

Ralayalseema university
kurnool

Sri sankaras degree college
kurnool

R somanath
bsc micro biology

OWASP TOP10 VULNERABILITY OVER VIEW POINT

Owasp top10 vulnerability

The OWASP (Open Web Application Security Project) Top 10 is a list of the 10 most critical security risks to web applications. The list is updated periodically to reflect the changing landscape of web security threats. As of my last update, here are the OWASP Top 10 vulnerabilities:

1. **Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing unauthorized data.
2. **Broken Authentication:** Broken authentication occurs when authentication and session management functions are improperly implemented, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other weaknesses to assume other users' identities.
3. **Sensitive Data Exposure:** Sensitive data exposure happens when an application does not properly protect sensitive data, such as financial, healthcare, or personal information. This can include encryption, proper storage, and handling of sensitive data.
4. **XML External Entities (XXE):** XXE occurs when an XML parser insecurely processes XML input, allowing attackers to execute arbitrary code, access files, or perform other malicious activities.
5. **Broken Access Control:** Broken access control occurs when restrictions on what authenticated users are allowed to do are not properly enforced. This can allow attackers to access unauthorized functionality or data.

1.Security Misconfiguration: Security misconfiguration happens when security settings are not properly configured, leaving vulnerabilities open for exploitation. This can include default configurations, incomplete or ad hoc configurations, open cloud storage, and more.


2.Cross-Site Scripting (XSS): XSS vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users. These scripts can steal session cookies, deface websites, redirect users to malicious sites, or perform other malicious actions.

3.Insecure Deserialization: Insecure deserialization occurs when untrusted data is used to abuse the logic of an application, leading to remote code execution, privilege escalation, or other attacks.


4.Using Components with Known Vulnerabilities: Using outdated or vulnerable components, such as libraries, frameworks, or other software modules, can introduce security vulnerabilities into an application.

5.Insufficient Logging & Monitoring: Insufficient logging and monitoring make it difficult to detect and respond to security incidents, allowing attackers to maintain persistence, escalate privileges, or exfiltrate data without being detected.

Altro mutual analysis



[Sign Out](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

[MY ACCOUNT](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

Hello Admin User

Welcome to Altro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The Altro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW010>.

Copyright © 2008, 2023, IBM Corporation. All rights reserved.

Altro analysis key points

- ▣ **Purpose and Scope:** Define the purpose of your analysis and its scope. What are you trying to achieve, and what specific aspects are you examining?
- ▣ **Data Collection:** Gather relevant data from credible sources. This could include numerical data, qualitative information, or a combination of both.
- ▣ **Data Organization:** Organize the data in a structured manner. This might involve categorizing information, creating tables, charts, or graphs for visualization, and ensuring data integrity.
- ▣ **Analysis Techniques:** Choose appropriate analysis techniques based on your objectives and the nature of the data. This could range from statistical analysis to qualitative interpretation or a combination of methods.
- ▣ **Identify Patterns and Trends:** Look for patterns, trends, or anomalies in the data. This could involve statistical analysis to identify correlations, time-series analysis to detect trends over time, or thematic analysis to uncover recurring themes in qualitative data.

Vulnerability identification and reporting

- When reporting vulnerability identifications, clarity and detail are essential for effective communication. Here are some key points to consider:
- **Description of Vulnerability:** Clearly describe the vulnerability, including its nature, potential impact, and affected systems or components.
- **Reproduction Steps:** Provide detailed steps to reproduce the vulnerability. This helps the recipient understand the issue and verify its existence.
- **Affected Versions/Systems:** Specify the versions or systems that are vulnerable. This helps in assessing the scope of the issue and determining which systems need immediate attention.
- **Severity Assessment:** Assess the severity of the vulnerability based on factors such as potential impact, ease of exploitation, and likelihood of occurrence.
- **Mitigation Recommendations:** Offer recommendations for mitigating the vulnerability. This could include temporary workarounds, patches, or configuration changes.
- **Proof of Concept (PoC):** If possible, provide a PoC demonstrating the vulnerability. This helps in validating the issue and understanding its underlying cause.

Key points for vulnerabilities

- ▣ **References and Resources:** Include references to any relevant documentation, advisories, or research that support your findings.
- ▣ **Contact Information:** Provide contact information for further discussion or clarification. This ensures that recipients can reach out for additional information or assistance.
- ▣ **Timeline:** If applicable, include a timeline of when the vulnerability was discovered, when it was reported, and any actions taken since discovery.
- ▣ **Confidentiality Considerations:** If the vulnerability involves sensitive information or systems, specify any confidentiality requirements or restrictions on disclosure.
- ▣ **Acknowledgment Request:** Request acknowledgment of receipt and confirmation of understanding of the reported vulnerability.
- ▣ **Follow-Up Plan:** Outline any plans for follow-up communication or collaboration to address the vulnerability.

Vulnerabilites scanning urland file with ip address



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



https://www.google.com/search?q=ibomma+telugu+movies&oq=ibomm&gs_lcrp=EgZjaHJvbWUqDQ

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

© Want to automate submissions? [Check our API](#), or [access your API key](#).

These can use ibomma website vulnerability check details

0
/ 93

Community Score

✓ No security vendors flagged this URL as malicious

Reanalyze Search Graph API

https://www.google.com/search?q=ibomma+telugu+movies&oq=ibomm&gs_lcrp=EgZjaHJvbWUqDQgAEAAygwEysQMYgAQyDQgAEAAygwEysQMYgAQyDQgBEAAygwEysQMYgAQyDQgCEAAygwEysQMYgAQyDQg

text/html

DETECTION

DETAILS

CONTENT

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

⚠ From Wiper to Ransomware: The Evolution of Agrius - according to source ArcSight Threat Intelligence - 6 months ago

↳ Contextual Indicators: The domain's Cisco Umbrella rank is 1 Contextual Indicators: The domain's Alexa rank is 1 Contextual Indicators: The URL is known benign by Check Point's Threat Cloud Contextual Indicators: The domain is popular among websites with good reputation Contextual Indicators: The domain is popular in the world Created On: 1997-09-15 VirusTotal Link: https://www.virustotal.com/gui/domain/191347bfe55d0ca9a574db77bc8648275ce258461450e793528e0cc6d2dcf85/detection Classification Description: Legitimate website which does not serve any malicious purpose.

Security vendors' analysis

Do you want to automate checks?

ArcSight Threat Intelligence	ⓘ Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
ALLabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfore.AI PreCrime	✓ Clean

Vulnerability with analysis

These are vulnerability we can use uRL and source ibomma web site and file and complete anaylsis

The screenshot displays the VirusTotal web interface for a specific URL. At the top left, a green circular badge shows '0' detections out of '93' total. A green checkmark icon and the text 'No security vendors flagged this URL as malicious' are prominently displayed. The analyzed URL is a Google search result for 'ibomma+telugu+movies'. Below the URL, the file type is identified as 'text/html'. The interface includes tabs for 'DETECTION', 'DETAILS', 'CONTENT', and 'COMMUNITY', with 'DETAILS' currently selected. A green banner encourages joining the VT Community. The 'Categories' section lists security vendors and their detection results. The 'History' section shows the first, last, and analysis submission times. The 'HTTP Response' section displays the final URL, serving IP address, and status code.

0 / 93

No security vendors flagged this URL as malicious

Reanalyze Search Graph

https://www.google.com/search?q=ibomma+telugu+movies&ooq=ibomm&gs_lcrp=EgZjaHJvbWUqDQgAEAAygwEYsQMigAQyDQgAEAAygwEYsQMigAQyDQgBEAAygwEYsQMigAQyDQg...

text/html

DETECTION DETAILS CONTENT COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Categories ⌵

BitDefender	searchengines
Xcitium Verdict Cloud	unknown
Sophos	search engines
Forcepoint ThreatSeeker	search engines and portals

History ⌵

First Submission	2024-03-15 13:32:20 UTC
Last Submission	2024-03-15 13:32:20 UTC
Last Analysis	2024-03-15 13:32:20 UTC

HTTP Response ⌵

Final URL

https://www.google.com/search?q=ibomma+telugu+movies&sca_esv=cbe20439333e335&gbv=1&sei=5k30ZYFLNr-p84PzrCS6Ao

Serving IP Address

108.177.120.99

Status Code

302

Vulnerability exploitation key points

When considering the exploitation of vulnerabilities, it's important to approach the topic responsibly and ethically. Here are key points to understand:

- ❖ **Understanding the Vulnerability:** Ensure a comprehensive understanding of the vulnerability, including its nature, impact, and affected systems. This understanding forms the basis for effective exploitation.
- ❖ **Legal and Ethical Considerations:** Adhere to all relevant laws, regulations, and ethical guidelines when exploring vulnerabilities. Unauthorized access to systems or data can have serious legal consequences.
- ❖ **Permission and Authorization:** Obtain explicit permission and authorization before attempting to exploit vulnerabilities. This may involve working within a controlled environment or obtaining consent from system owners.
- ❖ **Documentation and Reporting:** Document all steps taken during the exploitation process, including techniques used, findings, and outcomes. This documentation can serve as valuable insight for vulnerability remediation efforts.
- ❖ **Risk Assessment:** Evaluate the potential risks associated with exploiting the vulnerability, including potential impact on systems, data, and users.