

# Report

## Summaries

### Alert counts by risk and confidence

---

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence					
		User	Confirmed	High	Medium	Low	Total
Risk		High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Medium		0 (0.0%)	0 (0.0%)	3 (50.0%)	0 (0.0%)	0 (0.0%)	3 (50.0%)
Low		0 (0.0%)	0 (0.0%)	2 (33.3%)	0 (0.0%)	0 (0.0%)	2 (33.3%)
Informational		0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (16.7%)	1 (16.7%)
Total		0 (0.0%)	0 (0.0%)	5 (83.3%)	1 (16.7%)	1 (100%)	6

### Alert counts by site and risk

---

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

---

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Site		Risk				Informational Risk
		High	Medium	Low (>= Informational) (>= Medium) (>= Low)	Informational	
		= High	= Medium	>= Low	>= Informational	
<a href="http://zero.webappssecurity.com">http://zero.webappssecurity.com</a>		0 (0)	3 (3)	2 (5)	1 (6)	

### Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
<a href="#">Cross-Domain Misconfiguration</a>	Medium	15 (250.0%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	4 (66.7%)
<a href="#">Vulnerable JS Library</a>	Medium	1 (16.7%)
<a href="#">Absence of Anti-CSRF Tokens</a>	Low	4 (66.7%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	13 (216.7%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	3 (50.0%)
Total		6

# Alerts

Risk=Medium, Confidence=Medium (3)

<http://zero.webappsecurity.com> (3)

## Cross-Domain Misconfiguration (1)

- ▶ GET <http://zero.webappsecurity.com/>

## Missing Anti-clickjacking Header (1)

- ▶ GET <http://zero.webappsecurity.com/>

## Vulnerable JS Library (1)

- ▶ GET <http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js>

Risk=Low, Confidence=Medium (2)

<http://zero.webappsecurity.com> (2)

## Absence of Anti-CSRF Tokens (1)

- ▶ GET <http://zero.webappsecurity.com/>

## X-Content-Type-Options Header Missing (1)

- ▶ GET <http://zero.webappsecurity.com/>

Risk=Informational, Confidence=Low (1)

<http://zero.webappsecurity.com> (1)

## Information Disclosure - Suspicious Comments(1)

- GET `http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js`

# Appendix

## Alert types

---

This section contains additional information on the types of alerts in the report. **Cross-Domain Misconfiguration**

<b>Source</b>	raised by a passive scanner ( <a href="#">Cross-Domain Misconfiguration</a> )
<b>CWE ID</b>	<a href="#">264</a>
<b>WASC ID</b>	14
<b>Reference</b>	<ul style="list-style-type: none"><li>■ <a href="https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy">https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy</a></li></ul>

## Missing Anti-clickjacking Header

<b>Source</b>	raised by a passive scanner ( <a href="#">Anti-clickjacking Header</a> )
<b>CWE ID</b>	<a href="#">1021</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>■ <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a></li></ul>

## Vulnerable JS Library

<b>Source</b>	raised by a passive scanner ( <a href="#">Vulnerable JS Library</a> )
<b>CWE ID</b>	<a href="#">829</a>

## Reference

- <https://nvd.nist.gov/vuln/detail/CVE-2012-6708>
- <https://github.com/jquery/jquery/issues/2432>
- <http://research.insecurelabs.org/jquery/test/>
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
- <http://bugs.jquery.com/ticket/11290>
- <https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
- <https://nvd.nist.gov/vuln/detail/CVE-2015-9251>
- <https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b>
- <https://bugs.jquery.com/ticket/11974>
- <https://blog.jquery.com/2020/04/10/jquery-3-5-0released/>

## Absence of Anti-CSRF Tokens

### Source

raised by a passive scanner ([Absence of Anti-CSRF Tokens](#))

### CWE ID

[352](#)

### WASC ID

9

### Reference

- <http://projects.webappsec.org/Cross-Site-Request-Forgery>
- <http://cwe.mitre.org/data/definitions/352.html>

## X-Content-Type-Options Header Missing

**Source** raised by a passive scanner ([X-Content-Type-Options Header Missing](#))

**CWE ID** [693](#)

**WASC ID** 15

**Reference** ■ <http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>

■ [https://owasp.org/www-community/Security\\_Headers](https://owasp.org/www-community/Security_Headers)

## Information Disclosure - Suspicious Comments

**Source** raised by a passive scanner ([Information Disclosure - Suspicious Comments](#))

**CWE ID** [200](#)

**WASC ID** 13

The screenshot shows the OWASP ZAP interface in Standard Mode. The top navigation bar includes File, Edit, View, Analyse, Report, Tools, Import, Online, Help, and a menu for Standard Mode. The main window has tabs for Quick Start, Request, and Response. The Response tab is active, displaying the following details:

Header Text - Body Text -

HTTP/1.1 200 OK  
Date: Thu, 03 Mar 2022 15:23:48 GMT  
Server: Apache-Coyote/1.1  
Access-Control-Allow-Origin: \*

Cache-Control: no-cache, max-age=0, must-revalidate, no-store  
Content-Type: text/html; charset=UTF-8  
Content-Language: en-US

The Response body contains the following HTML code:

```
<!DOCTYPE html>
<html lang="en">
<head>
    meta charset="UTF-8"
    title="Personal Banking - Home - Credit Cards">
    meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
    meta http-equiv="X-UA-Compatible" content="IE=edge">
    <link rel="stylesheet" href="https://resources.rbsa-banking.com/css/bootstrap.css"/>
    <link rel="stylesheet" href="https://resources.rbsa-banking.com/css/app.css"/>
```

The bottom pane displays a list of alerts under the 'Alerts' tab:

- 0 Cross-Domain Misconfiguration (1)
- 1 Missing Anti-chrophising Header (4)
- 1 Vulnerable JS Library (2)
- 1 Absence of Anti-CSRF Tokens (4)
- 1 X-Content-Type-Options Header Missing (1)
- 1 Information Disclosure - Suspicious Comments (1)

Details for the first alert, 'Cross-Domain Misconfiguration', are shown:

**Cross-Domain Misconfiguration**  
URL: http://www.webscantestify.com/  
Risk: Low/Medium  
Confidence: Medium  
Parameter:  
Attack:  
Evidence: Access-Control-Allow-Origin: \*  
CWE ID: 264  
WASC ID: 14  
Source: Passive (10008 - Cross-Domain Misconfiguration)  
Description:  
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Other Info:  
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third-party domains, using unauthenticated APIs on this domain. Web browser implementations do...

At the bottom, there are 'Alerts' and 'Current Scan' status indicators.

```
<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Zero - Personal Banking - Loans - Credit Cards</title>

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<meta http-equiv="X-UA-Compatible" content="IE=Edge">

<link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>

<link type="text/css" rel="stylesheet" href="/resources/css/fontawesome.css"/>

<link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>

<script src="/resources/js/jquery-1.8.2.min.js"></script>

<script src="/resources/js/bootstrap.min.js"></script>

<script src="/resources/js/placeholders.min.js"></script>

<script type="text/javascript">

Placeholders.init({ 

  live: true, // Apply to future and modified elements too

  hideOnFocus: true // Hide the placeholder when the element receives focus

});
```

```
</script>

<script type="text/javascript">

$(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {

    if (xhr.status == 403) {

        window.location.reload();

    }

});;

</script>

</head>

<body>

<div class="wrapper">

<div class="navbar navbar-fixed-top">

<div class="navbar-inner">

<div class="container">

<a href="/index.html" class="brand">Zero Bank</a>

<div>

<ul class="nav float-right">

<li> <form action="/search.html"

class="navbar-search pull-right" style="padding-right: 20px">

<input type="text" id="searchTerm" name="searchTerm" class="searchquery" placeholder="Search"/>
```

```
</form>

</li>

<li>

    <button id="signin_button" type="button" class="signin btn btn-info">

        <i class="icon-signin"></i>Signin

    </button>

</li>

</ul>

</div>

</div>

</div>

<script type="text/javascript">

$(function() {

    var path = "/";

    $("#signin_button").click(function(event) {

        event.preventDefault();

        window.location.href = path + "login" + ".html";

    });

})
```

```
});

</script>

<div class="container">

    <div class="top_offset">

        <div class="row">

            <div class="span12">

                <div id="nav" class="clearfix">

                    <ul id="pages-nav">

                        <li id="homeMenu"><div><strong>Home</strong></div></li>

                        <li id="onlineBankingMenu"><div><strong>Online
Banking</strong></div></li>

                        <li id="feedback"><div><strong>Feedback</strong></div></li>

                    </ul>

                </div>

            </div>

        </div>

<script type="text/javascript">

$(function () {

    var path = "/";

    var featureIdToName = {
```

```
"index": "homeMenu",

"online-banking": "onlineBankingMenu",

"feedback": "feedback"

};

if (document.location.href.match("." + path + "$") != null) {

    $("#homeMenu").addClass("active");

} else {

    $.each(featureIdToName, function(featureId, featureName) {

        if (document.location.href.indexOf(featureId + ".html") >= 0) {

            $("#" + featureName).addClass("active");

        }

    });

}

$.each(featureIdToName, function(featureId, featureName) {

    $("#nav").on("click", "li[id='" + featureName + "']", function(event) {

        event.preventDefault();

        window.location.href = path + featureId + ".html";

    });

});
```

```
});

</script>

</div>

<div class="row">

<div class="span12">

<div id="carousel" class="carousel slide">

<div class="carousel-inner">

<div class="active item">



<div class="custom carousel-caption">

<h4>Online Banking</h4>

<p>Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.</p>

</div>

</div>

<div class="item">



<div class="custom carousel-caption">

<h4>Online Banking</h4>

<p>Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.</p>
```

```
</div>

</div>

<div class="item">



<div class="custom carousel-caption">

<h4>Online Banking</h4>

<p>Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.</p>
```

```
</div>

</div>

</div>

<a class="carousel-control custom left" href="#carousel" dataslide="prev">&lsaquo;</a>

<a class="carousel-control custom right" href="#carousel" dataslide="next">&rsaquo;</a>

</div>

</div>
```

```
<hr class="row-divider"/>

<div id="online_banking_features" class="row divider">

<div class="span3">
```

```
<h4><i class="icon icon-bookmark"></i> Online Banking</h4>

<p>Click the button below to view online banking features.</p>

<a id="online-banking" class="btn btn-small btn-info">More Services</a>

</div>

<div class="span3">

<div>

<h4><span class="headers" id="account_activity_link"><i class="icon icon-user"></i>Checking Account Activity</span></h4>

<p>Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other useful transactions.

</p>

</div>

</div>

<div class="span3">

<div>

<h4><span class="headers" id="transfer_funds_link"><i class="icon icon-random"></i>Transfer Funds</span></h4>

<p>Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your funds are available when you need them.

</p>

</div>

</div>

<div class="span3">
```

```
<div>

    <h4><span class="headers" id="money_map_link"><i class="icon iconlist-alt"></i>My Money Map</span></h4>

    <p>Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you manage your finances efficiently. With Money Map, you can create a budget, sort your finances into spending and savings categories, check the interest your accounts are earning, and gain new understanding of your patterns with the help of Zero's clear charts and graphs.

    </p>

</div>

</div>

</div>

<script type="text/javascript">

$(function() {

    $("#carousel").carousel({ interval: false });

    $("div").on("click", "a[id='online-banking']", function(event){

        event.preventDefault();

        window.location.href = "/" + "online-banking" + ".html";

    });

    var path = "/bank/";

    var featureIdToName = {

        "account_activity_link": "account-activity",
```

```
"transfer_funds_link": "transfer-funds",
"money_map_link": "money-map"
}

$.each(featureIdToName, function(featureId, featureName) {
    $("#" + online_banking_features).on("click", "span[id=" + featureId + "]", function(event) {
        event.preventDefault();
        window.location.href = path + featureName + ".html";
    });
});

});

</script>

</div>

</div>

<div class="clearfix push"></div>

</div>

<div class="extra">
    <div class="extra-inner">
        <div class="container">
            <div class="row">
```

```
<div class="span4">  
  
    <ul>  
  
        <li><span id="download_webinspect_link">Download  
WebInspect</span></li>
```

```
    </ul>  
  
</div>
```

```
<div class="span4">  
  
    <ul>  
  
        <li><span id="terms_of_use_link">Terms of Use</span></li>  
  
    </ul>  
  
</div>
```

```
<div class="span4">  
  
    <ul>  
  
        <li><span id="contact_hp_link">Contact Micro Focus</span></li>  
  
        <li><span id="privacy_statement_link">Privacy  
Statement</span></li>
```

```
    </ul>  
  
</div>  
  
</div>
```

```
<div class="row">
```

```
<div class="disclaimer span12">
```

The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating

the functionality and effectiveness of Micro Focus Fortify's WebInspect products in detecting and reporting

Web application vulnerabilities. This site is not a real banking site and any similarities to third party products

and/or Web sites are purely coincidental. This site is provided "as is" without warranty of any kind,

either express or implied. Micro Focus Fortify does not assume any risk in relation to your use of this Web site.

Use of this Web site indicates that you have read and agree to Micro Focus Fortify's Terms of Use found at

<https://www.microfocus.com/about/legal/#privacy>

and Micro Focus Fortify's Online Privacy Statement found at

<https://www.microfocus.com/about/legal/#privacy>.

<br/><br/>

Copyright © 2012-2018, Micro Focus Development Company. All rights reserved.

```
</div>
```

```
</div>
```

```
</div>
```

```
</div>

</div>

<script type="text/javascript">

$(function () {

    var path = "/";

    var attachClickHandler = function(selector, handler) {

        $(".extra").on('click', selector, handler);
    }

    var footerLinks = {

        "download_webinspect_link": { absolute: true, page:

"https://software.microfocus.com/en-us/products/webinspect-dynamicanalysis-dast/overview" },

        "contact_hp_link" : { absolute: true, page: "https://support.fortify.com"

},


        "privacy_statement_link": { absolute: true, page:

"https://www.microfocus.com/about/legal/#privacy" },


        "terms_of_use_link": { absolute: true, page:

"https://www.microfocus.com/about/legal/" }

    };

    $.each(footerLinks, function(linkId, link) {

        attachClickHandler('span[id="' + linkId + '"]', function(event) {
```

```
event.preventDefault();

if (link.absolute) {

    window.location.href = link.page;

} else {

    window.location.href = path + link.page + ".html";

}

});

});

});

</script>

</body>

</html>
```