URL shortener (Engineer 2)

Owner: Engineer 2
Reviewer:
Contributors:
Date Generated: Wed Dec 25 2024

OWASP Threat Dragon

Executive Summary

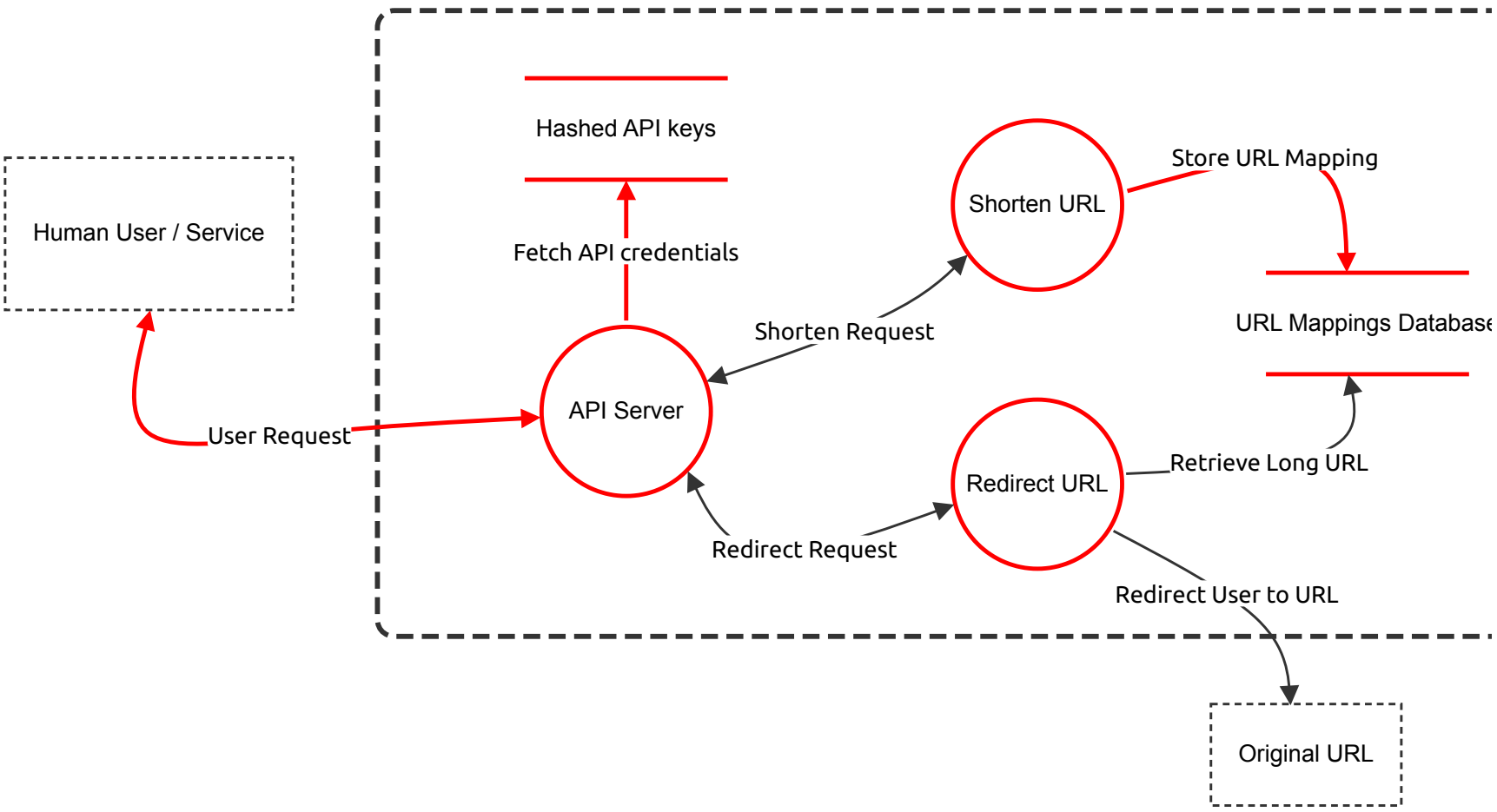
High level system description

The URL Shortener Service aims to provide a simple and efficient way for users to convert long URLs into short, easily shareable URLs. The service ensures functionality, reliability, and security while interacting with users and handling their data.

Summary

Total Threats	41
Total Mitigated	0
Not Mitigated	41
Open / High Priority	0
Open / Medium Priority	40
Open / Low Priority	0
Open / Unknown Priority	0

URL Shortener Service Architecture



URL Shortener Service Architecture

Human User / Service (Actor) - *Out of Scope*

Reason for out of scope: Incoming requests outside of application scope

Description: External services or human users may interact with the API for bulk operations or integrations.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Redirect URL (Process)

Description: Enables users to resolve short URLs and be redirected to the corresponding long URLs via a dedicated API.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	External connection	Spoofing	Medium	Open		An attacker can bypass the API server and connect directly to the URL shortener or URL redirect processes without authenticating.	Provide remediation for this threat or a reason if status is N/A
13	Unauthenticated link	Spoofing	Medium	Open		An attacker can connect to a server or peer over a link that isn't authenticated (and encrypted).	Provide remediation for this threat or a reason if status is N/A

Shorten URL (Process)

Description: Allows users to submit long URLs and receive shortened URLs via a dedicated API.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	External connection	Elevation of privilege	Medium	Open		An attacker can bypass the API server and connect directly to the URL shortener or URL redirect processes without authenticating.	Provide remediation for this threat or a reason if status is N/A
14	Unauthenticated link	Spoofing	Medium	Open		An attacker can connect to a server or peer over a link that isn't authenticated (and encrypted).	Provide remediation for this threat or a reason if status is N/A
38	Different validation paths	Elevation of privilege	Medium	Open		An attacker can force data through different validation paths which give different results.	Provide remediation for this threat or a reason if status is N/A
40	Malicious long URL	Elevation of privilege	Medium	Open		An attacker can provide a malicious long URL to be shortened to deceive other users unaware of the mapping.	Provide remediation for this threat or a reason if status is N/A
41	Validated data still under attacker's control	Elevation of privilege	Medium	Open		An attacker can enter data that is checked while still under the attacker's control and used later on the other side of a trust boundary	Provide remediation for this threat or a reason if status is N/A
42	Possible attacks with URLs	Elevation of privilege	Medium	Open		An attacker can try to craft a URL with injected scripts, causing a lot of different attacks, such as CSRF	Provide remediation for this threat or a reason if status is N/A

URL Mappings Database (Store)

Description: Data store containing the mappings between short URLs and their corresponding long URLs.

DATA STORED: Long URL, Short URL, UserID, CreationDate

Number	Title	Type	Priority	Status	Score	Description	Mitigations
23	Too broad permissions	Tampering	Medium	Open		An attacker can write to some resource because permissions are granted to the world or there are no ACLs.	Provide remediation for this threat or a reason if status is N/A
28	Denying registering the mapping	Repudiation	Medium	Open		An attacker can deny registering some mapping and there is no way to prove they didn't do that.	Provide remediation for this threat or a reason if status is N/A
36	Information disclosure	Information disclosure	Medium	Open		An attacker could read from the database and discover the mappings of other clients	Provide remediation for this threat or a reason if status is N/A
39	New STRIDE threat	Denial of service	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Original URL (Actor) *- Out of Scope*

Reason for out of scope: Original URL not in scope of URL shortener application

Description: Destination server of the original URL

Number	Title	Type	Priority	Status	Score	Description	Mitigations

API Server (Process)

Description: The API Server is the central component of the URL Shortener Service. It manages all interactions with users and external services, handling requests for both shortening URLs and redirecting from short URLs to their original long URLs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Brute-force attack	Spoofing	Medium	Open		An attacker could try one credential after another and there’s nothing to slow them down (online or offline).	
4	Anonymous connection	Spoofing	Medium	Open		An attacker can anonymously connect, because we expect authentication to be done at a higher level.	Provide remediation for this threat or a reason if status is N/A
5	Re-connection inconsistency	Spoofing	Medium	Open		An attacker can spoof a server because identifiers aren’t stored on the client and checked for consistency on re-connection (that is, there’s no key persistence).	Provide remediation for this threat or a reason if status is N/A
6	Unauthenticated link	Spoofing	Medium	Open		An attacker can connect to a server or peer over a link that isn’t authenticated (and encrypted).	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Credentials theft	Spoofing	Medium	Open		An attacker could steal credentials stored on the server and reuse them (for example, a key is stored in a world readable file).	Provide remediation for this threat or a reason if status is N/A
9	Password reuse	Spoofing	Medium	Open		An attacker who gets a password can reuse it (use stronger authenticators).	Provide remediation for this threat or a reason if status is N/A
10	Weaker or no authentication	Spoofing	Medium	Open		An attacker can choose to use weaker or no authentication.	Provide remediation for this threat or a reason if status is N/A
11	Old passwords disclosing	Spoofing	Medium	Open		An attacker could go after the way credentials are updated or recovered (account recovery doesn't require disclosing the old password).	Provide remediation for this threat or a reason if status is N/A
12	Default system passwords	Spoofing	Medium	Open		Your system ships with a default admin password and doesn't force a change.	Provide remediation for this threat or a reason if status is N/A
16	Different UserID	Spoofing	Medium	Open		An attacker can authenticate properly and then use a different UserID to exfiltrate and disclose data they are not entitled to see.	Provide remediation for this threat or a reason if status is N/A
17	Spreaded access control decisions	Tampering	Medium	Open		Your code makes access control decisions all over the place, rather than with a security kernel.	Provide remediation for this threat or a reason if status is N/A
19	Non-canonical names	Tampering	Medium	Open		An attacker can bypass permissions because you don't make names canonical before checking access permissions.	Provide remediation for this threat or a reason if status is N/A
20	State information control	Tampering	Medium	NotApplicable		An attacker can provide or control state information.	URL Shortener service is stateless
22	Parameter change after validation	Tampering	Medium	Open		An attacker can change parameters over a trust boundary and after validation (for example, important parameters in a hidden field in HTML or passing a pointer to critical memory).	Provide remediation for this threat or a reason if status is N/A
24	Security information in the logs	Repudiation	Medium	Open		A low privilege attacker can read interesting security information in the logs.	Provide remediation for this threat or a reason if status is N/A
25	Common key confusing information in the logs	Repudiation	Medium	Open		An attacker can use a shared key to authenticate as different principals, confusing the information in the logs.	Provide remediation for this threat or a reason if status is N/A
26	Repudation attempt	Repudiation	Medium	Open		An attacker can say "I didn't do that," and you would have no way to prove them wrong.	Provide remediation for this threat or a reason if status is N/A
27	System has no logs	Repudiation	Medium	Open		The system has no logs.	Provide remediation for this threat or a reason if status is N/A
29	Error messeges with sensitive content	Information disclosure	Medium	Open		An attacker can see error messages with security sensitive content.	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
37	Request Flooding	Denial of service	Medium	Open		An attacker can perform a lot of invalid API calls, and the server will have to process a large number of incorrect requests, possibly causing a crash.	Provide remediation for this threat or a reason if status is N/A
44	Command injection	Elevation of privilege	Medium	Open		An attacker can inject a command that the system will run at a higher privilege level.	Provide remediation for this threat or a reason if status is N/A

Hashed API keys (Store)

Description: Database containing hashed API keys for authentication purposes.

DATA STORED: Hashed API Key, UserID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Too broad permissions	Tampering	Medium	Open		An attacker can write to some resource because permissions are granted to the world or there are no ACLs.	Provide remediation for this threat or a reason if status is N/A
35	Information disclosure	Information disclosure	Medium	Open		An attacker could read from the database and discover API key hashes	Provide remediation for this threat or a reason if status is N/A

Redirect Request (Data Flow)

Description: The user submits a short URL to the API and gets redirected to the original Long URL.

DATA EXCHANGED: Short URL, Long URL

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Redirect User to URL (Data Flow)

Description: The user is redirected to the Long URL.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Retrieve Long URL (Data Flow)

Description: Long URL mapping is pulled from the database in order to redirect user.

DATA EXCHANGED: Short URL, Long URL, UserID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Shorten Request (Data Flow)

Description: The user submits a long URL to the API for shortening.

DATA EXCHANGED: Short URL, Long URL, UserID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Fetch API credentials (Data Flow)

Description: Hashed API keys are pulled to authenticate the user before performing any operation.

DATA EXCHANGED: Hashed API key

Number	Title	Type	Priority	Status	Score	Description	Mitigations
31	Data modification	Tampering	Medium	Open		An attacker can modify data in transit while an API key is saved in the database	Provide remediation for this threat or a reason if status is N/A
32	Data disclosure	Information disclosure	Medium	Open		An attacker can read content because messages (for example, an email or HTTP cookie) aren't encrypted even if the channel is encrypted.	Provide remediation for this threat or a reason if status is N/A

Store URL Mapping (Data Flow)

Description: The API Server processes the request for shortening a URL, generates a short URL, and stores the mapping between the short URL and the long URL in the URL Database.

DATA EXCHANGED: Short URL, Long URL

Number	Title	Type	Priority	Status	Score	Description	Mitigations
33	Data disclosure	Information disclosure	Medium	Open		THIS THREAT APPLIES TO ALL DATA FLOWS INSIDE THE TRUST BOUNDARY An attacker can read content because messages (for example, an email or HTTP cookie) aren't encrypted even if the channel is encrypted.	Provide remediation for this threat or a reason if status is N/A
34	Data manipulation	Tampering	Medium	Open		THIS THREAT APPLIES TO ALL DATA FLOWS INSIDE THE TRUST BOUNDARY An attacker can modify content of data flow while it's being transferred to another process.	Provide remediation for this threat or a reason if status is N/A

User Request (Data Flow)

Description: The User sends a request to the API Server to shorten a long URL or to get the redirect URL.

DATA EXCHANGED: Long URL, Short URL, API key

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	Data manipulation	Tampering	Medium	Open		An attacker can manipulate data because there's no integrity protection for data on the network.	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
30	Lack of data flow encryption	Information disclosure	Medium	Open		An attacker can read content because messages (for example, an email or HTTP cookie) aren't encrypted even if the channel is encrypted.	Provide remediation for this threat or a reason if status is N/A