GRIDWARE TOP 10 WEB APPLICATION VULNERABILITIES

Sydney Head Office
Level 12/189 Kent St,
Sydney NSW 2000

Telephone
1300 211 235

Email
info@gridware.com.au

Gridware

Listed below are the most common vulnerabilities as seen by the Gridware pentest team during web application engagements across the months of July, August and September 2022, along with their typical severity in brackets.

For the month of July 2022:

1. Unrestricted File Upload (high)
2. Vulnerable Javascript Library (high)
3. Improper Error Handling (medium)
4. Browser XSS Filter Misconfiguration (low)
5. Information disclosure (low)
6. Clickjacking (medium)
7. Broken Access Control (high)
8. Outdated Software (high)
9. TLS Cookie Without Secure Flag Set (medium)
10. SSL Certificate Expiration (medium)

For the month of August 2022:

1. Information disclosure (low)
2. Unrestricted File Upload (high)
3. Clickjacking (medium)
4. BEAST Attack (medium)
5. Strict Transport Security Misconfiguration (low)
6. Improper Error Handling (medium)
7. TLS Cookie Without Secure Flag Set (medium)
8. Browser XSS Filter Misconfiguration (low)
9. Content Sniffing Not Disabled (low)
10. Broken Access Control (high)

For the month of September 2022:

1. BREACH Attack Vulnerability (medium)
2. Browser XSS Filter Misconfiguration (low)
3. Strict Transport Security Misconfiguration (low)
4. Content Sniffing Not Disabled (low)
5. Unrestricted File Upload (high)
6. LUCKY13 Vulnerability (low)
7. ClickJacking (medium)
8. Cross Site Scripting (high)
9. Improper Error Handling (medium)
10. Stack Trace Error (high)

Level 12/189 Kent St, Sydney NSW 2000
1300 211 235
www.gridware.com.au

Gridware

Below are some basic summaries of the medium and high vulnerabilities that we frequently see in our top 10 web application vulnerabilities.

High Vulnerabilities
Unrestricted File Upload
Vulnerable Javascript Library
Broken Access Control
Outdated Software
Stack Trace Error
Cross Site Scripting

Medium Vulnerabilities
Improper Error Handling
Clickjacking
TLS Cookie Without Secure Flag Set
SSL Certificate Expiration
BEAST Attack
BREACH Attack

High Vulnerabilities

Unrestricted File Upload refers to a vulnerability of not having adequate controls to ensure files uploaded by a user are sufficiently validated or sanitised. This could potentially allow for the upload of malicious files and can lead to various outcomes including overloaded servers and could even result in a system takeover.

Vulnerable Javascript Library - Using components such as javascript libraries with associated vulnerabilities could mean that an attacker through enumeration techniques could discover a library that you're running that is vulnerable to an already documented exploit and it could potentially be as easy as executing the exploit against your website. This can chain to other attacks such as cross-site scripting, cross-site request forgery and buffer overflow. The vulnerable Javascript library has been placed in the high vulnerability category, because it is categorised by the vulnerability of the library itself, and the vulnerability could potentially be of high severity.

Broken Access Control refers to inadequate enforcement of policies that can lead to users acting outside of their intended permissions. One example of broken access control is modifying my ID to be the same as an admins ID, this might then allow a user to view sensitive data that only administrators should be able to see.

Outdated software is very similar to the vulnerable Javascript library vulnerability, however it encompasses all software, and isn't restricted to Javascript libraries.

Stack Trace Error - A stack trace is not a vulnerability by itself, however, it often will reveal information that could potentially be useful to an attacker. A hacker may "fiddle" around with a website to try and return a stack trace that may give away this useful information (such as a relative path on the web server) which can then be used in further attacks.

Cross Site Scripting (XSS) - A cross site scripting attack involves injecting malicious scripts into trusted websites and can compromise interactions that users have with a vulnerable web application, basically allowing the submission of a script in an input field. The result could be various outcomes such as the retrieval of a person's session cookie allowing the sending and retrieval of data that the victim is entitled to, and could include such things as credit card numbers.

Level 12/189 Kent St, Sydney NSW 2000
1300 211 235
www.gridware.com.au

Gridware

Gridware

Medium Vulnerabilities

Improper Error Handling - Improper error handling can lead to a variety of issues. A very common issue with improper error handling is when an error returns too much information which can assist an attacker in learning more about the way a website functions, and could allow the building of a sophisticated attack plan. An example of improper error handling is if the user types in an incorrect password and username, and receives an error "Incorrect Password/Username combination" and then tries again and receives "Incorrect password" it may tell the attacker that they have the correct username.

Clickjacking - Clickjacking is an attack that involves the use of multiple transparent layers to try to trick a user into clicking on something that is different than what the user thinks. It can lead to various outcomes such as using a transparent "sign in button" layer perfectly positioned over the top of the sign-in button that was already there, and it leads to a phishing website that looks the same where the user unknowingly submits their details.

TLS Cookie Without Secure Flag Set - The secure flag on a cookie stops the browser from submitting the cookie in requests that use an unencrypted HTTP connection, thus disallowing intercepted cookie data. If the secure flag is not set, an attack can eavesdrop on a connection, recover the cookie data and even potentially manipulate it. This can lead to the redirection of the user to a malicious site to steal information/data, or show the user false data.

SSL Certificate Expiration - When using an expired certificate, both encryption and authentication are at risk, resulting in both your website and users of your website being more susceptible to attacks and viruses.

BEAST Attack - Browser Exploit Against SSL/TLS (BEAST) is an attack that exploits network vulnerabilities that are using older cryptographic protocols to encrypt communications between the browser and a web server. Through the use of these old cryptographic protocols an attacker may be able to eavesdrop on these communications between a browser and the web server thus gathering information about a user.

BREACH Attack - The BREACH attack uncovers HTTPS secrets by attacking inbuilt HTTP data compression used by web servers. Much like above, it is a vulnerability that allows the recovery of information about a user.

For more information contact info@gridware.com.au
or call 1300 211 235