Agricultural Development Bank CMS Security Report

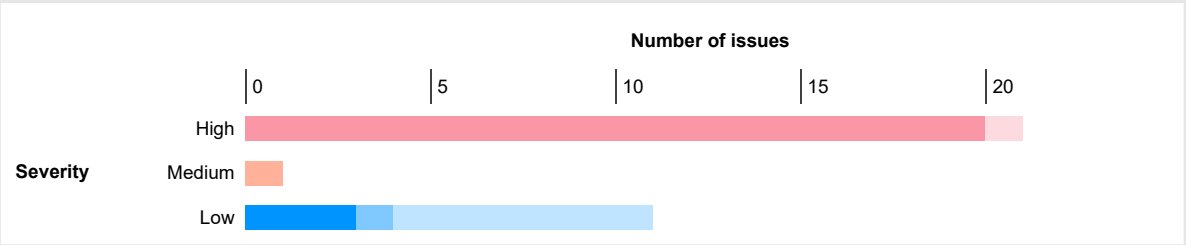
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	20	1	21
	Medium	0	1	0	1
	Low	3	1	7	11

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. High severity issues

1.1. SQL injection

There are 2 instances of this issue:

- /admin/blog-category/create [URL path filename]
- /admin/blogs/create [URL path filename]

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Remediation background

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize *every* variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

References

- Web Security Academy: SQL injection
- Using Burp to Test for Injection Flaws
- Web Security Academy: SQL Injection Cheat Sheet

Vulnerability classifications

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- CWE-116: Improper Encoding or Escaping of Output
- CAPEC-66: SQL Injection

1.1.1. https://adblbackend.peacenepal.com/admin/blog-category/create [URL path filename]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blog-category/create**

Issue detail

The URL path filename appears to be vulnerable to SQL injection attacks. The payload **'** was submitted in the URL path filename, and a database error message was returned. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be PostgreSQL.

Remediation detail

The application should handle errors gracefully and prevent SQL error messages from being returned in responses.

Request

```
GET /admin/blog-category/create' HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InFnclQ0NlRZVFBMRlRHakkwN2Q0MGc9PSIsInZhbHVlIjoia3R5d1pKNVFGYk8wd1lyM3dhUTRnYlFUUmZsdFMrSVljNHRsazEzSU00QlNEQVMvakdDUEE2RnpRWUlzeWdJbEdWMjRLa3RFZTBSb2cvd2Nld1ZnTUxXRUV5WWxEU3IxSU85YWp2VGU4V0MzZnQ1YlMrbVVvb2h4TlhqZFVVUnMiLCJtYWMiOiI0ZTM2Mjk5Njk2YTBiMjk5ODdmYjhkMjkzOWNmMDEzZmY4MzY1NDQ2NjQ3NTMwNzFjMDI3YmFjOGNmMWE4OGE2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blog-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 02 Oct 2024 12:07:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InhTZys2N1Myb3FwVDlTd1RlbDdnU1E9PSIsInZhbHVlIjoiTWdqd2I2U1cvMjVvVzYxWUIwL2tzenhqZWRaQWZWZExCQmtpbzM3d2phWStldnNJMjY4bTNqUlRrbjJUZi9UdmpmMTRxNHVVQ0N1SUVRdThVV0hoU3B1U3g1cEdJMjFzUFhnUHBUS2JHby9HcDBsY1ZxNlVrcFBYZUhpNzdjME0iLCJtYWMiOiI5NjlmNGI2MzcyOWQ3NDZhYWIyNGZmNGU0MDczZTRkN2ZmM2YxMDM2YTgzYWVhOTk4Y2Y0NjNlNzYyZDIyYjA4IiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 14:07:07 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1162892

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
BadMethodCallException: Method App\Http\Controllers\Admin\BlogCategoryController::show does not exist. in file /var/www/html/adbl-backend/vendor/lara
...[SNIP]...
"rows","running","savepoint","scope","scroll","search","second","seek","select","sensitive","session_user","set","show","similar","sin","sinh","skip","smallint","some","specific","specifictype","sql","sqlexception","sqlstate","sqlwarning","sqrt","start","static","stddev_pop","stddev_samp","submultiset","subset","substring","substring_regex","succeeds","sum","symmetric","system","system_time","system_user","tabl
...[SNIP]...
nction(e){return e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}var m=
{db2:n.default,mariadb:r.default,mysql:a.default,n1ql:o.default,plsql:i.default,postgresql:l.default,redshift:s.default,spark:c.default,sql:u.default,tsql:f.default};t.format=function(e){var t=arguments.length>
...[SNIP]...
```

1.1.2. https://adblbackend.peacenepal.com/admin/blogs/create [URL path filename]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blogs/create**

Issue detail

The URL path filename appears to be vulnerable to SQL injection attacks. The payload **'** was submitted in the URL path filename, and a database error message was returned. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

The database appears to be PostgreSQL.

Remediation detail

The application should handle errors gracefully and prevent SQL error messages from being returned in responses.

Request

```
GET /admin/blogs/create' HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
```

```
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkcxelpUNG5WZVlIclFmd0Jvb2UzTnc9PSIsInZhbHVlIjoicHV0cWtPYUhpYW52SVVLNlRxK0EvZ0tpSlNVMisvSnA2RDJnV0l0bEhLczZmc0J4V3JTRzhqU210N3MzZzFwaXVxQ1B3b1V0allSdmZWTUM3cHRBQ1psNnJKYjNoTXoyUVVDZTZXWHB4bHR2UXBWeEdHOHVxWFFEVjh5TzJlUlQiLCJtYWMiOiJlNWViYzc5ZTA3N2ViN2NjYTFmN2IzM2JjMjczNTIwZDZjYWY5OTdmNDE2M2NmOWQyMmM4MWI2YWQ1NmU2ZjgyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 02 Oct 2024 12:07:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImcwR0hNT1UvTHdEU2U1Z2JmTjNCTGc9PSIsInZhbHVlIjoiM1dHc3ZTUGVkclpOVU1XWTVwZHczUzB6TWprQkZuWENkMmJLL0c5Uld2b2llSkFacXhic2RrMEh3V3JGSVpVR1pZSFhyR1UwQUQrbjZRbFBSZ2pmaGNiKzMrc0JkaWlWRGl5eTZwOGp6Z0hycU1WRmdxMmtLOCtzSXhSTThDcnoiLCJtYWMiOiJjNTA1M2MxM2NhZjRjNWM5Y2E5NGNjMzE1MzhhOTMzZGQ2MjBkYTljYTZjZmMwNWI4OWM4NGJjNzYzZmUyZGEyIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:07:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1163211

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
BadMethodCallException: Method App\Http\Controllers\Admin\BlogController::show does not exist. in file /var/www/html/adbl-backend/vendor/laravel/fram
...[SNIP]...
"rows","running","savepoint","scope","scroll","search","second","seek","select","sensitive","session_user","set","show","similar","sin","sinh","skip","smallint","some","specific","specifictype","sql","sqlexception","sqlstate","sqlwarning","sqrt","start","static","stddev_pop","stddev_samp","submultiset","subset","substring","substring_regex","succeeds","sum","symmetric","system","system_time","system_user","tabl
...[SNIP]...
nction(e){return e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e})(e)}var m=
{db2:n.default,mariadb:r.default,mysql:a.default,n1ql:o.default,plsql:i.default,postgresql:l.default,redshift:s.default,spark:c.default,sql:u.default,tsql:f.default};t.format=function(e){var t=arguments.length>
...[SNIP]...
```

1.2. Client-side desync

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/admin-type**

Issue detail

The server appears to be vulnerable to client-side desync attacks. A POST request was sent to the path '/admin/admin-type' with a second request sent as the body. The server ignored the Content-Length header and did not close the connection, leading to the smuggled request being interpreted as the next request.

Issue background

Client-side desync (CSD) vulnerabilities occur when a web server fails to correctly process the Content-Length of POST requests. By exploiting this behavior, an attacker can force a victim's browser to desynchronize its connection with the website, typically leading to XSS.

Issue remediation

You can resolve this vulnerability by patching the server so that it either processes POST requests correctly, or closes the connection after handling them. You could also disable connection reuse entirely, but this may reduce performance. You can also resolve this issue by enabling HTTP/2.

References

- HTTP Request Smuggling
- Browser-Powered Desync Attacks

Vulnerability classifications

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

- CAPEC-33: HTTP Request Smuggling

Request 1

```
POST /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: keep-alive
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 325
Content-Type: application/x-www-form-urlencoded

GET /robots.txt HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
...[SNIP]...
```

Response 1

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:56:42 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/contents
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkNJTU03T0p2OU16UWlOekJCaEZWdmc9PSIsInZhbHVlIjoic2k4UUJ5VmJDQ29raVRxbmcyWEYvTFRRTDFiM3U3VDdIVDV1Wm
xMQ2E3ZUVOdmhnemV3SHhPTi9yaHRLMnovZUc5SmlXSzJiWXpXUUl2TVNlOTM1RjY1d1Znak1lamZnWWtzVkZGOXQ3SlVnMWIxbHFYeHlmSkpSTXQ5Skk1a
mUiLCJtYWMiOiIzNTcxYWY4YTIwYzRkNzQyYzJjNzYyOTI5MjI0Y2FlNGJlNTU3NDIwNDFlNzVmMTFkY2M3NWQyNTVjYzFlYWFmIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:56:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
Content-Length: 442

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/contents'" />

<title>Redirecting
...[SNIP]...
```

Request 2

```
GET /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:42 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjZFOTdEdVY5SGdNNjVzTVdxQnhUVXc9PSIsInZhbHVlIjoicUkzZzViZ3BZczlvcFQvRnJSa0p3UTNwYVFkOFdDUWVpT2lHMUZY
NE9SaE8xWGk4bmJaUnZvVEFCVUxVUGRYYlpYeHhKK2lJb3VXa1lROG1uYWxNK08rZnh2WDB2WmxGaEl6WFJrSFg3M1kyWmp6VStBWFNMWGdJV3Fib0JRS
lUiLCJtYWMiOiJmZTAyODYwYjk0MzY4YjEyMjg1OWFlNjlwMWZjMTg2YzRhZjcwZDVjNTBkMGE5NzM0OGY5MzJjNWY4ZjcwZTRlIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:56:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 73707

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

1.3. Cross-site scripting (DOM-based)

There are 18 instances of this issue:

- /admin/account-type-category/create
- /admin/account-type/create
- /admin/blogs/create
- /admin/contents/create
- /admin/interest-rates/create
- /admin/news/create
- /admin/offers/create
- /admin/popup/create
- /admin/press-release/create
- /admin/projects/create
- /admin/report-category/create
- /admin/report/create
- /admin/service-category/create
- /admin/services/create
- /admin/team/create
- /admin/training-hall/create
- /admin/training/create
- /admin/vendor-category/create

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based cross-site scripting arises when a script writes controllable data into the HTML document in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to visit the attacker's crafted URL in various ways, similar to the usual attack delivery vectors for reflected cross-site scripting vulnerabilities.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based cross-site scripting vulnerabilities is not to dynamically write data from any untrusted source into the HTML document. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing script code into the document. In many cases, the relevant data can be validated on a whitelist basis, to allow only content that is known to be safe. In other cases, it will be necessary to sanitize or encode the data. This can be a complex task, and depending on the context that the data is to be inserted may need to involve a combination of JavaScript escaping, HTML encoding, and URL encoding, in the appropriate sequence.

References

- Web Security Academy: Cross-site scripting
- Web Security Academy: DOM-based cross-site scripting

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

1.3.1. https://adblbackend.peacenepal.com/admin/account-type-category/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type-category/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/account-type-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImlNUnExR0U2cnFjR1NwaHcyZ3o1dUE9PSIsInZhbHVlIjoiT05VZ1NIY1RsakVYTHY1Ui8wdlkxQVhZYnFTelNTZ1NSMUpFRENOS
1FQeEdlbGNIalJvbm1NU0FlSFZUaEYzbkdRZVZGM3BVdVVQWUQzNFQ2QWRVM3ZXY0hza2hmcGY1QnRRclpCSjVpMXlvNUNuRmdueE5yRDVCK0FPVU15d0
EiLCJtYWMiOiI4YmQ2ZWViYjc4ZDRlZWExYTBhNWJlMjliN2I0ZjdkZTIzNzI0ZjA4NDdjZjU2ZTg1OThhOGRjNDc5ODg0MjQxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:23:01 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkhYelBmcUp1eUEvR2lIQ3k4dlkrWXc9PSIsInZhbHVlIjoibUZhWFFxMnVsTHdSdFhzdXNaU3M2MVI0WTBLcWRZTzI2Y3l1dWdQM
nFQV2JLMWpZWXlHK0tMT2hzOCt4eWdMbVNhZ2pLRG5kSVB3VWJOVGZ1SEYzRHdJTHc5cDE2MyszbkpoZDVVbjQyeDAwamVLWWhRNmx6UXZHMnc0V3lh
MkEiLCJtYWMiOiJlOTE0MDA1ODJlZjdmYTIzOGIzYTNlODAzZTIyY2M5YTJlMDdjYTcyNzM2ZjZmZmQzNjU0ODk1OWMzM2QzMDhkIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:23:01 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71557

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **excerpt[2]**.

The previous value reached the sink as:

```
hr50sni683%2527%2522`'"/hr50sni683/><hr50sni683/\>twhyqhu3bs&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/account-type-category/create:1049:30)
at Object.init (https://adblbackend.peacenepal.com/admin/account-type-category/create:1070:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/account-type-category/create:1077:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/account-type-category/create:1049:30)
at Object.init (https://adblbackend.peacenepal.com/admin/account-type-category/create:1070:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/account-type-category/create:1077:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.2. https://adblbackend.peacenepal.com/admin/account-type/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/account-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InV4OTE5WVZTdkkxR2Z4NWdlV0kya3c9PSIsInZhbHVlIjoid0Q4OTZQNXE0dGpubXBiN0xtVkdpdVFqR1NzTkJaTnlBRGpNUlVHNDFISitwbThMWGR5OFZnV050UlNSb0hmY2wxbzR3dEo3Tjk1aHFDN29Ra0tPT1JCdXEyVUxBRDVVclZhWkNYNGJWcjdDZXZoWWhGYlE3Mkx4amNrS2o0TFciLCJtYWMiOiI5MmRmZDlmNWNjMjIwODUxNGViOTQ0MmEyMDg1MjY1MDYxMWZhOTQxYTlkMDE2NDYyZGU3ZDUzNmQxZWUxYTY0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:20:34 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlhvMTlwenBOWjdQdGpTNzBtTEJBNkE9PSIsInZhbHVlIjoiNXlSQ21ieG1GSk05b2VJdnlUZWVHZEZIakdBNkFraTJlR20xWmY1eXlaSTZ1YUtQZDNDUklPTTdkN3QvM3hSbDZaZERlWFBYQ0tnZkhpSEtpdW9NQW5MRnNtajMxbXJ2NklPK0dkZ0M5ak4yOHFLbWlXbFQyN2lhemliOFlEMEwiLCJtYWMiOiI4MTY1ODQ5NTMyOGRhNDEyZGE2N2Y0MzQ5N2EzZjg3N2E2ZjdiMDNkN2ZiY2M5NmYwZDBjYzJlOTU0MDliZGExIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 13:20:34 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 82614

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **ratesFees[2]**.

The previous value reached the sink as:

```
pz67o1lasu%2527%2522`'"/pz67o1lasu/><pz67o1lasu/\>qs9q6fnpnr&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/account-type/create:1211:30)
at Object.init (https://adblbackend.peacenepal.com/admin/account-type/create:1232:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/account-type/create:1239:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
```

```
at demos (https://adblbackend.peacenepal.com/admin/account-type/create:1211:30)
at Object.init (https://adblbackend.peacenepal.com/admin/account-type/create:1232:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/account-type/create:1239:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.3. https://adblbackend.peacenepal.com/admin/blogs/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blogs/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/blogs/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkcxelpUNG5WZVlIclFmd0Jvb2UzTnc9PSIsInZhbHVlIjoicHV0cWtPYUhpYW52SVVLNlRxK0EvZ0tpSlNVMisvSnA2RDJnV0l0bEhLc
zZmc0J4V3JTRzhqU210N3MzZzFwaXVxQ1B3b1V0allSdmZWTUM3cHRBQ1psNnJKYjNoTXoyUVVDZTZXWHB4bHR2UXBWeEdHOHVxWFFEVjh5TzJlUlQiLCJt
YWMiOiJlNWViYzc5ZTA3N2ViN2NjYTFmN2IzM2JjMjczNTIwZDZjYWY5OTdmNDE2M2NmOWQyMmM4MWI2YWQ1NmU2ZjgyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:07:47 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImR6eGlRMXZxTW5iUXpNNndWRUE1MlE9PSIsInZhbHVlIjoicU9YblY1VFdzRVJLU3MyTitwelcyanRKS1NmQ3ZNTGJxOEVpd203
OHBidVA5bzFRbXZuNE8rU1Myc0xUYVB5VjJpY0YybnplQitZdGxBZWR0VXg3VFZnK1BnTFhYT0l4Z01iRWFaOS81TnBPOW9jaVZXZ2hONllGdGZDOUVNL0UiLC
JtYWMiOiJmOWUzMTU1NDMzNjgwYzNkNTQ3NWZlYzgxNzM4MmJmMzg3MTM0YTM0ZjhmZDVlMGRlZWNlOTBmOTIzZjQ4NjU0liwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:07:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71863

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **description[2]**.

The previous value reached the sink as:

```
kjrz11oon0%2527%2522`'"/kjrz11oon0/><kjrz11oon0/\>n32ub8vqka&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/blogs/create:1022:30)
at Object.init (https://adblbackend.peacenepal.com/admin/blogs/create:1043:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/blogs/create:1050:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/blogs/create:1022:30)
at Object.init (https://adblbackend.peacenepal.com/admin/blogs/create:1043:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/blogs/create:1050:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.4. https://adblbackend.peacenepal.com/admin/contents/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/contents/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkJvSVIwN3Y5YVJVRTdnNXlKSk1DTHc9PSIsInZhbHVlIjoiQmI0VFVhZFNXd1BHN1IlcGlEenNCbld2b2VETW5Zb255OTNzKytmakl
zWEg5TlhtQmVVNlg2elNQMmdQenNqQ015QmZRaG1ZTlB0eFQwYzROZ1B6NnluSkdhdXlsa0VKT0RUQTF3OHQ4ZTVGS0VBRHd6a2pJVmdxTlZDQ2dsVTQiLC
JtYWMiOiI1YzNiZTM3ZDc5Mzg4MDVlNGMyNTFhYjA5ZTc0ZjA4MzRlNjkyMTgwYjc1YzEyMDdmNzQwNTM3NzRhMGEyNTQ3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:14:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjNlREdlbW5Yc0pUdW05SFdwS3VIbXc9PSIsInZhbHVlIjoiejRQQ1hvdW5adkt1TXpCYVlqZ1U4WmZYUEdyeXJHRTFwaXczMCtVY
VlmdU9KdUZ0M0dZWlZZclFlZFVodzlBT1VQcnJ1cTl0TzdEUGJEckVKZkxwd0RtalZLdEJFQ3NHSG9sZTFlblZ6ZnRjVURKZHhvYzJ3UkdwdFY2Mm5uWloiLCJtYW
MiOiJjYmE5NWI1OTQ1NTU1MmRhZTFlZDIzMGVhMDI4MDJhYmI3NGU3YjYxY2Y5ZWZkMWU4ZDI0ZDVlOTc3NTk2MTdkIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 13:14:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 76351

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **multiData[2][description]**.

The previous value reached the sink as:

```
dd6klngbgx%2527%2522`'"/dd6klngbgx/><dd6klngbgx/\>ev9gte1ty5&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/contents/create:1101:30)
at Object.init (https://adblbackend.peacenepal.com/admin/contents/create:1122:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/contents/create:1129:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/contents/create:1101:30)
at Object.init (https://adblbackend.peacenepal.com/admin/contents/create:1122:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/contents/create:1129:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.5. https://adblbackend.peacenepal.com/admin/interest-rates/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/interest-rates/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/interest-rates/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkxQcnlzeWVpZXpJdTduUERNejNNMnc9PSIsInZhbHVlIjoiVUhxWFY5anBaMlNMMi80R2FGaFpFazNxUUpuait3ZTY0TzB0RnowbE5LbzRCRSt6ZWlUNXVFY0RKSVgyV1ZqYUVMQnFkSXJhajJ3T2lkdzlDdnRMaVlpMkV0N2tXQUUra1M5YW12K1FBM2d5ZXBOb3Y4bVhqUGJ1cUJQTzlFMDUiLCJtYWMiOiJiYmU2Y2M0YWRlNDVjNzRmN2JmMDE1ODdmMGJkNGZkMjA1ZjlmODFlZjUxMjIzOTZiYmYzMWE5Mzc2OGQ4ZDl4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/interest-rates
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:06:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkVaVDN6Ny9PaFhKMkl5dDNaSDBNV2c9PSIsInZhbHVlIjoiK3hZWTJ3SWYxbkVjR1BueFkrdUVlZTZpNGdabEZCbm9uS25VaGNXdVNBcnZBdFdCOEp2aU1uUFFkcGt0UWozaGx3cEpoaGJIalR3MTNvcHE3SGk1OTFQTDlJcDJuNXpvTTFLSDl4cnV0RTMvVTNZOFdMV2FVaHlpc0drR1kza0UiLCJtYWMiOiI3YmVmZGY3NzZmNmUwYmE0NDFlMTI1ZGUwMDg1NDM0Nzc3ZjAzZTRkZDdlNTZlMGFmZmRkZjcxYjVjMzJiMWYxIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:06:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 67963

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **content[2]**.

The previous value reached the sink as:

```
fqbjfizvs2%2527%2522`'"/fqbjfizvs2/><fqbjfizvs2/\>dsnt223des&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
```

```
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/interest-rates/create:982:30)
at Object.init (https://adblbackend.peacenepal.com/admin/interest-rates/create:1003:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/interest-rates/create:1010:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/interest-rates/create:982:30)
at Object.init (https://adblbackend.peacenepal.com/admin/interest-rates/create:1003:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/interest-rates/create:1010:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.6. https://adblbackend.peacenepal.com/admin/news/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/news/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/news/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhlMHZQWThLOFZYdnZQS2h5Z3NvL2c9PSIsInZhbHVlIjoielhsNW0vMC9SSFByYTdSZExGeTV1Q3I0ejI1blVKSmRJMVhPR2FS
TU5CNThzSFNNdVkvN3pDRENibjNJZVA0Rzh3b0x6R0d3ZU9yeVVTSUVXWnlEOWR2ZElWSERPY2EwY28vT0tlL1J2UmdrWnVKQ0dPOFo1Y01GQlRoelhROXliL
CJtYWMiOiI1MWIxN2UzYzk5MWMwYTI0Mjk0Mjc4ZWNmNzU5ZGMzYjU1MTI3ODg2ZGJlYzUzMmMzZTY2YjU5NTE4ZjdjYmFhliwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/news/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:37:51 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
```

```
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZ2NXkwZ2tiMVIld01SOFNKRW5qdWc9PSIsInZhbHVlIjoid3pjb1haSm9sazVuOEN1TnVNMjRHYkx0MjBUaHgvUjBGM29NdldIcXh
LU3BSWU5ZaEl5ZDBjVFkvblE2VUEvZ1RDUzFWMG5qSGxiQkU2MGNEYXhSYzg0RXdWdll2RGxkUnByc1ZyTUh2U0pFeTAzWVJSTUhPTjBYcWF6ZTlMdTEiLCJ
tYWMiOiIzZmM2NjAzZWI2ZTEzZDM1ZmNjNTgzZjU1YjVmOGRiNmJiYWRjNTdmM2VkYmVlYTNjMGNjYjUwMTMwYTMzYWQ5IiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:37:51 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 75453

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
ztjyw4vh70%2527%2522`'"/ztjyw4vh70/><ztjyw4vh70/\>jgvfwwbuyz&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/news/create:1105:30)
at Object.init (https://adblbackend.peacenepal.com/admin/news/create:1126:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/news/create:1133:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/news/create:1105:30)
at Object.init (https://adblbackend.peacenepal.com/admin/news/create:1126:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/news/create:1133:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.7. https://adblbackend.peacenepal.com/admin/offers/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/offers/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/offers/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVrdmhzcnFzSTRkQ1cvVksyTjNMY0E9PSIsInZhbHVlIjoiUjcwOVJqZytna0VYSmphQTE3NlFLN25xZlAxaWRUTzdkMHNuRjRpRkVqMlFTTWRZY1lVVURUTTBqOVQ4UEhnYWpBRnhsTlRXbUFtb09RRDJucXVNdVk3MG9oSHQrS0E4cVE1bDdRRzZMZWw3eCsyb0ZvcU0yTEN5T0lBM0dPMnkiLCJtYWMiOiJmOTczNTY3MTBjMDE1ZjRiNGI1MjBjODE3Yjc3Mjg3ZDI0MDU1OTNkZmY2NjhkMzRkNmFiZDQ2ZmVjODE4MGJkIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/offers/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:17:22 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImtVSEErYjB2UTRRQTRuS2VuZUkxU2c9PSIsInZhbHVlIjoiQVkySHNYTkFBTm9VNTFEcFFpYUg4WEhzSkR3NmtOeU83V0hhaURPWGt6bkRqSk55c0ZpQ2VQY2RGeEY0Tk1aYnJMbTJUb05oQ3RJaFpiRWNOYkdiNlJwUmtZUldGOTRBNS9DQzVzWkpGdjBNZXVOcWNVZ1FVdVhMeGM2UHI1TmUiLCJtYWMiOiJiMWI2NDVkNWY0ZWM3MjY2NmI2NWY0YTBjMTc4ZjYxOWI5MjJjOTdhMjk1YTQyZDQ1NjA5YjExYmUzY2E2MmFkIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:17:22 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 73608

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
htwzz80amq%2527%2522`'"/htwzz80amq/><htwzz80amq/\>krbprkc999&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
```

```
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/offers/create:1072:30)
at Object.init (https://adblbackend.peacenepal.com/admin/offers/create:1093:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/offers/create:1100:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/offers/create:1072:30)
at Object.init (https://adblbackend.peacenepal.com/admin/offers/create:1093:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/offers/create:1100:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.8. https://adblbackend.peacenepal.com/admin/popup/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/popup/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/popup/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjlzS0FXUG8ydmJQdVhWOEFDT2lMN3c9PSIsInZhbHVlIjoiMktiYkJzV2EyNS9aTVFvS1p2MzUrNlpOa0tNZUJhV3BBZUFTYUI4SjFpYkl6T0ozM1U5TjVQU3RGcGMxZHlTS1hJaklsazdUMHd3OG45SDZTSWtISGg0VjM1ZWJXNldNTkhkMWl1d0M3QmZEN2Z3dmtNbm8xRFF4UU82eG9QSmsiLCJtYWMiOiI4Zjc2MDhjM2Q1M2U3OTI5YjJlMmZhYzEwMmY2YzZhMDU1OGZiNjFlZWQ3NzkzMDk0NjIzMzc4NmVlOWQzYmM5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/popup/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:19:20 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
```

```
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZSU1ZsT1dEcTFnQ3lLZ0ZrK1duNWc9PSIsInZhbHVlIjoiSEFOamZQdHN2UDBpWFo1NHAyR2tuVUlsSEJWTnJHT2dwMTFwVW
9lY3FEcUkzSDk1TU85ZS9uQ1hlVUxpb250QVpuYkxXTUZHdDdya0ZRWCtkdjJySlIybloxQmllamJBQ1hrWnVhMFU3a2EzUzM2ZnZlUGhjK3ZxM3ZsY3F5eHYiLCJt
YWMiOiJhMjg0OTU2ZmRiZTk2ZDU4ODRhNzIyMmIxMmE2OWFiZWVhNzQ3MDI1NTkwYjE2YWRmNjc5ZjQyYTk4ZjMxOGViIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:19:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70407

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **description**.

The previous value reached the sink as:

```
vvm6qf8qsf%2527%2522`'"/vvm6qf8qsf/><vvm6qf8qsf/\>ludiwwx5p2&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/popup/create:1043:30)
at Object.init (https://adblbackend.peacenepal.com/admin/popup/create:1064:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/popup/create:1071:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/popup/create:1043:30)
at Object.init (https://adblbackend.peacenepal.com/admin/popup/create:1064:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/popup/create:1071:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.9. https://adblbackend.peacenepal.com/admin/press-release/create

Summary

Severity: **High**

Confidence: **Firm**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/press-release/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1


```
GET /admin/press-release/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImdwRkhaeXVxT05uRGRjeHZ3cDVqNWc9PSIsInZhbHVlIjoib09sVFdseWR2WnEwT1Bxb0R1L2RsWnVPQnl1M0dSMkl3UVY0ZT
VaaFFNRmJGalVzSzJYNFJRTFlYQno5KzZOOVpzYmV3cS9VeUlyZEh3anFpeEdpdFBPb2JYamFZb3hhVzB1NnV2RFJzQzBkWWxEeDF2NmtyR0s4SUZrYW9INlci
LCJtYWMiOiJiYTMwNzZkNWFlYzNmYTNiYjRhMmFhNzMxOTBmOTZmOTdlOTNlOGMyMWYyOGNlYTgwZjY0Zjk3OTFkNmRiYWMxliwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/press-release/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


Response 1


```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:41:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Imo0ZmQ5RUdwTDR3dThFZ0pTc1NDVWc9PSIsInZhbHVlIjoiMUs4Q0xYdXBSWjdPYmlCQUdiclJTcVZFaWtwSFpCZ0N3OElvVTI
Ud1JMOFp5cmVHZVVVWHJDSW1NZTZ5NXlGdjVUN2RzVHVSTXhBM3ovZGp2TDVjWlVKU0k3SFNYaUZlUHFGV0FncVFoWjRnazBVTC9ydEV2MFdWWFcyRDl
VTlEiLCJtYWMiOiI1MWQ1YjIxMjg2Yjg3NWE0OGQ0NjE2NDk2YmJlOTFhMjc0MjhlM2ZkY2IxNjlmODMyYmEwZjc1ZDExOGUzNzE5liwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:41:19 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 72289

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```


Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **description[2]**.

The previous value reached the sink as:

```
yq2a5k8nuh%2527%2522`'"/yq2a5k8nuh/><yq2a5k8nuh/\>mai16imwok&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
```

```
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/press-release/create:1052:30)
at Object.init (https://adblbackend.peacenepal.com/admin/press-release/create:1073:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/press-release/create:1080:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/press-release/create:1052:30)
at Object.init (https://adblbackend.peacenepal.com/admin/press-release/create:1073:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/press-release/create:1080:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.10. https://adblbackend.peacenepal.com/admin/projects/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/projects/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/projects/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjY4NmxCWGRrUmV0Sjk4NHJsdnlicUE9PSIsInZhbHVlIjoiaUJqNE9LbTl0aFhMaGROem1yWnp6ZThCZXhiVnpwWVplaEE1NmNCejMwcjY0SGllRGhSVzVtRllFbENUVkhYc0IMUjhOd0EySDBFZzJPSWQvVVJUTFEzZDVvUnV1TWFtM3BKWlUxeHhKQ3JsQ2ZVNWd1VEJFUjBSM0M0MkdMaTciLCJtYWMiOiIxZDNlMWJiZGQ3YWE4MzQzY2RhZTNhNmM1YjYzMWY1MjQ4ZjQ4YTM1ZTVlNzYwMjNhNjM3ZmY4ZTFmOWE5Yzc5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/projects/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:39:23 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjBLbmZFSUNJY1lEL21YVkNsZnNlclE9PSIsInZhbHVlIjoiZHJuM0NVVlBvUkNwVWl2K2kvOEVhSzNuem9aQjN6YSt3bjJSZFJMZnRBdzliSHdOQVBBK2NzQkFEZHoxWndEb0hISCtIUE9HRmV5VmtYVVZCQXdJSVZGL1lFTGFTcDJCVXhOckd2aXo1SE1YK3M5OGl3SkVPam5zTEV4Sy94bmQiLCJtYWMiOiI1YjI5MzA4ODNkN2Q3OTZmODA4YTMxMjJiMzQ3Yjk5OWRkNTY0ZDk0MDNhMGJkZWE0YmJhOGZhYTFkYWIyMzU3IiwidGFnIjoiIn0%3D;
```

```
expires=Wed, 02 Oct 2024 13:39:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 74122

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
t1syfkauez%2527%2522`'"/t1syfkauez/><t1syfkauez/\>xug3ggy7d0&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/projects/create:1088:30)
at Object.init (https://adblbackend.peacenepal.com/admin/projects/create:1109:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/projects/create:1116:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/projects/create:1088:30)
at Object.init (https://adblbackend.peacenepal.com/admin/projects/create:1109:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/projects/create:1116:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.11. https://adblbackend.peacenepal.com/admin/report-category/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report-category/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/report-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IllzRjBRQ2JrTTJqNG9BZHhIRG13TGc9PSIsInZhbHVlIjoiR0ZZQ2hZUlRsejVPMWZxRTMvUm5RRGNRRVJJdzFWK0JsdGFyL3RvLzJjdjVlZWs2eWd4SEF5MUlWQzdNNFRSa3hIbWx5aEZSUTAzMWJMaG1jdFVHZDRkRFpVSjMxNENGT0hmQ2hOYlcvVVFLTkVNZmpCL2dtTTFvbkdoS1VsUDUiLCJtYWMiOiI3ZTgzNzEzYTU1OGNhMDU1MTg2MzRjOWU5MmIxZjYzNDM5NDU3MzM4MGI4NzFlMmRiMjE1NTdiMDkxNzYzZDBmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:36:40 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImZmdVZMOVR0NDMxRUNGc1gzbDhUU1E9PSIsInZhbHVlIjoiYnR5V1JBR0xQVWhnK3Jrb2RER0d1QlVBVTQvcEtGKzNtNlZhdzZYN21MV0prekRrNjJQOFNVV2pxMnpvb3EvU2NUZFRtSVFNNUQ4Snp2am81K0FrTWxPTVdPbzc2ODcrNGtxc0x2ZFZKL1dIdzlaTTJtSVZBVlFJVG1aYVl6UE4iLCJtYWMiOiJkZDcwNjE3NDA5YmRiOTMyN2FlOTk1YmVlZThmNGVjYzY5YjcyYjNmYjZlZmFiMTc1ZTBkYzBhMjcxY2JjNDcyIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 13:36:40 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70640

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **excerpt[2]**.

The previous value reached the sink as:

```
qny4896jnu%2527%2522`'"/qny4896jnu/><qny4896jnu/\>orb7fpwccz&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/report-category/create:1032:30)
at Object.init (https://adblbackend.peacenepal.com/admin/report-category/create:1053:21)
```

```
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/report-category/create:1060:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/report-category/create:1032:30)
at Object.init (https://adblbackend.peacenepal.com/admin/report-category/create:1053:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/report-category/create:1060:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.12. https://adblbackend.peacenepal.com/admin/report/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/report/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlRGdEdJVXhYV3dqbHJqOVRLblNObWc9PSIsInZhbHVlIjoiVURvNTBLT0FNb2IwdVRydk1aUFVyK21yTW5PRXRMcmRCM21qb3d
jVGlZNDc3K3I0YVVNUW1SMW1KV01QZm9DdWNwWVRuZWNjQzNjQ0FMcVZ5Z3ZXNzBzZjBva05NdUxmcElkYUlaWVlzMFBKeVVUbFBKSTMvMnhNL1NiNTU4
bDYiLCJtYWMiOiJlMmI4OTFiYmVjYjg1OTI5ZjAwNDVjZWNmOWE0OTdhODMzZWMyNWQwODhlOTg0MjE5MTlmMjk3NmM0NDJhNjNmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:05:03 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IldIMnFUVWt4c3k5Tmt4UWkxa0xya3c9PSIsInZhbHVlIjoiU3F5NFAvcTlTRkxJb0U5YkRxK1l1b2VRVlZPb05QWEduVUVjN3FVVnEz
SnAzV2FxbHhnVnZNOE5UUHZGa1BlNzQrWjNiSGlIMEYxVkNMRmlxd3ZuclpiSGgyTDFZQUlXOTc3bUxpcG9PWUVlZ2w4QUNPQ1hhYk5ad2tVQ1NFKzMiLCJtYW
MiOiJiMjcxNjg5NTc5YWJlYzliZDZiMGM3M2ZlNWRiNjk5MTQ0NmNjMzYwZjg2NjQ4NzY1ZWJmNjk5ZmM5ZjViZDIyIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024
13:05:03 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 76260

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
peo5ktvpre%2527%2522`'"/peo5ktvpre/><peo5ktvpre/\>aryx3fqwj8&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/report/create:1096:30)
at Object.init (https://adblbackend.peacenepal.com/admin/report/create:1117:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/report/create:1124:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/report/create:1096:30)
at Object.init (https://adblbackend.peacenepal.com/admin/report/create:1117:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/report/create:1124:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.13. https://adblbackend.peacenepal.com/admin/service-category/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/service-category/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/service-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFlVU9zdnJNaEptSWR4aHB3a1ZOQnc9PSIsInZhbHVlIjoidnZxUXFIM2Y2WDR0NjJTUzlOQ1g2VVB6eGlEREpFVnE1WTZLOUhnN0JkRUZFdm01QVNhQXVtVW9FMUlEeWJtalBtd1VkWXR4Y0RCRHJ1UE15Yk05MGVuaDh6WGhkaCs2RGxkc0VBNnRwdDBJWmZ0MWQ5QlY0elpDMmxCQ0ZpdEoiLCJtYWMiOiIxYzM5OGQzMTFkYzgzM2ZkN2ZiNzliODljOWJmNjg1YjU4OTM4ZDkyZjE3MzY1MGU2MTBkZWI0MjQwNTdkMjBjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/service-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:26:58 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjN0c0xaSlpHT2doUUE3SDBXakhDRkE9PSIsInZhbHVlIjoienRLaGEvWkNXNnRTcWppWTR5UzNaMk1GbzJGbjBaaEhzbVpZRHNZYkQ2QkxKcis5WXYxb2FWdjJKZlFCUkpZcURqdUlSNGxwNTlEZy9YVUczcmIzWUpLUDdZL1FsZEY1TERrWTgwS2tRaTVKdVRjR3BhaWE1RDVjb3UzelZmeUMiLCJtYWMiOiJhOWMwZWYwNjViY2FkZTE1NDRkODFjZTg1Mzg4MzYxOGJiMjUxOGYzYzlhMzBjOTNkNDY2ODg5MWRkYjE5ODI3IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:26:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70295

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **excerpt[2]**.

The previous value reached the sink as:

```
r50vapphti%2527%2522`'"/r50vapphti/><r50vapphti/\>u2sfhucayg&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/service-category/create:1025:30)
at Object.init (https://adblbackend.peacenepal.com/admin/service-category/create:1046:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/service-category/create:1053:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/service-category/create:1025:30)
at Object.init (https://adblbackend.peacenepal.com/admin/service-category/create:1046:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/service-category/create:1053:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.14. https://adblbackend.peacenepal.com/admin/services/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/services/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/services/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImZnSDZhUUptdDU5RUJod3U2VUVWMlE9PSIsInZhbHVlIjoiY2N6bzgxSzh0U1YwWkxkRDQ0aUJtQkpKRDBqbGxhNkRvcjFzM05
ML2YveVM3dDJwYytzNG9pM3NhTTBPOGFySHovdXBwMmdCY09EMWtCcmtzenQyYk83bkNmUXlSUHJwbHdMbXk0bXlDMUt2cHozZ3ZwZXVoSnNMdXFMUnhX
bngiLCJtYWMiOiIxNDk0MzljZDdmMzlhNGIxNTllY2YzMDIwYWJlMzljZjU0YjJhNDM0NGQzYWVlNGFlZGRkZTRkMGZjNGMyYzhmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/services/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:24:08 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InhzZEphc1M5aDNzWEthcWdJcm9nbXc9PSIsInZhbHVlIjoiNGRDaTZ6M09FY3dObTR4U1JTRGthc3JpZ2NGb1ozT1ZzbEplU0psY
ndlcWU4TnhobS81TWNXcUR5b0NhN2E2ZEpRRWMrUVpWTDVIcUJvek1qOTZ0MEgvUlBMNTk0bDVDQ296TEs1QkpZTStrSmFrank3cXM3TWZjSUl6RlJSMWQiL
CJtYWMiOiI4ODdhNTAyZTU2OTRmMDJmODdkNGI2ODA5OGRkMGFjNmVhYTAzZjk2YzNiZDk5NzVmODkzY2UyOTdkZTJmYTk1IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:24:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 75066

<!DOCTYPE html>
<html lang="en">
```

```
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
mrl92yruap%2527%2522`'"/mrl92yruap/><mrl92yruap/\>jaw4vgibhv&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/services/create:1093:30)
at Object.init (https://adblbackend.peacenepal.com/admin/services/create:1114:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/services/create:1121:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/services/create:1093:30)
at Object.init (https://adblbackend.peacenepal.com/admin/services/create:1114:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/services/create:1121:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.15. https://adblbackend.peacenepal.com/admin/team/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/team/create HTTP/1.1
Host: adblbackend.peacenepal.com
```

```
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im9zcGdEYnpGS1hrV1YxeW5WTmlzVXc9PSIsInZhbHVlIjoiTzlHYlIXM3FVOTliZnR6eUp5bjlzcjU5bm5yVC9lV0YyWm9qWUZNK3F
EbVlmSHg4bVpnWFE5NERkNDITSnFBODRPVmY3UlJ6ZW4xcVpkY2dOMWpMZ2d2VUV2SnlNTkkxZmNlUTk3WEtCMkp3c25JRlhreWhBbmhWOVdocWdVSWgiL
CJtYWMiOiI2ZDJmMjlhZjNlNzVlOTQ5Y2EzZWVmOTQ2MDQ2N2JjOTYyMWQ4MWRjNTJhM2M5ODhhYWRiNDNjOGNjZjViODQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/team
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:09:05 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImNPOHlZeXhDRlJMdFVSZVJqYXBwMGc9PSIsInZhbHVlIjoidkd4VlZQR3pPTXlLRnREL3hRY0lEUTNXQ1RWc2gzRjI5TEVMbjRP
OXYxSWxiWnhkQ3RNck01K3hqOEZBNSsxYjV1RmVtS3FEMVhHSlNSUldpclc4SHlDeS9iQnNWTVhZd3pUWUVacXJGZXNzTkFFTjEvUWIyNEgxajJDK3NHeHkiL
CJtYWMiOiI2YWRiZmI1ZGRhMzdiMWU1MjA5MTEzNDVhOTk1YWNlOTc1MThhYTYzZmNmMDdjMjA5ODg5YzZmNmFmOTBlNTk0IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:09:05 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 72020

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **description[2]**.

The previous value reached the sink as:

```
yc7x5u7nlc%2527%2522`'"/yc7x5u7nlc/><yc7x5u7nlc/\>b882cugu6q&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/team/create:1041:30)
at Object.init (https://adblbackend.peacenepal.com/admin/team/create:1062:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/team/create:1069:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
```

```
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/team/create:1041:30)
at Object.init (https://adblbackend.peacenepal.com/admin/team/create:1062:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/team/create:1069:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.16. https://adblbackend.peacenepal.com/admin/training-hall/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training-hall/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/training-hall/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik80TGk4WnlRMzRQeFRiRE1RVC81Q0E9PSIsInZhbHVlIjoiUEgwZm9YYStZWFUvTmVOMk9TcUdPU1lERy80Rk5YcmRwZzdER
VlLVHB0U01qdGx6NEZQVm1SQVVMN1NjYVB2VjJndVZRNFJkRWhiSzBPOFpKR1lXM1F6M0M1UmM2SDlJWXUwUmFWUnlnbzJybkhncVpwb1ZUWktmMWt0M
FVrVXEiLCJtYWMiOiI0ZWJjYzViYmQ2MmU0MzQ2MTkzYWVlYTYwNzIzYmY0ZTEzZDFmOGU4ZGZkYmMxM2E1NjUwOWJlNDE3MzFkZGY4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training-hall
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:10:47 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ii9OR2M3SVVvcHM2ZGV6Yk5jVHRLbHc9PSIsInZhbHVlIjoiSXZLTEN4N2FaRDQ5ejRmTEFjdTludTM2ZjNlVStydWZyYVR6MXgw
WEVPLzJZeEJFN1pLOUlva2YzYlE3RU96RGVSMUJ5MEpFdmFiS2w1OTl5Y3VSME9tQzg1UnlUUzQ1SDVSbGdFaGNhVjhqb2RDQzBQZytQRDhGSmVZK0p2NT
YiLCJtYWMiOiIyYjhjMTA5MzljN2I4NmQ4NDMyYjY2NWUxMTBmZDIyOWNlMjgwYTFkNmVlZDVlYzdkMWUwMjczOGM5ZjY1YzJkIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:10:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71716

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
```

```
...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **description[2]**.

The previous value reached the sink as:

```
s5as55jnug%2527%2522`'"/s5as55jnug/><s5as55jnug/\>d7p6b14kj7&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/training-hall/create:1044:30)
at Object.init (https://adblbackend.peacenepal.com/admin/training-hall/create:1065:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/training-hall/create:1072:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/training-hall/create:1044:30)
at Object.init (https://adblbackend.peacenepal.com/admin/training-hall/create:1065:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/training-hall/create:1072:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.17. https://adblbackend.peacenepal.com/admin/training/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/training/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
```

```
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InFVZ1AxRlhTRnRFVlNsOE1VRTM0RXc9PSIsInZhbHVlIjoib3hSZDV4dStnc0hhVElqQ2JCclF1R1dCRU1VYUMrSUUvTU1DNS90
QmltaFlySWFCN05IN3M1RWdSVzArZ0w4OW1mVFdzSC9IYTNVSEVzbFBzeFVnQnZ3TW1CbTJwNjgyRno1UXRoRURoMnU0djEvNVpSdFh3UldTb2lReUpvbkkiL
CJtYWMiOiJmMWNiYzZmMDAxMzM0MzRlMDkwMWZhYTUzNjZkODM4OTJjYjNiYzc3ZTQxZjI1MTVjOGQwNGNmYmY5NDUyNTZlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:10:24 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZucW9nWnUrSHRZVE9XZTdVYTRRS3c9PSIsInZhbHVlIjoiUGpza2lXbHNHMlR2c3NjdDRqRjBWUmxkWGhhMlM4aXdpc1dNdU5
CdUUvTVNsVnZzK1ZmRllpN2U2MUJuREFUQmQ3Nkd4ZXZITnNSQXBKKzdSQ2JBMlJYWG0xTXRYOUZoYmtRQ0xYMm1XSHJra1BJUEZWNkx3ZVJ4QjVNSlpn
cXUiLCJtYWMiOiIyNDA0MGEwMzYyY2U3ODVmYzZjOWIxMjJiNDZiMTlhOWJhY2YzZDcxMTQxYTQxNmZiYTAyYmRiMTZkNTYyYzJmIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:10:24 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 76880

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has name **participants[2]**.

The previous value reached the sink as:

```
q3smywd40l%2527%2522`'"/q3smywd40l/><q3smywd40l/\>bfg25vjsd3&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/training/create:1105:30)
at Object.init (https://adblbackend.peacenepal.com/admin/training/create:1126:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/training/create:1133:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
```

```
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/training/create:1105:30)
at Object.init (https://adblbackend.peacenepal.com/admin/training/create:1126:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/training/create:1133:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

1.3.18. https://adblbackend.peacenepal.com/admin/vendor-category/create

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor-category/create**

Issue detail

The application may be vulnerable to DOM-based cross-site scripting. Data is read from **textarea.value** and passed to **jQuery.html**.

Request 1

```
GET /admin/vendor-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik1PT0NocDBhQ1pHV2RTblNmYmlaakE9PSIsInZhbHVlIjoicUdyMjA2NDRnZVBPV1Z1VHhrbkswM1N2ckFJUThCSEl6eXNhK1pX
WHF5OFFGdVBzQ3NRKzFqYmJ4bWMySFNQQlVOMGlMaSt2Y2dKOENxbjJudkhEbWJqZmRoQjR2WmJtWGlNMlRTRWd2Q0ZFOVprc2c2akV5VlY0UVJnRHhuR
FEiLCJtYWMiOiI5OWFjZDI2N2YwNzNiODlmZWNhYTMwZTczNWQ4MjViNjJmNzcyMTg4NmYzNTU3N2NhMDBkYzcyMzQzNWQzZmQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:28:48 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJleDFiNmJZTkZsYkliakh4YW1JR1E9PSIsInZhbHVlIjoiMDJJMGQ3U0szTTFEYTEzbTVNZWYrZDIvbWJ2SFlOOFZKd2dRbDArQX
UzSXBINnU3SUEwVlU5LzZGVW5FY0VtTklwVGZ2N25YNHBSa1B4S203di9rQ1YyNzZ6OXRaS29OSmFLdTRVbU1MOHE5djNDelZqWjRsVFZqckJXV3kwem0iLC
JtYWMiOiI4YzY3ZjU1ZWU1MTA4OTNlNzlhNThlN2E4MzJlNmIwNWRjNzNiOWE2NzBmMTAxZDIxYjJiOTZjMmQ3NDZlMzI5IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 13:28:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 68859

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Dynamic analysis

Data is read from **textarea.value** and passed to **jQuery.html**.

The source element has id **editor** and name **description[2]**.

The previous value reached the sink as:

```
f6ye51zou0%2527%2522`'"/f6ye51zou0/><f6ye51zou0/\>a7xt931xaq&
```

The stack trace at the source was:

```
at Object.JMubX (<anonymous>:1:508720)
at HTMLTextAreaElement.get [as value] (<anonymous>:1:510861)
at Object.val (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:8208:16)
at dom_value (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66703:42)
at Object.dom_html [as html] (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66722:16)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:31)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/vendor-category/create:1005:30)
at Object.init (https://adblbackend.peacenepal.com/admin/vendor-category/create:1026:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/vendor-category/create:1033:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

The stack trace at the sink was:

```
at Object.aCftg (<anonymous>:1:107738)
at _0x15c88e (<anonymous>:1:538365)
at Object.SfJdf (<anonymous>:1:117028)
at Object.hUwEy (<anonymous>:1:620037)
at Object.RAeJp (<anonymous>:1:624725)
at Object.apply (<anonymous>:1:631074)
at Editor.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:70220:22)
at Context.initializeModule (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67053:16)
at https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66965:15
at Array.forEach (<anonymous>)
at Context._initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66964:33)
at Context.initialize (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66910:12)
at new Context (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:66898:10)
at HTMLTextAreaElement.<anonymous> (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67184:23)
at Function.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:367:19)
at Object.each (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:202:17)
at Object.summernote (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:67180:10)
at demos (https://adblbackend.peacenepal.com/admin/vendor-category/create:1005:30)
at Object.init (https://adblbackend.peacenepal.com/admin/vendor-category/create:1026:21)
at HTMLDocument.<anonymous> (https://adblbackend.peacenepal.com/admin/vendor-category/create:1033:30)
at mightThrow (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3557:29)
at process (https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js:3625:12)
```

---

2. Medium severity issues

2.1. TLS cookie without secure flag set

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- **adbl_backend_session**

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any

HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Request 1

```
POST /admin/banner HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im15QUVZZWc4RThudjRqNURjUkhBdWc9PSIsInZhbHVlIjoiQ2NCT042RGpZdHNKTjNBYWhpZGI2SmxwUUEzN29CN1BoYmdY
K1NFZUVXYnBsSmIwZTk5TTNXZUJjMEFoMHhmbkdjbTh0ZHFHc28yUjM4eW5weFl0UWgzaUxoUmxYelViSzB1QkNsZEhQV2FUd1I4OFdkU0dkZEx0bGMyMGJC
QXkiLCJtYWMiOiJkMjBkZGQzZTY4MjMwMGY5ODJhYzgwM2FiYmIxMThiZWY5MzcyNTNmNDI2MjA3NDMyOTY3YWVhMjdlZDQ5NWE5IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/banner/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLyJSSzR42azygqKF
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1443

------WebKitFormBoundaryLyJSSzR42azygqKF
Content-Disposition: form-data; name="_token"

FnGiYUsubSQkMB6Hqxcwd6tZlnBGpJJw716LlqH8
------WebKitFormBoundaryLyJSSzR42azygqKF
Content-Disposition: form
...[SNIP]...
```

Response 1

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:18:26 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/banner/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjNMMWJxNzAxZkx5WWFiUW9jZzNDeEE9PSIsInZhbHVlIjoieFpseHI3NEVPbnliMzROYW1VWThpRThnM2VyTW5YZjRhcEdhaS8
vc2M5NDN6eEpIaW83MzlrdjFodWt4U1VZSTEzOFN3eTJUME1rV0JXWm5LZzJ5ZTF5MnlHREs1a0QzZldaR1hZZGV2WWhYa1V2aTU1dGFkVWtwMjdRRG5wMX
EiLCJtYWMiOiJhMGZmYjE5ODMwY2YyMzFlZTM0ZDEzMWYwNTRjMmVlODgzNGNiNGUyZjZhNzFjYjg2NzY5OTcyNDRhODBhZjMxIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:18:26 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 462

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/banner/create'" />

<title>Redire
...[SNIP]...
```

Request 2

```
POST /admin/branch-directory HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImNGMURTeFNnZmNmWVdIRzgwbDlKdUE9PSIsInZhbHVlIjoib0U5N2xuaGlGYmlkQUsvVi8zYkFVZll0emdtYmN5N1Z5QWxNSlJu
V2JoMDQ1K2pVNHpLRHQzYlc4NEIySkhIVW5leUhNT0xUN3ppVThnN2JYamRWSmlBYlZxZGlGZ3dhb2RMNHlYRFNoVjh2YmN3VGJhb2pvNmtWc1kyajNuK24iLC
JtYWMiOiIzMzcyZDk4YzIxOWMyYWRlNzRjZWRjYWI3ZjQxYzAwYWQ5N2I4ZDRmMTQ0MDlhYWI3YTNiNDg4ZGMxMGU4OWM1IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/branch-directory/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydXjrIYjvRWM9P9rv
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 2500

------WebKitFormBoundarydXjrIYjvRWM9P9rv
Content-Disposition: form-data; name="_token"

hM5czuLnDETA2crIbVOVQRL2gU8AtxvJSxKWrr22
------WebKitFormBoundarydXjrIYjvRWM9P9rv
Content-Disposition: form
...[SNIP]...
```

Response 2

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:33:09 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/branch-directory/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZHSHJrdXdBQjA5d2RMczdnSTdTYXc9PSIsInZhbHVlIjoiMW5YT0J5Mm83SCtDbGcwYUxtWmJXUXNBa2xUdE1DQlhmVFB5STl
JcWh1KzhjaFRETVZLV0VBaTJwTU5wbENzdTJIMnRWMXRoVkxxRi9EeGhZcnJ3WmNQcW9yWUgwTW1MRWIxekFTckg2TGJ0cFFKK1AycXpBdURVWnhnR0hE
NFMiLCJtYWMiOiI2ZDI1MjE4NzI1ZjM2ZTE1MzIwZDQ4YzhjNzcwOTQ2NDM1NjA0NjdkNTZmMzFiMjE1YzRhNWE4MmMyZGUwYzg1IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:33:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 502

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/branch-directory/create'" />

<ti
...[SNIP]...
```

Request 3

```
POST /admin/account-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ii9Fa0I1elc2Mm80WjVVS01RZzA3MXc9PSIsInZhbHVlIjoiYnlEU2ZMajRNVi9jRCtGR1BYQ1ZTSktPUDRPQ1d4UGR2UjVLM0lXSlc
ySHlwYjB1RWtlTUY1aUN0cFpkTXFKd25lQ2NPMXVxTXRZYUpOeW13Z1MzMldsb2dLY2czeUp1Y2NaUFp6cnJnNVN6Q2J6WUIxL0JKVE5wRUVaeGhNS0wiLCJt
YWMiOiI4YjY1ZWE2YzQ3MDFlMmJhMWVjMTNhYmYzNTczMmZjYjZiMDgyYTk5YzNiYmE0MjM0Y2ZlMmY2YTQ5Y2MyNDhjIiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCwkHzMMO62aUgNLr
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 4412

------WebKitFormBoundaryCwkHzMMO62aUgNLr
Content-Disposition: form-data; name="_token"

XHc3E9GxctiOaa5QQGzBXZusRV9Isy5hK1T1xw1M
------WebKitFormBoundaryCwkHzMMO62aUgNLr
Content-Disposition: form
...[SNIP]...
```

Response 3

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:20:33 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/account-type/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InV4OTE5WVZTdkkxR2Z4NWdlV0kya3c9PSIsInZhbHVlIjoid0Q4OTZQNXE0dGpubXBiN0xtVkdpdVFqR1NzTkJaTnlBRGpNUlVHN
DFISitwbThMWGR5OFZnV050UlNSb0hmY2wxbzR3dEo3Tjk1aHFDN29Ra0tPT1JCdXEyVUxBRDVVclZhWkNYNGJWcjdDZXZoWWhGYlE3Mkx4amNrS2o0TFciL
CJtYWMiOiI5MmRmZDlmNWNjMjIwODUxNGViOTQ0MmEyMDg1MjY1MDYxMWZhOTQxYTlkMDE2NDYyZGU3ZDUzNmQxZWUxYTY0IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:20:34 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 486

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/account-type/create'" />

<title>
...[SNIP]...
```

3. Low severity issues

3.1. Vulnerable JavaScript dependency

There are 4 instances of this issue:

- /admin/layout
- /backend/js/jquery-ui.js
- /backend/js/plugins.bundle.js
- /backend/plugins/datatables/datatables.bundle.js

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- CWE-1104: Use of Unmaintained Third Party Components
- A9: Using Components with Known Vulnerabilities

3.1.1. https://adblbackend.peacenepal.com/admin/layout

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/layout**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery-ui** version **1.10.3**, which has the following vulnerabilities:

- CVE-2021-41184: XSS in the `of` option of the `.position()` util
- CVE-2021-41183: XSS Vulnerability on text options of jQuery UI datepicker
- CVE-2021-41182: XSS in the `altField` option of the Datepicker widget
- CVE-2022-31160: XSS when refreshing a checkboxradio with an HTML-like initial text label

Request 1


```
GET /admin/layout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFwQ01Kd3pHSE1EWUlYMXQvMXJjalE9PSIsInZhbHVlIjoiZlNBSDdVQXNIenZWSS9CRHl6OWRRVjZTeFk2UnFkMllmODIzajVra
ll6SXFNbUNvdFMxVzdaSUpyL2ZTQXB1bjNKNGczRVpvcWY3d1VTUG5lTWxyM2xHT1Y5WGJhSWd6L3VWZ0U3Ulk0cTVqTENiSitsTjdt0JhMTBma3ppTWIiLCJt
YWMiOiJhMjU4ZGQyZGQwMjU1N2Y3ZWQ4Yjg2NjVhYjgwMTgwN2RlZGQwYmU5OGI0OTFlODU5OTIyOTllODYxMDUwZDdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


Response 1


```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:55:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Im5UWFllOHhXUmxFZ3ZBejZGTWFGeXc9PSIsInZhbHVlIjoic2Y2WmlCN2V4RUt2eVRYeTBMVGozaHc3K3VQYmhBc2JzWUN1Q
0RlL3N4T1JGaWRnOUpoQW10WmZPRkNIc3NvcUgyVHJjVklRdGJUMFI5NklDSUR4anFhaWU3UUFXYitYc1lySWoxK2tuVG90YjlEQTZiVlZqUGpiVlFkVjhIYTYiLC
JtYWMiOiI4ZDNhNDdkMmY2MzM0M2Y1YTY5NGU4NTZhZWIwZTIzY2JkNmVjNjQ1ZGRlYjRhMjZlMTIzNml1ZDA0OWE2MTMxIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 12:55:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70330

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
</script>
<script src="https://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/jquery-ui.min.js"></script>
...[SNIP]...
```

3.1.2. https://adblbackend.peacenepal.com/backend/js/jquery-ui.js

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/backend/js/jquery-ui.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery-ui** version **1.12.1**, which has the following vulnerabilities:

- CVE-2021-41184: XSS in the `of` option of the `.position()` util

- CVE-2021-41183: XSS Vulnerability on text options of jQuery UI datepicker
- CVE-2021-41182: XSS in the `altField` option of the Datepicker widget
- CVE-2022-31160: XSS when refreshing a checkboxradio with an HTML-like initial text label

Request 1

```
GET /backend/js/jquery-ui.js HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkdpSDQ4QS9HWkk0TXpSa2ovU005cmc9PSIsInZhbHVlIjoib05pbmlBeXY0OE1VQXl3YUVGSnRIZThKR2oyT2ltcXFpVFlHdE1BN
HFhT0JncXY1RldPWlZHQXpQYlN6dWV0WVFSL0hHR1JKeXdGak1Fend4bFBEaHc1Y0l3Wk42ZnhUSjloWlE2NDEycTVHdjZ1MFEwdDR6b05MeUVZUU9JWXgiL
CJtYWMiOiJmNzEzOTc2MWZiMjIzM2RmZThmODQwM2RhNzI0Yzk4YmFlNjNmY2Q1YmZmODAxNmM2Njg3ZDE0MDY5Yzg1MjQ0IiwidGFnIjoiIn0%3D
Referer: https://adblbackend.peacenepal.com/admin/dashboard
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:52:06 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "7f20a-615a622fabcf6-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/javascript
Content-Length: 520714

/*! jQuery UI - v1.12.1 - 2016-09-14
* http://jqueryui.com
* Includes: widget.js, position.js, data.js, disable-selection.js, effect.js, effects/effect-blind.js, effects/effect-bounce.js, effects/effect-clip.js, effects/effe
...[SNIP]...
```

3.1.3. https://adblbackend.peacenepal.com/backend/js/plugins.bundle.js

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/backend/js/plugins.bundle.js**

Issue detail

We observed 2 vulnerable JavaScript libraries.

We detected **jquery** version **3.4.1**, which has the following vulnerabilities:

- CVE-2020-11022: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
- CVE-2020-11023: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS

We also detected **moment.js** version **2.27.0**, which has the following vulnerabilities:

- CVE-2022-24785: This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg fr is directly used to switch moment locale.
- CVE-2022-31129: Regular Expression Denial of Service (ReDoS), Affecting moment package, versions >=2.18.0 <2.29.4

Request 1

```
GET /backend/js/plugins.bundle.js HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkFCRUpRNFpRU1FhNjV5R0VZQVpiMWc9PSIsInZhbHVlIjoiSGZlSVVZeVZvY3ZrdUVCZzZCeSs0UEhFOGloMWtzaGk5aGRTUD
```

```
BwN0svNHZQZXpSL2hJM2tvV0QyTEJNeFcxTXFKeFJCS2luV3lLeDlJcTQ4RjVna0dvWUlGdGZOQ2FuT3FNUDYrdEFJYkJVc01LVUc3VjN4aGNTZnh4emVIeUYiL
CJtYWMiOiJmOTQyNGUwNTE0OGJhOWQzNzQ1YmIxMDllYWZmMGUxNDE3NjI3ZDJjMTg2OGMzYjE4ZjA0YmY1ZTI4YjNhNWYxliwidGFnIjoiIn0%3D
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: Windows
Referer: https://adblbackend.peacenepal.com/admin/login
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:51:59 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "3d18e1-615a622fafb77-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/javascript
Content-Length: 4004065

/*!
* jQuery JavaScript Library v3.4.1
* https://jquery.com/
*
* Includes Sizzle.js
* https://sizzlejs.com/
*
* Copyright JS Foundation and other contributors
* Released under the MIT license
* https://jquery.org/license
*
* Date
...[SNIP]...
,Qt),Xt.lang=tt,W("X",0,0,"unix"),W("x",0,0,"valueOf"),le("x",ie),le("X",/[+-]?\d+(\.\d{1,3})?/),Le("X",function(e,a,t){t._d=new
Date(1e3*parseFloat(e))}),Le("x",function(e,a,t){t._d=new Date(G(e))}),M.version="2.27.0",e=Sa,M.fn=yt,M.min=function(){return Oa("isBefore",
[].slice.call(arguments,0))},M.max=function(){return Oa("isAfter",[].slice.call(arguments,0))},M.now=function(){return Date.now?Date.now():+new
Date},M.utc=c,M.unix=function(e){return Sa(1e3*e)},M.months=function(e,a){return
Dt(e,a,"months")},M.isDate=d,M.locale=oa,M.invalid=y,M.duration=Ga,M.isMoment=D,M.weekdays=function(e,a,t){return
Tt(e,a,t,"weekdays")},M.parseZone=function(){return Sa.apply(null,arguments).parseZone()},M.locale Data=ua,M.isDuration=Aa,M.monthsShort=function(e,a){return
Dt(e,a,"
...[SNIP]...
```

3.1.4. https://adblbackend.peacenepal.com/backend/plugins/datatables/datatables.bundle.js

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/backend/plugins/datatables/datatables.bundle.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **jszip** version **3.5.0**, which has the following vulnerability:

- CVE-2021-23413: Denial of Service (DoS)

Request 1

```
GET /backend/plugins/datatables/datatables.bundle.js HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImdlM3hKL0o3T0haa2d6N1VIekozQXc9PSIsInZhbHVlIjoiWmZ4KzhlN2hCM1YvZlFqZXZhcmtINWRIMEY0ajF3ZGwyQzdBbHNVN
VRiWGUzRUVaMlEzL2E5eUhacEZvemRwNGppSis4OU04eGJwcVo0NVJiQk9QSFF1ZzZsL2Z2QjRzSTZBS0RrNGxxbnl5L2Y2aktVR2o3dUZuM3FVL2d0STAiLCJt
YWMiOiIxY2M5NDQ4ODk3YzJkYmJjMTI0ZTA1NDU2ZjNkNDkwYTg2MTQ5NTI2ZDFkZDVhM2YzZmJiMmIyNTVlNGExODc1IiwidGFnIjoiIn0%3D
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:52:17 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "2e4a25-615a622fbd637-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/javascript
Content-Length: 3033637

/*! DataTables 1.10.19
* ..2008-2018 SpryMedia Ltd - datatables.net/license
*/

/**
* @summary DataTables
* @description Paginate, search and order HTML tables
* @version 1.10.19
* @file
...[SNIP]...
.fn.dataTable.AutoFill||require("datatables.net-autofill")(b,c);return a(c,b,b.document)}:a(jQuery,window,document)})(function(a)
{a=a.fn.dataTable;a.AutoFill.classes.btn="btn btn-primary";return a});

/*!

JSZip v3.5.0 - A JavaScript class for generating and reading zip files
<http://stuartk.com/jszip>
...[SNIP]...
```

3.2. Open redirection (reflected)

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/login**

Issue detail

The value of the **Referer** HTTP header is used to perform an HTTP redirect. The payload **http://at2a5x11vmx/a?https://adblbackend.peacenepal.com/admin/login** was submitted in the Referer HTTP header. This caused a redirection to the following URL:

- http://at2a5x11vmx/a?https://adblbackend.peacenepal.com/admin/login

The original request used the POST method, however it was possible to convert the request to use the GET method, to enable viable exploitation in a phishing attack.

Because the data used in the redirection is submitted within a header, the application's behavior is unlikely to be directly useful in lending credibility to a phishing attack. This limitation considerably mitigates the impact of the vulnerability.

Issue background

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Issue remediation

If possible, applications should avoid incorporating user-controllable data into redirection targets. In many cases, this behavior can be avoided in two ways:

- Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs.
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

If it is considered unavoidable for the redirection function to receive user-controllable input and incorporate this into the redirection target, one of the following measures should be used to minimize the risk of redirection attacks:

- The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a relative URL.
- The application should use URLs relative to the web root for all of its redirects, and the redirection function should validate that the URL received starts with a slash character. It should then prepend http://yourdomainname.com to the URL before issuing the redirect.
- The application should use absolute URLs for all of its redirects, and the redirection function should verify that the user-supplied URL begins with http://yourdomainname.com/ before issuing the redirect.

References

- Using Burp to Test for Open Redirections
- Fun With Redirects

Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Request 1

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdWJ6VW5GMFl3TkImajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHFML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: http://at2a5x11vmx/a?https://adblbackend.peacenepal.com/admin/login
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 109

_token=psvOCIIjyWEguowk14Vu2U2PGcuDN0PvKSvaqYOv&email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: http://at2a5x11vmx/a?https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjA2cENNbGhKTlZSeTFlRHgwcWFXZ2c9PSIsInZhbHVlIjoiZjVOS1BGTU9JZlVCQXliYTdjR1ROcDNRbHZiaHRRcUpXZjdoZytSSCtHSmRzMTd5ZFliOVhDT0dVQTA0V2tUWU93K2hUSCtmZ01yM1ZydnE1WCs4VlpBYkN1NWVaKzduM3FKYTB6bTBmSmRLWStJMGVZMjFMdHl1WnEybmt4VFUiLCJtYWMiOiI5NmFiNWY1ZTE0NTVjNjQzMjRlOWJjYzRlMWE0NDRjNjhlNGM3MDc4MzM0OWVhNDcyODAwMjg5MTY1ZWJjNmRhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 514

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='http://at2a5x11vmx/a?https://adblbackend.peacenepal.com/admin/login'" />


...[SNIP]...
```

3.3. Open redirection (DOM-based)

There are 3 instances of this issue:

- /admin/import/store-atm
- /admin/import/store-branch
- /admin/reset_password

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based open redirection vulnerabilities is not to dynamically set redirection targets using data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from introducing an arbitrary URL as a redirection target. In general, this is best achieved by using a whitelist of URLs that are permitted redirection targets, and strictly validating the target against this list before performing the redirection.

References

- Web Security Academy: Open redirection (DOM-based)

Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

3.3.1. https://adblbackend.peacenepal.com/admin/import/store-atm

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.hash** and passed to **fetch.body**.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Wed, 02 Oct 2024 11:56:37 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033742

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **fetch.body**.

The following value was injected into the source:

```
#pu4a6bhqdo=pu4a6bhqdo%27%22`'"/pu4a6bhqdo/><pu4a6bhqdo/\>yx1ako1w5i&
```

The previous value reached the sink as:

```
{"tabs":["stackTraceTab","requestTab","appTab","userTab","contextTab","debugTab"],"lineSelection":"#pu4a6bhqdo=pu4a6bhqdo%27%22`'\"/pu4
```

The stack trace at the source was:

```
at Object.aFxlM (<anonymous>:1:119263)
at Object._0xea57c5 [as proxiedGetterCallback] (<anonymous>:1:655360)
at get hash [as hash] (<anonymous>:1:247263)
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:385831
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:386379
```

```
at onClick (https://adblbackend.peacenepal.com/admin/import/store-atm:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/import/store-atm:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:104921)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:125759
at di (https://adblbackend.peacenepal.com/admin/import/store-atm:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/import/store-atm:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/import/store-atm:114:126234)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:132758
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:132766
at Pn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:292199)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/import/store-atm:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/import/store-atm:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/import/store-atm:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/import/store-atm:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/import/store-atm:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/import/store-atm:114:291823)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:114307
at Da (https://adblbackend.peacenepal.com/admin/import/store-atm:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
at Object.PIMjm (<anonymous>:1:7292)
at _0x136a58 (<anonymous>:1:155595)
at Object.UnYww (<anonymous>:1:126229)
at _0x54f27e (<anonymous>:1:679325)
```

The stack trace at the sink was:

```
at Object.nlHmJ (<anonymous>:1:639360)
at _0x162bca (<anonymous>:1:657342)
at Object.tSHMT (<anonymous>:1:539597)
at <anonymous>:1:551974
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:385969
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:386272
at new Promise (<anonymous>)
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:385875
at https://adblbackend.peacenepal.com/admin/import/store-atm:119:386379
at onClick (https://adblbackend.peacenepal.com/admin/import/store-atm:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/import/store-atm:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:104921)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:125759
at di (https://adblbackend.peacenepal.com/admin/import/store-atm:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/import/store-atm:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/import/store-atm:114:126234)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:132758
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:132766
at Pn (https://adblbackend.peacenepal.com/admin/import/store-atm:114:292199)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/import/store-atm:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/import/store-atm:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/import/store-atm:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/import/store-atm:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/import/store-atm:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/import/store-atm:114:291823)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:114307
at Da (https://adblbackend.peacenepal.com/admin/import/store-atm:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
```

This was triggered by a **click** event with the following HTML:

```
<button class="px-4 h-8 whitespace-nowrap border-b
            text-xs uppercase tracking-wider font
```

3.3.2. https://adblbackend.peacenepal.com/admin/import/store-branch

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-branch**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.hash** and passed to **fetch.body**.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
```

```
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Wed, 02 Oct 2024 11:56:38 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033762

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **fetch.body**.

The following value was injected into the source:

```
#b64jqr7ktx=b64jqr7ktx%27%22`'"/b64jqr7ktx/><b64jqr7ktx/\>oaaamxlog5&
```

The previous value reached the sink as:

```
{"tabs":["stackTraceTab","requestTab","appTab","userTab","contextTab","debugTab"],"lineSelection":"#b64jqr7ktx=b64jqr7ktx%27%22`'\"/b64
```

The stack trace at the source was:

```
at Object.aFxlM (<anonymous>:1:119263)
at Object._0xea57c5 [as proxiedGetterCallback] (<anonymous>:1:655360)
at get hash [as hash] (<anonymous>:1:247263)
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:385831
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:386379
at onClick (https://adblbackend.peacenepal.com/admin/import/store-branch:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/import/store-branch:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:104921)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:125759
at di (https://adblbackend.peacenepal.com/admin/import/store-branch:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/import/store-branch:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/import/store-branch:114:126234)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:132758
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:132766
at Pn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:292199)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/import/store-branch:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/import/store-branch:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/import/store-branch:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/import/store-branch:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/import/store-branch:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/import/store-branch:114:291823)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:114307
at Da (https://adblbackend.peacenepal.com/admin/import/store-branch:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
at Object.PIMjm (<anonymous>:1:7292)
at _0x136a58 (<anonymous>:1:155595)
at Object.UnYww (<anonymous>:1:126229)
at _0x54f27e (<anonymous>:1:679325)
```

The stack trace at the sink was:

```
at Object.nlHmJ (<anonymous>:1:639360)
at _0x162bca (<anonymous>:1:657342)
at Object.tSHMT (<anonymous>:1:539597)
at <anonymous>:1:551974
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:385969
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:386272
at new Promise (<anonymous>)
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:385875
at https://adblbackend.peacenepal.com/admin/import/store-branch:119:386379
at onClick (https://adblbackend.peacenepal.com/admin/import/store-branch:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/import/store-branch:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:104921)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:125759
at di (https://adblbackend.peacenepal.com/admin/import/store-branch:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/import/store-branch:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/import/store-branch:114:126234)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:132758
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:132766
```

```
at Pn (https://adblbackend.peacenepal.com/admin/import/store-branch:114:292199)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/import/store-branch:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/import/store-branch:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/import/store-branch:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/import/store-branch:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/import/store-branch:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/import/store-branch:114:291823)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:114307
at Da (https://adblbackend.peacenepal.com/admin/import/store-branch:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
```

This was triggered by a **click** event with the following HTML:

```
<button class="px-4 h-8 whitespace-nowrap border-b
           text-xs uppercase tracking-wider font
```

3.3.3. https://adblbackend.peacenepal.com/admin/reset_password

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.hash** and passed to **fetch.body**.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Wed, 02 Oct 2024 11:56:38 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033722

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

Dynamic analysis

Data is read from **location.hash** and passed to **fetch.body**.

The following value was injected into the source:

```
#n6mepq9853=n6mepq9853%27%22`'"/n6mepq9853/><n6mepq9853/\>fppvxu7hm7&
```

The previous value reached the sink as:

```
{"tabs":["stackTraceTab","requestTab","appTab","userTab","contextTab","debugTab"],"lineSelection":"#n6mepq9853=n6mepq9853%27%22`'\"/n6m
```

The stack trace at the source was:

```
at Object.aFxlM (<anonymous>:1:119263)
at Object._0xea57c5 [as proxiedGetterCallback] (<anonymous>:1:655360)
at get hash [as hash] (<anonymous>:1:247263)
at https://adblbackend.peacenepal.com/admin/reset_password:119:385831
at https://adblbackend.peacenepal.com/admin/reset_password:119:386379
```

```
at onClick (https://adblbackend.peacenepal.com/admin/reset_password:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/reset_password:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/reset_password:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/reset_password:114:104921)
at https://adblbackend.peacenepal.com/admin/reset_password:114:125759
at di (https://adblbackend.peacenepal.com/admin/reset_password:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/reset_password:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/reset_password:114:126234)
at https://adblbackend.peacenepal.com/admin/reset_password:114:132758
at https://adblbackend.peacenepal.com/admin/reset_password:114:132766
at Pn (https://adblbackend.peacenepal.com/admin/reset_password:114:292199)
at https://adblbackend.peacenepal.com/admin/reset_password:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/reset_password:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/reset_password:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/reset_password:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/reset_password:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/reset_password:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/reset_password:114:291823)
at https://adblbackend.peacenepal.com/admin/reset_password:114:114307
at Da (https://adblbackend.peacenepal.com/admin/reset_password:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
at Object.PIMjm (<anonymous>:1:7292)
at _0x136a58 (<anonymous>:1:155595)
at Object.UnYww (<anonymous>:1:126229)
at _0x54f27e (<anonymous>:1:679325)
```

The stack trace at the sink was:

```
at Object.nlHmJ (<anonymous>:1:639360)
at _0x162bca (<anonymous>:1:657342)
at Object.tSHMT (<anonymous>:1:539597)
at <anonymous>:1:551974
at https://adblbackend.peacenepal.com/admin/reset_password:119:385969
at https://adblbackend.peacenepal.com/admin/reset_password:119:386272
at new Promise (<anonymous>)
at https://adblbackend.peacenepal.com/admin/reset_password:119:385875
at https://adblbackend.peacenepal.com/admin/reset_password:119:386379
at onClick (https://adblbackend.peacenepal.com/admin/reset_password:119:386534)
at HTMLUnknownElement.y (https://adblbackend.peacenepal.com/admin/reset_password:114:103635)
at Object.Hn (https://adblbackend.peacenepal.com/admin/reset_password:114:103960)
at Kn (https://adblbackend.peacenepal.com/admin/reset_password:114:104921)
at https://adblbackend.peacenepal.com/admin/reset_password:114:125759
at di (https://adblbackend.peacenepal.com/admin/reset_password:114:125814)
at pi (https://adblbackend.peacenepal.com/admin/reset_password:114:126152)
at mi (https://adblbackend.peacenepal.com/admin/reset_password:114:126234)
at https://adblbackend.peacenepal.com/admin/reset_password:114:132758
at https://adblbackend.peacenepal.com/admin/reset_password:114:132766
at Pn (https://adblbackend.peacenepal.com/admin/reset_password:114:292199)
at https://adblbackend.peacenepal.com/admin/reset_password:114:127903
at Ti (https://adblbackend.peacenepal.com/admin/reset_password:114:127943)
at ja (https://adblbackend.peacenepal.com/admin/reset_password:114:115229)
at Ua (https://adblbackend.peacenepal.com/admin/reset_password:114:114503)
at t.unstable_runWithPriority (https://adblbackend.peacenepal.com/admin/reset_password:114:38308)
at Ws (https://adblbackend.peacenepal.com/admin/reset_password:114:148138)
at _n (https://adblbackend.peacenepal.com/admin/reset_password:114:291823)
at https://adblbackend.peacenepal.com/admin/reset_password:114:114307
at Da (https://adblbackend.peacenepal.com/admin/reset_password:114:114343)
at _0x4b2fd9 (<anonymous>:1:152233)
```

This was triggered by a **click** event with the following HTML:

```
<button class="px-4 h-8 whitespace-nowrap border-b
            text-xs uppercase tracking-wider font
```

3.4. Password field with autocomplete enabled

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin**

Issue detail

The page contains a form with the following action URL:

- https://adblbackend.peacenepal.com/admin/reset_password

The form contains the following password fields with autocomplete enabled:

- oldpassword
- newpassword
- confirmpassword

This issue was found in multiple locations under the reported path.

Issue background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Issue remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /admin/account-type-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IktERG1NMkpBa1VNQlJjRnNPVEk5SVE9PSIsInZhbHVlIjoiWFNobWNJOXROU1NwWG5UUkNuTG1jWnVSMWdPZ2tCMzE3NlFT
bEpkQ2prWVVnNm5tZHMxazJvL0FtUTNGVmNPV25RdnAxR3ZpMlpJMCszeW1RODlqQkR1eW9aVzhiZHk2aW1aUm85NnhXUER2Yjg5d21IbFpyNGJ6OE9WQm
hVQ3MiLCJtYWMiOiJmNjAxYjg5ODg2ZTFmZDgxMjE4ZWUzNWQ1NGIxYzkwYmQzODgyMmY3YjlmMjBiMjdhZWU2YTA2NjVhZThkZjM2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:52:41 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJMV2ZSZVJCZXVVaDJHRVQ3UVdGTmc9PSIsInZhbHVlIjoiT3pQeWhJVWU2OWFlNzdTNkJNclJaRlAyYmdham9mVDVwMlprdD
F5WGRCdTNRaUNSK0JLYWFlVFRpZVo3OElHRHlPMU8wdzFMbExJdHhvT21UNFNrVUJKNk5nMGx0R1lGRkVPMXZkVHBGSXlvQUNOU1BTdUNlSFpuWkRGK
2FkK3oiLCJtYWMiOiJiMmQ4ZjViODQzMzUxOTEwYjJjZmM2YjYxZjI1MDM0MDM4NDI5NTAwMzI1ODU5NTYxM2MzM2JiMDhhMmY0MWQyliwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:52:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 91873

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
</div>
<form method="POST" action="https://adblbackend.peacenepal.com/admin/reset_password" accept-charset="UTF-8" class="form-horizontal" id="Password"
enctype="multipart/form-data"><input name="_token" type="hidden" value="GBdsdunJ1Fe3OC5twkJhjElNaTd6BKvmAUDcX7g3">
...[SNIP]...
</label>
<input class="form-control" name="oldpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="newpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="confirmpassword" type="password" value="">
```

```
</div>
...[SNIP]...
```

Request 2

```
GET /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlplK054czJobzdRR25oTjlhYWRjVkE9PSIsInZhbHVlIjoiczUvSHJNV0p2NjM0bDNsdG5POExPQm53UGM2SHkrL3cyaE1oT3RYZXNMNHdmRGwwc08xRGpVeVFxK2Fya1g4amdnSWdxajJrRVVXaXJxQXdyUktBUWt5WktMaGkzV1NlRWYrWkE3cjh3T3VWc0pKRjRLVDczc1FzaEJLeGdmYkQiLCJtYWMiOiI0M2QyODZiMjY0YTBjYTc3NzA2ZmEwY2FkYTA5MTYxNzVlNTM1YWU3ZjcwZjQyM2M4YTc2ZThkMmI3ZGE1NzY3liwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:56:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlVBSmJqNGRENjlISENObIF4aDZZSmc9PSIsInZhbHVlIjoiWGY4QVF1dFplQUEwZGRFWExVUEtSK3NSbk9HU1lnbmlyRyt3NU5iczNkUGlTTUQ0SjV3b1hZRHQ3Slc5b2ZtZFFuUStMODB0M0RjU0daRUVSeUVPQXdNK2l0bUplK0oyOUljKy9HVGtiVUE5MzJwci9IT1o3U0phRjNNY05lWmwiLCJtYWMiOiI5YzEwZWNmZGM0MmI0YThlNGE4MjAyZmI5YjQzNWJlYzc4ODNiOWRkZTZhYTA1YWY3YjcwMWVhZGZhYjJiMDAzIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 12:56:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 73707

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
</div>
<form method="POST" action="https://adblbackend.peacenepal.com/admin/reset_password" accept-charset="UTF-8" class="form-horizontal" id="Password"
enctype="multipart/form-data"><input name="_token" type="hidden" value="j5DbxfLYBcCagZMMm0U3dHdHdo8cTcO2f1trl4Od">
...[SNIP]...
</label>
<input class="form-control" name="oldpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="newpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="confirmpassword" type="password" value="">
</div>
...[SNIP]...
```

Request 3

```
GET /admin/account-type-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImlNUnExR0U2cnFjR1NwaHcyZ3o1dUE9PSIsInZhbHVlIjoiT05VZ1NIY1RsakVYTHY1Ui8wdlkxQVhZYnFTelNTZ1NSMUpFRENOS1FQeEdIbGNIalJvbm1NU0FlSFZUaEYzbkdRZVZGM3BVdVVQWUQzNFQ2QWRVM3ZXY0hza2hmcGY1QnRRclpCSjVpMXIvNUNuRmdueE5yRDVCK0FPVU15d0EiLCJtYWMiOiI4YmQ2ZWViYjc4ZDRlZWExYTBhNWJlMjliN2I0ZjdkZTIzNzI0ZjA4NDdjZjU2ZTg1OThhOGRjNDc5ODg0MjQxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type-category/create
```

```
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:23:01 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkhYelBmcUp1eUEvR2lIQ3k4dlkrWXc9PSIsInZhbHVlIjoibUZhWFFxMnVsTHdSdFhzdXNaU3M2MVI0WTBLcWRZTzI2Y3l1dWdQM
nFQV2JLMWpZWXlHK0tMT2hzOCt4eWdMbVNhZ2pLRG5kSVB3VWJOVGZ1SEYzRHdJTHc5cDE2MyszbkpoZDVVbjQyeDAwamVLWWhRNmx6UXZHMnc0V3lh
MkEiLCJtYWMiOiJlOTE0MDA1ODJlZjdmYTIzOGIzYTNlODAzZTIyY2M5YTJlMDdjYTcyNzM2ZjZmZmQzNjU0ODk1OWMzM2QzMDhkIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:23:01 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71557

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
</div>
<form method="POST" action="https://adblbackend.peacenepal.com/admin/reset_password" accept-charset="UTF-8" class="form-horizontal" id="Password"
enctype="multipart/form-data"><input name="_token" type="hidden" value="8ZKRrkGFa7pe8WTP5xG4gMFLO3ob4eTOtybEhs1U">
...[SNIP]...
</label>
<input class="form-control" name="oldpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="newpassword" type="password" value="">
</div>
...[SNIP]...
</label>
<input class="form-control" name="confirmpassword" type="password" value="">
</div>
...[SNIP]...
```

3.5. Client-side HTTP parameter pollution (reflected)

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/login**

Issue detail

The value of the **Referer** HTTP header is copied into the response within the query string of a URL.

The payload **wnu&uvk=1** was submitted in the Referer HTTP header. This input was echoed as **wnu&uvk=1** within the "content" attribute of a "meta" tag.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary query string parameters into URLs in the application's response.

Issue background

Client-side HTTP parameter pollution (HPP) vulnerabilities arise when an application embeds user input in URLs in an unsafe manner. An attacker can use this vulnerability to construct a URL that, if visited by another application user, will modify URLs within the response by inserting additional query string parameters and sometimes overriding existing ones. This may result in links and forms having unexpected side effects. For example, it may be possible to modify an invitation form using HPP so that the invitation is delivered to an unexpected recipient.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

Issue remediation

Ensure that user input is URL-encoded before it is embedded in a URL.

References

- HTTP Parameter Pollution

Vulnerability classifications

- CWE-233: Improper Handling of Parameters
- CWE-20: Improper Input Validation
- CAPEC-460: HTTP Parameter Pollution (HPP)

Request 1

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdWJ6VW5GMFl3TklmajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHFML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: wnu&uvk=1
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 109

_token=psvOCIIjyWEguowk14Vu2U2PGcuDN0PvKSvaqYOv&email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:46 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/wnu&uvk=1
Set-Cookie:
adbl_backend_session=eyJpdiI6ImQySktBYjlBM01FT3VCaEZCeFMwN3c9PSIsInZhbHVlIjoiR21QcXFxRVpldUpSaWwyZEQzLzZ0UFREaUVaYnA4VTRFYnlrcWZ2dXppckdFOWlic3JyQk1oblRKdFNPem4rSFZxUTJWREdYWmZ5VUVNblAybXNURkFJbWx1NTJWcE1yWGlJSWhhSDlhVTcwWEhSMkdENmNjZ3pNanVHSmNBYzQiLCJtYWMiOiI2ZTI3M2M0MDVmMGQ4Yjc4YzdkYmIzYWZhYTIyMDM1MDU5MDBlZGFkOTQxNWNlMjZjZmE1YWMwZjRmODgwYjgwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 438

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/wnu&amp;uvk=1'" />

<title>Redirecting
...[SNIP]...
```

3.6. Strict transport security not enforced

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

Request 1

```
GET /admin/account-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InV4OTE5WVZTdkkxR2Z4NWdlV0kya3c9PSIsInZhbHVlIjoid0Q4OTZQNXE0dGpubXBiN0xtVkdpdVFqR1NzTkJaTnlBRGpNUlVHN
DFISitwbThMWGR5OFZnV050UlNSb0hmY2wxbzR3dEo3Tjk1aHFDN29Ra0tPT1JCdXEyVUxBRDVVclZhWkNYNGJWcjdDZXZoWWhGYlE3Mkx4amNrS2o0TFciL
CJtYWMiOiI5MmRmZDlmNWNjMjlwODUxNGViOTQ0MmEyMDg1MjY1MDYxMWZhOTQxYTlkMDE2NDYyZGU3ZDUzNmQxZWUxYTY0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:20:34 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlhvMTlwenBOWjdQdGpTNzBtTEJBNkE9PSIsInZhbHVlIjoiNXlSQ21ieG1GSk05b2VJdnlUZWVHZEZIakdBNkFraTJlR20xWmY1eXl
aSTZ1YUtQZDNDUklPTTdkN3QvM3hSbDZaZERlWFBYQ0tnZkhpSEtpdW9NQW5MRnNtajMxbXJ2NklPK0dkZ0M5ak4yOHFLbWlXbFQyN2lhemliOFlEMEwiLCJtY
WMiOiI4MTY1ODQ5NTMyOGRhNDEyZGE2N2Y0MzQ5N2EzZjg3N2E2ZjdiMDNkN2ZiY2M5NmYwZDBjYzJlOTU0MDliZGExIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 13:20:34 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 82614

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4. Informational issues

4.1. Cross-origin resource sharing

There are 80 instances of this issue:

- /admin/account-type
- /admin/account-type-category
- /admin/account-type-category/create
- /admin/account-type/create
- /admin/admin-type
- /admin/admin-type/create
- /admin/atm-location
- /admin/atm-location/create
- /admin/banner
- /admin/banner/create
- /admin/blog-category
- /admin/blog-category/create
- /admin/blogs
- /admin/blogs/create
- /admin/branch-directory
- /admin/branch-directory/create
- /admin/contact
- /admin/contents
- /admin/contents/create
- /admin/dashboard
- /admin/download
- /admin/download-category
- /admin/download-category/create
- /admin/download/create
- /admin/faq-category
- /admin/faq-category/create
- /admin/forex
- /admin/gallery
- /admin/gallery-video
- /admin/gallery-video/create
- /admin/gallery/create
- /admin/import/atm
- /admin/import/branch
- /admin/import/store-atm
- /admin/import/store-branch
- /admin/interest-rates
- /admin/interest-rates/create
- /admin/layout
- /admin/log
- /admin/login
- /admin/logout
- /admin/menu
- /admin/menu/create
- /admin/module
- /admin/module/create
- /admin/news
- /admin/news/create
- /admin/offers
- /admin/offers/create
- /admin/popup
- /admin/popup/create
- /admin/press-release
- /admin/press-release/create
- /admin/projects
- /admin/projects/create
- /admin/report
- /admin/report-category
- /admin/report-category/create
- /admin/report/create
- /admin/reset_password
- /admin/seos
- /admin/service-category
- /admin/service-category/create
- /admin/services
- /admin/services/create
- /admin/setting
- /admin/team
- /admin/team-category
- /admin/team-category/create
- /admin/team/create
- /admin/training
- /admin/training-hall
- /admin/training-hall-bookings
- /admin/training-hall/create
- /admin/training/create
- /admin/vendor
- /admin/vendor-category
- /admin/vendor-category/create
- /admin/vendor/create
- /admin/vendor/import

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access. CORS policies on pages containing sensitive information should be reviewed to determine whether it is appropriate for the application to trust both the intentions and security posture of any domains granted access.

Issue remediation

Any inappropriate domains should be removed from the CORS policy.

References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

Vulnerability classifications

- CWE-942: Overly Permissive Cross-domain Whitelist

4.1.1. https://adblbackend.peacenepal.com/admin/account-type

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:48 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
```

```
adbl_backend_session=eyJpdiI6IitCb0F3R2UrdWZHZm92SHlsZHM2Y0E9PSIsInZhbHVlIjoiV0kzSHI4akIGTWJtQ1cxY0RFTEtwZTFOWlptNkVJMVNBdm5KUEJ3L
3lOR3FDc2dmdEQwdUNCYmFnQlpzZ29Zd2xZT0VGVU5aMU5EdStWM1VZdEs0SXN2TUYvbWM5MzlaaDhJV2FEakVJNFdFYW5kMXBld00rQy9EVks4aXdHZVAi
LCJtYWMiOiJkY2Q0MjZjOWI5MWNmNzc2OGY3YTA1MjA5ZjQwZGQwMDJiYjBjM2I0NDk2NmFjOWMwYmQ0ODEwYzJhNTFhOGU2IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:59:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 342418

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.2. https://adblbackend.peacenepal.com/admin/account-type-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:49 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ikl3OXlvWUl5cndqUTduanBia0JpNFE9PSIsInZhbHVlIjoidE5OQzVZVEVPWFNPWVNJUlBwU0l4dHF3WWdkN1lKWEYycm45U3N
GbzZScG5hL0pDNGFXZU5ZS1VzZnM4MFJqZnorT0xNUW9pbktRelVqYnNRbjRZL2JpbEUvWm9aV3JNZzluQ0V4L2tEWXZDNzV6UWlWS05ibTR2ZURZbW94OU
oiLCJtYWMiOiI1ZDMwMGVhODZjN2ZkNjBlMmIzNjM0NTljOTNjYTc0ODk3NzE4OTAwM2QzMmI4MDM4MTZkMTI5ODk5N2QyNGJlIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:59:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 371544

<!DOCTYPE html>
```

```
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.3. https://adblbackend.peacenepal.com/admin/account-type-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InI3Wi9nUTJsczJqbkpoQzNNKzExeWc9PSIsInZhbHVlIjoiZDhCYk42MERkck9NankySmRlYjBGRTNkSFEvODR6Umg4cFRsUlFuU
0lFb0UvMlZqKzdGeC9HUHEvWEZycitZR3k1ejFkWXM1b251STBuMzRrN1U2YW1UNzVwSjdrNHBPQzVNM0ExUG1waWJ1U0w1eENzazZlSFFoMmRlMnlUY0MiL
CJtYWMiOiI1YTA2MzFmOWNmYjk0MzgzMmI3MzgzZTc1N2M3NzgwZDM4NWQ1NTdjN2RhODFjYTA2ZjcyZjk1OTRkOTRjNzQ4IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:59:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 85753

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.4. https://adblbackend.peacenepal.com/admin/account-type/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/account-type/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Im8zZjRsQ0Q5aDEwTVpSVGhlRC9PaFE9PSIsInZhbHVlIjoiTFlXSFNNNTI6aUZJU25ucWRJdmsvUFZuSk9lZUlqRVlVenFsNmV5M01xKzdJZy95RVVaVlUrRlk1UjhEaVZkdmlKSUhndHk4Ung5eGdjb05ueWhpcFBXZS9aMnZyK0w5VUtGSkFIQU5qYmppQVRtOHkzQlFzTDlDTm9yNjA2YzUiLCJtYWMiOiIwYWRkNzE0YTRhNDNlNmQyZDE0NjBiN2JiNjc0ZTk3MzllZTdlMjAxY2UxZWU5NjgwMTFiMWRhMTE5ODAyNWQxIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 13:59:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 99720

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.5. https://adblbackend.peacenepal.com/admin/admin-type

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/admin-type**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:49 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ino5Rk9IWS8rVHJiT2E3ZFhTU0lhcXc9PSIsInZhbHVlIjoiUzV1ZmQ5NW9kdjE5a2dheld5RDVLWVZHSmFjb1lkUlhIbURUNGNWa1F
EMnNMbXlFRDZQdTNEcnNlRGZMYWs2d1o5L0oxZzZZUWFWVWh4cEV0bnZTZWViVGh2aTVYWnZnWGpVelpMV3hLWHlxRFpuS3Z0Y29mVGplbEVXNjVGUWk
iLCJtYWMiOiI5MjYzYzg5YmE3NTk0NzU1Njg2OGVmZDdlOWI0ODUwNjYxOWVhOTY3YWMzOWRjNWNlN2FhNmY0N2RlMjU5ZTE4IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:56:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 74260

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.6. https://adblbackend.peacenepal.com/admin/admin-type/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/admin-type/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/admin-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/admin-type
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:50 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkdVbS8wb2JYYUd5VFJJN0dZcDlzNUE9PSIsInZhbHVlIjoidUs1U1hKWFJEVmppd0FibFhjU3pWVUg4dFJVQmNjZGtxaFpwU2w5
WndZOXdUbi9FMnBBa0ZqSXA5d3hhcHpqUUdDcHZlZTlrY3k4dVNiWnJkRVpjNi8yam9wblJCVWhiejdrNExhVkJwYm5EZDBaN2ZsRnprU2MvN25MemdEeGoiLCJt
YWMiOiI3MjNhMmJjNzAxOThkZmNmYzU0ZjgwZmUwNDFlMjI5Zjk0MjQ1YTg4MGQ4ZmZlOTllNGNmMmQ0NjIzMmE4MGNhIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 13:56:50 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 64579

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.7. https://adblbackend.peacenepal.com/admin/atm-location

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/atm-location**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/atm-location HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:57:43 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IndlZG5iRGpiWWRCeUtYUC95S1ZZMEE9PSIsInZhbHVlIjoiQmM0eVV6NlFnYmkrSVFCRENTQ0hqRWpZdU1ZWFVydnRuWW03
REkwRHc1RDFlY0tOQmltOXRnUGVEZERiS2R2SWQ3Y0hQY243V2htK3FEZ3EyeGFteWlwUVpvQnZBeEJNYVNNMVhpWGdJZjA5R2hLM01vRXdsMndmR09IdD
RRYmciLCJtYWMiOiIxYzc5MmM3MWI1ZDUzNzcyYTQ4MDUwNzhkOGQzZDc2MzZlYWNjYTAxMDhhNTlkYmVhYjBkYTViYzA1NTI3MGM5IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:57:43 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 78545

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.8. https://adblbackend.peacenepal.com/admin/atm-location/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/atm-location/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/atm-location/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/atm-location/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:58:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IldVcThaR3dMVzFEYkhUVG0xN1d2Ymc9PSIsInZhbHVlIjoiU01GSURjQnNrclJyU1lEWGN6ZjdZRGV6MlgyMmRkTFNlMG5GUElwc2k3K2JQbEkycnpqYTRkNnRqd3FlNE5KdnNrNFkyU2RSSzhCQ3RJb05mY0ZjVVZWSEZFcGFXNmR1dnQ4N1AxSGVleFlBb09lQ2pMbE1tQVdXZmtNQ1IwMUliLCJtYWMiOiJlYTE5M2YyOWRiZTIxOTc3N2Q0ZDk1NzI5NDhjMGQ0MzkzODZkYTA5OWJhNmRhMTU2Y2EyNTc5YjU0Yzc2MDE5IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:58:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 90998

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.9. https://adblbackend.peacenepal.com/admin/banner

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/banner**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/banner HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:57:59 GMT
Server: Apache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImNmNDZ2UEdjcHhlZW5LODRON0lwS0E9PSIsInZhbHVlIjoiWG5DYWgwQTFaNFFWMkZHWi9XTDVsM3lPYWg4RXNlQVIyU2h
mUVpmSExITkFaQ0pyUmpwdzlGcm85NlpiczJHOWpIcFZNc0l0Q21nRU81dmhQSGp0dWoxR2l4UFpVWkZIUElnRGlIVXBOcTVjYXllaEVNcW9zdDZGeTZ2OGFX
WWEiLCJtYWMiOiIxMmE0ZjQ2YmMzMTBlZjkwMTQyZWFjY2UwODkwNDhkYjgyOWNkZWQyYTQ3OGI5OTc1Y2M0YjVhNTZlNjAzMjE5IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:57:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 79399

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.10. https://adblbackend.peacenepal.com/admin/banner/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/banner/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/banner/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/banner/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:05:26 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IktDTzdIaVNsd2I0ZkxOQXk5WnVkK0E9PSIsInZhbHVlIjoidnZaeC9hMWszT1FnbGwyWUJJTUZ1YUlQeit5emU2RVdZVnRrTVpMW
GRzUU93aIIxTy84MkROeEZyMmE5NFBMMUh1Vk9DUThwVWxsYmlzTkZLYld0VmZvVXViNjduL1JzZFN4SEZXODdmY1IyREFSajlHLzFNQTRkTjUxa2RHeFYiLCJ
```

```
tYWMiOiJlYjc1ZjRmOGUwMGQ1MzQzNTFjMDViOTEwMGExY2FiMjNjZjcxMTQ0NGU5NTUwOGViYjBhYTllY2NhNjY1NmU0IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:05:26 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70890

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.11. https://adblbackend.peacenepal.com/admin/blog-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blog-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blog-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:41 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InFDMXpvMmYwbDNSWE9HREV2aG9vM0E9PSIsInZhbHVlIjoiU2s0K29EUjBOcU9EbzZldDBxWEdXQjdEdXdpTmp6Nm5RTnQ0
VGtHV0tDVWVKRklRTURGZ2l1ZVpQblVydUl3WnV4WTZKYU9aeTYxdkczWG4zRzhnZFpYWHNEYU0yM3gyVlZHM3RVYUhacnBCMFhGUXJRNTNUL2t0MHBG
UWszM2oiLCJtYWMiOiI2YjdjMDcyYzA4MmY4YjRhMjFlOTk1YzRiNWM3ZDYxNjcxYmI0NzU3MmMyODRmMGYzZTVmZjIyMDFiNjlmODM1IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:06:41 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71451

<!DOCTYPE html>
<html lang="en">
```

```
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.12. https://adblbackend.peacenepal.com/admin/blog-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blog-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blog-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blog-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:08:52 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxzeElkVDdkbkkyUHN5TjNXdVc0TEE9PSIsInZhbHVlIjoiV0ltWmluZFE4aW8wUGp5SENFL3UreXUyL21qVzB1L2FEQWxXSk1veX
dkdnI2bEVOaFlLTytpQTZSZlQwOUdhVGdFcHJoNVFvZCtVK1I5WXlBVkN4OE9kU0hWNnB0K3dkU3FBOC9yODl2YS9qejlQL3Q2SjVLN2diUVM2VlBvZkliLCJtYW
MiOiIzYWRlN2Y4NGM4YzIyMjk4Y2I4ZWQ5MDJkYWI0NDAyMTZlZjcwMWE5YzdkODY3YzQ0YzM5MDQ2NTVhNTlhYTQ5IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:08:53 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 67441

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.13. https://adblbackend.peacenepal.com/admin/blogs

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/blogs**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blogs HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:38 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImFWZFhnV0tsT2VSb2tGODV6T20zVkE9PSIsInZhbHVlIjoiWndKaGd3bWx5Z0szdXBUakd6QmhNL3VhYVNGSGFtWm1zMkxmcE
Z0QjFHU3U2Z1ZpWjZVVlp2QW1wVVFJRkdsaFh6VmlqczRiWUpmdmo3UFZMZzRDNzZaSHkxQ2psZ2VHVzZ6TWQ1S3hqOGZSL2lLaFJSNGh2aDhXaEVUWS9X
UHYiLCJtYWMiOiJiNGJlZDgwNjNmYWQ0NGM2YThiZTkxMTRjZWQ5YjYyODkxOWRkN2I2NTMzZmQ5MjA2MmZiZjJiY2I1M2ViZDY4IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:06:38 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 104431

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.14. https://adblbackend.peacenepal.com/admin/blogs/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/blogs/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blogs/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:12 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkE5bEFLdk5oWkV4QlRBSWxTcU8wM0E9PSIsInZhbHVlIjoiSEIzQ212LzFIWHdYQkNzTEx5Ti9nakthbjhnL2lPNk1pa3dYUjNoYlY5
Sm9VdER5Q2hkQlVGaEJrclBFVENWdWRDSTRFSHZnS1kzTmxUWFFTV3R5WXhrR1R1Mk9PbnRxdEZjbjloYlhwT1cwUXBoc0RNYkxnR3pWVExpRm44ZHQiLCJ
tYWMiOiI5ZTM1ODA2ZjM4MzlmMzY2NjMyYTgyYzZiNThjZWJjMjUyMTI0YTk2Zjg0Yzc5MzIzNDk0YzQxZTAwMGM3NjgyliwidGFnIjoiIn0%3D; expires=Wed, 02 Oct
2024 14:09:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71863

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.15. https://adblbackend.peacenepal.com/admin/branch-directory

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/branch-directory**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/branch-directory HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:01 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxOQlpjNDA3OWVZSEUxdmg0RmFpc1E9PSIsInZhbHVlIjoiY1Q1aVdYSnJTbURCUDcycC95ZSt3Y2U4cE16eGNYQTJsbFVvL2l
OWVcyZmsxY2liK1dEVEpLYmo5enA4bThRMFM5ZkJFZk0zeXkvKzJzUVpkWm52ZnpKWGVBK0lTZmRNTm5NYjlKL0J6aUZESkdkS1d0RTRNUVkvU3NTeTB3N0
MiLCJtYWMiOiIwMWI5MmIwNzEwY2M1OGQzZTEwZDQxZmM3OGY1MTA1YTkzNDA5NmVkMTg0MzIxMjFmMTQ0NTZhYzQ3Mzc3NWZhIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:06:01 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 76632

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.16. https://adblbackend.peacenepal.com/admin/branch-directory/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/branch-directory/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/branch-directory/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
```

MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/branch-directory/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com

Response 1

HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:07:41 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InN5YnpkRXVsdW9FT3NKT2FuRW42Rmc9PSIsInZhbHVlIjoiaTh5WGJURjhrTnRrdURyTGpBNDNDU0pSaDNZM2RFZ1hGSzA2Wm8xUTB1Ry9XWStGaFZETkY0QUwxL0YxTWVLZzhVUDZLYjZRcHJ0VHVIQzIzZGNaVWZkY1IyT1F1U3FqQU5zZzhWaFAvYUQ0Ympnd011UEUzS0VrWklMMmVsNnciLCJtYWMiOiI4MThiMzZlMjFkOTRhZTEwZGNmYWI0NDliMzkxZjU4OTk4NDM1NmE5NzdjNjgxN2FjYzQwMjdiOThjOGMzNTU2IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:07:41 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 95114

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...

4.1.17. https://adblbackend.peacenepal.com/admin/contact

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contact**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

GET /admin/contact HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:10:12 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImhBSW96TWk4cWVJb05yL2s0Y1FYZHc9PSIsInZhbHVlIjoiU0RrZE9RTGZXVEVESyt4TXhPWkhLWDZwc2ZiUC9DYm93VVdOS3dlcG9DSy8vV0wzenA0MDQrdk5jMWJUWmNnSmE2NFR3S01UeWNndlhyU0JFVjRHaTR1bWZmUmEzVGJoUEhxS01ybmY1Slhva0VRK3RvSTBuN0VXUTlZYzFlNG0iLCJtYWMiOiI4NGQwNWUxNTlmOTJmOThkZTM5ODg3ZTc1YWQwOWI5ZmU1MmZjYTJmMTNmODBkYzE3YjM0YjZiZDA1NTQwMmM3IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:10:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 170263

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.18. https://adblbackend.peacenepal.com/admin/contents

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/contents HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:28 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
```

```
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlE5cTZPa1ZLR3JMbVNqeGExczd5WkE9PSIsInZhbHVlIjoiODgzeGZKVk1IL2xlb09aNzJydWhmSzRFTm4wUnZKbHVMTVhuRHM
1UjdEd0VWdmpBSXRzY0pZblJ0b1Fna2x4Um45dVZ0M2dPVUN1QVRETnQ0SGNjRkxzRjBwRUNLcmRrTmRJeFlDVXZFWHZVNGRuTkJCWnY5MW15U29JTHE
wZVIiLCJtYWMiOiI2OWQ5YTM3NTc0ZDdhNDYxZDk0OGM5ZjU5OTBhZDFlNjExZGY1MWIwM2M3MDIzOWIzZjZjZjU4NTFjZjVhMzU2IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:09:28 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 242545

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.19. https://adblbackend.peacenepal.com/admin/contents/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/contents/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:43 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InFxSWdLTFNNZFFtSVFLdEUvdzRqTmc9PSIsInZhbHVlIjoiT2RtQ3N3cjlMNS84cXBNeFZ1TzVhYWtkbDdmMXVUWnVhSEh4dWU
wTlRPMkhqTGJleIrM0J4WXpCQmZJWnVrWEpwbTA3VExkaDNJWEtlVkRHQll5clczWXNVZytLdmpjQkcwZVZ1dDJFd3hvWEtBMzl0eXZqM0VNRDU3NGdOaE4iL
CJtYWMiOiI4NTk2MDQ0MTgzYzU4YmU2YjJlZTFkZDFhY2FjMTQ5NjQ0Mjg4ZTRhMzU1ZjdjNjY3OTEzMTM1ZjcxMjU3YWI1IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:09:43 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=UTF-8
Content-Length: 86438

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.20. https://adblbackend.peacenepal.com/admin/dashboard

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/dashboard**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/dashboard HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/login
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:10:30 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZlZktvZmhjTXNvak54RE05U2ZWZ3c9PSIsInZhbHVlIjoiSnpRM1lRbmNtTVRzRFpBVTdjNUF1ZXdDMDYrdGdxM3ZLR3cxeFVTN1
lsV2ZhSXNjRFBpT3JuK3RjTWhGamU4cEIrL0diRDI4SHpFZzBjeW51MEI3WjE4a2p6OW1DanpJWGVzRC9pWFNrMk90TXVGZkxKRVd5V2dDNEtzdm9TUysiLCJt
YWMiOiJkMWIxNzYwMDM3YzZhY2M2ODdmZDEwOWE0ZDc4Mjc4ZDI3OWRhOGU3NTcwZGQxYjM5Y2U3NzczYTI4Y2U5ZWY2IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:10:30 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 69665

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
```

...[SNIP]...

4.1.21. https://adblbackend.peacenepal.com/admin/download

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/download**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:11:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ik03MER1YVl3emlzank3Wm16d0dzSXc9PSIsInZhbHVlIjoibmxZenlRYnRFZEtLa1NZbEF1cnAxbnFMVy85YVRnQVJnN2R2QmlvV
Ed4TnN1cW56MHpFRDJvOWIrcVk2OEtxbUtZaE5BME11cExKTXd1SzNFYnYyMjJsdTRjNU1ieTUzWlJpdFVvKzBtY3Q1RVhvK1pieDdTVExlcm1LdTliVFoiLCJtYW
MiOiI0ZTIwYjdmOGQ5MDI1ZGIyNWQ3NTBlOTlkMjVlNDdjYzdmNzM4ZDAyZjJjZWY2MWFhOGRiNTY3MmQzOWYwMmIzIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:11:07 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 90495

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.22. https://adblbackend.peacenepal.com/admin/download-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/download-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjBZZlY1RFlUYmZnRUxMTkE5UFZjdlE9PSIsInZhbHVlIjoiU1JXZGhpRTNFYUd0NC8xdW9sNlNkZjVuZ3B0MUdMSnpzdlRFVTV0dzRRcVV2WkF6OVRTeXdYUWtoazJLZ1RKU2VMQnRtMTVyZTRRY3dxRXhLWjhXdDdyb01kZFR2UjJZSEFjeDIlb05ESExnSzJVdUpUSXh1K0NUK25tUWRESXoiLCJtYWMiOiJiNzlyZjZhNWQwM2UyNDFkMTgxYjExODViYmNkMDZhZDkwMjU0OWEwNzQ1NGRjZmYwM2Y5NDc0ZWRkNTc3MzM5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImdyZU9hZDVLWnBCV2RJNk9MMXdFeGc9PSIsInZhbHVlIjoid3BJcnhZWkVwcDZXNjdkV3d0SW1ScXVKZi9xS3UydHBSK0lCbDcyWTFvdzRvb3h1ZTJjV3JQbm5zNSs0NzhLZURXQ1BoaFFsN0FEdVRyMlZGYmtvN3NFUklrT0l1cnlldEVYN0V5NTFIbUtMaldBbUV3dHd6QjFJR2VyV0VtSHgiLCJtYWMiOiIxZjFiMmIyYzAzODZiODFlZWM0YTNlMjVmMDdhMGVhYWEwYTcxNTBkY2Q4Nzk5M2MzN2UzMTRlZjc4Mzk2ZWNjIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:05:19 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.23. https://adblbackend.peacenepal.com/admin/download-category/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/download-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IktjTWtyWjI0VkFJMmJRTS9jbzhJVnc9PSIsInZhbHVlIjoibFIrQU41Zm93UXUxSlZuTHI4UStLaDI2YW1Rd25ZOFI4bzBySHJvY295ZHI4T0NZNDJhbWh6RzI3dVNRY2ZzM3hDbVA4S1k5U215Tk5DbnpGWU0ycnlnTFgreXREOTg4OVA5U1phMURQWW1EODk4ZTVIVngxVDVjSzkwOGdha0UiLCJtYWMiOiJkNmY4NGJmNjViOTcyMDIxNDU2MjNjZWEwZTA1OWYxYmFiYzY1ZjI3YjU5MjhiMGU0NGNiYWQ3ZWExYjVkNDEyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/download-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:52 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImhiZlJNc2ZQOHU2cXZWWFBpS292ZXc9PSIsInZhbHVlIjoiS0h0Tzdnd3NSa3Y0YUxuMmNPWk9ta1p3MUJhWnJGODRCYy91am5YUFFxdTJQeENDNUlpc3FrUWlBVGFQeEwwa3hZOUNhdlFHNWFKWnNrcjgzWHVVdHdCTWJnV3gxdzltamhIYzBmVFcyRmhDOHA0OEFNeEloSVNoc04rTW9GNDUiLCJtYWMiOiI4ZjlhYjNkNjU2YzIxMTAyYWEyZDA1ZmQ2OTNkN2U3YzFhNDYwMjQ0YzgyMWU1NDU3YWZhNzMxZTA1NDAzYjVhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:05:52 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.24. https://adblbackend.peacenepal.com/admin/download/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/download/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InZ6NENzTEJaeU51MUZ3NzV4UkxWK2c9PSIsInZhbHVlIjoiWjkyWk03a0Y2S3k3S0N2WTVZRFA1a29MNEU0c0d2QTdTWGFyMz
```

```
VHMlRvU0Fya2g3bWY4MDdqNXFPWlJQSWUwVHA3WERqa2xad283T29vRVBNRENHYTZTV0JsMGNBbXNmeUkybGMra2k1SXdRdjNxb015UVd1QXBzcXcvY0lsUXliLCJtYWMiOiJmMGRiZjlhNWFiNWQ4MDUwMTdmZGE1Njk1Yjc1MGE1ZGM5ZDU0ODhmMGUxMWY4ZjNhMTQ4Zjg2ZmFmYThmYTcyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/download
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:27 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjdJdE9PQjNXSlBmVnNDQW1ZM20xOFE9PSIsInZhbHVlIjoidDZkd3plU2MxbjExZmlnSDJ3TDBtQklZZmNIQlZBRWRFZjJYOE1Vd3JJZ3cxRnJIUll6VWpJZEtCZWR6UjRtczlNTmZjakhNNkF4eHhRTnozM3k1MjFDSHk5YmpnUmthcFJmY0VGdmRUUk9Gc01kM3Fxc1ZaTFdNOU5SSWNRbkliLCJtYWMiOiJjZTJlM2FkZTRmYzRlYTUwZTczN2ViMTE3NDc1Mjc2MWM3ZTgwNWZkM2NmNjMwNTYzM2M5ODhhOWYwYWY5NTM0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:06:27 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.25. https://adblbackend.peacenepal.com/admin/faq-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/faq-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/faq-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjhQWXNtR0Q2MVY1Nit5R1hjWXY4anc9PSIsInZhbHVlIjoia0N2V2plYjBqbGRFc29zRUlDRUxleFg5VUtvaFduaUtUWDNzdXlkZU5OUEpNWkQvVlhzS09oS2x6RWdOaVpjeCt6QUtrQzNLMU1DUzNlSFE5MGxZdDh3L3ByQnlnenk3bkZiRTJwaVZZQlhOampQUENkdG54RStPT1ZER2tDTTAiLCJtYWMiOiI5N2U5ZWY4ZmI0ZWNlMjA2OGJhYzliYjE1OGNiNjgxNjRlZTA2MDNhMzY0Y2E3MDE4NGY2MmExMzY4Y2FlZmY4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:23 GMT
```

```
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InRjVmNBWEpPOTFVcFNuMWlqd2lWc3c9PSIsInZhbHVlIjoiTmNiUUJjeGlLY1laQzdSNnhnUDdrOURnLzVIY094ajJLTHdERlhMVk
RYaE9ldWJiWGxYRk04ejJhWGJXdjFLclhDbE1pTUt3MTdPN3pGZTVqcUVxbDMvSzNsc0gra0x5N3lwYVZSRXduUE8yblQyTHBoR3NLSlhBWGVWOGc2YjYiLCJtY
WMiOiJkMDg4YzAzYTVmMWQ4Njc4YmY2Y2NhNmQ3NTYzNDAyMTk1NDk0YTczMTdhYWMyOTE3ZGFhNzkyYzcwMzRjNmY2IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:05:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.26. https://adblbackend.peacenepal.com/admin/faq-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/faq-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/faq-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImJvZXVMYXFGd3hhNGk3V0FvalIFeEE9PSIsInZhbHVlIjoieC9JVHRHZWt3SEZJamVWQXRzeHdLdGdJUUZ6c1RNTTVsd1ZiZjlh
ZDYzT1o2UGgyNG9xT3QwWDR1am9zYU01T1BvZnJuc3k4MlV5bEd4Z2xZQlIIOXBQWEZ2NmY3dTF4bHRwZ0g2T0Q4R0Z5KzBDdXJ0c2JGZHpaVnIzalRQeVYiL
CJtYWMiOiJhOWFlNTI3M2M1ZjI0MjcxYjdlMmFlMTdlNDk0ZjFkMTkyN2NhY2QzMWQ2MzRjZjcyOTFkMzIxM2MyNTQ4MTAxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/faq-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImZzSDcxVGZTajRIU1NLM1JWenFmdWc9PSIsInZhbHVlIjoiTk5GZjE2Q3hlNmxLeUEvVW1VK2pkRXNueksxdXBtalhvbmVyN2VUV
UVJYkEwWmhBVUVGT245Uk5RTkdiTWV5enkycnZZdlJPOTc4cDBjRmxBRVR0czVwRFlzbE96M0kwa1c3U1gzZ09KdjRhM3dra2FRZGI5T1JEMFJCdE5RYmYiLCJ
tYWMiOiI3MjBiNmVhNWNlMjVmZDE4YmM5NTgzODVmY2MyNTUwODBlNjk4ZmU3M2QxNzljMmI2MzlkOWVmMjNmNTgwNDVlIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:05:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.27. https://adblbackend.peacenepal.com/admin/forex

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/forex**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/forex HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhMMW1zVThjRkVRdlhQWWZELzNtVEE9PSIsInZhbHVlIjoiUkVLVGI1Rko3MHExdTlzNTJSNGhhSXRBME5LNUdVdXlMSFl0WWs3bHlLWm5lVURRVWlpOGZOWnVycXJTU2pSOXhRejlFTUF1UGFPM3ZRMjUrYkllQVBxbGo5aXZVYm9tMzBhSG5pUHJaS0s3SjNCVVhtWVMwL3UvNmFOQ1Mxc08iLCJtYWMiOiJkMDU4NmJlNjM0ZGVhYmM0ZmY1MDhjMGQ0NzBjYjI0NGM0MTczY2E2MDE5MDY5YmM3ZGFkMTAxODkzMGJjMzczIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJNdDRlczNwMzF1UDBBblVaTjJpb1E9PSIsInZhbHVlIjoiQjJjYThhYVZHTmYvYnMxUEhTR0RNTjg2SUZaUDZQdm91UVhLVXVhR1BJZC96OVg3SjVjSFRTQTdVWTNiQitSTnd2U3hVanlCd3AzNUtCZHp4T0JBYlYxcDcyYmJQZlJQWjhybHNvK25xc0tHajlpSjVxZmVYV256c2grT01pQmMiLCJtYWMiOiI4Mzc0NTBkZGE2Y2IwYWQ5N2U3MzE3MTJiOGEzNjFkMzhjNzZmNjkzY2NiODc5Mml1YmNhNTg5YmRmODE3ZTRmIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:06:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.28. https://adblbackend.peacenepal.com/admin/gallery

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/gallery**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkVrbWk4UE8zMW1qS01CTHBHUFFwUHc9PSIsInZhbHVlIjoiM3Q1anIwK2YzV0ZNd3dtT2tSYXVEb0Y4WFQwclhnOVFOd2J6UXB
tY1E1ZUtJUWZRNGw5T2Iza3kvUzFCNGFSMzhtTnJsbnhlTEs2cHVnVDBTcFFDUkp1eklxQW1mY3hTdFMrM0ptbkFoYjNSeENUQkovSWxiMXF2NWxwK0p1WUUi
LCJtYWMiOiJiOTFhMzdkNTI1YmY5MGY0M2QwNTQwODI2ZGNiMGI0OTVjZWE0NDA1YzFhYzBkYjQwMjhmODExMTNlZGU1NWFhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:35 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ijg5WjFnbzJMaisweXB1YlB1TTVCWkE9PSIsInZhbHVlIjoiT1NEYXVNZEdnM2VlTEdmVUZEOWhFSnpkVkZ1QnJTY0FHa21EQ0pp
MjNQMHBWYit3azRvTVpkeGRIY1RreHFlbDFla1JPVG0xcTRnMHhlcUhqY2o4RnVobExSRHZNenJxMWpQUkc1RnFvdzR1akRtb2lpUzlYbUVWbCtPajdMc0siLCJtY
WMiOiI1YjE5NmQxYjg1ZWQxNDM1NGE5ZjQzYzYzZTM3NmQ4ODhlZTg3YzRhOThiMDk1NWZkODcyN2E1MjEyY2E1ZjYzIiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:06:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.29. https://adblbackend.peacenepal.com/admin/gallery-video

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/gallery-video**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery-video HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImwzbU9FV2oxUnpwQ1kxY3JOUzdHVVE9PSIsInZhbHVlIjoiMnh3RW1naG5EaGhxMG9tQ2g0a3BDdVowL2Y4VHdvT25rMnlISWZJN093Z1NkL08xWnlHL2t5NDQ1YkRJaGU1WEtaZnR0cUhOOFJPdFhGeHNRa2tEM0NYNCtnM2tqbUJRaVNWY2tHQkNoZmxPbW81N0lmMFZoOEtmdy9vbjBHZHciLCJtYWMiOiJkMzZjZWI0NzFhNDMxZDhmMTk0ZjNlOTRhNzBiMzQwNDdiYTkyODc5NTZiOTY4MmYzODdkZWYyNjkzNWJjOGQxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery-video/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:07:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ii9GdFJIdW1qQTdrVHpyeWtZTUpDNkE9PSIsInZhbHVlIjoiVHhtaUdDVFNaZ0FSQzhvd3B1ME1kdkJEREFTZlJtK25MOHE1L2tqUnBycmpRRlRYc0gxNitlZHRsYkJNK3ZHYk5OUW16NjViV041NkZYZnBCckhMZXhTZmhEYjZ6L1RNaGg1cEZSVEtmeVhFMEVaNVc2am0zY1pXTG9wWEdYUnUiLCJtYWMiOiI2NGY4NzY0ODZjODVmMzVhYzU5ZDA0MDU4OTNiMDU4ZmVkMmY3NmZmMzI1Mjg1YjliYmQyNzI1YjQyOTQzMjA4IiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:07:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.30. https://adblbackend.peacenepal.com/admin/gallery-video/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/gallery-video/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery-video/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImJ3a2JOS0ZNT3paZm0xWVNKUVFZamc9PSIsInZhbHVlIjoicHVjT3EzOWdLeGZHZ0tmaUVCNU1leHY1YXNYK1VUb3VEUjVoWl
```

```
NYQTM0TGlpMmd5K2NTaW1pRE85YTlDc0Y0SmkwTVp6NGZJT2JIMm0zeVFHbjRLWUZmb0Zwazg5dnJUTmI5Q0IrT0o2SGJ0aHRrdTByTjRCNGNYVU00VHJR
MTUiLCJtYWMiOiJiNzZhM2JmYmRiMTI0YzYwM2FmNzVkN2ZlMDJjNjlkM2I5YTMwMWU2NTEyMjBmYmQ4YmZhNWM2ZTQ1ZDY2ZDBlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery-video
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:08:22 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ii9HSzNJMW92c09aOVJYSjRzZ2NuWWc9PSIsInZhbHVlIjoiTG9Lb2NPTXBVZnI0R1kyQlRiMG4wVjBNY29TVzhPUTdjMXcxWnpF
V2V2SmhxcDVyZ1FWNytvL2hHbjFHblhIcE9DKzkyR2Q0Y2czZVg0L2hlcmNPcFZqUUJYaGprTVBDTTh5UHN0K3A2TE9xSmJMMnpKMnlrQWlLNDBYNHJZNU4iL
CJtYWMiOiI0ZGUzMmY2ZGU2ZDc5OTkwNzkyODE4NWJkMGM4MjE4NDY1OGZmNWRmNWUwNDA5ZTI1MjQ4ODRhNmM0NjY1YWNhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:08:22 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.31. https://adblbackend.peacenepal.com/admin/gallery/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/gallery/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InF4d3BjMVlrNTJGL24vR2poYXBCTkE9PSIsInZhbHVlIjoiZ0srZXhlY0VhQ1VTOFJFa3RQTVU2VDIzbjBPbm1zaS9HMk54akRGRE
J6QkxnaUlqT2RGT3lZNXpZTXZsaGl3MmpWc3F4ZTZDSDBieGc4RUJoWUtkcGpOK210bGhkYkNONEh5ZG1NY21UdmVFUXVVMEE2b0k0ZGJSa1NXUldkNXAiL
CJtYWMiOiJiY2JjMDc0ZWUyZDkwNzMwMDJkYzFhMjY5ZDcxNWVkYzNkMzRjOTlmZjcyZTI0NjJkMjdjNWVhMTlkY2U1YzUzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 05:08:02 GMT
```

```
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjErbWVwMmtXdGhpOG5RN01UeUxDaEE9PSIsInZhbHVlIjoiZDZDeVFsT3hGTVl0NWZUbVVaMDZkZVRCUzZwQTZYTmZWOWx
WTjdvdWREbXJDMCtUcFJ1YlZWZUZLaS91L0gyZ0p2U0RzWHErNzM2ODlONVB3WHQyU3BKcFJlZmt0UkpaNmxTOGpVajJaWHI5L2JwaIR6KzF4SEp3U25FME
szM2ciLCJtYWMiOiJhNDEyMjA4Mzc4Y2Y0ZDk4YmFhZjE4M2JhMGQzN2E3NWY1NjI3ZjQyMTZjMTA3ZjIyNTE1MjcwY2RiNTM0MjcxliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 07:08:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.32. https://adblbackend.peacenepal.com/admin/import/atm

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/atm**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNvMTh5d1VyZndXOVE0OGdFZXQyV0E9PSIsInZhbHVlIjoieThnU2w5dHI4Smt1d2pvcW9RWHpJTXEwWkgvd0E0TUQyN3RxcE
FoTmFVckR3WkZmOWo4STFXNnhYQXVVOGpSVEQraUJLbVh5UndEbDlkRHNFaDVGWmFqWTFwSCtCUCtRMVNNNTk4WEphTDRjQzVwazlETmxnWDJ3cmd
XT0pZNHMiLCJtYWMiOiI3OWNhNzQ0NmVlMDhmZDUxMzgxNDg1NmI2ODRlODcyZTIyYjYzODE4MDNmMWMwMmU2NjU2MDgzOGViMWE2NTBjIiwidGFnIjoiIn
0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/import/atm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:09:24 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjZDUUVZaERZY2htZ3hINzF1bnZ0REE9PSIsInZhbHVlIjoicHZjWVUzY3h3c29xN1lROFVVQjV2OXBTdnN4K3huRUhWSnZ2R3Zm
WCtDOU9RRWF0R0p1aUZ6QlFxMFhGKytuMzVDbVhucXlwQXkzVEpLazl1c3lBcnBiOHBlSklKd0J6UCtGejJVU0luT1VudFdHbW1VTk42SkpKM2dkSy9mbHliLCJtY
WMiOiI4YzY2ZjY2M2FlMDljYTYwNzk2NGJhYjMwNzhmZWY0N2YxNWJmYjlkMzI3NTc4OWVkMjUxYzkzYmE3MmJlZDQ2IiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct
2024 06:09:24 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.33. https://adblbackend.peacenepal.com/admin/import/branch

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/branch**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjZYOS9WNml0QUJXZ3FqL05JYStIU2c9PSIsInZhbHVlIjoiN0NzcDFnaFJ3d3MwdllpTDlZV09GQnRnYlF6YU5HZFhjcGtPSFNlOFB
RWXdJbHZmOTAyRTFCYnRWUjVWZ3NITmdPN2VNaUM0MHNNNFBvSFI0eXJMU3ZpUjVTa1VNditsQW1CblFOTFc3T0JOSUtuQkYrMnVtc1B0bVRvdnF6dUMiL
CJtYWMiOiIwMzM3OWI5Mjc3YWQ1ZDBhMTllZDViYjgzNzViNGZjMmJhOWYzYzBhMTQ0MDhlMGMxMWY4NjI1NjUzNDQ1YTlmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/import/branch
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:09:28 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlhDZFBkNG5pM3ZneDJVOC9iTWRBL2c9PSIsInZhbHVlIjoiR1gxdWpyQUcyNHNqcUZyd0oyKzFZOHRRZ3NPVTl0bm44d0RmTzN
QczNkOXVIRDJ4ck5qbHM4c0YyMWJhR2Y3S0tzUE5LUkJKb0dYVXZnY29hSDJnaHpLckEyeVRvdVV6SERVZDN0SzZwZml1UmpidWFjZlB0a2hacE1mQVZ4UHYi
LCJtYWMiOiJmMzZmOTAyM2JkZWZkNmU5MjlkZGRhMWE4OWE2MzEwMDFlMmVlNzBhYzI2ZjI1OTAzZTU5M2I5N2U2N2RiY2ZmIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:09:28 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.34. https://adblbackend.peacenepal.com/admin/import/store-atm

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/import/store-atm**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:12:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033046

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
```

4.1.35. https://adblbackend.peacenepal.com/admin/import/store-branch

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/import/store-branch**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:13:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033068

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
```

4.1.36. https://adblbackend.peacenepal.com/admin/interest-rates

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/interest-rates**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/interest-rates HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkpRdy80UGI0TjhMcnZVZlVlTmtnSEE9PSIsInZhbHVlIjoiQTRyQWxzVHpOK1dMTmlhNVNINmdpTFZlWGEvMHVSN2lmNGhWaEZ
SRExDK01uTW1GSFhmcGczMVBpaGR5VjQxdWlTNnJ2VXZqUDJZbXgwUHQydTRHRksyZ3dsNXZaTWNCTG1VbFA0eFU0WFRja05iVUZGZXg5eTZLeGRhdUJ
WNUIiLCJtYWMiOiJmNmQ0NjY1NmNjOWNkMGI2OWI2YmFkOTcxOGVhNGRiMzViNGU4MmVjNzZkNzliOTRlNGQ4YjhjNzBjNjExNThlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:13:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Iml5TkVlL0Q0Y1VFaE1EU0FCOUphblE9PSIsInZhbHVlIjoiMDVPY255UjlFWE1JNHFGOEhxN2t0SCs5bk5WcEkyYVh6c0Jvd2VxR
FhBZkZzWXVodDVZK0Y1T1FHTi9MZWxaSEhKZkJPWjJ3YlRlZURMWkJyZTJObUNaNXFTWEozcVE4SHg5ZDE1SGprSXRsTW5qU3R6YndJaXhlYk12RHNLWm
EiLCJtYWMiOiIwNjEwMDc4Mjk4YzA2OWViNDQyZDdhMTQ5YmY5MmY4YmNiZTQ2MTg5MzAyYTFmMTc1ZmYwZDU1NmIyZmEzYTVjIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:13:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
```

```
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.37. https://adblbackend.peacenepal.com/admin/interest-rates/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/interest-rates/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/interest-rates/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkxQcnlzeWVpZXpJdTduUERNejNNMnc9PSIsInZhbHVlIjoiVUhxWFY5anBaMlNMMi80R2FGaFpFazNxUUpuait3ZTY0TzB0RnowbE5LbzRCRSt6ZWlUNXVFY0RKSVgyV1ZqYUVMQnFkSXJhajJ3T2lkdzlDdnRMaVlpMkV0N2tXQUUra1M5YW12K1FBM2d5ZXBOb3Y4bVhqUGJ1cUJQTzlFMDUiLCJtYWMiOiJiYmU2Y2M0YWRlNDVjNzRmN2JmMDE1ODdmMGJkNGZkMjA1ZjlmODFlZjUxMjIzOTZiYmYzMWE5Mzc2OGQ4ZDI4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/interest-rates
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:15:37 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImRINXVXRDFPR1Y1UGZkSTNqVjlWVVE9PSIsInZhbHVlIjoiaUx6TVdEeGZ1U3JhZmZGV3UzUnNaNGlLZ28xTXZtMFBoL2tnVUU1YXpucCtxL1Z0YlRZb2FzdGxHNnRuUEwvcXNHRGJHNFZOQWJ4L28xb2pGbnZJcXltYlBWS3haL3NOdngzTytkcE1zRUpwWVFoSklSEw1eU9HMFVvcFJQZVciLCJtYWMiOiJiNjYxOWQ4Y2Y2NDhjNjExMmYyMzM0YmUxNDg0YmE1MjkwMmIyYTQ3MjlkODEyMzVlZDJmODkzZmYxY2IyZWFhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:15:37 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.38. https://adblbackend.peacenepal.com/admin/layout

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/layout**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/layout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFwQ01Kd3pHSE1EWUlYMXQvMXJjalE9PSIsInZhbHVlIjoiZlNBSDdVQXNIenZWSS9CRHl6OWRRVjZTeFk2UnFkMllmODIzajVral6SXFNbUNvdFMxVzdaSUpyL2ZTQXB1bjNKNGczRVpvcWY3d1VTUG5lTWxyM2xHT1Y5WGJhSWd6L3VWZ0U3Ulk0cTVqTENiSitsTjdtd0JhMTBma3ppTWIiLCJtYWMiOiJhMjU4ZGQyZGQwMjU1N2Y3ZWQ4Yjg2NjVhYjgwMTgwN2RlZGQwYmU5OGI0OTFlODU5OTIyOTllODYxMDUwZDdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:15:30 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImdDRy94a05Iak9MdnFKc3NicDh3R0E9PSIsInZhbHVlIjoibGlTQlVWUnd3bVFxZkNlOTl5empQSlhrTDZ0ejFmYklyTFVYSVk3NmRqUDdSVFZhaTdwRFpJRkJiSTQxbm5TNE5UajJuajRBVEdENUp4c2Eza0xnYmhjTWlLQTY5c3J5c2RMOG9hWnMxYnVJSysvV2o1WHducm1hT0RoRjRLYU8iLCJtYWMiOiI2YTM2MGZhNjUxNmY2NzVhNzY4MDNhOTJhNmNhMTQxZDFhNWMwNTRlZjNhNGE4YjE5MWM2MzllZjI1NzkyNTAzIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:15:30 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.39. https://adblbackend.peacenepal.com/admin/log

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/log**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/log HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFBL3hGSVhBSEM3d1ZUcHpLd2ZjYmc9PSIsInZhbHVlIjoiekFkZmlUdC9ZMG9RSXRWdHUyTGJQelFna2YrMkEveE9hQ2trNi9ia
nE3bk1iMFZ2cnQ1eC9MdEtHbTd5YlhaeXVRdmtUbGUyV29SU1NjNGFCMEZJWks1SkNUQ1lsWG84MlN4OWp1bTJ5aW9mWDVzQUkyY21vU2gyUVE5U2JPSFgi
LCJtYWMiOiI2YmE2MmJjYjNhNGY3MGM5ZGE4MTNkMWNmNjI0YjJkNDdkYzUzYmE4NTg2MzI4ZGE4NjNiMmZhMDA2YjZhZDVjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:16:38 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ild3NFRLclhYQS9TUitYU2NSM3Y5Qnc9PSIsInZhbHVlIjoiZ0dpNXNYcEJWMHpIMS9sZVJWZjFQTVA2Q2VVQVJSb0gzM0JnN29J
Mm11RjZjOGJXamdXZmNPWVd0dFFHTWhmZUxuaVpkcWZGeDdZRG1sRmF4T291WGc4WUpLVmlncDA2bTB1bmp1MHZkdU1kclp0WlNoTUpMZ21PdzlxV2hlU
kgiLCJtYWMiOiI2YzY5ZmFmMDkzODE1MTY0ZjhhZGYzNTNmMjcyZWVjOWJjZjNjZTk0Y2NhNWNlZjVhMzRmOWE1YjE3NDI2Mzk5IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:16:38 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.40. https://adblbackend.peacenepal.com/admin/login

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/login**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImE2ZWlzaDBsSVJpR05HN2U0VU5oSmc9PSIsInZhbHVlIjoia0lRSkVENm43UU56QVdMRzNDTFJDemZvNm9OQ1plczhKbUNaU
```

```
mNJV0hnM1FtTlhRaEw1ZThJbHhXNnJlb2l4ZzZVaUo2VlRkdWcyZ2IvcGlGbitGOGpyWFVGYU9GcXpnd3ExaG1ueVlRMGlTbVVmOVBRbTNGalhCalBha2RpQzAiL
CJtYWMiOiJlNjExOWUyNjQ3OTVlYmMwYTBmNWQ5NDU2YTBjODE3NzkzMTk0M2EzOTVlNjdjM2Q5ZjhhMWE1N2JhODg1MDMzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/dashboard
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2024 04:16:23 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Set-Cookie:
adbl_backend_session=eyJpdiI6IlE0a2tGNlMzOENPWW5QSGxZajIvdWc9PSIsInZhbHVlIjoiR1JRazZYNDZsRzVZZWVKclpNazFMMEJUb1VvZnh2YUxHdDlMZW0
2K1hyWS9WYlR6TmFDeGo3MGVkTkozcVNXVjlEcHBQVVhqL2lYS3AzTmd3azRuZERneis3aE5ycFdaWHVDRjhSY29IZHM1R1VIS3B1T1UxUFFyNzRxemtySEwiL
CJtYWMiOiIwNTMxZTg0YzJlMDRiOWVhZjdlYzdiMzA2ZjNjM2UzOWZiNDljYjFkNTBhZjNlZWMxM2NlOGYxMWQ2OTcyM2Q1IiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:16:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 7097

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.1.41. https://adblbackend.peacenepal.com/admin/logout

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/logout**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/logout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InpsUTZzNFpISXJRVXZBS01wbitUWmc9PSIsInZhbHVlIjoiajNUMm9NSGQ4cDBod3JzZ0hWbUxPTjJPWGJiSVdScnd5czZKejQxS
FNsNzFlb1F5T0dqYlhycU1IUlNQWm5LRld2MjArZndsRDNKU3FYS2htVWdWZGJTdy9hcVFCQnRRU2NLMTN3VnJZanFqY2FYMXp5cVM4VWVTc1c4WkVtaXliLC
JtYWMiOiIzNDBiMGI5YTM5NDc4NDg4OGM0YTQyZDE5ZTRkZWQwMzE4MmY4OWFhYjk1NGQ1NWY1NmUyZWQwNWFjY2l1MmFiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/dashboard
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:17:41 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImVONmdnMk5FTlVjWlMwZzhmb28vakE9PSIsInZhbHVlIjoicTl6WjM1bjNlVndQaVk1MjRlZll6Qkw0OXByT0U5MmJNQ0VNbS9EeTA1VGRjUFVVVGpzd1BpWUZtblZJd0dJMm9sQWtVQjNxM0pzZzFXMERvZVhhNkh0NHlBc1hhbUtDaitFVFZ2SnhlZXQwVXVWQUZlbHBEQUJDWmJ5VWp2R3oiLCJtYWMiOiIwNGM4ZTZjZDQwNWE5ZDdjMDdmMzUwMGI4NGY0YjM1NzI5MDk4MmU1MmNhYWQ5MmY3MzkzYzNhNmY5ZGRmYmM5IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:17:41 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.42. https://adblbackend.peacenepal.com/admin/menu

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/menu**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/menu HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNpbkxIbTRQUzZxMHgwVTVkc0hzdWc9PSIsInZhbHVlIjoiUGZKdEpGUFQxUy9iWUhLRU9NVTR2cjhWUUlDYWNNZ0UrS1NDOWFURzIvSDFmdjA0elc5RVRpaWZIekJFZ2pvNDA4cUYxa3g3UW03b3BjTlNDWUdLYUsrNXpRQVlrbGFZMFQ3TnVTTkl5cEJIcmorcnZpWVhHN3dBb0NoQ2FqSk0iLCJtYWMiOiI4MzgyMzAzYzQ0MDhiMzZkMWFiYmQxMzUxMDA4Y2NlNWU4Nzk5ZjcxODYzZmFkMTY2Njc1Y2UxMDljZWU3Nzg5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:18:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IngwQjY4Rmp5QnROM092aEtRZUJQcnc9PSIsInZhbHVlIjoicXF1Znc3SXZUdkkvNUkwa3NFYno3T3ZzODdJVmhpa1hQejNtRWU2UXhVanZ6clVxd3B1aDR5NnYwL2p4eHBvaUdWYkV1cVpiNHlBV29DUHErUlJyMGZQdUlJWjBUM1k4WW8xNWpja29xS1cxODBtTHpPR1FZYVpZMHpTTUl5bkEiLCJtYWMiOiI2Y2FiYTQwY2VmMTk4Zjg5MTI5ZDc3NjVkMTZhMWY1YzExODEzZjE3YjU3M2U1OGIyMjdmZGVjOTc2MGNhNmY5IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:18:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.43. https://adblbackend.peacenepal.com/admin/menu/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/menu/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/menu/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImxPaXZzYUFUZHFWNkpRVTZSZlo3aEE9PSIsInZhbHVlIjoiMjFSajdyem5QdVJ0WGVQR3owVWxiN1BsMjMxbHlSNXZEa2hnVlV
4TDNrMGtWOFZrNnNCK0xHUW16bUQxcGtJWGJzcm5aVU9VbFgvbkIyY1dXbjhLUDZXaW55SXdEOTR2N0hHMkdKWW5URWJmSUV3dzdYVXJPTWV4dDBnOD
dRZDgiLCJtYWMiOiIwY2NmZDY4NDllMGExMGIzYTU1OWQ2NGYyODgyZTYwN2FiNjcwMzNlN2FkNjNhNDlmNjdlNmZlMWJhMzgxMTdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:15 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImlvSzVZaW1pNDhCYTQxYUpQT1FSc2c9PSIsInZhbHVlIjoicVRGbDlaODRoN0FvOWNNNEw2eTJHa0hFeURMV2xzR05mTTlydF
I0UE5kK0hzNlBtRng0TVo5bncyY0FIQmU2SkZqQ2NlZ1NpOW9BSGsvUDRVdFlpSzh5TUpNVUxVVjdWZkNxZXJLbHlEL2JkLy96am1OdzVGbDl1WGIrMHFEWk8iL
CJtYWMiOiJjNDk2MzMzMjFlYzVlZTMwOGRlYzkxZmQwYmVkZDJiMDNmMzc1YTExYjMwOGIwYjg2NjNkNTEzMDliZjhhMDFhIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:19:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.44. https://adblbackend.peacenepal.com/admin/module

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/module**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/module HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkRBcGNmRElDTGF2QTZOMDFVZnY3OXc9PSIsInZhbHVlIjoiR0NRWUZ5eXIzZWdTMUpHSm9sK29mMFZrL3FWMkRDaGhHM0V0eEkxeGE0T3hENVg1VnV1eHAycWVxTFJJRGV0b3o0cVQ2anAvVUMvOFhNclJtZFVEWVJSclRIZEljNTVqd0tsWE9YZ1gwZTArOURQaEVWMzEzWkdGY2IxV0dJYWMiLCJtYWMiOiIxYzEzOGI3YjVlZDBhZTAxYWFkNzk3Y2FmNmZkZjk5YzAzOWQ5ZmFmNDk0MjY0MmYxMzhlZDIxNjYwMTgzMzBiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:18:48 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImRWRzkwRzVNTERyelJYRTYwaFB0bEE9PSIsInZhbHVlIjoiclJzSVBhMG9TNy9ORGZpUGlveGs0T1k0UjZlVHBsT0MxbmdkWWtPZm1wMUxWVlk0NHQyRlM4VVFML3RxSTUyRDQvWWNZQnAvMXc5WDgrUkNNOVBudzc5Skljb1laR25rRURqN1QzVG9ZWnVjWlF6R3JvZnZYUE9QMjd5anRUSGUiLCJtYWMiOiJmMmUyMWU4YTMyMzRjYmUwZjM1OTQzOGE0YzA4ZmY1NjQzYTY2OTMzZDA0MWFhZTJiMDM2NjExMzBkZGZmYzU0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:18:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.45. https://adblbackend.peacenepal.com/admin/module/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/module/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/module/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InlrK1dlbWUySUk2VDdaUC9vekhVRlE9PSIsInZhbHVlIjoiK2RKdC9EWlhmZVl1K3BKRjdhN2M5czljNHZtZkpLVkYvU0lLVTRuU2NPZE1kWHlnUTR1NGJ4Q01sRjF0bFdhYUtVMnY2emtzZlJrQ09rcVJRYVJQM28vTkpFY3dFTDNMR2ZsRkNaMEZ1RUhITSszVHZ4ekM3NGZVNktxeE9taXQiLCJtYWMiOiI5YjhmMmY1ZDU2NWUzYjE5YjZjNWQzYmFmZmMwYjllNWFmMWM3YjdlOThiN2M4OGU1NDI0MGNjMDkwMDEzODliIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/module
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IktkQ1VwbTdwN1lMMjlnK1daY05FZFE9PSIsInZhbHVlIjoiWTY0SVg0NmxJZ25LUHNyemltNEh0bGRnbXdRQXJ6K3JTVndvT01BZ0hockR5c3hKdVB3aXdLa29SM3hLN1ZVTlJ4NW9tNWlPR3ZDMnZLM2RoV1hwbWZuMktTRk9oSkdqNXZYcmdOTmI1YkZYcEJTcmpkWmlhQTA1Skl6d2NDalciLCJtYWMiOiJhMTkyYmIwYmE2ZWQzNjUyNjc5ZjZkNTMzMzIwY2Q5ZGU3N2MxMzUzZDhjZThmN2IxN2MzMDAyYjFjMmY5NWExIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:19:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.46. https://adblbackend.peacenepal.com/admin/news

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/news**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/news HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6IkxESis0SFIVcTlFT2htSlVaUms5MVE9PSIsInZhbHVlIjoiOVNBUFIIK09uTmpRZnNsMVFGSVZhZGcxeWp0enAvdG9xZ0FjL0FWW
m93QnhXVDNsQ2RQemlDWlhMN0I1MkRxckpSdmlYNHppZDFPSzJzSnVVS0o2UVBpZFZtSU1QbDZ1cTF1LzFTRDJNMzFmMmE3Mi9vZ0lkNzVIMktqSm40QWEi
LCJtYWMiOiIxNjM5MGY5ODk1MGI3N2E1Njc0ZDYzODIxNjgxZDMzMTg3YmNmNTA2OTVmM2NiNzgwYjUxMWUyMjY4Nzc4ODhhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImxqRndPU2Y3WER5UkxOZ2lGenZ5Wnc9PSIsInZhbHVlIjoiRFRSTmRmOVJFNG9VdXg1bEZwaFdtQnZ6eHVWQnM0K1M0L3piR
0taYjh5aENXelgyalY1TllNWEpRVjhsb05SN1hzeVdHQkNpQ1BtOHlHUFJVcExMQ2lnRGtLdjFYNWswL1c2MStDc1BBNVU4WXo3eEFKTFpLaUtSdUxxZlJhUVAiLC
JtYWMiOiJiMDA3ODkyN2ZmZjQzNWYyYjgxZDg5OWQ4NmRiNGFhNTI4OThlODM5YzI5OTcwY2NjMjgxNWJhNDhlNTFjNmFhIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:19:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.47. https://adblbackend.peacenepal.com/admin/news/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/news/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/news/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhlMHZQWThLOFZYdnZQS2h5Z3NvL2c9PSIsInZhbHVlIjoielhsNW0vMC9SSFByYTdSZExGeTV1Q3I0ejI1blVKSmRJMVhPR2FS
TU5CNThzSFNNdVkvN3pDRENibjNJZVA0Rzh3b0x6R0d3ZU9yeVVTSUVXWnlEOWR2ZElWSERPY2EwY28vT0tlL1J2UmdrWnVKQ0dPOFo1Y01GQlRoelhROXliL
CJtYWMiOiI1MWIxN2UzYzk5MWMwYTI0Mjk0Mjc4ZWNmNzU5ZGMzYjU1MTI3ODg2ZGJlYzUzMmMzZTY2YjU5NTE4ZjdjYmFhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/news/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:20:44 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ii9iK1I1ZEUvSURWeWRCTHpQaXZ3YlE9PSIsInZhbHVlIjoicE9tamVHdUE0U1VLYlhjaFJtdFZ0QTRuUWlUUDVUaUF5Y2ZlYS80anZnRFlJSlh4VVJEb0lCY1Y3Qm9SakxwZHpOdVBld1UzRUE5VnFpV3MyWXVHWU5hOUVsVC9wN05nL0V4S0ZNLzRGUHFVTFQ4UUFKYUt5dlJwKzhCWGU3UmwiLCJtYWMiOiI1YTYxMjNmYzBhMzFkZDAyNzk2OWI1YzM5NjRhMDBlNWQ3NzU4MmNjM2Y3YThiN2Q3OTUwMzJmZjVhNTIyNGZjIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:20:44 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.48. https://adblbackend.peacenepal.com/admin/offers

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/offers**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/offers HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IldWME1VYWY0MWJRMnFJcGlZYnRoR1E9PSIsInZhbHVlIjoiaStsZ2Nud05pN3B6SENrdXRzV2M2OWFlLzhNWG01VCttZHlJMlV4U25FY3JpRzl5dC9ZcGQxZmFlVjlDeXVKemsweEVkTWxQaDFtUlJWakRiN1R6MEk4Uzg2bzBNeTFld2V2akJJZnlJWTYwdFdBVmQzQTNvSjd3dFBla0JnZHciLCJtYWMiOiJkZDEwOTc4YjBiMWEzYWZmZDMxMGI1MjdjMzk0YzRkZjA2NWNiMzNjNjdlNzNjNzViNzI3MWM4YmE0ZGVjZjA4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:20:34 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjRLdVZpMmdGZCtCRCtGNUlkMnlMQnc9PSIsInZhbHVlIjoiRUczRFcrVG5nOEtEVE9mZmtXcjVkNkNUWDlEaEpqUmtWYVJzYkg4REwwVzBHa0Q4WFB0UEwvdlRmZlZsenlUYWZYYTFYaTA5RjhNSE11YVBMQ1RGZkkvMU5hcW1OREdYWEJ1YWllb0xYWSs3aXdPSGhwV2dQSXBBUkVib0YrUTQiLCJtYWMiOiI3NTgyNjU3NGY2YmNkYmQ2ZDM4ZmMyMmVhZTE0NzUyZjBmMDU1Mzg2NTEyNGI2MWU5NmUxMjYxOTUzM2Q0N2ExIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:20:34 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.49. https://adblbackend.peacenepal.com/admin/offers/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/offers/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/offers/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVrdmhzcnFzSTRkQ1cvVksyTjNMY0E9PSIsInZhbHVlIjoiUjcwOVJqZytna0VYSmphQTE3NlFLN25xZlAxaWRUTzdkMHNuRjRpRk
VqMlFTTWRZY1lVVURUTTBqOVQ4UEhnYWpBRnhsTlRXbUFtb09RRDJucXVNdVk3MG9oSHQrS0E4cVE1bDdRRzZMZWw3eCsyb0ZvcU0yTEN5T0lBM0dPMnki
LCJtYWMiOiJmOTczNTY3MTBjMDE1ZjRiNGI1MjBjODE3Yjc3Mjg3ZDI0MDU1OTNkZmY2NjhkMzRkNmFiZDQ2ZmVjODE4MGJkIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/offers/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:22 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkhRS0NRdGFURlB3VDVJMjFnVGVIVnc9PSIsInZhbHVlIjoib3hTUTdqU1NPRkM4WnBNTU96RWUyNnFrTEpFNi82SFpKdGozUHI
2OUJTWm5yS2VaK2tqWWZyYVA4R1Q4d1FESm9vZ1RZQlQ4R01abzdnT3c4SkFuZFdLRks4WVU1UDJWRUMrS1RUbzJ2aTE1QWNUWVc4dHpzV3VyTWYwNkx
Id2MiLCJtYWMiOiI1OWE3ZmFmMWRiMDU1OGU4OTY3MmY1NGIyZWMxZTdiNGYwMTUzZGQ2NmRjMjEzZDU0NDA3NjZkNWM0ZTMyMDE5IiwidGFnIjoiIn0%3
D; expires=Thu, 03 Oct 2024 06:21:22 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.50. https://adblbackend.peacenepal.com/admin/popup

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/popup**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/popup HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImtSc0xzUFEzLzRzVW9xMTcvOWFMNGc9PSIsInZhbHVlIjoiS3NzNjZzSm9mUUk0Q0VvZEYvQk04N3UyTzRyMWFGQmJjMENMdk9uZ3dEQkcxY2dvNVB6MEVtY3pIRzBoY3ZiOWdSaUUwMktxRzBKV1Y0cDFOQ3NrUHROMFVXSitCQVdxeVAzMmNsLzhobHdPbkVPQTlTaENpZUhnVnkvQzFXbSsiLCJtYWMiOiI3OTcyNDA1NmE3MGYzZTlhMjQyOWRlZGNkYjQ1YWZlYzQyODQ0NGIzYmUzNmU2ZDUxOGUzYjkzNzFhZmI1MDkyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkpwK0Y3cWZSbkdKcUxQQjJPVDlsVWc9PSIsInZhbHVlIjoiN3lFNk8yK1RKNTlGbEVpNEt4VFhVbk1lNDM2cDBNWU9lNnUremVNaEx0QVRPQTJ2akU0VEV2UlUxSGd2akY3ekkxVjdPV3ZDTFJrWUtPbzRHaXRkTWFMNklxK0FnMUlhL3pGNWpGeWxnYSttK1dTc3ZLME5aYVBqNzZnbDBJTi8iLCJtYWMiOiJlNDdjYTVkZDAxZmMwZDIxN2U3MzQ1ODZlMzAyMzk4OWEwZjM1ZTEwYzkwZjhkYTI1MWNhYTA4MGQwNmMwYjg4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:21:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.51. https://adblbackend.peacenepal.com/admin/popup/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/popup/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/popup/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjlzS0FXUG8ydmJQdVhWOEFDT2lMN3c9PSIsInZhbHVlIjoiMktiYkJzV2EyNS9aTVFvS1p2MzUrNlpOa0tNZUJhV3BBZUFTYUI4SjFpYkl6T0ozM1U5TjVQU3RGcGMxZHlTS1hJaklsazdUMHd3OG45SDZTSWtISGg0VjM1ZWJXNldNTkhkMWl1d0M3QmZEN2Z3dmtNbm8xRFF4UU82eG9QSmsiLCJtYWMiOiI4Zjc2MDhjM2Q1M2U3OTI5YjJlMmZhYzEwMmY2YzZhMDU1OGZiNjFlZWQ3NzkzMDk0NjlzMzc4NmVlOWQzYmM5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/popup/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ilo2RkV0THJjSGpCRzY1dFY1S05YZWc9PSIsInZhbHVlIjoiSWQ4akZXdHgvMHAvUzE0T0J6SlRKWUZwYXNYODlXay9xSDdvSTZOMHVIUjFlaXJVMnBEejdmWVJ1QUZJSWIvKzZlcWNodWxxU3BqeXBtd1A4My9sYkpsZ3VSNWthVy9xNzF0ZVVYTFFKcGU0SkxnVXlOejUvaFZOSVNXZ3cxY2wiLCJtYWMiOiI1YWJiZjE2ZDM3NGU4NmU4ODIzMThhYjk0MTAyYWIwZjA5ZDU0ODM0N2ZkN2NkMzQzOGJjODE5NGE1Njk3NmU0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:22:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.52. https://adblbackend.peacenepal.com/admin/press-release

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/press-release**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/press-release HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6InJaWmQvNWtiU2pDSkRwbmJOUnJ3bWc9PSIsInZhbHVlIjoiTDZ4djRJelUzNjlGcG9xc2NGR25JYmE5OWUvbHZqNWwwdmdsdW
1raVo5cldKeVppaGE3OUlFTkVpN1UwS2VSZXJ0SldIQmVZZ1dRSFh1aEEyWWlUWWJQYzRMbXlya2ZuZjdSSTZyZVQ2N0JEMVZNYjFXVnBsTFBHWGlLY3lTUU
giLCJtYWMiOiI4NTIyNzI5NmYzZmExNTE1MzFlMzg2OWY1MTk3MmMzZTIyMjM1Y2U3ZDdjMDcwMDc5ZjU2YjE4YTBlYThmMzUzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:57 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ild2aitKdUN0VnIyMXpIblpmWGVZMUE9PSIsInZhbHVlIjoidnlkaTI4aU1Zc2JLSTh0N21jRHpOOGpjUGJtaFVDb0F6QTVZa01HZEF
wOXhkVGM5dDcyV0tSK01zWEQ3KzBsUm8vY1hPL3p3VllvdGI4eHplaWg5alVQNjdiMHhycDZ0T3E1VmE3UldGbTdPUUhyMU9Xb2FtWkJuUVBERVdUMWciLCJt
YWMiOiJkMGY4MzIyM2FkMjllYjdjMDVlZTExZjE1M2FhZjBkNTU0YmRjYTE4MWE0OWIxZjJhOTJhZDI5ZmZhYzU5YTRjIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct
2024 06:21:57 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.53. https://adblbackend.peacenepal.com/admin/press-release/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/press-release/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/press-release/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImdwRkhaeXVxT05uRGRjeHZ3cDVqNWc9PSIsInZhbHVlIjoib09sVFdseWR2WnEwT1Bxb0R1L2RsWnVPQnl1M0dSMkI3UVY0ZT
VaaFFNRmJGalVzSzJYNFJRTFlYQno5KzZOOVpzYmV3cS9VeUlyZEh3anFpeEdpdFBPb2JYamFZb3hhVzB1NnV2RFJzQzBkWWxEeDF2NmtyR0s4SUZrYW9INlci
LCJtYWMiOiJiYTMwNzZkNWFlYzNmYTNiYjRhMmFhNzMxOTBmOTZmOTdlOTNlOGMyMWYyOGNlYTgwZjY0Zjk3OTFkNmRiYWMxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/press-release/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InhnUnhzQ1pGTE1YejhPTW9ySjFXU2c9PSIsInZhbHVlIjoiYXNpL2lVUzh2Q1pSc0VEMUZtNkhYQ3dETWM5dDFoWFYxUkZxaTN
QNC9xcWRtV0NuY2NxYzNIa2tPeThSeEd6amFxMlhaRUNpUjlzMENrK0RyeWJDYWYzNURmcGJCb2ZkU01EbWhYQ1hkSUNZUVpVbFk5bStTRlhTcDdZQzdEM0
UiLCJtYWMiOiJkODJkYWJlZTlmZmE2OWU1Y2E2MzUxYTlhNTQyNDA1Nzc2OWNjZmIwM2QwNTNlYWQ4NjI5YjNhMDExNTJjY2RkIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:00 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.54. https://adblbackend.peacenepal.com/admin/projects

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/projects**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/projects HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImhhTTBpT2RPTGVYRVVOZXJ4Ym9lbkE9PSIsInZhbHVlIjoiL3hnL0NaQlcwaS9BbkovSDV5Qk1HeDNtVGN4VGo0L05xZ1d5ZHFp
Ti9ZcEFUUWxNakIwYWdBV0dDQ1NGNGVFeXcveElnMisreDdxSVNxVjJTeFhmelBaeStJbTRWRkZPUzZCZVZxZFRhVDNLa3Z4M3c0bDhmSk1OQkxMeHIyY24iL
CJtYWMiOiJkYzQzNmFkNGUyZWIxZjAwMjE4Y2ZmODI3ZGYxMjY4NmMzMWJiOTg0MGUyZmYyNWIwZWM2ZDIxYzViZWUzMzNjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:31 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkpmTGlaNkV0SzNZWlNqR0s4cFB6L1E9PSIsInZhbHVlIjoiZnlNdXVzc051T0NCR1JXVWVOSHNEcS9QZHFOcjN3TGFlSzVnTnA0
eGcxVEVNNndibkk2OHVnZUdnTHBSYkJpVlI4UVRvQnY5U2VLUkM2UXBobjJQOUlwMjF3YkR6OTZsem1kdkFYK3VvMnNDNElBODBld0NuaHNTMDAvbGF5UkliL
CJtYWMiOiI0NTcwNGMwNjU5OThjZWZkNjQ4NzA1MzNkOGI3ZDE4YzFlMzY2MmY1NjAxYmM5MmY1YjcxZGRhZDE1ZTljNDYwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:22:31 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.55. https://adblbackend.peacenepal.com/admin/projects/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/projects/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/projects/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjY4NmxCWGRrUmV0Sjk4NHJsdnlicUE9PSIsInZhbHVlIjoiaUJqNE9LbTl0aFhMaGROem1yWnp6ZThCZXhiVnpwWVplaEE1NmNCejMwcjY0SGllRGhSVzVtRllFbENUVkhYc0lMUjhOd0EySDBFZzJPSWQvVVJUTFEzZDVvUnV1TWFtM3BKWlUxeHhKQ3JsQ2ZVNWd1VEJFUjBSM0M0MkdMaTciLCJtYWMiOiIxZDNlMWJiZGQ3YWE4MzQzY2RhZTNhNmM1YjYzMWY1MjQ4ZjQ4YTM1ZTVlNzYwMjNhNjM3ZmY4ZTFmOWE5Yzc5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/projects/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InQ3elB4Zm5UUTZldVdmZVpRckw3SkE9PSIsInZhbHVlIjoiVWdyaVFFWFVuY25NQWZscVM2OS8wSnJ3VHpMRVVZNXJiQ29NLzRhMHkxdlRneDRPa0x3VitIcFJ4LzdjL1dRdTc1ajI2M25sMEdxOEF1d3dRY2xhQ291Unp5MVkvM0pWWWh0dVp2K21GK2hwbFBwY29YczlRU21oR0ZNS0cxKzEiLCJtYWMiOiJmODg0NDY0YTI1ODkyYzZkYjliMmY2MGIwYmQ0ZWFmNzE4NWQ1NDUzNGQwYTU0MDZmNTU1YzJkMGY4MTU5MWYxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:19 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.56. https://adblbackend.peacenepal.com/admin/report

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/report**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlRjMVQrNUJvWnRTTDkyTnAyQWZhVWc9PSIsInZhbHVlIjoiL0xiUGkxVFYxVXJZY3Y4eGlZbndGWGdOUzd2M3JSYndBWllZejVse
GVIdnhBL2VFdlR1Ny93L3ZBdWVGTUJmNHl5b2dDTjNJbDI5RTUvSmlCbXFyTUxlVWd5V2hJSmNVT1V2bHU3Ull5Wmt0cUp1TzNIcDNidHJYOVRZSjFNK00iLCJt
YWMiOiJiMzBmOTFlZTI0MjBiNWQ3NWU2Y2YzNTI1NjY3ZThlZTZjYzk4MjViZWE0MjM3MzVkNmVlZmFkZTI1OGEzNTk4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:08 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InNxeFJZSjhNUS95UFNiMDlHWXFtUWc9PSIsInZhbHVlIjoiT09WZ0hTZENEM0N6bStmdXlIVUNOc3c3M0l1QzBrSW9oM1Zrd0c3K
3B2djFncHVaMDQwbTJ2QVYwUEp4bDc0d3pWeE11K0dGd0pQNEpBMWVUWW9HUHJjTUREWFdhcjVNbk9vTFBJbTFMOTdkN3dWUWJ3TnRRYTY2K1Y2Q09O
SloiLCJtYWMiOiJmZjA2NmQzNDM4MDc5NmNjNTQ2NjZkZDBjNjQ1ZTQzZmU3YjNlNjg0Nzk4OTg5MmZkZmYzY2QxYmZjNzJjODhiIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.57. https://adblbackend.peacenepal.com/admin/report-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/report-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9zWEZKNlgyNVJRUVI3ZWdyc3ZybIE9PSIsInZhbHVlIjoiUjBjUG9YSS9iVmpYN2sza1BBOEpVd1ZlelBpcXJZWkZUU0JtTStwMWd1WlU1VEo2NjNJNHdSNnVLalpLaEtlTzR1bmF4VTRCY3FvZjNwbTBjb2tVZnlhU1VteTYzYTRqZVVLSmliK2tIZXl3RWFuWkVqWk03d2dUTnVhc2NRQ00iLCJtYWMiOiI4OGE1MGM1ZWZhYTBjODBjMWQ0ZGM0Mzg0YzVjMWM1YzIxMzU1ZDBhMmUyMDk2ZjYwNDk1NTNlMjcwZmY1N2VlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:24:28 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjJiUE1xL2pEdWU2c3FvK0x3YWtBQUE9PSIsInZhbHVlIjoib0V6UTI0c1Rvemt6Smp2dTNVWkcwRk42cjZEd2pXZ2d1djRlcysydFpp
U0I4Q2JsNEtoSnNuNlBERnUvM2IvYzA1YkFZWlhRVlYwZnFybVZMZTVSdUx3YU5BNmRla0xYanA4dHc1SkRIMW9NVE9RYkN6Sk5adEdpZ3VDN2paeksiLCJtYW
MiOiI2MmVlNTk0N2RkNzk1NmM3OTQ0OTVhMTI2ZmIwYTIxNWZmMjQwZTI0YmRiYWRjYzYwOGQwZjBmZjliZWVjMDkwIiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:24:28 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.58. https://adblbackend.peacenepal.com/admin/report-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6IllzRjBRQ2JrTTJqNG9BZHhIRG13TGc9PSIsInZhbHVlIjoiR0ZZQ2hZUlRsejVPMWZxRTMvUm5RRGNRRVJJdzFWK0JsdGFyL3RvLzJjdjVIZWs2eWd4SEF5MUlWQzdNNFRSa3hIbWx5aEZSUTAzMWJMaG1jdFVHZDRkRFpVSjMxNENGT0hmQ2hOYlcvVVFLTkVNZmpCL2dtTTFvbkdoS1VsUDUiLCJtYWMiOiI3ZTgzNzEzYTU1OGNhMDU1MTg2MzRjOWU5MmIxZjYzNDM5NDU3MzM4MGI4NzFlMmRiMjE1NTdiMDkxNzYzZDBmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:25:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjBEQlNIVmdBTnY3SCtlNDBQNkQ1T3c9PSIsInZhbHVlIjoiTnBWTDdLWGNoaU9EMUljLzlySE9WMzVvVyszRnozMzEvVFBDQkpxcEJKUUxGOUs1cVBaVkovVGtoMmVmNzd3TVBFK205dGc3UTJ3c3RrM1poTHFTaXJYVGRRbVg1VmtEOWtlb0JUUzhsMU1lUGMwQjRjRkN0K1lpQmpwK0FyWW8iLCJtYWMiOiI4MjIyZmI5MmRhZjJjMTc0Y2ZjNDJmMDEyNWZkZDU4MTJhZDQwNzU1ZDI0NDRlZDIyNzkwZDhhNGUyZTFmMzliIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:25:07 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.59. https://adblbackend.peacenepal.com/admin/report/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlRGdEdJVXhYV3dqbHJqOVRLblNObWc9PSIsInZhbHVlIjoiVURvNTBLT0FNb2IwdVRydk1aUFVyK21yTW5PRXRMcmRCM21qb3djVGlZNDc3K3i0YVVNUW1SMW1KV01QZm9DdWNwWVRuZWNjQzNjQ0FMcVZ5Z3ZXNzBzZjBva05NdUxmcElkYUlaWVlzMFBKeVVUbFBKSTMvMnhNL1NiNTU4bDYiLCJtYWMiOiJlMmI4OTFiYmVjYjg1OTI5ZjAwNDVjZWNmOWE0OTdhODMzZWMyNWQwODhlOTg0MjE5MTlmMjk3NmM0NDJhNjNmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:24:15 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImhqbUxlWUZpcGF6VnBiNzFrZmpvSmc9PSIsInZhbHVlIjoiV1FYYVJsMWVkV0JwL3E1NkYxc0l1L2NpNElDejFFcHAvV01PSlFXbjl
wSjQ0emtzSDJsSGtQS1VKOHRBTGVZOXZGVnA3WU50OEc2MEs5TFRWVEJGaUoySnBod1Vwb0UzQUJxOGo2TG5rb3huS2J6M0F6N1VyWURxQnRHSGVMN
C8iLCJtYWMiOiJmYzRlY2Q4YWFjZjczZDBmOGQwMGU3Y2JmYTk2NTVkYWNhZTRlOGIyNjA2ZWJiMTE3MDQ4MmVjNGNkZjEyM2E0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:24:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.60. https://adblbackend.peacenepal.com/admin/reset_password

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:28:35 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033024

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

4.1.61. https://adblbackend.peacenepal.com/admin/seos

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/seos**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/seos HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik5OR2JmL3BmdGYzcG9hM0MwbklkZGc9PSIsInZhbHVlIjoiR1AwNWJReVhlOHIraTRCVEMvUGFQWDFNSDZYQUhsUmx4eGw3bzAxc1FtUUNkaXhXYWpmMS95RVlyTzlwRzhCMDh2eHVlZ3l3dGpvYU15d01LaDEyVENLdDZCTUtKQ1VHd2V2eU9ncUxFa1JibTZsRjRBWCtwbUVHZTF5ZTliRkYiLCJtYWMiOiI4ZDNjNjRhNjMzM2RkOTg0MTBmNDRjYWViNmQ2OWMxY2YyNjcyMTVhZjIyOTgzOWFhZDAyMjk0Y2Y3OTkwYzIyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:45:36 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ink4K1lSRHlZRU56d3B6V2dwQnJCOHc9PSIsInZhbHVlIjoidWV6Wmw1TndiTWVjQXlzdVViM1BtK3VVdFFKWTVUOFdjTkpDS1JuOTRVaVA4eVpkOS9YM3Y4dWh6ZFhvc0xycHE2cTBmUm1zK2Q0L09mY0ZOQTB1cFQ4dnhSQjI2NEpHNnlUVlB2RkZLemJpOEtreGZKbTJYSHRSOHFUMEIIMWUiLCJtYWMiOiJiMzRhN2JjMWU0ODYxNzMzYWYyZDRkMmExY2FkOTYxNmU1OGQ4MWU2OWE4OThiODk3NTFhOTE2MDMxNjA3MDczIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:45:36 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.62. https://adblbackend.peacenepal.com/admin/service-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/service-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/service-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImlzdW1pSVNSVkE2RGMzYURnVldSd0E9PSIsInZhbHVlIjoiU0pIR2M0QkhBM1ErSkc0QnVCeGRxYUdOcnZHSldMclBRZ0tzTWh
wV2oxRktXdGhBbk1McXBKMGR4VzhPUmVIa0ZYdG9JU0hmbzRielRVL3ZmUy9ycmpOb2M3SXo0ZHlxL1ZPbzNvaHpPck9KWEMzMFdHaERZZUpvUGx5NEwzK
3YiLCJtYWMiOiIxMzcxZWU5MTJmNDFjNTU4Yzk2NmIxNjI2YTA3ZDFlNTQ0ZmVkNjg0YjRhOTgxOGNlMzkyMjAzOGRlNjFmMDc0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:45:48 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Im54SThGSE1HZlpOY0tNL2FRRHJVSEE9PSIsInZhbHVlIjoiYk9UVGNlZmtuWmxVMWtCczZwb215QXdoVzNuYU1lUGkxNmtKWG
RETXNZNGRXeU9GL0xLb2lNR3dTUVdsUVhnZGFpU0t4Wk5tUDdBNWR4dXBZblFjRVdDNjRsRzFBZjEwTjUrbkN0QXRUeG9PVUFGNENCd0NYOCtiU21rRkNRS
3QiLCJtYWMiOiI0ZjM4YTRiNjBiOWVhZTU3N2Q3ZjcxZDcyMDUzMTc3ZTZjNjlmZDRhZWNmZmM1YzVkN2FmMWVhOTY1MDNjODMyliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:45:48 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.63. https://adblbackend.peacenepal.com/admin/service-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/service-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/service-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6ImFlVU9zdnJNaEptSWR4aHB3a1ZOQnc9PSIsInZhbHVlIjoidnZxUXFIM2Y2WDR0NjJTUzlOQ1g2VVB6eGlEREpFVnE1WTZLOUh
nN0JkRUZFdm01QVNhQXVtVW9FMUlEeWJtalBtd1VkWXR4Y0RCRHJ1UE15Yk05MGVuaDh6WGhkaCs2RGxkc0VBNnRwdDBJWmZ0MWQ5QlY0elpDMmxCQ0
ZpdEoiLCJtYWMiOiIxYzM5OGQzMTFkYzgzM2ZkN2ZiNzliODljOWJmNjg1YjU4OTM4ZDkyZjE3MzY1MGU2MTBkZWI0MjQwNTdkMjBjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/service-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkZLM1B1cnZYTThBUktIOXVHQ3FsUVE9PSIsInZhbHVlIjoia1VsWlJtNXVMcjZQUXM2WXQ5V0dWZHo1QjM5UlBuSjVPZnpmSVV
6TXFQNklrZk5PdkQwMmFkMVRQaUJuQ2tLd0QzbkV1V2Q1SHdpa2VyaXJzdmdXbnNmZ1B0aUR3UVp1QUFab3BndmtsZUxOT2Y4MW4vK0pxOGZ5S3VseUN2R
GgiLCJtYWMiOiI3ZWUyY2IwNDRmNmU0N2ZmNDFkNmJkMzFiMjYzODNmMGJmMWMyNzI5MWI3ZDUxMjE3ZTI3NTViY2U4MzMyZGQ0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:46:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.64. https://adblbackend.peacenepal.com/admin/services

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/services**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/services HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlQ1YUluZUo2ZmpjR2hXOEM0SFp0Smc9PSIsInZhbHVlIjoiK1Q3V0JwTkhianVSdVEyWkwySGJ1SDZseWRCRWJGdzVuRy94Nk
M0TUNqTEZhdTM2bHlrWXdaQjFBQU1aMUNIUTZvTVdGN2dWYlRDNVRHbHlrTHEzSmU2YThrTTlLem9QMDRJb05DaS8vM1RaUGo4Ym1QWXowbG42MlNQdn
NLV3AiLCJtYWMiOiJmYWI2MGFlNmY0MTljOGRkMGY5MDA1YzE0MmEzODg3NTQwNWNlNWZlNmY2ZjhjMDdhZjk0ZTM1YmVlYzY1YmM2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:21 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJJNW9waE9zV3lHeWgzY01JQVAzUEE9PSIsInZhbHVlIjoiZVlJeDQ2WGpOdlRoSmxWa0xTZTl6enV0UjBFTFBnSU5vWE5VYkFkcVZ4QUNlcWk4S1FUU2xiTUVmYkx4RWRyZUl5MTMraEwyMVhkWGtjZitEV2p5Q0Nwc3J0MXJ3VVZYTVFvaDRuQnZpbWN6VGlsR2cvNWRueXJNdjhIZXY0aU4iLCJtYWMiOiJjMDExZDczNTA1Y2Q0OWYwZTkxZjRmNWM1OWYwNjdlZjE3MGFlNGEzOTg1OTgzY2ZjYmM3NjdjMzAxNTkyN2QwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:46:21 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.65. https://adblbackend.peacenepal.com/admin/services/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/services/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/services/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImZnSDZhUUptdDU5RUJod3U2VUVWMlE9PSIsInZhbHVlIjoiY2N6bzgxSzh0U1YwWkxkRDQ0aUJtQkpKRDBqbGxhNkRvcjFzM05ML2YveVM3dDJwYytzNG9pM3NhTTBPOGFySHovdXBwMmdCY09EMWtCcmtzenQyYk83bkNmUXlSUHJwbHdMbXk0bXlDMUt2cHozZ3ZwZXVoSnNMdXFMUnhXbngiLCJtYWMiOiIxNDk0MzljZDdmMzlhNGIxNTllY2YzMDIwYWJlMzljZjU0YjJhNDM0NGQzYWVlNGFlZGRkZTRkMGZjNGMyYzhmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/services/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ikd6ZTEvTGV5NnZDdTBwWno4d2k1VlE9PSIsInZhbHVlIjoibnhkMXFPM0hvbll3a2JHbmE1cTJ5L1VTT0hKTjRvc0IvNGJJZ0ZrSEdQQVorSEkyQjZuRDRMYUxUYzdJZU9xVko2Y3RsUkFvaldMb3hJVkRRVFdpenV1R1E1M1NNcW5JLzlwMUduUUFqL3pKY2VaZjh3dk9jN2hwd0JwQm5xUS8iLCJtYWMiOiI2OTNiNmNlZGVlYWI5NTU4ZWMxMDQ1NWZmYWZmMzViOTg1ZTdmM2IxNzBhMjkxNGYyNGUyZTliNTU3NDFjYzAwIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:48:07 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.66. https://adblbackend.peacenepal.com/admin/setting

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/setting**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/setting HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ijg0NFowMk1YY3hRWldabElkclgwVkE9PSIsInZhbHVlIjoibUZsL0ZnUnFWRU9YSkhwRnE4MGNaWExISjVnK0hVV0J5VVZCampPUk13ejRnaXF3ZndjWjdnUmo5NE9mNFhWM2cxb1EzR1NUeHlQdW94d1pPanBrZjQ3MlBpV0JoUk5SenZINEQrRGFPa0tnRzBVMGdod1U0RzBYaGVjWFFxb1oiLCJtYWMiOiJjNzI1Mzc4ODlhYTUwZGUwNDA4OWRhMWU1NjM0OTU1NGM3NTM2MDEwNWZhZGNjMjc0OWZhNWFiMzE0MDZjYjhlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/setting
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlVxZGdDY0lta2cwdnNxR1ZBVjhNWVE9PSIsInZhbHVlIjoiZTgwc3NpZ3NLN0RDUDdpZzdSd25uWllxTjRYRTk1T0dqejFGTXloSUNIYzM4TEFtalhwOVYybklwVzVnblFSSXVETXhPOGdZbEpMRi9XbmQzcTV4TW9XblNlRFI5RGJYZGU0dnpCbHBWTFRYaTBvaXY3RFVOcFVRdDBVdkVFa0QiLCJtYWMiOiIyNTZjM2I3OWRiZTNkNGJmYWQ0M2JmZGY5OTM4NzE1ZTVhZDc1ZjM4NDBmMjE3NTQ3NDgwNTcyMzBiMTcwYTg0IiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:46:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.67. https://adblbackend.peacenepal.com/admin/team

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/team**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjVaa0pKYSs1U3hZWTEvanBXWmxoN0E9PSIsInZhbHVlIjoiT3J4SE96S3B4aytyUXlnWHdiZWFuYzUwWFBjSGozSHJLNTdObTZa
cGFDV0FJa0NMd0hmVFFZZC9XUG5HOGpibldDQWlaK01ySkVoNmU2VC9LR0JDb2d1MS9YbkhtL05sSkgxTzA4YTl6bit0WWxKeWVoYzl5YS95ZHRYb3RVemEiL
CJtYWMiOiI3MDRlNzZlNGM4ODM2NjlmYjdmYWRhZGE3OGE2ZDY3NDQ2MTQ2MGZkMGE1NzJhYTZjYTc1YjZkMGZhY2NiZWU0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:47:02 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkhLNUhjTWdNS2Z3NEpZM01Cei95eUE9PSIsInZhbHVlIjoicERWRjhTdWlNOUFHRGxTdHRXbk56NDBLUWFJK0UyZUUyaDdWTj
kweW1SWmdnc2FFN3VNb2M5NDR5c2F4b1IvNWcrKy9MVXBsQmgyMTk5WUxkYnVRVHBlR0o0SGNrQkd3aEd1M0dIWTdKOWFabW1Ia0ZnVkd0cDVYLy9OZjBz
bVMiLCJtYWMiOiJkZDhlNjVjMjIzMmI5YjJiOGNkMjlhZjBhMTRjZmEyZTAxYmZhYjFkOWE3MmMyMzlkZDJlNTBjMDJhM2IxMzZlIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:47:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.68. https://adblbackend.peacenepal.com/admin/team-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/team-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlJNUEpLQURKQzZnRjZSZW1RQWRWVEE9PSIsInZhbHVlIjoiZFIydHRaR3c3K0k1QXdWYklPenlDTVBSaXhZTk1leHJjT09LTm9zcXhmOFZHdzFBU0w3QzRMdE5ZNzN5ODZLMDNtUDdjeTJOYkM0MGV1UjlxYmkzb2xpVDloSWVpOVZ0Sk5IaGs1V2xudEVSb0RwcW0rbjN3eE5rbW1aRHpQMlciLCJtYWMiOiJlMmJjNDY1ZjAwZTc3MjFmODFmM2RjODMwZjVlZmYzNjViNTZkOTlkNDg3NzViY2FjOTgxMDVjMDE1OTM1MmUyliwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:47:18 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjFuTkZOU0ZHOXdkVE5aRzI3aGdGY0E9PSIsInZhbHVlIjoiVHZPV0FKMEJQT1ZleTlFSXd2UVR0MmRBdWdqSE1sRzJHbHhNSFNtTzNQbkYwN2YzZUM0WmE0a285bjdqb1dNajU3R2Ftb0g5QWZ5WEJ1eENqdWhzb2w4TlEweTVvNUd0VXdTL0tZRXg5UTBBM01TVmMwSStRT1FLd3pmc1RncEEiLCJtYWMiOiJkNjRmZWNjNWYyMDQyMjNiYTYyNDU0Y2Q4NzZlYjlwYjkyNTczYTY2NjdkMTMwY2FiMWViZWI5ZGNmYjIzZWM2IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:47:18 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.69. https://adblbackend.peacenepal.com/admin/team-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6Ik5ac1BnczladzZreURFejRsNHZweHc9PSIsInZhbHVlIjoiQVlxZ0MyS3p6TVF5NldmZkJwUitpbkpDaWJqU3dhUjJDb20yUVo5VFphQUJRR1ZTTENqK1FoN3dISUlWY2ltSnJjajYwZHkwL1ZpZ2tCVitNVzZHcGNwWWxCTE02VWs2UDZwbFhENkZ3Qlp5T3QvbXAzMnVNSDBSUVR0OGkzVDciLCJtYWMiOiJhMDczNzFhZjFjNzQyMjlkOGNjYWI3YzBiNTczNTU4N2E3YTFlYTI0MzY2ZGZiMmRiODA1MmJlMTBmZTIzMDJmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/team-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:02 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IndONGRwNW9ENG92bi9WN3RLOElqdEE9PSIsInZhbHVlIjoiMFRTa3ozaW54aDNXbGdtZ2hVMllqdHJrRFk2Ym1abVoxcG9WdGh1aG1pdXExQ1BPWjJGQmppaHUzU0E2RnlLeUNPYVJza3BDYWNNQm8yWkdiM3pHY0NBN3o2K3A4YVhuQVJJeXFCUVBPVkVxLzlVeFgrSVhMUmQzdWVOTVpZc1EiLCJtYWMiOiJmYml0M2I2MjBmNmUxY2IxMTJlNGNhOWFkNjJmZjg3MGEzZDNkM2U1ZTZiN2ZiODdmMjk2MjZlOWVlNzY1NWEyliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.70. https://adblbackend.peacenepal.com/admin/team/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im9zcGdEYnpGS1hrV1YxeW5WTmlzVXc9PSIsInZhbHVlIjoiTzlHYlIXM3FVOTliZnR6eUp5bjlzcjU5bm5yVC9lV0YyWm9qWUZNK3FEbVlmSHg4bVpnWFE5NERkNDITSnFBODRPVmY3UlJ6ZW4xcVpkY2dOMWpMZ2d2VUV2SnlNTkkxZmNlUTk3WEtCMkp3c25JRlhreWhBbmhWOVdocWdVSWgiLCJtYWMiOiI2ZDJmMjlhZjNlNzVlOTQ5Y2EzZWVmOTQ2MDQ2N2JjOTYyMWQ4MWRjNTJhM2M5ODhhYWRiNDNjOGNjZjViODQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/team
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:09 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImZxdExJblJJUzdUd21wKzFkbmFYQmc9PSIsInZhbHVlIjoianVRTXJvZzNqaE1KRUc4ZEI0UXVuTHE2c2FLK09kTS9SNU1zeEFH
RDBBdXBGRWozeVJHdDJkVkdQdk5XWFF4Uyt4QUdXSitkM2padEJJWkhXdVVsc1FKaGRXcFdrUUVzN1pVYmNjVGptWFFtOGlEbXdna21VQ1BOcE96eDVKQjEi
LCJtYWMiOiI5YmNiMjIxNjIyNGU3MzczMzdmZjZkYWFmY2I4OGM1Njc4OWY0ZDhiZWQ1MzhjYjg0OWExZGY2YmY5ZDMxNmFlIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.71. https://adblbackend.peacenepal.com/admin/training

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im93dDZpVE1lWVhCTVgyU29TUEdPZnc9PSIsInZhbHVlIjoiVU85QUhCaWQ1WUdDL2RRRUE5RnFBZVdFSjFXMmlXL3JvdTBpYj
R1MnovcURQaTlnUlBxZ25wZllnTm9QTDc5SVY2cXM1bmNiT1d0WU16d2paazFTUUgwWlZ4NDhSWkRyUTRDV3hTZ0pLV1QxL3AyL1NnL1dWbnNPYmZsR2UxV
kUiLCJtYWMiOiIzMDNhNTBkNzllYzQyNjQyMmM4YWYzZDU4NmFhNGI5NzRhNjAzMmE2ODE0NThlYTk2NjdmMjYyMmQ2NTk0YmY3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:14 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZyVWdpUStLQUFUVFoydG5QdFlGL3c9PSIsInZhbHVlIjoiTDlncWR5Z0dteWd2Y3A4bFRRZmg1bmd0dTVVVVlMa3BwT2ppbnds
REFpMXlGcE5ZM1FIK0ZnbEJMYzZST3poYVdJMjU2YjZKL1gwTElXMElmK29CNjEvQWwwZ2lNMGJOMG5ibEhKazNORzNIaklhSVZQM0wvSFRLQjVOMHV3cVli
LCJtYWMiOiI2M2JiNzA0ZWFkZmFkNzhjOGIwMjI4MzE2MWUxYTIzMGFjYmFkMzUzZjgzMWExMTljMWM2YzY1NTQ3MGY3MTExIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.72. https://adblbackend.peacenepal.com/admin/training-hall

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training-hall**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlhQRHV1ZWNBMDdnMFBOZmR1MXdxclE9PSIsInZhbHVlIjoiQ1Q3Vm1YaVo5NXlFQmd5SmJUN0ljdlVoeTFPblFjUjM1SHZyRGZtaU9MbDZ0U0ErUlR6WGtmeXZJZ3pEbnNwQXNGUnh0MFZaODl5UVVtL3hjdkZ1VnBqTmpVRlluckM5OVpJVjI5MVo4cTB5a1dDeExzbmFqQVZ0bTZGOHludWoiLCJtYWMiOiJiOWI4YjA2ZjYzM2EzNDg3OGFmMjQ1ZjE0Yjc4OGY4ZjM3YmRmODY1MDRlNmEwNWUyMTA1MmZhMWViMmRlOTNjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Inl0TXJzUFArN2o4ZDJDUUlRSGtoMWc9PSIsInZhbHVlIjoiZ29oVy9zOTg5bHZQYmlGQkFTWGJ3TUJhVjhXTHdTOFE4RUVpa0JFQjVvVDBjOWNrblVNUjJoWVE1SHdTTVJBVmpWSlNqNVN3MFN5ODlITTR6M0U1UjFPSjhrcWgxOG1Qbzl6ZWRLWG10ZXRZSytkNHovUFgrUU0veC9rejhQZXgiLCJtYWMiOiJhMDU5OWFlYjYzMTIxNmIxNWIyNzExYzRhOGYzOTI5NzZiNTViYTczOWM2M2MxM2M2ZGEyYTU0MWFmZDY0MGE3IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:19 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.73. https://adblbackend.peacenepal.com/admin/training-hall-bookings

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/training-hall-bookings**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall-bookings HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik84OVRLQXdkTFB3dUk5Yy9TQlFycmc9PSIsInZhbHVlIjoiY2phc3RKOElWZSt3WFB4Mk1RQlF4enE0RWFXTFc1d1E5NTRCTVB
EVlIxSjl0NGdRc2NaZGREYzlXZEFlUDBLR3M3dGlpT25lYnhxK09YeXlXVm9LakFvN293aU9TRUYra1FPdU0vKzVJclQ2NDJqT3VpUDZMb042Rzl1bElsQm4iLCJtY
WMiOiJkYzk4YWE0NDIxNTg4YjVmMzU3ODMzNTYxMjc3M2Y5MGMyNDQxMTFiZmQwMTQ4NTExNTIyMTFiYTk4ZTU2MDZlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Imo5N3pHUnIxOHV5MXVYaHJuV1dnS1E9PSIsInZhbHVlIjoiUVdzS25YOFBDbVZoZjJDQ3I4Wm9UTFU2WGQ4UW00Ulk4SThsW
WczRWxBMEVCZCtvSjFZRitMZjN2V1QybFhIdWhadWJVdThRWnpQaWJpeFhOUGNaU2hyZTlOK0wyQ2RMR1lOdG5pa1RVQmJtSm95Vm1tMGhDTEluclpya1orU
k4iLCJtYWMiOiJiMWU4ZjliZGY3YjY3MGY5YmY2NzcyOTVmMDIxMjVkYzczNjJhM2UwMmQxYTAyMWUyOTA0ZWI0YjQ2MWVkYzQ1IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:06 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.74. https://adblbackend.peacenepal.com/admin/training-hall/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/training-hall/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik80TGk4WnlRMzRQeFRiRE1RVC81Q0E9PSIsInZhbHVlIjoiUEgwZm9YYStZWFUvTmVOMk9TcUdPU1lERy80Rk5YcmRwZzdER
VlLVHB0U01qdGx6NEZQVm1SQVVMN1NjYVB2VjJndVZRNFJkRWhiSzBPOFpKR1lXM1F6M0M1UmM2SDlJWXUwUmFWUnlnbzJybkhncVpwb1ZUWktmMWt0M
FVrVXEiLCJtYWMiOiI0ZWJjYzViYmQ2MmU0MzQ2MTkzYWVlYTYwNzIzYmY0ZTEzZDFmOGU4ZGZkYmMxM2E1NjUwOWJlNDE3MzFkZGY4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training-hall
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:12 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Im1WSDdqYTJvSnNCZVhrMjJKa0JTelE9PSIsInZhbHVlIjoiSDFKZ09Ed1l0UXo2RDBMWU41SThVaUVBYlM0M203UThZY2NTd1R
WRVhRNUNydm1tbnFUaTVpRGwyM1BjLzNRTzhnQktLYmJSV0lzMnYyU3lweElOTTlsRktUS2tUUm9sb1VUQ21MZ3dRVnFOSTFHRmFsNm9jR0hIMUo5dXZHbE0
iLCJtYWMiOiIyODU1MGI4MDYzZDYxYjgxNjk3MDIxMzIwMGM3YTU0NjlkMzkyMGNmZmZjYWMwNzMyOTkyN2MyMjMzY2IxZDlkIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.75. https://adblbackend.peacenepal.com/admin/training/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
```

```
adbl_backend_session=eyJpdiI6InFVZ1AxRlhTRnRFVlNsOE1VRTM0RXc9PSIsInZhbHVlIjoib3hSZDV4dStnc0hhVElqQ2JCclF1R1dCRU1VYUMrSUUvTU1DNS90QmltaFlySWFCN05IN3M1RWdSVzArZ0w4OW1mVFdzSC9lYTNVSEVzbFBzeFVnQnZ3TW1CbTJwNjgyRno1UXRoRURoMnU0djEvNVpSdFh3UldTb2lReUpvbkkiLCJtYWMiOiJmMWNiYzZmMDAxMzM0MzRlMDkwMWZhYTUzNjZkODM4OTJjYjNiYzc3ZTQxZjI1MTVjOGQwNGNmYmY5NDUyNTZlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:02 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IktaUjd6OG9ZdGZ5OUNCaXpvYkpmVFE9PSIsInZhbHVlIjoianl5MXVxTlE2a2doUlJlVU5zWnVxSWhkRk51eWtlc1FxKzhyL0taM2UzQkpsYWd5OVoyZFIzNThrU1NaV3JkbEpsaUhyTkpNS0FGYWRHcExxRHdIcGlSeHZtd2pCQVkwdzRZMXJ3Z210Z3E5N3lyMi9tRUsrQjdncEJlK1hUazgiLCJtYWMiOiI3NDgxZTg3NzhmZDNjMGM0MTVmOGFiOWZlYWVmMGRhNGQyNGQ4OWViYWEwYmZjNjJjN2QzY2VmMml0Zjk0ODEyIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:49:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.76. https://adblbackend.peacenepal.com/admin/vendor

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNMY0F2UnZySGkwNjZZaW5HQVhKSnc9PSIsInZhbHVlIjoiVi9EanFwbGZRWU9LOTdBYXVFTHRwT0gvTURobHdsZVo2V3l5SmNPRjdLUUFLRnJEdXgvZDNzNUk2bElKdFdCQXdaVE1xVUhma2tqdVUwY2RXcUNCblhZQTcxMzB3NmtQK3VDd2lvd0tJR1pia1VDUU9YVjhGQ3FiaEw2a2JQTS8iLCJtYWMiOiI3OTgyM2YzNDdlODVmMDFhMjZjNTgxNDYwNDE4YjgzZGM2ZTI0YzAwZTVhZjMyYTc4OGM0MWNmMGIxMDRjOGMyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:47 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImNiVXdwV2VKZzlVdXk3VjhNRE9ZYkE9PSIsInZhbHVlIjoiWHRYTUFQaHdhVjRBMjFXZXdCSnV1V2JrMjVaVWo2dVJyaW1MMWd
hWmQ1UUxhUFdiaWNDdGVnWm5layt5MGJmWUd1KzJDMCttbmVZaDhwcHJLV3Q3a1B2cmhhZmdESTNmR2NSNGIvQjk3Wis0bWtlWWdyV1pEd1A2cnVidklxeX
QiLCJtYWMiOiI4NDgyM2I5MzQ0NzhjZmY1NTE2ZGVmYjk1NTZiNGQwZGI1MTIyNDFlYTUyMzU2YjNkNmI5MGZkYWQ3OWU5YzVjIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.77. https://adblbackend.peacenepal.com/admin/vendor-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IklLZ2pHZ0s3eWFZWkZCVWdsTnMzUGc9PSIsInZhbHVlIjoiZEsxQ1RiRnRJeXBQNTVNTHRHMkVIOEZRRFhVZmVoTjNpTUJwb
ml5UmJuQzZ5YlhqK2s3SGlJeldWYXVJL0Y4bXVseEtVQTZtT1JITHN6SEpVL1p3WTlqSFlaSnkwNmRDRm9FeDFOUmdwT2VhdjZLNEJnQ243aDBIOWhmcjNFYko
iLCJtYWMiOiJiMWJkZTJjMTZhMmVkZmFhMTdiODA5YzgyZTg1ZWNmOGJhNThhNTZhNGQyNGFjZjQ0MzE4ZGNhNGU5YjhiMjQzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:55 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkplVDRvRzByOE9PWTRLQ1FPbEVoQ1E9PSIsInZhbHVlIjoiTHBkZDdObldFUCtVY2g3Q2l4Y1hlS0ZrcExKcGsySURmTUFjV1Jac
UdxSDdhd3dhaHRSL1BMdC8rUGZjTUZrSlhZaVlvVkU5Wlo3eis5Wk5EM20wc2ZOZ1AzUDlNMjlmOHdtdFZBODFCbGdyTjhwQ2RJWk9qUnF4MDI5NS9UWmQiLC
JtYWMiOiI2NjNkOWQ0M2MwMTg5YjA4ZDg3NGU0NjhlM2E1NjY0MjgyZDI1MjVjN2ZkMWYyNzUzZDhhMmI3NzBhNjY5ODMzIiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:49:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.78. https://adblbackend.peacenepal.com/admin/vendor-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik1PT0NocDBhQ1pHV2RTblNmYmlaakE9PSIsInZhbHVlIjoicUdyMjA2NDRnZVBPV1Z1VHhrbkswM1N2ckFJUThCSEl6eXNhK1pX
WHF5OFFGdVBzQ3NRKzFqYmJ4bWMySFNQQlVOMGlMaSt2Y2dKOENxbjJudkhEbWJqZmRoQjR2WmJtWGlNMlRTRWd2Q0ZFOVprc2c2akV5VlY0UVJnRHhuR
FEiLCJtYWMiOiI5OWFjZDI2N2YwNzNiODlmZWNhYTMwZTczNWQ4MjViNjJmNzcyMTg4NmYzNTU3N2NhMDBkYzcyMzQzNWQzZmQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:51:39 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InRVQUwrajhOaEpzdHd0UnBjZnZpc1E9PSIsInZhbHVlIjoiSWlERGgwZHR4Vm1FbGJHZmw5V0hNbUQrcXNEUXlOSE0vN3RoaX
VvNVFaeWN5OGlKQXUvL1BZYVQvWGRuQ3VTZTgyMWVjNFAwbi8wTGJFanlkSVFqN0RDcjFVZk9WL1JuWjdibFBhSXFhY29jZTNwcGc1NTlQY2o2RHZxYm9Xc
04iLCJtYWMiOiI2ZmQzMWI3OWUyYmVjOThjY2FkYzdmNjQ0NjNlNjJkYzA4YjdhMzBhNjEyNjI4Y2NlZWM4NjQ0NWVhZDE5ZDQxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:51:39 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.79. https://adblbackend.peacenepal.com/admin/vendor/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/vendor/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImxLaTNZZXc3eGlBSXpwVzllNnVuUFE9PSIsInZhbHVlIjoia2Q0OHE0OVRaUURDVU53NnJaZ09BYkx4WnNJYUM5bjUzaVFFQU
M0bmsrV25sam1DRWtUSUtZTVBHMmV1NE95US8rMFlNbGlXYnZzd09RVzEwc1RnYnhrTWl0dlVLVW1oWnRYejRyemlhNll2aWl6NnN1b3FJNHQ3TE5vZWxWcDc
iLCJtYWMiOiJmYTNiM2ZlM2M1NmFmYmYzNDdjNDJhNDBjODVhN2U4NDRiNTBlM2ViMDkzMzgxYTk1MGM0OTg3ZjcyODJjZjY0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:50:10 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImZUcDEvc1RYczhlc3JhNEdXSDNUNUE9PSIsInZhbHVlIjoibHhNMlVhUkE3b002MHZhMXJHQnVlWVExb3Z2dHF4YmhzbjM4TFF
hQ09FSDJZUkUyYkFjN2pWZkwzRU1GZkhCc3BpRnJqSXgrak1tVmFjeFhTajd4L2hESDQ1a1dPcVZVVHJ4UkNNYUFuTElsUTVFb1IhZERjcXhNQUNwem5zY3giLC
JtYWMiOiJiMTE0NWFmOGY4OTBkZTQzNDQ5MmMwNmVlODk2NmY5YWUzZmY0NWMzYWY5NTc1MDU1OGIzMmQ2YjJmZTc4ZDFkIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:50:10 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.1.80. https://adblbackend.peacenepal.com/admin/vendor/import

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/vendor/import**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request.

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor/import HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhRdFp3WlhhNHI0ZFZaL2thVURyT1E9PSIsInZhbHVlIjoiOWl3Vmt2U2EyVkZqOW9iVFZ6UWlBa0E1NmpVbWdYRFcvdFR6Tlp2V
zJRSUZrRGZNOXVoeFJ3bnAwNnQ2clBuNTY1YSttUFhyT2ZXK09KZmc0ZEY0Z3BqaXVvNzJmTk9OMG92NWt3OVMxZ2lyYXlhSjNYTE1TQkNCYmtsazdJWHciLC
JtYWMiOiI5OWRiNGIwYzY1ZjcwZDU2NTRiMjI0NjJhN2I0YWU3YjRlYzQ5ZjU2NWViNTU2MTRkZjFhNzg1NWJjNDhlMTU3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://adblbackend.peacenepal.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:50:17 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IndFYWxsNWJsbWQvWkxCZXdlb21Sa0E9PSIsInZhbHVlIjoiUDBLOGNCNmo0V2pndXoxVzBpSjhsNUR6U1cxMGQ3MVNKUXdpZ
lAzVTlDVlQ1b2pFcVdZTGMrU2RTSk9LRDAzaTJyUE95UmhrUWMxeTdmdUNnTE1rc0w1dHhDK0w3UU02NEZTY1FETFdNQ2g3NDVxODBBNGo4M08ydmZLUFJ
BdDgiLCJtYWMiOiI3NzA0OTUwMmJjZTRlZDY0YWMwMDIwZTY2OTMzZjI2NjEzMTdkY2U3ZjEzZDgzMzZlNmM0YTUyNWEzMjNhNDkxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:50:17 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2. Cross-origin resource sharing: arbitrary origin trusted

There are 80 instances of this issue:

- /admin/account-type
- /admin/account-type-category
- /admin/account-type-category/create
- /admin/account-type/create
- /admin/admin-type
- /admin/admin-type/create
- /admin/atm-location
- /admin/atm-location/create
- /admin/banner
- /admin/banner/create
- /admin/blog-category
- /admin/blog-category/create
- /admin/blogs
- /admin/blogs/create
- /admin/branch-directory
- /admin/branch-directory/create
- /admin/contact
- /admin/contents
- /admin/contents/create
- /admin/dashboard
- /admin/download
- /admin/download-category
- /admin/download-category/create
- /admin/download/create
- /admin/faq-category
- /admin/faq-category/create
- /admin/forex
- /admin/gallery

- /admin/gallery-video
- /admin/gallery-video/create
- /admin/gallery/create
- /admin/import/atm
- /admin/import/branch
- /admin/import/store-atm
- /admin/import/store-branch
- /admin/interest-rates
- /admin/interest-rates/create
- /admin/layout
- /admin/log
- /admin/login
- /admin/logout
- /admin/menu
- /admin/menu/create
- /admin/module
- /admin/module/create
- /admin/news
- /admin/news/create
- /admin/offers
- /admin/offers/create
- /admin/popup
- /admin/popup/create
- /admin/press-release
- /admin/press-release/create
- /admin/projects
- /admin/projects/create
- /admin/report
- /admin/report-category
- /admin/report-category/create
- /admin/report/create
- /admin/reset_password
- /admin/seos
- /admin/service-category
- /admin/service-category/create
- /admin/services
- /admin/services/create
- /admin/setting
- /admin/team
- /admin/team-category
- /admin/team-category/create
- /admin/team/create
- /admin/training
- /admin/training-hall
- /admin/training-hall-bookings
- /admin/training-hall/create
- /admin/training/create
- /admin/vendor
- /admin/vendor-category
- /admin/vendor-category/create
- /admin/vendor/create
- /admin/vendor/import

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.

If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

Issue remediation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

References

- Web Security Academy: Cross-origin resource sharing (CORS)
- Exploiting CORS Misconfigurations

Vulnerability classifications

- CWE-942: Overly Permissive Cross-domain Whitelist

4.2.1. https://adblbackend.peacenepal.com/admin/account-type

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/account-type**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ywttefhiddaz.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ywttefhiddaz.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:49 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlVCUy9nZ2FBTWErZkRCbHc0bStCN3c9PSIsInZhbHVlIjoiL3hkcUVGZEQzSWswTFd6VjJDdVhsS0VpWUtTRkcwSlJLaUJZcXRQ
WGt2M0xyT1hleGxvVFhQL0k1UmRXbHI2RTlwTStYdnlBOHo5UE9BYSs2UGU4ZUt1UzZHeThyVGNVdXZadWFHYjZmdjFLeHd6RC9hUXRRMkRib3l5TFdIN3UiLC
JtYWMiOiJkY2JmYTg3ZTgyOGFlZWYxMzEzZjZkY2VkMmQzNGNkODY0ZDZlOTdmODQxMDgzZWYxNTIyYzgwMzljNmE0YjFkIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:59:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 342933

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.2. https://adblbackend.peacenepal.com/admin/account-type-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/account-type-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://fyloegdnwwrg.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://fyloegdnwwrg.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:50 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImJmUjdEYXhGK2t3YTI0ZlBva0MyS2c9PSIsInZhbHVlIjoici9LcmVNOWRVOUlpL2pIajd2OSszMEdDYzNtZkVlU3NPZ1k5aThLT1J
MaHFyd2V5eSs4TmZ4UTRCT2dlRDZ0NHAxdDNoNWZFaTFUU3VzUlVLMlBaVkcwQk9OcUR1RWh6VXpBOWNLdWNkQUhOeGxqelZEejVCVXJ5ZWpIUnRhYzki
LCJtYWMiOiIyNGFhY2YyZWE3MTRkZjUyMDg4ODFhYzgwYmEyNjM5NDgwNTFlMWFmNTljNzVhMDdlYzZiOTA4MTEwMjY1NDEzIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:59:50 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 371544

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.3. https://adblbackend.peacenepal.com/admin/account-type-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gqecudgkkoui.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://gqecudgkkoui.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:46 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZNZHcraDBrQjA0bGFvR2tYa2h4V0E9PSIsInZhbHVlIjoiNCs2bklmK21ueDVCUzZXeCt3ZEQxRkxUWWxSZlVsM2VQM1JhZTU2U
3JZNHhKSGJFbEhET3liOWRwNVBRaEJzUk5lQVJROXFocmJESExYdUgxMElsTFFNeElyVEpSQ0dxTjBHdmlEdXRzUjhrV2tsS0tzM01qbUt5ODR5Nklwb2oiLCJtY
WMiOiI5MmZmNmY3MGFmY2MxMzdkMGRiNTQxZTU1NjEzMjBlZmZhYmRhMDU1NGEwYjMwYzU4OTFmMDUyNjk0NDA4OWE4IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:59:46 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 86621

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.4. https://adblbackend.peacenepal.com/admin/account-type/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://dbptkvrevljt.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/account-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://dbptkvrevljt.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:59:55 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlU4YjQ2ZzhQZVg3SDNITUtwU2NIOVE9PSIsInZhbHVlIjoiNG9Vc1VobnJjVVUrVGMxMkUwL2lqc2NtRnBEanZublU4LzdjUkgzOEll
RXhUcDNTUnRkS004Zk9zbkRsdTl4dmtSS2dkbENwNlFDczBTNGpzQ3g5akpGZ3VzOVdPT2VlMURONUnJLTzlIVDRzVE50bmp4ci9NZ0x2bkJQa0xmUlYiLCJtYWMi
OiIxZmM4OWM2MGExNTZlZmQ0YjA3MTY2MGM5Njg0OTY4ZmRiOWY1NGZkZmYxMTlhMDQ5YTY5OTE2MDUxMmQzMDJiIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:59:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 99720

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.5. https://adblbackend.peacenepal.com/admin/admin-type

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/admin-type**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://mqtkvfqzoycf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Origin: https://mqtkvfqzoycf.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:50 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlRlYVlsaXh0Q0p1K3JHbnl0a3ZEK1E9PSIsInZhbHVlIjoiNENLUjJCeVBaaVlxa01xQW1TTm1EVk5JaWVpUGowTmJhWitlTjVYMW1BNWZBMStVbFVYRVAxWHNxTGFhTW5zYUQvOFRSTmhmVWdmbDAyd0Q2dzgvdCtvUWJnei8rNXQzcCt6NDBBVlZ3allZOXU3Sm90dThOUG5sMjV5SVBwa1kiLCJtYWMiOiJiZDU0M2RhNGQzNjc5YjI5NTJlMDlhZmIwN2I0MTIyNTE5MDI5YzRjNzExYmM0MDNlOWIzYjg0Y2NjNDYwZDQyliwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 13:56:50 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 74260

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.6. https://adblbackend.peacenepal.com/admin/admin-type/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/admin-type/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jmiukguxnkzf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/admin-type/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/admin-type
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://jmiukguxnkzf.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:51 GMT
```

```
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ing0MWxWVVVYQmdjVUF3Q2FRUFZPK1E9PSIsInZhbHVlIjoiVWw2bDNZMnZUeHhtTVJUZW5FWXJ1cjdKYXZwV0RiZlpsaGVve
FpMR1lpUCtpdGs0RVFUcDN1U0RpOGdXSFJrdXVFdmhqd2FTZUhSeCs0SzdBRUdOOVlleTRoSzU4VzVSQlpzLzBqdVRpMkZQVXEvdk5iektBNTFTaFF3K1BBak
8iLCJtYWMiOiIzNDUwYWEzNGFlZWJiN2M1MDI4YWM2Y2RmNmMzNzNkZGY2N2VhMzQyOGEzMGE1NWU0MzhlZWYzNmQ1OTQ1M2JlIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:56:51 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 65094

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.7. https://adblbackend.peacenepal.com/admin/atm-location

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/atm-location**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jzebuigklyad.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/atm-location HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://jzebuigklyad.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:57:46 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
```

```
Set-Cookie:
adbl_backend_session=eyJpdiI6IkFoRUFRQjg1ZWNES3RqK2ZKS2RueXc9PSIsInZhbHVlIjoid0YrUVdhSC91RHhDLzZwMldobkE3ZVl0aGh5NzRuazFXOHFMNGJt
MDU1WEptVnZvM1IvSm1PQjFFbVU1ZFFHV09RcWg3czgraXBTOVFtQmUvQkpwMXUveUs3UU4zYkVwMXMydzBqZGNHeGFIUG0rOUZMaEowZU5BNkxzdG1tN
28iLCJtYWMiOiI3ODc4MzUzNTVlMzdjZTI5ODE1ZmU4MjFlMTZhOTY2MjRjYzc3YzBiN2ZkMjkwZjdkMzMwNDg0OWUwOWFmOTQyIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:57:46 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 79125

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.8. https://adblbackend.peacenepal.com/admin/atm-location/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/atm-location/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ckjnrddssbwq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/atm-location/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/atm-location/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ckjnrddssbwq.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:58:22 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlNBZG5PVDVpZkVPWmcrVWNUOTU3dnc9PSIsInZhbHVlIjoiK04rdkE1SytHamhZZmQvdFpad21pNzlqWlcxbnNObjZQWnZKNUY2
N3JJSHp5UEZrMGMzczV0MnEydm1ST2RCRFpBYmg2VmxWbnVieUs1K0pLWmVjc0ZVU2VXWGlPTVNmdVczYkd3NnNHbXJpa2dVQ1g0UHREUjJCZVYySlpMTl
liLCJtYWMiOiJlMzAyMTNiZjlwMDczYTQ2ZGYxOTNmZDNiNzg5MTU0NzMyZjkyZjUwZWVmYThlNGJlOWRiYzRmMmZiNjFlMWQ2liwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:58:22 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 90483

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.9. https://adblbackend.peacenepal.com/admin/banner

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/banner**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://djkwurslinpe.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/banner HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://djkwurslinpe.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:58:00 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlU5Wm10b3lJR3dLeStLMXBDUFc1Snc9PSIsInZhbHVlIjoibzZ1SzRBOVRveEdXTW5PVk5HSEdnT0crMmVjSERzU1lxOEtmZjJ3Yj
hWMkREdUY5Tm1ZdEtXWXdNYXVYR01pUVpkc2krUlhRWDd1cVBLRWxYVm03bFBsMVN6M0Y4T3J6d1h4NlFhS09FMzVMSDNrZ3p6NDFqSk9BcmZqTFVLTGgi
LCJtYWMiOiI0ODc4ZGY3NGI1NWY1NmYyOTNhMmJkODQ4Njk4YjUyYzViMTlhMjU1YWE1OGNhMzg3M2ZjMGI3ZWY1Nzg1NjUyIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:58:01 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 79426

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
```

...[SNIP]...

4.2.10. https://adblbackend.peacenepal.com/admin/banner/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/banner/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://dgcblztogpax.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/banner/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/banner/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://dgcblztogpax.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:05:27 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImN1U2k1bnMrOThIaUp6THBDMTZlWFE9PSIsInZhbHVlIjoiUmhxVkdKUkZqc3RMUXRKY0FlOFBPM2FQRzFXbFNmeVJuTEtHN
U9vNldSUG1iOUhabzBPaVRxSkxUUDhVci9sOENVVVA4cnhNQXhXV3lsMnVnNy9kbXppcXJBbDQvS0tBSCtSZGgwMXVVWnhEODZ0NFZZc3V2T3R2bm42UGt3
WGEiLCJtYWMiOiJhNjA5ZDk0YzlmODdjNmY2ODdlYWZjMzhkYzM2MzNkNmVlMGQyOGJjNDQxZDY3MzAwNDQ4ZjQxMDU0NjAyMzMxIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:05:27 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71556

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.11. https://adblbackend.peacenepal.com/admin/blog-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/blog-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://srxylwzwkmxe.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blog-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://srxylwzwkmxe.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:42 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImRzOGl3SkV2SU9LMlJ6NmlKcmg2d0E9PSIsInZhbHVlIjoibDFXbUprZWpHV1RFdXI1Zk0wV3g3L0ZSNDJEcGIxQ05HZVYrTnBiZ
UFKeW9JREdtcjJZMHI1WmwyODhDSUxQYVRKSlFySGtqc1R6cURBOVRFV0ppT3FvR3ltbVplUTRhNGFpamZ4MFE2T0l4SnBBb2JUMDVCSkNpczVFNWxBekEiL
CJtYWMiOiJlMDgxMjhlNjU0ZjEyZGExZjcyZGMzYmQ1M2ZiMDg4YzliN2FhYjFkYThiNjBlMDBhYmYzNmQyNDM2NjUxNzY1IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:06:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71451

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.12. https://adblbackend.peacenepal.com/admin/blog-category/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/blog-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jklddpryvcvl.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1


```
GET /admin/blog-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blog-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://jklddpryvcvl.com
```


Response 1


```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:08:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ik1HVWk5ZncrWFpDSWxZNXVoNWtYcmc9PSIsInZhbHVlIjoidmJ6V1ZlVzlTbjZlZTBMb2pTVDdwNmo2ZnEwQlFGNGlsbTJ5cDhNRFRXOWpYa3NxeWE2eUlJR3RLNzdRVEpUV1dZTkJyWGRCL3o2TWJCdmxMR2I3QldkVk5zVjZxbk83ZmhRY3dWR0JCOVZheGQ4UjlmWUtEMzJRcHcvMTZPSUEiLCJtYWMiOiIzYTc4ZjNlZDhkNTBhNTg2NThlZDQ3OWJhMjQ2ZmFmNjEwOGEzMGQ5YWQzOWUzNTg3YTM0ZmMyMWQxZTAyNDBhIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:08:53 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 68105

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.13. https://adblbackend.peacenepal.com/admin/blogs

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/blogs**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jltyjcvwvbao.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blogs HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://jltyjcvwvbao.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:39 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjZFSkljYXBTMXorWkxPQlljbDRyZnc9PSIsInZhbHVlIjoiK3R5L04zczQ0TVJ3WkVUdlhXZjZYaTZvYWJ2UXd6MVZkNzB1eWxtNE5S
UndwWi85L1VMSm0wck1DWHhWcWhyOTFvTTUrZUhsNkxYU2cxWWJnMEtjdFo5UHplNjBwMzBic25OL3czVktaRy9WWjY5ejFqbWZ6dHk1TWNueHVyeHEiLCJtY
WMiOiJlYWIxYzVlZTQ1YmE2MDE4MWRmYmYyYjZlZDYyOWY1YjFiODlkNjRjZWI5OGQ0OTFiM2ZiNGI1ZDIyNTkwM2Q5IiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 14:06:39 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 104431

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.14. https://adblbackend.peacenepal.com/admin/blogs/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blogs/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://hsioqewehway.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/blogs/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://hsioqewehway.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:13 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkVMRzcxbUxsNHJnS0NZQldMLy9jTFE9PSIsInZhbHVlIjoiOWhsMEhGS2EvZUhPZW9ldXBzQ2xOWkh6bUJGeSsxVjR1NjVyYnFo
dXFPM3Q0WlpMZ1dVUGhJeVJHMHcrUnJLanh6bHdBYkhpekVkYXlsNnRSeG5oZzZ2Y2JaSHpxUTl0Zyt3NU1hdnVTdWhJU010YXRqR0Y4cXBzeGJ5RkI4d0oiLCJ
tYWMiOiI4NTU4MGNjYmEyNTVmZmE5ZjA2ZDZiNDg3ZDlmOThiYzI1YjFmOTNjNzM1YzY5NzNiOWQyNjRjYzZmMTAwMDUyIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 14:09:13 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71863

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.15. https://adblbackend.peacenepal.com/admin/branch-directory

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/branch-directory**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://mhcmrsnxvfll.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/branch-directory HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://mhcmrsnxvfll.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:06:01 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ik1JSHRqdCtPUk9WdjV3OEk0NEpneVE9PSIsInZhbHVlIjoiY2FGT1VBNmJqckVOSmZmdUdxMHNYWlVhU1M2Mlo2M1dYaDJpM0
xURGJpL3NEK3FEMG9FQzEwM1ZjQWRiT3UzZml0b2lzVG1ybjFReE5WRlFRN0J4eGswN0V0ajExSDdLeE4ySW0vRkFZOENuVkdOdXI4ZVZ4d053SVk2RGtyUX
UiLCJtYWMiOiI4NjJlYTYyYmFkOGRjMGI5ODM4ZWNhYzlkMDVmNTY4ZDY4MmNkMWNkMzhlNGM1MjUxNmUzNjVlYmFkMmJmNWNhIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:06:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 76069

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.16. https://adblbackend.peacenepal.com/admin/branch-directory/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/branch-directory/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ihcfroiysvvp.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/branch-directory/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/branch-directory/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Origin: https://ihcfroiysvvp.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:07:42 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImVVaGJDZERjeFdxSk4yVGpXYitUMkE9PSIsInZhbHVlIjoiNzc3WjVRbVRvYjhpYU9FNjhsdm1yZjZZV3JzWEJMR1NnUmtDUGhWUXFGZVNzQzA0bGhuNmVWcndQVlNnWTVrck5RZTdudk9MS0ZzOW4ybTBNd2QyUytRVzJETW1zL2tXOTZqWExpSlBoZG1NWXpMQzZNcjN2ejVFaTA0c2IxL3EiLCJtYWMiOiI1ZWNlY2Y1ZTM1NmRlNGJjNmJiNjNkNjgxOWI3NmJhYjJjYTlxOTczYjRjNmVhMzc3OTA0M2EzOTExZjRjYjFhIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 14:07:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 95114

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.17. https://adblbackend.peacenepal.com/admin/contact

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contact**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://kqvyvyuyrqdg.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/contact HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://kqvyvyuyrqdg.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:10:13 GMT
```

```
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InpqK3JZWk0vZFptM3k3QVY0WWdacGc9PSIsInZhbHVlIjoiRUhTMXNBMVdDbjFrNnVPUzE3WUxObVp0M2xDM0xaTTRXQTU2dmhRRzZ3QlNWdFlHOGxBSEc0QStwaVY1Z3IyZlZSNnJJelF1R1IyNmRYbmplYzZuNE5BS3BwWXh5WWlyRUdjaHVZdXFCcDQwL0dxRjAvdk14UW5GV1MrRUg3elYiLCJtYWMiOiJmMzQyODMwNTMwNmEzNzBkMmNhNmNiNWMzODRhZDYxOWRmMWZmN2U4YjYyZmRmZWY2MmVlYzc5MTBkZDViNDk1IiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 14:10:13 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 170816

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.18. https://adblbackend.peacenepal.com/admin/contents

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://vwflgvfotlyn.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/contents HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTNMWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZnRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://vwflgvfotlyn.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
```

```
Set-Cookie:
adbl_backend_session=eyJpdiI6Imx5UCtVWmFwTXM3Wm1sWWFaWEkxUVE9PSIsInZhbHVlIjoiUGpvYWw1bWFSMkhocmdOTlZZYjlJU1JDRTU5ZjlvbXdvR21XV
Vl3d0pvd1FMVlUyZUNsNVpZLzR4VExnSjNqUmVFbTRtanZENVI1YkRqbSsvMFlEMkdqd1ErcEpOaDhzMXU0MG9VTG5MazFsczlUSkxDL1R1RVVMUW01bmJzT
WQiLCJtYWMiOiI5MWM3NDc1YTBiMjRiMmJhNzJlMzFiMDNmYmQ1ZGQwYWQyNTM1ODdlMmM3ODVlMWU1NTg1ZDllMDZiMTFlNWE3IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:09:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 247045

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.19. https://adblbackend.peacenepal.com/admin/contents/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://uhqhsbuqeshf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/contents/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://uhqhsbuqeshf.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:09:44 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkQxang5dkpQdGkzU2pqYkdYTHlqY3c9PSIsInZhbHVlIjoidTRaaHNaR0swdThzSWFNUjQwSGx4eE9kYmJScnFwemtYc1djWFhZN
HNQRk10YmQrczVmdWNNa2pibUFaanViV1hIMi9FdWhhOVVlUWkrOXlDQ2owbnI3WSswbm1iM2R3QWJkaEx5TXZkb0NuTElRVlMvc0xtTHFDRmlqMU1wblUiLCJ
tYWMiOiJiODdiNmE4MzJjOGZlYTBhNzQ3YmQzMDJhMDY5MmZkYzBmY2RhZDA5NDBkNWJiMjFhOTU0YWY1Y2ZlZjU1NWVhIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:09:44 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Content-Length: 86991

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.20. https://adblbackend.peacenepal.com/admin/dashboard

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/dashboard**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://kvdxexvhehrp.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/dashboard HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/login
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://kvdxexvhehrp.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:10:31 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImRRSHBMN29ONmlJdUlVY3Q2SnpFMXc9PSIsInZhbHVlIjoiRUo0NW15OEl1cHU0Ry9PNDhBelY2SDB1bHViSFZwYTc1VFBKV3
FTTGJyRjZRaFZUeG53SmF4cVJDQXh3cG83ZTRuTFN6VnRxbnZBdHdlWEc2UHRrYW9VTUo0NlFQYTdKVEVoaHRsVnQ4eitkV21LNDEva1dpQ1NmUFVBano3N
jkiLCJtYWMiOiJjOTYyMmJlN2RiYjJmYzZlZDM1ZGFhZjI4MjcwZGE4ZWNiNzU0ZTMxYjJiYjdmZmIyYTQ0MjY3NThlZDBhYWVkliwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 14:10:31 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 69001

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
```

...[SNIP]...

4.2.21. https://adblbackend.peacenepal.com/admin/download

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/download**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://evwnnraanwwp.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlBOb1VtZDFxUFkvRHp5VkN6am55Vnc9PSIsInZhbHVlIjoiQk5CaFJRRCthVDBpUzNsQlFxSUp6U21oN3N5OW5WV3BvR1pOMTN
MWmEybWw4Z1prRzJ4M1RsZXAxV2M5TFc4S1pUYSs2N2hPMHNacTFrM1RFbnUrWWtnMUZGTmQyVXRVS0l1cmZOUkdob3lheEJiQVU0cENWVHBwSEo1eEZ
nRW8iLCJtYWMiOiI2MzlmY2VlNDA1Yjk1Y2U1ZTE2N2Y2ZjlhYTQwY2QyZTY5ODhlZWUxNmYyM2M5YWMzM2UwMTJiMzEyNWFiMjQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://evwnnraanwwp.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:11:08 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxmRUNvYmNFbnc1c1NOM3ZCRitpK3c9PSIsInZhbHVlIjoidVNiNDh0OUlBM3l3SmNkZ0VNOGE2cG9IS1IndXdYVjhlSnRma0tPU
TZ3eVU5OU5oNXh5a09uTzBoZU1YbzZ6ZXArTno3NEVOV0JwVUh4QjJYK0pOa1o5eFZrbFoyZ1pFSFg2Q2FrWXhwNWZwUEw1a3ZaNWZPSkcrZUZRT1J6RlciL
CJtYWMiOiI2OTQ3MDQzM2NkYjFhMzc0Mjk0MjRiMzI5N2U2YWRhZDk2OTQxZWFiY2YwOGMxZjFhYTgwZmQ1ZTNkYTFmNDg0IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:11:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 90495

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.22. https://adblbackend.peacenepal.com/admin/download-category

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/download-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://avyppuotynbg.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjBZZlY1RFlUYmZnRUxMTkE5UFZjdlE9PSIsInZhbHVlIjoiU1JXZGhpRTNFYUd0NC8xdW9sNlNkZjVuZ3B0MUdMSnpzdlRFVTV0dzRRcVV2WkF6OVRTeXdYUWtoazJLZ1RKU2VMQnRtMTVyZTRRY3dxRXhLWjhXdDdyb01kZFR2UjJZSEFjeDIIb05ESExnSzJVdUpUSXh1K0NUK25tUWRESXoiLCJtYWMiOiJiNzIyZjZhNWQwM2UyNDFkMTgxYjExODViYmNkMDZhZDkwMjU0OWEwNzQ1NGRjZmYwM2Y5NDc0ZWRkNTc3MzM5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://avyppuotynbg.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:20 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ing3WXg2YlRvdm13SU1kOUhoTWp5Wnc9PSIsInZhbHVlIjoiZlJwWUIrUERnelAraHIvenluVS9uUEQ5NFg3TFpJWUJFOEQyTjk3MmZMYXcwMkpHQ0N0a1FaaXRkYWQ1N0llVEhzaS8yc0Q1WjJMU2V2U3ZRc0VBbjZjcEg5ZUdPemhaY1pLU0gxdis4Z1BWendhQklwZzYyRGdmQ3FkV0ZtQVgiLCJtYWMiOiJiMjRjOWMxNDg3NmEzNjk3MWFjNzNjMTYxNWJhOWM2MWQxMzViMDFhMjAwNmQxMTRlMzVjODhiZDA3MDU5MDMxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:05:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.23. https://adblbackend.peacenepal.com/admin/download-category/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/download-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://lchhkhskcwxx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IktjTWtyWjI0VkFJMmJRTS9jbzhJVnc9PSIsInZhbHVlIjoibFIrQU41Zm93UXUxSlZuTHI4UStLaDI2YW1Rd25ZOFI4bzBySHJvY295ZHI4T0NZNDJhbWh6RzI3dVNRY2ZzM3hDbVA4S1k5U215Tk5DbnpGWU0ycnlnTFgreXREOTg4OVA5U1phMURQWW1EODk4ZTVIVngxVDVjSzkwOGdha0UiLCJtYWMiOiJkNmY4NGJmNjViOTcyMDIxNDU2MjNjZWEwZTA1OWYxYmFiYzY1ZjI3YjU5MjhiMGU0NGNiYWQ3ZWExYjVkNDEyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/download-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://lchhkhskcwxx.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:52 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlltUXlLdHdlZDZqZkJtT0dTL01TOFE9PSIsInZhbHVlIjoieFJNOVF6NkF1bUFPVllSNUVnTFowaVhDZlRzQzdFMXpkaGVjeHZxTGhYN3ZLaUhpSlpUQlkxd0JnVlRUeStXQU05M2pjMnJXdkJjaE8xbTlzQUpFNXNYeGhTMWw5QmtOUmVTUzdwWUdERGVvMDU0TGxGNTVNSWxKWU5pZmhvL0QiLCJtYWMiOiI1N2ZlMWQ5N2NmNjllN2ViMTdjZGZiODNhODE2YzU4MTlmMjc1OTc3ZTc0NDIwM2M2MzRiMjBiMGE2MzM3MDZhIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:05:52 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.24. https://adblbackend.peacenepal.com/admin/download/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/download/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wgmxgdhaidfv.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/download/create HTTP/1.1
Host: adblbackend.peacenepal.com
```

```
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InZ6NENzTEJaeU51MUZ3NzV4UkxWK2c9PSIsInZhbHVlIjoiWjkyWk03a0Y2S3k3S0N2WTVZRFA1a29MNEU0c0d2QTdTWGFyMz
VHMlRvU0Fya2g3bWY4MDdqNXFPWlJQSWUwVHA3WERqa2xad283T29vRVBNRENHYTZTV0JsMGNBbXNmeUkybGMra2k1SXdRdjNxb015UVd1QXBzcXcvY0l
sUXIiLCJtYWMiOiJmMGRiZjlhNWFiNWQ4MDUwMTdmZGE1Njk1Yjc1MGE1ZGM5ZDU0ODhmMGUxMWY4ZjNhMTQ4Zjg2ZmFmYThmYTcyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/download
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://wgmxgdhaidfv.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:27 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkJhMXhHY2djUVM1QkVtL0JkczNYVlE9PSIsInZhbHVlIjoiL2dIb2FES0c5WUpvcU81NXRFbXRNZEJnQ2VuNjNudlNmWklkU2VYSn
NJdXdKalJaZGFaRE1ad3R0eVNLZ3Z5elRDWkIySmMzNzI4LzZ0TXFyc1I5QWVSUWJlUGx6dm1PVGx6bVErMGRLcmtOejlCa0Q0NDkvSFhmcXNrZVdhZzgiLCJtY
WMiOiJlZjMyM2ZmOWExYWQ4MjE0YjdjNDIwYThhMzliZDEzY2E0ZDUyYjRiZTA2ZDMyMDc0MzhlNGM4NmFiZWQ3YWNlIiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:06:27 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.25. https://adblbackend.peacenepal.com/admin/faq-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/faq-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://kkrubneqtkaz.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/faq-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjhQWXNtR0Q2MVY1Nit5R1hjWXY4anc9PSIsInZhbHVlIjoia0N2V2plYjBqbGRFc29zRUlDRUxleFg5VUtvaFduaUtUWDNzdXlkZU5
OUEpNWkQvVlhzS09oS2x6RWdOaVpjeCt6QUtrQzNLMU1DUzNISFE5MGxZdDh3L3ByQnlnenk3bkZiRTJwaVZZQlhOampQUENkdG54RStPT1ZER2tDTTAiLCJtY
WMiOiI5N2U5ZWY4ZmI0ZWNlMjA2OGJhYzliYjE1OGNiNjgxNjRlZTA2MDNhMzY0Y2E3MDE4NGY2MmExMzY4Y2FlZmY4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
Origin: https://kkrubneqtkaz.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:23 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Imc4Z1VoSXIvcmNBd2FjdDg1S2RKZnc9PSIsInZhbHVlIjoiWmprNmdYRVFjUmFyWmJHMUhETnRiZEVYRG03VlVWN3V2b2hFak
RZRnpTVkV4VVU1KzZodzJQc2pUc1dIY0hjaXB1eThDZjh0ZUExK3FJL2RzbmRudEl1dHhZOFZiZTJ5b09XMHlXN2Rhbnp6eCtNMlB1Z243RDJHek1SU2duVWEiLC
JtYWMiOiJiYWIyYWIyMGE5NTFmYjY3Y2E4OTQ4MmY5NmM3OTIyOGFkMGY3YzcyODFiNjMxMWYxOTU5M2IzZmE3ZDVmNjE1IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:05:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.26. https://adblbackend.peacenepal.com/admin/faq-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/faq-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://mdbwdcoerfsd.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/faq-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImJvZXVMYXFGd3hhNGk3V0FvallFeEE9PSIsInZhbHVlIjoieC9JVHRHZWt3SEZJamVWQXRzeHdLdGdJUUZ6c1RNTTVsd1ZiZjlh
ZDYzT1o2UGgyNG9xT3QwWDR1am9zYU01T1BvZnJuc3k4MlV5bEd4Z2xZQlIIOXBQWEZ2NmY3dTF4bHRwZ0g2T0Q4R0Z5KzBDdXJ0c2JGZHpaVnIzalRQeVYiL
CJtYWMiOiJhOWFlNTI3M2M1ZjI0MjcxYjdlMmFlMTdlNDk0ZjFkMTkyN2NhY2QzMWQ2MzRjZjcyOTFkMzIxM2MyNTQ4MTAxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/faq-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://mdbwdcoerfsd.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:05:55 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
```

```
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImJWYVh6b3pHcE1HWlBnQnV3cmlZalE9PSIsInZhbHVlIjoidjlDR1NtcW15ZDBXZzZvczV2ZDZKUnNNaWtHSjA5ZXljbThCR2VKYlI
2MWcwS0ptMHkycXNnUTRvSmU2WW5FRTJmc0h6ZTNuR3E5ZlRhcmptbjlPdHd6RGJLUUN1VkRTOG9hZUdJL2VraVdzbEVBZWxjdGZlYTBWTjZ2WEZvNHliLCJ
tYWMiOiI4ZjQxNTU1Y2JjMDNhZmY1ZTAyZmFhODgzMmMyMDI1ZjliNzRlMGRkNmYxOTY0Y2I0OWUwOWJmMDViMDExM2Y4IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:05:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.27. https://adblbackend.peacenepal.com/admin/forex

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/forex**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wnxqbpmzzmcs.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/forex HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhMMW1zVThjRkVRdlhQWWZELzNtVEE9PSIsInZhbHVlIjoiUkVLVGI1Rko3MHExdTlzNTJSNGhhSXRBME5LNUdVdXlMSFl0WW
s3bHlLWm5lVURRVWlpOGZOWnVycXJTU2pSOXhRejlFTUF1UGFPM3ZRMjUrYkllQVBxbGo5aXZVYm9tMzBhSG5pUHJaS0s3SjNCVVhtWVMwL3UvNmFOQ1Mx
c08iLCJtYWMiOiJkMDU4NmJlNjM0ZGVhYmM0ZmY1MDhjMGQ0NzBjYjI0NGM0MTczY2E2MDE5MDY5YmM3ZGFkMTAxODkzMGJjMzczIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://wnxqbpmzzmcs.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxwMWdxWmhvQlVHSGpieElnTWE5SGc9PSIsInZhbHVlIjoiS25NZHk5SU1NSFJpcHppemVlWnhCUDBoTThhU2lHZWoxZkhJRFI
1WGFxSFovOWt2L3IwcHQ4UlVIcjZPMFRGV0NCRTFINXNTMTlpTUIxWGFRWjEyWHJTT0kvMnluYmx4UHRlVzJRZkFoQkxNNVBMVFhwLzRsVHdXenN6Z1NKUk
liLCJtYWMiOiI4MWI1YzZmYTQ3YjVkYTY3Njk1OTZlNGVhZDJlYWFhOTdiOWE4ZWNjYWU0YmFjZjZhMmFjY2M1YzQwNWM2NDVkliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:06:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
```

```
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.28. https://adblbackend.peacenepal.com/admin/gallery

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/gallery**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://jhbmtqmwwfeg.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkVrbWk4UE8zMW1qS01CTHBHUFFwUHc9PSIsInZhbHVlIjoiM3Q1anIwK2YzV0ZNd3dtT2tSYXVEb0Y4WFQwclhnOVFOd2J6UXB
tY1E1ZUtJUWZRNGw5T2Iza3kvUzFCNGFSMzhtTnJsbnhlTEs2cHVnVDBTcFFDUkp1eklxQW1mY3hTdFMrM0ptbkFoYjNSeENUQkovSWxiMXF2NWxwK0p1WUUi
LCJtYWMiOiJiOTFhMzdkNTI1YmY5MGY0M2QwNTQwODI2ZGNiMGI0OTVjZWE0NDA1YzFhYzBkYjQwMjhmODExMTNlZGU1NWFhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://jhbmtqmwwfeg.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:06:36 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InBJWG1JMUZqeCsrQW9lRmVESWUvRVE9PSIsInZhbHVlIjoiS0dZQnY5RGRwcFZTSVF6aXgwZWN0Vkp2NHJuU1dpT1luSHpve
FhwNVFMV2ozTmFXWDNEYUorb0JFWlljMktIa1NKUU95d2pRVy9DNWNaNEc4TlJDMEs0cnA5OWsrcVJiWjdaTU1oMW02Tk5zSjlGOWE4eithU1RPVFJNb094dlEi
LCJtYWMiOiI0NjgxYWFkZjRjYTEwNzhmMmNmMWRmMzAyNmMxZDUzODNiY2JiNThkZTNjYWQ3MWJmYzVlYjU1OTIwYTVkMWMxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:06:36 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.29. https://adblbackend.peacenepal.com/admin/gallery-video

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/gallery-video**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://awpwqhncurou.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery-video HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImwzbU9FV2oxUnpwQ1kxY3JOUzdHVVE9PSIsInZhbHVlIjoiMnh3RW1naG5EaGhxMG9tQ2g0a3BDdVowL2Y4VHdvT25rMnlISWZ
JN093Z1NkL08xWnlHL2t5NDQ1YkRJaGU1WEtaZnR0cUhOOFJPdFhGeHNRa2tEM0NYNCtnM2tqbUJRaVNWY2tHQkNoZmxPbW81N0lmMFZoOEtmdy9vbjBHZH
ciLCJtYWMiOiJkMzZjZWI0NzFhNDMxZDhmMTk0ZjNlOTRhNzBiMzQwNDdiYTkyODc5NTZiOTY4MmYzODdkZWYyNjkzNWJjOGQxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery-video/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://awpwqhncurou.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:07:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImdRY0V0akE0WkFjNVpkRjljNjlOR1E9PSIsInZhbHVlIjoiNStMVFl1UkhzVWpMT3EvUGRPOWl0R1dmckdNUzFZOC9aYUNCeFJK
V1RnYTBONUYrZ056YjZEbG96UWxmVlBxV1NMOE1NUS9GeGtoajRkbUdPaUNwYm1rdlCK001RitJVG1oT09WQ0RkTU5ycjB1R1Q1MkZsbTFpSUFlakYxUU4iL
CJtYWMiOiIyN2Q1OGZkZDk5NWRkYzA5YzE5NjQ3MmMzYzIxMDBhNTljOTE0NDZkMjJjNWM3ZDdkNjg3M2RiOGNmOTI0YzQ1IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:07:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.30. https://adblbackend.peacenepal.com/admin/gallery-video/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/gallery-video/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://awtkztztjxnt.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery-video/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImJ3a2JOS0ZNT3paZm0xWVNKUVFZamc9PSIsInZhbHVlIjoicHVjT3EzOWdLeGZHZ0tmaUVCNU1IeHY1YXNYK1VUb3VEUjVoWlNYQTM0TGlpMmd5K2NTaW1pRE85YTlDc0Y0SmkwTVp6NGZJT2JIMm0zeVFHbjRLWUZmb0Zwazg5dnJUTmI5Q0lrT0o2SGJ0aHRrdTByTjRCNGNYVU00VHJRMTUiLCJtYWMiOiJiNzZhM2JmYmRiMTI0YzYwM2FmNzVkN2ZlMDJjNjlkM2I5YTMwMWU2NTEyMjBmYmQ4YmZhNWM2ZTQ1ZDY2ZDBlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery-video
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://awtkztztjxnt.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:08:23 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjFkRTNFeEMxaUVsZmwyOVBRLzRURnc9PSIsInZhbHVlIjoidEVUU0UxQWxwZjl4YXZjZXJKMDZmL2JGZHlWai9TSm42bndhWC8wZ1IlMDZHZzVvUHY0VVdlR1FGTjZreEhjd3RoQmxabjFxRU1CSjZWaDc1M25NcDVraXlJTVR0M1hKV2x2MWxtdXllUWxKbFlRcHVCMnNFY1FycGVpY1IrbVQiLCJtYWMiOiIwM2MwNzNiMGM5OTk1YTBkNDNjNzBjNWI0OGIwNDIyZDgzZTg3NjQ1MmQ1ZjQ2Zjg3N2JkODhiOWU3MTcxNTRlIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:08:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.31. https://adblbackend.peacenepal.com/admin/gallery/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/gallery/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://glpyvbnvnuqp.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/gallery/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InF4d3BjMVlrNTJGL24vR2poYXBCTkE9PSIsInZhbHVlIjoiZ0srZXhlY0VhQ1VTOFJFa3RQTVU2VDIzbjBPbm1zaS9HMk54akRGREJ6QkxnaUlqT2RGT3lZNXpZTXZsaGl3MmpWc3F4ZTZDSDBieGc4RUJoWUtkcGpOK210bGhkYkNONEh5ZG1NY21UdmVFUXVVMEE2b0k0ZGJSa1NXUldkNXAiLCJtYWMiOiJiY2JjMDc0ZWUyZDkwNzMwMDJkYzFhMjY5ZDcxNWVkYzNkMzRjOTlmZjcyZTI0NjJkMjdjNWVhMTlkY2U1YzUzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/gallery/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://glpyvbnvnuqp.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 05:08:03 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkJaZW1xZHUvT1FwaUxaci9mQWFnTEE9PSIsInZhbHVlIjoia0dOSFRQVVliSE5LK201ZzlsN05YRW1NS1JHY0NKT1ROcHVnS1dOalNuM3ZzenU0cDMxWTA1ZXcwdisvUHVqb3hSRGtYV0MvVG8xamRRRXplV1Z3Rm12MW5IOHF0cGZpT1NUQU1xdzJtc1h6Y1J1SHRwc0ZQalordWt1ZERRZGIiLCJtYWMiOiIyYzlmNGU3ZjVkMTBlOTVjN2I1ZTM4NTAyNDdhZTMxYTA1NTZkZjEyM2Q4OWU5MTQ5ZTFmYTUwNjdiODhhODRmIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 07:08:03 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.32. https://adblbackend.peacenepal.com/admin/import/atm

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/atm**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://guipvpllylmq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNvMTh5d1VyZndXOVE0OGdFZXQyV0E9PSIsInZhbHVlIjoieThnU2w5dHI4Smt1d2pvcW9RWHpJTXEwWkgvd0E0TUQyN3RxcEFoTmFVckR3WkZmOWo4STFXNnhYQXVVOGpSVEQraUJLbVh5UndEbDlkRHNFaDVGWmFqWTFwSCtCUCtRMVNNNTk4WEphTDRjQzVwazlETmxnWDJ3cmdXT0pZNHMiLCJtYWMiOiI3OWNhNzQ0NmVlMDhmZDUxMzgxNDg1NmI2ODRlODcyZTIyYjYzODE4MDNmMWMwMmU2NjU2MDgzOGViMWE2NTBjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/import/atm
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

```
Origin: https://guipvpllylmq.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:09:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InFtMVNMMFNPTWJRNTNoaitLQVA2R3c9PSIsInZhbHVlIjoiaFVNcVk2SFhReHZrcEx5NWtacVFwTjFwLy9kYVg0aW4vMFM4RFpzd3FsZVlXQUhBdVArc0FZMFRtOFhocmV5dVRXTmlnZDlqR2JNNlB6djZBaXV2cE41a2hEdTJzaWZTR2kwdjR3eThVRDVjWW4vV3kxYzE5R1NjT20xOXNFemkiLCJtYWMiOiI1ZjYxZGE1ZDNjYTMyNmMwZGU5ODIzZGYwZWJhMDhiYTUzZDQ5YzIyYWEwZWRkMmVkMzY1MTNhN2UxZGIzNWZlIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:09:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.33. https://adblbackend.peacenepal.com/admin/import/branch

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/branch**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://pfvmtswinobq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjZYOS9WNml0QUJXZ3FqL05JYStlU2c9PSIsInZhbHVlIjoiN0NzcDFnaFJ3d3MwdllpTDlZV09GQnRnYlF6YU5HZFhjcGtPSFNlOFBRWXdJbHZmOTAyRTFCYnRWUjVWZ3NITmdPN2VNaUM0MHNNNFBvSFI0eXJMU3ZpUjVTa1VNditsQW1CblFOTFc3T0JOSUtuQkYrMnVtc1B0bVRvdnF6dUMiLCJtYWMiOiIwMzM3OWI5Mjc3YWQ1ZDBhMTllZDViYjgzNzViNGZjMmJhOWYzYzBhMTQ0MDhlMGMxMWY4NjI1NjUzNDQ1YTlmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/import/branch
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://pfvmtswinobq.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:09:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
```

```
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkZnd3phK1BxeTVlek1SUmNhbEE5bFE9PSIsInZhbHVlIjoiQ1l0WS9keWVPbENEWExabmxMQWhlWVNmOU1GdE1Va0haZk5CWDRDK21UaUVUWnJjTmFxN0dYN1V4cFdVQmxETVFkcm1sd3dVZFFOUFR2YnljSUlxVUV1cjZpdVJvV1BvOU9jRjkrc3ZERXYvRDV3SUZSUDZsamtzNDNhaWkrbXEiLCJtYWMiOiI5OGQzN2VlOWY1NThiMGQyMTZlZTk3Y2FkZjA0ZDE3MDMzMGIzNTI2NWM0NjY5MzM0MGY5N2UwYzI2ZjU3NDJmIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:09:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.34. https://adblbackend.peacenepal.com/admin/import/store-atm

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://imawhyuagish.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://imawhyuagish.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:12:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033024

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
```

4.2.35. https://adblbackend.peacenepal.com/admin/import/store-branch

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/import/store-branch**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://kvewixfmbuvy.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://kvewixfmbuvy.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:13:30 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033046

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
```

4.2.36. https://adblbackend.peacenepal.com/admin/interest-rates

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/interest-rates**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://htgomghttbxn.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/interest-rates HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkpRdy80UGI0TjhMcnZVZlVlTmtnSEE9PSIsInZhbHVlIjoiQTRyQWxzVHpOK1dMTmlhNVNINmdpTFZIWGEvMHVSN2lmNGhWaEZ
SRExDK01uTW1GSFhmcGczMVBpaGR5VjQxdWlTNnJ2VXZqUDJZbXgwUHQydTRHRksyZ3dsNXZaTWNCTG1VbFA0eFU0WFRja05iVUZGZXg5eTZLeGRhdUJ
WNUIiLCJtYWMiOiJmNmQ0NjY1NmNjOWNkMGI2OWI2YmFkOTcxOGVhNGRiMzViNGU4MmVjNzZkNzliOTRlNGQ4YjhjNzBjNjExNThlIiwidGFnIjoiIn0%3D
```

```
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://htgomghttbxn.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:14:00 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IiswbTJBcGNtUVFPSmJtbW1JdlJzVWc9PSIsInZhbHVlIjoib1Yzb2hNNjY1WkxlYmVZTkZuQ1N4SGFsRDJuWWFSSWhrZmNId2VuMUJSc3NpanFpQWdkbnhKSWw4aThQdGJYN0NvUGZtYnQ5RWhrV1h5d2VkaGRtck82cFk0TmFOZUJ2NnZqODFDYzhxMWMvLzdOY2ZJUmdSZTN0NXJMYWp6SzliLCJtYWMiOiIzMjQ4M2I0NGQzNzQ4ZGE2MzZjZGRlZTgyMDczYTQyZWUwMmY0NTkwODk1ZmM4MjdhM2NlOGY2NjU3NGM4N2Y4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:14:00 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.37. https://adblbackend.peacenepal.com/admin/interest-rates/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/interest-rates/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://bhmbfknpauoq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/interest-rates/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkxQcnlzeWVpZXpJdTduUERNejNNMnc9PSIsInZhbHVlIjoiVUhxWFY5anBaMlNMMi80R2FGaFpFazNxUUpuait3ZTY0TzB0RnowbE5LbzRCRSt6ZWlUNXVFY0RKSVgyV1ZqYUVMQnFkSXJhajJ3T2lkdzlDdnRMaVlpMkV0N2tXQUUra1M5YW12K1FBM2d5ZXBOb3Y4bVhqUGJ1cUJQTzlFMDUiLCJtYWMiOiJiYmU2Y2M0YWRlNDVjNzRmN2JmMDE1ODdmMGJkNGZkMjA1ZjlmODFlZjUxMjIzOTZiYmYzMWE5Mzc2OGQ4ZDI4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/interest-rates
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://bhmbfknpauoq.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:15:37 GMT
```

```
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjdCNnVFcUVGeUV1ZWhBeVBDTk1HckE9PSIsInZhbHVlIjoiY3Z2Z1FCc0tacUY1YXE2NzByQ0ZwaFNUKzIwc1RZbjZBK0EyM0VOKzQ5TFhuSllySlV3UFdLU08yb1FKaTlnME03VlIrZzNiWG5WN1c1Uys2c0xIRjJrY1RKR2JoTXpWeWFZZEZNV2lLMjk2cUtDVlVZTTNqUWYybE5vYXhNRHgiLCJtYWMiOiI1ODcyMThiYmIzMWZmYmJmNDJkNTA0OTAyNmJmODE4ZmYwMTlmMWQ5ODQ1NmEwZDE3NzcyNGFlYThjMzdjNjc0IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:15:37 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.38. https://adblbackend.peacenepal.com/admin/layout

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/layout**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://pktgtpgeyitz.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/layout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFwQ01Kd3pHSE1EWUlYMXQvMXJjalE9PSIsInZhbHVlIjoiZlNBSDdVQXNIenZWSS9CRHl6OWRRVjZTeFk2UnFkMllmODIzajVrall6SXFNbUNvdFMxVzdaSUpyL2ZTQXB1bjNKNGczRVpvcWY3d1VTUG5lTWxyM2xHT1Y5WGJhSWd6L3VWZ0U3Ulk0cTVqTENiSitsTjdtd0JhMTBma3ppTWliLCJtYWMiOiJhMjU4ZGQyZGQwMjU1N2Y3ZWQ4Yjg2NjVhYjgwMTgwN2RlZGQwYmU5OGI0OTFlODU5OTIyOTllODYxMDUwZDdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://pktgtpgeyitz.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:15:31 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlljbzVmZ1NSakNQYTB0citYaU5sTUE9PSIsInZhbHVlIjoiZEcwSDFUOStkRDZQdUhIdTI2UjF5Z3VMVnZ6QU9paHBhRWNzb1FYb21McXh4elFLWFZQNndrdzBMa1NDYm1vd2lQUWlGN0xDWGR0aHNWWnpuL1dkVGhNZC9ZaXlXTmNtSjRqeFN5UkFmYXJ2ZG5XTldZM1RSMnhJdDR5VUF1blUiLCJtYWMiOiJkMDQzOGJiMmZlZDNiZmUwOWVkODVkMjQ5NGY4NTg3NzE5NjU0Y2QzZDA2OWM4N2RkYTAxNWYzOTQ2MmQ4NzkyliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:15:31 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
```

```
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.39. https://adblbackend.peacenepal.com/admin/log

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/log**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://tzjpfdlqisub.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/log HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFBL3hGSVhBSEM3d1ZUcHpLd2ZjYmc9PSIsInZhbHVlIjoiekFkZmlUdC9ZMG9RSXRWdHUyTGJQelFna2YrMkEveE9hQ2trNi9ia
nE3bk1iMFZ2cnQ1eC9MdEtHbTd5YlhaeXVRdmtUbGUyV29SU1NjNGFCMEZJWks1SkNUQ1lsWG84MlN4OWp1bTJ5aW9mWDVzQUkyY21vU2gyUVE5U2JPSFgi
LCJtYWMiOiI2YmE2MmJjYjNhNGY3MGM5ZGE4MTNkMWNmNjI0YjJkNDdkYzUzYmE4NTg2MzI4ZGE4NjNiMmZhMDA2YjZhZDVjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://tzjpfdlqisub.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:16:38 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjVCVGN6b2t1am1pYlY3eGlHeHdIU3c9PSIsInZhbHVlIjoiUGNHaWNXTHdMc1JiR1VwaXRnMDlGZ1p0TDE0VHpzN1VqdGk5YTQ5
V3dwOUY1TEJzd2RyU3UyOFdKNmNPU2Q5ZzNmNjNNK091a2xRc2hnaGh0WDJFeml0MVFrWEpFQzI1NGs2WDJVRk1nS210T29xMGHla2Vmam55Vi85elFhNX
EiLCJtYWMiOiIyMzJjNDVjYjE0MjI1OWVmMGFjZmU1OGY4MTIwMjIzZmY3YWRjZWJiYzkzZDgyZGJmOTM0ZTM1MGE3YjU3ZGQwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:16:39 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.40. https://adblbackend.peacenepal.com/admin/login

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/login**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://iveqnwonarua.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImE2ZWlzaDBsSVJpR05HN2U0VU5oSmc9PSIsInZhbHVlIjoia0lRSkVENm43UU56QVdMRzNDTFJDemZvNm9OQ1plczhKbUNaU
mNJV0hnM1FtTlhRaEw1ZThJbHhXNnJlb2l4ZzZVaUo2VlRkdWcyZ2IvcGlGbitGOGpyWFVGYU9GcXpnd3ExaG1ueVlRMGlTbVVmOVBRbTNGalhCalBha2RpQzAiL
CJtYWMiOiJlNjExOWUyNjQ3OTVlYmMwYTBmNWQ5NDU2YTBjODE3NzkzMTk0M2EzOTVlNjdjM2Q5ZjhhMWE1N2JhODg1MDMzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/dashboard
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://iveqnwonarua.com
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2024 04:16:24 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Set-Cookie:
adbl_backend_session=eyJpdiI6InF3T0VQRFY0cTNKcEYveXBzYzBBT1E9PSIsInZhbHVlIjoiTW5weTYvMW5ZNkxDMUNkYmxwNGJFT3RNMjRNb1RJYnZqZHQr
Q0MzaStzMlM2ZUU1bEZGZ1RXOTJXVHlqaUJwNDNhT1RZcHJpa2lUTFhNeFoyTWxWV1Q3STdoVG9uSUNNU1VFQWJlZVZmUkw2S2xNN0pucjVlWnpnTnlDZD
EwcXkiLCJtYWMiOiJmMzBlMjllMWYzYzJhZWE2NzE2M2YyNjFkMDE3YzQ2YjU4NWM1OGE4Nzg1ZjIwMjc3YWJlOWZjNDlkZjczZWUwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:16:24 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 7097

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.2.41. https://adblbackend.peacenepal.com/admin/logout

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/logout**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://hieawgbvalue.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/logout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InpsUTZzNFpISXJRVXZBS01wbitUWmc9PSIsInZhbHVlIjoiajNUMm9NSGQ4cDBod3JzZ0hWbUxPTjJPWGJiSVdScnd5czZKejQxS
FNsNzFlb1F5T0dqYlhycU1IUlNQWm5LRld2MjArZndsRDNKU3FYS2htVWdWZGJTdy9hcVFCQnRRU2NLMTN3VnJZanFqY2FYMXp5cVM4VWVTc1c4WkVtaXIiLC
JtYWMiOiIzNDBiMGI5YTM5NDc4NDg4OGM0YTQyZDE5ZTRkZWQwMzE4MmY4OWFhYjk1NGQ1NWY1NmUyZWQwNWFjY2I1MmFiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/dashboard
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://hieawgbvalue.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:17:42 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkhXMXdJZEIjRlg1cGlmSm9mMDB5Y1E9PSIsInZhbHVlIjoiRlNCT0o0V0Jzd1YrWDlUWlFQK1N6bU5EWlFJdEI3WjBFZENzUXBlZ
DhnbnFqa1VSNWdWNVVIS0wyVTZKSExxNE5pVERqQi9lcXlxMG9UMUhiMnFlRzdEd2FxWXFacXNBYm9saFBacnJYVFFyM3ZRMlRXUzlPR0pCUGFBY3RRQ3Ei
LCJtYWMiOiI3NTMzNzZjMzE5ZjEwMDUxNGRkZjRiMjE4MzViOTFjMTA1MzA0ZTYxYjI2N2E3NGY2NTQwNjk0OTFjYjljMmJhIiwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:17:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.42. https://adblbackend.peacenepal.com/admin/menu

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/menu**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ctyprhrqtrzy.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/menu HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNpbkxIbTRQUzZxMHgwVTVkc0hzdWc9PSIsInZhbHVlIjoiUGZKdEpGUFQxUy9iWUhLRU9NVTR2cjhWUUlDYWNNZ0UrS1NDO
WFURzIvSDFmdjA0elc5RVRpaWZIekJFZ2pvNDA4cUYxa3g3UW03b3BjTlNDWUdLYUsrNXpRQVlrbGFZMFQ3TnVTTkl5cEJIcmorcnZpWVhHN3dBb0NoQ2FqSk0i
LCJtYWMiOiI4MzgyMzAzYzQ0MDhiMzZkMWFiYmQxMzUxMDA4Y2NlNWU4Nzk5ZjcxODYzZmFkMTY2Njc1Y2UxMDljZWU3Nzg5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ctyprhrqtrzy.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:18:12 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjRNNCtQdTY5anlIZ1BzcTYreC9zdXc9PSIsInZhbHVlIjoiT2hTMEUwOUFlYUFkRTVzN3pYSUhkL1lVSG9UZmVCNlBPWUJCOHlZ
QXA1dy9jVnFSdTJHaUNOQkRjVXc0T2I0RUZNellLbDd4K3R3dGV5OFFXVVJyUndFSlpWeTliUUpkTldJU29EKzZlUi9Bc2pOMG83aWVOQjdaOGFDWDVYWDAiL
CJtYWMiOiI2NDAwMWYzYjI1Mzg3NWU1YWEyZmU3MzE1ZmJlZTNhYjhlYTI4ZThjNDBjYjQ1ZDNhNTgyNDA5YTY2NzNhY2MyIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:18:12 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.43. https://adblbackend.peacenepal.com/admin/menu/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/menu/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://osmqvhlxslxk.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/menu/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImxPaXZzYUFUZHFWNkpRVTZSZlo3aEE9PSIsInZhbHVlIjoiMjFSajdyem5QdVJ0WGVQR3owVWxiN1BsMjMxbHlSNXZEa2hnVlV
4TDNrMGtWOFZrNnNCK0xHUW16bUQxcGtJWGJzcm5aVU9VbFgvbkIyY1dXbjhLUDZXaW55SXdEOTR2N0hHMkdKWW5URWJmSUV3dzdYVXJPTWV4dDBnOD
```

```
dRZDgiLCJtYWMiOiIwY2NmZDY4NDllMGExMGIzYTU1OWQ2NGYyODgyZTYwN2FiNjcwMzNlN2FkNjNhNDlmNjdlNmZlMWJhMzgxMTdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/menu
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://osmqvhlxslxk.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:15 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImE2SHJPQWROdldjTDhDdnh5Q3RYTUE9PSIsInZhbHVlIjoiSUxLOUFiN3haZzRYT2FNU1Q2c1d2SzN4SmFKNEJxVzE3SWp1Y2
F6clQxcDNPVjVNdlRWTEozQ0NUbFEvUFNCSEMrQ0U0REpQSG1UbDdvbmFFckVZbmRGdmlNRW1LcUtoRjVJNS9HeUlaTUx1WndjdlMdElxWlFnMkdwRUt4VFIi
LCJtYWMiOiIzZGE2MjA2NjFhMWE4ODEyMTY5Y2I1YTgxMmFmOTUzZGZjMDdlYWE5ZmMzNzU1ZTZlOGViNmQ3MmEwMjMxMzc4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:19:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.44. https://adblbackend.peacenepal.com/admin/module

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/module**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wseurmuhozdu.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/module HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkRBcGNmRElDTGF2QTZOMDFVZnY3OXc9PSIsInZhbHVlIjoiR0NRWUZ5eXIzZWdTMUpHSm9sK29mMFZrL3FWMkRDaGhHM0
V0eEkxeGE0T3hENVg1VnV1eHAycWVxTFJJRGV0b3o0cVQ2anAvVUMvOFhNclJtZFVEWVJSclRlZEljNTVqd0tsWE9YZ1gwZTArOURQaEVWMzEzWkdGY2IxV0d
JYWMiLCJtYWMiOiIxYzEzOGI3YjVlZDBhZTAxYWFkNzk3Y2FmNmZkZjk5YzAzOWQ5ZmFmNDk0MjY0MmYxMzhlZDIxNjYwMTgzMzBiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://wseurmuhozdu.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:18:48 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjdDb2djNXlOSHdibkV3empJWTAxUHc9PSIsInZhbHVlIjoiLzBXWFNnc0pMbGNqSStRU053RVVBWjNwYWRISGp3bStNOUpnZmtmaEJ4V2t5bTdITi83WlhzZlFRSXB3OUJrOXhTY3phTXVoZXR4cHZiSEF4S1ZsMll5dkkzWWU2U0sySVE3NmQ2YWU1TUVPUkpXSlJ2MVQzWTRQdlNFemtHRzAiLCJtYWMiOiJmNWJiNWY4MmRjZjRjOGJlN2QzZWYwZjVmNzQyMGNhNTJhY2E5OWRmNzU5ZDdiZDE0N2VlZTg0ODQ1NGM1YmMxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:18:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.45. https://adblbackend.peacenepal.com/admin/module/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/module/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://qovccgewwpwu.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/module/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InlrK1dlbWUySUk2VDdaUC9vekhVRlE9PSIsInZhbHVlIjoiK2RKdC9EWlhmZVl1K3BKRjdhN2M5czljNHZtZkpLVkYvU0lLVTRuU2NPZE1kWHlnUTR1NGJ4Q01sRjF0bFdhYUtVMnY2emtzZlJrQ09rcVJRYVJQM28vTkpFY3dFTDNMR2ZsRkNaMEZ1RUhITSszVHZ4ekM3NGZVNktxeE9taXQiLCJtYWMiOiI5YjhmMmY1ZDU2NWUzYjE5YjZjNWQzYmFmZmMwYjllNWFmMWM3YjdlOThiN2M4OGU1NDI0MGNjMDkwMDEzODliIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/module
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://qovccgewwpwu.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:46 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlFFQ01XTkZYOHRRVnpEcExUUHFMVHc9PSIsInZhbHVlIjoiUC9TVXQzV2o5RnJIMzRrR0xPeFlIM3ZGVG90aHhpZWdTY2d3cjBaRDBWSmpidEpJczdNcVJMcHp4blNMZVkvdVIwaXk5Yk85RDFZMHFLbHZzdktjNjVtQ1haSVFHeVlPMEdicUVReVZzZDkvTDkwOUl5RjdmdlJKNmJvdVZ6a28iLCJtYWMiOiI4M2MyMWJhNThiN2YxY2MxYTVkM2YzYmNhMmE2OTQ2Njg0MDM0NzI5YzQ3NDg2ZmI2NTZkNjZhYWIwOGMyYTFjIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:19:46 GMT; Max-Age=7200; path=/; httponly; samesite=lax
```

```
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.46. https://adblbackend.peacenepal.com/admin/news

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/news**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gfzvpunwuosa.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/news HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkxESis0SFlVcTlFT2htSlVaUms5MVE9PSIsInZhbHVlIjoiOVNBUFlIK09uTmpRZnNsMVFGSVZhZGcxeWp0enAvdG9xZ0FjL0FWW
m93QnhXVDNsQ2RQemlDWlhMN0l1MkRxckpSdmlYNHppZDFPSzJzSnVVS0o2UVBpZFZtSU1QbDZ1cTF1LzFTRDJNMzFmMmE3Mi9vZ0lkNzVIMktqSm40QWEi
LCJtYWMiOiIxNjM5MGY5ODk1MGI3N2E1Njc0ZDYzODIxNjgxZDMzMTg3YmNmNTA2OTVmM2NiNzgwYjUxMWUyMjY4Nzc4ODhhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://gfzvpunwuosa.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:19:26 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlIrODNRbEIzS3BPUDFwNlJQM3lka3c9PSIsInZhbHVlIjoiaERlbWdHZTV3cDhFc2gzakFtd3hSTUQ4a2VaZStTQnVGT0ZjQ0FMWkg
zbnR3Q2RIT3dxVFg4UjAybW83UlA1b0Vjd0tqK1BoazliWmJhZnNyZjFEV2RlNXc2OEhLVk9BbmdJekl3eE1ORFVxT0dOdy9PbVdyakNEa0o5d2NsTzliLCJtYWMiOiI
1Y2RlMjU2YmNlZDU0ODY5ODY1MTk2MzU3ZmMwMjg2MGQxYzcwY2FlMjRhNDk4ZGVlOWZhYzhmMmJmMjg4YzczIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct
2024 06:19:26 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.47. https://adblbackend.peacenepal.com/admin/news/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/news/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://hkrigxmdytqx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/news/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhlMHZQWThLOFZYdnZQS2h5Z3NvL2c9PSIsInZhbHVlIjoielhsNW0vMC9SSFByYTdSZExGeTV1Q3I0ejI1blVKSmRJMVhPR2FS
TU5CNThzSFNNdVkvN3pDRENibjNJZVA0Rzh3b0x6R0d3ZU9yeVVTSUVXWnlEOWR2ZElWSERPY2EwY28vT0tlL1J2UmdrWnVKQ0dPOFo1Y01GQlRoelhROXIiL
CJtYWMiOiI1MWIxN2UzYzk5MWMwYTI0Mjk0Mjc4ZWNmNzU5ZGMzYjU1MTI3ODg2ZGJlYzUzMmMzZTY2YjU5NTE4ZjdjYmFhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/news/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://hkrigxmdytqx.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:20:45 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InNEV3ZvS0F3cTJLTmQ2TUpwUTBMT1E9PSIsInZhbHVlIjoiK1F0NS9PNmNMeFl0UmtVU0V4M05NQ1NXS2ZLbUs4cDNwZXZQ
UlRZQ01rejhrYXVUelFBb3d6SUN6QjlSFlCYWN1dHVUTkZ1dUlFdW1lN0JyOE5nYkdqek4wSEpWM1pyTUFlSGFTb2owRmZmaitpVDMwcUhJUGVnR2FxTWcvQk
0iLCJtYWMiOiJlNDk0YmUzZGNmZTdiNDgxYmIwYWUwZDI0NDE1NmJmZjUzYjBjYTg0NGNjZWQ3YWUwM2IwZDFhOGRlMmIwODgyIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:20:45 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.48. https://adblbackend.peacenepal.com/admin/offers

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/offers**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://uqkcpfvhbnsl.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/offers HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IldWME1VYWY0MWJRMnFJcGlZYnRoR1E9PSIsInZhbHVlIjoiaStsZ2Nud05pN3B6SENrdXRzV2M2OWFlLzhNWG01VCttZHlJMlV4U25FY3JpRzI5dC9ZcGQxZmFlVjlDeXVKemsweEVkTWxQaDFtUlJWakRiN1R6MEk4Uzg2bzBNeTFld2V2akJJZnlJWTYwdFdBVmQzQTNvSjd3dFBla0JnZHciLCJtYWMiOiJkZDEwOTc4YjBiMWEzYWZmZDMxMGI1MjdjMzk0YzRkZjA2NWNiMzNjNjdlNzNjNzViNzI3MWM4YmE0ZGVjZjA4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://uqkcpfvhbnsl.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:20:35 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InVXcnNZMHhkbzRDUEptV3U4RzRqdXc9PSIsInZhbHVlIjoiSGk4NjRYYURKWGVSV1lGVmo2S05BTGtNWHJ4Z3Bscm1FKzJ5clZOeVA3MmV4QkRSYmhWTDhveng4R2lyMnQzOFhzR08wVTRNc2l3T1htclVZL2NqOU84QjdxYUxJc1MweVExYVgrY0dXRTFvOFZ3QWFrWU1kSEFYRVZKTWh5SG4iLCJtYWMiOiIxMmE2NTE2YzZmMDFmOWVlOTJlYzA2YzUyM2U1OGUxZDVmODFjY2YzYzlhY2I3MDRlYzU2NWI0MjRiYWIxZTIlIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:20:35 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.49. https://adblbackend.peacenepal.com/admin/offers/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/offers/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wpswlvenurjf.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/offers/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVrdmhzcnFzSTRkQ1cvVksyTjNMY0E9PSIsInZhbHVlIjoiUjcwOVJqZytna0VYSmphQTE3NlFLN25xZlAxaWRUTzdkMHNuRjRpRk
VqMlFTTWRZY1IVVURUTTBqOVQ4UEhnYWpBRnhsTlRXbUFtb09RRDJucXVNdVk3MG9oSHQrS0E4cVE1bDdRRzZMZWw3eCsyb0ZvcU0yTEN5T0lBM0dPMnki
LCJtYWMiOiJmOTczNTY3MTBjMDE1ZjRiNGI1MjBjODE3Yjc3Mjg3ZDI0MDU1OTNkZmY2NjhkMzRkNmFiZDQ2ZmVjODE4MGJkIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/offers/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://wpswlvenurjf.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:23 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImhWcWUxZ2FzUXlLZXhVUmtQSDh1YUE9PSIsInZhbHVlIjoiV1BMSTVabGJmajFjeEYwUEtNRkxPckhpbWZLZWp4Vm5ybm5SZ0
9lcFVUcTQ3YWtiSlQvOExrVzM3bUVxTklsbEdkZFdPZXFZK3VTMVIrb2dKKzQzSDIlbXBmSXpIWU50RUxzMzVRcXVHeVVLTHlKcE1kZmY4MS92ODM0MHZLcGoi
LCJtYWMiOiIyZWE5MWJjNWQyZGM0OGI4ZGQ1OGViMjY3YzcwOTFkZGYxNDlkMjg0NGJkYmUwMzc0OWYzY2ZkMjhjMmJmYWFhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:21:23 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.50. https://adblbackend.peacenepal.com/admin/popup

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/popup**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://njbqfxybtxrx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/popup HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImtSc0xzUFEzLzRzVW9xMTcvOWFMNGc9PSIsInZhbHVlIjoiS3NzNjZzSm9mUUk0Q0VvZEYvQk04N3UyTzRyMWFGQmJjMENMd
k9uZ3dEQkcxY2dvNVB6MEVtY3pIRzBoY3ZiOWdSaUUwMktxRzBKV1Y0cDFOQ3NrUHROMFVXSitCQVdxeVAzMmNsLzhobHdPbkVPQTlTaENpZUhnVnkvQzFXb
SsiLCJtYWMiOiI3OTcyNDA1NmE3MGYzZTlhMjQyOWRlZGNkYjQ1YWZlYzQyODQ0NGIzYmUzNmU2ZDUxOGUzYjkzNzFhZml1MDkyliwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
```

```
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://njbqfxybtxrx.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ik95NjB2QStKSEY1RWNDcjZnOWtCemc9PSIsInZhbHVlIjoiL1A4YlRZQlpVT3RkQXgydisvQ2tURGQwYndra01tZWlYSEg2bzVxRXN4YkQrR3FuaU1JZHlrd2l4ai96ZTRMczh3Mlk2V2VkbE9VbXhTekFJY0pwMnYrWVNaT2djMmNGMDgxVkdBbFhDb0lJaDF0SFVnZlNiRUtjUFZFM0dYOEliLCJtYWMiOiJmODNjMTk4MWQwODNmMzY1OTJkZWY0MDZiNzRjYWE3MTZmZDk0M2Y0MTczMDliMTg1MjhjMDU0NTQ0M2YxNWVlIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:21:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.51. https://adblbackend.peacenepal.com/admin/popup/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/popup/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://nmezbndzoexz.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/popup/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjlzS0FXUG8ydmJQdVhWOEFDT2lMN3c9PSIsInZhbHVlIjoiMktiYkJzV2EyNS9aTVFvS1p2MzUrNlpOa0tNZUJhV3BBZUFTYUI4SjFpYkl6T0ozM1U5TjVQU3RGcGMxZHlTS1hJaklsazdUMHd3OG45SDZTSWtlSGg0VjM1ZWJXNldNTkhkMWI1d0M3QmZEN2Z3dmtNbm8xRFF4UU82eG9QSmsiLCJtYWMiOiI4Zjc2MDhjM2Q1M2U3OTI5YjJlMmZhYzEwMmY2YzZhMDU1OGZiNjFlZWQ3NzkzMDk0NjlzMzc4NmVlOWQzYmM5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/popup/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://nmezbndzoexz.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:55 GMT
Server: Apache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjYzY1BiUGlDQzFwSGVWdG14UFJFTVE9PSIsInZhbHVlIjoiRjIxQUttNnVqU253WGozQzQvdGxuWVNFRitYUmVVWUtldmwwbDh5VTE0MjZUYWV4Z2JmSW5pcGdQdS9sV0dVb0FZV1NCWXR4eWhYVDB5VEJvSmlETU9VMSswdFZUR3l2UXFuQy9iaHU4SXNWVDI3SEd1cm1Wd3hpK2d2am93KzMiLCJtYWMiOiI1YTViMjIyYjg5MDMwMjJjMjliMTY5Mzc5MjBhOTA4MWNiNzZiNGRjNTE4ZTQyOTVmZGI3NjkyZTYwZDQwMzk0IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:22:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.52. https://adblbackend.peacenepal.com/admin/press-release

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/press-release**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ddxxzsaitclc.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/press-release HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InJaWmQvNWtiU2pDSkRwbmJOUnJ3bWc9PSIsInZhbHVlIjoiTDZ4djRJelUzNjlGcG9xc2NGR25JYmE5OWUvbHZqNWwwdmdsdW1raVo5cldKeVppaGE3OUlFTkVpN1UwS2VSZXJ0SldlQmVZZ1dRSFh1aEEyWWlUWWJQYzRMbXlya2ZuZjdSSTZyZVQ2N0JEMVZNYjFXVnBsTFBHWGlLY3lTUUgiLCJtYWMiOiI4NTIyNzI5NmYzZmExNTE1MzFlMzg2OWY1MTk3MmMzZTIyMjM1Y2U3ZDdjMDcwMDc5ZjU2YjE4YTBlYThmMzUzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ddxxzsaitclc.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:21:58 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImxBNlgxeHRNQ0t2cFRoU0FIOWNPZmc9PSIsInZhbHVlIjoib1dteUt3WHV2dTFHOTNhT0N5ajhUamgvU3d2Zml5eDg4SVpIY2cxckF5cVRPaEllUTBIdUhubERRU3paQ0FPTVd5MGdmYmNBMW5MZUkydU1YYkRCSktlRXB6dFpQeElYaFNUamh5YTRwUmg4NGVSN2JYcXZpc3NFVmJWV2tQZmkiLCJtYWMiOiI3YjYyODEyYjZhMDBhMzk2N2NmM2YwMmViYzY1ZmE1Mjg4ZjA3NzhhZTMzOTZiMTk5MDRlNzM1ZTFjZTIyNDUwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:21:58 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.53. https://adblbackend.peacenepal.com/admin/press-release/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/press-release/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gyqrmcimpzpo.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/press-release/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImdwRkhaeXVxT05uRGRjeHZ3cDVqNWc9PSIsInZhbHVlIjoib09sVFdseWR2WnEwT1Bxb0R1L2RsWnVPQnl1M0dSMkl3UVY0ZT
VaaFFNRmJGalVzSzJYNFJRTFlYQno5KzZOOVpzYmV3cS9VeUlyZEh3anFpeEdpdFBPb2JYamFZb3hhVzB1NnV2RFJzQzBkWWxEeDF2NmtyR0s4SUZrYW9INlci
LCJtYWMiOiJiYTMwNzZkNWFlYzNmYTNiYjRhMmFhNzMxOTBmOTZmOTdlOTNlOGMyMWYyOGNlYTgwZjY0Zjk3OTFkNmRiYWMxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/press-release/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://gyqrmcimpzpo.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:00 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Im9adlZCby9UWk15eGVmQlNadzNPVGc9PSIsInZhbHVlIjoicFlEM1AzUjZDUS9qcEdoM29IMHhzTFZSamh1YmJGbmNtQWluY3pr
bCtRK1pGZ0hZbEg5Z001bXEvNEVnbWJHY1Z5Q0wwSVJGUlhkYmxQZEN6V3oxRTBYT3Uzd1RqVURmeWRaQW9mbTgvOXNHeUtqVERhanZvRCttVFAyYllvRS
siLCJtYWMiOiJiOTAwYzQyNGY3MmU2NzI5MjRiZDIxOGY1NzEwOGU5NTMwYjBkOGJiZjFlNjJmNmE5ZTMzZGVkZTQ0ZmJjMGI3IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:00 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.54. https://adblbackend.peacenepal.com/admin/projects

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/projects**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://pwlviogioxde.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/projects HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImhhTTBpT2RPTGVYRVVOZXJ4Ym9lbkE9PSIsInZhbHVlIjoiL3hnL0NaQlcwaS9BbkovSDV5Qk1HeDNtVGN4VGo0L05xZ1d5ZHFpTi9ZcEFUUWxNakIwYWdBV0dDQ1NGNGVFeXcveElnMisreDdxSVNxVjJTeFhmelBaeStJbTRWRkZPUzZCZVZxZFRhVDNLa3Z4M3c0bDhmSk1OQkxMeHIyY24iLCJtYWMiOiJkYzQzNmFkNGUyZWIxZjAwMjE4Y2ZmODI3ZGYxMjY4NmMzMWJiOTg0MGUyZmYyNWIwZWM2ZDIxYzViZWUzMzNjliwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://pwlviogioxde.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:32 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlFqRUI3VVo4OFEyWnJMRVBOMVZxZkE9PSIsInZhbHVlIjoiSTZwUW1mck9BLzRhUHkyNjNEbE9HNDJ2K2hvMG1NSUJYQlhrYVVyUWtEakdZdVdIZkFaekxtS2orZEpRTzBXWlV4UEVhbHpaYUhTbytYcy9GOEJ3VUxRaW5mYnNHZ3VDSmI1UERHSS9sMWZxdzNSejFST1pLTzVnbjc0R3RrMUQiLCJtYWMiOiJjNTkzZjZhOGQ0NGVjYTQ0MThkNTZlNjA0NjBkMGQ2MGYzNmRjMDhmMGU5ZTU3ZWRhNTYxZDNjNzY1NDVmMTI2IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:22:32 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.55. https://adblbackend.peacenepal.com/admin/projects/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/projects/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://dwpvhsrnaiha.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/projects/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjY4NmxCWGRrUmV0Sjk4NHJsdnlicUE9PSIsInZhbHVlIjoiaUJqNE9LbTl0aFhMaGROem1yWnp6ZThCZXhiVnpwWVplaEE1NmNCejMwcjY0SGllRGhSVzVtRllFbENUVkhYc0lMUjhOd0EySDBFZzJPSWQvVVJUTFEzZDVvUnV1TWFtM3BKWlUxeHhKQ3JsQ2ZVNWd1VEJFUjBSM0M0MkdMaTciLCJtYWMiOiIxZDNlMWJiZGQ3YWE4MzQzY2RhZTNhNmM1YjYzMWY1MjQ4ZjQ4YTM1ZTVlNzYwMjNhNjM3ZmY4ZTFmOWE5Yzc5IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/projects/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://dwpvhsrnaiha.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:20 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InIzZjMrMWFGeGpzNDllUW5jVUl6OWc9PSIsInZhbHVlIjoiQmJRc3ZxazhkOUhtUHJLT0Z5WlJDSVVFY1hwNGk4TDVqWkM2R2NNaDBWVWpzeEZOZzA2RmdQWUZhK1k4TXU0Nkt0QTMwMTBsTFgrRGl3bmUwUGhQbWlkbFVodkxqWTZKK0xzV3ZqNFNOTCtmbWs2N0pCMDh5Ylg4Z2x2eWdvajEiLCJtYWMiOiI4YmJhNDA2ZDZmMDIxMDBlZDg0YjBhOWZlYzJlYzU3MzRjMzUyNTk0NGEzYWQ5N2ViYjFmNmUyZWQxODFiMzMwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.56. https://adblbackend.peacenepal.com/admin/report

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://xwjubppmydrt.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report HTTP/1.1
Host: adblbackend.peacenepal.com
```

```
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlRjMVQrNUJvWnRTTDkyTnAyQWZhVWc9PSIsInZhbHVlIjoiL0xiUGkxVFYxVXJZY3Y4eGlZbndGWGdOUzd2M3JSYndBWlZejVse
GVIdnhBL2VFdlR1Ny93L3ZBdWVGTUJmNHI5b2dDTjNJbDI5RTUvSmlCbXFyTUxlVWd5V2hJSmNVT1V2bHU3Ull5Wmt0cUp1TzNIcDNidHJYOVRZSjFNK00iLCJt
YWMiOiJiMzBmOTFlZTI0MjBiNWQ3NWU2Y2YzNTI1NjY3ZThlZTZjYzk4MjViZWE0MjM3MzVkNmVlZmFkZTI1OGEzNTk4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://xwjubppmydrt.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:09 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImdVUEdQTmJQcjQzR3cyVlVFc2RwZUE9PSIsInZhbHVlIjoibTJhckZrM2o5TGlVcGp5a0txSFVEQXVPUkJjc2F1V20vTTlTcTFVb3R
oSU1zNVlmQVpjS1JlVDhMeC9vK0k5V2g1bjh6Y0dUUnJ5bHZJTlArVm9wWHZUcGoxVjM4aG9ZMzdlVEtQUEozRlhkOUhHOVdaaEw1Y3NTbUZXVm04VnciLCJtY
WMiOiIwZjhjNDZiMTA0MTM2NTlmODBjODYzNWE2ZjA5MTViNGZlMmQxMWU5MDdiMzFjNTJlMzQwNzNmZWIyY2UwYTg5liwidGFnIjoiIn0%3D; expires=Thu, 03
Oct 2024 06:23:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.57. https://adblbackend.peacenepal.com/admin/report-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://qzvpmitysekh.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9zWEZKNlgyNVJRUVI3ZWdyc3ZyblE9PSIsInZhbHVlIjoiUjBjUG9YSS9iVmpYN2sza1BBOEpVd1ZlelBpcXJZWkZUU0JtTStwMW
d1WlU1VEo2NjNJNHdSNnVLalpLaEtlTzR1bmF4VTRCY3FvZjNwbTBjb2tVZnlhU1VteTYzYTRqZVVLSmliK2tlZXl3RWFuWkVqWk03d2dUTnVhc2NRQ00iLCJtYWM
iOiI4OGE1MGM1ZWZhYTBjODBjMWQ0ZGM0Mzg0YzVjMWM1YzIxMzU1ZDBhMmUyMDk2ZjYwNDk1NTNlMjcwZmY1N2VlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
Origin: https://qzvpmitysekh.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:24:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ii9YalBTaUNYUWx6OENPQjJNbUFCeEE9PSIsInZhbHVlIjoiV3phakJYWDF6SHRXSlkvcElQWlltSVpmQlhGRm1YTEEyZUZaZk12V2tnbzVzOGxRVitrWWtiWWg4bXVrcmo5RFdpblZ3UlRNQlZ3UjdCRFlvbmlBTnA3VmNqY0pvWXZEc0hjdCtqdW9IOUJPUmxlRFVOeEYwem01V05CeHRtUWYiLCJtYWMiOiI0Mzg2ZTA4MGZlMWE5YzQzZGVjNmMyMDJiMzhkOWRkYjMxOWZiOTE2NzI2M2UzZWIyZDljZGZiNWRhYTM5YjJmIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:24:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.58. https://adblbackend.peacenepal.com/admin/report-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://csngatfvhfgs.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IllzRjBRQ2JrTTJqNG9BZHhIRG13TGc9PSIsInZhbHVlIjoiR0ZZQ2hZUlRsejVPMWZxRTMvUm5RRGNRRVJJdzFWK0JsdGFyL3RvLzJjdjVlZWs2eWd4SEF5MUlWQzdNNFRSa3hIbWx5aEZSUTAzMWJMaG1jdFVHZDRkRFpVSjMxNENGT0hmQ2hOYlcvVVFLTkVNZmpCL2dtTTFvbkdoS1VsUDUiLCJtYWMiOiI3ZTgzNzEzYTU1OGNhMDU1MTg2MzRjOWU5MmIxZjYzNDM5NDU3MzM4MGI4NzFlMmRiMjE1NTdiMDkxNzYzZDBmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://csngatfvhfgs.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:25:08 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
```

```
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkdoSVlyL0hXZlU5K2FKUVJoWlB6TEE9PSIsInZhbHVlIjoicmtjSzN0SlNkekVxV2o1NW5VQmpReXJ2bkxEVjNVMHVmOERvQzBU
QkpaVEFKbjhmbklsR1NiaVRJVVh5d0dZbjJEdGQySnRQY01pTGl1VC9Wb3ZRQlFzYW4zQUY4Q3JraStWcWI1MmZWTmlwK3duSndsYllpc2g1UWVReEZqQ2ciLC
JtYWMiOiJhMzhmMTc2NGI4YTNhYjdjYTkxMDEzZWZjMmU2ODg2ZjhhNWRiZWVmNDE2MGRmNmYzZWViYWRmZmZlZTJmZjcwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:25:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.59. https://adblbackend.peacenepal.com/admin/report/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/report/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://kgkrsomxqets.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/report/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlRGdEdJVXhYV3dqbHJqOVRLblNObWc9PSIsInZhbHVlIjoiVURvNTBLT0FNb2IwdVRydk1aUFVyK21yTW5PRXRMcmRCM21qb3d
jVGlZNDc3K3l0YVVNUW1SMW1KV01QZm9DdWNwWVRuZWNjQzNjQ0FMcVZ5Z3ZXNzBzZjBva05NdUxmcElkYUlaWVlzMFBKeVVUbFBKSTMvMnhNL1NiNTU4
bDYiLCJtYWMiOiJlMmI4OTFiYmVjYjg1OTI5ZjAwNDVjZWNmOWE0OTdhODMzZWMyNWQwODhlOTg0MjE5MTlmMjk3NmM0NDJhNjNmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/report
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://kgkrsomxqets.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:24:16 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ikx5d0lFTUFnVW0rRHZEWWpuZHN4c0E9PSIsInZhbHVlIjoiS21tTG1ITGQzdXpsbXpmMWI1RitTdTRjRU9PaVRwRjNiYXpsbTVUR
FNjaHE0TDliRE5Zcmd2RjZleDdQOEZ1N1pjdHBIS2wvNG9ZQUlGdHdReVNtZHlNZjc4UjB1RTRpVUlmS1RQRE0zZmY1Y1RWSHBIY2F5dHZESWoweVRWZGwiL
CJtYWMiOiIzZWM3NDEyN2ZlMzQzYzZlOWFlZjE5YjNiOWVkNTgwNTY5ZTQ5ZGYyYzJmMGEyNzk2YTlmOGVlZmE0NWUzYTI5IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:24:16 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
```

```
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.60. https://adblbackend.peacenepal.com/admin/reset_password

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://zqbuvbjeswsx.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: https://zqbuvbjeswsx.com
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:28:37 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033004

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

4.2.61. https://adblbackend.peacenepal.com/admin/seos

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/seos**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://zqbgmpoojnhv.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/seos HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik5OR2JmL3BmdGYzcG9hM0MwbklkZGc9PSIsInZhbHVlIjoiR1AwNWJReVhlOHIraTRCVEMvUGFQWDFNSDZYQUhsUmx4eGw3bzAxc1FtUUNkaXhXYWpmMS95RVlyTzIwRzhCMDh2eHVlZ3l3dGpvYU15d01LaDEyVENLdDZCTUtKQ1VHd2V2eU9ncUxFa1JibTZsRjRBWCtwbUVHZTF5ZTliRkYiLCJtYWMiOiI4ZDNjNjRhNjMzM2RkOTg0MTBmNDRjYWViNmQ2OWMxY2YyNjcyMTVhZjIyOTgzOWFhZDAyMjk0Y2Y3OTkwYzIyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://zqbgmpoojnhv.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:45:37 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxZYXVtTEluQmQ1cCt6TFAzRzNZd3c9PSIsInZhbHVlIjoibHRXaXRTdzlBbWMrSXpEMEl5bWJ5M2hxWjlUTGNrd3R4MDE2TldWZmFTYUtlZVRkQUZJL3B1aGlKNmxtV1JiSXJhS2JBdml0a3ZTdldMVmlka1FkbTltR0dUcXczRDFKaE1wa2l0VkFLNlNiNy9NS1NHcnllc01oWHpaOFFuNUkiLCJtYWMiOiJhNjZjY2Y4YzE0ODdmY2RkYzZlZGYzMDZkYTI5NzI5MTk4ZGEzYWYxMDEyYTQ3MDMwNmU2OTVmZmVjZWE5NDkyIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:45:37 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.62. https://adblbackend.peacenepal.com/admin/service-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/service-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://otkeqxliyivt.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/service-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
Cookie:
adbl_backend_session=eyJpdiI6ImlzdW1pSVNSVkE2RGMzYURnVldSd0E9PSIsInZhbHVlIjoiU0pIR2M0QkhBM1ErSkc0QnVCeGRxYUdOcnZHSldMclBRZ0tzTWh
wV2oxRktXdGhBbk1McXBKMGR4VzhPUmVIa0ZYdG9JU0hmbzRielRVL3ZmUy9ycmpOb2M3SXo0ZHlxL1ZPbzNvaHpPck9KWEMzMFdHaERZZUpvUGx5NEwzK
3YiLCJtYWMiOiIxMzcxZWU5MTJmNDFjNTU4Yzk2NmIxNjI2YTA3ZDFlNTQ0ZmVkNjg0YjRhOTgxOGNlMzkyMjAzOGRlNjFmMDc0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://otkeqxliyivt.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:45:49 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkYydjY3WmFOYzZGeitEd0ppWFJuM0E9PSIsInZhbHVlIjoiRFJtZ1dqRnovOWdGZGV4MjVGdUNYSjlPeHRYNmxlNWZhd2Vmdzh
GeGh4NHk5QWVtRVNqRUI5YXN2Nlczek4xZ0JDaXhydXRTUTVBNjJEdmdDV29wVEVPZlRPWkdDRWdxeE9oSE5TQytoWGlWWTFXSW03UjlabEphKzNwSTVMc
HEiLCJtYWMiOiI3Yzg0ZDNhNmQzMGFiZWQ5MjRkNTNiZWZkNzRjYWMwNTNmZTE2ZjlmMDAyMWIwMTI0MTNmNDQwZmJlYjRjZmM1IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:45:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.63. https://adblbackend.peacenepal.com/admin/service-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/service-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://dwjsaagzzvwb.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/service-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFlVU9zdnJNaEptSWR4aHB3a1ZOQnc9PSIsInZhbHVlIjoidnZxUXFIM2Y2WDR0NjJTUzlOQ1g2VVB6eGlEREpFVnE1WTZLOUh
nN0JkRUZFdm01QVNhQXVtVW9FMUlEeWJtalBtd1VkWXR4Y0RCRHJ1UE15Yk05MGVuaDh6WGhkaCs2RGxkc0VBNnRwdDBJWmZ0MWQ5QlY0elpDMmxCQ0
ZpdEoiLCJtYWMiOiIxYzM5OGQzMTFkYzgzM2ZkN2ZiNzliODljOWJmNjg1YjU4OTM4ZDkyZjE3MzY1MGU2MTBkZWI0MjQwNTdkMjBjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/service-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://dwjsaagzzvwb.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:31 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkdJdzVhalZrOFR6ZEhKQ3R4ald6cVE9PSIsInZhbHVlIjoiOXYzc2xPQXpyNGFaN3I0Ym1XbTdUUjNHWDRRc0VYRDZpS3JzRGpo
OHVhSGRuTVc4dEp5N05jcG0zNVB5cnpmN3ZGSkV5eFBsczNxZW9hNEZtNVcvZGpadkVyRWtZclVaUFVCZUtSSGYralZubTlTa0wrREpOOVFhUWF6YUdsVW8iL
CJtYWMiOiI5OTFlNzBkMzIzMzEwMDJkMGIxYjBjZWY0MmM0YjBlNmI3NGQyMTQ5ZThjODlmYTAxODE3MWNkMmI0OGFjNTliIiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:46:31 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.64. https://adblbackend.peacenepal.com/admin/services

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/services**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://isergutkdavm.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/services HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlQ1YUluZUo2ZmpjR2hXOEM0SFp0Smc9PSIsInZhbHVlIjoiK1Q3V0JwTkhianVSdVEyWkwySGJ1SDZseWRCRWJGdzVuRy94Nk
M0TUNqTEZhdTM2bHlrWXdaQjFBQU1aMUNIUTZvTVdGN2dWYlRDNVRHbHlrTHEzSmU2YThrTTlLem9QMDRJb05DaS8vM1RaUGo4Ym1QWXowbG42MlNQdn
NLV3AiLCJtYWMiOiJmYWI2MGFlNmY0MTljOGRkMGY5MDA1YzE0MmEzODg3NTQwNWNlNWZlNmY2ZjhjMDdhZjk0ZTM1YmVlYzY1YmM2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://isergutkdavm.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:22 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkVubmk0QzN4M2gveG5LSVBiSHFTc3c9PSIsInZhbHVlIjoiSFdOSDJZNHR3MmtZSVV2OTNWbFd0Y2tlYlBoTm9RczVTRkY0ZTQv
bzJ2OUpMRUpFdFN4dEROejRPUFhaSVRzLzk0S0VsVU1jYW9VT1lYUUFoam9LMGErV2J5OWlORUE2dS9odW03YWs5K1M0cWVsN2JVSE9aVU95UVFjckM0e
WoiLCJtYWMiOiJjYzZmYWU3YTRhYmU0ZmZlN2ZiMDAyNjNmNWJiMTQ5YTM4YzBkOTA1MzQyZDUzYWFlZTdiZjgxZmQxMTZiYzAyliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:46:22 GMT; Max-Age=7200; path=/; httponly; samesite=lax
```

```
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.65. https://adblbackend.peacenepal.com/admin/services/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/services/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://cdtakxxhabde.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/services/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImZnSDZhUUptdDU5RUJod3U2VUVWMlE9PSIsInZhbHVlIjoiY2N6bzgxSzh0U1YwWkxkRDQ0aUJtQkpKRDBqbGxhNkRvcjFzM05
ML2YveVM3dDJwYytzNG9pM3NhTTBPOGFySHovdXBwMmdCY09EMWtCcmtzenQyYk83bkNmUXlSUHJwbHdMbXk0bXlDMUt2cHozZ3ZwZXVoSnNMdXFMUnhX
bngiLCJtYWMiOiIxNDk0MzljZDdmMzlhNGIxNTllY2YzMDIwYWJlMzljZjU0YjJhNDM0NGQzYWVlNGFlZGRkZTRkMGZjNGMyYzhmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/services/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://cdtakxxhabde.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:08 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InY3cnEzYkoxWGhMUWh0dERRVzUwY0E9PSIsInZhbHVlIjoiRHh1WC9tL0haWU5DUUJiNFNsSVRLQzJWekFNWnZJNThNR0NH
dWVRdW9McDFiWEltckxDYWNHak15TkdRQXlZdmxJRzhTMEFtdFdpN3lQNWc2SHZjWG91TjlwZk9jYlZHZ3ISb2hjSmFvN1FtNGpXNlo3R2JJZG9GZXVBUlZMWU
4iLCJtYWMiOiI0NWYyZjIyNDRhMzQxMWZkMGE5YWZjZmZhYWYwZGMwOWM1MWZiYjRjYjQyNjM0NGFiNzg0YzAyNTc2ODkwMWVhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.66. https://adblbackend.peacenepal.com/admin/setting

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/setting**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://dppmkkdysjau.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/setting HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ijg0NFowMk1YY3hRWldabElkclgwVkE9PSIsInZhbHVlIjoibUZsL0ZnUnFWRU9YSkhwRnE4MGNaWExISjVnK0hVV0J5VVZCampPUk13ejRnaXF3ZndjWjdnUmo5NE9mNFhWM2cxb1EzR1NUeHlQdW94d1pPanBrZjQ3MlBpV0JoUk5SenZINEQrRGFPa0tnRzBVMGdod1U0RzBYaGVjWFFxb1oiLCJtYWMiOiJjNzI1Mzc4ODlhYTUwZGUwNDA4OWRhMWU1NjM0OTU1NGM3NTM2MDEwNWZhZGNjMjc0OWZhNWFiMzE0MDZjYjhlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/setting
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://dppmkkdysjau.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:46:55 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImhXTUtzZnVsZXA3azlKVzg5Q3hKNXc9PSIsInZhbHVlIjoiRTVMZy9jZmNOV1FuLzRPeGl0SGRzOUVMMll3YVVRR0d1MWFDVWFzNlQzOTVTalljaXdxRFlaYUxTTFdOcVhuYVRIb2xoWk1xeDU3SjlaWU9xT1ZUWG91Vkt6WFFCSk9SRGFVdXVxeUlTK2RCRE9MTDZUenpQN0d1NDhIUHBySFAiLCJtYWMiOiIzMTFhNDJkYjgyMGE1MzRlOTJhMGQ0MzkyOWM1MjgwYWI2YjljZDkyYzI3YzY0NTZhNjFlY2VmNjBkZTA1MTIxliwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:46:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.67. https://adblbackend.peacenepal.com/admin/team

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/team**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://uskroolggyxq.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IjVaa0pKYSs1U3hZWTEvanBXWmxoN0E9PSIsInZhbHVlIjoiT3J4SE96S3B4aytyUXlnWHdiZWFuYzUwWFBjSGozSHJLNTdObTZa
cGFDV0FJa0NMd0hmVFFZZC9XUG5HOGpibldDQWlaK01ySkVoNmU2VC9LR0JDb2d1MS9YbkhtL05sSkgxTzA4YTl6bit0WWxKeWVoYzl5YS95ZHRYb3RVemEiL
CJtYWMiOiI3MDRlNzZlNGM4ODM2NjlmYjdmYWRhZGE3OGE2ZDY3NDQ2MTQ2MGZkMGE1NzJhYTZjYTc1YjZkMGZhY2NiZWU0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://uskroolggyxq.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:47:03 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjNQeFFtYVFodFNLYzhseTJRRlhOVkE9PSIsInZhbHVlIjoiUmo4UW1XczhvU3NzMUZNMkxoeUNiOGVTS1E5UzdKY1I2RUtkSmVu
SFZKenc1ZTBhdEpjdzkwVzRLYTFuN0FIWU9XZEtFNzhrVmZOb3h1V0ZURmxiRFNzYTBrM1U2TGgreVgwYmN0SDROSWlsaDZEc0QySGxUTWY4bFVRTWZqN
DciLCJtYWMiOiJkODBiNjhmOTI4NDMwNDJhNDY0ZjM2MzMzMjUxMTUzMGE2MjNiMmIwNDI3MmQ4MzAyMWNhNjM5MDM0MzBlNDQwIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:47:03 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.68. https://adblbackend.peacenepal.com/admin/team-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ktvwueyjnwbj.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlJNUEpLQURKQzZnRjZSZW1RQWRWVEE9PSIsInZhbHVlIjoiZFIydHRaR3c3K0k1QXdWYklPenlDTVBSaXhZTk1leHJjT09LTm9zcXhmOFZHdzFBU0w3QzRMdE5ZNzN5ODZLMDNtUDdjeTJOYkM0MGV1UjlxYmkzb2xpVDloSWVpOVZ0Sk5laGs1V2xudEVSb0RwcW0rbjN3eE5rbW1aRHpQMlciLCJtYWMiOiJlMmJjNDY1ZjAwZTc3MjFmODFmM2RjODMwZjVlZmYzNjViNTZkOTlkNDg3NzViY2FjOTgxMDVjMDE1OTM1MmUyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ktvwueyjnwbj.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:47:19 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlVkbFNNQjdYSVlVa21CbDR3bFZpUWc9PSIsInZhbHVlIjoiUXZUdkNvY2FORFF6VWx3Nks3R25SWXN0WWhQQ0QwdXN1ajV5RmNXb25DY2tjVXFRRitiTXpXYzJxdXRMS29hOUIrb3o1ZElJTktlc0Y4d2lnOFloNWMwd21pTGw1NmVvRjUwWUZQeXQ3ZWQwN3hNMXFZanZkWUtQZU5HUWVqYWkiLCJtYWMiOiJmMTNlNzI4YTlhNjcyMmJmNzI5NjIyMTU3YmE4NWJjZDdhOGYxYjc5Njk2YWRmZmY0MzU4NDMyZjg2ZWQ0NzI3IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:47:19 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.69. https://adblbackend.peacenepal.com/admin/team-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://iahcmotzbahy.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik5ac1BnczladzZreURFejRsNHZweHc9PSIsInZhbHVlIjoiQVlxZ0MyS3p6TVF5NldmZkJwUitpbkpDaWJqU3dhUjJDb20yUVo5VFphQUJRR1ZTTENqK1FoN3dISUlWY2ltSnJjajYwZHkwL1ZpZ2tCVitNVzZHcGNwWWxCTE02VWs2UDZwbFhENkZ3Qlp5T3QvbXAzMnVNSDBSUVR0OGkzVDciLCJtYWMiOiJhMDczNzFhZjFjNzQyMjlkOGNjYWI3YzBiNTczNTU4N2E3YTFlYTI0MzY2ZGZiMmRiODA1MmJlMTBmZTIzMDJmIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
```

```
Referer: https://adblbackend.peacenepal.com/admin/team-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://iahcmotzbahy.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:02 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IkxTTTdtckppMVEzcGcwVDMzUE9EQ1E9PSIsInZhbHVlIjoiaXRteEFONDA3c2NmR0x2Zll0OFVNaXk4UE5acGV4NERrWSszbU9rakNuT2J1SjUwenVBQVZyQkE5Y0VDTXZRRlJvTS9SNXNMS2tiMjVTWmFNcU95T1h2SmRxSVNUdWlGTk9LNzR2K0hZcGtLQ2MwNFRwMXZoY2ZjbmFueGVicmciLCJtYWMiOiJkOTgyYWNiZmM5MDYyYzZjYTY5MjkyMTk5ZmQxYzdmZGY2YjQzMDRiODJiZTJjMTZjM2ZlMjgzYjhjODA4OThmIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:48:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.70. https://adblbackend.peacenepal.com/admin/team/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/team/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://gxtgbumrispy.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/team/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im9zcGdEYnpGS1hrV1YxeW5WTmlzVXc9PSIsInZhbHVlIjoiTzlHYlIXM3FVOTliZnR6eUp5bjlzcjU5bm5yVC9lV0YyWm9qWUZNK3FEbVlmSHg4bVpnWFE5NERkNDlTSnFBODRPVmY3UlJ6ZW4xcVpkY2dOMWpMZ2d2VUV2SnlNTkkxZmNlUTk3WEtCMkp3c25JRlhreWhBbmhWOVdocWdVSWgiLCJtYWMiOiI2ZDJmMjlhZjNlNzVlOTQ5Y2EzZWVmOTQ2MDQ2N2JjOTYyMWQ4MWRjNTJhM2M5ODhhYWRiNDNjOGNjZjViODQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/team
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://gxtgbumrispy.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:11 GMT
Server: Apache
```

```
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjRYbFR6bTV4SHZtbzJuUTE3d2xoK2c9PSIsInZhbHVlIjoiYk55WjRIYUhIcEVVMDd1cjBabW5QZnpWcjF6Y3RveEZoUEZMRVMvM
khWa09pYzF5c29zVWJJYzh3NzdLWDZETnR0VzcxRUM3eUVNNzlLRVRzeG9tOVZMSGNqNzVnejcyeXc5OGI4RTN1WXhTOXlyZElwb2VnWVBxLzlOR3A3OFMiL
CJtYWMiOiIzY2Y0NGJhODJmZmRkNzlmNGVjOTlhY2RmNzQ1MTc4ZTdjMGRjMjc2MjAwOGNmNWQ1ZmZjYWVlNTQzZDExYWU4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.71. https://adblbackend.peacenepal.com/admin/training

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://njnzekzfynor.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im93dDZpVE1lWVhCTVgyU29TUEdPZnc9PSIsInZhbHVlIjoiVU85QUhCaWQ1WUdDL2RRRUE5RnFBZVdFSjFXMmlXL3JvdTBpYj
R1MnovcURQaTlnUlBxZ25wZllnTm9QTDc5SVY2cXM1bmNiT1d0WU16d2paazFTUUgwWlZ4NDhSWkRyUTRDV3hTZ0pLV1QxL3AyL1NnL1dWbnNPYmZsR2UxV
kUiLCJtYWMiOiIzMDNhNTBkNzllYzQyNjQyMmM4YWYzZDU4NmFhNGI5NzRhNjAzMmE2ODE0NThlYTk2NjdmMjYyMmQ2NTk0YmY3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://njnzekzfynor.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:15 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImNVWFB0d2E2QW10WkErZHU0T3daMEE9PSIsInZhbHVlIjoiOFgrRnRNTGhINit3OVJ5WVdHNE94ZEdhV25wcm9qcFVoOEVxR
UFkM25ZY3Roc3FXK0dXbDd2ejNhWWJkaDVpdGxGMkhHZVE2NlB6ekQ3TVBKaXZuZ3dwcGRuaUgxbXBENFpheVlvWmdzMEdaWWlNYloxRmM0L0VmU1RWa
DBybE4iLCJtYWMiOiI3YmJjNjhiZjBmMjE5OTA1ZmFmMjMwNDUzMmRmY2ZhM2VkNTdjNjkzMzQ3ZTk0ZDEzNjBmZjczYjY3M2Q3Yml4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:48:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430
```

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.72. https://adblbackend.peacenepal.com/admin/training-hall

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training-hall**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://zsqlnhbpyaty.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlhQRHV1ZWNBMDdnMFBOZmR1MXdxclE9PSIsInZhbHVlIjoiQ1Q3Vm1YaVo5NXlFQmd5SmJUN0ljdlVoeTFPblFjUjM1SHZyRGZtaU9MbDZ0U0ErUlR6WGtmeXZJZ3pEbnNwQXNGUnh0MFZaODl5UVVtL3hjdkZ1VnBqTmpVRlluckM5OVpJVjI5MVo4cTB5a1dDeExzbmFqQVZ0bTZGOHludWoiLCJtYWMiOiJiOWI4YjA2ZjYzM2EzNDg3OGFmMjQ1ZjE0Yjc4OGY4ZjM3YmRmODY1MDRlNmEwNWUyMTA1MmZhMWViMmRlOTNjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://zsqlnhbpyaty.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:48:20 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IjJoOUUzUFB4aGdXMExLbko0OGYvSnc9PSIsInZhbHVlIjoidkkzZTFodFgzTk0wOFRrNEhZV0o0a3VnbWV1anpLUUhmd1RLbjVBR2xLbUVYSjZWVndjeEh1WHQxV3JPUkRnS0ljVDNuMGExYUhDVzFIaEkrdmxCZkZpZFI1dVNhUUJDVll6N3FGRXcwb1RmWGJmcTQxRkVqbkZKZThGeit4OGQiLCJtYWMiOiJhNjBjZTZiNmQxYThjYjZhMDllZmEwZDQzMTBiZGU5Mzg1MjhjMWFlYjU0YWE0YzkxNWJiODhlMjM3ZGY2NTFmIiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct 2024 06:48:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.73. https://adblbackend.peacenepal.com/admin/training-hall-bookings

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/training-hall-bookings**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://zpyorvprtaii.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall-bookings HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik84OVRLQXdkTFB3dUk5Yy9TQlFycmc9PSIsInZhbHVlIjoiY2phc3RKOElWZSt3WFB4Mk1RQlF4enE0RWFXTFc1d1E5NTRCTVB
EVlIxSjI0NGdRc2NaZGREYzlXZEFlUDBLR3M3dGlpT25lYnhxK09YeXlXVm9LakFvN293aU9TRUYra1FPdU0vKzVJclQ2NDJqT3VpUDZMb042RzI1bElsQm4iLCJtY
WMiOiJkYzk4YWE0NDIxNTg4YjVmMzU3ODMzNTYxMjc3M2Y5MGMyNDQxMTFiZmQwMTQ4NTExNTIyMTFiYTk4ZTU2MDZlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://zpyorvprtaii.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6Ijg1SjZud0VWZjZQZjdZY2hHS0VKdFE9PSIsInZhbHVlIjoiK2ZHSFU1RS9NQU8vWmI4U2Nnd2czdU1WMU0zaE8xVkRKeTVFNEsy
eldqMll4dko2amFtcVBIbWhNZUNLcGxtcHUwT0wwUnNrc2xCdUw1bmpUYW5TZyt5RXc0cmJoQmc2M3RrNUxhcjlpRWJSTWI1VlcrZk4yaXl5YVNYRUljcUoiLCJtYW
MiOiI0NzE4ZDhlZWU1NzI1YWI1NzQxOWZmYTAwOWFkZWM3YzQ4NjI1NjdkMzIwYzQxZTk3YTIzMzUyZDE5YTc4MTU5IiwidGFnIjoiIn0%3D; expires=Thu, 03 Oct
2024 06:49:06 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.74. https://adblbackend.peacenepal.com/admin/training-hall/create

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/training-hall/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://uadhqnbikncj.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training-hall/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik80TGk4WnlRMzRQeFRiRE1RVC81Q0E9PSIsInZhbHVlIjoiUEgwZm9YYStZWFUvTmVOMk9TcUdPU1lERy80Rk5YcmRwZzdER
VlLVHB0U01qdGx6NEZQVm1SQVVMN1NjYVB2VjJndVZRNFJkRWhiSzBPOFpKR1lXM1F6M0M1UmM2SDlJWXUwUmFWUnlnbzJybkhncVpwb1ZUWktmMWt0M
FVrVXEiLCJtYWMiOiI0ZWJjYzViYmQ2MmU0MzQ2MTkzYWVlYTYwNzIzYmY0ZTEzZDFmOGU4ZGZkYmMxM2E1NjUwOWJlNDE3MzFkZGY4IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training-hall
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://uadhqnbikncj.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:13 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InMwdjNrdUtpcEJMR3BoTHUzS1lxM3c9PSIsInZhbHVlIjoiNjVzYVgrM095MzZQSFBIcVBTMTZxRlNqZmtFcU5kbXJWSWRBbDBNa
mJQWC8rNWJXWFJwUUZ3YjJENmFhWWZtL0Ntbzhvem9pKzlUOUJkVTY3UTBNQldsSE1CNlFXYmVtRHJHZXVUQVZ1aHJ6NkN6WUdEVSsvcDM4ejlpY2ZVUT
UiLCJtYWMiOiI2ZmI1YThhZGE2YzFhYzUzZWQ3YTBlNDRiYTJmZDFkZTk2MDY4NjIxMzEyYjdkNDhhMTZlOTQyZGNlNTg4MGVjIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:13 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.75. https://adblbackend.peacenepal.com/admin/training/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/training/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://ynlzztamjgyo.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/training/create HTTP/1.1
Host: adblbackend.peacenepal.com
```

```
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InFVZ1AxRlhTRnRFVlNsOE1VRTM0RXc9PSIsInZhbHVlIjoib3hSZDV4dStnc0hhVElqQ2JCclF1R1dCRU1VYUMrSUUvTU1DNS90
QmltaFlySWFCN05IN3M1RWdSVzArZ0w4OW1mVFdzSC9IYTNVSEVzbFBzeFVnQnZ3TW1CbTJwNjgyRno1UXRoRURoMnU0djEvNVpSdFh3UldTb2lReUpvbkkiL
CJtYWMiOiJmMWNiYzZmMDAxMzM0MzRlMDkwMWZhYTUzNjZkODM4OTJjYjNiYzc3ZTQxZjI1MTVjOGQwNGNmYmY5NDUyNTZlIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/training
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://ynlzztamjgyo.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:03 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlNDMmpzTnZHeU9OcExNc1ZMZXBiRFE9PSIsInZhbHVlIjoiYTFLcjI3WXZ5NmRqVEFDZDUySk83V2hEbVU3RHQ4UDJsZ01ZTm
s2NTZQS3lKRkhINWxJVXYvQlZEaEtkWGFOcmwyclFsWHl0ajllbCtqL0szdjlwWTQya1dUYUJ1VGVuYmZncnNoSlJ1anhaaWxDUDFRTzFvS2VXWTBtNTdMYW8iL
CJtYWMiOiI5NTc4OGY5NTgzM2Q2ZWZmYjE1ZTgzNDQ1NGI2MWI1ZTdhNjg4NDY5NGZjYTQ1MDQ5ZTgxYTViMGIyN2IyMWMyIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:03 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.76. https://adblbackend.peacenepal.com/admin/vendor

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://wlxjdgsphney.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkNMY0F2UnZySGkwNjZZaW5HQVhKSnc9PSIsInZhbHVlIjoiVi9EanFwbGZRWU9LOTdBYXVFTHRwT0gvTURobHdsZVo2V3l5Sm
NPRjdLUUFLRnJEdXgvZDNzNUk2bElKdFdCQXdaVE1xVUhma2tqdVUwY2RXcUNCblhZQTcxMzB3NmtQK3VDd2lvd0tJR1pia1VDUU9YVjhGQ3FiaEw2a2JQTS8i
LCJtYWMiOiI3OTgyM2YzNDdlODVmMDFhMjZjNTgxNDYwNDE4YjgzZGM2ZTI0YzAwZTVhZjMyYTc4OGM0MWNmMGIxMDRjOGMyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
```

```
Sec-CH-UA-Mobile: ?0
Origin: https://wlxjdgsphney.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:47 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InZnNEF3ait6WXU3OEYvVndReVQ3WkE9PSIsInZhbHVlIjoiVytXSm1mOUlnMDE5K1cvVmtQWkttR0RCREs3alhxOXhKZnJzVDlY
RytLajVaenllVU1XRm9lNCtOclJQVHpsMEQ1QzIrd2lLa3ZKTi9LVENQSkV5SWVILzZFOXJxNzRHVXVHOVVlNEpBTmEwTGhXOFJ1YnQ1cFQ2Ymduck50WHEiLC
JtYWMiOiIxOWJhNTk1NGZhNTUzYTUwYTU5YzVlYmYyYjUyZWYwZmEwZTA3NDlyY2MzODE0ZDJlNThmZGQ3YjY3MTNhYTAyliwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.77. https://adblbackend.peacenepal.com/admin/vendor-category

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor-category**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://opsjrkdrodfe.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IklLZ2pHZ0s3eWFZWkZCVWdsTnMzUGc9PSIsInZhbHVlIjoiZEsxQ1RiRnRJeXBQNTVNTHRHMkVIOEZRRFhVZmVoTjNpTUJwb
mI5UmJuQzZ5YlhqK2s3SGlJeldWYXVJL0Y4bXVseEtVQTZtT1JITHN6SEpVL1p3WTlqSFlaSnkwNmRDRm9FeDFOUmdwT2VhdjZLNEJnQ243aDBIOWhmcjNFYko
iLCJtYWMiOiJiMWJkZTJjMTZhMmVkZmFhMTdiODA5YzgyZTg1ZWNmOGJhNThhNTZhNGQyNGFjZjQ0MzE4ZGNhNGU5YjhiMjQzIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://opsjrkdrodfe.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:49:56 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
```

```
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InNuMUVYTTFyNWxmVG8rd1EwWUd3bUE9PSIsInZhbHVlIjoiUlA0R1FQUlN3eG5MVlovRXF5MmZ0NlJrMkZxS0hTQW1Yajd0dThBQnFiMmlCaHUvNEI2b3UwSEtjSVNoWW9kSjZZaEs2M20yblJCd0lGWklBblhYWWh2UnRmclJ2elZYaHFGL0tEM2cyZzZvdW1ldkkzNnI2WTV5TjZxWTZaaW4iLCJtYWMiOiI0MDMwNDRmZmE4MGZhNmM1MWFjZjU5NDkwNDE4MDlhNGMxOWY2NjhmNWM3YzkxMGEwMTQ5ZTAxNTc4Mzc0ODVhIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:49:56 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.78. https://adblbackend.peacenepal.com/admin/vendor-category/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor-category/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://lseswgtjcpis.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor-category/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik1PT0NocDBhQ1pHV2RTblNmYmlaakE9PSIsInZhbHVlIjoicUdyMjA2NDRnZVBPV1Z1VHhrbkswM1N2ckFJUThCSEl6eXNhK1pXWHF5OFFGdVBzQ3NRKzFqYmJ4bWMySFNQQlVOMGlMaSt2Y2dKOENxbjJudkhEbWJqZmRoQjR2WmJtWGlNMlRTRWd2Q0ZFOVprc2c2akV5VlY0UVJnRHhuRFEiLCJtYWMiOiI5OWFjZDI2N2YwNzNiODlmZWNhYTMwZTczNWQ4MjViNjJmNzcyMTg4NmYzNTU3N2NhMDBkYzcyMzQzNWQzZmQwIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor-category/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://lseswgtjcpis.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:51:40 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InREaWZHVHFpSnhRVjlqeVF3NGhiNEE9PSIsInZhbHVlIjoiVlhTUkxSWk00QXBqdEdjWGRYN3l3NUU5NGg2UnVMQjNIVjM4WjBwbTRWTzdCQk8yREF5QVJzTE9NMC9lcUl0MFU0QjNxQ0FVRWZXM0pLUithYVh4TUpBd056S0w5WlFMK1dUWEhPaXFsVVV2RHdqTGg5OE9FRm1ZeVliRk52cGgiLCJtYWMiOiIyNTJhNjhhMjE1NTIyMmNkNjA3MzBkZmMxYzE0OTk1MzI0YTM3OWVjZmM3NDc0OGRkNTJiY2IxZGUxY2Y3MTk3IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:51:40 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
```

```
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.79. https://adblbackend.peacenepal.com/admin/vendor/create

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/vendor/create**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://btktnqplgyor.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImxLaTNZZXc3eGlBSXpwVzlINnVuUFE9PSIsInZhbHVlIjoia2Q0OHE0OVRaUURDVU53NnJaZ09BYkx4WnNJYUM5bjUzaVFFQU
M0bmsrV25sam1DRWtUSUtZTVBHMmV1NE95US8rMFlNbGlXYnZzd09RVzEwc1RnYnhrTWl0dlVLVW1oWnRYejRyemlhNll2aWl6NnN1b3FJNHQ3TE5vZWxWcDc
iLCJtYWMiOiJmYTNiM2ZlM2M1NmFmYmYzNDdjNDJhNDBjODVhN2U4NDRiNTBlM2ViMDkzMzgxYTk1MGM0OTg3ZjcyODJjZjY0IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://btktnqplgyor.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:50:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImtTYzBMM3BUYlZOQkNIWVN5YWh3V3c9PSIsInZhbHVlIjoiQjc5OElEcWZ3c3BDbUREY1dHNVBocE91dHAxSmVrV203VnpoRkx
NeDJvcEx0cjZkTnYweEJZR3FxS3c0aERucW9ObUoxU01TeTlzbDBVUTJ3Tk8rQzhmTW9BR29WMTErM2ZzNUdkcTVqWGxxYUZhTU1RTlFuYXNhcTEzdXkySHUi
LCJtYWMiOiI1YjE0ZmVkNmI2YWFhYTI3ZDBiZGNjYTUzOWI3YTllYWMyMjY2N2I0MTUxZWUwNWMxZjZmOTcwODA0MjkwMTIxIiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:50:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.2.80. https://adblbackend.peacenepal.com/admin/vendor/import

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/vendor/import**

Issue detail

The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain.

The application allowed access from the requested origin **https://encdrmeqaerj.com**

If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.

Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks.

Request 1

```
GET /admin/vendor/import HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InhRdFp3WlhhNHI0ZFZaL2thVURyT1E9PSIsInZhbHVlIjoiOWl3Vmt2U2EyVkZqOW9iVFZ6UWlBa0E1NmpVbWdYRFcvdFR6Tlp2V
zJRSUZrRGZNOXVoeFJ3bnAwNnQ2clBuNTY1YSttUFhyT2ZXK09KZmc0ZEY0Z3BqaXVvNzJmTk9OMG92NWt3OVMxZ2lyYXlhSjNYTE1TQkNCYmtsazdJWHciLC
JtYWMiOiI5OWRiNGIwYzY1ZjcwZDU2NTRiMjI0NjJhN2I0YWU3YjRlYzQ5ZjU2NWViNTU2MTRkZjFhNzg1NWJjNDhlMTU3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/vendor
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Origin: https://encdrmeqaerj.com
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:50:18 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6IlViMnNVWEZSMXZZclB0UzREUk9LTVE9PSIsInZhbHVlIjoibTVJNy9Gbk0zTWd5MVJGTndqN0FxOFBpN1NTeXBhUk9oRDFlSkd
WY00xQmd6dWtyK1NMZVJncHZWVGlueVV2RDM4OEZiU3dNSWY4eEduUS9JUVQ0Q0Njd21oZXUvRU40SlVTL01xYzJzR1dKS2dxVndySnhqdENMYmU5K0FtZ
zAiLCJtYWMiOiJkODA1N2ZlOWE1ODM2NTk2ZTc1ZWI4NGE0ODAzZmM4MjkyZDZlMzEyZWM0YzU2Y2QwYzY4NmI4YWJjNTc1OWQ3IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:50:18 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.3. Cross-site request forgery

Summary

Severity: **Information**

Confidence: **Tentative**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/login**

Issue detail

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

The original request contains parameters that look like they may be anti-CSRF tokens. However the request is successful if these parameters are removed.

The application appears to block the request cross-domain by checking the Referer header. However, the request is successful if the Referer header is removed. Note that various techniques exist which enable cross-domain requests to be issued without a Referer header.

Issue background

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Issue remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

References

- Web Security Academy: Cross-site request forgery
- Using Burp to Test for Cross-Site Request Forgery
- The Deputies Are Still Confused

Vulnerability classifications

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery

Request 1

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdWJ6VW5GMFl3TklmajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHFML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/login
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 109

_token=psvOCIIjyWEguowk14Vu2U2PGcuDN0PvKSvaqYOv&email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 1

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 10:52:03 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6InRJMHdlNHRQVHk4T2QxL3FreXhNUFE9PSIsInZhbHVlIjoic3hneENjTTJNd3UyQVdJYlI2WFdHa0RRb09xU21nQ25tVEZBZ21zVW1IVkNEOG1sYTFNZEMrWWNLZUZjMG9HM3JJTytrOTlEMTBMSmNuZVZGSDhMSXdxcXUzVnp3OHRQVm52ZWh3SnFyQ2x3V3F2SGNwS090SHhpa2dERHJQbU0iLCJtYWMiOiI1YzVkZTcwYmVhOWZjMDY5YTQyMWYzNzIyMjJhMDMzMDNkYTM4MjAzN2YxOGVlYjM4NWM0NjFhYThmNmQ3YzQ5IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:52:03 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
```

```
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

Request 2

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdWJ6VW5GMFI3TklmajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHFML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 61

email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 2

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:23:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/admin/login
Set-Cookie:
adbl_backend_session=eyJpdiI6ImNWZzRwVEZmSXpKM2pLY1hZRlUrS1E9PSIsInZhbHVlIjoibk9aeEM1VTg1MG1ETEQxYkFuRFJNdHhUUUxJeXllbWpIMkhlMlFPZnNrVUpTZitqM1N1WlJLcXVYNTRhNWt4TVFIQ0Q4MGVHUmpqSW9DTnlCcWJUaGtQaDlndmFLc2YyMXZQY3BCclQycU1EMGJ2STVCR2NMeGVkVWNHMzlPOGYiLCJtYWMiOiI4ZDhlODhiZGQ5NzQ0MmRhMGM0NDcwZTZmMzkyNWQ2Zjc0MTcyYjRiZjBiN2VmNjY1MWM3MDZjMGJlMWMwN2Y4IiwidGFnIjoiIn0%3D;
expires=Thu, 03 Oct 2024 06:23:53 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 430

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/login'" />

<title>Redirecting to
...[SNIP]...
```

4.4. Spoofable client IP address

Summary

Severity:	**Information**
Confidence:	**Tentative**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue description

If an application trusts an HTTP request header like X-Forwarded-For to accurately specify the remote IP address of the connecting client, then malicious clients can spoof their IP address. This behavior does not necessarily constitute a security vulnerability, however some applications use client IP addresses to enforce access controls and rate limits. For example, an application might expose administrative functionality only to clients connecting from the local IP address of the server, or allow a certain number of failed login attempts from each unique IP address. Consider reviewing relevant functionality to determine whether this might be the case.

Issue remediation

HTTP request headers such as X-Forwarded-For, True-Client-IP, and X-Real-IP are not a robust foundation on which to build any security measures, such as access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to spoofing.

If the platform application server returns incorrect information about the client's IP address due to the presence of any particular HTTP request header, then the server may need to be reconfigured, or an alternative method of identifying clients should be used.

Vulnerability classifications

- CWE-16: Configuration

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:28:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032928

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

Request 2

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
```

Response 2

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:29:00 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032988

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

4.5. User agent-dependent response

There are 3 instances of this issue:

- /admin/import/store-atm
- /admin/import/store-branch
- /admin/reset_password

Issue description

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.

To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

Vulnerability classifications

- CWE-16: Configuration

4.5.1. https://adblbackend.peacenepal.com/admin/import/store-atm

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:12:24 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032948

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
ier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928744,"message":"The GET method is not supported for route admin\/import\/store-atm. Supported methods: POST.","glows":
[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/adb
...[SNIP]...
);","56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95
Safari\/537.36"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027,
\u0027SYSTEM VERSIONED\u0027) order by table_name","time":6.96,"connection_name":"mysql","bindings":[],"microtime":1727928744.467329},{"sql":"select *
from `site_settings`","time":1.12,"connection_name":"mysql","bindings":
[],"microtime":1727928744.468784}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-
backend","application_version":null,"tracking_uuid":"9dda0702-6be0-46cd-8224-f5b8e7e33a86","handled":null},"shareableReport":{"notifier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928744,"message":"The GET method is not supported for route admin\/import\/store-atm. Supported methods: POST.","glows":
[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/adb
...[SNIP]...
);","56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95
Safari\/537.36"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
```

...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027, \u0027SYSTEM VERSIONED\u0027) order by table_name","time":6.96,"connection_name":"mysql","bindings":[],"microtime":1727928744.467329},{"sql":"select * from `site_settings`","time":1.12,"connection_name":"mysql","bindings":[],"microtime":1727928744.468784}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-backend","application_version":null,"tracking_uuid":"9dda0702-6be0-46cd-8224-f5b8e7e33a86","handled":null},"config":{"editor":"phpstorm","theme":"auto","hideSolutions":false,"remoteSitesPath":"\/var\/www\/html\/adbl-backend","localSitesPath":"","enableShareButton":true,"enableRunnableSolut
...[SNIP]...

Request 2

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
```

Response 2

HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:12:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033028

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
ier":"Laravel Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotAllowedHttpException","seen_at":1727928745,"message":"The GET method is not supported for route admin\/import\/store-atm. Supported methods: POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/adb
...[SNIP]...
);","56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027, \u0027SYSTEM VERSIONED\u0027) order by table_name","time":5.73,"connection_name":"mysql","bindings":[],"microtime":1727928745.161055},{"sql":"select * from `site_settings`","time":0.99,"connection_name":"mysql","bindings":[],"microtime":1727928745.162391}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-backend","application_version":null,"tracking_uuid":"15097ad0-c358-461f-980f-19c402aad415","handled":null},"shareableReport":{"notifier":"Laravel Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotAllowedHttpException","seen_at":1727928745,"message":"The GET method is not supported for route admin\/import\/store-atm. Supported methods: POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/adb
...[SNIP]...
);","56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027, \u0027SYSTEM VERSIONED\u0027) order by table_name","time":5.73,"connection_name":"mysql","bindings":[],"microtime":1727928745.161055},{"sql":"select * from `site_settings`","time":0.99,"connection_name":"mysql","bindings":[],"microtime":1727928745.162391}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-backend","application_version":null,"tracking_uuid":"15097ad0-c358-461f-980f-19c402aad415","handled":null},"config":{"editor":"phpstorm","theme":"auto","hideSolutions":false,"remoteSitesPath":"\/var\/www\/html\/adbl-backend","localSitesPath":"","enableShareButton":true,"enableRunnableSolut
...[SNIP]...

4.5.2. https://adblbackend.peacenepal.com/admin/import/store-branch

Summary

Severity: **Information**

Confidence: **Firm**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/import/store-branch**

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:13:54 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032972

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
ier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928834,"message":"The GET method is not supported for route admin\/import\/store-branch. Supported methods:
POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/
...[SNIP]...
,"56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95
Safari\/537.36"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027,
\u0027SYSTEM VERSIONED\u0027) order by table_name","time":8.91,"connection_name":"mysql","bindings":[],"microtime":1727928834.428159},{"sql":"select *
from `site_settings`","time":0.93,"connection_name":"mysql","bindings":
[],"microtime":1727928834.429433}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-
backend","application_version":null,"tracking_uuid":"0c5b54b8-a642-4e4d-94cc-3e7a520d7490","handled":null},"shareableReport":{"notifier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928834,"message":"The GET method is not supported for route admin\/import\/store-branch. Supported methods:
POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/
...[SNIP]...
,"56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95
Safari\/537.36"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027,
\u0027SYSTEM VERSIONED\u0027) order by table_name","time":8.91,"connection_name":"mysql","bindings":[],"microtime":1727928834.428159},{"sql":"select *
from `site_settings`","time":0.93,"connection_name":"mysql","bindings":
[],"microtime":1727928834.429433}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-
backend","application_version":null,"tracking_uuid":"0c5b54b8-a642-4e4d-94cc-3e7a520d7490","handled":null},"config":
{"editor":"phpstorm","theme":"auto","hideSolutions":false,"remoteSitesPath":"\/var\/www\/html\/adbl-
backend","localSitesPath":"","enableShareButton":true,"enableRunnableSolut
...[SNIP]...
```

Request 2

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:13:55 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033052

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
ier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928835,"message":"The GET method is not supported for route admin\/import\/store-branch. Supported methods:
POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/
...[SNIP]...
,"56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1
Mobile\/9B176 Safari\/7534.48.3"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46
(KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027,
\u0027SYSTEM VERSIONED\u0027) order by table_name","time":6.36,"connection_name":"mysql","bindings":[],"microtime":1727928835.090044},{"sql":"select *
from `site_settings`","time":2.04,"connection_name":"mysql","bindings":
[],"microtime":1727928835.092447}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-
backend","application_version":null,"tracking_uuid":"467fa400-8b4b-49e2-8e8e-ca52aaf76666","handled":null},"shareableReport":{"notifier":"Laravel
Client","language":"PHP","framework_version":"10.48.17","language_version":"8.2.21","exception_class":"Symfony\\Component\\HttpKernel\\Exception\\MethodNotA
llowedHttpException","seen_at":1727928835,"message":"The GET method is not supported for route admin\/import\/store-branch. Supported methods:
POST.","glows":[],"solutions":[],"documentation_links":[],"stacktrace":[{"file":"\/var\/www\/html\/
...[SNIP]...
,"56":""},"arguments":[],"application_frame":false}],"context":{"request":{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-
branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46 (KHTML, like Gecko) Version\/5.1
Mobile\/9B176 Safari\/7534.48.3"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip,
deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit\/534.46
(KHTML, like Gecko) Version\/5.1 Mobile\/9B176 Safari\/7534.48.3","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
le_collation as `collation` from information_schema.tables where table_schema = \u0027pn_adbl\u0027 and table_type in (\u0027BASE TABLE\u0027,
\u0027SYSTEM VERSIONED\u0027) order by table_name","time":6.36,"connection_name":"mysql","bindings":[],"microtime":1727928835.090044},{"sql":"select *
from `site_settings`","time":2.04,"connection_name":"mysql","bindings":
[],"microtime":1727928835.092447}]},"stage":"local","message_level":null,"open_frame_index":null,"application_path":"\/var\/www\/html\/adbl-
backend","application_version":null,"tracking_uuid":"467fa400-8b4b-49e2-8e8e-ca52aaf76666","handled":null},"config":
{"editor":"phpstorm","theme":"auto","hideSolutions":false,"remoteSitesPath":"\/var\/www\/html\/adbl-
backend","localSitesPath":"","enableShareButton":true,"enableRunnableSolut
...[SNIP]...
```

4.5.3. https://adblbackend.peacenepal.com/admin/reset_password

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:28:39 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
```

```
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032928

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

Request 2

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
```

Response 2

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:28:39 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033008

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

4.6. Input returned in response (reflected)

There are 15 instances of this issue:

- /admin/account-type-category [title[1] parameter]
- /admin/atm-location [_token parameter]
- /admin/blog-category/create [URL path filename]
- /admin/blogs/create [URL path filename]
- /admin/contents [multiData[1][title] parameter]
- /admin/import/store-atm [Referer HTTP header]
- /admin/import/store-atm [User-Agent HTTP header]
- /admin/import/store-atm [name of an arbitrarily supplied URL parameter]
- /admin/import/store-branch [Referer HTTP header]
- /admin/import/store-branch [User-Agent HTTP header]
- /admin/import/store-branch [name of an arbitrarily supplied URL parameter]
- /admin/login [Referer HTTP header]
- /admin/reset_password [Referer HTTP header]
- /admin/reset_password [User-Agent HTTP header]
- /admin/reset_password [name of an arbitrarily supplied URL parameter]

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Vulnerability classifications

- CWE-20: Improper Input Validation
- CWE-116: Improper Encoding or Escaping of Output

4.6.1. https://adblbackend.peacenepal.com/admin/account-type-category [title[1] parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/account-type-category**

Issue detail

The value of the **title[1]** request parameter is copied into the application's response.

Request 1

```
POST /admin/account-type-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkRkNENHNUZVcTBwNWFjbjRZcXVCclE9PSIsInZhbHVlIjoiWmhWa1IxaW9QOThScnhENXFoRGxVOTNNVlA5NlRtOVlXaCt1a2d
PMHJlVHZlNy9TajJVNjlKQUdUeWJaVnhyelNmeDJ0akVOUmpmeEwrQ2J3aFVGd1BKSWg5SkF4eENSQk9XaXh0bHcwdEEySUdvQ0JoR2FXVjRVTFp6dlZRemoi
LCJtYWMiOiIyYzI4YmY5MDk4MzI1OWEyZDMxZGZmMGFmYmVjNThkYWM5ODNkMmQ0MDEzNjg2Mjk0ZmM0MWFmNGRjNjk5YjJjIiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type-category/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFbwkx8ZBjpyVvIsB
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1238

------WebKitFormBoundaryFbwkx8ZBjpyVvIsB
Content-Disposition: form-data; name="_token"

8ZKRrkGFa7pe8WTP5xG4gMFLO3ob4eTOtybEhs1U
------WebKitFormBoundaryFbwkx8ZBjpyVvIsB
Content-Disposition: form-data; name="title[1]"

t51uxqg9ej
------WebKitFormBoundaryFbwkx8ZBjpyVvIsB
Content-Disposition: form-data; name="excerpt[1]"


------WebKitFormBoundaryFbwkx8ZBjpyVvIsB
Content-Disposition: form-data; name="files"; filename=""

...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:51:07 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjkvWWNqMU00dzhSNXhWN2tPam5IekE9PSIsInZhbHVlIjoic1lFQkdjUURMMEtTQ0dkNnQrck9sZGJaSG01SktzeFJyMGlFSVRIR2
QrVkh6RWdBRllkWWQxYmdrUVZXM1InZDJnTVlLV3pxNEV5OFVVSFdvejdJQmlaRXUvZVQvdVNnUkpjVmJZR3RCV1o1bStrMVBSM3h5Smc1NzZZaHBNK3liLCJt
YWMiOiJmMGI2YTBhNGQ4YzQ3NmIyNWQ2OWQ0YTMzMjJhOTVhYjA2N2JlNmZkZmI3ODNhZGI1ZTViZmQ0N2RhNTcyM2YyliwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:51:07 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 104682

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

```
<td>t51uxqg9ej</td>
...[SNIP]...
```

4.6.2. https://adblbackend.peacenepal.com/admin/atm-location [_token parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/atm-location**

Issue detail

The value of the **_token** request parameter is copied into the application's response.

Request 1

```
POST /admin/atm-location HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlNsWWphK2V1RnlsS3IzU2wvdHhMSVE9PSIsInZhbHVlIjoiZVpYRUxNWFdjS0ZQMUpiQjJkR0pLQ05EbUhqOVo1eW5Uc1MrVlBF
WkYzVHV2UEIveDl4ODlMU2tjZkZpTFpiK1EvK0hEOUVnUjQyTGlVOVNKcUlSUWNtekdOa2o1QmhGNDdEUkw2ODdxUytOVHFCOFc1aUhhbUovQ2VLc0lsSG8iL
CJtYWMiOiIyN2IzMDgwOWRlNDg3NzQ4NmU5OTI5YTliZDJlYmNiZmE3ZGQ1Mzk1ZGQ4ZDk1MGEzMjk0YTFlODk5YWE1ZTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/atm-location/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1HZjSmazjk8SYT82
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1407

------WebKitFormBoundary1HZjSmazjk8SYT82
Content-Disposition: form-data; name="_token"

cE50UTXNxAEwjbImq7j0PeM50QCUMlL0y0psZipxhy5kc69zd9
------WebKitFormBoundary1HZjSmazjk8SYT82
Content-Disposition: form-data; name="title[1]"

952030
------WebKitFormBoundary1HZjSmazjk8SYT82
Content-Disposition: form-data; name="address[1]"

64
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:49:58 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJSODg0K09VcDhKaS9PT3cwV1ErU3c9PSIsInZhbHVlIjoiVUxRajdzTGdFVUw4ZFVuSmhWSUdCWmhLTExhMHJIMXVQSGp5YU
ZTQjdndWlZNmNCY3B5UzhRbTd0UERQZS93RjNpU24weVZROWdEemVZVStlRnAxUlZhcGFBYVphblV5cWMyTTZjT3F0eUd4RGVXOUFCTU81WjZPL2tjcU1oR
DYiLCJtYWMiOiIwMjlkMTQxNzYzNDYyYjg5NjNjYzJiYjhjYmViMGUzZjUzOTM1NThlMWQwMTIxMTkxZjJlNGM3NDIwNDhiZGIxIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 13:49:58 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 91241

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
```

```
...[SNIP]...
<input name="_token" type="hidden" value="cE50UTXNxAEwjbImq7j0PeM50QCUMlL0y0psZipxhy5kc69zd9">
...[SNIP]...
<input name="_token" type="hidden" value="cE50UTXNxAEwjbImq7j0PeM50QCUMlL0y0psZipxhy5kc69zd9">
...[SNIP]...
```

4.6.3. https://adblbackend.peacenepal.com/admin/blog-category/create [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blog-category/create**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

```
GET /admin/blog-category/createkg785f1gj5 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InFnclQ0NlRZVFBMRlRHakkwN2Q0MGc9PSIsInZhbHVlIjoia3R5d1pKNVFGYk8wd1IyM3dhUTRnYlFUUmZsdFMrSVljNHRsazEzS
U00QlNEQVMvakdUEE2RnpRWUlzeWdJbEdWMjRLa3RFZTBSb2cvd2Nld1ZnTUxXRUV5WWxEU3IxSU85YWp2VGU4V0MzZnQ1YlMrbVVvb2h4TlhqZFVVUnMi
LCJtYWMiOiI0ZTM2Mjk5Njk2YTBiMjk5ODdmYjhkMjkzOWNmMDEzZmY4MzY1NDQ2NjQ3NTMwNzFjMDI3YmFjOGNmMWE4OGE2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blog-category
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 02 Oct 2024 12:07:29 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjZraUdEUDJiUlZQM1I0eUVHc3M1NEE9PSIsInZhbHVlIjoiVWJJVFIjZlR1NndnaE9ESFZDSHlSYjhCTGlHRGtHY01pMytna3RpVWl
PQ2puZitVU2xDMVZoc1ZWRndDZVphUUN4aGRiVHpXRERUR2xHbkpna1p2WWtlT0RNTGhuRHZ0eURiUGJVVmdpanVrR2hreTlMeDNhZWgwRjhpc0cwRDQiLC
JtYWMiOiIyZDY0ODBiYzVjMmU3NWFiOGY1MDk0MTkyYTY0ZTk1MWUxNzMwZjJlZWIxMWM4ZjIzOWYzNTA4NDY0ZmM3MDQ1IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 14:07:29 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1162884

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
BadMethodCallException: Method App\Http\Controllers\Admin\BlogCategoryController::show does not exist. in file /var/www/html/adbl-backend/vendor/lara
...[SNIP]...
,"55":"$kernel->\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/blog-category\/createkg785f1gj5","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":[],"body"
...[SNIP]...
ndor-category":86,"projects":87,"interest-rates":88,"training":89,"training-hall":90,"training-hall-bookings":91}},"route":{"route":"admin.blog-
category.show","routeParameters":
{"blog_category":"createkg785f1gj5"},"controllerAction":"App\\Http\\Controllers\\Admin\\BlogCategoryController@show","middleware":
["web","preventBackHistory","auth:admin"]},"user":{"id":1,"admin_type_id":1,"first_name":"Superadmin","mi
...[SNIP]...
,"55":"$kernel->\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/blog-category\/createkg785f1gj5","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":[],"body"
...[SNIP]...
ndor-category":86,"projects":87,"interest-rates":88,"training":89,"training-hall":90,"training-hall-bookings":91}},"route":{"route":"admin.blog-
category.show","routeParameters":
{"blog_category":"createkg785f1gj5"},"controllerAction":"App\\Http\\Controllers\\Admin\\BlogCategoryController@show","middleware":
```

["web","preventBackHistory","auth:admin"]},"user":{"id":1,"admin_type_id":1,"first_name":"Superadmin","mi
...[SNIP]...

4.6.4. https://adblbackend.peacenepal.com/admin/blogs/create [URL path filename]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/blogs/create**

Issue detail

The value of the URL path filename is copied into the application's response.

Request 1

GET /admin/blogs/creates9xzaf3rdl HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkcxelpUNG5WZVlIclFmd0Jvb2UzTnc9PSIsInZhbHVlIjoicHV0cWtPYUhpYW52SVVLNlRxK0EvZ0tpSlNVMisvSnA2RDJnV0l0bEhLczZmc0J4V3JTRzhqU210N3MzZzFwaXVxQ1B3b1V0allSdmZWTUM3cHRBQ1psNnJKYjNoTXoyUVVDZTZXWHB4bHR2UXBWeEdHOHVxWFFEVjh5TzJlUlQiLCJtYWMiOiJlNWViYzc5ZTA3N2ViN2NjYTFmN2IzM2JjMjczNTIwZDZjYWY5OTdmNDE2M2NmOWQyMmM4MWI2YWQ1NmU2ZjgyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0

Response 1

HTTP/1.1 500 Internal Server Error
Date: Wed, 02 Oct 2024 12:07:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Ik82ZlVuZlFESTRsak9vbFpIS1ZlUUE9PSIsInZhbHVlIjoiaHFmTVNxazJ6UEt3MFVMNHdaeUQwbmZrblNselloZGc4anMyRzJCTCtsNUEybDhqK3RLcFJFc2pqWGwxOXhoWlo5MTFxT09xYzlKalhwb2ZhUzNjQ2JNcXFMc3lMZWtyL0FRS0o3M0EwclNVVHgxOUdhczNDeGVtNS80RVp1ZTMiLCJtYWMiOiI1YTc1NDljMjA5Y2IzNTJlYTBiNDIzMmU0NTI2MTc2NTMxNTgwZWNmOWFiMTI2MTZmZTA5YTEwODQyOGI4OWQwIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct 2024 14:07:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1164373

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
BadMethodCallException: Method App\Http\Controllers\Admin\BlogController::show does not exist. in file /var/www/html/adbl-backend/vendor/laravel/fram
...[SNIP]...
,"54":"","55":"$kernel->\u003Eterminate($request, $response);","56":""}],"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/blogs\/creates9xzaf3rdl","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":[],"body"
...[SNIP]...
A@burpcollaborator.net","fax":"697077","url":"http:\/\/burpcollaborator.net\/TSGNhDNz","lat":"976683","long":"792636"},"errors":{}},"route":
{"route":"admin.blogs.show","routeParameters":{"blog":"creates9xzaf3rdl"},"controllerAction":"App\\Http\\Controllers\\Admin\\BlogController@show","middleware":
["web","preventBackHistory","auth:admin"]},"user":{"id":1,"admin_type_id":1,"first_name":"Superadmin","middle_nam
...[SNIP]...
,"54":"","55":"$kernel->\u003Eterminate($request, $response);","56":""}],"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/blogs\/creates9xzaf3rdl","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":[],"body"
...[SNIP]...
A@burpcollaborator.net","fax":"697077","url":"http:\/\/burpcollaborator.net\/TSGNhDNz","lat":"976683","long":"792636"},"errors":{}},"route":
{"route":"admin.blogs.show","routeParameters":{"blog":"creates9xzaf3rdl"},"controllerAction":"App\\Http\\Controllers\\Admin\\BlogController@show","middleware":
["web","preventBackHistory","auth:admin"]},"user":{"id":1,"admin_type_id":1,"first_name":"Superadmin","middle_nam
...[SNIP]...

4.6.5. https://adblbackend.peacenepal.com/admin/contents [multiData[1][title] parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contents**

Issue detail

The value of the **multiData[1][title]** request parameter is copied into the application's response.

Request 1

```
POST /admin/contents HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlV4cVNWekhhTkV4WGNBQjNuL3BOcXc9PSIsInZhbHVlIjoiQ21zTVVFaGJNLzQzaThMYmhibld3NEFNMDBzY2l1SHRBaEt0dnBK
WlJPbllacjYzUk11bWtlMmhLMEROZjFiY2ZmemlLVkg2L1ZOaUtCT1hYQUlKajVtdnJ3eHhmcEI3MzA3cXh1QW5URzE5T0FybjhBeG9SM1IJL2xnZW5FZGMiLCJtYW
MiOiJiYzIzN2QxMTA3ZjE1NjI0YzRhZjQwMDBmMDNjMWI2OTk1MTFiNzAyMjQxMThlOWUyNThiYWFhMDJjZDIxM2I4IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPFTTPswROeAT4MRM
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1808

------WebKitFormBoundaryPFTTPswROeAT4MRM
Content-Disposition: form-data; name="_token"

10MBTIrTJmsYgA3g8vYlKPGQzQPREyA3M7CetkNV
------WebKitFormBoundaryPFTTPswROeAT4MRM
Content-Disposition: form-data; name="multiData[1][title]"

ixqyxy0ns3
------WebKitFormBoundaryPFTTPswROeAT4MRM
Content-Disposition: form-data; name="multiData[1][excerpt]"


------WebKitFormBoundaryPFTTPswROeAT4MRM
Content-Disposition: form-data; name="multiData[
...[SNIP]...
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 12:08:37 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlNzSzdOejh3Snl0d21ZMlJLSjRMclE9PSIsInZhbHVlIjoiMmlQQUdkdndndW12ZlArMnhkRXdOU1pOYnZKdnpuR1FFbEtKR3gyMnov
cFdQcXFjemV6VGpsQU5sS0dVazFiTkRDRE9lL09EMFlOcHlBMnNzVEVheXpwdVhJU2t2SndVMTJ5TVYzYzhueHBWWmFEbnVxT05GL0o5OTArRUlReU0iLCJtY
WMiOiJiMzQ3ZmNiMjIzZjVkMzM4YjU4YTBlOTNjNDU3NzExZTdjZTY0MTNjZDRkZmUwZWI5ZDQ2YWNkYjlhODVhYzhkIiwidGFnIjoiIn0%3D; expires=Wed, 02 Oct
2024 14:08:37 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 154652

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<td>ixqyxy0ns3</td>
```

```
...[SNIP]...
<td>ixqyxy0ns3</td>
...[SNIP]...
```

4.6.6. https://adblbackend.peacenepal.com/admin/import/store-atm [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The value of the **Referer** HTTP header is copied into the application's response.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/auzexpl8xf
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:10:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033040

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/auzexpl8xf"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
...[SNIP]...
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/auzexpl8xf"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
...[SNIP]...
```

4.6.7. https://adblbackend.peacenepal.com/admin/import/store-atm [User-Agent HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The value of the **User-Agent** HTTP header is copied into the application's response.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
```

```
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36kd5z7xlq5s
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:09:34 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032986

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
d.peacenepal.com\/admin\/import\/store-atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36kd5z7xlq5s"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36kd5z7xlq5s","connection":"close","cache-
control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
d.peacenepal.com\/admin\/import\/store-atm","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/108.0.5359.95 Safari\/537.36kd5z7xlq5s"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36kd5z7xlq5s","connection":"close","cache-
control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
```

4.6.8. https://adblbackend.peacenepal.com/admin/import/store-atm [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /admin/import/store-atm?w5np7kefgh=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:08:15 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033004

<!DOCTYPE html>
```

<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
:"","55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-atm?w5np7kefgh=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"w5np7kefgh":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...
:"","55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-atm?w5np7kefgh=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"w5np7kefgh":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...

4.6.9. https://adblbackend.peacenepal.com/admin/import/store-branch [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-branch**

Issue detail

The value of the **Referer** HTTP header is copied into the application's response.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/kcinuj4klz
```

Response 1


```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:12:14 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033062

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
**...[SNIP]...**
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/kcinuj4klz"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
**...[SNIP]...**
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/kcinuj4klz"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
**...[SNIP]...**
```

4.6.10. https://adblbackend.peacenepal.com/admin/import/store-branch [User-Agent HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**

Path: **/admin/import/store-branch**

Issue detail

The value of the **User-Agent** HTTP header is copied into the application's response.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.361yo2z888hf
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:10:57 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033012

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
eacenepal.com\/admin\/import\/store-branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.361yo2z888hf"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.361yo2z888hf","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
eacenepal.com\/admin\/import\/store-branch","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.361yo2z888hf"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.361yo2z888hf","connection":"close","cache-control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
```

4.6.11. https://adblbackend.peacenepal.com/admin/import/store-branch [name of an arbitrarily supplied URL parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/import/store-branch**

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /admin/import/store-branch?9je4a0fcqd=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:09:36 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033024

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
,"55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-branch?9je4a0fcqd=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"9je4a0fcqd":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...
,"55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/import\/store-branch?9je4a0fcqd=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"9je4a0fcqd":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...
```

4.6.12. https://adblbackend.peacenepal.com/admin/login [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/login**

Issue detail

The value of the **Referer** HTTP header is copied into the application's response.

Request 1

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdW
J6VW5GMFl3TklmajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHF
ML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3
D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: nfi67l3qsl
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 109

_token=psvOCIIjyWEguowk14Vu2U2PGcuDN0PvKSvaqYOv&email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/nfi67l3qsl
Set-Cookie:
adbl_backend_session=eyJpdiI6IlBqVUdWVlFtTGExS0hXd0pqK2ZmdFE9PSIsInZhbHVlIjoicUMvL2c2K3hzUTdtWU9zQm45TGhKYUNMK1lva0tPY0xSdUdqY3h1Y
U91N3g3YTlSRFlwdWVBa1htMkNIR3phaXlzMjRKQ25rWkVJMkpXRW8ybFVYdE5ldmovazJYVUQ5WHc2UW40MGtNYWx6RmJFK25iSld6dTl5MTBHeXFCc2wiLC
JtYWMiOiJiMDBiMDNlMTM4ODEyNTQwMzAxYTM1NjE1OTE4NjkzMDkwNzFmM2RiZGRiYmY4YTFkZjJiMWIyN2IzYmMzZDI3IiwidGFnIjoiIn0%3D; expires=Thu,
```

```
03 Oct 2024 06:22:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 426

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/nfi67l3qsl'" />

<title>Redirecting to https://adblbackend.peacenepal.com/nfi67l3qsl</title>
...[SNIP]...
<a href="https://adblbackend.peacenepal.com/nfi67l3qsl">https://adblbackend.peacenepal.com/nfi67l3qsl</a>
...[SNIP]...
```

4.6.13. https://adblbackend.peacenepal.com/admin/reset_password [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The value of the **Referer** HTTP header is copied into the application's response.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/9lwr5px04x
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:26:17 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033020

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/9lwr5px04x"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
...[SNIP]...
illa\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36","connection":"close","cache-
control":"max-age=0","referer":"https:\/\/example.com\/9lwr5px04x"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":true,"app_env":"local"},"dumps":[],"logs":[],"que
...[SNIP]...
```

4.6.14. https://adblbackend.peacenepal.com/admin/reset_password [User-Agent HTTP header]

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**

Path: **/admin/reset_password**

Issue detail

The value of the **User-Agent** HTTP header is copied into the application's response.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36wkn68her8p
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:24:50 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032968

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
kend.peacenepal.com\/admin\/reset_password","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML,
like Gecko) Chrome\/108.0.5359.95 Safari\/537.36wkn68her8p"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36wkn68her8p","connection":"close","cache-
control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
kend.peacenepal.com\/admin\/reset_password","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML,
like Gecko) Chrome\/108.0.5359.95 Safari\/537.36wkn68her8p"},"request_data":{"queryString":[],"body":[],"files":[]},"headers":
{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-agent":"Mozilla\/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36wkn68her8p","connection":"close","cache-
control":"max-age=0"},"cookies":[],"session":[],"env":
{"php_version":"8.2.21","laravel_version":"10.48.17","laravel_locale":"en","laravel_config_cached":false,"app_debug":
...[SNIP]...
```

4.6.15. https://adblbackend.peacenepal.com/admin/reset_password [name of an arbitrarily supplied URL parameter]

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://adblbackend.peacenepal.com**

Path: **/admin/reset_password**

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Request 1

```
GET /admin/reset_password?a72183quc3=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 04:23:27 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032986

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
54":"","55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/reset_password?a72183quc3=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"a72183quc3":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...
54":"","55":"$kernel-\u003Eterminate($request, $response);","56":""},"arguments":[],"application_frame":false}],"context":{"request":
{"url":"https:\/\/adblbackend.peacenepal.com\/admin\/reset_password?a72183quc3=1","ip":null,"method":"GET","useragent":"Mozilla\/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.5359.95 Safari\/537.36"},"request_data":{"queryString":{"a72183quc3":"1"},"body":[],"files":
[]},"headers":{"host":"adblbackend.peacenepal.com","accept-encoding":"gzip, deflate","accept":"*\/*","accept-language":"en-US;q=0.9,en;q=0.8","user-
agent":"Mozilla\/5.0 (Window
...[SNIP]...
```

4.7. Cross-domain Referer leakage

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/forex**

Issue detail

The page was loaded from a URL containing a query string:

- https://adblbackend.peacenepal.com/admin/forex

The response contains the following link to another domain:

- https://fonts.googleapis.com/css?family=Poppins:300,400,500,600,700

Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- Referer Policy
- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /admin/forex?date=2024-10-02 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkVxV0ErNXJNdWZtWklweGZoRit6bVE9PSIsInZhbHVlIjoicnlmMFNyb3JQVjZtczdiZWF0bHFQcHB2czdaMkVYSERZQ0k4NkV6NE
xTcVo3TGpsOFExb05yOXhjTVF2MVRicVY3MVNnUnpPY0gvUkhiY3ZJWUh5T2ttUEU0LzgvdWxLSTFtUWVBcm9XNERobnUrWWg3UUhPOXZQQXNTanU1MTEiL
CJtYWMiOiIzNWFjOTk5MGQ0ODc3MjkwZjIxOTVjM2UxY2FmYzJkODJmMGNlNjFiMGIxNTQ3NjU5MjA4NDcyMzkwMGRhODZjIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/forex?date=2024-10-02
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:07:16 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Im1VeXpuYVZ0MHo1THhUQUxJdzRoSGc9PSIsInZhbHVlIjoiYTJJV1R4cEVibVE4NFFlUEM1cnpiV1AxZzhMVDhjSUN1YU9hYm5F
R05HY1VFUldxMGV4TjJQMURTMGtGSm9ubUd3OHhrZmxFTFJoSGw4aytLa1BqOTlFR1FPTHBEamVnMDBwSHNLc2ZVSzVnTmZFZXowSVVrMW1IOXROOVlp
OXMiLCJtYWMiOiJmMDU1ZjljNjZjZTg3YmRjYjcwMTNiODI1ZTc5ZmE1OTlhYmE5YWQ1NDg5MDE2ZTUwYzg1ZWQ3OTYxNzU3NjAwIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:07:16 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 67900

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<link href="https://adblbackend.peacenepal.com/adbl/images/favicon.ico" type="image/jpg" rel="icon" sizes="32x32" />
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Poppins:300,400,500,600,700" />
<style>
...[SNIP]...
```

4.8. Cross-domain script include

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/layout**

Issue detail

The response dynamically includes the following script from another domain:

- https://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/jquery-ui.min.js

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Request 1


```
GET /admin/layout HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImFwQ01Kd3pHSE1EWUlYMXQvMXJjalE9PSIsInZhbHVlIjoiZlNBSDdVQXNIenZWSS9CRHl6OWRRVjZTeFk2UnFkMllmODIzajVra
ll6SXFNbUNvdFMxVzdaSUpyL2ZTQXB1bjNKNGczRVpvcWY3d1VTUG5lTWxyM2xHT1Y5WGJhSWd6L3VWZ0U3Ulk0cTVqTENiSitsTjdt0JhMTBma3ppTWliLCJt
YWMiOiJhMjU4ZGQyZGQwMjU1N2Y3ZWQ4Yjg2NjVhYjgwMTgwN2RlZGQwYmU5OGI0OTFlODU5OTIyOTllODYxMDUwZDdhIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```


Response 1


```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:55:59 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6Im5UWFllOHhXUmxFZ3ZBejZGTWFGeXc9PSIsInZhbHVlIjoic2Y2WmlCN2V4RUt2eVRYeTBMVGozaHc3K3VQYmhBc2JzWUN1Q
0RlL3N4T1JGaWRnOUpoQW10WmZPRkNIc3NvcUgyVHJjVklRdGJUMFI5NklDSUR4anFhaWU3UUFXYitYc1IySWoxK2tuVG90YjlEQTZiVlZqUGpiVlFkVjhIYTYiLC
JtYWMiOiI4ZDNhNDdkMmY2MzM0M2Y1YTY5NGU4NTZhZWIwZTIzY2JkNmVjNjQ1ZGRlYjRhMjZlMTIzNml1ZDA0OWE2MTMxIiwidGFnIjoiIn0%3D; expires=Wed,
02 Oct 2024 12:55:59 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 70330

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
</script>
<script src="https://ajax.googleapis.com/ajax/libs/jqueryui/1.10.3/jquery-ui.min.js"></script>
...[SNIP]...
```

4.9. File upload functionality

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin**

Issue detail

The page contains a form which is used to submit a user-supplied file to the following URL:

- https://adblbackend.peacenepal.com/admin/blogs

Note that Burp has not identified any specific security vulnerabilities with this functionality, and you should manually review it to determine whether any problems exist.This issue was found in multiple locations under the reported path.

Issue background

File upload functionality is commonly associated with a number of vulnerabilities, including:

- File path traversal
- Persistent cross-site scripting
- Placing of other client-executable code into the domain
- Transmission of viruses and other malware
- Denial of service

You should review file upload functionality to understand its purpose, and establish whether uploaded content is ever returned to other application users, either through their normal usage of the application or by being fed a specific link by an attacker.

Some factors to consider when evaluating the security impact of this functionality include:

- Whether uploaded content can subsequently be downloaded via a URL within the application.
- What Content-type and Content-disposition headers the application returns when the file's content is downloaded.
- Whether it is possible to place executable HTML/JavaScript into the file, which executes when the file's contents are viewed.
- Whether the application performs any filtering on the file extension or MIME type of the uploaded file.
- Whether it is possible to construct a hybrid file containing both executable and non-executable content, to bypass any content filters - for example, a file containing both a GIF image and a Java archive (known as a GIFAR file).
- What location is used to store uploaded content, and whether it is possible to supply a crafted filename to escape from this location.
- Whether archive formats such as ZIP are unpacked by the application.
- How the application handles attempts to upload very large files, or decompression bomb files.

Issue remediation

File upload functionality is not straightforward to implement securely. Some recommendations to consider in the design of this functionality include:

- Use a server-generated filename if storing uploaded files on disk.
- Inspect the content of uploaded files, and enforce a whitelist of accepted, non-executable content types. Additionally, enforce a blacklist of common executable formats, to hinder hybrid file attacks.
- Enforce a whitelist of accepted, non-executable file extensions.
- If uploaded files are downloaded by users, supply an accurate non-generic Content-Type header, the X-Content-Type-Options: nosniff header, and also a Content-Disposition header that specifies that browsers should handle the file as an attachment.
- Enforce a size limit on uploaded files (for defense-in-depth, this can be implemented both within application code and in the web server's configuration).
- Reject attempts to upload archive formats such as ZIP.

References

- Various proof-of-concept files
- An XSS polyglot attack

Vulnerability classifications

- CWE-434: Unrestricted Upload of File with Dangerous Type
- CAPEC-17: Using Malicious Files

Request 1

```
GET /admin/blogs/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkcxelpUNG5WZVllclFmd0Jvb2UzTnc9PSIsInZhbHVlIjoicHV0cWtPYUhpYW52SVVLNlRxK0EvZ0tpSlNVMisvSnA2RDJnV0l0bEhLc
zZmc0J4V3JTRzhqU210N3MzZzFwaXVxQ1B3b1V0allSdmZWTUM3cHRBQ1psNnJKYjNoTXoyUVVDZTZXWHB4bHR2UXBWeEdHOHVxWFFEVjh5TzJlUlQiLCJt
YWMiOiJlNWViYzc5ZTA3N2ViN2NjYTFmN2IzM2JjMjczNTIwZDZjYWY5OTdmNDE2M2NmOWQyMmM4MWI2YWQ1NmU2ZjgyIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/blogs
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:07:47 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
```

```
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImR6eGlRMXZxTW5iUXpNNndWRUE1MlE9PSIsInZhbHVlIjoicU9YblY1VFdzRVJLU3MyTitwelcyanRKS1NmQ3ZNTGJxOEVpd203
OHBidVA5bzFRbXZuNE8rU1Myc0xUYVB5VjJpY0YybnplQitZdGxBZWR0VXg3VFZnK1BnTFhYT0l4Z01iRWFaOS81TnBPOW9jaVZXZ2hONllGdGZDOUVNL0UiLC
JtYWMiOiJmOWUzMTU1NDMzNjgwYzNkNTQ3NWZlYzgxNzM4MmJmMzg3MTM0YTM0ZjhmZDVlMGRlZWNlOTBmOTIzZjQ4NjU0IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:07:47 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71863

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<div class="custom-file">
<input type="file" class="custom-file-input" name="image" id="image-file">
<label class="custom-file-label selected" for="image-file">
...[SNIP]...
```

Request 2

```
GET /admin/branch-directory/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlZHSHJrdXdBQjA5d2RMczdnSTdTYXc9PSIsInZhbHVlIjoiMW5YT0J5Mm83SCtDbGcwYUxtWmJXUXNBa2xUdE1DQlhmVFB5STl
JcWh1KzhjaFRETVZLV0VBaTJwTU5wbENzdTJlMnRWMXRoVkxxRi9EeGhZcnJ3WmNQcW9yWUgwTW1MRWIxekFTckg2TGJ0cFFKK1AycXpBdURVWnhnR0hE
NFMiLCJtYWMiOiI2ZDI1MjE4NzI1ZjM2ZTE1MzIwZDQ4YzhjNzcwOTQ2NDM1NjA0NjdkNTZmMzFiMjE1YzRhNWE4MmMyZGUwYzg1IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/branch-directory/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:33:09 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6ImswbWxSY0FINTgzbDNDcmlIb1Y2OGc9PSIsInZhbHVlIjoidnFIREk1R2lqTjhsSTYyZkJsaW5oK29FUDB5QzBOL1MrV3N4NDJJR
1hUV0UwSWZYVTFNNHYwLzU3RzNPSGx0dG5Nb0RhWkVGYUp1WS9TRS9zTmF3aE9aK1dYa09tVUxDUHg1TzZXMFFQYnYwazMrN1NoOWhhNUJDN1dwcjRI
NDAiLCJtYWMiOiJjMzcwYjJjMmNmMjRmZjA1NmNlNWI3ZTA4ZjE4MDYzNmRmMjJmNzcyNzYxMmM4ZmZkMzUwNjViNTA3NjA1MjJhIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:33:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 96007

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<div class="custom-file">
<input type="file" class="custom-file-input" name="photo" id="image-file">
<label class="custom-file-label selected" for="image-file">
...[SNIP]...
```

Request 3

```
GET /admin/contents/create HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
```

```
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkJvSVIwN3Y5YVJVRTdnNXlKSk1DTHc9PSIsInZhbHVlIjoiQmI0VFVhZFNXd1BHN1IlcGlEenNCbld2b2VETW5Zb255OTNzKytmakI
zWEg5TlhtQmVVNlg2elNQMmdQenNqQ015QmZRaG1ZTlB0eFQwYzROZ1B6NnluSkdhdXlsa0VKT0RUQTF3OHQ4ZTVGS0VBRHd6a2pJVmdxTlZDQ2dsVTQiLC
JtYWMiOiI1YzNiZTM3ZDc5Mzg4MDVlNGMyNTFhYjA5ZTc0ZjA4MzRlNjkyMTgwYjc1YzEyMDdmNzQwNTM3NzRhMGEyNTQ3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents/create
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:14:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjNlREdlbW5Yc0pUdW05SFdwS3VIbXc9PSIsInZhbHVlIjoiejRQQ1hvdW5adkt1TXpCYVlqZ1U4WmZYUEdyeXJHRTFwaXczMCtVY
VlmdU9KdUZ0M0dZWlZZclFlZFVodzlBT1VQcnJ1cTl0TzdEUGJEckVKZkxwd0RtalZLdEJFQ3NHSG9sZTFlblZ6ZnRjVURKZHhvYzJ3UkdwdFY2Mm5uWloiLCJtYW
MiOiJjYmE5NWI1OTQ1NTU1MmRhZTFlZDIzMGVhMDI4MDJhYmI3NGU3YjYxY2Y5ZWZkMWU4ZDI0ZDVlOTc3NTk2MTdkIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 13:14:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 76351

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<div class="custom-file">
<input type="file" class="custom-file-input" name="banner" id="banner-file">
<label class="custom-file-label selected" for="banner-file">
...[SNIP]...
```

4.10. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially

bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CAPEC-103: Clickjacking

Request 1

```
GET /admin/account-type-category HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IktERG1NMkpBa1VNQlJjRnNPVEk5SVE9PSIsInZhbHVlIjoiWFNobWNJOXROU1NwWG5UUkNuTG1jWnVSMWdPZ2tCMzE3NlFTbEpkQ2prWVVnNm5tZHMxazJvL0FtUTNGVmNPV25RdnAxR3ZpMlpJMCszeW1RODlqQkR1eW9aVzhiZHk2aW1aUm85NnhXUER2Yjg5d21IbFpyNGJ6OE9WQmhVQ3MiLCJtYWMiOiJmNjAxYjg5ODg2ZTFmZDgxMjE4ZWUzNWQ1NGIxYzkwYmQzODgyMmY3YjlmMjBiMjdhZWU2YTA2NjVhZThkZjM2IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:52:41 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlJMV2ZSZVJCZXVVaDJHRVQ3UVdGTmc9PSIsInZhbHVlIjoiT3pQeWhJVWU2OWFlNzdTNkJNclJaRlAyYmdham9mVDVwMlprdDF5WGRCdTNRaUNSK0JLYWFlVFRpZVo3OElHRHlPMU8wdzFMbExJdHhvT21UNFNrVUJKNk5nMGx0R1lGRkVPMXZkVHBGSXlvQUNOU1BTdUNlSFpuWkRGK2FkK3oiLCJtYWMiOiJiMmQ4ZjViODQzMzUxOTEwYjJjZmM2YjYxZjI1MDM0MDM4NDI5NTAwMzI1ODU5NTYxM2MzM2JiMDhhMmY0MWQyIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:52:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 91873

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Request 2

```
GET /admin/admin-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IlplK054czJobzdRR25oTjlhYWRjVkE9PSIsInZhbHVlIjoiczUvSHJNV0p2NjM0bDNsdG5POExPQm53UGM2SHkrL3cyaE1oT3RYZXNMNHdmRGwwc08xRGpVeVFxK2Fya1g4amdnSWdxajJrRVVXaXJxQXdyUktBUWt5WktMaGkzV1NlRWYrWkE3cjh3T3VWc0pKRjRLVDczc1FzaEJLeGdmYkQiLCJtYWMiOiI0M2QyODZiMjY0YTBjYTc3NzA2ZmEwY2FkYTA5MTYxNzVlNTM1YWU3ZjcwZjQyM2M4YTc2ZThkMmI3ZGE1NzY3IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:56:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlVBSmJqNGRENjlISENObIF4aDZZSmc9PSIsInZhbHVlIjoiWGY4QVF1dFplQUEwZGRFWExVUEtSK3NSbk9HU1InbmlyRyt3NU5ic
zNkUGlTTUQ0SjV3b1hZRHQ3Slc5b2ZtZFFuUStMODB0M0RjU0daRUVSeUVPQXdNK2l0bUplK0oyOUljKy9HVGtiVUE5MzJwci9IT1o3U0phRjNNY05IWmwiLCJtY
WMiOiI5YzEwZWNmZGM0MmI0YThlNGE4MjAyZmI5YjQzNWJlYzc4ODNiOWRkZTZhYTA1YWY3YjcwMWVhZGZhYjJiMDAzIiwidGFnIjoiIn0%3D; expires=Wed, 02
Oct 2024 12:56:11 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 73707

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

Request 3

```
GET /admin/atm-location HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InEzdmc1bkxSRUU0RkVXUVpnUFZmM1E9PSIsInZhbHVlIjoiMnB6THVkRlJ2VzV3M3l0VGRmdE5tSzZXRUwxSmh3VGhXMTNGR
jBMaG1mN25QQzV4ejJ1SkpsMlVIZUl3R2UweERQY2wxQ1FtOWRmUlY0OFpZbTR4cUtla091L3lIR2RKZmFVangxVUV3TjV5ZXNOWC9oeXBFcjRyUTFFQVNyZW
UiLCJtYWMiOiIyYjI2MDBlODIyNTllYTI2MDM2ZjUwZWIyMDNhNGRhMmEyNGM0YzZmYjlmNDkyODRhYmE5YTFkODhlNmE3NTQxIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:53:01 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InZrZGdjUlBKZEpBMEVsSDM2UFFsZ2c9PSIsInZhbHVlIjoiR1dPVWR6SElFREpkU1h0d0xIUXlpWWkxL3pZVlNEeGFKRWhKcU4z
T1hlUnc2UnJqSC9DZFpjMUgrV3R0bEM0U3JmdFl5SnRqbUhQZWpsam11RUQydVZHNE02TGpSZ0xPZlp2NWppQU9uKzVNb1pDL09yWk1seGZLYkJseUFlalliLC
JtYWMiOiIzYTkyYWIxMjBiYTY2NzQwYWIxM2JjZjRmMDAxNjY0OWE1OTgyODNmMzRlZmU2NzNjOWVmNTc2NWZjNTFkMTcwIiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:53:01 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 78545

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
```

4.11. Link manipulation (reflected)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/login**

Issue detail

The value of the **Referer** HTTP header is copied into the response within the path of a URL.

The payload **nfi67l3qsl** was submitted in the Referer HTTP header. This input was echoed unmodified within the response header **Location**.

This proof-of-concept attack demonstrates that it is possible to modify the URL to reference an arbitrary path. It is also possible to control the query string of the URL to perform HTTP client-side parameter pollution attacks.

Issue background

Link manipulation occurs when an application embeds user input into the path or domain of URLs that appear within application responses. An attacker can use this vulnerability to construct a link that, if visited by another application user, will modify the target of URLs within the response. It may be possible to leverage this to perform various attacks, such as:

- Manipulating the path of an on-site link that has sensitive parameters in the URL. If the response from the modified path contains references to off-site resources, then the sensitive data might be leaked to external domains via the Referer header.
- Manipulating the URL targeted by a form action, making the form submission have unintended side effects.
- Manipulating the URL used by a CSS import statement to point to an attacker-uploaded file, resulting in CSS injection.
- Injecting on-site links containing XSS exploits, thereby bypassing browser anti-XSS defenses, since those defenses typically do not operate on on-site links.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

Issue remediation

Consider using a whitelist to restrict user input to safe values. Please note that in some situations this issue will have no security impact, meaning no remediation is necessary.

References

- Using path manipulation to hijack Flickr accounts

Vulnerability classifications

- CWE-73: External Control of File Name or Path
- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

Request 1

```
POST /admin/login HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ik9ZdmFLRy9sYTRGM2pGbDNvS1FQUXc9PSIsInZhbHVlIjoid1FBekxjSFVkVDJLUzUrdWJsSEFZLzdHMElxQ3BWK1MzYndOdWJ6VW5GMFl3TklmajBFLzQ1TmVQUlJSZFU3dDBwdXV4UmNmbC85a0wveURpRGR3YmNGcHF0K25PaFFBcWpFZ3F6VmhzNmJJVkJWcG9vb0ZEUzBZaVJlTHFML1UiLCJtYWMiOiI1OWFkNWUwMDFkOTgyNmQ3Y2QxMGFiMTMzMDdhNjM4NGE0NWJhZGQwOGU1YmY3NjA2YzU3MjYzMDE2NjczYTM2IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: nfi67l3qsl
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 109

_token=psvOCIIjyWEguowk14Vu2U2PGcuDN0PvKSvaqYOv&email=PkmVKMdB%40burpcollaborator.net&password=h1T%21e7y%21C7
```

Response 1

```
HTTP/1.1 302 Found
Date: Thu, 03 Oct 2024 04:22:25 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
```

```
Cache-Control: no-cache, private
Location: https://adblbackend.peacenepal.com/nfi67l3qsl
Set-Cookie:
adbl_backend_session=eyJpdiI6IlBqVUdWVlFtTGExS0hXd0pqK2ZmdFE9PSIsInZhbHVlIjoicUMvL2c2K3hzUTdtWU9zQm45TGhKYUNMK1Iva0tPY0xSdUdqY3h1Y
U91N3g3YTlSRFlwdWVBa1htMkNIR3phaXIzMjRKQ25rWkVJMkpXRW8ybFVYdE5ldmovazJYVUQ5WHc2UW40MGtNYWx6RmJFK25iSld6dTl5MTBHeXFCc2wiLC
JtYWMiOiJiMDBiMDNlMTM4ODEyNTQwMzAxYTM1NjE1OTE4NjkzMDkwNzFmM2RiZGRiYmY4YTFkZjJiMWIyN2IzYmMzZDI3IiwidGFnIjoiIn0%3D; expires=Thu,
03 Oct 2024 06:22:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 426

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/nfi67l3qsl'" />

<title>Redirecting to
...[SNIP]...
```

4.12. DOM data manipulation (reflected DOM-based)

There are 9 instances of this issue:

- /admin/import/store-atm [Referer HTTP header]
- /admin/import/store-atm [name of an arbitrarily supplied URL parameter]
- /admin/import/store-atm [name of an arbitrarily supplied URL parameter]
- /admin/import/store-branch [Referer HTTP header]
- /admin/import/store-branch [name of an arbitrarily supplied URL parameter]
- /admin/import/store-branch [name of an arbitrarily supplied URL parameter]
- /admin/reset_password [Referer HTTP header]
- /admin/reset_password [name of an arbitrarily supplied URL parameter]
- /admin/reset_password [name of an arbitrarily supplied URL parameter]

Issue background

Reflected DOM-based vulnerabilities arise when data is copied from a request and echoed into the application's immediate response within a part of the DOM that is then processed in an unsafe way by a client-side script. An attacker can leverage the reflection to control a part of the response (for example, a JavaScript string) that can be used to trigger the DOM-based vulnerability.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Issue remediation

The most effective way to avoid DOM-based DOM data manipulation vulnerabilities is not to dynamically write to DOM data fields any data that originated from any untrusted source. If the desired functionality of the application means that this behavior is unavoidable, then defenses must be implemented within the client-side code to prevent malicious data from being stored. In general, this is best achieved by using a whitelist of permitted values.

References

- Web Security Academy: DOM data manipulation

Vulnerability classifications

- CWE-20: Improper Input Validation
- CAPEC-153: Input Data Manipulation

4.12.1. https://adblbackend.peacenepal.com/admin/import/store-atm [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **02y37qzlfz** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-atm HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/02y37qzlfz
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:10 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033040

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
```

Dynamic analysis

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **02y37qzlfz** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://example.com/w24xvcmq04
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:261807)
```

```
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm:124:12
```

4.12.2. https://adblbackend.peacenepal.com/admin/import/store-atm [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **g1jfv7jzgs** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-atm?g1jfv7jzgs=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033006

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...
```

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **g1jfv7jzgs** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://adblbackend.peacenepal.com/admin/import/store-atm?vfapg1ftfg=1
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:77449)
```

```
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:124:12
```

4.12.3. https://adblbackend.peacenepal.com/admin/import/store-atm [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-atm**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **g1jfv7jzgs** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-atm?g1jfv7jzgs=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

Content-Length: 1033006

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-atm. Supported met
...[SNIP]...

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **g1jfv7jzgs** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
f3b53azqos
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-atm?g1jfv7jzgs=1:124:12
```

4.12.4. https://adblbackend.peacenepal.com/admin/import/store-branch [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-branch**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **aamg5xamp7** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-branch HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/aamg5xamp7
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:11 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033062

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
```

Dynamic analysis

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **aamg5xamp7** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://example.com/elrk8fk1l7
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:261807)
```

```
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch:124:12
```

4.12.5. https://adblbackend.peacenepal.com/admin/import/store-branch [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-branch**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **w5ct9i0wre** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-branch?w5ct9i0wre=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033026

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...
```

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **w5ct9i0wre** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://adblbackend.peacenepal.com/admin/import/store-branch?pk27uavr1t=1
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:77449)
```

```
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:124:12
```

4.12.6. https://adblbackend.peacenepal.com/admin/import/store-branch [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/import/store-branch**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **w5ct9i0wre** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/import/store-branch?w5ct9i0wre=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

Content-Length: 1033026

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/import/store-branch. Supported
...[SNIP]...

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **w5ct9i0wre** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
uyzvqpo6sj
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:77449)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232770
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:232948
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:284067)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:119:420531)
at https://adblbackend.peacenepal.com/admin/import/store-branch?w5ct9i0wre=1:124:12
```

4.12.7. https://adblbackend.peacenepal.com/admin/reset_password [Referer HTTP header]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **u8xd3rw6mf** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/reset_password HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://example.com/u8xd3rw6mf
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:10 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1033018

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

Dynamic analysis

The value of the **Referer** HTTP header is copied into a JavaScript string literal. The payload **u8xd3rw6mf** was submitted in the Referer HTTP header.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://example.com/eesbtviz74
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password:114:77449)
at https://adblbackend.peacenepal.com/admin/reset_password:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/reset_password:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password:114:77449)
at https://adblbackend.peacenepal.com/admin/reset_password:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password:114:261807)
```

```
at lh (https://adblbackend.peacenepal.com/admin/reset_password:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password:124:12
```

4.12.8. https://adblbackend.peacenepal.com/admin/reset_password [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **kpj6wknxbx** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/reset_password?kpj6wknxbx=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1032986

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...
```

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **kpj6wknxbx** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
https://adblbackend.peacenepal.com/admin/reset_password?q7zis8kur7=1
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:77449)
```

```
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLSpanElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:77449)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:124:12
```

4.12.9. https://adblbackend.peacenepal.com/admin/reset_password [name of an arbitrarily supplied URL parameter]

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/reset_password**

Issue detail

The application may be vulnerable to reflected DOM-based DOM data manipulation.

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **kpj6wknxbx** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

Request 1

```
GET /admin/reset_password?kpj6wknxbx=1 HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 405 Method Not Allowed
Date: Thu, 03 Oct 2024 05:15:06 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
allow: POST
Cache-Control: no-cache, private
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
```

Content-Length: 1032986

<!DOCTYPE html>
<html lang="en" class="auto">
<!--
Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException: The GET method is not supported for route admin/reset_password. Supported metho
...[SNIP]...

Dynamic analysis

The name of an arbitrarily supplied URL parameter is copied into a JavaScript string literal. The payload **kpj6wknxbx** was submitted in the name of an arbitrarily supplied URL parameter.

The string containing the payload is then passed to **element.textContent**.

The previous value reached the sink as:

```
e57e13zsd0
```

The stack trace at the source was:

```
at Object.nnqvX (<anonymous>:1:52127)
at _0x5e555e (<anonymous>:1:265367)
at Object.izdMQ (<anonymous>:1:600060)
at HTMLElement.set [as textContent] (<anonymous>:1:618185)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:77449)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:124:12
```

The stack trace at the sink was:

```
at Object.pHgWq (<anonymous>:1:116374)
at Object.HLwEK (<anonymous>:1:600385)
at HTMLElement.set [as textContent] (<anonymous>:1:618382)
at Bt (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:77449)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232770
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:232948
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233348
at Tp (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:233364)
at fh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262141)
at uh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:262001)
at sh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261807)
at lh (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:261573)
at Xm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:259884)
at Vm (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:256829)
at wg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:284067)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289337
at Km (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:260264)
at Kg (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:289323)
at t.render (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:114:296404)
at window.ignite (https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:119:420531)
at https://adblbackend.peacenepal.com/admin/reset_password?kpj6wknxbx=1:124:12
```

4.13. Email addresses disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/admin/contact**

Issue detail

The following email addresses were disclosed in the response:

- test@yopmail.com
- dd@dd.com
- wewewe@hh.com
- legaciryk@ff.com
- legaciryk@mailinator.com
- nrupenz@gmail.com
- aaaaaa@bbbb.com
- dfg@gmail.com
- zxzx@ff.com
- testt@gmail.cc
- ads@gmail.com
- abc@gmail.com
- qodyka@mailinator.com
- newtest@gg.com
- test@test.om
- info@adbl.gov.np
- asd@gmail.com
- test@gmail.com
- taman.neupane@gmail.com
- mhr.dipesh.2022@gmail.com

Numerous email addresses were found to be disclosed and the above are a sample subset.

This issue was found in multiple locations under the reported path.

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /admin/contact HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVyR2c0NHAzbjRCa3lVcE5WbnV3NkE9PSIsInZhbHVlIjoiemR5MW9KL3IxNzNodmFheUkvaERKdTlCUE5ja3lXbTVhelZnY1ovRHVVTGo5VE1VU1IxdHlkWmR5Y2JGRThtNTByMEtMREovNWtZbytmTjFSKzBBL21YS1puY3VXWTh0YXlFWnE1cDB0dDVycm1IR25pQWp0UDdtOXM4SE8wbW4iLCJtYWMiOiI0MmIwYmU0NGE5NjEwN2Y0N2ViMzc0NWJkYTQwODIzZjUyNGYyNTE1MjJmMjE0YTA0MTY1MGM5Yzg0ZGE3NjJiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:55:14 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IngyNjNKaFhGcUxwUWhxd09WWWZjTEE9PSIsInZhbHVlIjoiZnBvZWowTEppc3RMR1BiQ3ZaY24zUVdXY1cwWUYzWFhLT1dTWDBDYzV0Z0E1eTFJcjJUWGZ6Q0Jka2txQzZBME9YYm1EZExaanlXNXZNVnRNMlBOaHVtY2JkSEg2Szl1QlM4eEM2T0k5dnV3cXZtQ25VK1BUQ0ZGeXJzM0t4R2MiLCJtYWMiOiI3YThhNmViM2UyOGIwNTFmYmIyODk4NjJkODI3NzQyMTZiOGI4NWMzMDFlZTQwZTFhMDRmYzliOTE1YWFlZGU3IiwidGFnIjoiIn0%3D;
```

```
expires=Wed, 02 Oct 2024 12:55:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 170263

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<td>test@yopmail.com</td>
...[SNIP]...
<td>test@yopmail.com</td>
...[SNIP]...
```

Request 2

```
GET /admin/contact HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVyR2c0NHAzbjRCa3lVcE5WbnV3NkE9PSIsInZhbHVlIjoiemR5MW9KL3IxNzNodmFheUkvaERKdTlCUE5ja3lXbTVhelZnY1ovRH
VVTGo5VE1VU1IxdHlkWmR5Y2JGRThtNTByMEtMREovNWtZbytmTjFSKzBBL21YS1puY3VXWTh0YXlFWnE1cDB0dDVycm1IR25pQWp0UDdtOXM4SE8wbW4iL
CJtYWMiOiI0MmIwYmU0NGE5NjEwN2Y0N2ViMzc0NWJkYTQwODIzZjUyNGYyNTE1MjJmMjE0YTA0MTY1MGM5Yzg0ZGE3NjJiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 2

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:55:14 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IngyNjNKaFhGcUxwUWhxd09WWWZjTEE9PSIsInZhbHVlIjoiZnBvZWowTEppc3RMR1BiQ3ZaY24zUVdXY1cwWUYzWFhLT1dTW
DBDYzV0Z0E1eTFJcjJUWGZ6Q0Jka2txQzZBME9YYm1EZExaanlXNXZNVnRNMlBOaHVtY2JkSEg2Szl1QlM4eEM2T0k5dnV3cXZtQ25VK1BUQ0ZGeXJzM0t4R2
MiLCJtYWMiOiI3YThhNmViM2UyOGIwNTFmYmIyODk4NjJkODI3NzQyMTZiOGI4NWMzMDFlZTQwZTFhMDRmYzliOTE1YWFlZGU3IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:55:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 170263

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<td>dd@dd.com</td>
...[SNIP]...
```

Request 3

```
GET /admin/contact HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6InVyR2c0NHAzbjRCa3lVcE5WbnV3NkE9PSIsInZhbHVlIjoiemR5MW9KL3IxNzNodmFheUkvaERKdTlCUE5ja3lXbTVhelZnY1ovRH
```

```
VVTGo5VE1VU1IxdHlkWmR5Y2JGRThtNTByMEtMREovNWtZbytmTjFSKzBBL21YS1puY3VXWTh0YXlFWnE1cDB0dDVycm1IR25pQWp0UDdtOXM4SE8wbW4iL
CJtYWMiOiI0MmIwYmU0NGE5NjEwN2Y0N2ViMzc0NWJkYTQwODIzZjUyNGYyNTE1MjJmMjE0YTA0MTY1MGM5Yzg0ZGE3NjJiIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/contents
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
```

Response 3

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:55:14 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IngyNjNKaFhGcUxwUWhxd09WWWZjTEE9PSIsInZhbHVlIjoiZnBvZWowTEppc3RMR1BiQ3ZaY24zUVdXY1cwWUYzWFhLT1dTW
DBDYzV0Z0E1eTFJcjJUWGZ6Q0Jka2txQzZBME9YYm1EZExaanlXNXZNVnRNMlBOaHVtY2JkSEg2Szl1QlM4eEM2T0k5dnV3cXZtQ25VK1BUQ0ZGeXJzM0t4R2
MiLCJtYWMiOiI3YThhNmViM2UyOGIwNTFmYmIyODk4NjJkODI3NzQyMTZiOGI4NWMzMDFlZTQwZTFhMDRmYzliOTE1YWFlZGU3IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 12:55:15 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 170263

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">

...[SNIP]...
<td>wewewe@hh.com</td>
...[SNIP]...
```

4.14. Credit card numbers disclosed

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/backend/js/plugins.bundle.js**

Issue detail

The following credit card number was disclosed in the response:

- 4394113113123

Issue background

Applications sometimes disclose sensitive financial information such as credit card numbers. Responses containing credit card numbers may not represent any security vulnerability - for example, a number may belong to the logged-in user to whom it is displayed. If a credit card number is identified during a security assessment it should be verified, then application logic reviewed to identify whether its disclosure within the application is necessary and appropriate.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-388: Error Handling
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
GET /backend/js/plugins.bundle.js HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
```

```
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkFCRUpRNFpRU1FhNjV5R0VZQVpiMWc9PSIsInZhbHVlIjoiSGZlSVVZeVZvY3ZrdUVCZzZCeSs0UEhFOGloMWtzaGk5aGRTUD
BwN0svNHZQZXpSL2hJM2tvV0QyTEJNeFcxTXFKeFJCS2luV3lLeDlJcTQ4RjVna0dvWUlGdGZOQ2FuT3FNUDYrdEFJYkJVc01LVUc3VjN4aGNTZnh4emVIeUYiL
CJtYWMiOiJmOTQyNGUwNTE0OGJhOWQzNzQ1YmIxMDllYWZmMGUxNDE3NjI3ZDJjMTg2OGMzYjE4ZjA0YmY1ZTI4YjNhNWYxliwidGFnIjoiIn0%3D
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: Windows
Referer: https://adblbackend.peacenepal.com/admin/login
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:51:59 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "3d18e1-615a622fafb77-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/javascript
Content-Length: 4004065

/*!
* jQuery JavaScript Library v3.4.1
* https://jquery.com/
*
* Includes Sizzle.js
* https://sizzlejs.com/
*
* Copyright JS Foundation and other contributors
* Released under the MIT license

...[SNIP]...
<polygon points=\"4 11.439 4 11 3 11 3 12 3.755 12 4 11.439\">
...[SNIP]...
```

4.15. Robots.txt file

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/robots.txt**

Issue detail

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the web site that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may therefore help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas, and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

Vulnerability classifications

- CWE-200: Information Exposure

Request 1

```
GET /robots.txt HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2024 04:04:17 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "18-615a622fc4398"
Accept-Ranges: bytes
Content-Length: 24
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/plain

User-agent: *
Disallow:
```

4.16. Cacheable HTTPS response

There are 2 instances of this issue:

- /backend/images/login.svg
- /robots.txt

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

4.16.1. https://adblbackend.peacenepal.com/backend/images/login.svg

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/backend/images/login.svg**

Request 1

```
GET /backend/images/login.svg HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6IkFCRUpRNFpRU1FhNjV5R0VZQVpiMWc9PSIsInZhbHVlIjoiSGZISVVZeVZvY3ZrdUVCZzZCeSs0UEhFOGloMWtzaGk5aGRTUDBwN0svNHZQZXpSL2hJM2tvV0QyTEJNeFcxTXFKeFJCS2luV3lLeDlJcTQ4RjVna0dvWUlGdGZOQ2FuT3FNUDYrdEFJYkJVc01LVUc3VjN4aGNTZnh4emVIeUYiL
```

```
CJtYWMiOiJmOTQyNGUwNTE0OGJhOWQzNzQ1YmIxMDllYWZmMGUxNDE3NjI3ZDJjMTg2OGMzYjE4ZjA0YmY1ZTI4YjNhNWYxliwidGFnIjoiIn0%3D
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Mobile: ?0
Sec-CH-UA-Platform: Windows
Referer: https://adblbackend.peacenepal.com/admin/login
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 10:52:00 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "1e303-615a622faad56"
Accept-Ranges: bytes
Content-Length: 123651
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: image/svg+xml

<?xml version="1.0" encoding="UTF-8"?>
<svg width="747px" height="547px" viewBox="0 0 747 547" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
<title>l
...[SNIP]...
```

4.16.2. https://adblbackend.peacenepal.com/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/robots.txt**

Request 1

```
GET /robots.txt HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Response 1

```
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2024 11:56:38 GMT
Server: Apache
Last-Modified: Tue, 09 Apr 2024 08:59:15 GMT
ETag: "18-615a622fc4398"
Accept-Ranges: bytes
Content-Length: 24
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/plain

User-agent: *
Disallow:
```

4.17. Base64-encoded data in parameter

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/**

Issue detail

The following parameter appears to contain Base64-encoded data:

- **adbl_backend_session = {"iv":"myAEYeg8E8nv4j5DcRHAug==","value":"CcBON6DjYtsJN3Aahidb6JlpQA37oB7PhbgX+SEeEWbplJb0e99M3WeBc0Ah0xfnGcm8tdqGso2R38ynpxYtQh3iLhRlXzUbK0uBCIdHPWaTwR88WdSGddLtIc20bBAy","mac":"d20ddd3e682300f982ac803abbb118bef937253f426207432967aea27ed495a9","tag":""}**

This issue was found in multiple locations under the reported path.

Issue background

Applications sometimes Base64-encode parameters in an attempt to obfuscate them from users or facilitate transport of binary data. The presence of Base64-encoded data may indicate security-sensitive information or functionality that is worthy of further investigation. The data should be reviewed to determine whether it contains any interesting information, or provides any additional entry points for malicious input.

Vulnerability classifications

- CWE-310: Cryptographic Issues
- CWE-311: Missing Encryption of Sensitive Data
- CAPEC-37: Retrieve Embedded Sensitive Data

Request 1

```
POST /admin/banner HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Im15QUVZZWc4RThudjRqNURjUkhBdWc9PSIsInZhbHVlIjoiQ2NCT042RGpZdHNKTjNBYWhpZGI2SmxwUUEzN29CN1BoYmdY
K1NFZUVXYnBsSmlwZTk5TTNXZUJjMEFoMHhmbkdjbTh0ZHFHc28yUjM4eW5weFl0UWgzaUxoUmxYelViSzB1QkNsZEhQV2FUd1I4OFdkU0dkZEx0bGMyMGJC
QXkiLCJtYWMiOiJkMjBkZGQzZTY4MjMwMGY5ODJhYzgwM2FiYmIxMThiZWY5MzcyNTNmNDI2MjA3NDMyOTY3YWVhMjdlZDQ5NWE5IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/banner/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLyJSSzR42azygqKF
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1443

------WebKitFormBoundaryLyJSSzR42azygqKF
Content-Disposition: form-data; name="_token"

FnGiYUsubSQkMB6Hqxcwd6tZInBGpJJw716LlqH8
------WebKitFormBoundaryLyJSSzR42azygqKF
Content-Disposition: form
...[SNIP]...
```

Response 1

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:18:26 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/banner/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IjNMMWJxNzAxZkx5WWFiUW9jZzNDeEE9PSIsInZhbHVlIjoieFpseHI3NEVPbnliMzROYW1VWThpRThnM2VyTW5YZjRhcEdhaS8
vc2M5NDN6eEpIaW83MzlrdjFodWt4U1VZSTEzOFN3eTJUME1rV0JXWm5LZzJ5ZTF5MnlHREs1a0QzZldaR1hZZGV2WWhYa1V2aTU1dGFkVWtwMjdRRG5wMX
EiLCJtYWMiOiJhMGZmYjE5ODMwY2YyMzFlZTM0ZDEzMWYwNTRjMmVlODgzNGNiNGUyZjZhNzFjYjg2NzY5OTcyNDRhODBhZjMxliwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:18:26 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 462

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/banner/create'" />

<title>Redire
...[SNIP]...
```

Request 2

```
POST /admin/branch-directory HTTP/1.1
Host: adblbackend.peacenepal.com
```

```
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6ImNGMURTeFNnZmNmWVdIRzgwbDlKdUE9PSIsInZhbHVlIjoib0U5N2xuaGlGYmlkQUsvVi8zYkFVZlI0emdtYmN5N1Z5QWxNSlJuV2JoMDQ1K2pVNHpLRHQzYlc4NEIySkhIVW5leUhNT0xUN3ppVThnN2JYamRWSmlBYlZxZGlGZ3dhb2RMNHlYRFNoVjh2YmN3VGJhb2pvNmtWc1kyajNuK24iLCJtYWMiOiIzMzcyZDk4YzIxOWMyYWRlNzRjZWRjYWI3ZjQxYzAwYWQ5N2I4ZDRmMTQ0MDlhYWI3YTNiNDg4ZGMxMGU4OWM1IiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/branch-directory/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydXjrIYjvRWM9P9rv
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 2500

------WebKitFormBoundarydXjrIYjvRWM9P9rv
Content-Disposition: form-data; name="_token"

hM5czuLnDETA2crIbVOVQRL2gU8AtxvJSxKWrr22
------WebKitFormBoundarydXjrIYjvRWM9P9rv
Content-Disposition: form
...[SNIP]...
```

Response 2

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:33:09 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/branch-directory/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6IlZHSHJrdXdBQjA5d2RMczdnSTdTYXc9PSIsInZhbHVlIjoiMW5YT0J5Mm83SCtDbGcwYUxtWmJXUXNBa2xUdE1DQlhmVFB5STlJcWh1KzhjaFRETVZLV0VBaTJwTU5wbENzdTJlMnRWMXRoVkxxRi9EeGhZcnJ3WmNQcW9yWUgwTW1MRWIxekFTckg2TGJ0cFFKK1AycXpBdURVWnhnR0hENFMiLCJtYWMiOiI2ZDI1MjE4NzI1ZjM2ZTE1MzIwZDQ4YzhjNzcwOTQ2NDM1NjA0NjdkNTZmMzFiMjE1YzRhNWE4MmMyZGUwYzg1IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:33:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 502

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/branch-directory/create'" />

<ti
...[SNIP]...
```

Request 3

```
POST /admin/account-type HTTP/1.1
Host: adblbackend.peacenepal.com
Accept-Encoding: gzip, deflate
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=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
adbl_backend_session=eyJpdiI6Ii9Fa0I1elc2Mm80WjVVS01RZzA3MXc9PSIsInZhbHVlIjoiYnlEU2ZMajRNVi9jRCtGR1BYQ1ZTSktPUDRPQ1d4UGR2UjVLM0lXSlcySHlwYjB1RWtITUY1aUN0cFpkTXFKd25lQ2NPMXVxTXRZYUpOeW13Z1MzMldsb2dLY2czeUp1Y2NaUFp6cnJnNVN6Q2J6WUIxL0JKVE5wRUVaeGhNS0wiLCJtYWMiOiI4YjY1ZWE2YzQ3MDFlMmJhMWVjMTNhYmYzNTczMmZjYjZiMDgyYTk5YzNiYmE0MjM0Y2ZlMmY2YTQ5Y2MyNDhjIiwidGFnIjoiIn0%3D
Origin: https://adblbackend.peacenepal.com
Upgrade-Insecure-Requests: 1
Referer: https://adblbackend.peacenepal.com/admin/account-type/create
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCwkHzMMO62aUgNLr
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="108", "Chromium";v="108"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 4412

------WebKitFormBoundaryCwkHzMMO62aUgNLr
Content-Disposition: form-data; name="_token"

XHc3E9GxctiOaa5QQGzBXZusRV9Isy5hK1T1xw1M
------WebKitFormBoundaryCwkHzMMO62aUgNLr
Content-Disposition: form
...[SNIP]...
```

Response 3

```
HTTP/1.1 302 Found
Date: Wed, 02 Oct 2024 11:20:33 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, Authorization, X-Localization, apiKey
Cache-Control: max-age=0, must-revalidate, no-store, nocache, private
Location: https://adblbackend.peacenepal.com/admin/account-type/create
0: Pragma
1: no-cache
2: Expires
3: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
adbl_backend_session=eyJpdiI6InV4OTE5WVZTdkkxR2Z4NWdlV0kya3c9PSIsInZhbHVlIjoid0Q4OTZQNXE0dGpubXBiN0xtVkdpdVFqR1NzTkJaTnlBRGpNUlVHN
DFISitwbThMWGR5OFZnV050UlNSb0hmY2wxbzR3dEo3Tjk1aHFDN29Ra0tPT1JCdXEyVUxBRDVVclZhWkNYNGJWcjdDZXZoWWhGYlE3Mkx4amNrS2o0TFciL
CJtYWMiOiI5MmRmZDlmNWNjMjIwODUxNGViOTQ0MmEyMDg1MjY1MDYxMWZhOTQxYTlkMDE2NDYyZGU3ZDUzNmQxZWUxYTY0IiwidGFnIjoiIn0%3D;
expires=Wed, 02 Oct 2024 13:20:34 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Content-Security-Policy: frame-ancestors 'self' https://*.peacenepal.com;
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 486

<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8" />
<meta http-equiv="refresh" content="0;url='https://adblbackend.peacenepal.com/admin/account-type/create'" />

<title>
...[SNIP]...
```

4.18. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://adblbackend.peacenepal.com**
Path:	**/**

Issue detail

The server presented a valid, trusted TLS certificate. This issue is purely informational.

The server presented the following certificates:

Server certificate

Issued to:	adblbackend.peacenepal.com
Issued by:	R10
Valid from:	Thu Aug 08 11:27:21 NPT 2024
Valid to:	Wed Nov 06 11:27:20 NPT 2024

Certificate chain #1

Issued to:	R10
Issued by:	ISRG Root X1
Valid from:	Wed Mar 13 05:45:00 NPT 2024
Valid to:	Sat Mar 13 05:44:59 NPT 2027

Certificate chain #2

Issued to:	ISRG Root X1
Issued by:	ISRG Root X1
Valid from:	Thu Jun 04 16:49:38 NPT 2015
Valid to:	Mon Jun 04 16:49:38 NPT 2035

Issue background

TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.

It should be noted that various attacks exist against TLS in general, and in the context of HTTPS web connections in particular. It may be possible for a determined and suitably-positioned attacker to compromise TLS connections without user detection even when a valid TLS certificate is used.

References

- SSL/TLS Configuration Guide

Vulnerability classifications

- CWE-295: Improper Certificate Validation
- CWE-326: Inadequate Encryption Strength
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Report generated by Burp Suite web vulnerability scanner v2022.11.4, at Thu Oct 03 11:18:47 NPT 2024.