

Information exposure through query strings in url

WatchStar

Description

Information exposure through query strings in URL is when sensitive data is passed to parameters in the URL. This allows attackers to obtain sensitive data such as usernames, passwords, tokens (authX), database details, and any other potentially sensitive data. Simply using HTTPS does not resolve this vulnerability.

Risk Factors

Threat Agents: App Specific Attack Vectors: Average Security Weakness (prevalence): Common Security Weakness (detectability): Difficult Technical Impacts: Moderate Business Impacts: App Specific

Examples

Regardless of using encryption, the following URL will expose information in the locations detailed below: https://vulnerablehost.com/authuser?user=bob&authz_token=1234&expire=1500000000

The parameter values for `user`, `authz_token`, and `expire` will be exposed in the following locations when using HTTP or HTTPS:

- Referer Header
- Web Logs
- Shared Systems
- Browser History
- Browser Cache
- Shoulder Surfing

When not using an encrypted channel, all of the above and the following:

- Man-in-the-Middle

Exposure Proof-of-Concept

The following figure displays how an internal attacker can potentially exploit this vulnerability as the request above is captured in the server logs even when requested via an encrypted channel:

<https://vulnerablehost.com/information-exposure-log.png>

The OWASP Foundation

works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Important Community Links

[Community](#)

[Attacks](#)

[Vulnerabilities \(You are here\)](#)

[Controls](#)

Upcoming Global Events

[Global AppSec SF October 19th-23rd](#)

[Global AppSec Dublin February 15-19th, 2021](#)

Related Attacks

- [Forced browsing](#)

References

- [Testing for Exposed Session Variables \(OTG-SESS-004\)](#)
- [Top 10-2017 A3-Sensitive Data Exposure](#)
- [Top 10 2013-A6-Sensitive Data Exposure](#)
- [CWE-598: Information Exposure Through Query Strings in GET Request](#)
- [4.4.1.1. Threat: Eavesdropping or Leaking Authorization "codes"](#)
- [Passwords Submitted Using GET Method](#)

[Edit on Github](#)

Spotlight: WhiteHat Security

Corporate Supporters

WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. Through a combination of technology, over a decade of intelligence metrics, and the judgment of people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry.



[Become a corporate supporter](#)

[PRIVACY](#) [SITEMAP](#) [CONTACT](#)



Open Web Application Security Project, OWASP, Global AppSec, AppSec Days, AppSec California, SnowFROC, LASCON, and the OWASP logo are trademarks of the OWASP Foundation. Unless otherwise specified, all content on the site is Creative Commons Attribution-ShareAlike v4.0 and provided without warranty of service or accuracy. For more information, please refer to our [General Disclaimer](#). Copyright 2020, OWASP Foundation, Inc.