hexens × mintify

Jan.24

MINTIFY
BLACKBOX SECURITY REVIEW

CONTENTS

ABOUT HEXENS

Hexens is a cybersecurity company that strives to elevate the standards of security in Web 3.0, create a safer environment for users, and ensure mass Web 3.0 adoption.

Hexens has multiple top-notch auditing teams specialized in different fields of information security, showing extreme performance in the most challenging and technically complex tasks, including but not limited to: Infrastructure Audits, Zero Knowledge Proofs / Novel Cryptography, DeFi and NFTs. Hexens not only uses widely known methodologies and flows, but focuses on discovering and introducing new ones on a day-to-day basis.

In 2022, our team announced the closure of a $4.2 million seed round led by IOSG Ventures, the leading Web 3.0 venture capital. Other investors include Delta Blockchain Fund, Chapter One, Hash Capital, ImToken Ventures, Tenzor Capital, and angels from Polygon and other blockchain projects.

Since Hexens was founded in 2021, it has had an impressive track record and recognition in the industry: Mudit Gupta - CISO of Polygon Technology - the biggest EVM Ecosystem, joined the company advisory board after completing just a single cooperation iteration. Polygon Technology, 1inch, Lido, Hats Finance, Quickswap, Layerswap, 4K, RociFi, as well as dozens of DeFi protocols and bridges, have already become our customers and taken proactive measures towards protecting their assets.

METHODOLOGY

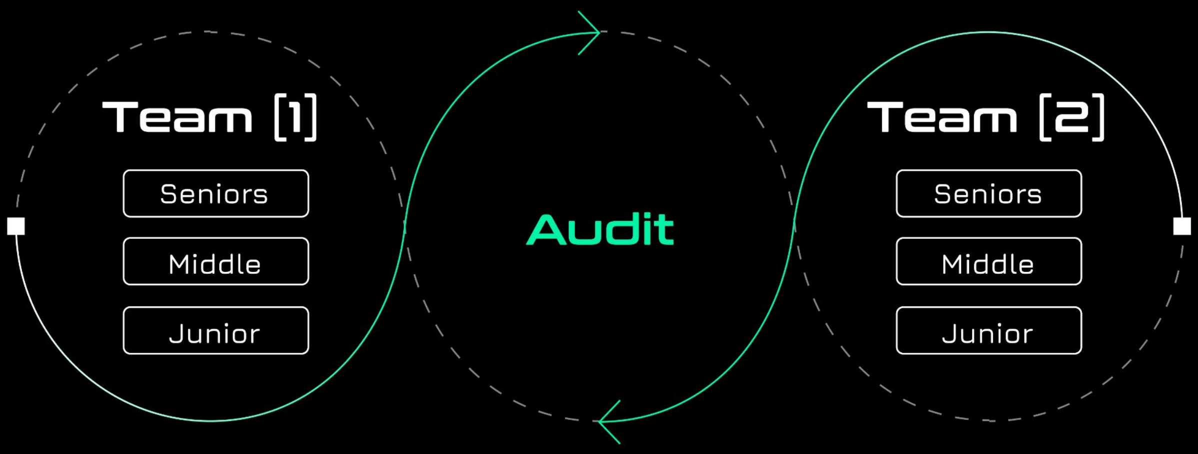
COMMON AUDIT PROCESS

Companies often assign just one engineer to one security assessment with no specified level. Despite the possible impeccable skills of the assigned engineer, it carries risks of the human factor that can affect the product's lifecycle.

Auditor*
Audit

HEXENS METHODOLOGY

Hexens methodology involves 2 teams, including multiple auditors of different seniority, with at least 5 security engineers. This unique cross-checking mechanism helps us provide the best quality in the market.



SEVERITY STRUCTURE

The vulnerability severity is calculated based on two components

- Impact of the vulnerability
- Probability of the vulnerability

IMPACT	PROBABILITY			
	Rare	Unlikely	Likely	Very Likely
Low / Info	Low / Info	Low / Info	Medium	Medium
Medium	Low / Info	Medium	Medium	High
High	Medium	Medium	High	Critical
Critical	Medium	High	Critical	Critical

SEVERITY CHARACTERISTICS

Vulnerabilities can range in severity and impact, and it's important to understand their level of severity in order to prioritize their resolution. Here are the different types of severity levels of vulnerabilities:

CRITICAL

Vulnerabilities with this level of severity can result in significant financial losses or reputational damage. They often allow an attacker to gain complete control of a contract, directly steal or freeze funds from the contract or users, or permanently block the functionality of a protocol. Examples include infinite mints and governance manipulation.

HIGH

Vulnerabilities with this level of severity can result in some financial losses or reputational damage. They often allow an attacker to directly steal yield from the contract or users, or temporarily freeze funds. Examples include inadequate access control integer overflow/underflow, or logic bugs.

MEDIUM

Vulnerabilities with this level of severity can result in some damage to the protocol or users, without profit for the attacker. They often allow an attacker to exploit a contract to cause harm, but the impact may be limited, such as temporarily blocking the functionality of the protocol. Examples include uninitialized storage pointers and failure to check external calls.

LOW

Vulnerabilities with this level of severity may not result in financial losses or significant harm. They may, however, impact the usability or reliability of a contract. Examples include slippage and front-running, or minor logic bugs.

INFORMATIONAL

Vulnerabilities with this level of severity are regarding gas optimizations and code style. They often involve issues with documentation, incorrect usage of EIP standards, best practices for saving gas, or the overall design of a contract. Examples include not conforming to ERC20, or disagreement between documentation and code.

It's important to consider all types of vulnerabilities, including informational ones, when assessing the security of the project. A comprehensive security audit should consider all types of vulnerabilities to ensure the highest level of security and reliability.

SCOPE

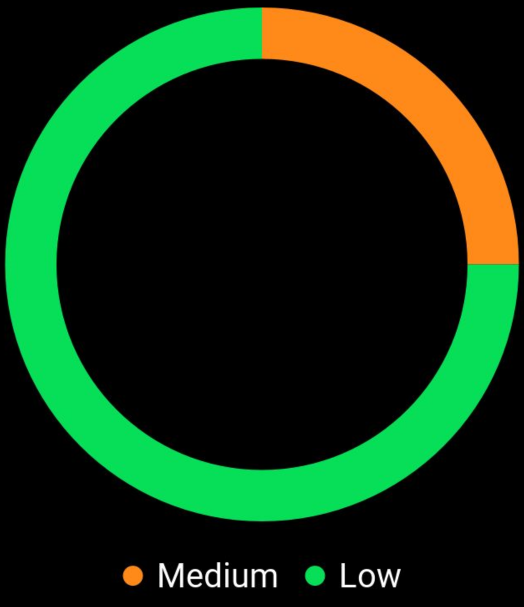
The analyzed web resources are located on:
*.mintify.xyz

SUMMARY

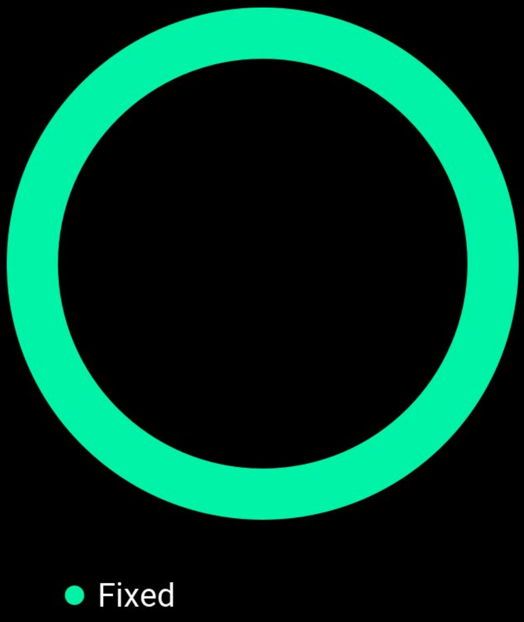
SEVERITY	NUMBER OF FINDINGS
CRITICAL	0
HIGH	0
MEDIUM	1
LOW	3
INFORMATIONAL	0

TOTAL: 4

SEVERITY



STATUS



WEAKNESSES

This section contains the list of discovered weaknesses.

MNTF-3. API KEY EXPOSURE

SEVERITY: Medium

REMEDIATION: Key Concealment: Refrain from embedding API keys directly in the code.

Access Restriction: Rigorously control and validate access to API keys.

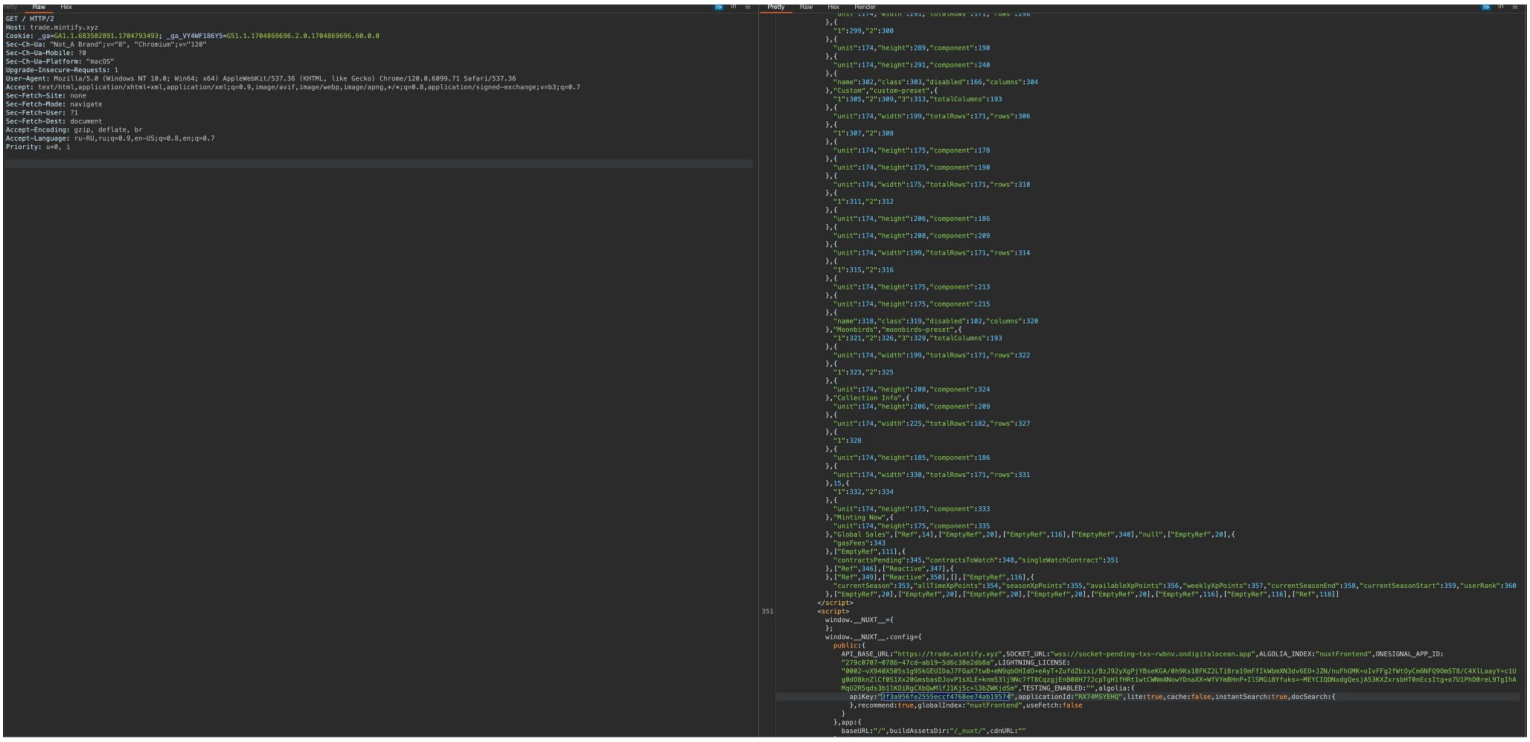
Secure Storage: Utilize secure storage methods, avoiding hardcoded keys.

Monitoring: Establish proactive monitoring measures to swiftly identify and respond to any unauthorized activities.

STATUS: fixed

DESCRIPTION:

The inadvertent exposure of API keys has been detected, posing a significant risk of unauthorized access to sensitive systems.



```
GET / HTTP/2
Host: trade.mintify.xyz
Cookie: _ga=GA1.1.683502891.1704793493; _ga_VY4WF186Y5=GS1.1.1704869696.2.0.1704869696.60.0.0
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
```

```
            "unit":174,"width":291,"totalRows":171,"rows":298
          },{
            "1":299,"2":300
          },{
            "unit":174,"height":289,"component":190
          },{
            "unit":174,"height":291,"component":240
          },{
            "name":302,"class":303,"disabled":166,"columns":304
          },"Custom","custom-preset",{
            "1":305,"2":309,"3":313,"totalColumns":193
          },{
            "unit":174,"width":199,"totalRows":171,"rows":306
          },{
            "1":307,"2":308
          },{
            "unit":174,"height":175,"component":178
          },{
            "unit":174,"height":175,"component":190
          },{
            "unit":174,"width":175,"totalRows":171,"rows":310
          },{
            "1":311,"2":312
          },{
            "unit":174,"height":206,"component":186
          },{
            "unit":174,"height":208,"component":209
          },{
            "unit":174,"width":199,"totalRows":171,"rows":314
          },{
            "1":315,"2":316
          },{
            "unit":174,"height":175,"component":213
          },{
            "unit":174,"height":175,"component":215
          },{
            "name":318,"class":319,"disabled":102,"columns":320
          },"Moonbirds","moonbirds-preset",{
            "1":321,"2":326,"3":329,"totalColumns":193
          },{
            "unit":174,"width":199,"totalRows":171,"rows":322
          },{
            "1":323,"2":325
          },{
            "unit":174,"height":208,"component":324
          },"Collection Info",{
            "unit":174,"height":206,"component":209
          },{
            "unit":174,"width":225,"totalRows":182,"rows":327
          },{
            "1":328
          },{
            "unit":174,"height":185,"component":186
          },{
            "unit":174,"width":330,"totalRows":171,"rows":331
          },15,{
            "1":332,"2":334
          },{
            "unit":174,"height":175,"component":333
          },"Minting Now",{
            "unit":174,"height":175,"component":335
          },"Global Sales",["Ref",14],["EmptyRef",20],["EmptyRef",116],["EmptyRef",340],"null",["EmptyRef",20],{
            "gasFees":343
          },["EmptyRef",111],{
            "contractsPending":345,"contractsToWatch":348,"singleWatchContract":351
          },["Ref",346],["Reactive",347],{
          },["Ref",349],["Reactive",350],[],["EmptyRef",116],{
            "currentSeason":353,"allTimeXpPoints":354,"seasonXpPoints":355,"availableXpPoints":356,"weeklyXpPoints":357,"currentSeasonEnd":358,"currentSeasonStart":359,"userRank":360
          },["EmptyRef",20],["EmptyRef",20],["EmptyRef",20],["EmptyRef",20],["EmptyRef",20],["EmptyRef",116],["EmptyRef",116],["Ref",118]]
        </script>
        <script>
          window.__NUXT__={
          };
          window.__NUXT__.config={
            public:{
              API_BASE_URL:"https://trade.mintify.xyz",SOCKET_URL:"wss://socket-pending-txs-rwbnv.ondigitalocean.app",ALGOLIA_INDEX:"nuxtFrontend",ONESIGNAL_APP_ID:
              "279c0707-0786-47cd-ab19-5d6c38e2db8a",LIGHTNING_LICENSE:
              "0002-vX940X505s1g95kGEUIDaJ7FOaX7twB+eN9qbOHIdO+eAyT+ZufdZbixi/BzJ92yXgPjYBseKGA/0h9Ks1BFKZ2LTiBra19mFfIkWbmXN3dv6EO+JZN/nuFhGMK+oIvFFg2fWtOyCm6NFQ9OmST8/C4XlLaayY+c1U
              g0dO8knZlCf0S1Xx20GmsbasDJovP1sXLE+knm53lj9Nc7fT8CqzgjEnB08H77JcpTgH1fHRt1wtCWNmANowYDnaXX+WfVYmBHnP+IlSMGi8Yfuks=-MEYCIQDNxdgQesjA53KXZxrsbHT0nEcsItg+o7U1PhD0reL9TgIhA
              MqU2R5qds3b1lKOiRgCXbQwMlfJ1Kj5c+l3bZWKjdSm",TESTING_ENABLED:"",algolia:{
                apiKey:"3f3a956fe2555eccf4768ee74ab19574",applicationId:"RX74MSYEHQ",lite:true,cache:false,instantSearch:true,docSearch:{
                },recommend:true,globalIndex:"nuxtFrontend",useFetch:false
              }
            },app:{
              baseURL:"/",buildAssetsDir:"/_nuxt/",cdnURL:""
```

MNTF-1. CLOUDFLARE EXTERNAL IMAGE RESIZE

SEVERITY: Low

REMEDIATION: Access Restriction: Implement strict access controls for the external image resizing function.

Authentication: Introduce authentication mechanisms to validate requests for image resizing.

Monitoring: Set up a monitoring system to detect unusual activity and suspicious image resizing requests.

Update and Patching: Regularly update Cloudflare software and apply patches to mitigate potential vulnerabilities.

STATUS: fixed

DESCRIPTION:

https://trade.mintify.xyz/cdn-cgi/image/width/<External_Server>

https://api.mintify.xyz/cdn-cgi/image/width/<External_Server>

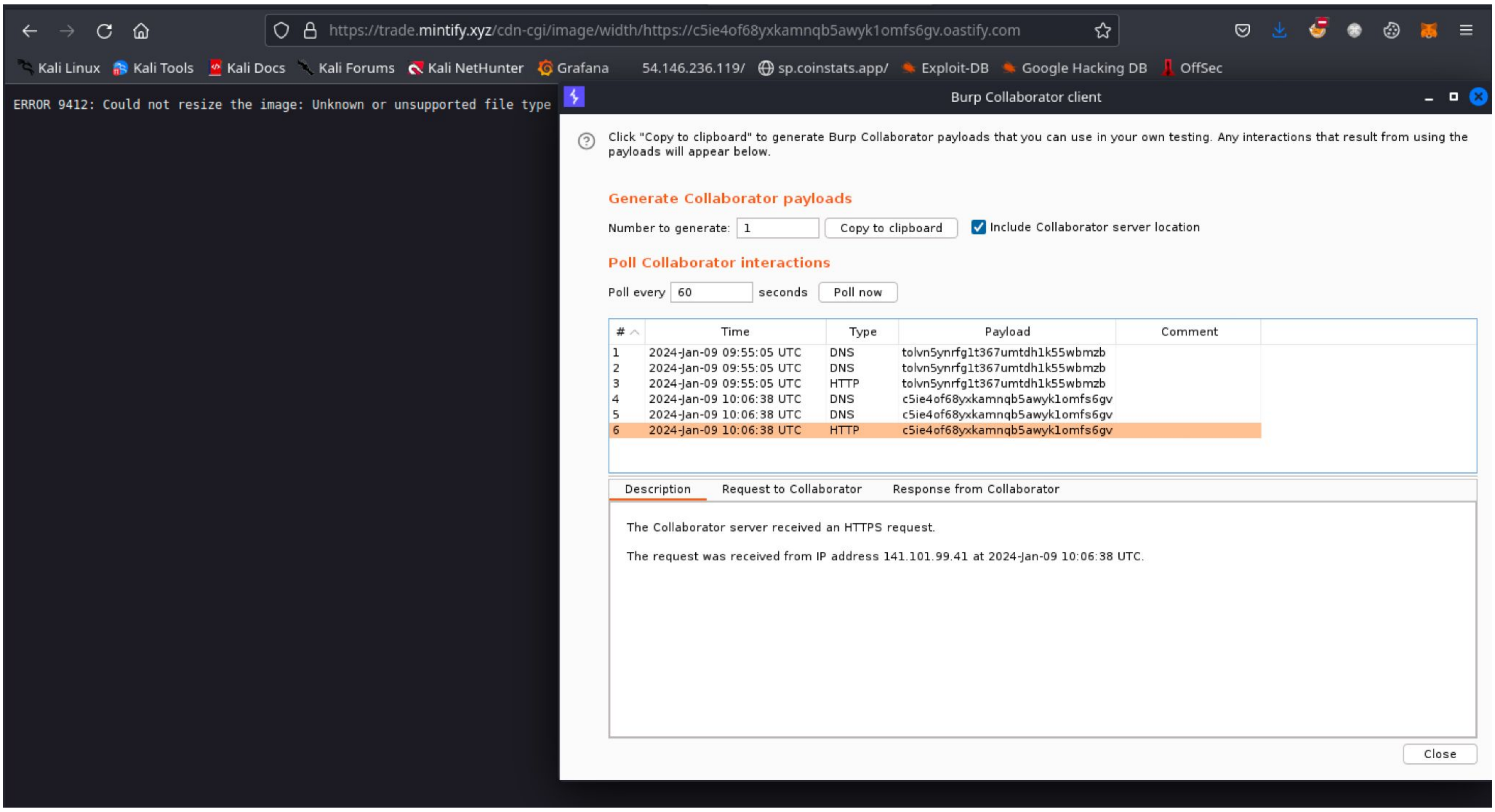
https://t2.mintify.xyz/cdn-cgi/image/width/<External_Server>

https://app.mintify.xyz/cdn-cgi/image/width/<External_Server>

https://store.mintify.xyz/cdn-cgi/image/width/<External_Server>

https://genesis-metas.mintify.xyz/cdn-cgi/image/width/<External_Server>

A vulnerability has been identified in the external image resizing mechanism through Cloudflare, potentially leading to insecure image operations and exploitable scenarios.



```
ERROR 9412: Could not resize the image: Unknown or unsupported file type
```

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 Copy to clipboard ☑ Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
1	2024-Jan-09 09:55:05 UTC	DNS	tolvn5ynrfg1t367umtdh1k55wbmzb	
2	2024-Jan-09 09:55:05 UTC	DNS	tolvn5ynrfg1t367umtdh1k55wbmzb	
3	2024-Jan-09 09:55:05 UTC	HTTP	tolvn5ynrfg1t367umtdh1k55wbmzb	
4	2024-Jan-09 10:06:38 UTC	DNS	c5ie4of68yxkamnqb5awyk1omfs6gv	
5	2024-Jan-09 10:06:38 UTC	DNS	c5ie4of68yxkamnqb5awyk1omfs6gv	
6	2024-Jan-09 10:06:38 UTC	HTTP	c5ie4of68yxkamnqb5awyk1omfs6gv	

Description | Request to Collaborator | Response from Collaborator

The Collaborator server received an HTTPS request.

The request was received from IP address 141.101.99.41 at 2024-Jan-09 10:06:38 UTC.

MNTF-2. FULL PATH DISCLOSURE VIA POOR EXCEPTION HANDLING

SEVERITY: Low

REMEDIATION: Secure Exception Handling: Rectify exception handling to prevent path exposure.

Information Restriction: Minimize error details to avoid revealing system structure.

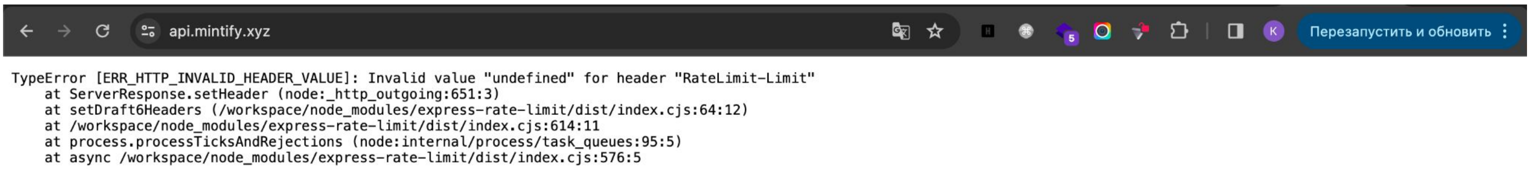
Security Logging: Maintain secure event logs to detect potential exploitation attempts.

Code Audits: Regularly audit code to identify and address such vulnerabilities.

STATUS: fixed

DESCRIPTION:

A vulnerability allowing the exposure of full file paths due to improper exception handling has been identified. This could lead to leakage of confidential information and create an opportunity for potential attacks.



```
TypeError [ERR_HTTP_INVALID_HEADER_VALUE]: Invalid value "undefined" for header "RateLimit-Limit"
    at ServerResponse.setHeader (node:_http_outgoing:651:3)
    at setDraft6Headers (/workspace/node_modules/express-rate-limit/dist/index.cjs:64:12)
    at /workspace/node_modules/express-rate-limit/dist/index.cjs:614:11
    at process.processTicksAndRejections (node:internal/process/task_queues:95:5)
    at async /workspace/node_modules/express-rate-limit/dist/index.cjs:576:5
```

MNTF-4. CORS, ARBITRARY DOMAIN TRUST

SEVERITY: Low

REMEDIATION: Access Restriction: Allow access only to trusted domains.

CORS Headers: Configure CORS headers to define access rules.

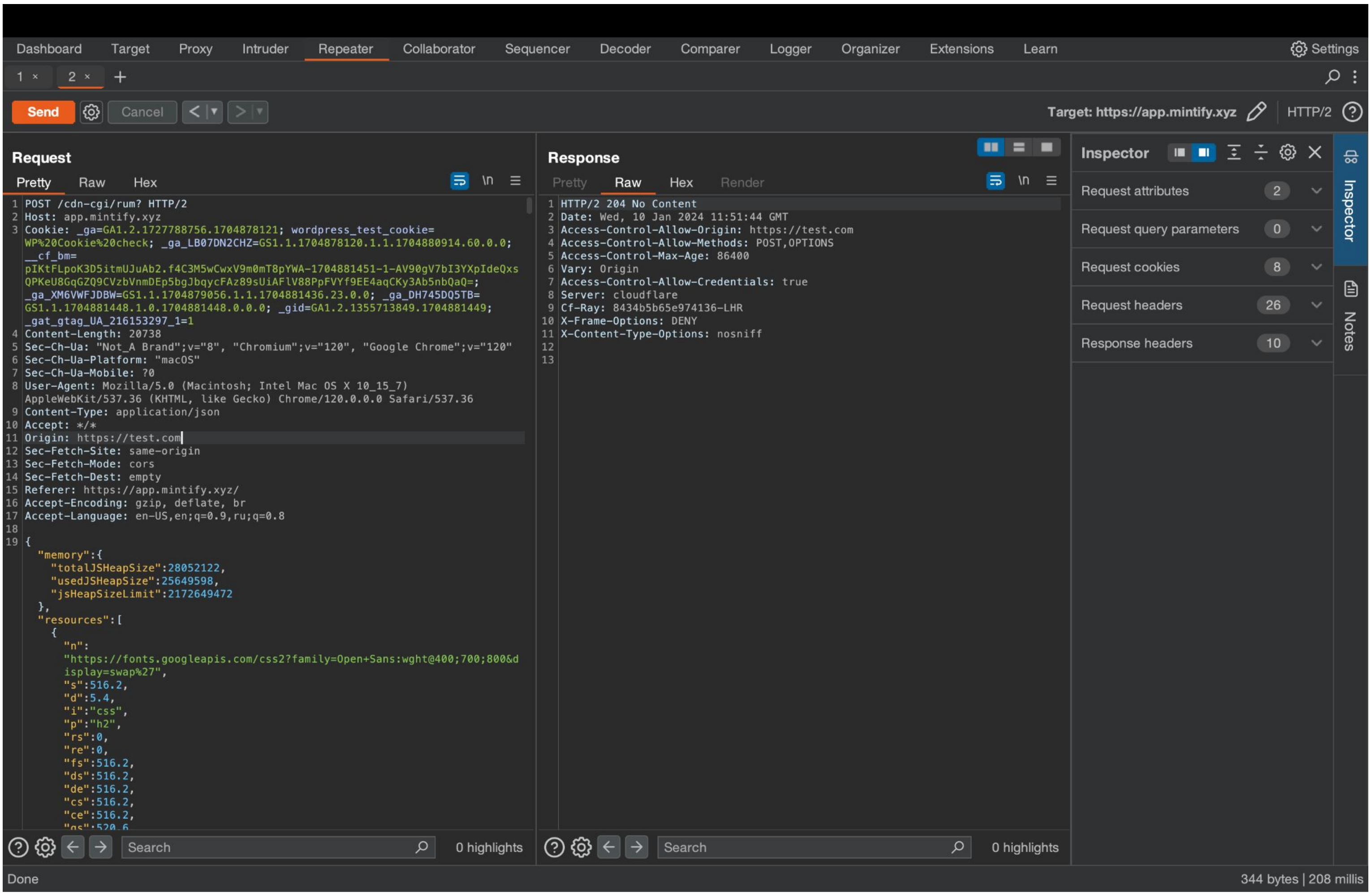
Trust Verification: Verify domains before granting access to requests.

Regular Audits: Conduct periodic security audits to detect and address such vulnerabilities.

STATUS: fixed

DESCRIPTION:

A vulnerability in CORS has been identified, allowing arbitrary domains to access resources and creating the potential for cross-site attacks.



```
POST /cdn-cgi/rum? HTTP/2
Host: app.mintify.xyz
Cookie: _ga=GA1.2.1727788756.1704878121; wordpress_test_cookie=
WP%20Cookie%20check; _ga_LB07DN2CHZ=GS1.1.1704878120.1.1.1704880914.60.0.0;
__cf_bm=
pIKtFLpoK3D5itmUJuAb2.f4C3M5wCwxV9m0mT8pYWA-1704881451-1-AV90gV7bI3YXpIdeQxs
QPKeU8GqGZQ9CVzbVnmDEp5bgJbqycFAz89sUiAFlV88PpFVYf9EE4aqCKy3Ab5nbQaQ=;
_ga_XM6VWFJDBW=GS1.1.1704879056.1.1.1704881436.23.0.0; _ga_DH745DQ5TB=
GS1.1.1704881448.1.0.1704881448.0.0.0; _gid=GA1.2.1355713849.1704881449;
_gat_gtag_UA_216153297_1=1
Content-Length: 20738
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120", "Google Chrome";v="120"
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: https://test.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.mintify.xyz/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ru;q=0.8

{
  "memory":{
    "totalJSHeapSize":28052122,
    "usedJSHeapSize":25649598,
    "jsHeapSizeLimit":2172649472
  },
  "resources":[
    {
      "n":
      "https://fonts.googleapis.com/css2?family=Open+Sans:wght@400;700;800&d
      isplay=swap%27",
      "s":516.2,
      "d":5.4,
      "i":"css",
      "p":"h2",
      "rs":0,
      "re":0,
      "fs":516.2,
      "ds":516.2,
      "de":516.2,
      "cs":516.2,
      "ce":516.2,
      "gs":520.6
```

```
HTTP/2 204 No Content
Date: Wed, 10 Jan 2024 11:51:44 GMT
Access-Control-Allow-Origin: https://test.com
Access-Control-Allow-Methods: POST,OPTIONS
Access-Control-Max-Age: 86400
Vary: Origin
Access-Control-Allow-Credentials: true
Server: cloudflare
Cf-Ray: 8434b5b65e974136-LHR
X-Frame-Options: DENY
X-Content-Type-Options: nosniff


```

hexens