安全
- Oracle 日志文件信息泄露
- 查询中接受的主体参数
- 检测到隐藏目录
- 发现可能的服务器路径泄露模式
- 检测到应用程序测试脚本

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题:	3
中等严重性问题:	4
低严重性问题:	23
参考严重性问题:	29
报告中包含的严重性问题总数:	59
扫描中发现的严重性问题总数:	59

常规信息

扫描文件名称: 20190418-1st
扫描开始时间: 2019/4/18 14:27:06
测试策略: Default

主机	172.31.3.33
端口	7001
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	JavaAppServer

登陆设置

登陆方法:	提示
并发登陆:	已启用
JavaScript 执行文件:	已禁用
会话中检测:	已启用
会话中模式:	\\(Development\\) 北京首发投资控股有限公司 公司工作区
跟踪或会话标识 cookie:	JSESSIONID
跟踪或会话标识参数:	<u>uref</u> v v

```
nav_id
__token
__uref
__uref
__uref
v
__token
__uref
```

登陆序列:

```
http://172.31.3.33:7001/bluedoor
http://172.31.3.33:7001/bluedoor/login/req/usercheck
http://172.31.3.33:7001/bluedoor/login/req
http://172.31.3.33:7001/bluedoor/landing
http://172.31.3.33:7001/bp/g/nav/index?__uref=uuu166938215
http://172.31.3.33:7001/webant/js/blank.htm
http://172.31.3.33:7001/gs/ojet/lux/js/libs/lux/v4.1.0/debug/componen
ts/breadcrumbs/luxbreadcrumbs_template.html?v=18.8
http://172.31.3.33:7001/gs/ojet/templates/nav/iframe.tmpl.html?
v=18.8
http://172.31.3.33:7001/bp/g/nav/data/menutree
http://172.31.3.33:7001/bp/nav/company/home?__uref=uuu166938215t1
http://172.31.3.33:7001/bp/nav/user/company_home?
__uref=uuu166938215t1
http://172.31.3.33:7001/mapviewer/fsmc/jslib/oraclemaps.js
http://172.31.3.33:7001/bp/nav/user/company_home?
__uref=uuu166938215t1
http://172.31.3.33:7001/gs/ojet/templates/comp/picker/userprofile.t
pl.html?v=18.8
http://172.31.3.33:7001/bp/share/get_map_server_info
```

摘要












问题类型 11

TOC

问题类型	问题的数量
高 已解密的登录请求	3 
中 登录错误消息凭证枚举	1 
中 跨站点请求伪造	3 
低 “Content-Security-Policy”头缺失或不安全	4 
低 “X-Content-Type-Options”头缺失或不安全	5 
低 “X-XSS-Protection”头缺失或不安全	5 
低 Oracle 日志文件信息泄露	6 
低 查询中接受的主体参数	1 
低 检测到隐藏目录	2 
参 发现可能的服务器路径泄露模式	1 
参 检测到应用程序测试脚本	28 

有漏洞的 URL 16

TOC

URL	问题的数量
高 http://172.31.3.33:7001/bluedoor	4 
高 http://172.31.3.33:7001/bluedoor/login/req	3 
中 http://172.31.3.33:7001/bluedoor/viewPasswordPolicy	2 
中 http://172.31.3.33:7001/bp/g/nav/index	1 
低 http://172.31.3.33:7001/bluedoor/login/req/usercheck	1 
低 http://172.31.3.33:7001/webant/js/dhtmltreeview.js	3 
低 http://172.31.3.33:7001/studio/js/jquery-sha256.min.js	2 
低 http://172.31.3.33:7001/unifier_js/bluedoor/login_c.js	2 
低 http://172.31.3.33:7001/webant/js/i18n/UnifierMenu.js	2 
低 http://172.31.3.33:7001/webant/js/i18n/UnifierTab.js	2 
低 http://172.31.3.33:7001/bp/nav/	16 

低	http://172.31.3.33:7001/bp/nav/company/	16	<div><div></div></div>
低	http://172.31.3.33:7001/bp/nav/user/	2	<div><div></div></div>
低	http://172.31.3.33:7001/g/	1	<div><div></div></div>
低	http://172.31.3.33:7001/pub/	1	<div><div></div></div>
参	http://172.31.3.33:7001/webant/js/i18n/UnifierString.js	1	<div><div></div></div>

修订建议 11

TOC

修复任务	问题的数量
高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	3 <div><div></div></div>
中 向每个错误登录尝试发出相同的错误消息	1 <div><div></div></div>
中 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	3 <div><div></div></div>
低 除去服务器中的测试脚本	28 <div><div></div></div>
低 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	2 <div><div></div></div>
低 关闭跟踪，限制对日志文件的访问，或者将其除去	6 <div><div></div></div>
低 将服务器配置为使用安全策略的“Content-Security-Policy”头	4 <div><div></div></div>
低 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	5 <div><div></div></div>
低 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	5 <div><div></div></div>
低 请勿接受在查询字符串中发送的主体参数	1 <div><div></div></div>
低 为 Web 服务器或 Web 应用程序下载相关的安全补丁	1 <div><div></div></div>

安全风险 8

TOC

风险	问题的数量
高 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	3 <div><div></div></div>
中 可能会升级用户特权并通过 Web 应用程序获取管理许可权	1 <div><div></div></div>
中 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	3 <div><div></div></div>
低 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	21 <div><div></div></div>
低 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	15 <div><div></div></div>
低 可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	2 <div><div></div></div>
参 可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	1 <div><div></div></div>
参 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	28 <div><div></div></div>






原因 7

TOC

原因	问题的数量
高 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	3 
中 已向用户显示可能包含敏感调试信息的异常和错误消息	1 
中 应用程序使用的认证方法不充分	3 
低 Web 应用程序编程或配置不安全	15 
低 Web 服务器或应用程序服务器是以不安全的方式配置的	8 
参 未安装第三方产品的最新补丁或最新修补程序	1 
参 在生产环境中留下临时文件	28 

WASC 威胁分类

TOC

威胁	问题的数量
传输层保护不足	3 
可预测资源位置	28 
跨站点请求伪造	3 
蛮力	1 
信息泄露	24 

按问题类型分类的问题

高

已解密的登录请求 3

TOC

问题 1 / 3

TOC

已解密的登录请求

严重性:

高

CVSS 分数: 8.5

URL:

<http://172.31.3.33:7001/bluedoor/login/req>

实体:

req (Page)

风险:

可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值:

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 识别了不是通过 SSL 发送的登录请求。

测试请求和响应:

```
POST /bluedoor/login/req HTTP/1.1
Content-Length: 128
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/67.0.3396.79 Safari/537.36
Host: 172.31.3.33:7001
Cookie: JSESSIONID=BllovIt_fMZVyw4Ku5-DYMzCgq4E00ff11837uN9T90zUEL6OL-32!1186003145
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://172.31.3.33:7001
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.9

mode=user&redirect=&loginFor=&form2=true&username=test&password=1E052A3DAB54FF26772BCF14A9E64A3D7
FD15CB448DB2A2258A057B2EBBE02B3

HTTP/1.1 200 OK
Content-Length: 158
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=Rj0vIv9dJZVGM15K5HDzsVRHW9Eig3rqF4qNOq-15eDDL3_dt5B3!1186003145; path=/;
```

```
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:29:43 GMT
Content-Type: application/json
Cache-Control: max-age=0, no-store, no-cache
```

```
{
  "next": "",
  "redirect": "",
  "view": "",
  "authRefresh": "",
  "daysToExpiration": "",
  "error": "",
  "passwordExpired": "",
  "passwordExpiringSoon": ""
}
```

问题 2 / 3

TOC

已解密的登录请求

严重性: **高**

CVSS 分数: 8.5

URL: <http://172.31.3.33:7001/bluedoor/login/req>

实体: password (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时，始终使用 **SSL** 和 **POST**（主体）参数。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```
POST /bluedoor/login/req HTTP/1.1
Content-Length: 64
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 172.31.3.33:7001
Cookie: JSESSIONID=jAMvILLZJOC4jmu9HMOvezzz-YNqEK-WvkNCSjQ6o4jcCT6uySAr!1186003145
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://172.31.3.33:7001
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.9
```

```

mode=user&redirect=&loginFor=&form2=true&username=test&password=

HTTP/1.1 200 OK
X-XSS-Protection: 1; mode=block
Content-Length: 197
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-store, no-cache
Date: Thu, 18 Apr 2019 06:27:29 GMT
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Type: application/json


{
  "next": "/skirelogin",
  "redirect": "",
  "view": "",
  "authRefresh": "",
  "daysToExpiration": "",
  "error": "Invalid Username or Password",
  "passwordExpired": "",
  "passwordExpiringSoon": ""
}

```

问题 3 / 3

TOC

已解密的登录请求

严重性: 

CVSS 分数: 8.5

URL: <http://172.31.3.33:7001/bluedoor>

实体: password (Parameter)

风险: 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因: 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```

POST /bluedoor HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=Rj0vIv9dJZVGM15K5HDzsVRHW9Eig3rqF4qNOq-15eDDL3_dT5B3!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Content-Length: 128
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

```

Content-Type: application/x-www-form-urlencoded

mode=user&redirect=&loginFor=&form2=true&username=test&password=9E521114A31E70FFBB5BB95AC7B2D093B9964FF57201B51A1EAC56D73E49BC2E

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:30:13 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```
<!DOCTYPE html><html lang="zh_CN"><head><title>Primavera Unifier &#x767b;&#x5f55;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "zh_CN",
    "token": "8652626395787713664",
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "#-1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "true",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>
<link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico" />
<link rel="stylesheet" href="/unifier_js/bluedoor/login_c.css?18.8" type="text/css" />
<style type="text/css">
.login-page {
  width: 100%;
  margin-left: 0;
}
.branding {
  margin: 0;
  margin-left: calc(50% - 200px);
}
.consent.retrodialog .ui-dialog-content {
```

```

        width: calc(95% + 8px) !important;
        padding: 0px;
        margin: 10px;
    }
    .ui-dialog.consent, .ui-dialog.consent .ui-dialog-content, .ui-dialog.consent .ui-dialog-
buttonset {
        background: #F3F3F3 !important;
    }
    .ui-dialog.consent .ui-dialog-buttonpane{
        padding-right: 5px;
        margin-top: 0px;
        padding-top: 0px;
        background-color: #f3f3f3 !important;
    }
    .ui-dialog.consent .ui-dialog-buttonset > button:first-child, .ui-dialog.consent .ui-dialog-
buttonset > button:first-child .ui-button-text{
        background-color: #616977;
        background-image: none;
    }
}
</style>

<script type="text/javascript" src="/unifier_js/bluedoor/landing.js?18.8" ></script>
<script type="text/javascript">
// framebusting
if(self != top){ top.location = self.location; }

var shortcut = {
    username: '',
    p: '0',
    m: 'user',
    k: 'unifier'
};
shortcut.id = '';
shortcut.open_rec = true;

P.application = 'Unifier';
P.loginPath = '/unifier'
P.ssoProvider = '';
P.ssoLogout = '';
P.loginPath = P.ssoLogout;

P.loginrole = '0';
P.navMode = 'user';

P.servletPath = '/bluedoor';
P.logoutRedirect = '';

P.consentInfo =
{
    "enabled":false
}

</script>
</head>

<body class="background-info-tech">
    <div class="login-page">
        <div class="branding">
            
            <div class="app-family-logo app-name">Unifier</div>
        </div>

        <div id="processing" class="page-spinner page-loading-spinner page-spinner-
static">
            <div class="spinner-label" id="loading-modal-label">                正在加载...</div>
            <div class="spinner-large load
...
...
...

```

问题 1 / 1

TOC

登录错误消息凭证枚举

严重性: 中

CVSS 分数: 6.4

URL: <http://172.31.3.33:7001/bluedoor/login/req>

实体: req (Page)

风险: 可能会升级用户特权并通过 Web 应用程序获取管理许可权

原因: 已向用户显示可能包含敏感调试信息的异常和错误消息

固定值: 向每个错误登录尝试发出相同的错误消息

差异: cookie 已从请求除去: `FIcvJFxFvFH0Apg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`参数 从以下位置进行控制: `test` 至: `atestWithSomeChars`参数 从以下位置进行控制: `1E052A3DAB54FF26772BCF14A9E64A3D7FD15CB448DB2A2258A057B2EBBE02B3`至: `a1E052A3DAB54FF26772BCF14A9E64A3D7FD15CB448DB2A2258A057B2EBBE02B3WithSomeChars`

推理: 测试发现应用程序在用户名字段无效时会发布一条错误消息, 在密码字段无效时会发布另一条错误消息。此行为可能让攻击者能够使用蛮力技术来枚举有效的用户名和密码。

测试请求和响应:

```
POST /bluedoor/login/req HTTP/1.1
Content-Length: 142
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 172.31.3.33:7001
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://172.31.3.33:7001
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.9

mode=user&redirect=&loginFor=&form2=true&username=atestWithSomeChars&password=1E052A3DAB54FF26772BCF14A9E64A3D7FD15CB448DB2A2258A057B2EBBE02B3

HTTP/1.1 200 OK
Content-Length: 197
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=QC0vOy1LJGc5Fx0ObI5mJJv7cdqQkAUcUMuiZL3eVlhvk_AzGsB0!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:56:08 GMT
Content-Type: application/json
Cache-Control: max-age=0, no-store, no-cache
```

```

{
  "next": "/skirelogin",
  "redirect": "",
  "view": "",
  "authRefresh": "",
  "daysToExpiration": "",
  "error": "Invalid Username or Password",
  "passwordExpired": "",
  "passwordExpiringSoon": ""
}

POST /bluedoor/login/req HTTP/1.1
Content-Length: 142
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 172.31.3.33:7001
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://172.31.3.33:7001
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.9

mode=user&redirect=&loginFor=&form2=true&username=test&password=a1E052A3DAB54FF26772BCF14A9E64A3D
7FD15CB448DB2A2258A057B2EBBE02B3WithSomeChars

HTTP/1.1 200 OK
Content-Length: 292
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=-GUvOy1l4qS15MEPyS0GQJndFjbSV5M8ZBZZ6DR9FL7x_pZb9QPI!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:56:08 GMT
Content-Type: application/json
Cache-Control: max-age=0, no-store, no-cache

{
  "next": "/skirelogin",
  "redirect": "",
  "view": "",
  "authRefresh": "",
  "daysToExpiration": "",
  "error": "Login attempts to this account have exceeded the maximum allowed. This account has been
  locked. Contact your Administrator.",
  "passwordExpired": "",
  "passwordExpiringSoon": ""
}

POST /bluedoor/login/req HTTP/1.1
Content-Length: 142
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 172.31.3.33:7001
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://172.31.3.33:7001

```

```
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.9

mode=user&redirect=&loginFor=&form2=true&username=atestWithSomeChars&password=1E052A3DAB54FF26772
BCF14A9E64A3D7FD15CB448DB2A2258A057B2EBBE02B3

HTTP/1.1 200 OK
Content-Length: 197
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=bGwvOy1200R1oFfGR31ejTLJhgB4uBYPjGX2AhyCvH8wT5EbcdXu!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:56:08 GMT
Content-Type: application/json
Cache-Control: max-age=0, no-store, no-cache

{
  "next": "/skirelogin",
  "redirect": "",
  "view": "",
  "authRefresh": "",
  "daysToExpiration": "",
  "error": "Invalid Username or Password",
  "passwordExpired": "",
  "passwordExpiringSoon": ""
}
```

中

跨站点请求伪造 3

TOC

问题 1 / 3

TOC

跨站点请求伪造

严重性: **中**

CVSS 分数: 6.4

URL: <http://172.31.3.33:7001/bluedoor>

实体: bluedoor (Page)

风险: 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异: 标题 从以下位置进行控制: <http://172.31.3.33:7001/bluedoor> 至:

<http://bogus.referer.ibm.com>

推理: 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应:

```
POST /bluedoor HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.ibm.com
Cookie: JSESSIONID=FicvJFxJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:31:33 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="zh_CN"><head><title>Primavera Unifier &#x767b;&#x5f55;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "zh_CN",
    "token": "1468919253826338277",
    "isDevelopment": false
  },
  "UserVariable":
  {
```

```

    "date":
    {
        "shortformat": "yyyy/MM/dd",
        "timezone": "Asia/Shanghai",
        "dateformat": "yyyy/MM/dd hh:mm a",
        "localformat": " (UTC+8)"
    },
    "number":
    {
        "decimalSymbol": ".",
        "negativeCurrencyFormat": "#-1.1",
        "negativeDecimalFormat": "-1.1",
        "digitGrouping": "#,##0",
        "showCurrencySymbol": "true",
        "positiveCurrencyFormat": "#1.1",
        "groupingSymbol": ",",
    }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>
<link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico" />
<link rel="stylesheet" href="/unifier_js/bluedoor/login_c.css?18.8" type="text/css" />
<style type="text/css">
.login-page {
    width: 100%;
    margin-left: 0;
}
.branding {
    margin: 0;
    margin-left: calc(50% - 200px);
}
.consent.retrodialog .ui-dialog-content {
    width: calc(95% + 8px) !important;
    padding: 0px;
    margin: 10px;
}
.ui-dialog.consent, .ui-dialog.consent .ui-dialog-content, .ui-dialog.consent .ui-dialog-
buttonset {
    background: #F3F3F3 !important;
}
.ui-dialog.consent .ui-dialog-buttonpane{
    padding-right: 5px;
    margin-top: 0px;
    padding-top: 0px;
    background-color: #f3f3f3 !important;
}
.ui-dialog.consent .ui-dialog-buttonset > button:first-child, .ui-dialog.consent .ui-dialog-
buttonset > button:first-child .ui-button-text{
    background-color: #616977;
    background-image: none;
}
</style>

<script type="text/javascript" src="/unifier_js/bluedoor/landing.js?18.8" ></script>
<script type="text/javascript">
// framebusting
if(self != top){ top.location = self.location; }

var shortcut = {
    username: '',
    p: '0',
    m: 'user',
    k: 'unifier'
};
shortcut.id = '';
shortcut.open_rec = true;

P.application = 'Unifier';
P.loginPath = '/unifier'
P.ssoProvider = '';
P.ssoLogout = '';
P.loginPath = P.ssoLogout;

```

```

P.loginrole = '0';
P.navMode = 'user';

P.servletPath = '/bluedoor';
P.logoutRedirect = '';

P.consentInfo =
{
  "enabled":false
}

</script>
</head>

<body class="background-info-tech">
  <div class="login-page">
    <div class="branding">
      
      <div class="app-family-logo app-name">Unifier</div>
    </div>

    <div id="processing" class="page-spinner page-loading-spinner page-spinner-static">
      <div class="spinner-label" id="loading-modal-label">正在加载...</div>
      <div class="spinner-large loading-spinner-large">
        <div class="dot dot1"></div>
        <div class="dot dot2"></div>
        <div class="dot dot3"></div>
      </div>
    </div>
  </div>
  ...
  ...
  ...

```

问题 2 / 3

TOC

跨站点请求伪造

严重性: **中**

CVSS 分数: 6.4

URL: <http://172.31.3.33:7001/bluedoor/viewPasswordPolicy>

实体: viewPasswordPolicy (Page)

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

差异: **标题** 从以下位置进行控制: <http://172.31.3.33:7001/bluedoor> 至:

<http://bogus.referer.ibm.com>

推理: 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应:

```

GET /bluedoor/viewPasswordPolicy?username=undefined HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.ibm.com
Cookie: JSESSIONID=FicvJFxFvFHoApg5oFD5Dz_RsU4DWFZjcmRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:31:34 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="zh_CN"><head><title>&#x5bc6;&#x7801;&#x7b56;&#x7565;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "de": "German",
      "zh_TW": "Chinese (Traditional)",
      "ru": "Russian",
      "ko": "Korean",
      "ja": "Japanese",
      "en": "English",
      "zh_CN": "Chinese (Simplified)",
      "it": "Italian",
      "pt_BR": "Portuguese (Brazil)",
      "fr": "French",
      "nl": "Dutch",
      "es": "Spanish"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "zh_CN",
    "token": "1468919253826338277",
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "#-1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "true",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"

```

```

type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/dhtmltreeview.js?18.8" ></script>
<script type="text/javascript">
function init()
{
    loadPWDValue();
}

pwdBean = new Object();
pwdBean['companyid'] = '0';
pwdBean['min_length'] = '6';
pwdBean['max_length'] = '0';
pwdBean['min_numericchar'] = '1';
pwdBean['min_alpchar'] = '1';
pwdBean['min_spechar'] = '1';
pwdBean['chk_uname'] = '1';
pwdBean['chk_fname'] = '1';
pwdBean['chk_prevpwd'] = '0';
pwdBean['pwd_validfor'] = '180';
pwdBean['inform_exp'] = '7';
pwdBean['max_attempts'] = '5';
pwdBean['max_inactive'] = '360';

function loadPWDValueOld()
{
    // var fm = document.all;
    var fm = document.getElementsByTagName();
    var pwdBeanSet=0;
    for (var name in pwdBean)
        pwdBeanSet=1;

    for(i=0;i<fm.pwdCheck.length;i++)
    {
        var obj1=eval("fm."+fm.pwdCheck[i].value)
        var checkValue=fm.pwdCheck[i].value;
        if((pwdBeanSet == 0)|| (eval("pwdBean."+checkValue) == 'undefined'))||
(eval("pwdBean."+checkValue) == '0')){
            obj1.value = "";
            fm.pwdCheck[i].checked = false;
        }
        else{
            obj1.value = pwdBean.checkValue;
            fm.pwdCheck[i].checked = true;
        }
    }
}

function loadPWDValue()
{
    // var fm = document.all;
    var fm = document.getElementsByTagName();

    var pwdBeanSet=0;
    for (var name in pwdBean) {
        pwdBeanSet = 1;
    }

    var inputEls = document.getElementsByName("pwdCheck");

    for(i=0; i < inputEls.length; i++) {
        var obj1 = fm[inputEls[i].value];
        var checkValue = inputEls[i].value;
        if((pwdBeanSet == 0) ||
            (pwdBean[checkValue] == 'undefined') ||
            (pwdBean[checkValue] == '0')) {
            obj1.value = "";
            inputEls[i].checked = false;
        }
    }
}

```

```

else{
    obj1.value = pwdBean[checkValue];
    // fm.pwdCheck[i].checked = true;
    inputEls[i].checked = true;
}

}

}
if(window.opener)
    jQuery(window.opener).unload(function(
    ...
    ...
    ...

```

原始响应

测试响应



问题 3 / 3

TOC

跨站点请求伪造

严重性: **中**

CVSS 分数: 6.4

URL: <http://172.31.3.33:7001/bp/g/nav/index>

实体: __uref (Parameter)

风险: 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

原因: 应用程序使用的认证方法不充分

固定值: 验证“Referer”头的值，并对每个提交的表单使用 **one-time-nonce**

差异: 参数 从以下位置进行控制: **uuu812352716t1** 至: **1uuu812352716t11**

推理: 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应:

```
GET /bp/g/nav/index?__uref=1uuu812352716t11 HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FicvJFvJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:48:41 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html>
<html lang="zh_CN">
<head>
  <title>Primavera Unifier</title>
  <meta http-equiv="x-ua-compatible" content="IE=edge"/>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico">
```

```
<link rel="stylesheet" href="/gs/ojet/css/main.min.css?18.8" type="text/css" />
<script type="text/javascript" src="/gs/ojet/lux/js/libs/jquery/jquery-3.1.1.min.js?18.8" >
</script>
<script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script>
<script type="text/javascript" src="/upk/ias_helper.js?18.8" ></script>
```

```
<script type="text/javascript" src="/webant/js/il8n/UnifierMenu_zh_CN.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/il8n/UnifierMessage_zh_CN.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/il8n/UnifierString_zh_CN.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/il8n/UnifierTab_zh_CN.js?18.8" ></script>
```

```
<script type="text/javascript">
  _P =
  {
    "SystemVariable":
    {
      "locales":
      {
        "de": "German",
        "zh_TW": "Chinese (Traditional)",
        "ru": "Russian",
        "ko": "Korean",
        "ja": "Japanese",
        "en": "English",
        "zh_CN": "Chinese (Simplified)",
        "it": "Italian",
        "pt_BR": "Portuguese (Brazil)",
        "fr": "French",
        "nl": "Dutch",
        "es": "Spanish"
      },
      "codeVersion": "18.8",
      "uref": "1uuu812352716t11",
      "il8ndebug": 0,
      "loginTimeout": 1200,
      "locale": "zh_CN",
      "token": "1468919253826338277",
      "isDevelopment": false
    },
    "UserVariable":
    {
      "date":
      {
```

```

        "shortformat": "yyyy/MM/dd",
        "timezone": "Asia/Shanghai",
        "dateformat": "yyyy/MM/dd hh:mm a",
        "localformat": " (UTC+8)"
    },
    "number": {
        "decimalSymbol": ".",
        "negativeCurrencyFormat": "#-1.1",
        "negativeDecimalFormat": "-1.1",
        "digitGrouping": "#,##0",
        "showCurrencySymbol": "true",
        "positiveCurrencyFormat": "#1.1",
        "groupingSymbol": ","
    }
}
};

jQuery.extend(_P, {
    shortcut :
    {
        "p": 0,
        "projectname": "",
        "company_id": 1000,
        "t": "home",
        "isCCAdmin": false,
        "user_id": 1009,
        "isowner": 1,
        "guid": "2577B2C5-BE5D-70D9-6E75-930C00971E04",
        "k": null,
        "m": "user"
    },
    loginPath : '/unifier',
    data :
    {
        "app": "Unifier",
        "upkHelpURL": "",
        "invalid_bookmark": false,
        "tabs":
        [
            {
                "mode": "user",
                "toptab": "home",
                "tooltip": "主页",
                "pid": 0,
                "menuwidth": "180",
                "title": "主页",
                "menu_id": ""
            },
            {
                "mode": "user",
                "toptab": "company",
                "tooltip": "公司工作区",
                "active": true,
                "pid": 0,
                "menuwidth": "180",
                "title": "公司工作区",
                "menu_id": "uxddm"
            }
        ],
        "helpUrl": "http://docs.oracle.com/cd/E91461_01/help/en",
        "upkHelpApp": "app.PrimaveraUnifier;en",
        "setting":
        {
            "lockedTabs": 0
        },
        "navbean":
        {
            "ssoProvider": "",
            "logo_id": 0,
            "hasUPW": true,
            "proxylist":
            [
            ],
            "profileImageId": 0,
            "oracle_logo_src": "/gs/uni/nav/resources/images/header/oracle_logo_white.png",
            "lastLoginDate": "2019/04/18 02:29 下午",
            "ssoLogout": ""
        }
    }
});

```



```

"loginFor":
{
},
"init_status":1,
"navView":"user",
"ldap":"",
"loginRole":0,
"primavera_logo_src":"/gs/uni/nav/resources/images/header/primavera_logo_black.png",
"user":
{
  "registry":"unifier",
  "firstname":"测试用户",
  "companyId":1000,
  "companies":
  [
    {
      "companyid":1000,
      "companyregistry":"unifier",
      "shortname":"北京首发投资控股有限公司",
      "upper_shortname":"北京首发投资控股有限公司"
    }
  ],
  "ownerCompanyId":1000,
  "showDash":true,
  "userid":1009,
  "lastname":"test"
},
"oimEnabled":"false",
"profileImageSig":"480e740321ce42f7d98887509c2156f2f5983be9fecab628f311191e6b67c2ff"
},
"scanAllowed":false,
"maxRecent":true,
"displayElement":null,
"hide_new_ui":false,
"root":"/gs/uni/nav/",
"serverType":"dev",
"keyLocations":
[
  {
    "mode":"user",
    "pid":0,
    "toptab":"home",
    "title":"主页",
    "active":true
  }
],
...
...
...

```

问题 1 / 4

TOC

“Content-Security-Policy”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: http://172.31.3.33:7001/bluedoor

实体: bluedoor (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全**固定值:** 将服务器配置为使用安全策略的“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应:

```
POST /bluedoor HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FicvJFvJvFH0Apg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Content-Length: 65
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

username=test&email=test%40altoromutual.com&question=&answer=1234
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:31:33 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="zh_CN"><head><title>Primavera Unifier &#x767b;&#x5f55;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
```

```

src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"zh_CN",
    "token":"1468919253826338277",
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"#-1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"true",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":","
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>
<link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico" />
<link rel="stylesheet" href="/unifier_js/bluedoor/login_c.css?18.8" type="text/css" />
<style type="text/css">
.login-page {
  width: 100%;
  margin-left: 0;
}
.branding {
  margin: 0;
  margin-left: calc(50% - 200px);
}
.consent.retrodialog .ui-dialog-content {
  width: calc(95% + 8px) !important;
  padding: 0px;
  margin: 10px;
}
.ui-dialog.consent, .ui-dialog.consent .ui-dialog-content, .ui-dialog.consent .ui-dialog-
buttonset {
  background: #F3F3F3 !important;
}
.ui-dialog.consent .ui-dialog-buttonpane{
  padding-right: 5px;
  margin-top: 0px;
  padding-top: 0px;
  background-color: #f3f3f3 !important;
}
.ui-dialog.consent .ui-dialog-buttonset > button:first-child, .ui-dialog.consent .ui-dialog-
buttonset > button:first-child .ui-button-text{
  background-color: #616977;
  background-image: none;
}
</style>

```

```

<script type="text/javascript" src="/unifier_js/bluedoor/landing.js?18.8" ></script>
<script type="text/javascript">
// framebusting
if(self != top){ top.location = self.location; }

var shortcut = {
  username: '',
  p: '0',
  m: 'user',
  k: 'unifier'
};
shortcut.id = '';
shortcut.open_rec = true;

P.application = 'Unifier';
P.loginPath = '/unifier'
P.ssoProvider = '';
P.ssoLogout = '';
P.loginPath = P.ssoLogout;

P.loginrole = '0';
P.navMode = 'user';

P.servletPath = '/bluedoor';
P.logoutRedirect = '';

P.consentInfo =
{
  "enabled":false
}

</script>
</head>

<body class="background-info-tech">
<div class="login-page">
  <div class="branding">
    
    <div class="app-family-logo app-name">Unifier</div>
  </div>

  <div id="processing" class="page-spinner page-loading-spinner page-spinner-
static">
    <div class="spinner-label" id="loading-modal-label">      正在加载...</div>
    <div class="spinner-large loading-spinner-large">
      <div class="dot dot1"></div>

    ...
    ...
    ...

```

“Content-Security-Policy”头缺失或不安全

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bluedoor/viewPasswordPolicy>

实体: viewPasswordPolicy (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用安全策略的“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应:

```
GET /bluedoor/viewPasswordPolicy?username=undefined HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=F1cvJFvJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:31:34 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="zh_CN"><head><title>&#x5bc6;&#x7801;&#x7b56;&#x7565;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "de": "German",
      "zh_TW": "Chinese (Traditional)",
      "ru": "Russian",
      "ko": "Korean",
      "ja": "Japanese",
      "en": "English",
      "zh_CN": "Chinese (Simplified)",
      "it": "Italian",
      "pt_BR": "Portuguese (Brazil)",
      "fr": "French",
      "nl": "Dutch",
      "es": "Spanish"
    },
    "codeVersion": "18.8",
```

```

        "uref": "",
        "i18ndebug": 0,
        "loginTimeout": 1200,
        "locale": "zh_CN",
        "token": "1468919253826338277",
        "isDevelopment": false
    },
    "UserVariable": {
        "date": {
            "shortformat": "yyyy/MM/dd",
            "timezone": "Asia/Shanghai",
            "dateformat": "yyyy/MM/dd hh:mm a",
            "localformat": " (UTC+8)"
        },
        "number": {
            "decimalSymbol": ".",
            "negativeCurrencyFormat": "#-1.1",
            "negativeDecimalFormat": "-1.1",
            "digitGrouping": "#,##0",
            "showCurrencySymbol": "true",
            "positiveCurrencyFormat": "#1.1",
            "groupingSymbol": ",",
        }
    }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/dhtmltreeview.js?18.8" ></script>
<script type="text/javascript">
function init()
{
    loadPwDValue();
}

pwdBean = new Object();
pwdBean['companyid'] = '0';
pwdBean['min_length'] = '6';
pwdBean['max_length'] = '0';
pwdBean['min_numericchar'] = '1';
pwdBean['min_alpchar'] = '1';
pwdBean['min_specchar'] = '1';
pwdBean['chk_uname'] = '1';
pwdBean['chk_fname'] = '1';
pwdBean['chk_prevpwd'] = '0';
pwdBean['pwd_validfor'] = '180';
pwdBean['inform_exp'] = '7';
pwdBean['max_attempts'] = '5';
pwdBean['max_inactive'] = '360';

function loadPwDValueOld()
{
    // var fm = document.all;
    var fm = document.getElementsByTagName();
    var pwdBeanSet=0;
        for (var name in pwdBean)
            pwdBeanSet=1;

    for(i=0;i<fm.pwdCheck.length;i++)
    {
        var obj1=eval("fm."+fm.pwdCheck[i].value)
        var checkValue=fm.pwdCheck[i].value;
        if((pwdBeanSet == 0)|| (eval("pwdBean."+checkValue) == 'undefined')){
            (eval("pwdBean."+checkValue) == '0')){
                obj1.value = "";
                fm.pwdCheck[i].checked = false;
            }
        }
        else{

```

```

        obj1.value = pwdBean.checkValue;
        fm.pwdCheck[i].checked = true;
    }

    }

function loadPWDValue()
{
    // var fm = document.all;
    var fm = document.getElementsByTagName();

    var pwdBeanSet=0;
    for (var name in pwdBean) {
        pwdBeanSet = 1;
    }

    var inputEls = document.getElementsByName("pwdCheck");

    for(i=0; i < inputEls.length; i++) {
        var obj1 = fm[inputEls[i].value];
        var checkValue = inputEls[i].value;
        if((pwdBeanSet == 0) ||
            (pwdBean[checkValue] == 'undefined') ||
            (pwdBean[checkValue] == '0')) {
            obj1.value = "";
            inputEls[i].checked = false;
        }
        else{
            obj1.value = pwdBean[checkValue];
            // fm.pwdCheck[i].checked = true;
            inputEls[i].checked = true;
        }
    }
}

if(window.opener)
    jQuery(window.opener).un
...
...
...

```

问题 3 / 4

TOC

“Content-Security-Policy”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bluedoor/login/req/usercheck>

实体: usercheck (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用安全策略的“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应:

```
POST /bluedoor/login/req/usercheck HTTP/1.1
Content-Length: 13
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 172.31.3.33:7001
Cookie: JSESSIONID=FicvJFvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
X-Requested-With: XMLHttpRequest
Connection: Keep-Alive
Referer: http://172.31.3.33:7001/bluedoor
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept-Language: en-US

username=test

HTTP/1.1 200 OK
X-XSS-Protection: 1; mode=block
Content-Length: 32
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, no-store, no-cache
Date: Thu, 18 Apr 2019 06:31:35 GMT
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Type: application/json

{
  "salt": "7052C144110D56D0"
}
```

“Content-Security-Policy”头缺失或不安全	
严重性:	低
CVSS 分数:	5.0
URL:	http://172.31.3.33:7001/webant/js/dhtmlmlistview.js
实体:	dhtmlmlistview.js (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应:

```
GET /webant/js/dhtmlmlistview.js?l8.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor/viewPasswordPolicy?username=undefined
Cookie: JSESSIONID=FicvJFvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
```



```

Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 10 Feb 2017 09:55:10 GMT
Accept-Ranges: bytes
Content-Length: 42489
Date: Thu, 18 Apr 2019 06:31:35 GMT
Content-Type: text/javascript; charset=UTF-8

/*
All content Copyright ♦ 2002-2003 Skire Inc..
*/

var LOCAL_TOP_PATH;

//Arrows for Sorting
var DArrow=new Image()
var UArrow=new Image()
DArrow.src="/webant/images/DownArrow.gif";
UArrow.src="/webant/images/UpArrow.gif";

//HTML fragments used in list view.
var stTab="<table style=\"width:100%;table-layout:fixed;\" ";
var stRow="<tr ";
var edRow="</tr>";
var stCol="<td ";
var edCol="</td>";
var edTab="</table>";

// state variables used during a column resize
var GObj=null;
var SortOrder="<";
var bDragSort=false;

// variables used for local sorting
var localsort_isAscending = false;
var localsort_lastColNum = 0;

// default mouse over cursor
var theMouseOverCursor = 'hand';

// mininum width of a column (global)
var minWidth = 50;

// variables used only in the main (name='') list view
var selectedColNum=-1;
var listHeight = "83.5%";
var listDataHeight = "97%";
var arrListViewHeading;
var arrListViewData=new Array();
var arrOtherHeading;
var arrOtherProperties=new Array();
var RightAlignedCols;
var CenterAlignedCols;
var CenterAlignedHead;
var RightAlignedHead;
var StringTypeCols = ""; // for local sort string column, with i18nSort flag on
var NumericTypeCols = ""; // for local sort numeric column, with i18nSort flag on
var searchType;
var totalPages=1;
var arrSearchResult;
var arrSubHeading=new Array();
var my_submit_search;
var spanFindHTML;
var lastViewSearch;
var defaultViewSearch="all";
var searchshow=false;

var bInitialized=false;
var G_arrData_linkto_otherProperties = false; // for improving local sorting performance
//Edited By Anandraj For Selection for the TextBoxes
var i18nSort = false;

function EnableSelect()
{

```

```

E=event.srcElement.type
if(E=="text" || E=="textarea")
    return true;
else
    return false;
}

function setI18nSort(doI18nSort) {
    i18nSort = doI18nSort;
}

function UpdateList()
{
    if (!bInitialized) {
        setTimeout('UpdateList();',100);
        return;
    }
    UpdateListView();
    UpdateArrow();
    UpdateSummary();
    ResetPointer();
}

function InitListView()
{
    searchType = defaultViewSearch;
    lastViewSearch = defaultViewSearch;
    page_is_digits();
    var ListView=document.getElementById("ListView");
    if (ListView.style.height)
        listHeight = ListView.style.height;
    else
    {
        if (mainform)
        {
            var formSpace = 19;
            listHeight = document.body.offsetHeight - mainform.offsetHeight -
formSpace;

            if (listHeight>=0)
                ListView.style.height = listHeight + "px";
        }
    }

    UpdateListView(1);
    try {
        if(eval(LOCAL_TOP_PATH).showLoading)
            eval(LOCAL_TOP_PATH).showLoading(self);
    }
    catch(e) {}
    setTimeout('bInitialized = true;',300);
}

// Functions to support multiple lists in tab-ed form
// Each list is controlled by a <div> with id=ListViewXXX where XXX is the list view name
function UpdateListView(firsttime)
{
    if (!bInitialized && firsttime == null) {
        setTimeout('UpdateListView();',100);
    }
    else {
        setMouseOverCursor('hand');
        UpdateListViewByName('');
    }
}

function UpdateListViewByName(name)
{
    var ss = new Array();

    var oLV=document.getElementById("ListView" + name);
    var oLVHeading=document.getElementById("ListViewHeading" + name);
    var oLVData=document.getElementById("ListViewData" + name);
    var arrHeading = eval("arrListViewHeading" + name);
    var arrData = eval("arrListViewData" + name);
    var CoulmnWidth=new Array();

    ss.push(stTab);
    ss.push(" style='table-layout:fixed;width:100%' ");

```

```

ss.push(" id=oListView");
ss.push(name);
ss.push(">");
ss.push(stRow);
ss.push(" style=\"height:15px;\">");

//Heading
eval("arrListViewIndex"+name+" = new Array()");
var arrIndex = eval("arrListViewIndex" + name);
var cindex = 0;
for(i=0;i<arrHeading.length;i++)
{
    CoulmnWidth[i]=arrHeading[i][0];
    if (CoulmnWidth[i] == 0)
        continue;
    arrIndex[i] = cindex++;

    var Tstr=arrHeading[i][1];
    var AImg="&nbsp;<img style=\"display:none;\" id="+name+"AI" + i + "
src=\"/webant/images/UpArrow.gif\" >";
    var TAlign=""; // align may need to follow data view

    var SortFunc="OnClick=";
    if (name == '')
        SortFunc += "SortListView(" + i + ")";
    else
        SortFunc += "LocalSortListView(" + i + ",\"" + name + "\")";

    //***** center or right align
    ...
    ...
    ...

```

低

“X-Content-Type-Options”头缺失或不安全 5

TOC

问题 1 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: http://172.31.3.33:7001/unifier_js/bluedoor/login_c.js

实体: login_c.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异:

推理: AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /unifier_js/bluedoor/login_c.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FicvJFvJvFH0Apg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Last-Modified: Thu, 15 Mar 2018 08:23:08 GMT
Accept-Ranges: bytes
Content-Length: 17627
Date: Thu, 18 Apr 2019 06:41:38 GMT
Content-Type: text/javascript; charset=UTF-8

var P = {
  winname: "unifier_top",

  initCheck: function(){

    if(P.loginForWeblogic){
      if(!P.errorMsg)
        this.clearErrMsg();
      this.enableLogin();

      return true;
    }

    if (this.initStatus != '1' && P.loginrole != 250){
      if(this.errorMsg && this.errorMsg != '')
        this.setErrMsg(this.errorMsg,true);
      this.setLoginFocus();
      setTimeout("loginInitCheck()", 2000);
      return false;
    }

    this.clearErrMsg();
    if(P.redirect_result){
      loginHandler(P.redirect_result);
      P.redirect_result = null;
      if(this.logoutRedirect == '')
        this.enableLogin();
    }
    else if (P.ssoProvider) {
      if ($('#security').length > 0)
        this.enableLogin();
      else
        loginSubmit(true);
    }
    else if(this.logoutRedirect != '')
      window.location.replace(this.logoutRedirect)
    else
      this.enableLogin();
    return true;
  },

  setLoginFocus: function(){
    if ($("#username").length>0 && $("#username").val() == '')
      $("#username").focus();
    else
      $("#password").focus();
  },

  checkException: function(resultJson, jqxhr){
    var status = jqxhr.status;
    if (status == 202 || status == 206) {
      P.setErrMsg((JSON.parse(resultJson)).message);
      return true;
    }
    return false;
  },

  setErrMsg: function(errMsg,retainFormCss){
```

```

        $(".errMsgClass").show();
        $(".errMsgClass").html(errMsg);
        $(".login-form").removeClass('form-animation');
        if(!retainFormCss)
            setTimeout(function(){ $(".login-form").addClass('form-animation') }, 0);
    },

    clearErrMsg: function(){
        $(".errMsgClass").html('');
        $(".errMsgClass").hide();
    },

    enableLogin: function(){
        if(!P.loginForWeblogic){
            if(P.submit_link) // already connected with handlers
                return;
            P.submit_link = $("#lsubmit").click(function(event){
                event.preventDefault();
                event.stopPropagation();
                if (P.authRefresh === "true" || P.ssoProvider == 'weblogic') {
                    window.location.reload();
                }
                else {
                    loginSubmit();
                }
            });
            $("#unamePword").keypress(function(event){
                if(event.which == 13){
                    loginSubmit();
                }
            });
            $("#fcancel").click(function(event){
                event.preventDefault();
                event.stopPropagation();
                fcancelSubmit();
            });
            $("#fsubmit").click(function(event){
                event.preventDefault();
                event.stopPropagation();
                fpasswordSubmit();
            });
            $("#fsignin").click(function(event){
                event.preventDefault();
                event.stopPropagation();
                fcancelSubmit();
            });
            if(shortcut.username){
                $('#username').val(shortcut.username);
                if (P.loginrole < 250) {
                    $('#username').prop('readonly', true);
                    $('#username').addClass("readonly");
                }

                $("#password").focus();
            } else {
                $("#username").focus();
            }
        }
        else
        {
            $("#username").focus();
            if (P.errorMsg)
                P.setErrMsg(P.errorMsg);
        }

        $("#lsubmit").prop('disabled', false);
    },

    getLoginPath: function(){
        if(!P.loginrole)
            return "/login";
        else if(P.loginrole == 1000)
            return "/qa";
        else if(P.loginrole == 300)
            return "/it";
        else if(P.loginrole == 250)
            return "/admin";
    }
}

```

```

        else if(P.loginrole == 200)
            return "/cs";
        else if(P.loginrole == 100)
            return "/ps";
        return "/login";
    },

    relogin: function(force){
        if(!force && P.unifier_top && !P.unifier_top.closed){
            P.unifier_top.focus();
            return;
        }
        if(!force && P.unifier_password && !P.unifier_password.closed){
            P.unifier_password.focus();
            return;
        }
        if(P.ssoProvider && P.ssoLogout) {
            window.location.replace(P.ssoLogout);
            return;
        }
        if(P.ssoProvider == 'weblogic') {
            window.location.reload();
            return;
        }
        if(this.logoutRedirect != ''){
            window.location.replace(this.logoutRedirect + P.servletPath +
this.getLoginPath())
            return;
        }
        if(force) this.last_submit = new Date();

        $('#login_frm').removeClass('hidden');
        $('#unamePwd').removeClass('hidden');
        $('#changePwd').addClass('hidden');

        $('#username').val("");
        $('#username').focus();
    }
}

function forgetPassword() {
    if (P.initStatus == '1'){
        P.clearErrMsg();

        $('#unamePwd').addClass('hidden').addClass('form-animation');
        $('#forgot').removeClass('hidden');
        $('#pwsent').addClass('hidden');

        $('#fusername').attr("type","text");
        $('#femail').attr("type","text");

        $
    }
}

```

“X-Content-Type-Options”头缺失或不安全

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/webant/js/dhtmllistview.js>

实体: dhtmllistview.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异:

推理: AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值, 这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /webant/js/dhtmllistview.js?l8.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor/viewPasswordPolicy?username=undefined
Cookie: JSESSIONID=F1cvJFxFvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Last-Modified: Fri, 10 Feb 2017 09:55:10 GMT
Accept-Ranges: bytes
Content-Length: 42489
Date: Thu, 18 Apr 2019 06:31:35 GMT
Content-Type: text/javascript; charset=UTF-8
```

```
/*
All content Copyright © 2002-2003 Skire Inc..
*/
```

```
var LOCAL_TOP_PATH;
```

```
//Arrows for Sorting
var DArrow=new Image()
var UArrow=new Image()
DArrow.src="/webant/images/DownArrow.gif";
UArrow.src="/webant/images/UpArrow.gif";
```

```
//HTML fragments used in list view.
var stTab="<table style=\"width:100%;table-layout:fixed;\" ";
var stRow="<tr ";
var edRow="</tr>";
var stCol="<td ";
var edCol="</td>";
var edTab="</table>";
```

```
// state variables used during a column resize
var GObj=null;
var SortOrder="<";
var bDragSort=false;
```

```
// variables used for local sorting
var localsort_isAscending = false;
var localsort_lastColNum = 0;
```

```
// default mouse over cursor
var theMouseOverCursor = 'hand';
```

```

// mininum width of a column (global)
var minWidth = 50;

// variables used only in the main (name='') list view
var selectedColNum=-1;
var listHeight = "83.5%";
var listDataHeight = "97%";
var arrListViewHeading;
var arrListViewData=new Array();
var arrOtherHeading;
var arrOtherProperties=new Array();
var RightAlignedCols;
var CenterAlignedCols;
var CenterAlignedHead;
var RightAlignedHead;
var StringTypeCols = ""; // for local sort string column, with il8nSort flag on
var NumericTypeCols = ""; // for local sort numeric column, with il8nSort flag on
var searchType;
var totalPages=1;
var arrSearchResult;
var arrSubHeading=new Array();
var my_submit_search;
var spanFindHTML;
var lastViewSearch;
var defaultViewSearch="all";
var searchshow=false;

var bInitialized=false;
var G_arrData_linkto_otherProperties = false; // for improving local sorting performance
//Edited By Anandraj For Selection for the TextBoxes
var il8nSort = false;

function EnableSelect()
{
    E=event.srcElement.type
    if(E=="text" || E=="textarea")
        return true;
    else
        return false;
}

function setIl8nSort(doIl8nSort) {
    il8nSort = doIl8nSort;
}

function UpdateList()
{
    if (!bInitialized) {
        setTimeout('UpdateList();',100);
        return;
    }
    UpdateListView();
    UpdateArrow();
    UpdateSummary();
    ResetPointer();
}

function InitListView()
{
    searchType = defaultViewSearch;
    lastViewSearch = defaultViewSearch;
    page_is_digits();
    var ListView=document.getElementById("ListView");
    if (ListView.style.height)
        listHeight = ListView.style.height;
    else
    {
        if (mainform)
        {
            var formSpace = 19;
            listHeight = document.body.offsetHeight - mainform.offsetHeight -
formSpace;
            if (listHeight>=0)
                ListView.style.height = listHeight + "px";
        }
    }

    UpdateListView(1);
}

```



```

try {
    if(eval(LOCAL_TOP_PATH).showLoading)
        eval(LOCAL_TOP_PATH).showLoading(self);
    }
catch(e) {}
setTimeout('bInitialized = true;',300);
}

// Functions to support multiple lists in tab-ed form
// Each list is controlled by a <div> with id=ListViewXXX where XXX is the list view name
function UpdateListView(firsttime)
{
    if (!bInitialized && firsttime == null) {
        setTimeout('UpdateListView();',100);
    }
    else {
        setMouseOverCursor('hand');
        UpdateListViewByName('');
    }
}

function UpdateListViewByName(name)
{
    var ss = new Array();

    var oLV=document.getElementById("ListView" + name);
    var oLVHeading=document.getElementById("ListViewHeading" + name);
    var oLVData=document.getElementById("ListViewData" + name);
    var arrHeading = eval("arrListViewHeading" + name);
    var arrData = eval("arrListViewData" + name);
    var CoulmnWidth=new Array();

    ss.push(stTab);
    ss.push(" style='table-layout:fixed;width:100%' ");
    ss.push(" id=oListView");
    ss.push(name);
    ss.push(">");
    ss.push(stRow);
    ss.push(" style=\"height:15px;\">");

    //Heading
    eval("arrListViewIndex"+name+" = new Array()");
    var arrIndex = eval("arrListViewIndex" + name);
    var cindex = 0;
    for(i=0;i<arrHeading.length;i++)
    {
        CoulmnWidth[i]=arrHeading[i][0];
        if (CoulmnWidth[i] == 0)
            continue;
        arrIndex[i] = cindex++;

        var Tstr=arrHeading[i][1];
        var AImg="&nbsp;<img style=\"display:none;\" id="+name+"AI" + i + "
src=\"/webant/images/UpArrow.gif\" >";
        var TAlign=""; // align may need to follow data view

        var SortFunc="OnClick=";
        if (name == '')
            SortFunc += "SortListView(" + i + ")";
        else
            SortFunc += "LocalSortListView(" + i + ",\"" + name + "\"";

        //***** center or right align
    }
    ...
    ...
    ...

```

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/webant/js/i18n/UnifierMenu.js>

实体: UnifierMenu.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异:

推理: AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值, 这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /webant/js/i18n/UnifierMenu.js?l8.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FlcvJFvJvFHoApg5oFD5Dz_RsU4DWFZjOMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 31 Jul 2018 06:28:08 GMT
Accept-Ranges: bytes
Content-Length: 27238
Date: Thu, 18 Apr 2019 06:41:40 GMT
Content-Type: text/javascript; charset=UTF-8
```

```
var UnifierMenu = {
  "Delete" : "Delete",
  "Left" : "Left",
  "Summary Cost Sheet" : "Summary Cost Sheet",
  "Query" : "Query",
  "View References" : "View References",
  "Last Deployment" : "Last Deployment",
  "Stop" : "Stop",
  "Move Down" : "Move Down",
  "Reply to All" : "Reply to All",
  "Export To Repository" : "Export To Repository",
  "Curve Distribution" : "Curve Distribution",
  "Check In" : "Check In",
  "Save & Lock" : "Save & Lock",
  "Deployed" : "Deployed",
  "User Mapping" : "User Mapping",
  "Insert" : "Insert",
  "Data Mapping" : "Data Mapping",
  "To Unifier Users" : "To Unifier Users",
  "End Discussion Group" : "End Discussion Group",
  "Editable (Required)" : "Editable (Required)",
  "Reload" : "Reload",
  "Company Dashboard" : "Company Dashboard",
  "PDF Format" : "PDF Format",
  "Move Up" : "Move Up",
  "Add Notes" : "Add Notes",
  "Owner Companies" : "Owner Companies",
  "Disable" : "Disable",
  "Shell Data Cube" : "Shell Data Cube",
  "Space" : "Space",
  "Status" : "Status",
  "Linked Records" : "Linked Records",
```

"My Documents" : "My Documents",
 "Lump Sum Line Item" : "Lump sum Line Item",
 "Run GC" : "Run GC",
 "Gantt" : "Gantt",
 "Role Attributes" : "Role Attributes",
 "Resource Booking" : "Resource Booking",
 "Timesheet" : "Timesheet",
 "My uMails" : "My uMails",
 "Unlock" : "Unlock",
 "Organize Folders" : "Organize Folders",
 "All Projects" : "All Projects",
 "Update Projects" : "Update Projects",
 "Curve Setup" : "Curve Setup",
 "Column Data" : "Column Data",
 "Delete Job" : "Delete Job",
 "Line" : "Line",
 "Fund Attributes" : "Fund Attributes",
 "Unhide" : "Unhide",
 "Flag for Follow up" : "Flag for Follow up",
 "Activate" : "Activate",
 "Last Published" : "Last Published",
 "From External Source" : "From External Source",
 "Uploaded in last 30 days" : "Uploaded in last 30 days",
 "Resource Properties" : "Resource Properties",
 "Detail Curves" : "Detail Curves",
 "Copy Cost" : "Copy Cost",
 "Planning" : "Planning",
 "Zoom In" : "Zoom In",
 "Update User Type" : "Update User Type",
 "Based on a Template" : "Based on a Template",
 "Send Data" : "Send Data",
 "Rows..." : "Rows...",
 "Wrap" : "Wrap",
 "All..." : "All...",
 "Lock Cluster" : "Lock Cluster",
 "Unlocked" : "Unlocked",
 "Selection" : "Selection",
 "Uploaded in last 7 days" : "Uploaded in last 7 days",
 "Migration History..." : "Migration History...",
 "HTML Format" : "HTML Format",
 "Drop Index" : "Drop Index",
 "Un-Publish" : "Un-Publish",
 "Errors/Warnings" : "Errors/Warnings",
 "Fill By" : "Fill By",
 "Unload" : "Unload",
 "Access Information" : "Access Information",
 "Breakdown" : "Breakdown",
 "Remove Attachment" : "Remove Attachment",
 "Search By Content" : "Search By Content",
 "Selected" : "Selected",
 "Download" : "Download",
 "Elbow" : "Elbow",
 "Table Indexes" : "Table Indexes",
 "Advance to Next Phase" : "Advance to Next Phase",
 "Columns" : "Columns",
 "Withdraw Submission" : "Withdraw Submission",
 "Get Data" : "Get Data",
 "Cancel Reservation" : "Cancel Reservation",
 "Publish Metadata" : "Publish Metadata",
 "Standard..." : "Standard...",
 "Unlock Cluster" : "Unlock Cluster",
 "Published" : "Published",
 "Forward" : "Forward",
 "Submit" : "Submit",
 "Asset Class" : "Asset Class",
 "Add Member" : "Add Member",
 "Index Rate" : "Index Rate",
 "Add" : "Add",
 "Delete Summary" : "Delete Summary",
 "Summary Schedule of Values Sheet" : "Summary Schedule of Values Sheet",
 "Assign to Funds" : "Assign to Funds",
 "Spelling..." : "Spelling...",
 "Start" : "Start",
 "Regular" : "Regular",
 "Column Details..." : "Column Details...",
 "Project/Shell" : "Project/Shell",
 "Assignments" : "Assignments",
 "Attachment" : "Attachment",

```

"About Unifier" : "About Unifier",
"Upgrade" : "Upgrade",
"Distribute" : "Distribute",
"RFB" : "RFB",
"Add Rows" : "Add Rows",
"Summary Worksheet" : "Summary Worksheet",
"Cash Flow Summary Curve" : "Cash Flow Summary Curve",
"Deploy to Gateway" : "Deploy to Gateway",
"Migrate Projects into Shells..." : "Migrate Projects into Shells...",
"Archive Project" : "Archive Project",
>Delete Rows..." : "Delete Rows...",
"Transfer Focus" : "Transfer Focus",
>Select Shell" : "Select Shell",
"Validation" : "Validation",
>Select Line Items" : "Select Line Items",
>Add Assignee to Current Step..." : "Add Assi
...
...
...

```

问题 4 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/webant/js/i18n/UnifierTab.js>

实体: UnifierTab.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异:

推理: AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应:

```

GET /webant/js/i18n/UnifierTab.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FlcvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Tue, 31 Jul 2018 06:28:10 GMT
Accept-Ranges: bytes
Content-Length: 3963
Date: Thu, 18 Apr 2019 06:41:40 GMT
Content-Type: text/javascript; charset=UTF-8

```

```

var UnifierTab = {
  "Time Sheet Line Items" : "Time Sheet Line Items",

```

```

"Query" : "Query",
"Address" : "Address",
"Activity" : "Activity",
"Segments" : "Segments",
"User Mapping" : "User Mapping",
"Security" : "Security",
"Space Types" : "Space Types",
"Data Mapping" : "Data Mapping",
"Assignment" : "Assignment",
"Month" : "Month",
"Tracking Gantt" : "Tracking Gantt",
"Currency" : "Currency",
"Permission" : "Permission",
"Tags" : "Tags",
"Settings" : "Settings",
"Parameters" : "Parameters",
"Main Form" : "Main Form",
"Adjustment" : "Adjustment",
"Data Mapping - Level" : "Data Mapping - Level",
"Workflow" : "Workflow",
"Roles" : "Roles",
"Grouping" : "Grouping",
"Booking Transactions" : "Booking Transactions",
"Add Range" : "Add Range",
"Project" : "Project",
"Transactions" : "Transactions",
"Statuses" : "Statuses",
"Template File" : "Template File",
"Projects/Shells" : "Projects/Shells",
"Distribution" : "Distribution",
"Validator Log" : "Validator Log",
"Dds list" : "Dds list",
"Resources" : "Resources",
"Rule" : "Rule",
"Current" : "Current",
"Week" : "Week",
"Members" : "Members",
"Value Set" : "Value Set",
"Data Mapping - Columns" : "Data Mapping - Columns",
"Notification" : "Notification",
"Cell Details" : "Cell Details",
"Behavior Set" : "Behavior Set",
"Gantt Chart" : "Gantt Chart",
"SmartForm" : "SmartForm",
"Groups" : "Groups",
"Business Processes" : "Business Processes",
"Breakdown" : "Breakdown",
"Activity Codes" : "Activity Codes",
"Structure" : "Structure",
"Download" : "Download",
"Progress" : "Progress",
"Define Blocks" : "Define Blocks",
"Calendar" : "Calendar",
"Columns" : "Columns",
"Custom" : "Custom",
"Data Mapping - Cost Attributes" : "Data Mapping - Cost Attributes",
"Sort Order" : "Sort Order",
"Custom Fields" : "Custom Fields",
"Layout" : "Layout",
"Day" : "Day",
"Data Mapping - Space Types" : "Data Mapping - Space Types",
"Curves" : "Curves",
"Task" : "Task",
"Record Copy" : "Record Copy",
"Region Format" : "Region Format",
"Attributes" : "Attributes",
"Mobile Log" : "Mobile Log",
"Data Set" : "Data Set",
"Process" : "Process",
"Organize" : "Organize",
"Proj. User" : "Proj. User",
"Permissions" : "Permissions",
"Dependencies" : "Dependencies",
"Element Log" : "Element Log",
"P6 Data Sources" : "P6 Data Sources",
"Send Email Test" : "Send Email Test",
"Sample Data" : "Sample Data",
"Programs" : "Programs",

```

```

"Views" : "Views",
"Resource" : "Resource",
"Step Settings" : "Step Settings",
"General" : "General",
"Unique" : "Unique",
"Notifications" : "Notifications",
"WBS Codes" : "CBS Codes",
"Server Connection Test" : "Server Connection Test",
"Cache" : "Cache",
"Options" : "Options",
"Report File" : "Report File",
"Rates" : "Rates",
"Referenced" : "Referenced",
"Projects" : "Projects",
"Hardcopy" : "Hardcopy",
"Step" : "Step",
"Properties" : "Properties",
"Proxy" : "Proxy",
"Consolidation" : "Consolidation",
"Auto Sequence" : "Auto Sequence",
"Skills" : "Skills",
"Data Elements" : "Data Elements",
"Custom Print" : "Custom Print",
"Preferences" : "Preferences",
"Lineitems" : "Line Items",
"Notes" : "Notes",
"Line Items" : "Line Items",
"Co. Currency" : "Co. Currency",
"Codes" : "Codes",
"Integration" : "Integration",
"Navigation" : "Navigation",
"Vendors" : "Vendors",
"Auto Creation" : "Auto Creation",
"Shells" : "Shells",
"Info" : "Info",
"Standards" : "Standards",
"Formula Log" : "Formula Log",
"Contact" : "Contact",
"Data Source" : "Data Source",
"Filter" : "Filter",
"Schedule" : "Schedule",
"Find" : "Find",
"Summary" : "Summary",
"Links" : "Links",
"Workflow Progress" : "Workflow Progress",
"Proj. Group" : "Proj. Group",
"Location" : "Location",
"Cash Flow" : "Cash Flow",
"Link Elements" : "Link Elements",
_end:""
}

```

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/studio/js/jquery-sha256.min.js>

实体: jquery-sha256.min.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异:

推理: AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值, 这可能会更大程度地暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /studio/js/jquery-sha256.min.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FlcvJFvFHoApg5oFD5Dz_RsU4DWFZjOMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Fri, 06 Mar 2015 10:20:46 GMT
Accept-Ranges: bytes
Content-Length: 3119
Date: Thu, 18 Apr 2019 06:41:40 GMT
Content-Type: text/javascript; charset=UTF-8

/**
 * SHA256 Hash Algorithm Plugin
 *
 * @version 1.1 (17/08/2012)
 * @requires jQuery v1.2.6+
 * @author Alex Weber <alexweber.com.br>
 * @copyright Copyright (c) 2008-2009, Alex Weber
 * @see http://anmar.eu.org/projects/jssha2/
 * @see http://pajhome.org.uk/crypt/md5
 *
 * Distributed under the terms of the new BSD License
 * http://www.opensource.org/licenses/bsd-license.php
 *
 */
(function(f){var m=8;var k=function(q,t){var s=(q&65535)+(t&65535);var r=(q>>16)+(t>>16)+(s>>16);return(r<<16)|(s&65535)};var e=function(r,q){return(r>>>q)|(r<<(32-q))};var g=function(r,q){return(r>>>q)};var a=function(q,s,r){return((q&s)^(~q&r))};var d=function(q,s,r){return((q&s)^(q&r)^(s&r))};var h=function(q){return(e(q,2)^e(q,13)^e(q,22))};var b=function(q){return(e(q,6)^e(q,11)^e(q,25))};var p=function(q){return(e(q,7)^e(q,18)^g(q,3))};var l=function(q){return(e(q,17)^e(q,19)^g(q,10))};var c=function(r,s){var E=new Array(1116352408,1899447441,3049323471,3921009573,961987163,1508970993,2453635748,2870763221,3624381080,310598401,607225278,1426881987,1925078388,2162078206,2614888103,3248222580,3835390401,4022224774,264347078,604807628,770255983,1249150122,1555081692,1996064986,2554220882,2821834349,2952996808,3210313671,3336571891,3584528711,113926993,338241895,666307205,773529912,1294757372,1396182291,1695183700,1986661051,2177026350,2456956037,2730485921,2820302411,3259730800,3345764771,3516065817,3600352804,4094571909,275423344,430227734,506948616,659060556,883997877,958139571,1322822218,1537002063,1747873779,1955562222,2024104815,2227730452,2361852424,2428436474,2756734187,3204031479,3329325298);var t=new Array(1779033703,3144134277,1013904242,2773480762,1359893119,2600822924,528734635,1541459225);var q=new Array(64);var G,F,D,C,A,y,x,w,v,u;var B,z;r[s>>5]|=128<<(24-s%32);r[((s+64)>>9)<<4+15]=s;for(var v=0;v<r.length;v+=16)
```

```

{G=t[0];F=t[1];D=t[2];C=t[3];A=t[4];y=t[5];x=t[6];w=t[7];for(var u=0;u<64;u++){if(u<16)
{q[u]=r[u+v]}else{q[u]=k(k(k(l(q[u-2])),q[u-7]),p(q[u-15])),q[u-
16])}B=k(k(k(k(w,b(A)),a(A,y,x)),E[u]),q[u]);z=k(h(G),d(G,F,D));w=x;x=y;y=A;A=k(C,B);C=D;D=F;F=G;
G=k(B,z)}t[0]=k(G,t[0]);t[1]=k(F,t[1]);t[2]=k(D,t[2]);t[3]=k(C,t[3]);t[4]=k(A,t[4]);t[5]=k(y,t[5]
);t[6]=k(x,t[6]);t[7]=k(w,t[7])}return t};var j=function(t){var s=Array();var q=(1<m)-1;for(var
r=0;r<t.length*m;r+=m){s[r>>5]|=(t.charCodeAt(r/m)&q)<<(24-r%32)}return s};var n=function(s){var
r="0123456789abcdef";var t="";for(var q=0;q<s.length*4;q++){t+=r.charAt((s[q>>2]>>((3-
q%4)*8+4))&15)+r.charAt((s[q>>2]>>((3-q%4)*8))&15)}return t};var o=function(s,v){var
u=j(s);if(u.length>16){u=c(u,s.length*m)}var q=Array(16),t=Array(16);for(var r=0;r<16;r++)
{q[r]=u[r]^909522486;t[r]=u[r]^1549556828}var w=c(q.concat(j(v)),512+v.length*m);return
c(t.concat(w),512+256)};var i=function(q){q=typeof q=="object"?f(q).val():q.toString();return
q};f.extend({sha256:function(q){q=i(q);return n(c(j(q),q.length*m))},sha256hmac:function(q,r)
{q=i(q);r=i(r);return n(o(q,r))},sha256config:function(q)
{m=parseInt(q||8)};f.fn.sha256=function(r){f.sha256config(r);var q=i(f(this).val());var
s=f.sha256(q);f.sha256config(8);return s}})(jQuery);

```

低

“X-XSS-Protection”头缺失或不安全 5

TOC

问题 1 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性:

低

CVSS 分数: 5.0

URL:

<http://172.31.3.33:7001/webant/js/dhtmlmlistview.js>

实体:

dhtmlmlistview.js (Page)

风险:

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因:

Web 应用程序编程或配置不安全

固定值:

将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```

GET /webant/js/dhtmlmlistview.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor/viewPasswordPolicy?username=undefined
Cookie: JSESSIONID=F1cvJFxFvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

```

```

HTTP/1.1 200 OK
Last-Modified: Fri, 10 Feb 2017 09:55:10 GMT
Accept-Ranges: bytes
Content-Length: 42489

```



```

Date: Thu, 18 Apr 2019 06:31:35 GMT
Content-Type: text/javascript; charset=UTF-8

/*
All content Copyright ♦ 2002-2003 Skire Inc..
*/

var LOCAL_TOP_PATH;

//Arrows for Sorting
var DArrow=new Image()
var UArrow=new Image()
DArrow.src="/webant/images/DownArrow.gif";
UArrow.src="/webant/images/UpArrow.gif";

//HTML fragments used in list view.
var stTab="<table style=\"width:100%;table-layout:fixed;\" ";
var stRow="<tr ";
var edRow="</tr>";
var stCol="<td ";
var edCol="</td>";
var edTab="</table>";

// state variables used during a column resize
var GObj=null;
var SortOrder="<";
var bDragSort=false;

// variables used for local sorting
var localsort_isAscending = false;
var localsort_lastColNum = 0;

// default mouse over cursor
var theMouseOverCursor = 'hand';

// minimum width of a column (global)
var minWidth = 50;

// variables used only in the main (name='') list view
var selectedColNum=-1;
var listHeight = "83.5%";
var listDataHeight = "97%";
var arrListViewHeading;
var arrListViewData=new Array();
var arrOtherHeading;
var arrOtherProperties=new Array();
var RightAlignedCols;
var CenterAlignedCols;
var CenterAlignedHead;
var RightAlignedHead;
var StringTypeCols = ""; // for local sort string column, with i18nSort flag on
var NumericTypeCols = ""; // for local sort numeric column, with i18nSort flag on
var searchType;
var totalPages=1;
var arrSearchResult;
var arrSubHeading=new Array();
var my_submit_search;
var spanFindHTML;
var lastViewSearch;
var defaultViewSearch="all";
var searchshow=false;

var bInitialized=false;
var G_arrData_linkto_otherProperties = false; // for improving local sorting performance
//Edited By Anandraj For Selection for the TextBoxes
var i18nSort = false;

function EnableSelect()
{
    E=event.srcElement.type
    if(E=="text" || E=="textarea")
        return true;
    else
        return false;
}

function setI18nSort(doI18nSort) {
    i18nSort = doI18nSort;
}

```

```

}

function UpdateList()
{
    if (!bInitialized) {
        setTimeout('UpdateList();',100);
        return;
    }
    UpdateListView();
    UpdateArrow();
    UpdateSummary();
    ResetPointer();
}

function InitListView()
{
    searchType = defaultViewSearch;
    lastViewSearch = defaultViewSearch;
    page_is_digits();
    var ListView=document.getElementById("ListView");
    if (ListView.style.height)
        listHeight = ListView.style.height;
    else
    {
        if (mainform)
        {
            var formSpace = 19;
            listHeight = document.body.offsetHeight - mainform.offsetHeight -
formSpace;
            if (listHeight>=0)
                ListView.style.height = listHeight + "px";
        }
    }

    UpdateListView(1);
    try {
        if(eval(LOCAL_TOP_PATH).showLoading)
            eval(LOCAL_TOP_PATH).showLoading(self);
    }
    catch(e) {}
    setTimeout('bInitialized = true;',300);
}

// Functions to support multiple lists in tab-ed form
// Each list is controlled by a <div> with id=ListViewXXX where XXX is the list view name
function UpdateListView(firsttime)
{
    if (!bInitialized && firsttime == null) {
        setTimeout('UpdateListView();',100);
    }
    else {
        setMouseOverCursor('hand');
        UpdateListViewByName('');
    }
}

function UpdateListViewByName(name)
{
    {
        var ss = new Array();

        var oLV=document.getElementById("ListView" + name);
        var oLVHeading=document.getElementById("ListViewHeading" + name);
        var oLVData=document.getElementById("ListViewData" + name);
        var arrHeading = eval("arrListViewHeading" + name);
        var arrData = eval("arrListViewData" + name);
        var CoulmnWidth=new Array();

        ss.push(stTab);
        ss.push(" style='table-layout:fixed;width:100%' ");
        ss.push(" id=oListView");
        ss.push(name);
        ss.push(">");
        ss.push(stRow);
        ss.push(" style=\"height:15px;\">");

        //Heading
        eval("arrListViewIndex"+name+" = new Array()");
        var arrIndex = eval("arrListViewIndex" + name);

```

```

var cindex = 0;
for(i=0;i<arrHeading.length;i++)
{
    CoulmnWidth[i]=arrHeading[i][0];
    if (CoulmnWidth[i] == 0)
        continue;
    arrIndex[i] = cindex++;

    var Tstr=arrHeading[i][1];
    var AImg="&nbsp;<img style=\"display:none;\" id="+name+"AI" + i + "
src=\"/webant/images/UpArrow.gif\" >";
    var TAlign=""; // align may need to follow data view

    var SortFunc="OnClick=";
    if (name == '')
        SortFunc += "SortListView(" + i + ")";
    else
        SortFunc += "LocalSortListView(" + i + ",\"" + name + "\")";

    //***** center or right align
    ...
    ...
    ...

```

问题 2 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/studio/js/jquery-sha256.min.js>

实体: jquery-sha256.min.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```

GET /studio/js/jquery-sha256.min.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Fri, 06 Mar 2015 10:20:46 GMT
Accept-Ranges: bytes
Content-Length: 3119
Date: Thu, 18 Apr 2019 06:41:40 GMT

```

Content-Type: text/javascript; charset=UTF-8

```
/**
 * SHA256 Hash Algorithm Plugin
 *
 * @version 1.1 (17/08/2012)
 * @requires jQuery v1.2.6+
 * @author Alex Weber <alexweber.com.br>
 * @copyright Copyright (c) 2008-2009, Alex Weber
 * @see http://anmar.eu.org/projects/jssha2/
 * @see http://pajhome.org.uk/crypt/md5
 *
 * Distributed under the terms of the new BSD License
 * http://www.opensource.org/licenses/bsd-license.php
 */
(function(f){var m=8;var k=function(q,t){var s=(q&65535)+(t&65535);var r=(q>>16)+(t>>16)+(s>>16);return(r<<16)|(s&65535)};var e=function(r,q){return(r>>>q)|(r<<(32-q))};var g=function(r,q){return(r>>>q)};var a=function(q,s,r){return((q&s)^((~q)&r))};var d=function(q,s,r){return((q&s)^(q&r)^(s&r))};var h=function(q){return(e(q,2)^e(q,13)^e(q,22))};var b=function(q){return(e(q,6)^e(q,11)^e(q,25))};var p=function(q){return(e(q,7)^e(q,18)^g(q,3))};var l=function(q){return(e(q,17)^e(q,19)^g(q,10))};var c=function(r,s){var E=new Array(1116352408,1899447441,3049323471,3921009573,961987163,1508970993,2453635748,2870763221,3624381080,310598401,607225278,1426881987,1925078388,2162078206,2614888103,3248222580,3835390401,4022224774,264347078,604807628,770255983,1249150122,1555081692,1996064986,2554220882,2821834349,2952996808,3210313671,3336571891,3584528711,113926993,338241895,666307205,773529912,1294757372,1396182291,1695183700,1986661051,2177026350,2456956037,2730485921,2820302411,3259730800,3345764771,3516065817,3600352804,4094571909,275423344,430227734,506948616,659060556,883997877,958139571,1322822218,1537002063,1747873779,1955562222,2024104815,2227730452,2361852424,2428436474,2756734187,3204031479,3329325298);var t=new Array(1779033703,3144134277,1013904242,2773480762,1359893119,2600822924,528734635,1541459225);var q=new Array(64);var G,F,D,C,A,Y,X,W,V,U;var B,Z;R[s>>5]|=128<<(24-s%32);R[(s+64>>9)<<4]+15=s;for(var v=0;v<R.length;v+=16){G=t[0];F=t[1];D=t[2];C=t[3];A=t[4];Y=t[5];X=t[6];W=t[7];for(var u=0;u<64;u++){if(u<16){q[u]=R[u+v]}else{q[u]=k(k(k(l(q[u-2])),q[u-7]),p(q[u-15])),q[u-16])}B=k(k(k(k(w,b(A))),a(A,Y,X)),E[u]),q[u];z=k(h(G),d(G,F,D));w=X;x=Y;y=A;A=k(C,B);C=D;D=F;F=G;G=k(B,Z)}t[0]=k(G,t[0]);t[1]=k(F,t[1]);t[2]=k(D,t[2]);t[3]=k(C,t[3]);t[4]=k(A,t[4]);t[5]=k(Y,t[5]);t[6]=k(X,t[6]);t[7]=k(W,t[7])}return t};var j=function(t){var s=Array();var q=(1<<m)-1;for(var r=0;r<t.length*m;r+=m){s[r>>5]|=(t.charCodeAt(r/m)&q)<<(24-r%32)}return s};var n=function(s){var r="0123456789abcdef";var t="";for(var q=0;q<s.length*4;q++){t+=r.charAt((s[q>>2]>>((3-q%4)*8+4))&15)+r.charAt((s[q>>2]>>((3-q%4)*8))&15)}return t};var o=function(s,v){var u=j(s);if(u.length>16){u=c(u,s.length*m)}var q=Array(16),t=Array(16);for(var r=0;r<16;r++){q[r]=u[r]^909522486;t[r]=u[r]^1549556828}var w=c(q.concat(j(v)),512+v.length*m);return c(t.concat(w),512+256)};var i=function(q){q=typeof q=="object"?f(q).val():q.toString();return q};f.extend({sha256:function(q){q=i(q);return n(c(j(q),q.length*m))},sha256hmac:function(q,r){q=i(q);r=i(r);return n(o(q,r))},sha256config:function(q){m=parseInt(q||8)};f.fn.sha256=function(r){f.sha256config(r);var q=i(f(this).val());var s=f.sha256(q);f.sha256config(8);return s}})(jQuery);
```

“X-XSS-Protection”头缺失或不安全

严重性: **低**

CVSS 分数: 5.0

URL: http://172.31.3.33:7001/unifier_js/bluedoor/login_c.js

实体: login_c.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```
GET /unifier_js/bluedoor/login_c.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=F1cvJFxFvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Last-Modified: Thu, 15 Mar 2018 08:23:08 GMT
Accept-Ranges: bytes
Content-Length: 17627
Date: Thu, 18 Apr 2019 06:41:38 GMT
Content-Type: text/javascript; charset=UTF-8
```

```
var P = {
  winname: "unifier_top",

  initCheck: function(){

    if(P.loginForWeblogic){
      if(!P.errorMsg)
        this.clearErrMsg();
      this.enableLogin();

      return true;
    }

    if (this.initStatus != '1' && P.loginrole != 250){
      if(this.errorMsg && this.errorMsg != '')
        this.setErrMsg(this.errorMsg,true);
      this.setLoginFocus();
      setTimeout("loginInitCheck()", 2000);
      return false;
    }

    this.clearErrMsg();
    if(P.redirect_result){
      loginHandler(P.redirect_result);
      P.redirect_result = null;
      if(this.logoutRedirect == '')
        this.enableLogin();
    }
    else if (P.ssoProvider) {
      if ($('#security').length > 0)
        this.enableLogin();
      else
```

```

        loginSubmit(true);
    }
    else if(this.logoutRedirect != '')
        window.location.replace(this.logoutRedirect)
    else
        this.enableLogin();
    return true;
},

setLoginFocus: function(){
    if ($("#username").length>0 && $("#username").val() == '')
        $("#username").focus();
    else
        $("#password").focus();
},

checkException: function(resultJson, jqxhr){
    var status = jqxhr.status;
    if (status == 202 || status == 206) {
        P.setErrMsg((JSON.parse(resultJson)).message);
        return true;
    }
    return false;
},

setErrMsg: function(errMsg,retainFormCss){
    $(".errMsgClass").show();
    $(".errMsgClass").html(errMsg);
    $(".login-form").removeClass('form-animation');
    if(!retainFormCss)
        setTimeout(function(){ $(".login-form").addClass('form-animation') },0);
},

clearErrMsg: function(){
    $(".errMsgClass").html('');
    $(".errMsgClass").hide();
},

enableLogin: function(){
    if(!P.loginForWeblogic){
        if(P.submit_link) // already connected with handlers
            return;
        P.submit_link = $("#lsubmit").click(function(event){
            event.preventDefault();
            event.stopPropagation();
            if (P.authRefresh === "true" || P.ssoProvider == 'weblogic') {
                window.location.reload();
            }
            else {
                loginSubmit();
            }
        });
        $("#unamePword").keypress(function(event){
            if(event.which == 13){
                loginSubmit();
            }
        });
        $("#fcancel").click(function(event){
            event.preventDefault();
            event.stopPropagation();
            fcancelSubmit();
        });
        $("#fsubmit").click(function(event){
            event.preventDefault();
            event.stopPropagation();
            fpasswordSubmit();
        });
        $("#fsignin").click(function(event){
            event.preventDefault();
            event.stopPropagation();
            fcancelSubmit();
        });
        if(shortcut.username){
            $('#username').val(shortcut.username);
            if (P.loginrole < 250) {
                $('#username').prop('readonly', true);
                $('#username').addClass("readonly");
            }
        }
    }
}

```

```

        $("#password").focus();
    } else {
        $("#username").focus();
    }
}

else
{
    $("#username").focus();
    if (P.errorMsg)
        P.setErrMsg(P.errorMsg);
}

$("#lsubmit").prop('disabled', false);
},

getLoginPath: function() {

    if(!P.loginrole)
        return "/login";
    else if(P.loginrole == 1000)
        return "/qa";
    else if(P.loginrole == 300)
        return "/it";
    else if(P.loginrole == 250)
        return "/admin";
    else if(P.loginrole == 200)
        return "/cs";
    else if(P.loginrole == 100)
        return "/ps";
    return "/login";
},

relogin: function(force) {
    if(!force && P.unifier_top && !P.unifier_top.closed) {
        P.unifier_top.focus();
        return;
    }
    if(!force && P.unifier_password && !P.unifier_password.closed) {
        P.unifier_password.focus();
        return;
    }
    if(P.ssoProvider && P.ssoLogout) {
        window.location.replace(P.ssoLogout);
        return;
    }
    if(P.ssoProvider == 'weblogic') {
        window.location.reload();
        return;
    }
    if(this.logoutRedirect != '') {
        window.location.replace(this.logoutRedirect + P.servletPath +
this.getLoginPath())
        return;
    }
    if(force) this.last_submit = new Date();

    $('#login_frm').removeClass('hidden');
    $('#unamePwd').removeClass('hidden');
    $('#changePwd').addClass('hidden');

    $('#username').val("");
    $('#username').focus();
}

}

function forgetPassword() {
    if (P.initStatus == '1') {
        P.clearErrMsg();

        $('#unamePwd').addClass('hidden').addClass('form-animation');
        $('#forgot').removeClass('hidden');
        $('#pwsent').addClass('hidden');

        $('#fusername').attr("type", "text");
        $('#femail').attr("type", "text");

        $

```

...
...
...

问题 4 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/webant/js/i18n/UnifierTab.js>

实体: UnifierTab.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```
GET /webant/js/i18n/UnifierTab.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=F1cvJFvJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
Last-Modified: Tue, 31 Jul 2018 06:28:10 GMT
Accept-Ranges: bytes
Content-Length: 3963
Date: Thu, 18 Apr 2019 06:41:40 GMT
Content-Type: text/javascript; charset=UTF-8
```

```
var UnifierTab = {
  "Time Sheet Line Items" : "Time Sheet Line Items",
  "Query" : "Query",
  "Address" : "Address",
  "Activity" : "Activity",
  "Segments" : "Segments",
  "User Mapping" : "User Mapping",
  "Security" : "Security",
  "Space Types" : "Space Types",
  "Data Mapping" : "Data Mapping",
  "Assignment" : "Assignment",
  "Month" : "Month",
  "Tracking Gantt" : "Tracking Gantt",
  "Currency" : "Currency",
  "Permission" : "Permission",
  "Tags" : "Tags",
  "Settings" : "Settings",
  "Parameters" : "Parameters",
```


"Main Form" : "Main Form",
 "Adjustment" : "Adjustment",
 "Data Mapping - Level" : "Data Mapping - Level",
 "Workflow" : "Workflow",
 "Roles" : "Roles",
 "Grouping" : "Grouping",
 "Booking Transactions" : "Booking Transactions",
 "Add Range" : "Add Range",
 "Project" : "Project",
 "Transactions" : "Transactions",
 "Statuses" : "Statuses",
 "Template File" : "Template File",
 "Projects/Shells" : "Projects/Shells",
 "Distribution" : "Distribution",
 "Validator Log" : "Validator Log",
 "Dds list" : "Dds list",
 "Resources" : "Resources",
 "Rule" : "Rule",
 "Current" : "Current",
 "Week" : "Week",
 "Members" : "Members",
 "Value Set" : "Value Set",
 "Data Mapping - Columns" : "Data Mapping - Columns",
 "Notification" : "Notification",
 "Cell Details" : "Cell Details",
 "Behavior Set" : "Behavior Set",
 "Gantt Chart" : "Gantt Chart",
 "SmartForm" : "SmartForm",
 "Groups" : "Groups",
 "Business Processes" : "Business Processes",
 "Breakdown" : "Breakdown",
 "Activity Codes" : "Activity Codes",
 "Structure" : "Structure",
 "Download" : "Download",
 "Progress" : "Progress",
 "Define Blocks" : "Define Blocks",
 "Calendar" : "Calendar",
 "Columns" : "Columns",
 "Custom" : "Custom",
 "Data Mapping - Cost Attributes" : "Data Mapping - Cost Attributes",
 "Sort Order" : "Sort Order",
 "Custom Fields" : "Custom Fields",
 "Layout" : "Layout",
 "Day" : "Day",
 "Data Mapping - Space Types" : "Data Mapping - Space Types",
 "Curves" : "Curves",
 "Task" : "Task",
 "Record Copy" : "Record Copy",
 "Region Format" : "Region Format",
 "Attributes" : "Attributes",
 "Mobile Log" : "Mobile Log",
 "Data Set" : "Data Set",
 "Process" : "Process",
 "Organize" : "Organize",
 "Proj. User" : "Proj. User",
 "Permissions" : "Permissions",
 "Dependencies" : "Dependencies",
 "Element Log" : "Element Log",
 "P6 Data Sources" : "P6 Data Sources",
 "Send Email Test" : "Send Email Test",
 "Sample Data" : "Sample Data",
 "Programs" : "Programs",
 "Views" : "Views",
 "Resource" : "Resource",
 "Step Settings" : "Step Settings",
 "General" : "General",
 "Unique" : "Unique",
 "Notifications" : "Notifications",
 "WBS Codes" : "CBS Codes",
 "Server Connection Test" : "Server Connection Test",
 "Cache" : "Cache",
 "Options" : "Options",
 "Report File" : "Report File",
 "Rates" : "Rates",
 "Referenced" : "Referenced",
 "Projects" : "Projects",
 "Hardcopy" : "Hardcopy",
 "Step" : "Step",

```

"Properties" : "Properties",
"Proxy" : "Proxy",
"Consolidation" : "Consolidation",
"Auto Sequence" : "Auto Sequence",
"Skills" : "Skills",
"Data Elements" : "Data Elements",
"Custom Print" : "Custom Print",
"Preferences" : "Preferences",
"Lineitems" : "Line Items",
"Notes" : "Notes",
"Line Items" : "Line Items",
"Co. Currency" : "Co. Currency",
"Codes" : "Codes",
"Integration" : "Integration",
"Navigation" : "Navigation",
"Vendors" : "Vendors",
"Auto Creation" : "Auto Creation",
"Shells" : "Shells",
"Info" : "Info",
"Standards" : "Standards",
"Formula Log" : "Formula Log",
"Contact" : "Contact",
"Data Source" : "Data Source",
"Filter" : "Filter",
"Schedule" : "Schedule",
"Find" : "Find",
"Summary" : "Summary",
"Links" : "Links",
"Workflow Progress" : "Workflow Progress",
"Proj. Group" : "Proj. Group",
"Location" : "Location",
"Cash Flow" : "Cash Flow",
"Link Elements" : "Link Elements",
_end:""
}

```

问题 5 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/webant/js/i18n/UnifierMenu.js>

实体: UnifierMenu.js (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```

GET /webant/js/i18n/UnifierMenu.js?l18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor

```

Cookie: JSESSIONID=FicvJFxFvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Tue, 31 Jul 2018 06:28:08 GMT
Accept-Ranges: bytes
Content-Length: 27238
Date: Thu, 18 Apr 2019 06:41:40 GMT
Content-Type: text/javascript; charset=UTF-8

```
var UnifierMenu = {
  "Delete" : "Delete",
  "Left" : "Left",
  "Summary Cost Sheet" : "Summary Cost Sheet",
  "Query" : "Query",
  "View References" : "View References",
  "Last Deployment" : "Last Deployment",
  "Stop" : "Stop",
  "Move Down" : "Move Down",
  "Reply to All" : "Reply to All",
  "Export To Repository" : "Export To Repository",
  "Curve Distribution" : "Curve Distribution",
  "Check In" : "Check In",
  "Save & Lock" : "Save & Lock",
  "Deployed" : "Deployed",
  "User Mapping" : "User Mapping",
  "Insert" : "Insert",
  "Data Mapping" : "Data Mapping",
  "To Unifier Users" : "To Unifier Users",
  "End Discussion Group" : "End Discussion Group",
  "Editable (Required)" : "Editable (Required)",
  "Reload" : "Reload",
  "Company Dashboard" : "Company Dashboard",
  "PDF Format" : "PDF Format",
  "Move Up" : "Move Up",
  "Add Notes" : "Add Notes",
  "Owner Companies" : "Owner Companies",
  "Disable" : "Disable",
  "Shell Data Cube" : "Shell Data Cube",
  "Space" : "Space",
  "Status" : "Status",
  "Linked Records" : "Linked Records",
  "My Documents" : "My Documents",
  "Lump Sum Line Item" : "Lump sum Line Item",
  "Run GC" : "Run GC",
  "Gantt" : "Gantt",
  "Role Attributes" : "Role Attributes",
  "Resource Booking" : "Resource Booking",
  "Timesheet" : "Timesheet",
  "My uMails" : "My uMails",
  "Unlock" : "Unlock",
  "Organize Folders" : "Organize Folders",
  "All Projects" : "All Projects",
  "Update Projects" : "Update Projects",
  "Curve Setup" : "Curve Setup",
  "Column Data" : "Column Data",
  "Delete Job" : "Delete Job",
  "Line" : "Line",
  "Fund Attributes" : "Fund Attributes",
  "Unhide" : "Unhide",
  "Flag for Follow up" : "Flag for Follow up",
  "Activate" : "Activate",
  "Last Published" : "Last Published",
  "From External Source" : "From External Source",
  "Uploaded in last 30 days" : "Uploaded in last 30 days",
  "Resource Properties" : "Resource Properties",
  "Detail Curves" : "Detail Curves",
  "Copy Cost" : "Copy Cost",
  "Planning" : "Planning",
  "Zoom In" : "Zoom In",
  "Update User Type" : "Update User Type",
  "Based on a Template" : "Based on a Template",
  "Send Data" : "Send Data",
  "Rows..." : "Rows...",
```

```

"Wrap" : "Wrap",
"All..." : "All...",
"Lock Cluster" : "Lock Cluster",
"Unlocked" : "Unlocked",
"Selection" : "Selection",
"Uploaded in last 7 days" : "Uploaded in last 7 days",
"Migration History..." : "Migration History...",
"HTML Format" : "HTML Format",
"Drop Index" : "Drop Index",
"Un-Publish" : "Un-Publish",
"Errors/Warnings" : "Errors/Warnings",
"Fill By" : "Fill By",
"Unload" : "Unload",
"Access Information" : "Access Information",
"Breakdown" : "Breakdown",
"Remove Attachment" : "Remove Attachment",
"Search By Content" : "Search By Content",
"Selected" : "Selected",
"Download" : "Download",
"Elbow" : "Elbow",
"Table Indexes" : "Table Indexes",
"Advance to Next Phase" : "Advance to Next Phase",
"Columns" : "Columns",
"Withdraw Submission" : "Withdraw Submission",
"Get Data" : "Get Data",
"Cancel Reservation" : "Cancel Reservation",
"Publish Metadata" : "Publish Metadata",
"Standard..." : "Standard...",
"Unlock Cluster" : "Unlock Cluster",
"Published" : "Published",
"Forward" : "Forward",
"Submit" : "Submit",
"Asset Class" : "Asset Class",
"Add Member" : "Add Member",
"Index Rate" : "Index Rate",
"Add" : "Add",
>Delete Summary" : "Delete Summary",
"Summary Schedule of Values Sheet" : "Summary Schedule of Values Sheet",
"Assign to Funds" : "Assign to Funds",
"Spelling..." : "Spelling...",
"Start" : "Start",
"Regular" : "Regular",
"Column Details..." : "Column Details...",
"Project/Shell" : "Project/Shell",
"Assignments" : "Assignments",
"Attachment" : "Attachment",
>About Unifier" : "About Unifier",
"Upgrade" : "Upgrade",
"Distribute" : "Distribute",
"RFB" : "RFB",
"Add Rows" : "Add Rows",
"Summary Worksheet" : "Summary Worksheet",
"Cash Flow Summary Curve" : "Cash Flow Summary Curve",
"Deploy to Gateway" : "Deploy to Gateway",
"Migrate Projects into Shells..." : "Migrate Projects into Shells...",
"Archive Project" : "Archive Project",
>Delete Rows..." : "Delete Rows...",
"Transfer Focus" : "Transfer Focus",
>Select Shell" : "Select Shell",
"Validation" : "Validation",
>Select Line Items" : "Select Line Items",
"Add Assignee to Current Step..." : "Add Assi
...
...
...

```

Oracle 日志文件信息泄露

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: sqlnet.log (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 关闭跟踪, 限制对日志文件的访问, 或者将其除去

差异: cookie 已从请求除去: `F1cvJFxJvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`参数 已从请求除去: `uuu812352716t1`路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/sqlnet.log`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/sqlnet.log? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=VIgvPECD-Vr8LZZJTbqyVEGmrE9_6BMM-uYahce58DaQpelUi0so!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:18 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref": "",
    "i18ndebug":0,

```

```

        "loginTimeout":1200,
        "locale":"en",
        "token":null,
        "isDevelopment":false
    },
    "UserVariable":
    {
        "date":
        {
            "shortformat":"yyyy/MM/dd",
            "timezone":"Asia/Shanghai",
            "dateformat":"yyyy/MM/dd hh:mm a",
            "localformat": "(UTC+8)"
        },
        "number":
        {
            "decimalSymbol":".",
            "negativeCurrencyFormat":"-#1.1",
            "negativeDecimalFormat":"-1.1",
            "digitGrouping":"#,##0",
            "showCurrencySymbol":"false",
            "positiveCurrencyFormat":"#1.1",
            "groupingSymbol":", "
        }
    }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxymaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !='undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}

```

```
</script>
</head>
</html>
```

问题 2 / 6

TOC

Oracle 日志文件信息泄露

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bp/nav/user/>

实体: sqlnet.trc (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 关闭跟踪, 限制对日志文件的访问, 或者将其除去

差异: **cookie** 已从请求除去: `FICvJFxJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`

参数 已从请求除去: `uuu812352716t1`

路径 从以下位置进行控制: `/bp/nav/user/company_home` 至: `/bp/nav/user/sqlnet.trc`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/user/sqlnet.trc? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/nav/company/home?__uref=uuu221487287t1
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=CcMvPKL8wcAMW_DQbLha34Jb9BqnlU90YrIq5ct6hpEvnzYKcBhM!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:44 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init({
  "SystemVariable":
```

```

{
  "locales":
  {
    "en": "English"
  },
  "codeVersion": "18.8",
  "uref": "",
  "il8ndebug": 0,
  "loginTimeout": 1200,
  "locale": "en",
  "token": null,
  "isDevelopment": false
},
"UserVariable":
{
  "date":
  {
    "shortformat": "yyyy/MM/dd",
    "timezone": "Asia/Shanghai",
    "dateformat": "yyyy/MM/dd hh:mm a",
    "localformat": " (UTC+8)"
  },
  "number":
  {
    "decimalSymbol": ".",
    "negativeCurrencyFormat": "-#1.1",
    "negativeDecimalFormat": "-1.1",
    "digitGrouping": "#,##0",
    "showCurrencySymbol": "false",
    "positiveCurrencyFormat": "#1.1",
    "groupingSymbol": ",",
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/il8n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) != 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

}

window.onload = function(){
if (window.name != "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

  try {

```



```

        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 3 / 6

TOC

Oracle 日志文件信息泄露

严重性:	低
CVSS 分数:	5.0
URL:	http://172.31.3.33:7001/bp/nav/
实体:	sqlnet.trc (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值:	关闭跟踪，限制对日志文件的访问，或者将其除去

差异: **cookie** 已从请求除去: `F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/sqlnet.trc`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/sqlnet.trc? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=AF0vPEGnn_u9LBQv_vh2WnVnE3JqtBhm_c86npABD8I6ErmvTYoI!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:19 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```

```

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "il8ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/il8n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
if (window.name !== "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)

```

```

        self.parent.UResetSubmit();

        if (self.pointer_is_set_to_wait)
            self.ResetPointer();
        else if (self.parent && self.parent.pointer_is_set_to_wait)
            self.parent.ResetPointer();

        try {
            topWin = eval(LOCAL_TOP_PATH);
        } catch(e) {
            window.location.replace('/index.html');
            return;
        };
        U.AlertByKey("session_expired",sessionExpiredCallback)
    }
}
</script>
</head>
</html>

```

问题 4 / 6

TOC

Oracle 日志文件信息泄露

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: sqlnet.log (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 关闭跟踪，限制对日志文件的访问，或者将其除去

差异: **cookie** 已从请求除去: `F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/sqlnet.log`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/sqlnet.log? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=bNwvPDmUBb1jU17tdS4Dhxno2yb2ufakXZgqQBu7ru1Nbx6pgWLD!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge

```

```
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:17 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "il8ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/il8n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}
```

```

    }
}

window.onload = function(){
  if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

问题 5 / 6

TOC

Oracle 日志文件信息泄露

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: sqlnet.trc (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 关闭跟踪，限制对日志文件的访问，或者将其除去

差异: **cookie** 已从请求除去: `F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/sqlnet.trc`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/sqlnet.trc? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=Jv8vPESAPs1PlYk1L083LQC_LzPf2h_9Teuko5OdNdZEOUmWuoK2!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:19 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "il8ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/il8n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  }
```

```

    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 6 / 6

TOC

Oracle 日志文件信息泄露

严重性:	低
CVSS 分数:	5.0
URL:	http://172.31.3.33:7001/bp/nav/user/
实体:	sqlnet.log (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因:	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值:	关闭跟踪，限制对日志文件的访问，或者将其除去

差异: cookie 已从请求除去: F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
 参数 已从请求除去: uuu812352716t1
 路径 从以下位置进行控制: /bp/nav/user/company_home 至: /bp/nav/user/sqlnet.log

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/user/sqlnet.log? HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/nav/company/home?__uref=uuu221487287t1
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=f88vPKCoviJW05taja5QpFULuf43plrA5yTUVJ68x8VzbsZngQHeC!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:43 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": "(UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```



```

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

低

查询中接受的主体参数 ①

TOC

问题 1 / 1

TOC

查询中接受的主体参数

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/bluedoor>

实体: bluedoor (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

差异: 主体参数 已从请求除去: test
查询参数 已添加至请求: test
主体参数 已从请求除去: test@altoromutual.com
查询参数 已添加至请求: test@altoromutual.com
主体参数 已从请求除去: --
查询参数 已添加至请求: --
主体参数 已从请求除去: 1234
查询参数 已添加至请求: 1234
方法 从以下位置进行控制: POST 至: GET

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”类似, 这表明应用程序处理了查询总提交的主体参数。

测试请求和响应:

```
GET /bluedoor?username=test&email=test%40altoromutual.com&question=&answer=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FicvJFxJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145
Connection: Keep-Alive
Host: 172.31.3.33:7001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:31:33 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="zh_CN"><head><title>Primavera Unifier &#x767b;&#x5f55;</title><meta
http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/><link rel="shortcut icon"
href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript"
src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript"
src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript"
src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
```

```

    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "zh_CN",
    "token": "1468919253826338277",
    "isDevelopment": false
  },
  "UserVariable": {
    "date": {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number": {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "#-1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "true",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString_zh_CN.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab_zh_CN.js?18.8" ></script>
<link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico" />
<link rel="stylesheet" href="/unifier_js/bluedoor/login_c.css?18.8" type="text/css" />
<style type="text/css">
.login-page {
  width: 100%;
  margin-left: 0;
}
.branding {
  margin: 0;
  margin-left: calc(50% - 200px);
}
.consent.retrodialog .ui-dialog-content {
  width: calc(95% + 8px) !important;
  padding: 0px;
  margin: 10px;
}
.ui-dialog.consent, .ui-dialog.consent .ui-dialog-content, .ui-dialog.consent .ui-dialog-
buttonset {
  background: #F3F3F3 !important;
}
.ui-dialog.consent .ui-dialog-buttonpane{
  padding-right: 5px;
  margin-top: 0px;
  padding-top: 0px;
  background-color: #f3f3f3 !important;
}
.ui-dialog.consent .ui-dialog-buttonset > button:first-child, .ui-dialog.consent .ui-dialog-
buttonset > button:first-child .ui-button-text{
  background-color: #616977;
  background-image: none;
}
</style>

<script type="text/javascript" src="/unifier_js/bluedoor/landing.js?18.8" ></script>
<script type="text/javascript">
// framebusting
if(self != top){ top.location = self.location; }

var shortcut = {
  username: '',
  p: '0',
  m: 'user',
  k: 'unifier'

```

```

};
shortcut.id = '';
shortcut.open_rec = true;

P.application = 'Unifier';
P.loginPath = '/unifier'
P.ssoProvider = '';
P.ssoLogout = '';
P.loginPath = P.ssoLogout;

P.loginrole = '0';
P.navMode = 'user';

P.servletPath = '/bluedoor';
P.logoutRedirect = '';

P.consentInfo =
{
  "enabled":false
}

</script>
</head>

<body class="background-info-tech">
  <div class="login-page">
    <div class="branding">
      
      <div class="app-family-logo app-name">Unifier</div>
    </div>

    <div id="processing" class="page-spinner page-loading-spinner page-spinner-static">
      <div class="spinner-label" id="loading-modal-label"> 正在加载...</div>
      <div class="spinner-larg
...
...
...

```

低

检测到隐藏目录 2

TOC

问题 1 / 2

TOC

检测到隐藏目录

严重性: **低**

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/g/>

实体: g/ (Page)

风险: 可能会检索有关站点文件系统结构的信息, 这可能会帮助攻击者映射此 Web 站点

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 对禁止的资源发布“404 - Not Found”响应状态代码, 或者将其完全除去

差异: 路径 从以下位置进行控制: `/bluedoor` 至: `/g/`

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

测试请求和响应:

```
GET /g/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Content-Length: 1166
Date: Thu, 18 Apr 2019 06:33:14 GMT
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Draft//EN">
<HTML>
<HEAD>
<TITLE>Error 403--Forbidden</TITLE>
</HEAD>
<BODY bgcolor="white">
<FONT FACE=Helvetica><BR CLEAR=all>
<TABLE border=0 cellspacing=5><TR><TD><BR CLEAR=all>
<FONT FACE="Helvetica" COLOR="black" SIZE="3"><H2>Error 403--Forbidden</H2>
</FONT></TD></TR>
</TABLE>
<TABLE border=0 width=100% cellpadding=10><TR><TD VALIGN=top WIDTH=100% BGCOLOR=white><FONT
FACE="Courier New"><FONT FACE="Helvetica" SIZE="3"><H3>From RFC 2068 <i>Hypertext Transfer
Protocol -- HTTP/1.1</i></H3>
</FONT><FONT FACE="Helvetica" SIZE="3"><H4>10.4.4 403 Forbidden</H4>
</FONT><P><FONT FACE="Courier New">The server understood the request, but is refusing to fulfill
it. Authorization will not help and the request SHOULD NOT be repeated. If the request method was
not HEAD and the server wishes to make public why the request has not been fulfilled, it SHOULD
describe the reason for the refusal in the entity. This status code is commonly used when the
server does not wish to reveal exactly why the request has been refused, or when no other
response is applicable.</FONT></P>
</FONT></TD></TR>
</TABLE>

</BODY>
</HTML>
```

检测到隐藏目录

严重性: 低

CVSS 分数: 5.0

URL: <http://172.31.3.33:7001/pub/>

实体: pub/ (Page)

风险: 可能会检索有关站点文件系统结构的信息, 这可能会帮助攻击者映射此 Web 站点

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 对禁止的资源发布“404 - Not Found”响应状态代码, 或者将其完全除去

差异: 路径 从以下位置进行控制: `/bluedoor` 至: `/pub/`

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

测试请求和响应:

```
GET /pub/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Content-Length: 0
Date: Thu, 18 Apr 2019 06:33:37 GMT
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Content-Type: text/html; charset=UTF-8
```

问题 1 / 1

TOC

发现可能的服务器路径泄露模式

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/webant/js/i18n/UnifierString.js>

实体: UnifierString.js (Page)

风险: 可能会检索 Web 服务器安装的绝对路径, 这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

原因: 未安装第三方产品的最新补丁或最新修补程序

固定值: 为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异:

推理: 响应应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应:

```
GET /webant/js/i18n/UnifierString.js?18.8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bluedoor
Cookie: JSESSIONID=FicvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145
Connection: keep-alive
Host: 172.31.3.33:7001
Accept: */*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Tue, 31 Jul 2018 06:28:10 GMT
Accept-Ranges: bytes
Content-Length: 455137
Date: Thu, 18 Apr 2019 06:41:46 GMT
Content-Type: text/javascript; charset=UTF-8

var UnifierString = {
  "All Notifications" : "All Notifications",
  "Summary Cost Sheet" : "Summary Cost Sheet",
  "Attachments Preview" : "Attachments Preview",
  "Day {0} from close of reporting period" : "Day {0} from close of reporting period",
  "Company Id not found for project {0}" : "Company Id not found for project {0}",
  "Director:" : "Director:",
  "Inform User Before Expiration" : "Inform User Before Expiration",
  "The import of package has been successful and below changes have been performed for this environment {0}" : "The import of package has been successful and below changes have been performed for this environment {0}",
  "Project Title" : "Project Title",
  "Password expiration:" : "Password expiration:",
  "Expand Groups" : "Expand Groups",
```

```

"Edit Drilldown Block" : "Edit Drilldown Block",
"Bid Invitation" : "Bid Invitation",
"Accepted" : "Accepted",
"is_project_mail" : "is_project_mail",
"Fund Attributes" : "Fund Attributes",
"The following elements will be cleared. Click Yes to continue.<BR><BR>" : "The
following elements will be cleared. Click Yes to continue.<BR><BR>",
"Query Timeout (millis):" : "Query Timeout (millis):",
"With Folder Structure" : "With Folder Structure",
"<b>{0}</b> is sent to you for <b>{1}</b>." : "<b>{0}</b> is sent to you for <b>{1}
</b>.",
"No permission to Data Cube." : "No permission to Data Cube.",
"Contact your system administration for details" : "Contact your system administration
for details",
"Bcc" : "Bcc",
"Net Book Value:" : "Net Book Value:",
"Schedule Sheet Properties updated Successfully" : "Schedule Sheet Properties updated
Successfully",
"Bcc:" : "Bcc:",
"Activity Templates" : "Activity Templates",
"Do you want to continue import" : "Do you want to continue import",
"Project Phase:" : "Project Phase:",
"Hard Booked" : "Hard Booked",
"Q" : "Q",
"Selected projects updating completed with some errors" : "Selected projects updating
completed with some errors",
"Budget and Progress Method Setup" : "Budget and Progress Method Setup",
"Title:" : "Title:",
"Add selected Users" : "Add selected Users",
"Breakdown" : "Breakdown",
"Y" : "Y",
"Main View" : "Main View",
"There is no connection between Unifier and Content Repository" : "There is no
connection between Unifier and Content Repository",
"Directory" : "Directory",
"Default Profile for new records" : "Default Profile for new records",
"Email Subscription:" : "Email Subscription:",
"Center" : "Center",
"Date Function" : "Date Function",
"Remove Attachments" : "Remove Attachments",
"Gate Conditions" : "Gate Conditions",
"Generic Cost Sheet" : "Generic Cost Sheet",
"Inherited from Group" : "Inherited from Group",
"uCAD Editable" : "uCAD Editable",
"Step Editors:" : "Step Editors:",
"Red" : "Red",
"Ref" : "Ref",
"Valid Finish Date is required." : "Valid Finish Date is required.",
"Consolidate comments" : "Consolidate comments",
"Cashflow Curve Refresh: History" : "Cashflow Curve Refresh: History",
"Project Phases" : "Project Phases",
"Import {0} From {1}" : "Import {0} From {1}",
"Deselect" : "Deselect",
"Select the folder structures to be added or updated in the destination environment" :
"Select the folder structures to be added or updated in the destination environment",
"Query Parameters" : "Query Parameters",
"System Usage" : "System Usage",
"Contract Data" : "Contract Data",
"TCPI(BAC)" : "TCPI(BAC)",
"Add" : "Add",
"Save As Snapshot new" : "Save As Snapshot new",
"Configuration pack
...
...
...

"Source Data Element:" : "Source Data Element:",
"Search" : "Search",
"Save Record information to Document<br> Manager:" : "Save Record information to
Document<br> Manager:",
"space_mgr_text1" : "Note: The \'.dwf\' and \'.unf\' files associated with each drawing
file must be uploaded.",
"space_mgr_text2" : "By default, the \'.dwf\' and \'.unf\' files are located either in
the folder that contains the corresponding \'.dwg\' files or in C:\Program Files
(x86)\Oracle\Primavera-Unifier\uCAD\data on your Computer.",
"Publish to Document Manager" : "Publish to Document Manager",
"SOAP Services" : "SOAP Services",
"Import from Design Repository" : "Import from Design Repository",

```



```
"Email Subscription->Successful Creation" : "Email Subscription->Successful Creation",
...
...
...
```

参

检测到应用程序测试脚本 28

TOC

问题 1 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFxFvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145](#)
参数 已从请求除去: [uuu812352716t1](#)
路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/company/test>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=mHMvPIkg3mQwprZz6IxhDJsLty82gwnzt6WUkJ0uT7iNnvYGH42v!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:37 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !='undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
if (window.name != "aframe") {
  if (self.UAlreadySubmitted)

```

```

        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 2 / 28

TOC

检测到应用程序测试脚本

严重性:	参考
CVSS 分数:	0.0
URL:	http://172.31.3.33:7001/bp/nav/
实体:	test (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=ZisvPImkNKhRcTNGwqivVnmQk8XNJa-z-nC2jyyNjYmcQKy-zwB!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff

```

Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:37 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref": "",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) != 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
```

```

        self.parent.close();
    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 3 / 28

TOC

检测到应用程序测试脚本

严重性:	参考
CVSS 分数:	0.0
URL:	http://172.31.3.33:7001/bp/nav/company/
实体:	test.php (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去服务器中的测试脚本

差异: cookie 已从请求除去: `F1cvJFxFjvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.php`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/test.php? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

```

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=7CMvPInzhE4xuqZ2nid6GfjWZN_SwcB0au54LBFdUGiML-SgyaBM!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:37 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }
}
```

```

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
    if (window.name !== "aframe") {
        if (self.UAlreadySubmitted)
            self.UResetSubmit();
        else if (self.parent && self.parent.UAlreadySubmitted)
            self.parent.UResetSubmit();

        if (self.pointer_is_set_to_wait)
            self.ResetPointer();
        else if (self.parent && self.parent.pointer_is_set_to_wait)
            self.parent.ResetPointer();

        try {
            topWin = eval(LOCAL_TOP_PATH);
        } catch(e) {
            window.location.replace('/index.html');
            return;
        };
        U.AlertByKey("session_expired",sessionExpiredCallback)
    }
}
</script>
</head>
</html>

```

问题 4 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.php3 (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFvJvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/company/test.php3](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.php3? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=9ZEvPI4ZD2EtXbvN--m8qvjQWBs3TqW65aNMe_AwJo1ZGptCMG3T!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:38 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "il8ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": "(UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/il8n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/il8n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```



```

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

问题 5 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.php (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/test.php>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.php? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=2A4vPIuRBmGppKNtyYNVwiAGvdFmIH_jGss03nAjYuvIq45Hq0Lo!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:38 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ","
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
```

```

type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxyMaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.asp (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJFvJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`

参数 已从请求除去: `uuu812352716t1`

路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.asp`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.asp? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu812352716t1
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=ocgvPJAvlbPVReP6FHbyPd4wUz2kPzKdQe-2WZqmEckKk-5IWB84!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:39 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
```

```

{
  "date":
  {
    "shortformat": "yyyy/MM/dd",
    "timezone": "Asia/Shanghai",
    "dateformat": "yyyy/MM/dd hh:mm a",
    "localformat": " (UTC+8)"
  },
  "number":
  {
    "decimalSymbol": ".",
    "negativeCurrencyFormat": "-#1.1",
    "negativeDecimalFormat": "-1.1",
    "digitGrouping": "#,##0",
    "showCurrencySymbol": "false",
    "positiveCurrencyFormat": "#1.1",
    "groupingSymbol": ",",
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) != 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
if (window.name != "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

  try {
    topWin = eval(LOCAL_TOP_PATH);
  } catch(e) {
    window.location.replace('/index.html');
    return;
  };
  U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性:

参考

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.php3 (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: cookie 已从请求除去: `FIcvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`参数 已从请求除去: `uuu812352716t1`路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.php3`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.php3? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=fqsvPJE0DP9JY09Iy-Pld9iY0dZeoZGXzkD5EsNjMGP5hOGDU_0Q!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:39 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init({
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
```

```

        "i18ndebug":0,
        "loginTimeout":1200,
        "locale":"en",
        "token":null,
        "isDevelopment":false
    },
    "UserVariable":
    {
        "date":
        {
            "shortformat":"yyyy/MM/dd",
            "timezone":"Asia/Shanghai",
            "dateformat":"yyyy/MM/dd hh:mm a",
            "localformat":" (UTC+8)"
        },
        "number":
        {
            "decimalSymbol":".",
            "negativeCurrencyFormat":"-#1.1",
            "negativeDecimalFormat":"-1.1",
            "digitGrouping":"#,##0",
            "showCurrencySymbol":"false",
            "positiveCurrencyFormat":"#1.1",
            "groupingSymbol":", "
        }
    }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxymaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !=='undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
    if (window.name !== "aframe") {
        if (self.UAlreadySubmitted)
            self.UResetSubmit();
        else if (self.parent && self.parent.UAlreadySubmitted)
            self.parent.UResetSubmit();

        if (self.pointer_is_set_to_wait)
            self.ResetPointer();
        else if (self.parent && self.parent.pointer_is_set_to_wait)
            self.parent.ResetPointer();

        try {
            topWin = eval(LOCAL_TOP_PATH);
        } catch(e) {
            window.location.replace('/index.html');
            return;
        };
        U.AlertByKey("session_expired",sessionExpiredCallback)
    }
}

```

```
}  
</script>  
</head>  
</html>
```

问题 8 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.aspx (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJFxFvFH0Agg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`

参数 已从请求除去: `uuu812352716t1`

路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.aspx`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.aspx? HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287  
Connection: keep-alive  
Host: 172.31.3.33:7001  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK  
X-Frame-Options: sameorigin  
Set-Cookie: JSESSIONID=ur4vPJGVSV60DNTh_NFNi-Boay9a476F6-GVi7xg_d8RjvwmtYDx!1186003145; path=/  
HttpOnly  
X-Content-Type-Options: nosniff  
Expires: Wed, 31 Dec 1969 23:59:59 GMT  
x-ua-compatible: IE=edge  
X-XSS-Protection: 1; mode=block  
Date: Thu, 18 Apr 2019 06:57:39 GMT  
Content-Type: text/html; charset=UTF-8  
Cache-Control: max-age=0, no-store, no-cache  
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-  
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-  
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script  
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script  
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script  
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(  
{
```



```

"SystemVariable":
{
  "locales":
  {
    "en":"English"
  },
  "codeVersion":"18.8",
  "uref": "",
  "i18ndebug":0,
  "loginTimeout":1200,
  "locale":"en",
  "token":null,
  "isDevelopment":false
},
"UserVariable":
{
  "date":
  {
    "shortformat":"yyyy/MM/dd",
    "timezone":"Asia/Shanghai",
    "dateformat":"yyyy/MM/dd hh:mm a",
    "localformat":" (UTC+8)"
  },
  "number":
  {
    "decimalSymbol":".",
    "negativeCurrencyFormat":"-#1.1",
    "negativeDecimalFormat":"-1.1",
    "digitGrouping":"#,##0",
    "showCurrencySymbol":"false",
    "positiveCurrencyFormat":"#1.1",
    "groupingSymbol":", "
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch (e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

}

window.onload = function(){
if (window.name !== "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();
}

```

```

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 9 / 28

TOC

检测到应用程序测试脚本

严重性:	参考
CVSS 分数:	0.0
URL:	http://172.31.3.33:7001/bp/nav/
实体:	test.asp (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJFxFjvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.asp`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test.asp? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=1xQvPJ90aD5nYF2kxPqNbLcS628uK2nEPkGVzhh6U3Z_vtRm9gw!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:39 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```

```

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !=='undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
  }
}

```

```

else if (self.parent && self.parent.UAreadySubmitted)
    self.parent.UResetSubmit();

if (self.pointer_is_set_to_wait)
    self.ResetPointer();
else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 10 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.cgi (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0ApG5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/company/test.cgi](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/test.cgi? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=id8vPJ8ZbUjIvId136SKQU99wm_ZxumxAKFREb9V5HHnhLdGGAA!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT

```

```
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:39 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch (e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}
```

```

    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 11 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.htm (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.htm`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/test.htm? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=GgwvPJNNhZfSAslX6MbBgKxOgbuxnGrJsvyLiIKEAv327up3w3p6!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8" type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }
}
```

```
try {
```

```

        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 12 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.aspx (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/test.aspx>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:


```
GET /bp/nav/test.aspx? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=8VEvPJMyRJV3YtXVK5stDtCBK78mpsPHo816ijpkgsnMQ3Wz2Hu!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
}</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

问题 13 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.html (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu11186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/company/test.html>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.html? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=ki4vPJPF2F2QURM4HVC_asqsSqB9I3Ylv786v7vjUWWLHKovtOzpC!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ""
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
```

```

type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxyMaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) != 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.cgi (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `FIcvJFvJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`

参数 已从请求除去: `uuu812352716t1`

路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.cgi`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.cgi? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu812352716t1
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=sCsvPJPZlBu36yIr0uAP_P8GpTYCIulgVR2QRb3fKYy_UM0T4q1f!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
```

```

{
  "date":
  {
    "shortformat": "yyyy/MM/dd",
    "timezone": "Asia/Shanghai",
    "dateformat": "yyyy/MM/dd hh:mm a",
    "localformat": " (UTC+8)"
  },
  "number":
  {
    "decimalSymbol": ".",
    "negativeCurrencyFormat": "-#1.1",
    "negativeDecimalFormat": "-1.1",
    "digitGrouping": "#,##0",
    "showCurrencySymbol": "false",
    "positiveCurrencyFormat": "#1.1",
    "groupingSymbol": ",",
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) != 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
if (window.name != "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

  try {
    topWin = eval(LOCAL_TOP_PATH);
  } catch(e) {
    window.location.replace('/index.html');
    return;
  };
  U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性:

参考

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.cfm (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: cookie 已从请求除去: `F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZj0MRV70QSY5yzMSQrEMqu!1186003145`参数 已从请求除去: `uuu812352716t1`路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.cfm`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.cfm? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=VmwvPJRIrtqA7JIPWQkhILzUZmaiaa2TKwxOnQSZfLGcoqQjMoF8!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init({
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
```

```

        "i18ndebug":0,
        "loginTimeout":1200,
        "locale":"en",
        "token":null,
        "isDevelopment":false
    },
    "UserVariable":
    {
        "date":
        {
            "shortformat":"yyyy/MM/dd",
            "timezone":"Asia/Shanghai",
            "dateformat":"yyyy/MM/dd hh:mm a",
            "localformat":" (UTC+8)"
        },
        "number":
        {
            "decimalSymbol":".",
            "negativeCurrencyFormat":"-#1.1",
            "negativeDecimalFormat":"-1.1",
            "digitGrouping":"#,##0",
            "showCurrencySymbol":"false",
            "positiveCurrencyFormat":"#1.1",
            "groupingSymbol":",",
        }
    }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxymaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !=='undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
    if (window.name !== "aframe") {
        if (self.UAlreadySubmitted)
            self.UResetSubmit();
        else if (self.parent && self.parent.UAlreadySubmitted)
            self.parent.UResetSubmit();

        if (self.pointer_is_set_to_wait)
            self.ResetPointer();
        else if (self.parent && self.parent.pointer_is_set_to_wait)
            self.parent.ResetPointer();

        try {
            topWin = eval(LOCAL_TOP_PATH);
        } catch(e) {
            window.location.replace('/index.html');
            return;
        };
        U.AlertByKey("session_expired",sessionExpiredCallback)
    }
}

```



```
}  
</script>  
</head>  
</html>
```

问题 16 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.htm (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJFxFvFH0Agg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`

参数 已从请求除去: `uuu812352716t1`

路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.htm`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.htm? HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287  
Connection: keep-alive  
Host: 172.31.3.33:7001  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK  
X-Frame-Options: sameorigin  
Set-Cookie: JSESSIONID=UBsvPJR6ivqqIvSoQIhKONxMdEdhznbrUZazDMobjKLuZJmvINIK!1186003145; path=/  
HttpOnly  
X-Content-Type-Options: nosniff  
Expires: Wed, 31 Dec 1969 23:59:59 GMT  
x-ua-compatible: IE=edge  
X-XSS-Protection: 1; mode=block  
Date: Thu, 18 Apr 2019 06:57:40 GMT  
Content-Type: text/html; charset=UTF-8  
Cache-Control: max-age=0, no-store, no-cache  
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-  
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-  
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script  
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script  
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script  
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(  
{
```

```

"SystemVariable":
{
  "locales":
  {
    "en":"English"
  },
  "codeVersion":"18.8",
  "uref":"",
  "i18ndebug":0,
  "loginTimeout":1200,
  "locale":"en",
  "token":null,
  "isDevelopment":false
},
"UserVariable":
{
  "date":
  {
    "shortformat":"yyyy/MM/dd",
    "timezone":"Asia/Shanghai",
    "dateformat":"yyyy/MM/dd hh:mm a",
    "localformat":" (UTC+8)"
  },
  "number":
  {
    "decimalSymbol":".",
    "negativeCurrencyFormat":"-#1.1",
    "negativeDecimalFormat":"-1.1",
    "digitGrouping":"#,##0",
    "showCurrencySymbol":"false",
    "positiveCurrencyFormat":"#1.1",
    "groupingSymbol":", "
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch (e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

}

window.onload = function(){
if (window.name !== "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();
}

```

```

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 17 / 28

TOC

检测到应用程序测试脚本

严重性:	参考
CVSS 分数:	0.0
URL:	http://172.31.3.33:7001/bp/nav/company/
实体:	test.pl (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `FIcvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.pl`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/test.pl? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=x3QvPJSeiNouiqwFo6LZqxI28eKdYrHa8-gznzmoDx1HX7tc5g8!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```

```

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !=='undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
  }
}

```

```

else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.URResetSubmit();

if (self.pointer_is_set_to_wait)
    self.ResetPointer();
else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 18 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.html (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFxFvFHoApG5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu11186003145](#)
参数 已从请求除去: [uuu812352716t1](#)
路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/test.html](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test.html? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=DssvPJTQZV6KPUge2AVDt6G8mspZoP9Two2iRBPkWStTFR_YGt5C!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT

```

```
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch (e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}
```

```

    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 19 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.cfm (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.cfm`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test.cfm? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=BwUvPJUFgEGknpYxOS53oXAMFPJm8ETEJzQWlqUVfvUp7nlxyH3E!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8" type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }
}
```

```
try {
```



```

        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 20 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.dbf (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFxFjvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/company/test.dbf](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.dbf? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=sTwvPJT-dJtUPSOPkkV7jMt9X4aG9GueIC20LgZeJyWdY9zhYxs_!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
}</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8" type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8" type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

问题 21 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.shtml (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/company/test.shtml>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.shtml? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=D3cvPJWPR5EWPVNpojYQTyghj1_G4Kvfjni2_-y4mUndK-vLy_K!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat": "yyyy/MM/dd",
      "timezone": "Asia/Shanghai",
      "dateformat": "yyyy/MM/dd hh:mm a",
      "localformat": " (UTC+8)"
    },
    "number":
    {
      "decimalSymbol": ".",
      "negativeCurrencyFormat": "-#1.1",
      "negativeDecimalFormat": "-1.1",
      "digitGrouping": "#,##0",
      "showCurrencySymbol": "false",
      "positiveCurrencyFormat": "#1.1",
      "groupingSymbol": ""
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
```

```

type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxyMaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.pl (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFvJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/test.pl](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.pl? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu812352716t1
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=oswvPJv9SjYc56JRW4eQNEddl3Pgiz11Y3-O4Q7V6NtsRDwQIkii!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
    "i18ndebug": 0,
    "loginTimeout": 1200,
    "locale": "en",
    "token": null,
    "isDevelopment": false
  },
  "UserVariable":
```

```

{
  "date":
  {
    "shortformat": "yyyy/MM/dd",
    "timezone": "Asia/Shanghai",
    "dateformat": "yyyy/MM/dd hh:mm a",
    "localformat": " (UTC+8)"
  },
  "number":
  {
    "decimalSymbol": ".",
    "negativeCurrencyFormat": "-#1.1",
    "negativeDecimalFormat": "-1.1",
    "digitGrouping": "#,##0",
    "showCurrencySymbol": "false",
    "positiveCurrencyFormat": "#1.1",
    "groupingSymbol": ",",
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) != 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
if (window.name != "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

  try {
    topWin = eval(LOCAL_TOP_PATH);
  } catch(e) {
    window.location.replace('/index.html');
    return;
  };
  U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性:

参考

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/company/>

实体: test.txt (Page)

风险: 可能会下载临时脚本文件, 这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: cookie 已从请求除去: `F1cvJFxJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`参数 已从请求除去: `uuu812352716t1`路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.txt`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/company/test.txt? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=mgMvPJZICWV6M1AQiFLKklw0isKVlaKI76v1amzJ5Q3-8plo3q0Y!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:40 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"><script type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init({
  "SystemVariable":
  {
    "locales":
    {
      "en": "English"
    },
    "codeVersion": "18.8",
    "uref": "",
```



```

        "i18ndebug":0,
        "loginTimeout":1200,
        "locale":"en",
        "token":null,
        "isDevelopment":false
    },
    "UserVariable":
    {
        "date":
        {
            "shortformat":"yyyy/MM/dd",
            "timezone":"Asia/Shanghai",
            "dateformat":"yyyy/MM/dd hh:mm a",
            "localformat":" (UTC+8)"
        },
        "number":
        {
            "decimalSymbol":".",
            "negativeCurrencyFormat":"-#1.1",
            "negativeDecimalFormat":"-1.1",
            "digitGrouping":"#,##0",
            "showCurrencySymbol":"false",
            "positiveCurrencyFormat":"#1.1",
            "groupingSymbol":",",
        }
    }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
    if (topWin && !topWin.closed && topWin.login) {
        topWin.proxymaster = '';
        topWin.login();
    }

    try {
        window.close();
    } catch(e) {
        if (typeof(topWin) !=='undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
    if (window.name !== "aframe") {
        if (self.UAlreadySubmitted)
            self.UResetSubmit();
        else if (self.parent && self.parent.UAlreadySubmitted)
            self.parent.UResetSubmit();

        if (self.pointer_is_set_to_wait)
            self.ResetPointer();
        else if (self.parent && self.parent.pointer_is_set_to_wait)
            self.parent.ResetPointer();

        try {
            topWin = eval(LOCAL_TOP_PATH);
        } catch(e) {
            window.location.replace('/index.html');
            return;
        };
        U.AlertByKey("session_expired",sessionExpiredCallback)
    }
}

```

```
}  
</script>  
</head>  
</html>
```

问题 24 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.dbf (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Agg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/test.dbf](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.dbf? HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287  
Connection: keep-alive  
Host: 172.31.3.33:7001  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK  
X-Frame-Options: sameorigin  
Set-Cookie: JSESSIONID=nGQvPJZR4AjcJEI6PPTV-gAPzAYFQBWs6kYnxW1luUHTkw4wxpbO!1186003145; path=/  
HttpOnly  
X-Content-Type-Options: nosniff  
Expires: Wed, 31 Dec 1969 23:59:59 GMT  
x-ua-compatible: IE=edge  
X-XSS-Protection: 1; mode=block  
Date: Thu, 18 Apr 2019 06:57:40 GMT  
Content-Type: text/html; charset=UTF-8  
Cache-Control: max-age=0, no-store, no-cache  
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-  
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-  
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script  
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script  
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script  
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(  
{
```

```

"SystemVariable":
{
  "locales":
  {
    "en":"English"
  },
  "codeVersion":"18.8",
  "ueref":"",
  "i18ndebug":0,
  "loginTimeout":1200,
  "locale":"en",
  "token":null,
  "isDevelopment":false
},
"UserVariable":
{
  "date":
  {
    "shortformat":"yyyy/MM/dd",
    "timezone":"Asia/Shanghai",
    "dateformat":"yyyy/MM/dd hh:mm a",
    "localformat":" (UTC+8)"
  },
  "number":
  {
    "decimalSymbol":".",
    "negativeCurrencyFormat":"-#1.1",
    "negativeDecimalFormat":"-1.1",
    "digitGrouping":"#,##0",
    "showCurrencySymbol":"false",
    "positiveCurrencyFormat":"#1.1",
    "groupingSymbol":","
  }
}
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch (e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

}

window.onload = function(){
if (window.name !== "aframe") {
  if (self.UAlreadySubmitted)
    self.UResetSubmit();
  else if (self.parent && self.parent.UAlreadySubmitted)
    self.parent.UResetSubmit();

  if (self.pointer_is_set_to_wait)
    self.ResetPointer();
  else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();
}

```

```

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

检测到应用程序测试脚本

严重性:	参考
CVSS 分数:	0.0
URL:	http://172.31.3.33:7001/bp/nav/company/
实体:	test.jsp (Page)
风险:	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	在生产环境中留下临时文件
固定值:	除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `FIcvJfXJvFHoApg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/company/test.jsp`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/company/test.jsp? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=Jg8vPJbB-VfQ-Gt2skQGgFBQyzZ71UOf_LfARXZg2WpBjKYKGFh-!1186003145; path=/; HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:41 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked

```

```

<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !=='undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
  }
}

```

```

else if (self.parent && self.parent.UAreadySubmitted)
    self.parent.UResetSubmit();

if (self.pointer_is_set_to_wait)
    self.ResetPointer();
else if (self.parent && self.parent.pointer_is_set_to_wait)
    self.parent.ResetPointer();

try {
    topWin = eval(LOCAL_TOP_PATH);
} catch(e) {
    window.location.replace('/index.html');
    return;
};
U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 26 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.shtml (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: [F1cvJFxFvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: [/bp/nav/company/home](#) 至: [/bp/nav/test.shtml](#)

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test.shtml? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=I80vPJcTsLNJ2ss_yiH152j3__Za4ladgRJ6TTfGI-s5Dvf_iAdd!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT

```

```
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:41 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !='undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}
```

```

    }
}

window.onload = function(){
if (window.name != "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 27 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.txt (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: 除去服务器中的测试脚本

差异: **cookie** 已从请求除去: `F1cvJfXJvFH0Apg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145`
参数 已从请求除去: `uuu812352716t1`
路径 从以下位置进行控制: `/bp/nav/company/home` 至: `/bp/nav/test.txt`

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```

GET /bp/nav/test.txt? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```



```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=NrIvPJd4cv8wdhK9ederjzzgrY6xvKg5ou8aKX3QmabKFVz5V6Ev!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:41 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":",",
    }
  }
});</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```
function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxymaster = '';
    topWin.login();
  }
}
```

```
try {
```

```

        window.close();
    } catch(e) {
        if (typeof(topWin) !== 'undefined') {
            topWin.clickToLogout = true;
            topWin.close();
        }
        else if (self.parent) {
            self.parent.close();
        }
    }
}

window.onload = function(){
if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
        self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
        self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
        self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
        self.parent.ResetPointer();

    try {
        topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
        window.location.replace('/index.html');
        return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
}
}
</script>
</head>
</html>

```

问题 28 / 28

TOC

检测到应用程序测试脚本

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://172.31.3.33:7001/bp/nav/>

实体: test.jsp (Page)

风险: 可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

原因: 在生产环境中留下临时文件

固定值: [除去服务器中的测试脚本](#)

差异: **cookie** 已从请求除去: [F1cvJfXJvFH0Agg5oFD5Dz_RsU4DWFZjoMRV70QSY5yzMSQrEMqu!1186003145](#)

参数 已从请求除去: [uuu812352716t1](#)

路径 从以下位置进行控制: </bp/nav/company/home> 至: </bp/nav/test.jsp>

推理: AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求和响应:

```
GET /bp/nav/test.jsp? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://172.31.3.33:7001/bp/route/1/i-projectname?__uref=uuu221487287
Connection: keep-alive
Host: 172.31.3.33:7001
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
Set-Cookie: JSESSIONID=w-YvPJf-hSqt5e9-YVzePOmR7i16PM8odWHEld2GjglmGTCSxeBm!1186003145; path=/;
HttpOnly
X-Content-Type-Options: nosniff
Expires: Wed, 31 Dec 1969 23:59:59 GMT
x-ua-compatible: IE=edge
X-XSS-Protection: 1; mode=block
Date: Thu, 18 Apr 2019 06:57:41 GMT
Content-Type: text/html; charset=UTF-8
Cache-Control: max-age=0, no-store, no-cache
Transfer-Encoding: chunked
```

```
<!DOCTYPE html><html lang="en"><head><title>Unifier Notification</title><meta http-equiv="X-UA-
Compatible" content="IE=edge"/><meta http-equiv="Content-Type" content="text/html; charset=UTF-
8"/><link rel="shortcut icon" href="/unifier_js/bluedoor/images/favicon.ico"/><script
type="text/javascript" src="/studio/js/jquery-1.12.3.min.js?18.8" ></script><script
type="text/javascript" src="/studio/js/jquery-ui-1.12.1.custom.min.js?18.8" ></script><script
type="text/javascript" src="/webant/js/unifier_util.js?18.8" ></script><script>U.init(
{
  "SystemVariable":
  {
    "locales":
    {
      "en":"English"
    },
    "codeVersion":"18.8",
    "uref":"",
    "i18ndebug":0,
    "loginTimeout":1200,
    "locale":"en",
    "token":null,
    "isDevelopment":false
  },
  "UserVariable":
  {
    "date":
    {
      "shortformat":"yyyy/MM/dd",
      "timezone":"Asia/Shanghai",
      "dateformat":"yyyy/MM/dd hh:mm a",
      "localformat":" (UTC+8)"
    },
    "number":
    {
      "decimalSymbol":".",
      "negativeCurrencyFormat":"-#1.1",
      "negativeDecimalFormat":"-1.1",
      "digitGrouping":"#,##0",
      "showCurrencySymbol":"false",
      "positiveCurrencyFormat":"#1.1",
      "groupingSymbol":", "
    }
  }
}</script><link rel="stylesheet" href="/webant/jquery/css/jquery-ui-1.12.1.custom.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/pgbu/css/icons-unifier.css?18.8"
type="text/css" /><link rel="stylesheet" href="/gs/uni/nav/resources/css/menuIcon.css?18.8"
type="text/css" /><link rel="stylesheet" href="/webant/inc.css?18.8" type="text/css" /><script
type="text/javascript" src="/webant/js/i18n/UnifierMenu.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierMessage.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierString.js?18.8" ></script><script
type="text/javascript" src="/webant/js/i18n/UnifierTab.js?18.8" ></script>

<script type="text/javascript" src="/webant/js/menubar.js?18.8" ></script>
<script type="text/javascript" src="/webant/js/gen_validation.js?18.8" ></script>
<script type="text/javascript">
```

```

function sessionExpiredCallback() {
  if (topWin && !topWin.closed && topWin.login) {
    topWin.proxyMaster = '';
    topWin.login();
  }

  try {
    window.close();
  } catch(e) {
    if (typeof(topWin) !== 'undefined') {
      topWin.clickToLogout = true;
      topWin.close();
    }
    else if (self.parent) {
      self.parent.close();
    }
  }
}

window.onload = function(){
  if (window.name !== "aframe") {
    if (self.UAlreadySubmitted)
      self.UResetSubmit();
    else if (self.parent && self.parent.UAlreadySubmitted)
      self.parent.UResetSubmit();

    if (self.pointer_is_set_to_wait)
      self.ResetPointer();
    else if (self.parent && self.parent.pointer_is_set_to_wait)
      self.parent.ResetPointer();

    try {
      topWin = eval(LOCAL_TOP_PATH);
    } catch(e) {
      window.location.replace('/index.html');
      return;
    };
    U.AlertByKey("session_expired",sessionExpiredCallback)
  }
}
</script>
</head>
</html>

```

修订建议

高

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

TOC

该任务修复的问题类型

- 已解密的登录请求

常规

1. 确保所有登录请求都以加密方式发送到服务器。
2. 请确保敏感信息，例如：
 - 用户名
 - 密码
 - 社会保险号码
 - 信用卡号码
 - 驾照号码
 - 电子邮件地址
 - 电话号码
 - 邮政编码

一律以加密方式传给服务器。

中

向每个错误登录尝试发出相同的错误消息

TOC

该任务修复的问题类型

- 登录错误消息凭证枚举

常规

对每个错误的登录尝试发出相同的错误消息，不管是哪个字段发生错误，特别是用户名或密码字段错误。

该任务修复的问题类型

- 跨站点请求伪造

常规

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

例如，使用能防御 CSRF 的软件包，例如 OWASP CSRFGuard -

[http://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)

另一个示例为“ESAPI 会话管理”控件，其中包括针对 CSRF 的组件 -

<http://www.owasp.org/index.php/ESAPI>

[2] 确保应用程序中没有跨站点脚本编制问题 (CWE-79)，因为通过使用攻击者控制的脚本可绕过大部分 CSRF 防御。

[3] 为每个表单生成唯一的现时标志，将现时标志放到表单中，并在接收表单时验证现时标志。请确保现时标志是不可预测的 (CWE-330) -

<http://www.cgisecurity.com/articles/csrf-faq.shtml>

请注意，通过使用 XSS (CWE-79) 可绕过这一点。

[4] 识别特别危险的操作。在用户执行危险操作时，发送单独的确认请求以确保是用户自己希望执行该操作。请注意，通过使用 XSS (CWE-79) 可绕过这一点。

[5] 使用“两次提交的 cookie”方法，如 Felten 和 Zeller 所述：

在用户访问站点时，该站点应生成伪随机值，并将其设置为用户机器上的 cookie。站点应要求每次表单提交都包括该值作为表单和 cookie 值。向站点发送 POST 请求时，只有表单和 cookie 值相同时才应将该请求视为有效。

由于同源策略，攻击者无法读取或修改 cookie 中存储的值。要以用户的身份成功提交表单，攻击者必须正确猜出伪随机值。如果伪随机值的保密性很强，这将是极端困难的。此技巧需要 JavaScript，因此对于禁用了 JavaScript 的浏览器可能无效 -

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.1445>

请注意，使用 XSS (CWE-79) 有可能绕过这一点，或者在使用支持攻击者从 HTTP 请求中读取原始头的 Web 技术时也有可能绕过这一点。

[6] 请勿对触发状态更改的任何请求使用 GET 方法。

[7] 检查 HTTP Referer 头以查看请求是否源自预期的页面。这可能会破坏合法功能，因为用户或代理可能已出于隐私原因而禁止发送 Referer。请注意，通过使用 XSS (CWE-79) 可绕过这一点。

攻击者可能使用 XSS 来生成欺骗性的 Referer，或从允许使用其 Referer 的页面生成恶意请求。

该任务修复的问题类型

- 检测到应用程序测试脚本

常规

不可将测试/暂时脚本遗留在服务器上，未来要避免出现这个情况。
确保服务器上没有非正常操作所必备的其他脚本。

低

对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

TOC

该任务修复的问题类型

- 检测到隐藏目录

常规

如果不需要禁止的资源，请将其从站点中除去。
可能的话，请发出改用“404 — 找不到”响应状态代码，而不是“403 — 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

低

关闭跟踪，限制对日志文件的访问，或者将其除去

TOC

该任务修复的问题类型

- Oracle 日志文件信息泄露

常规

关闭跟踪，限制日志和跟踪文件的访问权，或除去它们。

低

将服务器配置为使用安全策略的“Content-Security-Policy”头

TOC

该任务修复的问题类型

- “Content-Security-Policy”头缺失或不安全

常规

将服务器配置为发送“Content-Security-Policy”头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

关于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

关于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx_http_headers_module.html

低

将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

TOC

该任务修复的问题类型

- “X-XSS-Protection”头缺失或不安全

常规

配置您的服务器，以确保在所有传出请求上发送值为“1”（即已启用）的“X-XSS-Protection”报头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

关于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

关于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx_http_headers_module.html

低

将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

TOC

该任务修复的问题类型

- “X-Content-Type-Options”头缺失或不安全

常规

将服务器配置为针对所有外发请求发送具有值“nosniff”的“X-Content-Type-Options”头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

关于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

关于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_http_headers_module.html

低

请勿接受在查询字符串中发送的主体参数

TOC

该任务修复的问题类型

- 查询中接受的主体参数

常规

重新对应用程序编程以禁用对查询中列出的 POST 参数的处理

低

为 Web 服务器或 Web 应用程序下载相关的安全补丁

TOC

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

常规

咨询

已解密的登录请求

TOC

测试类型:

应用程序级别测试

威胁分类:

传输层保护不足

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

安全性风险:

可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

受影响产品:

CWE:

523

X-Force:

52471

引用:

金融隐私权: 格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 SB1386

技术描述:

在应用程序测试过程中, 检测到将未加密的登录请求发送到服务器。由于登录过程中所使用的部分输入字段 (例如: 用户名、密码、电子邮件地址、社会安全号等) 是个人敏感信息, 因此建议通过加密连接 (例如 **SSL**) 将其发送到服务器。

任何以明文传给服务器的信息都可能被窃, 稍后可用来电子欺骗身份或伪装用户。

此外, 若干隐私权法规指出, 用户凭证之类的敏感信息一律以加密方式传给 **Web** 站点。

登录错误消息凭证枚举

TOC

测试类型:

应用程序级别测试

威胁分类:

蛮力

原因:

已向用户显示可能包含敏感调试信息的异常和错误消息

安全性风险:

可能会升级用户特权并通过 **Web** 应用程序获取管理许可权

受影响产品:

CWE:

204

X-Force:

52666

引用:

“Blocking Brute-Force Attacks”作者: Mark Burnett

技术描述:

当试图利用不正确的凭证来登录时，当用户输入无效的用户名和无效的密码时，应用程序会分别生成不同的错误消息。通过利用该行为，攻击者可以通过反复试验（蛮力攻击技术）来发现应用程序的有效用户名，再继续尝试发现相关联的密码。

这样会得到有效用户名和密码的枚举，攻击者可以用来访问帐户。利用的样本如下：

如果下列请求收到不同的错误消息，就有可能对站点发出蛮力攻击并枚举用户名和密码：

```
[1] GET /login.asp?username=BAD_USERNAME&password=correct_password
```

```
[2] GET /login.asp?username=correct_username&password=BAD_PASSWORD
```

跨站点请求伪造

TOC

测试类型:

应用程序级别测试

威胁分类:

跨站点请求伪造

原因:

应用程序使用的认证方法不充分

安全性风险:

可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

受影响产品:

CWE:

352

X-Force:

6784

引用:

跨站点伪造请求 [Wiki](#) 页面

“JavaScript 劫持”，作者: [Fortify](#)

跨站点请求伪造培训模块

技术描述:

即使是格式正确、有效且一致的请求也可能已在用户不知情的情况下发送。因此，**Web** 应用程序应检查所有请求以发现其不合法的迹象。此测试的结果指示所扫描的应用程序没有执行此操作。此脆弱性的严重性取决于受影响应用程序的功能。例如，对搜索页面的 **CSRF** 攻击的严重性低于对转账或概要文件更新页面的 **CSRF** 攻击。如果某个 **Web** 服务器设计为接收客户机的请求时无任何机制来验证该请求是否确实是客户机发送的，那么攻击者就有可能诱导客户机向该 **Web** 服务器误发请求，而该请求将视为真实请求。这可通过 **URL**、图像装入、**XMLHttpRequest** 等来完成，并可导致数据暴露或意外的代码执行。如果用户当前已登录到受害者站点，请求将自动使用用户的凭证（包括会话 **cookie**、**IP** 地址和其他浏览器认证方法）。通过使用此方法，攻击者可伪造受害者的身份，并以其身份提交操作。

“Content-Security-Policy”头缺失或不安全

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品:

CWE:

200

引用:

有用 HTTP 头列表
内容安全策略简介

技术描述:

“Content-Security-Policy”头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本编制。请务必正确设置该头值，使其不会阻止网站的正确操作。例如，如果该头设置为阻止执行内联 JavaScript，则网站不得在其页面内使用内联 JavaScript。

为了防止跨站点脚本编制，请务必为‘default-src’策略或‘script-src’和‘object-src’设置正确值。应避免不安全值，如‘*’、‘data:’、‘unsafe-inline’或‘unsafe-eval’。

此外，为了防止跨框架脚本编制或点击劫持，请务必为‘frame-ancestors’策略设置正确值。应避免不安全值，如‘*’或‘data:’。

“X-Content-Type-Options”头缺失或不安全

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品:

CWE:

200

引用:

有用 [HTTP 头列表](#)
减少 [MIME 类型安全风险](#)

技术描述:

“X-Content-Type-Options”头（具有“nosniff”值）防止 **IE** 和 **Chrome** 忽略响应的内容类型。
此操作可能防止不可信内容（例如，用户上传内容）在用户浏览器上执行（例如，在恶意命名之后）。

“X-XSS-Protection”报头缺失或不安全

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 **Web** 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品:

CWE:

200

引用:

有用 [HTTP 头列表](#)
[IE XSS 过滤器](#)

技术描述:

值为‘1’的“X-XSS-Protection”报头强制跨站点脚本编制过滤器进入启用模式，即使用户已禁用。
此过滤器内置于最新版本的 **Web** 浏览器（**IE 8 +**、**Chrome 4+**）中，在缺省情况下通常为已启用状态。虽然此过滤器不是第一个也不是唯一一个针对跨站点脚本编制的防御程序，但它可以作为额外保护层。

Oracle 日志文件信息泄露

TOC

测试类型:

基础结构测试

威胁分类:

信息泄露

原因:

Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险:

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品:

CWE:

200

X-Force:

52270

引用:

FrontPage 服务器扩展：安全考虑

技术描述:

Oracle 有一个称为“sqlnet.log”的日志文件，以及一个称为“sqlnet.trc”的跟踪文件。这些文件包含跟踪输出和错误消息，可能会显现敏感性信息。

攻击者可以利用这个问题来获取关于服务器机器的敏感信息，从而进一步攻击站点。利用的样本如下：

http://[SERVER]/sqlnet.log

http://[SERVER]/sqlnet.trc

查询中接受的主体参数

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

超文本传输协议 (HTTP/1.1) 语义和内容:

GET
POST

技术描述:

GET 请求设计的目的在于查询服务器，而 POST 请求用于提交数据。但是，除了技术目的之外，攻击查询参数比攻击主体参数更容易，因为向原始站点发送链接或在博客或注释中发布链接更容易，而且得到的结果比另一种方法更好，为了攻击带有主体参数的请求，攻击者需要创建其中包含表单的页面，当受害者访问表单时就会提交表单。说服受害者访问他不了解的页面比让受害者访问原始站点要难很多。因此，不建议支持可到达查询字符串的主体参数。

检测到隐藏目录

TOC

测试类型:

基础结构测试

威胁分类:

信息泄露

原因:

Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险:

可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点

受影响产品:

CWE:

200

X-Force:

52599

技术描述:

Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。

内容的敏感度越高，此问题也可能越严重。

发现可能的服务器路径泄露模式

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

未安装第三方产品的最新补丁或最新修补程序

安全性风险:

可能会检索 **Web** 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 **Web** 应用程序文件系统结构的信息

受影响产品:

CWE:

200

X-Force:

52839

技术描述:

AppScan 检测到包含文件绝对路径的响应（例如，**Windows** 中的 `c:\dir\file`，或 **Unix** 中的 `/dir/file`）。攻击者可能能够利用这一信息访问服务器机器目录结构上的敏感信息，进而对站点发起进一步攻击。

检测到应用程序测试脚本

TOC

测试类型:

应用程序级别测试

威胁分类:

可预测资源位置

原因:

在生产环境中留下临时文件

安全性风险:

可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

CWE:

531

X-Force:

52497

技术描述:

公共用户可以通过简单的冲浪（即按照 **Web** 链接）来访问站点上的特定页面。不过，也有页面和脚本可能无法通过简单的冲浪来访问（即未链接的页面和脚本）。

攻击者也许能够通过猜测名称（例如 **test.php**、**test.asp**、**test.cgi**、**test.html** 等）来访问这些页面。

名为“**test.php**”的脚本的请求示例

http://[SERVER]/test.php

有时开发者会忘记从生产环境中除去某些调试或测试页面。这些页面有可能包括 **Web** 用户所不应访问的敏感信息。它们也可能易受到攻击，且/或有助于攻击者获取服务器的相关信息，以帮助进行攻击。利用的样本如下：

http://[SERVER]/test.php

http://[SERVER]/test.asp

http://[SERVER]/test.aspx

http://[SERVER]/test.html

http://[SERVER]/test.cfm

http://[SERVER]/test.cgi