VantagePoint

Upland Software – RO Innovation Application Penetration Test

August 2, 2021

Contents

1. Executive Summary

Founded in 2010 and headquartered in Austin, TX, Upland Software, Inc. provides cloud-based enterprise work management software in the United States, Canada, and internationally. Upland Software contracted with VantagePoint to perform a web application-oriented penetration test against a defined environment to assist in discovering flaws and weaknesses. Testing was performed per industry best practices and focused upon the Open Web Application Security Project's (OWASP) top vulnerabilities which represent industry consensus on the most critical security risks to web applications along with general security best practices testing. The test against the client provided environment occurred between July 16th, 2021 and August 2nd, 2021.

The purpose of this test was to perform an application level, authenticated assessment of an environment emulating the internet-facing equivalent hosts provided as part of the scope of this engagement, with the goal to evaluate existing security controls and measures, and to provide recommendations for improvement. Based on this objective, VantagePoint has concluded that significant gaps in security coverage exist, and the RO Innovation application received an overall grade of **D**. This rating was most heavily influenced by a Broken Access Controls vulnerability which allows an API user to access all data stored within the application. Areas of improvement have been identified, and Upland Software should formulate a remediation plan to mitigate findings uncovered during the assessment.

Company Background

VantagePoint Consulting provides the experts you need to enhance your security posture, reduce your risk, and facilitate compliance efforts. Our team of consultants are seasoned, highly certified security and compliance veterans that are committed to customer success and ensuring that our customers' security and compliance goals are met or exceeded. Our services span the spectrum of Information Security and Compliance from security strategy and governance, to technical testing, and compliance readiness. Our many years of experience and sole focus on customer success make us a valuable partner for any company.

Assumptions and Constraints

The project scope, as defined in the Statement of Work, outlines the depth of these evaluation activities. The security assessment was conducted in a manner designed to be as thorough as possible. All scans were performed with "safe checks enabled". Potentially destructive tests, such as Denial of Service (DoS) attacks, were not performed. However, given the nature of the security tests, system availability can be, and sometimes is, affected.

Manual testing was performed to provide a deep-dive analysis and validate automated scan results. Nevertheless, some documented vulnerabilities may be false positives. Likewise, existing vulnerabilities may not have been reported due to limitations in testing tools, time boundaries, deltas between the tested systems and the production environment, and/or limitation in scope.

File uploads were not allowed and therefore not tested. Limited API testing was performed, but not to the full extent of an API test.

VantagePoint believes the statements made in this document provide an accurate assessment of Upland Software's current security as it relates to the scope of the assessment. As environments change, and new vulnerabilities are made public, an organization's overall security posture will change. Such changes may affect the validity of this assessment. Therefore, the findings described in this report describe a "snapshot" in time.

Objectives and Scope

Prior to testing, Upland Software provided VantagePoint with an application URL and corresponding user credentials. The scope of the penetration test was limited to this URL, and other services running on this host. The penetration test was conducted from two views. First, as an unauthenticated attacker and second, as an authenticated user. The URL is listed below:

- https://www.shimbonda.com/RVPen/
- https://www.shimbonda.com/API/swagger/ui/index.html

Account	Permissions
Sssp1portal	SSSP1 Portal
Sssp1refmgr	SSP1 RefMgr
Sssp2portal	SSP2 Portal
Sssp2refmgr	SSSP2 RefMgr

Using a mixture of techniques and scanning tools, these URLs were assessed for occurrences of published top vulnerabilities:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross Site Scripting (XSS)
8. Missing Function Level Access Control
9. Insecure Deserialization
10. Insufficient Logging and Monitoring
11. Insecure Direct Object References
12. Cross-Site Request Forgery (CSRF)
13. Unvalidated Redirects and Forwards
14. Components with Known Vulnerabilities

Findings Rating Methodology

VantagePoint determines the risk posed by vulnerabilities based on three main criteria: risk to users, risk to infrastructure, and attack complexity.

Risk to users is how a vulnerability may impact users of the application and their data. Low risk issues may only affect single users or non-critical data, while high risk vulnerabilities may be able to easily compromise data on large numbers of users, or highly sensitive data such as payment card information.

Risk to infrastructure measures the impact of a vulnerability to the hardware and network the application runs on. Low risk findings could involve possible service impacts given a large-scale denial of service attack, which VantagePoint would not simulate. High risk vulnerabilities would include flaws that would allow an attacker to execute code on the server, or an easily triggered denial of service condition.

Attack Complexity gauges how difficult it would be for an attacker to execute an attack against users or infrastructure. Some attacks require specific conditions be met for a successful attack, such as a certain network posture such as the ability to man-in-the-middle a victim, or access to a prohibitively large amount of computing resources. A higher attack complexity will lower the risk of a finding.

The overall risk rating for the finding is a sum of the above criteria to give an overall risk posed by the vulnerability. This gives an at-a-glance indication of the risk posed to your organization to help easily understand the issue and prioritize remediation efforts.

Application Rating Methodology

Current Application Risk: D

Severity	Risk
D	The application contains security flaws that require immediate remediation and pose a severe risk to users or infrastructure. Vulnerabilities are easy to exploit over the network and lead to significant compromise of user data or the ability to gain access to underlying infrastructure, likely without any form of authentication. Multiple vulnerabilities in the same functionality of the application, or attacks that can be chained together may increase the overall risk posed by the application.
C	High risk applications contain security flaws which should receive priority attention. These flaws can be directly exploited to attack users or infrastructure; however, some constraints may impact the ease of attack. Authentication or a specific network posture may be necessary to exploit the vulnerabilities. Multiple vulnerabilities in the same functionality of the application, or attacks that can be chained together may increase the overall risk posed by the application.
B	Medium risk applications do not contain major security flaws but may contain issues which should be considered for remediation soon. Vulnerabilities may present limited vectors for attack or may pose significant difficulty for an attacker to successfully exploit. Multiple vulnerabilities in the same functionality of the application, or attacks that can be chained together may increase the overall risk posed by the application.
A	Low risk applications present a limited attack surface and contain no significantly exploitable flaws; however, some security best practices may not be followed.
A+	The application was found to contain no major security flaws and adheres strongly to industry best practices for security.

Findings Summary

Severity	Identified	Remediated	Remaining
Critical	1	0	1
High	1	0	1
Medium	1	0	1
Low	4	0	4
Informational	4	0	4
Totals	**11**	**0**	**11**

Conclusion

VantagePoint has successfully completed the application assessment of the URL defined in the scope. Overall, VantagePoint has found the security controls in place within scope of the assessment to contain significant vulnerabilities which require immediate attention.

We recommend that the issues contained in this report be evaluated and a remediation plan formed. We would like to thank Upland Software for their assistance in making the assessment go smoothly and for the opportunity to help the organization assess and improve their security posture.

Project Team

The following team members were involved in this assessment:

Team Member	Role	Contact Information
Danny Tijerina	Project Manager	danny@vantagepoint.co
Colin Szost	Penetration Tester / Report Writer	cszost@vantagepoint.co

2. Detailed Analysis and Breakdown

Detailed Conclusion

VantagePoint has successfully completed the application assessment of the URL defined in the scope. Overall, VantagePoint has found the security controls in place within scope of the assessment to contain significant vulnerabilities which require immediate attention.

Most notably, the API lacks proper access controls. Any API user can access and alter any data stored within the application. This includes viewing requests and nominations belonging to other tenants, and changing the status or deleting this data. The use of sequential identifiers makes scraping the application trivial and one compromised account compromises the entire application.

Another significant vulnerability is the use of static login tokens. Logging into the application from a specific URL redirects the user to a URL containing a static token. This token allows anyone who visits the URL to login as that particular user, bypassing the need for a username and password. If this link were compromised, it would compromise the user’s account and any data they have access to.

In addition, VantagePoint also recommends several other changes to include additional layers of security such as tightening the CORS policy and updating outdated JavaScript resources.

We recommend that the issues contained in this report be evaluated and a remediation plan formed. We would like to thank Upland Software for their assistance in making the assessment go smoothly and for the opportunity to help the organization assess and improve their security posture.

Detailed Findings Table

Severity: CRITICAL

Issues ID#	Description
1.	Broken Access Controls

Severity: HIGH

Issues ID#	Description
2.	Static Login Token

Severity: MEDIUM

Issues ID#	Description
3.	Insecure CORS (Cross-Origin Resource Sharing) Policy

Severity: LOW

Issues ID#	Description
4.	Application Potentially Vulnerable to Clickjacking
5.	Password Field With Autocomplete Enabled
6.	Outdated JavaScript Resources
7.	Excessive Session Timeout

Severity: Informational

Issues ID#	Description
8.	Wildcard Certificate Exposes Potential Certificate Forgery
9.	Concurrent Logins Allowed
10.	Sequential Identifiers
11.	Insecure Content Security Policy

Reconnaissance

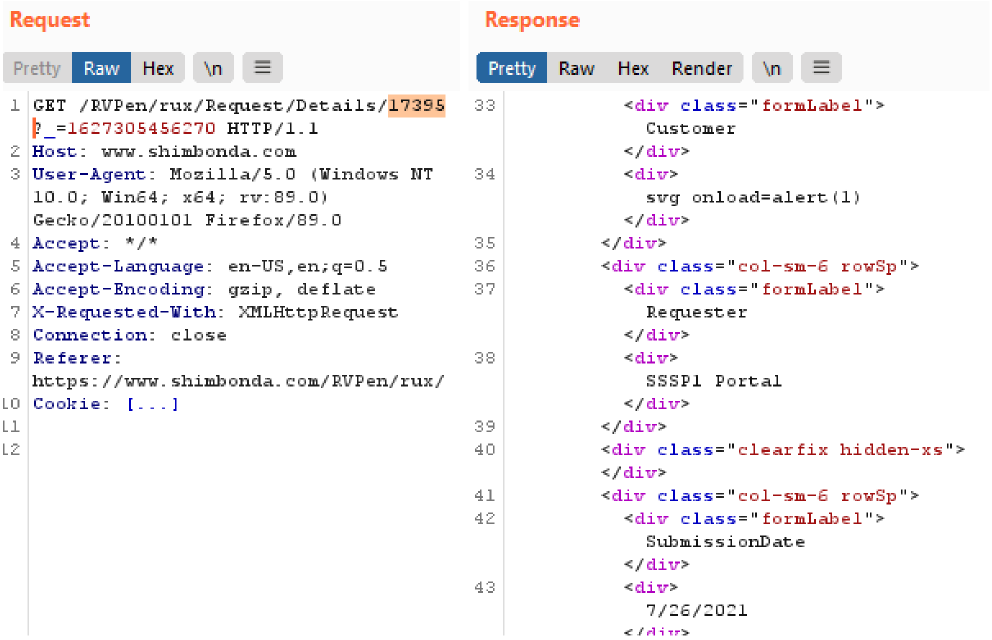
Host	IP Address	Ports	Server	Session Cookie
www.shimbonda.com	52.200.39.102	80/tcp, 443/tcp	Microsoft-IIS/10.0	.AspNet.ApplicationCookie

Finding Details

Critical Risk Findings

Issue ID #1	**Broken Access Controls**
Attributes	**Overall Risk: Critical** **User Risk:** Critical **Infrastructure Risk:** None **Attack Complexity:** Low
Description	The application API suffers a widespread lack of access controls. Any use with API access is able to view and alter data belonging to any user or tenant. A single compromised account or malicious user jeopardizes all users and data stored within the application. In addition, the application uses sequential numeric identifiers for data. Further details can be seen in the “Sequential Identifiers” finding below. Using sequential identifiers makes it easy for an attacker to quickly scrape the application for all data stored within. From the API, VantagePoint was able to view and delete nominations and requests, and change the status of requests. Assets were also accessible but both tenants appeared to have access to the same assets. In addition to the API, request details were also accessible through the web application. This was not an API focused test. VantagePoint had limited documentation and data to test with. However, it appears that this is a systemic issue, and not limited to the examples provided in this report. A thorough review of the API code should be performed, and an API specific pentest considered. All API endpoints should be considered vulnerable until confirmed otherwise. Due to the fact users can access and alter data of other tenants, this vulnerability has a much greater potential for damage resulting in a compromise, and the finding has been increased from High to Critical.
Affected Locations	Systemic https://www.shimbonda.com/API/, https://www.shimbonda.com/RVPen/rux/Request/Details/[Request_ID]

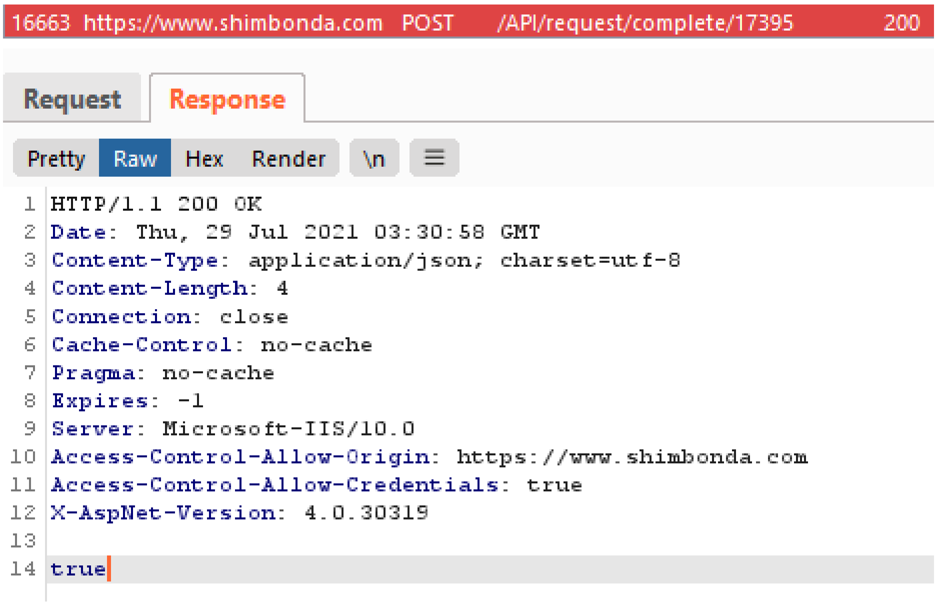
Evidence



```
GET /RVPen/rux/Request/Details/17395
?_=1627305456270 HTTP/1.1
Host: www.shimbonda.com
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:89.0)
Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer:
https://www.shimbonda.com/RVPen/rux/
Cookie: [...]
```

```
      <div class="formLabel">
        Customer
      </div>
      <div>
        svg onload=alert(1)
      </div>
    </div>
    <div class="col-sm-6 rowSp">
      <div class="formLabel">
        Requester
      </div>
      <div>
        SSSP1 Portal
      </div>
    </div>
    <div class="clearfix hidden-xs">
    </div>
    <div class="col-sm-6 rowSp">
      <div class="formLabel">
        SubmissionDate
      </div>
      <div>
        7/26/2021
      </div>
```

Figure 1 – Changing the Request ID grants access to any request details.

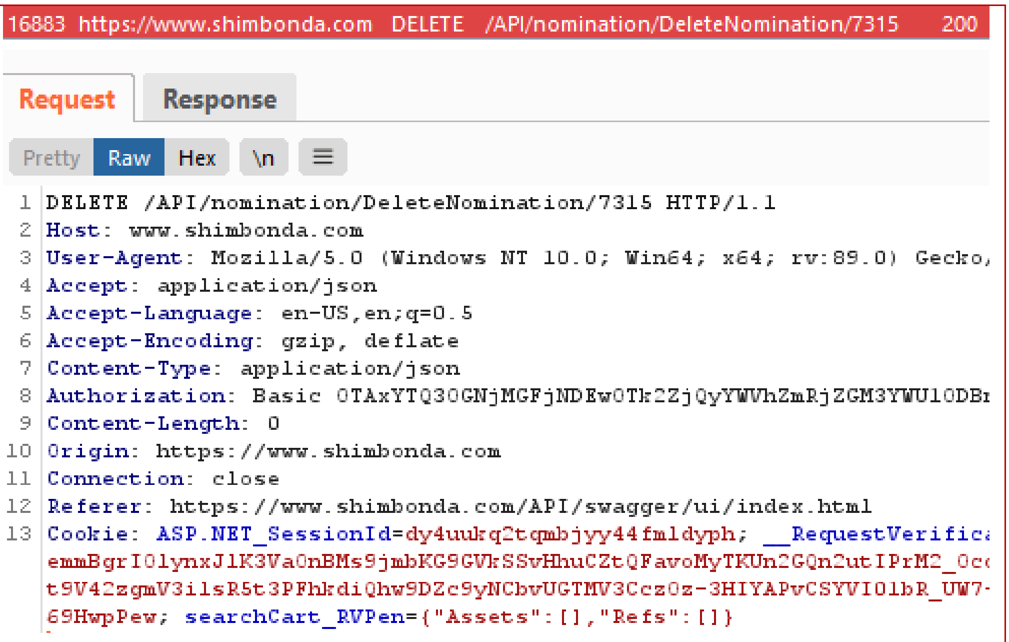


```
16663  https://www.shimbonda.com  POST  /API/request/complete/17395  200
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Jul 2021 03:30:58 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 4
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: https://www.shimbonda.com
Access-Control-Allow-Credentials: true
X-AspNet-Version: 4.0.30319

true
```

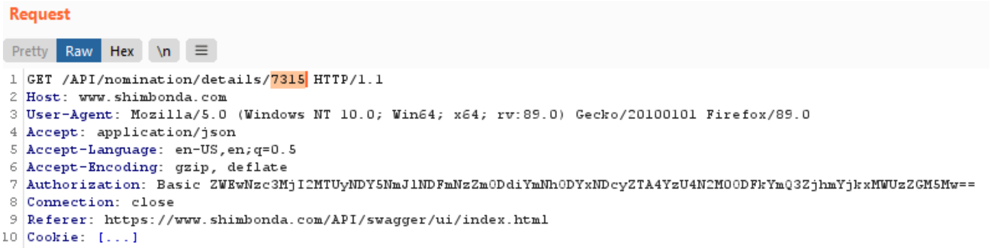
. Figure 2 – Users can complete requests for other tenants.



16883 https://www.shimbonda.com DELETE /API/nomination/DeleteNomination/7315 200
Request
Response
Pretty
Raw
Hex
\n
☰

```
DELETE /API/nomination/DeleteNomination/7315 HTTP/1.1
Host: www.shimbonda.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko,
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Basic OTAxYTQ3OGNjMGFjNDEwOTk2ZjQyYWVhZmRjZGM3YWU1ODB
Content-Length: 0
Origin: https://www.shimbonda.com
Connection: close
Referer: https://www.shimbonda.com/API/swagger/ui/index.html
Cookie: ASP.NET_SessionId=dy4uukq2tqmbjyy44fmldyph; __RequestVerific
emmBgrI0lynxJ1K3Va0nBMs9jmbKG9GVkSSvHhuCZtQFavoMyTKUn2GQn2utIPrM2_Oc
t9V42zgmV3ilsR5t3PFhkdiQhw9DZc9yNCbvUGTMV3Ccz0z-3HIYAPvCSYVI01bR_UW7-
69HwpPew; searchCart_RVPen={"Assets":[],"Refs":[]}
```

Figure 3 – Users can delete nominations of other tenants.



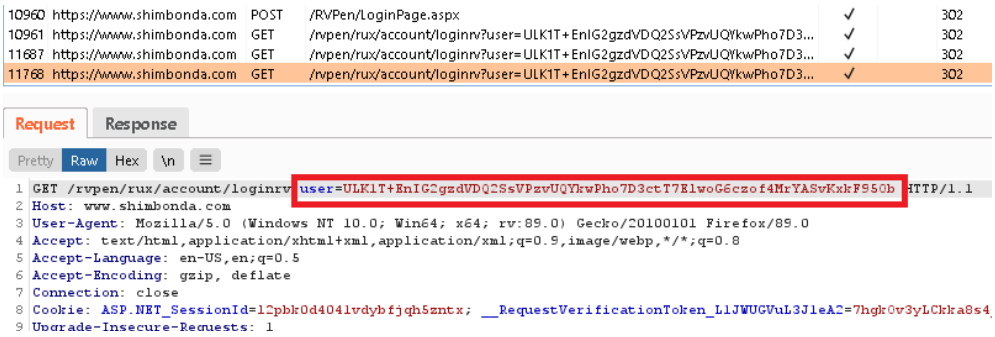
```
GET /API/nomination/details/7315 HTTP/1.1
Host: www.shimbonda.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic ZWEwNzc3MjI2MTUyNDY5NmJ1NDFmNzZm0DdiYmNh0DYxNDcyZTA4YzU4N2M0ODFkYmQ3ZjhmYjkxMWUzZGM5Mw==
Connection: close
Referer: https://www.shimbonda.com/API/swagger/ui/index.html
Cookie: [...]
```

Figure 4 – Users can iterate through nomination IDs.

Remediation	Ensure proper access controls are enforced by the application.
References	• https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A5-Broken_Access_Control • https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html • https://owasp-top-10-proactive-controls-2018.readthedocs.io/en/latest/c7-enforce-access-controls.html

High Risk Findings

Issue ID #2	**Static Login Token**
Attributes	**Overall Risk:** High **User Risk:** High **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	When a user logs in at https://www.shimbonda.com/RVPen/LoginPage.aspx, if the login is successful, they will be redirected to a link that will complete the login process. This redirect contains a link with a token as a GET parameter. This login token can then be used to bypass any need for a login for the account, and the token doesn't seem to expire. URLs are stored in a variety of locations such as the user's browser, access logs on the server, and by any proxies that may have handled the request. If an attacker compromises any of these sources, they will have full access to the account, and the victim will have no way to invalidate this token to secure their account. Depending on the compromised source, such as a proxy or server access logs, multiple users could be at risk.
Affected Location	https://www.shimbonda.com/rvpen/rux/account/loginrv?user=ULK1T+EnIG2gzdVDQ2SsVPzvUQYkwPho7D3ctT7ElwoG6czof4MrYASvKxkF95Ob

Evidence	
	10960 https://www.shimbonda.com POST /RVPen/LoginPage.aspx ✓ 302
	10961 https://www.shimbonda.com GET /rvpen/rux/account/loginrv?user=ULK1T+EnIG2gzdVDQ2SsVPzvUQYkwPho7D3... ✓ 302
	11687 https://www.shimbonda.com GET /rvpen/rux/account/loginrv?user=ULK1T+EnIG2gzdVDQ2SsVPzvUQYkwPho7D3... ✓ 302
	11768 https://www.shimbonda.com GET /rvpen/rux/account/loginrv?user=ULK1T+EnIG2gzdVDQ2SsVPzvUQYkwPho7D3... ✓ 302
	Request Response
	Pretty Raw Hex \n ≡
	`GET /rvpen/rux/account/loginrv user=ULK1T+EnIG2gzdVDQ2SsVPzvUQYkwPho7D3ctT7ElwoG6czof4MrYASvKxkF95Ob HTTP/1.1`
	`Host: www.shimbonda.com`
	`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0`
	`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8`
	`Accept-Language: en-US,en;q=0.5`
	`Accept-Encoding: gzip, deflate`
	`Connection: close`
	`Cookie: ASP.NET_SessionId=12pbk0d404lvdybfjqh5zntx; __RequestVerificationToken_L1JWUGVuL3JleA2=7hgk0v3yLCkka8s4`
	`Upgrade-Insecure-Requests: 1`
	
	Figure 5 – The authToken is sent in the URL as a GET parameter.

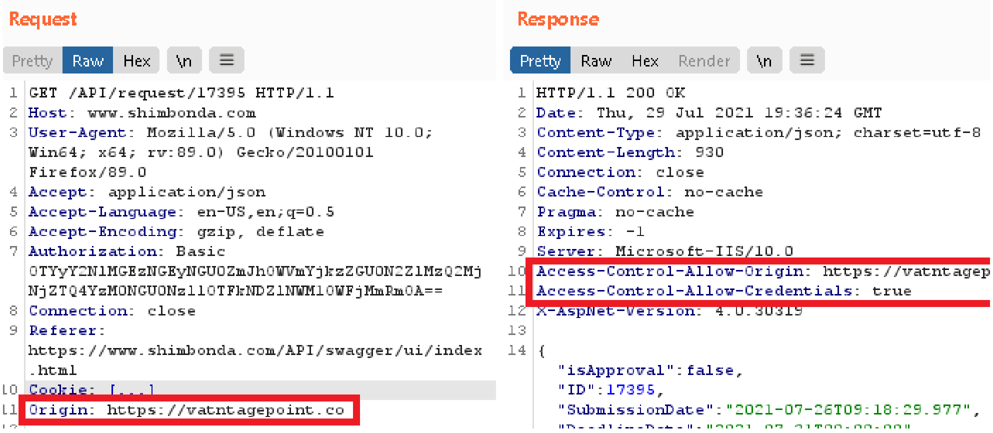
Remediation	Do not send sensitive information as a GET URL parameter. Sensitive data should be sent as a POST parameter to avoid getting cached or stored by browsers, proxies, or logs. Authentication information should be set as a cookie or HTTP header.

References	- https://owasp.org/www-community/vulnerabilities/Information_exposure_through_query_strings_in_url

Medium Risk Findings

Issue ID #3	**Insecure CORS (Cross-Origin Resource Sharing) Policy**
Attributes	**Overall Risk:** Medium **User Risk:** Medium **Infrastructure Risk:** None **Attack Complexity:** Low
Description	Part of the application defines an HTLM5 Cross-Origin Resource Sharing policy. This alters the browser's Same Origin Policy and allows scripts to read data from the application. If a user visits a malicious domain, this CORS policy could allow an attacker to access the application. Additionally, the "Vary: Origin" header was not present, which may allow proxies to cache sensitive information and enable cache poisoning attacks. While this would normally be rated a low risk, the server also issued an "Access-Control-Allow-Credentials" header set to true. This allows scripts to interact with authenticated sessions, exposing sensitive data and functionality. In light of this, the risk has been increased to Medium.
Affected Locations	https://www.shimbonda.com/API/

Evidence



```
GET /API/request/17395 HTTP/1.1
Host: www.shimbonda.com
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:89.0) Gecko/20100101
Firefox/89.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic
OTYyY2NlMGEzNGEyNGU0ZmJhOWVmYjkzZGU0N2Z1MzQ2Mj
NjZTQ4YzMONGU0Nz11OTFkNDZ1NWM1OWFjMmRmOA==
Connection: close
Referer:
https://www.shimbonda.com/API/swagger/ui/index
.html
Cookie: [...]
Origin: https://vatntagepoint.co
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Jul 2021 19:36:24 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 930
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: https://vatntagep
Access-Control-Allow-Credentials: true
X-AspNet-Version: 4.0.30319

{
  "isApproval":false,
  "ID":17395,
  "SubmissionDate":"2021-07-26T09:18:29.977",
```

Figure 6 – The server accepts the arbitrary origin and sets the "Access-Control-Allow-Credentials" header to "true".

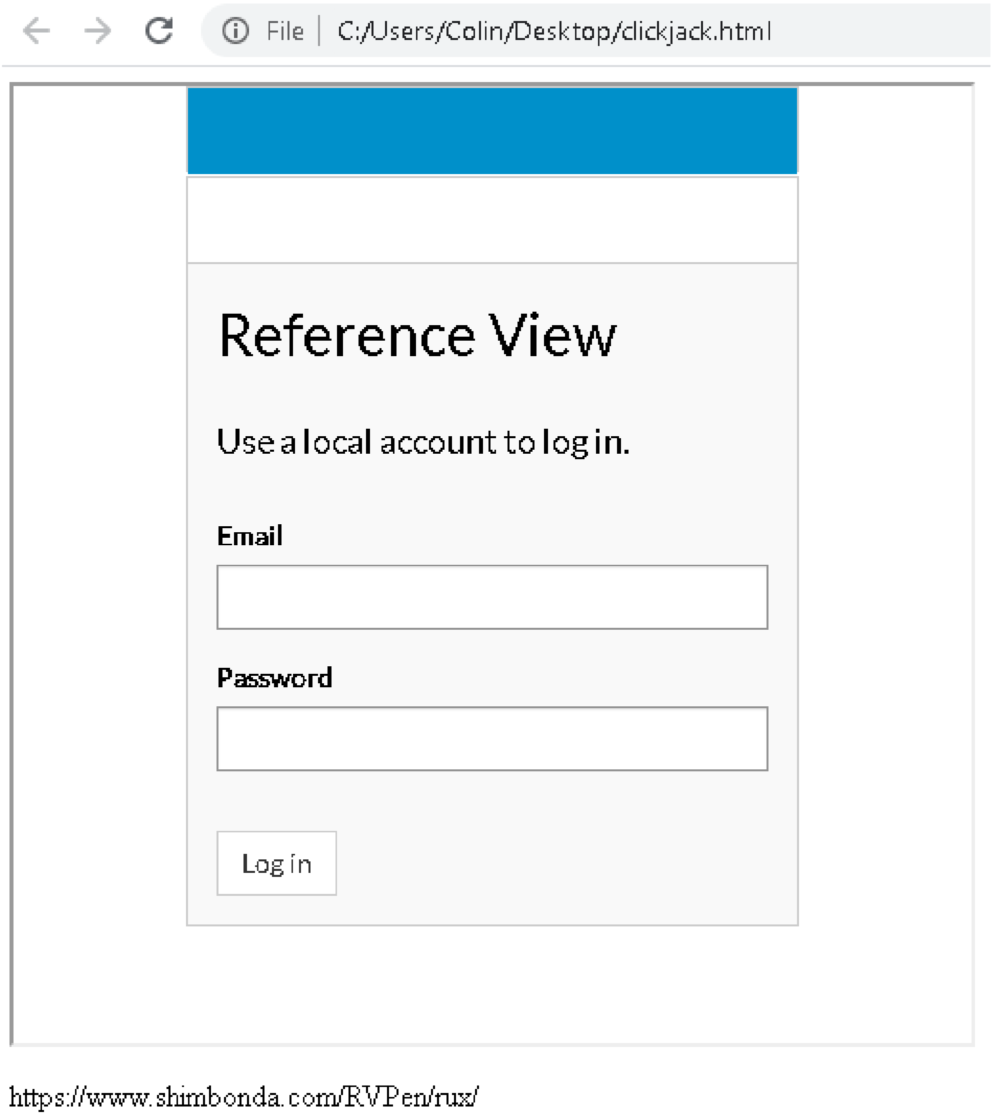
Remediation

The application should use a whitelist of trusted domains instead of accepting any origin.

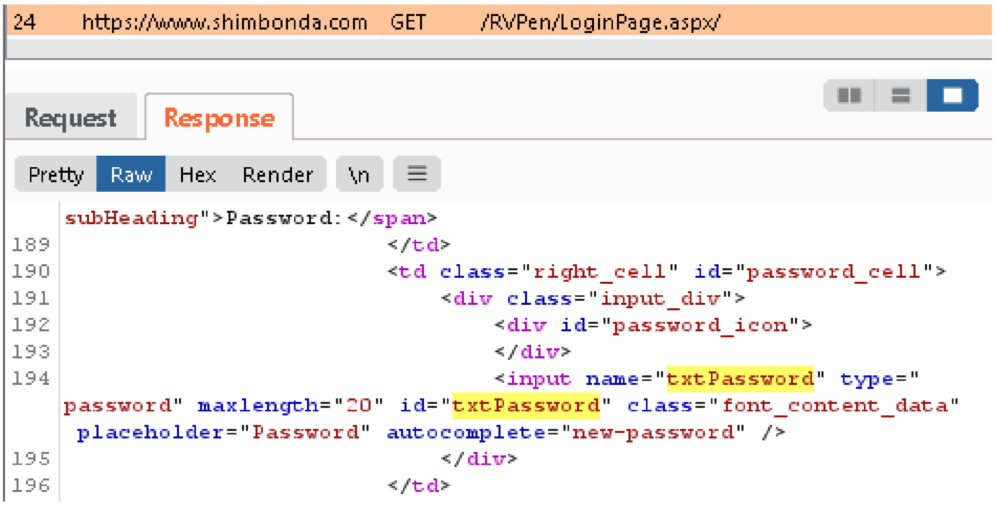
References	- https://www.owasp.org/index.php/CORS_OriginHeaderScrutiny - https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

Low Risk Findings

Issue ID #4	**Application Potentially Vulnerable to Clickjacking**
Attributes	**Overall Risk:** Low **User Risk:** Medium **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	VantagePoint identified multiple pages that are susceptible to frame-able responses. This means it is possible for a web page controlled by an attacker to load the content of these responses within an iframe on the attacker's page. 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 causes them to unwittingly carry out malicious actions or steal credentials.
Affected Locations	https://www.shimbonda.com/RVPen/rux/

Evidence	 File | C:/Users/Colin/Desktop/clickjack.html Reference View Use a local account to log in. Email Password Log in https://www.shimbonda.com/RVPen/rux/ *Figure 7 – Clickjack POC*
Remediation	To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options to DENY or the value SAMEORIGIN to allow framing by pages on the same origin as the response itself.
References	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options • https://cwe.mitre.org/data/definitions/693.html

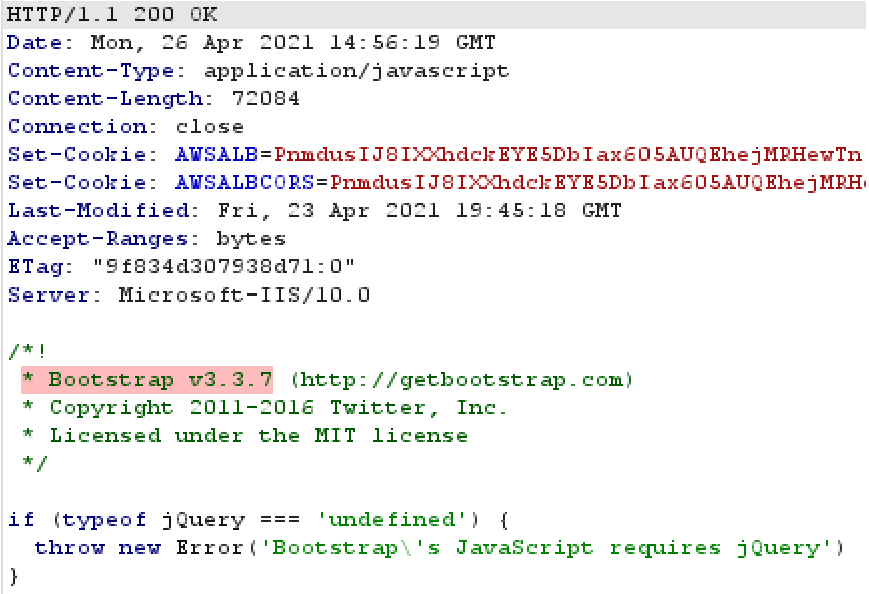
Issue ID #5	**Password Field With Autocomplete Enabled**
Attributes	**Overall Risk:** Low **User Risk:** Medium **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	The autocomplete feature stores sensitive data in the browser that could (depending on the make and version of the browser) be extracted when the user visits a malicious or compromised website, or if a different user on the local machine gains access to that local browser data store. If credentials are being stored, it may be possible to bypass the web application's authentication mechanism with the stolen credentials.
Affected Location	https://www.shimbonda.com/RVPen/LoginPage.aspx

Evidence	 24 https://www.shimbonda.com GET /RVPen/LoginPage.aspx/
	
	`subHeading">Password:</span>`
	`</td>`
	`<td class="right_cell" id="password_cell">`
	`<div class="input_div">`
	`<div id="password_icon">`
	`</div>`
	`<input name="txtPassword" type="password" maxlength="20" id="txtPassword" class="font_content_data" placeholder="Password" autocomplete="new-password" />`
	`</div>`
	`</td>`
	Figure 8 – Response returned with our user input

Remediation	Disable Browser Autocomplete: The autocomplete attribute must be set to “off” on all forms and fields that contain confidential and restricted information. Use the **AUTOCOMPLETE=’OFF’** attribute (to protect all form fields), or for individual sensitive form input fields, as appropriate.
References	- https://cwe.mitre.org/data/definitions/200.html

Issue ID #6	**Outdated JavaScript Resources**
Attributes	**Overall Risk:** Low **User Risk:** Low **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	The application includes an outdated version of the jQuery JavaScript library. This library contains known vulnerabilities and it is recommended to update to the latest version. While VantagePoint was not able to exploit this library, changes to the application or a more dedicated attacker could discover a way to exploit vulnerable functions. The application was found to use the following vulnerable library: **Bootstrap:** 3.3.7 **Location:** https://www.shimbonda.com/RVPen/rux/Scripts/bootstrap.js **jQuery:** 1.9.1 **Location:** https://www.shimbonda.com/RVPen/ScriptDialog/javascripts/jquery.min.js **prototype:** 1.5.0 **Location:** https://www.shimbonda.com/RVPen/ScriptDialog/javascripts/prototype.js
Affected Hosts	https://www.shimbonda.com/RVPen/

Evidence

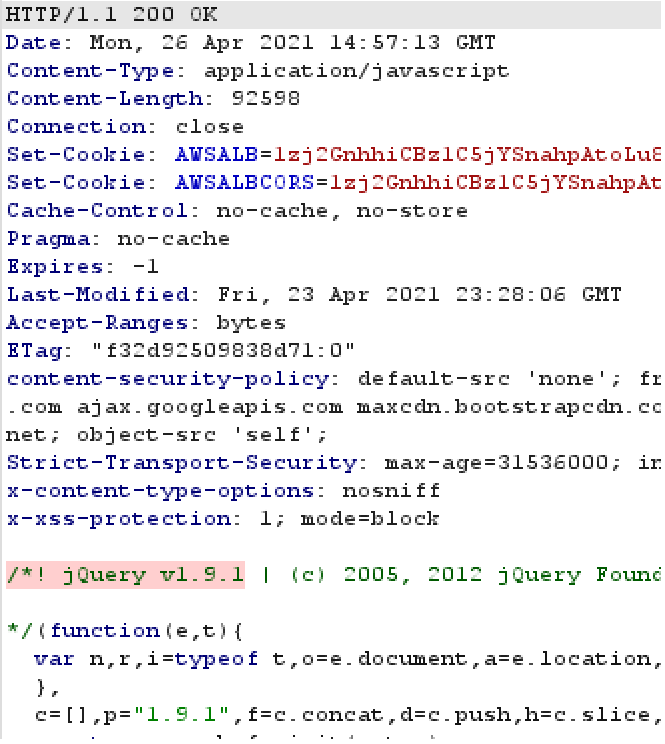


```
HTTP/1.1 200 OK
Date: Mon, 26 Apr 2021 14:56:19 GMT
Content-Type: application/javascript
Content-Length: 72084
Connection: close
Set-Cookie: AWSALB=PnmdusIJ8IXXhdckEYE5DbIax605AUQEhejMRHewTn
Set-Cookie: AWSALBCORS=PnmdusIJ8IXXhdckEYE5DbIax605AUQEhejMRH
Last-Modified: Fri, 23 Apr 2021 19:45:18 GMT
Accept-Ranges: bytes
ETag: "9f834d307938d71:0"
Server: Microsoft-IIS/10.0

/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */

if (typeof jQuery === 'undefined') {
  throw new Error('Bootstrap\'s JavaScript requires jQuery')
}
```

Figure 9 – An outdated version of jQuery is used by the application.



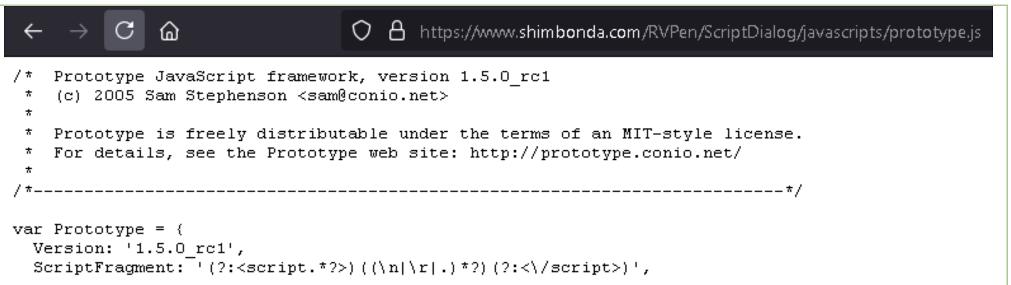
```
HTTP/1.1 200 OK
Date: Mon, 26 Apr 2021 14:57:13 GMT
Content-Type: application/javascript
Content-Length: 92598
Connection: close
Set-Cookie: AWSALB=1zj2GnhhiCBz1C5jYSnahpAtoLu
Set-Cookie: AWSALBCORS=1zj2GnhhiCBz1C5jYSnahpAt
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Last-Modified: Fri, 23 Apr 2021 23:28:06 GMT
Accept-Ranges: bytes
ETag: "f32d92509838d71:0"
content-security-policy: default-src 'none'; fr
.com ajax.googleapis.com maxcdn.bootstrapcdn.cc
net; object-src 'self';
Strict-Transport-Security: max-age=31536000; in
x-content-type-options: nosniff
x-xss-protection: 1; mode=block

/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Found

*/(function(e,t){
  var n,r,i=typeof t,o=e.document,a=e.location,
  },
  c=[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,
```

Figure 10 – An outdated version of jQuery is used by the application.

<table>
<tr>
<td></td>
<td>



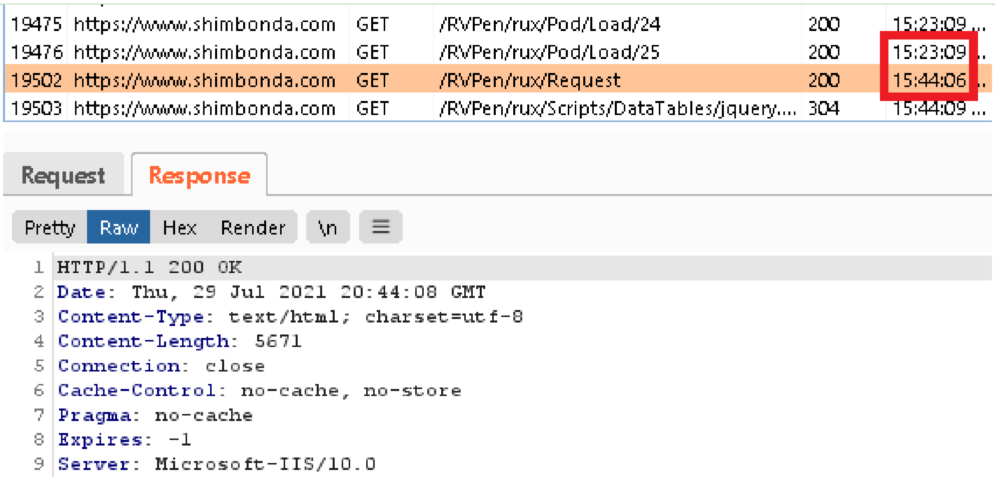
https://www.shimbonda.com/RVPen/ScriptDialog/javascripts/prototype.js

```
/*  Prototype JavaScript framework, version 1.5.0_rc1
 *  (c) 2005 Sam Stephenson <sam@conio.net>
 *
 *  Prototype is freely distributable under the terms of an MIT-style license.
 *  For details, see the Prototype web site: http://prototype.conio.net/
 *
/*--------------------------------------------------------------------------*/

var Prototype = {
  Version: '1.5.0_rc1',
  ScriptFragment: '(?:<script.*?>)((\n|\r|.)*?)(?:<\/script>)',
```

Figure 11 – An outdated version of jQuery is used by the application.

</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Upgrade the JavaScript libraries used to the latest version. The latest version of jQuery is 3.6.0, Bootstrap is 5.0.2, prototype is 1.7.3.</td>
</tr>
<tr>
<td><b>References</b></td>
<td>• https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
• https://nvd.nist.gov/vuln/detail/CVE-2019-11358</td>
</tr>
</table>

<table>
<tr><th>Issue ID #7</th><th>Excessive Session Timeout</th></tr>
<tr><td><b>Attributes</b></td><td><b>Overall Risk:</b> Low
<b>User Risk:</b> Medium
<b>Infrastructure Risk:</b> None
<b>Attack Complexity:</b> Medium</td></tr>
<tr><td><b>Description</b></td><td>Authenticated sessions remain active for over twenty minutes without user activity. This can allow give an attacker more time to carry out attacks. With physical access to the user’s computer, an attacker can wait until the user leaves their computer unattended. A longer session timeout gives more leeway to a brute-force attack against session IDs as well.</td></tr>
<tr><td><b>Affected Locations</b></td><td>https://www.shimbonda.com/RVPen/, https://www.shimbonda.com/API/</td></tr>
<tr><td><b>Evidence</b></td><td>

<pre>
19475 https://www.shimbonda.com GET /RVPen/rux/Pod/Load/24   200 15:23:09 ...
19476 https://www.shimbonda.com GET /RVPen/rux/Pod/Load/25   200 15:23:09 ...
19502 https://www.shimbonda.com GET /RVPen/rux/Request   200 15:44:06 ...
19503 https://www.shimbonda.com GET /RVPen/rux/Scripts/DataTables/jquery.... 304 15:44:09 ...
</pre>

<pre>
HTTP/1.1 200 OK
Date: Thu, 29 Jul 2021 20:44:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 5671
Connection: close
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/10.0
</pre>
<i>Figure 12 – Sessions remain active for over 20 minutes of inactivity.</i>
</td></tr>
<tr><td><b>Remediation</b></td><td>VantagePoint recommends invalidating sessions that have shown no activity in over twenty minutes. For applications that contain sensitive data or functionality, a stricter timeout of ten or even five minutes may be preferred.</td></tr>
<tr><td><b>References</b></td><td><ul><li>https://www.owasp.org/index.php/Session_Timeout</li><li>https://www.owasp.org/index.php/Session_Management_Cheat_Sheet</li></ul></td></tr>
</table>

Informational Risk Findings

Issue ID #8

Wildcard Certificate Exposes Potential Certificate Forgery

Attributes

Overall Risk: Informational
User Risk: Low
Infrastructure Risk: None
Attack Complexity: High

Description

It is considered a general best practice to avoid using wild card certificates. Wildcard certificates are often used to secure many hosts with the same certificate. However, as a guiding principle, certificates should be used to authenticate just one entity, which aligns with the principle of least privilege.

Although this is a staging environment, where there is little to no impact, it is worth ensuring this is resolved before deployment since, by sharing the private key portion of the certificate with several other hosts, the attack surface is expanded and increases the chances of exposing this secret. In the case an attacker does come into possession of the wildcard certificate private key, they will be able to forge certificates for any of the hosts that use it. Note that the TLS certificate are signed for *.shimbonda.com, rather than for specific subdomains.

Affected Hosts

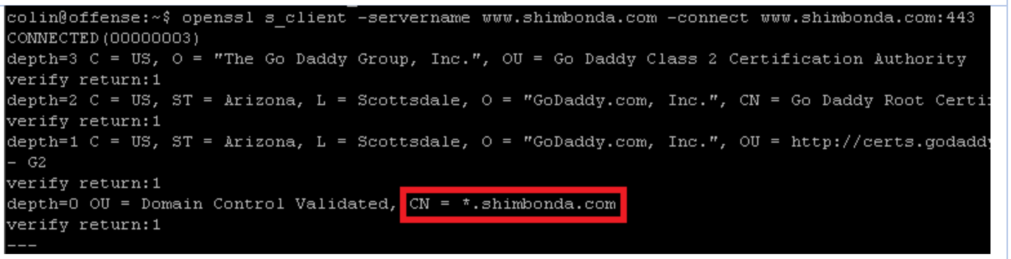
https://www.shimbonda.com

Test Method

Run the following command, and observer the wildcard certificate in use:

```
openssl s_client -connect shimbonda.com:443
```

Evidence



```
colin@offense:~$ openssl s_client -servername www.shimbonda.com -connect www.shimbonda.com:443
CONNECTED(00000003)
depth=3 C = US, O = "The Go Daddy Group, Inc.", OU = Go Daddy Class 2 Certification Authority
verify return:1
depth=2 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", CN = Go Daddy Root Certi
verify return:1
depth=1 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godadd
- G2
verify return:1
depth=0 OU = Domain Control Validated, CN = *.shimbonda.com
verify return:1
---
```

Figure 13 – The SSL certificate is signed for all subdomains of shimbonda.com.

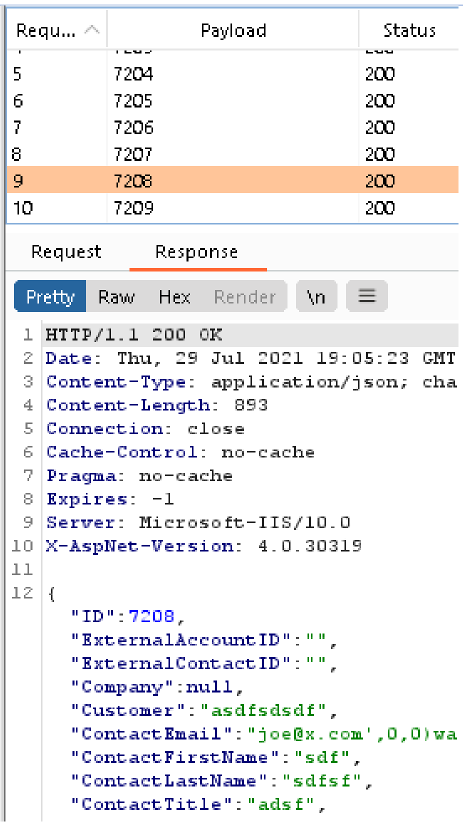
Remediation

Avoid the use of wildcard certificates. Consider adding specific certificate for specific domains or switch to using multi-domain certificates, which can stand in for wild card domains, but include more flexibility, by using a "Subject Alternative Name" that allows the specification of additional host names; like IP addresses, common names, or sites, to be protected under a single SSL certificate.

References

- https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Issue ID #9	Concurrent Logins Allowed
Attributes	**Overall Risk:** Informational **User Risk:** Indirect **Infrastructure Risk:** None **Attack Complexity:** Low
Description	The application permits multiple valid session tokens. Maintaining multiple valid sessions for a user may result in concurrency faults that could arise when records within the application are updated simultaneously by different active sessions. This could result in inconsistent data, exceptions, and may result in a loss of logged illegitimate activity on a compromised account, if legitimate activity is taking place at the same time. Additionally, users are less likely to notice that their accounts have been compromised. They may also be more likely to share accounts that permit concurrent login sessions. Additionally, there may be data integrity problems due to multiple simultaneous logins.
Affected Host	https://www.shimbonda.com
Remediation	Invalidate old, still existing session tokens when the user logs in. The user should be notified upon login that their previous session existed, and users of the old sessions should be notified that the sessions have been invalidated due to another login. Users should have security-relevant actions available to them (change password, report account compromise) if they do not recognize the other logins.
References	• OWASP Session Management ○ https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Simultaneous_Session_Logons

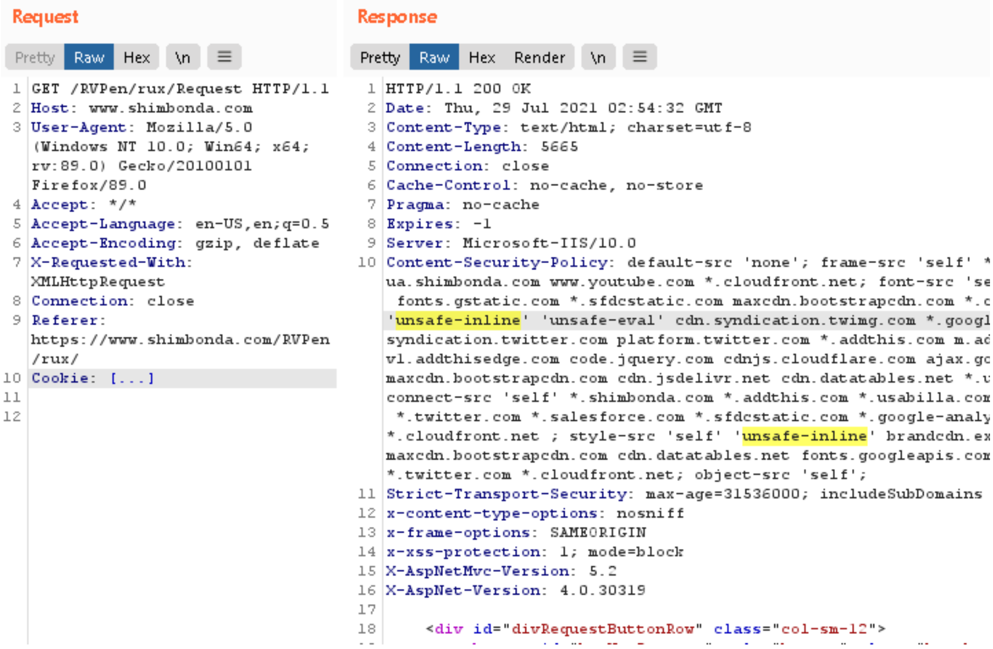
Issue ID #10	**Sequential Identifiers**
Attributes	**Overall Risk:** Low **User Risk:** Low **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	Application IDs for timesheets, expense reports, and other data are identified by sequential integers. While this is not a security risk on its own, if an attacker were to gain access to the system, identifying data with sequential integers makes it very easy to iterate through all the data on the system, making it trivial to scrape large amounts of data even with little knowledge of how the application works.
Affected Host	Systemic
Evidence	 *Figure 14 – An enumeration of nomination details.*

Requ...	Payload	Status
5	7204	200
6	7205	200
7	7206	200
8	7207	200
9	7208	200
10	7209	200

```
HTTP/1.1 200 OK
Date: Thu, 29 Jul 2021 19:05:23 GMT
Content-Type: application/json; cha
Content-Length: 893
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319

{
   "ID":7208,
   "ExternalAccountID":"",
   "ExternalContactID":"",
   "Company":null,
   "Customer":"asdfsdsdf",
   "ContactEmail":"joe@x.com',0,0)wa
   "ContactFirstName":"sdf",
   "ContactLastName":"sdfsf",
   "ContactTitle":"adsf",
```

Remediation	Use cryptographically secure guids (Globally Unique Identifiers) to identify data. This makes it impossible for attackers to easily discover content, users, and other valuable information in the event of a breach or attack.
References	• https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

Issue ID #11	Insecure Content Security Policy
Attributes	**Overall Risk:** Informational **User Risk:** Medium **Infrastructure Risk:** None **Attack Complexity:** Medium
Description	The application does include a "Content-Security-Policy" (CSP) header in responses, however the defined policy includes some weak configurations. The inclusion of this HTTP header lets the application define a whitelist of trusted sources and or source types from which the browser can include as content. A CSP header can reduce the impact of attacks such as Cross-Site Scripting by preventing an attacker from utilizing malicious JavaScript code hosted on another domain.
Affected Locations	https://www.shimbonda.com/RVPen/
Evidence	 Request GET /RVPen/rux/Request HTTP/1.1 Host: www.shimbonda.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate X-Requested-With: XMLHttpRequest Connection: close Referer: https://www.shimbonda.com/RVPen/rux/ Cookie: [...] Response HTTP/1.1 200 OK Date: Thu, 29 Jul 2021 02:54:32 GMT Content-Type: text/html; charset=utf-8 Content-Length: 5665 Connection: close Cache-Control: no-cache, no-store Pragma: no-cache Expires: -1 Server: Microsoft-IIS/10.0 Content-Security-Policy: default-src 'none'; frame-src 'self' * ua.shimbonda.com www.youtube.com *.cloudfront.net; font-src 'se fonts.gstatic.com *.sfdcstatic.com maxcdn.bootstrapcdn.com *.c 'unsafe-inline' 'unsafe-eval' cdn.syndication.twimg.com *.googl syndication.twitter.com platform.twitter.com *.addthis.com m.ad v1.addthisedge.com code.jquery.com cdnjs.cloudflare.com ajax.go maxcdn.bootstrapcdn.com cdn.jsdelivr.net cdn.datatables.net *.u connect-src 'self' *.shimbonda.com *.addthis.com *.usabilla.com *.twitter.com *.salesforce.com *.sfdcstatic.com *.google-analy *.cloudfront.net ; style-src 'self' 'unsafe-inline' brandcdn.ex maxcdn.bootstrapcdn.com cdn.datatables.net fonts.googleapis.com *.twitter.com *.cloudfront.net; object-src 'self'; Strict-Transport-Security: max-age=31536000; includeSubDomains x-content-type-options: nosniff x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block X-AspNetMvc-Version: 5.2 X-AspNet-Version: 4.0.30319 <div id="divRequestButtonRow" class="col-sm-12"> *Figure 15 – The “unsafe-inline” directive is included in the CSP header.*
Remediation	Configure the server to include a “Content-Security-Policy” HTTP header in responses: Content-Security-Policy: default-src self;

	The above example CSP header will provide basic protections, but the header can restrict or allow several different sources and source types. Further documentation can be found listed in the references section below.
References	• https://www.owasp.org/index.php/Content_Security_Policy • https://www.w3.org/TR/CSP/ • https://www.html5rocks.com/en/tutorials/security/content-security-policy/

3. Methodology

VantagePoint uses a combination of automated and manual analysis to perform a rigorous assessment of the environment under the scope of this report. In addition to the tests and supporting evidence presented in prior sections, we leverage published OWASP testing protocols such as those listed below:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling
- Cryptography
- Business Logic Testing
- Client-Side Testing

Tools and Technology

VantagePoint uses a variety of testing tools and technologies to perform automated analysis of client environments. Below is a list of the major tools used for testing:

- Burp Proxy Pro (https://portswigger.net/burp)
- Nikto (https://cirt.net/Nikto2)
- Nmap (https://nmap.org/)
- Testssl.sh (https://testssl.sh/)
- sqlmap (http://sqlmap.org/)
- curl (https://curl.haxx.se/)
- openssl s_client (https://www.openssl.org/docs/manmaster/man1/s_client.html)

Goals and Objectives

The goals and objectives of the assessment are as follows:

- Identify “alive” hosts on the network using scanning automation
- Identify open ports on hosts serving content to the Internet
- Discover applicable servers via banners
- Perform research on servers, host operating systems, and other applicable attack vectors to perform additional analysis
- Identify vulnerabilities in system services or operating systems in a manual and automated fashion while operating in “passive” mode
- Validate vulnerabilities to provide evidence and remove false positives
- Inventory and prioritize vulnerabilities based on real-world security risk
- Identify remediation steps for vulnerabilities
- Report on all of the above steps