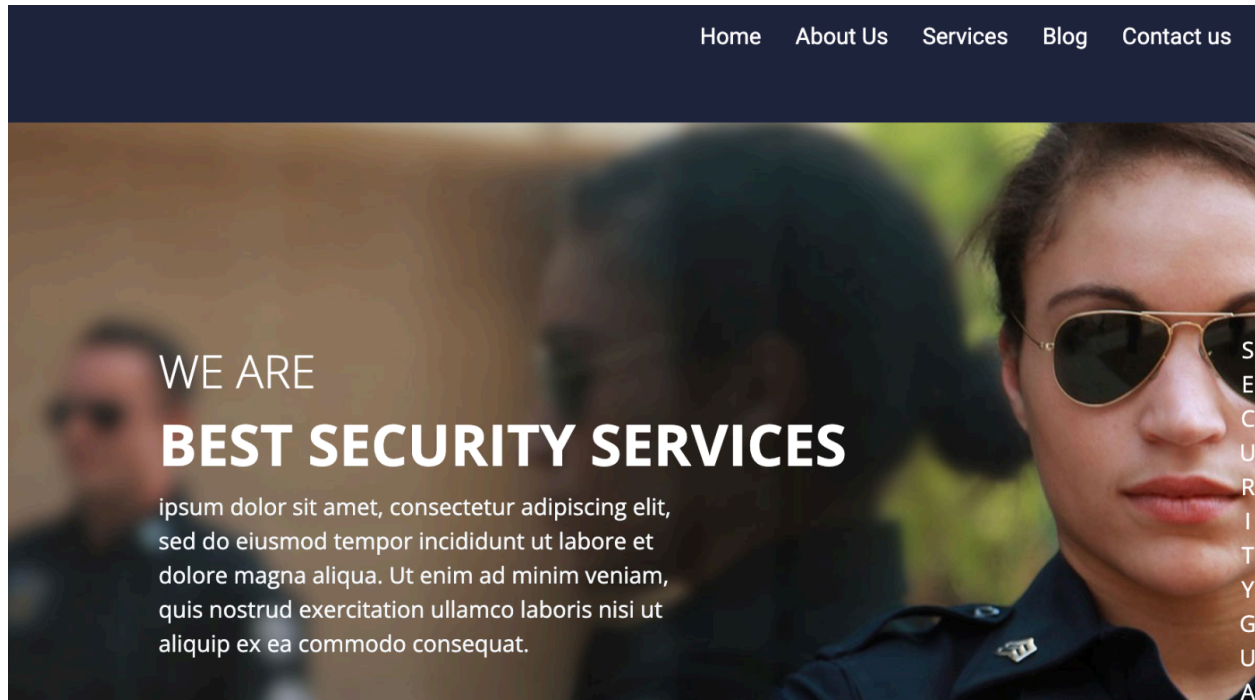


SevereQA

Web Application Penetration Test Final Report



Prepared For Royal Security Services

Date 05/09/2024

Tested By Pablo V., Sec

TABLE OF CONTENTS

Engagement Contacts	1
Executive Summary	2
Approach	2
Scope	3
Rules Of Engagement	3
Overview	4
Technical Summary	5
Site Mapping	5
Discovery	6
Information Gathering	6
Passive Intelligence	6
Active Intelligence	6
Corporate Intelligence	6
Personnel Intelligence	6
Vulnerability Assessment	7
Detailed Walkthrough / Post Exploitation	8
Remediation Summary	11
Short-Term	11
Medium-Term	11
Long-Term	11
Technical Findings Resources	12

ENGAGEMENT CONTACTS

CLIENT CONTACTS			
PRIMARY CONTACT	TITLE	EMAIL	PHONE NUMBER
Lorenzo Jones	Chief Executive Officer	lojo511@royalsec.com	212-456-4455
Julia Gonzalez	Chief Tech. Officer	jugo401@royalsec.com	212-456-4490

LOCATION INFORMATION

Royal Security Services
73 Canal Street
New York, NY 10010
212.456.7890

Url: **https://pentest-ground.com:81/**
Server: 172.16.69.2
Address: 172.16.69.2
NetRange: 172.16.0.0 - 172.31.255.255
CIDR: 172.16.0.0/12
Nameserver: ns1.linode.com
Host Company: Linode - London
IPV4 Address: 178.79.134.182 IPV6: **not found!**
Domain Registrar: **not found!**

ASSESSOR CONTACTS			
ASSESSOR CONTACT	TITLE	EMAIL	PHONE NUMBER
Pablo V.	Security Consultant	pablofvergara@msn.com	631-202-2929

EXECUTIVE SUMMARY

Royal Security Services contracted **SevereQA** with performing a **Penetration Test/Security Assessment** of their information systems to identify security weaknesses, and determine their impact to **Royal Security Services**. The purpose of this assessment is to verify the effectiveness of the security controls put in place by **Royal Security Services** to secure business-critical information.

These systems have been identified as **business-critical** and, if compromised, could cause material harm to **Royal Security Services**.

For more insights on reporting, visit: <http://www.pentest-standard.org/index.php/Reporting>

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

CONCLUSION

Having evaluated said findings, with a high degree of confidence, SevereQA has determined the overall risk to be in the range of **High**.

Concerning finds include **User Harvesting Flaw** at login and an XSS at the blog section's editor. The lack of MFA and CAPTCHA leave the application exposed to a wide range of attacks, ranging from brute-force attacks to phishing, even ransomware.

In a similar manner, the lack of weak password enforcement presents an opportunity for a **Password Spray** attack.

Another discovery of great concern was an **Indirect Object Reference (IDOR)** issue at login, where the cookie persisted long after the tester logged out, allowing access to the dashboard to persist when navigating back to the previous page from the current one.

There were other features of the application that were not functional and could not be tested.

Please see the **post exploitation** section for details and recommendations on next steps.

SCOPE

The scope of this assessment, as provided was **<https://pentest-ground.com:81/>**. With the following features under test

FEATURES UNDER TEST			
FEATURE #	FEATURE NAME	DESCRIPTION	PRIORITY
1	Home Page	Basic Landing; Potential for site defacement	MEDIUM
2	About Us	Description of company; culture; values	MEDIUM
3	Services	Types of services offered; low threat vector	Low
4	Blog	Static content pulled in from DB	MEDIUM
5	Contact Us	Form - submit comment	MEDIUM-HIGH
6	Login	Form - authentication for return customers	HIGH
7	Search	Input - search for services	MEDIUM-HIGH
8	Register	Form - sign up as a customer of RSS	MEDIUM
9	Newsletter	Input - sign up to receive RSS newsletter	MEDIUM-HIGH

Urls in scope:

- Home - <https://pentest-ground.com:81/>
- About Us - <https://pentest-ground.com:81/about>
- Services - <https://pentest-ground.com:81/services>
- Blog - <https://pentest-ground.com:81/blog>
 - <https://pentest-ground.com:81/create>
 - <https://pentest-ground.com:81/1/edit>
 - <https://pentest-ground.com:81/2/edit>
- Contact Us - <https://pentest-ground.com:81/contact>
- Login - <https://pentest-ground.com:81/login>
- Search - <https://pentest-ground.com:81/search>
- Clients - <https://pentest-ground.com:81/clients>
- <https://pentest-ground.com:81/console>

APPROACH

SevereQA performed testing under a “black box” approach from **05/09/2024** to **06/20/2024** without credentials or any advance knowledge of **Royal Security Services** internally facing environment with the goal of identifying unknown weaknesses.

In an effort to test **Royal Security Services**’ ability to defend against direct and indirect attack, the Security Analyst executed a comprehensive suite of tests employing the open web application security (OWASP) top-10, PTES, and NIST frameworks. These tests include, but were not limited to, web application scans, exploitation of weakened services and vulnerability conformation.

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, **Royal Security Services** allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

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 Thursday **May 9**, 2024
- b. Time limit: **Open**

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 be 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 **Julia Gonzalez, CTO**, employed at **Royal Security Services** do hereby grant Pablo Vergara, Security Analyst, employee of **SevereQA** full permission to perform the following **Penetration Test** on 05/09/24 - 06/20/24, 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 Royal Security Services has with {consultancy}, and may be subject to legal action.**

ASSESSMENT RESULTS

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. Financial Impact Rating - \$\$\$\$	0 - 3d	0
High (7 - 9)	High risk of compromise and/or loss of business reputation Financial Impact Rating - \$\$\$	3 - 5d	8
Medium (4 - 6)	Moderate risk of compromise Financial Impact Rating - \$\$	1w - 2w	3
Low (1 - 3)	Low Risk / Minimal impact Financial Impact Rating - \$	2w	12
Informational	Negligible risk, but worth noting in the likelihood that attacks could be chained together	+2w	13

ASSESSMENT SUMMARY

CRITICALS

After extensive testing, including vulnerability scans, as well as manual and automation testing, Tester found no **Criticals**.

HIGHS

The list of **High** vulnerabilities include the following:

- User Harvesting Flaw at login
- No login required to update a blog post
- IDOR at ./dashboard
- Missing CAPTCHA / MFA implementation
- Embedded XSS at phone number input
- No CSP
- Weak password enforcement

Why this matters

The lack of MFA and/or CAPTCHA exposes the application to User Harvesting, Password spraying, and so on. Weak password enforcement is also concerning. Without hardening the authentication workflow, the application is vulnerable to a myriad of attacks, most pernicious of which is ransomware. At the blog section, the lack of an authentication mechanism when editing a blog post is problematic.

Remediation for these finds must occur immediately.

MEDIUMS

The list of **Medium** vulnerabilities include no HSTS header in the response. Tester discovered the application is susceptible to clickjacking. It was also discovered that the OPTIONS method for API calls is not disabled.

Why this matters

Taken individually, the finds were not harmful to the application. However, these finds have the potential for worse if they were combined with other payloads. Remediation for these finds must be taken into consideration.

TECHNICAL SUMMARY

SevereQA began all testing activities from the perspective of an unauthenticated user on the internal network. Royal Security Services did not provide Tester any additional information (ie, operating system or configuration info.).

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

Information Gathering

During the recon/information gathering phase, Tester engaged with the application as any other user of the site, understanding the different features and workflows. 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 Burp Suite.

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

Information Gathering

Passive Intelligence

Results: Nothing substantial.

Active Intelligence

Results: Inconclusive; could not obtain accurate results based on the url provided.

Corporate Intelligence

Results: Out of scope.

Personnel Intelligence

Results: Out of scope.

Vulnerability Assessment

In this section, a definition of the methods used to identify the vulnerability as well as the evidence/classification of the vulnerability should be present. In addition this section should include:

- Summary of results w. Nessus - The target "network" was not scanned because IP address resolution failed.
- Summary of results w. Zed Attack Proxy (ZAP)

Mediums

- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration
- Sub Resource Integrity Attribute Missing
- Vulnerable JS Library

Low

- Cookie - No HTTPOnly Flag
- Cookie without Security Flag
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion
- Dangerous JS Functions
- Missing Anti-Clickjacking Header
- Permissions Policy Header Not Set
- Secure Pages Include Mixed Content
- Server Leaks Version Info. via "Server" HTTP Response Header Field
- Strict-Transport-Security Header Not Set
- X-Content-Type-Options Header Missing

DETAILED WALKTHROUGH / POST EXPLOITATION

ISSUE: LOGIN	RISK/EXPOSURE SCORE	CVSS SCORE
USER HARVESTING FLAW	9	6.2

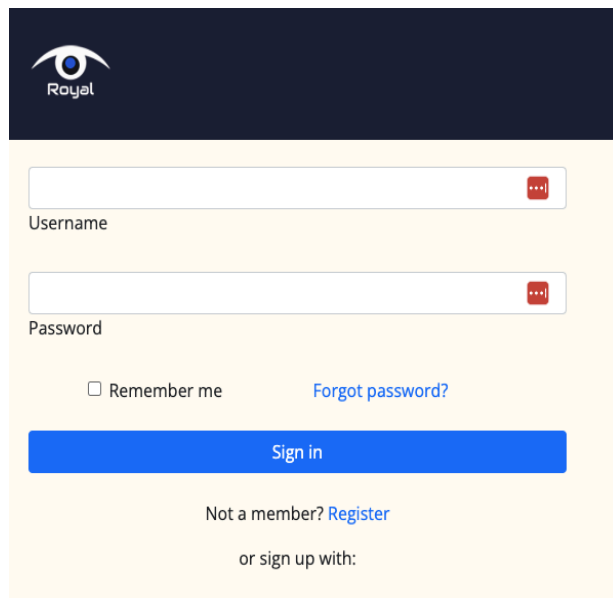
Exploit Target in Scope

- <https://pentest-ground.com:81/login>

OWASP Top-10 Exploit type

- [API-2:2023 Broken Authentication \(API\)](#)

Screenshot



The screenshot shows a login page for a service named 'Royal'. The page has a dark blue header with the 'Royal' logo. Below the header is a light yellow background containing the login form. The form includes a 'Username' field, a 'Password' field, a 'Remember me' checkbox, a 'Forgot password?' link, a blue 'Sign in' button, and a 'Not a member? Register' link. At the bottom, it says 'or sign up with:'.

Steps to reproduce

1. Launch site and attempt to login with any username & password

Outcome

- Able to log in with any credential (incl. admin/qwerty)

Remediation

- <https://portswigger.net/blog/preventing-username-enumeration>

Remediation Schedule (required)

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

ISSUE: LOGIN

No MFA APPLIED

RISK/EXPOSURE SCORE

8

CVSS SCORE

7

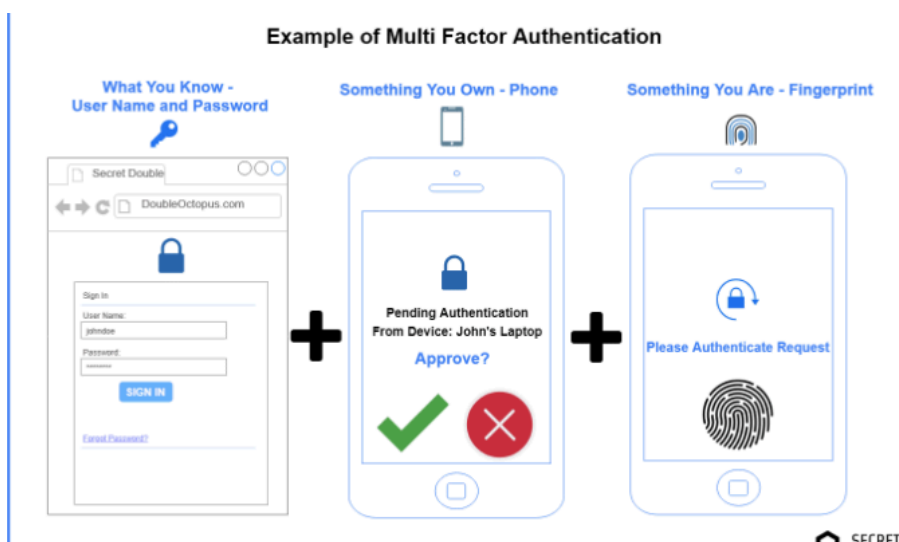
Exploit Target in Scope

- <https://pentest-ground.com:81/login>

OWASP Top-10 Exploit type

- [A07:2021 – Identification and Authentication Failures](#)

Screenshot



Steps to reproduce

1. Launch site and log in with any valid credential

Outcome

Attacks Successful

- No MFA encountered during login (registration / forgot password - not tested: link broken)

Remediation

- Employ MFA - <https://cloud.google.com/identity-platform/docs/web/mfa>

Remediation Schedule (required)

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

ISSUE: **ADMIN DASHBOARD**
SESSION PERSISTS AFTER LOGOUT

RISK/EXPOSURE SCORE
9

CVSS SCORE
5.0

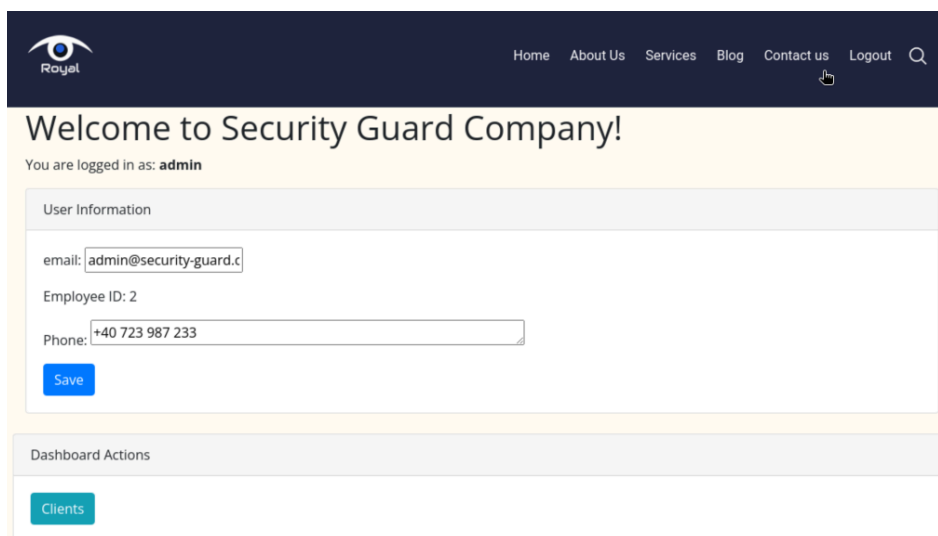
Exploit Target in Scope

- <https://pentest-ground.com:81/clients>

OWASP Top-10 Exploit type

- [Session Management Vulnerability](#) (possible IDOR)

Screenshot



Prerequisite

None

Steps to reproduce

1. Launch site and log in
2. Navigate to Dashboard
3. Log out
4. Click back

Outcome

Attacks Successful

- User is able to get re-authenticated even when the log out session was supposedly terminated

Remediation

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Remediation Schedule (required)

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

ISSUE: **DASHBOARD**
XSS IN SOURCE CODE

RISK/EXPOSURE SCORE
5

CVSS SCORE
4.6

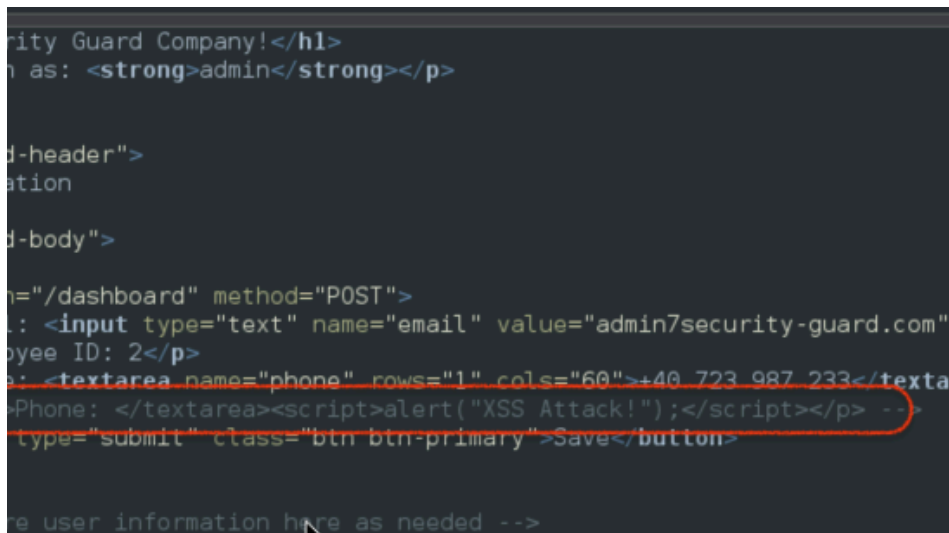
Exploit Target in Scope

- Admin Dashboard - https://pentest-ground.com:81/dashboard

OWASP Top-10 Exploit type

- Source code inspection (XSS in comments)

Screenshot



The screenshot displays a snippet of HTML source code. A red circle highlights a line containing an XSS payload: `<script>alert('XSS Attack!');</script>`. The payload is embedded within a `<textarea>` element, which is part of a form for updating user information. The code also shows an email input field and a 'Save' button.

Prerequisite

Admin is logged in

Steps to reproduce

1. Inspect the source code at phone number input

Outcome

Anomaly Discovered

- Phone input has an embedded XSS script which could be utilized for malicious purposes if uncommented

Remediation

- Removal of this bit of code should suffice

Remediation Schedule (required)

- Within .5 Business Days - a quick win!

ISSUE: **GENERAL**

No CSP HEADERS FOUND

RISK/EXPOSURE SCORE

5

CVSS SCORE

5.3

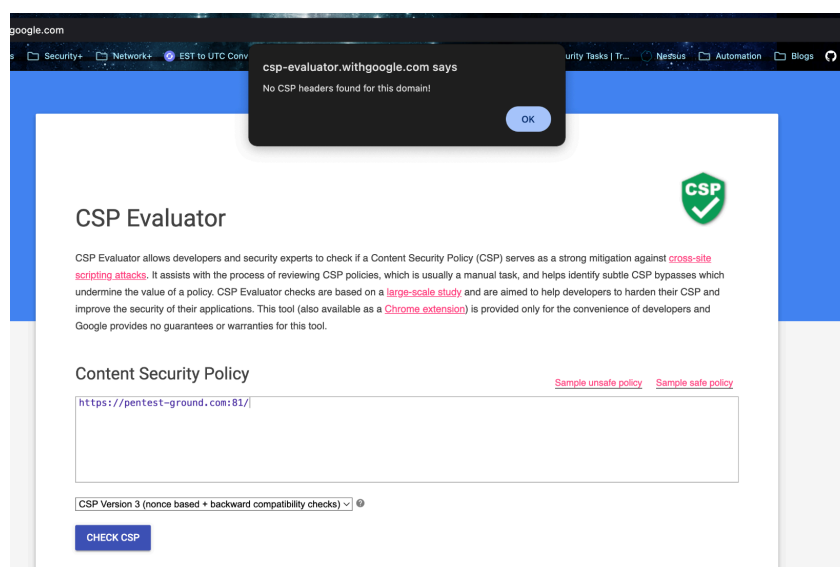
Exploit Target in Scope

- <https://pentest-ground.com:81>

OWASP Top-10 Exploit type

- Client-side testing for Content Security Policy Header

Screenshot



Prerequisite

Use: <https://csp-evaluator.withgoogle.com/>

Steps to reproduce

1. Open evaluator, paste the target url, and submit

Outcome

Issue Discovered

- The lack of CSP exposes the application to XSS (Cross-Site Scripting), clickjacking, and cross-site leak vulnerabilities (*issues that were discovered later on during testing*)

Remediation

- Visit [Defense in Depth](#) for explicit guidance on how to fix these issues, which resolves the others as well

Remediation Schedule (required)

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

ISSUE: **BLOG - EDIT**

RISK/EXPOSURE SCORE

CVSS SCORE

XSS INJECTION VULNERABILITY

8

7.5

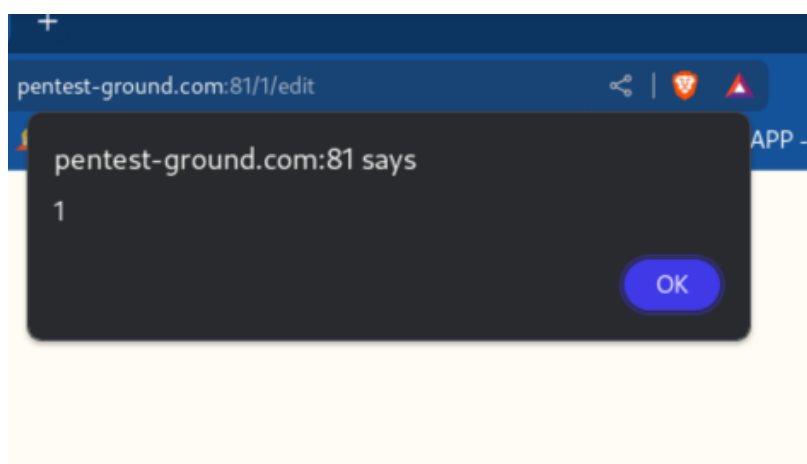
Exploit Target in Scope

- Blog Form Update - <https://pentest-ground.com:81/1/edit>

OWASP Top-10 Exploit type

- [WSTG-INPV-01 - Testing for Reflected Cross Site Scripting](#)

Screenshot



Prerequisite

None. Users not needing to be logged in is problematic in itself and should be addressed!

Steps to reproduce

1. Copy and paste link into the browser - notice no login is required to make edits to a blog post
2. In the title input field, enter `<script>alert (document.cookie)</script>`
3. Submit the form

Outcome

Vulnerability Discovered

- XSS script executed successfully

Remediation

- Removal of this bit of code should suffice

Remediation Schedule (required)

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

ISSUE: **BLOG - EDIT**

RISK/EXPOSURE SCORE

CVSS SCORE

ABLE TO CREATE/UPDATE W/O

8

8.1

LOGIN

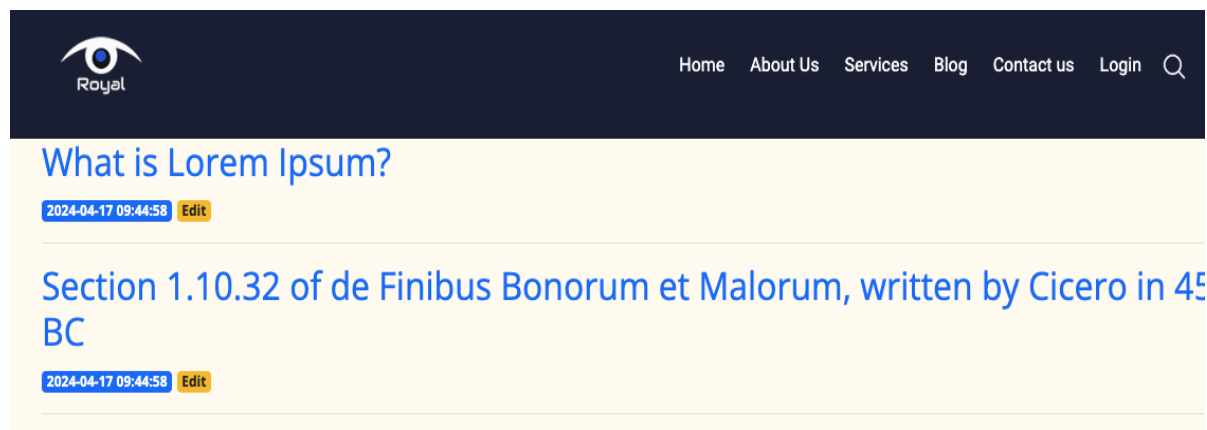
Exploit Target in Scope

- Blog Form Update - <https://pentest-ground.com:81/1/edit>

OWASP Top-10 Exploit type

- Input Validation

Screenshot



Steps to reproduce

1. Launch site and navigate to the **blog** section
2. Click on any of the displayed entries
3. In the browser address bar, edit the url so it reads {domain}/id/edit, where **id** is selected blog post
4. Make an update and submit

Outcome

Vulnerability Discovered

- The lack of an authentication mechanism for making updates makes this finding especially problematic as it exposes a potential attack vector, not limited to XSS injection (as stated previously)

Remediation

- Removal of this bit of code should suffice

Remediation Schedule (required)

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

REMEDIATION SUMMARY

For the issues pertaining to the **username harvesting flaw** SevereQA recommends the following:

For the **login page**, implement MFA and login attempts counter. The error messaging may require simplifying it to something generic. For example: “*Your login attempt was unsuccessful. If you continue to have trouble, contact support.*”

A host of other issues discovered during testing which indirectly impacted the successful completion of the penetration test:

1. Registration link is not working
2. Forgot Password link is non-functional
3. Newsletter - no effect when email is submitted
4. Landing page image has text on image
5. Services page unresponsive when buttons are clicked
6. <https://pentest-ground.com:81/about> - broken image on ABOUT US page
7. <https://pentest-ground.com:81/blog> - page integrity - footer not fixed to bottom of page
8. <https://pentest-ground.com:81/contact?> - Phone Number Input - no validation shown for non-numeric values
9. <https://pentest-ground.com:81/> - Search - IE-11 - UI breaks when enabling search input

TECHNICAL FINDINGS RESOURCES

CVEs, links, etc. go here

- [IDOR Cheat Sheet](#)
- [File Upload Cheat Sheet](#)
- [CSRF Cheat Sheet](#)