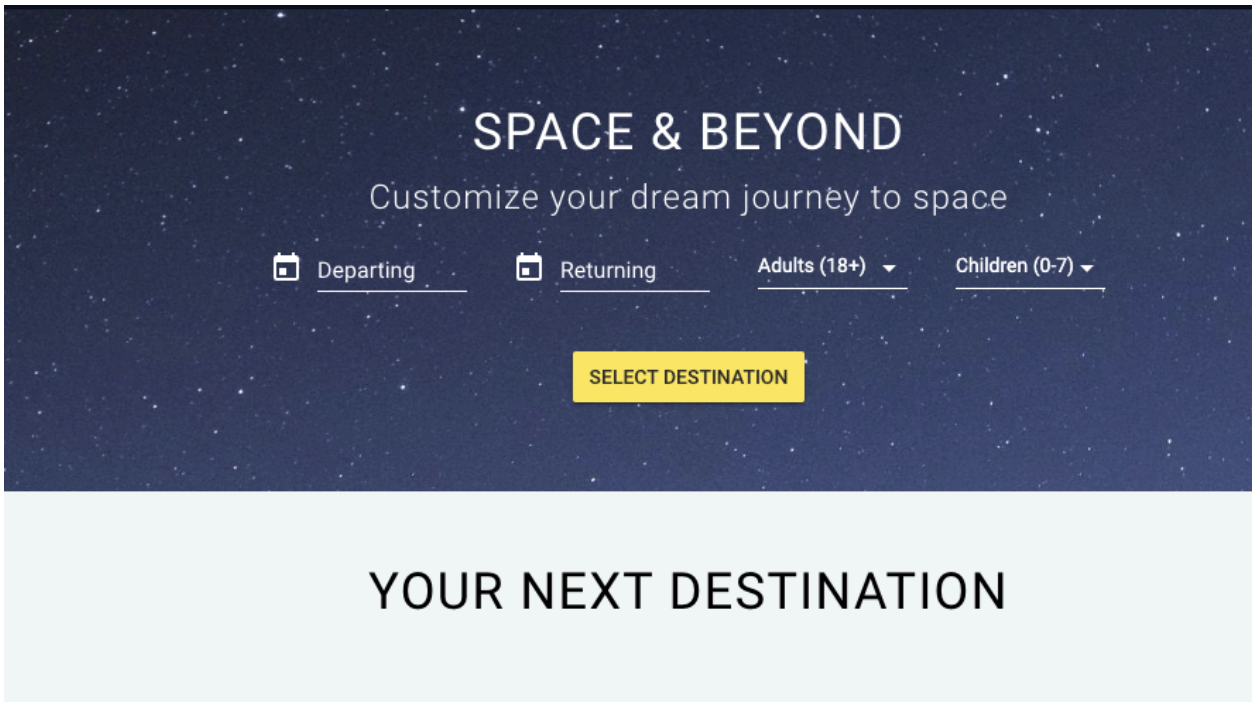
# SevereQA

## Web Application Penetration Test

**Final Report**




| | |
|---|---|
| **Prepared For** | Testim - **Space & Beyond** |
| **Date** | April 2, 2024 |
| **Tested By** | Pablo V., Security Analyst |

Table of Contents


**Engagement Contacts** **1**

**Executive Summary** **2**

- Approach 2
- Rules Of Engagement 3
- Permission / Authorization 3
- Scope 4
- Overview 6

**Technical Summary** **7**

- Information Gathering 7
- Site Mapping 7
- Discovery 7
- Exploitation 7

**Detailed Walkthrough / Post Exploitation** **8**

**Remediation Summary** **19**

- Short-Term 19
- Medium-Term 19
- Long-Term 19

**Technical Findings Resources** **20**

## Engagement Contacts

| Client Contacts | | | |
|---|---|---|---|
| Primary Contact | Title | Email | Phone Number |
| Joe Momma | Chief Executive Officer | jmomma@testim.com | 212-333-4455 |
| Guillermo Rojas | CISO | grojas@testim.com | 212-333-4920 |

## Location Information

**Space & Travel**
1 Copernicus Lane - Suite 301
% Astrium, DigitalGlobe
Palo Alto, CA94304
https://demo.testim.io/

| Assessor Contacts | | | |
|---|---|---|---|
| Assessor Contact | Title | Email | Phone Number |
| Pablo V. | Security Consultant | pablofvergara@msn.com | 631-202-2929 |

## Executive Summary

**Testim** contracted **SevereQA** with performing a **Security Audit** of their web application - ***Space & Travel.com*** - to identify security weaknesses, determine the impact to **Testim**. The purpose of this assessment is to verify the effectiveness of the security controls put in place by **Testim** to secure business-critical information.

These systems have been identified as **business-critical** and contain important information which, if accessed inappropriately, could cause material harm to **Testim**.

For more insights on reporting, visit: Reporting - The Penetration Testing Execution Standard

### Approach

**SevereQA** performed testing under a "black box" approach from **April 2, 2024**, to **April 10, 2024** without credentials or any advance knowledge of **Testim's** internally facing environment with the goal of identifying unknown weaknesses.

In an effort to test **Testim**'s ability to defend against direct and indirect attack, **Security Analyst** executed a comprehensive suite of tests.

Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible.

Testing was performed remotely via a host that was provisioned specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential.

**SevereQA** sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If **SevereQA** were able to gain a foothold in the internal network, **Testim** allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

This report represents the findings from the assessment and the associated remediation recommendations to help **Testim** strengthen its security posture.

## Rules Of Engagement

*Below is an expressed understanding between Client & Consultancy regarding the rules of engagement associated with the work to be performed. Amendments to this ROE will be attached to this document, with proper acknowledgment noted.*

1. What is the ROE for this penetration test?
   a. Non-invasive; Non-destructive demonstration of impact caused by found vulnerability
   b. Testing will be conducted in a secure, unintrusive environment on a dedicated system
   c. No need to test physical security
   d. Web Application - All features
   e. API testing as necessary

2. What is the schedule?
   a. Starting 04/02/2024
   b. Time limit: 1 week, 8hrs per day during operating hours, remote (on-site tbd)

3. Who will be notified of the PT and when?
   *Security Analyst will halt all testing should a **critical** issue be found and / or RCE is established; data is leaked*
   a. CEO will be notified of any critical / high severity issues (zero-days)
   b. CISO / CTO / Tech Lead will notified of all issues

4. What systems or networks are off limits?
   a. Only the supplied target system is to be tested. All else is off limits, inclusive of the servers and load balancers
   b. All networks are off limits

## Permission / Authorization

☐ I **Guillermo R., CISO**, employed at **Testim** do hereby grant **Pablo Vergara, Security Analyst**, employee of **SevereQA** full permission to perform the following: **Security Audit** on April 2, 2024 based on the defined scope and ROE. The Security Analyst has been debriefed on expectations and acknowledges what is and is not in scope, and that **failure to abide by the terms expressed in this SOW constitute a violation of the arrangement Testim has with SevereQA, and may be subject to legal action.**

## Scope

The scope of this assessment, as provided was **https://demo.testim.io/**.

Server: 172.16.69.2
Address: 172.16.69.2#53 | 108.158.61.54
Nameserver: hope.ns.cloudflare.com
Host Company: Amazon
IPV4 Address: 18.66.171.40 IPV6: 2600:9000:2245:b000:2:3286:bb80:93a1
Domain Registrar: N/A
22/tcp filtered ssh
80/tcp open http

With the following features under test

| Features Under Test | | | |
|---|---|---|---|
| Feature # | Feature Name | Description | Priority |
| 1 | Site Login | User can authenticate and see their travel purchases | High |
| 2 | Checkout Workflow | User selects planet and books their travel destination | High |
| 3 | Destination Selection | User can select dates to book their vacation | Medium |
| 4 | Planet Selection | User can select destination by name or planet color | Medium |
| 5 | Price Slider | User can filter home page results by price | Low |
| 6 | Apply Promo | User can apply a discount code for additional savings | Low |

Upon completion of the penetration test, the following tally of what was discovered is shown in the chart below:

| Information Security Risk Rating Scale | | | |
|---|---|---|---|
| **Value** | **Description** | **Remediation Schedule** | **Count** |
| **Criticals (10 - *n*)** | Extreme risk of compromise; Loss of financial information, reputation, etc.<br>Financial Impact Rating - **$$$$** | 0 - 3d | 0 |
| **High (7 - 9)** | High risk of compromise and/or loss of business reputation<br>Financial Impact Rating - **$$$** | 3 - 5d | 6 |
| **Medium (4 - 6)** | Moderate risk of compromise<br>Financial Impact Rating - **$$** | 1w - 2w | 3 |
| **Low (1 - 3)** | Low / Negligible risk; Minimal impact<br>Financial Impact Ratinge - **$** | 2w | 5 |
| **Informational** | No Impact or Risk | +2w | 11 |

## Overview

Among the results of the findings were not many **Criticals**, a few number of **Highs,** several **Mediums,** and a substantial number of **Low**(s) and **Informational**(s). Having evaluated said findings, with a high degree of confidence, SevereQA has determined the overall risk to be in the range of **Medium-High**.

**Why this matters**

The **[High]** findings were somewhat concerning. The site is not employing sufficient validation for username or password strength. It was discovered that anyone can authenticate with test credentials as short as one (1) character. Password strength was not enforced. Along with the weak login architecture, the lack of any kind of CAPTCHA or multi-factor authentication opens up the possibilities for brute-force authentication, username harvesting, and more.

The [Medium] results include vulnerabilities like the Content Security Policy header not being set, relative path confusion, subresource integrity attribute is missing, and relative path confusion.

While seemingly benign on the surface, it can be possible to string a substantial amount of **[Low]** and **[Informational]** issues and chain a more sinister proof-of-concept.

## Technical Summary

SevereQA began all testing activities from the perspective of an unauthenticated user on the internal network. **Testim** provided the tester with **the url** but did not provide additional information such as operating system or configuration information. The steps take were:

- Recon & Information Gathering
- Site Mapping
- Discovery
- Exploitation

### Information Gathering

During the recon/information gathering step, tester employed basic OSINT strategies and tactics to learn as much as they could about the infrastructure, tech stack, open ports, and so on.

### Site Mapping

During the site mapping step, tester executed an automated script using feroxbuster to map the breadth of the application, and wrote the results to a text file. The result was a list of urls in scope that were fed to the proxy tool ZAP.

### Discovery

Tester explored the application as a normal user, inspecting all front-end elements and API calls. They then directed their efforts towards the above-mentioned targets in scope looking for flaws in the logic and any vulnerabilities therein.

### Exploitation

Tester executed a series of test scenarios addressing OWASP Top 10 : 2021, as well as the following domains:

1. Information Gathering
2. Configuration & Deployment Management
3. Identity Management
4. Authentication
5. Authorization
6. Session Management
7. Input Validation
8. Error Handling
9. Weak Cryptographic Security
10. Business Logic / Design Vulnerabilities
11. Client-Side Vulnerabilities
12. Other Common Issues

## Login - Form Input Fields Are Inadequately Labeled — Risk/Exposure Score: 2

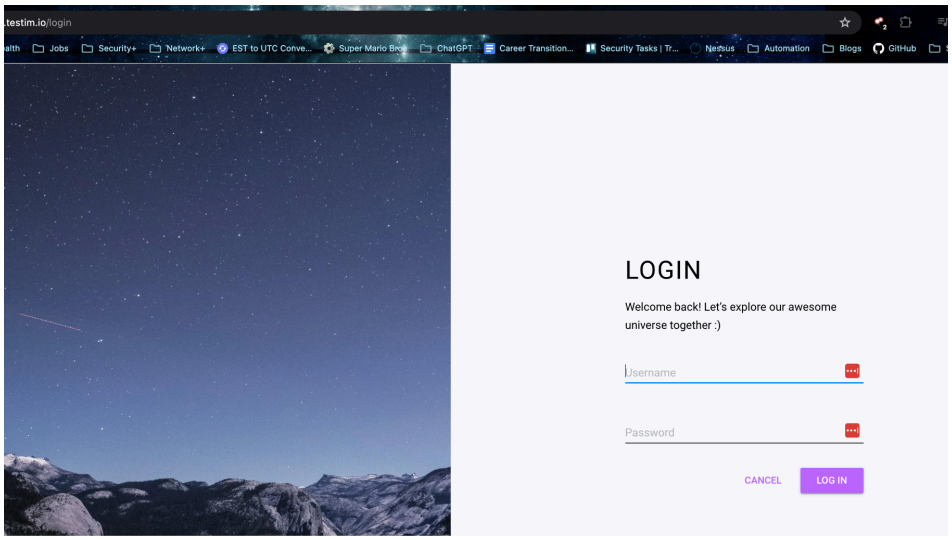
Exploit Target in Scope

- https://demo.testim.io/login

OWASP Top-10 Exploit type

- WSTG-BUSL-03 - Test Integrity Checks

Screenshot




Steps to reproduce

1. Launch site and navigate to login

Outcome

Attack not performed

- Inputs are using placeholder text to identify the input types

Remediation

- Inputs need to be properly labeled. Username / Password inputs need to employ field labels

Remediation Schedule (required)

- Within **1** Sprint

## Issue: Login - No Validation for Invalid Logins Credentials  Risk/Exposure Score: 9

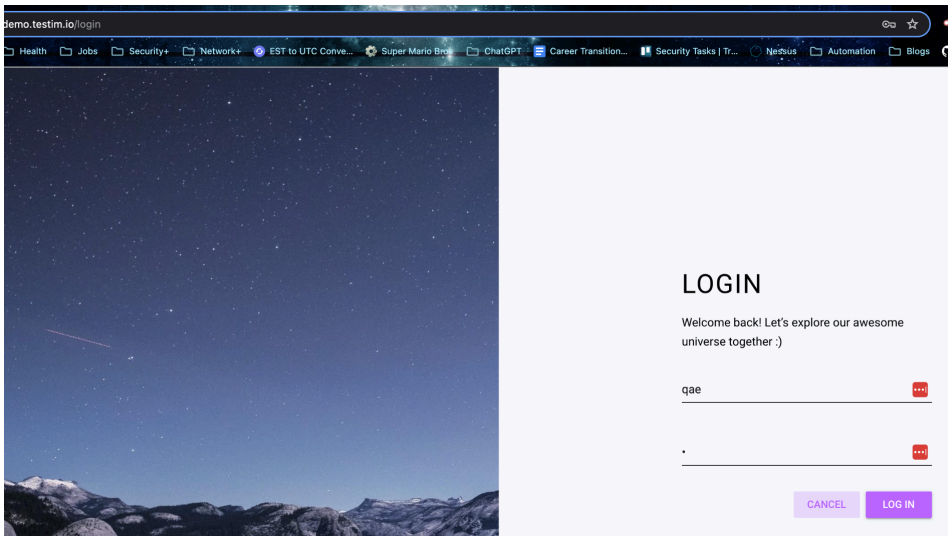
### Exploit Target in Scope

- https://demo.testim.io/login

### OWASP Top-10 Exploit type

- WSTG-BUSL-01 - Test Business Logic Data Validation
- WSTG-ERRH-01 - Testing for Improper Error Handling

### Screenshot




### Steps to reproduce

1. Launch site & click “Login”
2. Enter any value in the username and password input and submit form
   Tested with:
   a. Random name / **three letter username / single letter password**
   c. “admin” / “admin” .. and all other common weak usernames/passwords

### Outcome

Attacks Successful

- Using credentials with weak passwords, or character lengths as short as 1 character, tester successfully authenticated to the site. User displayed was always “John”

### Remediation

- Login form needs to account for character lengths for username and password

### Remediation Schedule (required)

- Within **1** Sprint

## LOGIN - PASSWORD STRENGTH NOT OBSERVED — RISK/EXPOSURE SCORE: 9

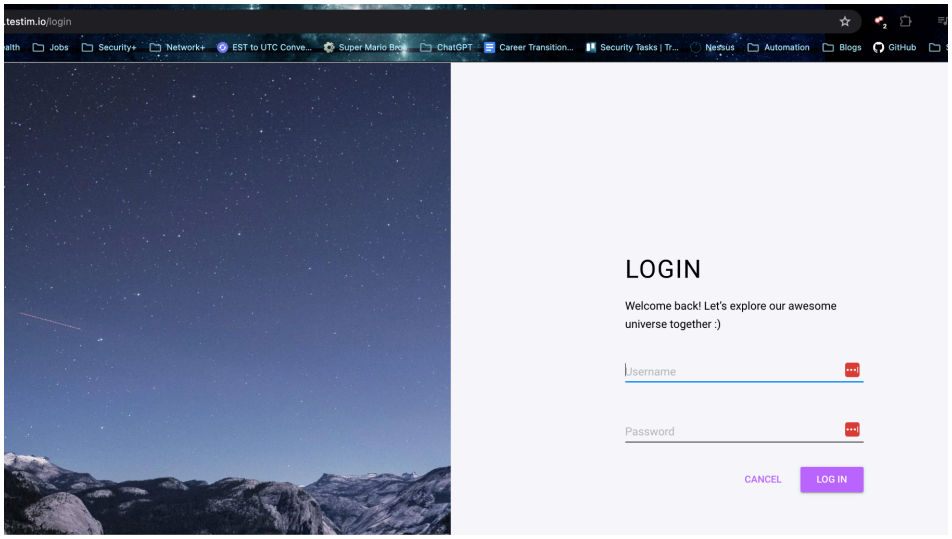
### Exploit Target in Scope

- https://demo.testim.io/login

### OWASP Top-10 Exploit type

- WSTG-ATHN-07 - Testing for Weak Password Policy

### Screenshot




### Steps to reproduce

1. Launch site & click “Login”
2. Submit login with any value in the username and password having 1 character or weak phrase

### Outcome

Attacks Successful

- Login never properly validates for password strength

### Remediation

- Best Practices for Password Strength: https://passwordtester.org/
- Password Storage Cases

### Remediation Schedule (required)

- Within **5** Business Days or **1** Sprint

## LOGIN - **NO CAPTCHA / MFA EMPLOYED** RISK/EXPOSURE SCORE: **8**

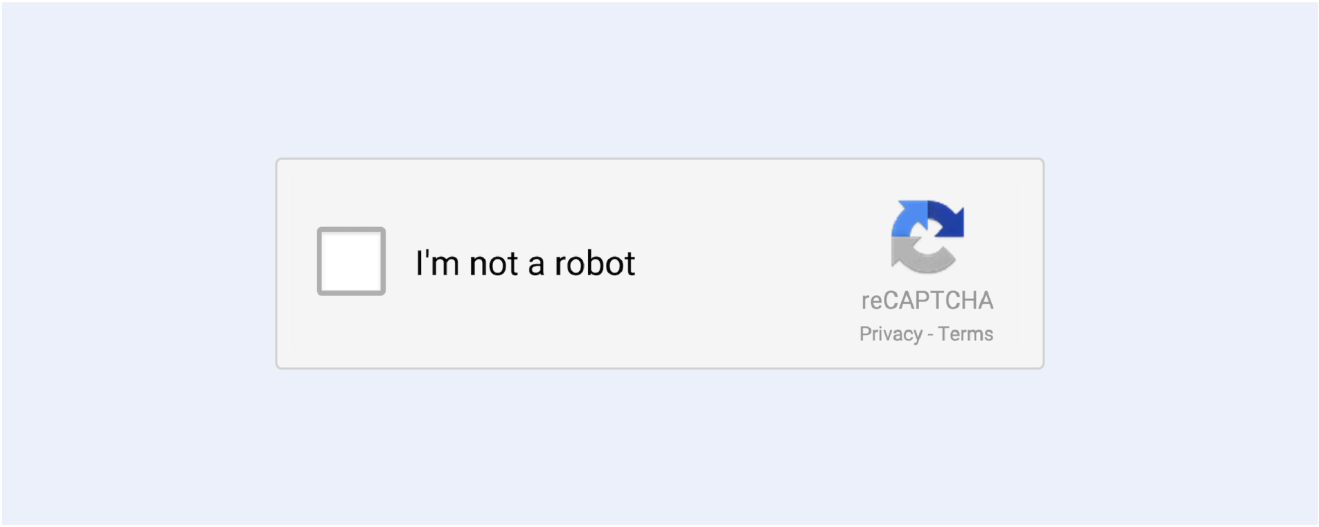
Exploit Target in Scope

- https://demo.testim.io/login

OWASP Top-10 Exploit type

- WSTG-AUTH-11 - Testing Multi-Factor Authentication (MFA)

Screenshot (expectation)




Steps to reproduce

1. Launch site & click “Login”
2. Enter any value in the username and password input and submit form

Outcome

No Attack Needed

- User is never prompted to verify identity via security question, CAPTCHA, or SMS/OTP

Remediation

- It is highly recommended that at least two of the following factors are required to authentication:
  - Passwords, PINs and security questions
  - Hardware / Software tokens - PIN; Email; SMS / Phone Call

Remediation Schedule (required)

- Within **7** Business Days **1** Sprint

## CHECKOUT - CUSTOM HEADER VULNERABILITY — RISK/EXPOSURE SCORE: 7

### Exploit Target in Scope

- https://demo.testim.io/checkout

### OWASP Top-10 Exploit type

- WSTG-ATHZ-02 - Testing for Bypassing Authorization Schema

### Request

```
GET https://demo.testim.io/checkout HTTP/1.1
host: demo.testim.io
X-Rewrite-URL: /donotexist2
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="122", "Not(A:Brand";v="24", "Brave";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
content-length: 0
```

### Response

```
HTTP/1.1 404 Not Found
Content-Type: text/html
Content-Length: 1173
Connection: keep-alive
Last-Modified: Thu, 17 Aug 2017 09:35:35 GMT
ETag: "1cfc9b11094c26d6daac003b9f8f2411"
x-amz-error-code: NoSuchKey
x-amz-error-message: The specified key does not exist.
x-amz-error-detail-Key: checkout
x-amz-request-id: 9APBT9AJNX886WJB
x-amz-id-2: 6lScZ6PFwLkyizXQZSl1Dv3Uifhaha0f4ntTA+ZwKiA9G7JwvPB3ZB8RD1QCrP0Sq0L8LH4JwpM=
Date: Fri, 05 Apr 2024 18:08:24 GMT
Server: AmazonS3
Vary: Accept-Encoding
X-Cache: Error from cloudfront
Via: 1.1 8770cedbbb1c2feb157dc67ce83fe00c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: JFK50-P1
X-Amz-Cf-Id: rvFP3nZwjB0mGX-jh8pk7Koe3C73vWNmDd7XMZyljDSyt6zkcpLmzQ==
```

```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Space & Beyond | Testim.io demo</title>
    <meta name="description" content="A demo website to show off what you can do with Testim.io.">
    <meta name="author" content="Testim.io">
    <meta name="viewport" content="initial-scale=1.0,user-scalable=no,maximum-scale=1,width=device-width">
    <meta name="viewport" content="initial-scale=1.0,user-scalable=no,maximum-scale=1" media="(device-height: 568px)">

    <meta name="format-detection" content="telephone=no">
    <meta name="HandheldFriendly" content="True">
    <meta http-equiv="cleartype" content="on">
    <style>
      .layout {
        display: flex;
        min-height: 100vh;
```

Steps to reproduce

1. With Proxy On, Launch site
2. Enter travel dates
3. Select planet
4. Proceed with checkout flow
5. In the proxy, send the request to the request editor
6. Add a custom header & send the request

Outcome

Attacks Successful

- Encountered a 404 error which means application supports the special request headers.

Remediation

- Employ the least privilege principles on the users, roles, and resources to ensure that no unauthorized access occurs.

Remediation Schedule (required)

- Within **5 - 10** Business Days or **1** Sprint

## Checkout Flow Is Not Working — Risk/Exposure Score: 6

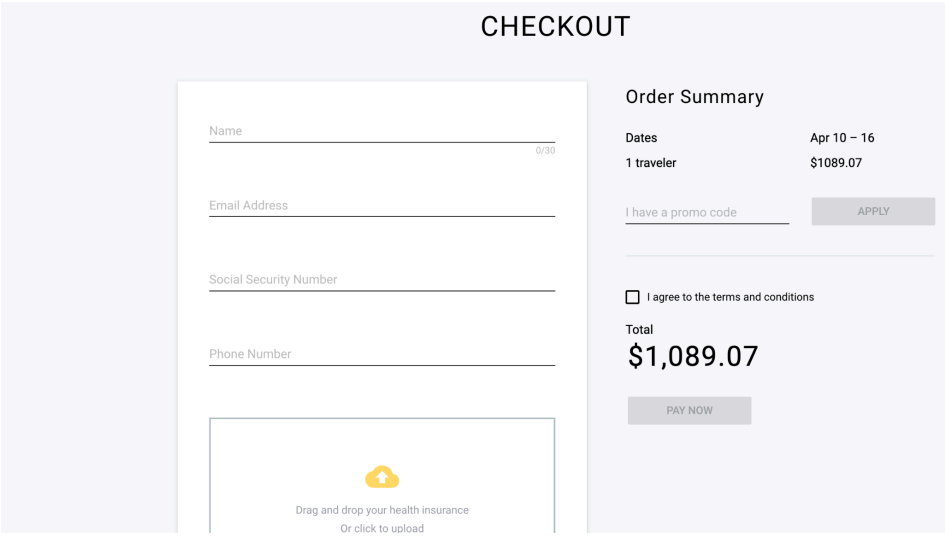
### Exploit Target in Scope

- https://demo.testim.io/checkout

### OWASP Top-10 Exploit type

- WSTG-BUSL-01 Test Business Logic Data Validation
- WSTG-BUSL-10 - Test Payment Functionality

### Screenshot




### Steps to reproduce

1. Launch site
2. Enter travel dates
3. Select planet
4. Proceed with checkout flow (fill form)
5. Check “Agree to terms” and submit form

### Outcome

No Attack Necessary

- Checkout flow is not operational

### Remediation

- Fix required for checkout workflow

### Remediation Schedule (required)

- Within **5** Business Days (**urgent!**)

## Access Control Origin Not Set — Risk/Exposure Score: 5

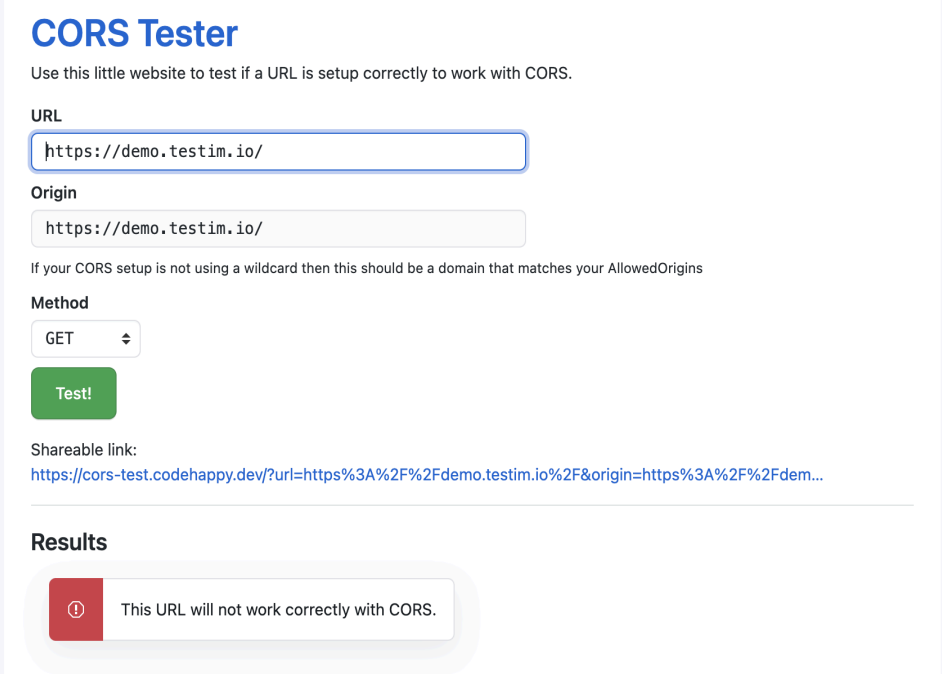
Exploit Target in Scope

- https://demo.testim.io/

OWASP Top-10 Exploit type

- WSTG-CLNT-07 Testing Cross Origin Resource Sharing

Screenshot




Steps to reproduce

1. Visit https://cors-test.codehappy.dev/
2. Enter site url wait for response

Outcome

- Site does not have the access-control-allow-origin header set to *. Without this header, requests from other domains cannot be made to it via a user's browser.

Remediation

- If Dev has access to the server for the URL, they'll need to modify it to add the access-control-allow-origin header. If not, they'll need to upload the file somewhere else.

Remediation Schedule (required)

- Within 5 - 10 Business Days or **1** Sprint

## Content Security Policy Header Not Set — Risk/Exposure Score: 6

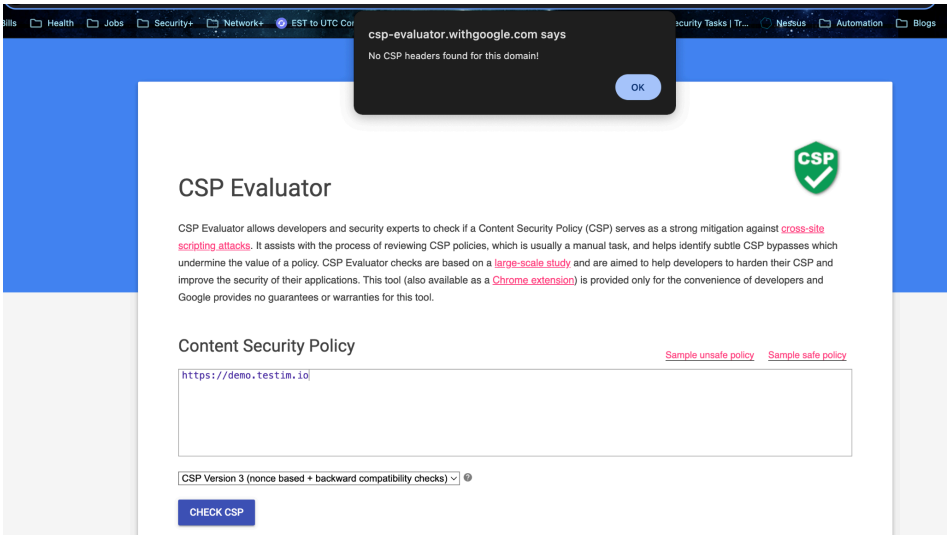
### Exploit Target in Scope

- https://demo.testim.io

### OWASP Top-10 Exploit type

- Test for Content Security Policy Header

### Screenshot




### Steps to reproduce

1. Paste url into https://csp-evaluator.withgoogle.com/

### Outcome

- Result showed a lack of CSP employed on the site which presents potential opportunities for stored, reflected, and some DOM XSS attacks

### Remediation

- Apply policy enforcement guidelines, found here: Strict-policy
- CSP Directive Reference: https://content-security-policy.com/
- Content Security Policy Level 3 (W3C): https://w3c.github.io/webappsec-csp/

### Remediation Schedule (required)

- Within **5 - 10** Business Days or **1** Sprint

## Relative Path Confusion — Risk/Exposure Score: 3

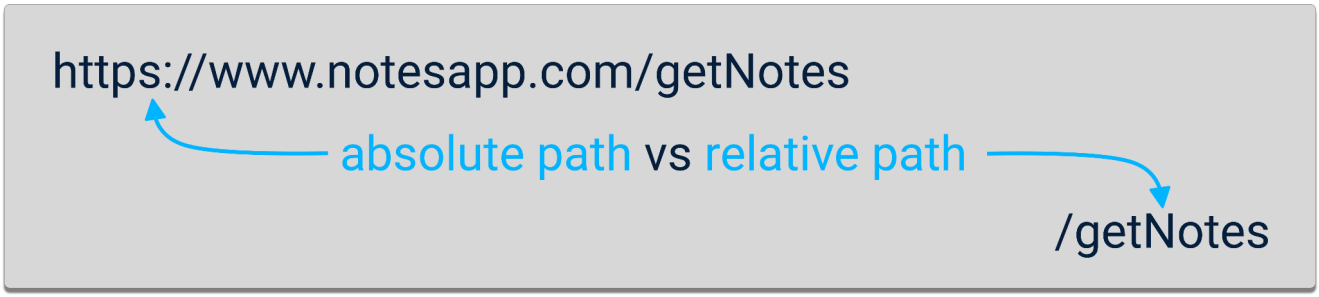
Exploit Target in Scope

- https://demo.testim.io

OWASP Top-10 Exploit type

- A05:2021 Security Misconfiguration

Screenshot




Steps to reproduce

1. Issue raised by active scanner

Outcome

- Found instances where site can be tricked into permissively parsing the “cross-content” response, using techniques such as framing, then the web browser may be fooled into interpreting HTML as CSS (or other content types), leading to an XSS vulnerability

Remediation

- https://arxiv.org/abs/1811.00917
- https://hsivonen.fi/doctype/
- https://www.w3schools.com/tags/tag_base.asp

Remediation Schedule (required)

- Within **5 - 10** Business Days or **1** Sprint

## SubResource Integrity Attribute Missing — Risk/Exposure Score: 3

Exploit Target in Scope

- https://demo.testim.io

OWASP Top-10 Exploit type

- A05:2021 Security Misconfiguration

Screenshot


Steps to reproduce

1. Issue raised by active scanner

Outcome

- The integrity attribute is missing on a script or link tag served by the external server

Remediation

- Provide a valid integrity attribute to the tag.
- https://www.zaproxy.org/docs/alerts/90003/
- https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Remediation Schedule (required)

- Within **5 - 10** Business Days or **1** Sprint

## Remediation Summary

For the issues pertaining to the **login** SevereQA recommends the following:

`LOGIN` – For the **login page**, implement MFA and login attempts counter. The error messaging can be something generic. For example: "*Your login attempt was unsuccessful. If you continue to have trouble, contact support.*"

`REGISTRATION` – Site needs a way to create users properly. At the moment, all logins point to user "John" without anything relevant (dashboard, profile, purchase history, etc.) to show.

`CHECKOUT` – The **Checkout** workflow for booking a reservation requires immediate attention. Submission of a user's travel destination is not working. The file upload feature has no proper context and should either be updated to reflect why the user needs to upload anything, or remove it altogether. Bonus coupons were not provided to test the input further, but some measure of validation is required for non-alpha numeric values.

### Short-Term

- Address the checkout issue
- Strengthen password requirement

### Medium-Term

- Send user email or SMS with PIN for login verification

### Long-Term

- Employ CAPTCHA or Token for login

## Technical Findings Resources

*CVEs, links, etc. go here*

- *IDOR Cheat Sheet*
- *File Upload Cheat Sheet*
- *CSRF Cheat Sheet*