OWASP TOP 10 2017

10 Most Critical Web Security Risks of 2017

Made by Mehdi KERKAR & AbdelKarim YAHIAOUI

2017/2018

WHAT IS THE OWASP

WHAT IS THE OWASP

OWASP (Open Web Application Security Project) is an international organization. OWASP is an open community dedicated to enabling organizations to **conceive**, **develop**, **acquire**, **operate**, and **maintain** applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

What is the OWASP Top 10?

The **OWASP Top 10** is an awareness document for Web application security. The list represents a consensus among leading security experts regarding the greatest software risks for Web applications. These risks are based on the frequency of discovered security defects, the severity of the vulnerabilities, and the magnitude of their potential business impact. The OWASP Top 10 also has a variety of remediation guidelines encouraging developers to mitigate vulnerabilities and code defensively.

1

INJECTION

Allowing untrusted data to be sent as part of a command or query

INJECTION

WHAT IS IT?

Websites and apps occasionally need to run commands on the underlying database or operating system to add or delete data, execute a script, or start other apps. If unverified inputs are added to a command string or a database command, attackers can launch commands at will to take control of a server, device, or data.

HOW DOES IT WORK?

If a website, app, or device incorporates user input within a command, an attacker can insert a “payload” command directly into said input. If that input is not verified, an attacker then “injects” and runs their own commands.

WHY IS IT BAD?

Once attackers can make commands, they can control your website, apps, and data.

2

BROKEN AUTHENTICATION

Incorrectly implemented
authentication and session
management functions

BROKEN AUTHENTICATION

WHAT IS IT?

Authentication is the process for making sure it’s really you accessing your accounts and data. Generally, it’s facilitated by a username and password combination, but complexity is added when people forget or change their passwords or want to update their email addresses. It gets even more complex as a site, app, or device itself becomes bigger, broader, and more connected with other sites, apps, or devices.

HOW DOES IT WORK?

In the simplest attacks, passwords can be guessed or stolen if left unprotected. As complexities are added, attackers can find other areas where user credentials or sessions have inadequate protections and then hijack a user’s access, and eventually their data.

WHY IS IT BAD?

If attackers can hijack a user’s or administrator’s session, they have access to everything available within that account, from data to account control.

3

SENSITIVE DATA EXPOSURE

Many web technologies weren’t designed to handle financial or personal data transfers

SENSITIVE DATA EXPOSURE

WHAT IS IT?

Sensitive data, such as credit card numbers, health data, or passwords, should have extra protection given the potential of damage if it falls into the wrong hands. There are even regulations and standards designed to protect sensitive data. But, if sensitive data is stored, transmitted, or protected by inadequate methods, it can be exposed to attackers.

HOW DOES IT WORK?

If data is stored or transferred as plain text, if older/weaker encryption is used, or if data is decrypted carelessly, attackers can gain access and exploit the data.

WHY IS IT BAD?

Once an attacker has passwords and credit card numbers, they can do real damage.

4

XML ETERNAL ENTITIES

XML “entities” can be used to request local data or files

XML EXTERNAL ENTITIES

WHAT IS IT?

XML is a data format used to describe different data elements. XML also uses “entities” to help define related data, but entities can access remote or local content, as harmless as pulling a current stock price from a third party website. Entities can, however, be used to request local data or files, which could then be returned — even if that data was never intended for outside access.

HOW DOES IT WORK?

An attacker sends malicious data lookup values asking the site, device, or app to request and display data from a local file. If a developer uses a common or default filename in a common location, an attacker’s job is easy.

WHY IS IT BAD?

Attackers can gain access to any data stored locally, or can further pivot to attack other internal systems.

5

BROKEN ACCESS CONTROL

Improper enforcement of what authenticated users are allowed to do

BROKEN ACCESS CONTROL

WHAT IS IT?

Access control, or authorization, is how web apps let different users access different content, data, or functions. It’s kind of how Netflix limits people on their “standard” plan to HD content, while “premium” users can watch 4K. When it’s broken, you can access more than you should be able to.

HOW DOES IT WORK?

Sometimes, gaining unauthorized access is as simple as manually entering an unlinked URL in a browser, such as http://example.com/admin.

WHY IS IT BAD?

As with other vulnerabilities, attackers can gain access to (and modify) data, accounts, and functions that they shouldn’t.

6

SECURITY MISCONFIGURATION

Manual, ad hoc, insecure, or lack of security configurations that enable unauthorized access

SECURITY MISCONFIGURATION

WHAT IS IT?

Exactly what its name implies, security misconfiguration is when you've overlooked some vulnerabilities. This includes using default credentials, leaving files unprotected on public servers, having known-but-unpatched flaws, and more, and at any layer of the software stack. In other words, it's your fault.

HOW DOES IT WORK?

People get busy, things get missed, prioritization decisions are made... and vulnerabilities are left unchecked.

WHY IS IT BAD?

It makes it easy for even novice attackers to find and access your valuable systems and data. Luckily most of these types of vulnerabilities are also easy for you to find and fix.

7

CROSS-SITE SCRIPTING (XSS)

A web application includes untrusted data in a new web page without proper validation

CROSS-SITE SCRIPTINT (XSS)

WHAT IS IT?

XSS allows malicious code to be added to a web page or app, say via user comments or form submissions used to define the subsequent action. Since HTML mixes control statements, formatting, and the requested content into the web page’s source code, it allows an opportunity for unsanitized code to be used in the resulting page.

HOW DOES IT WORK?

When a web page or app utilizes user-entered content as part of a resulting page without checking for bad stuff, a malicious user could enter content that includes HTML entities.

WHY IS IT BAD?

Attackers can change the behavior of an app, direct data to their own systems, or corrupt or overwrite existing data.

8

INSECURE DESERIALIZATION

Receipt of hostile serialized objects resulting in remote code execution

INSECURE DESERIALIZATION

WHAT IS IT?

Before data is stored or transmitted, the bits are often serialized so that they can be later restored to the data's original structure. Reassembling a series of bits back into a file or object is called deserialization.

HOW DOES IT WORK?

Deserialized data can be modified to include malicious code, which is likely to cause issues if the application does not verify the data's source or contents before deserialization.

WHY IS IT BAD?

Attackers can build illegitimate objects that execute commands within an infected application.

9

USING COMPONENTS WITH KNOWN VULNERABILITIES

Finding and exploiting already-known vulnerabilities before they are fixed

USING COMPONENTS WITH KNOWN VULNERABILITIES

WHAT IS IT?

When vulnerabilities become known, vendors generally fix them with a patch or update. The process of updating the software eliminates or mitigates said vulnerability.

HOW DOES IT WORK?

Organizations sometimes fail to keep software up-to-date, especially if their stacks are large or complex, or if it would require a significant undertaking to validate their systems or products after an update. When an exploit is made public or a patch is released, attackers know some organizations will not act immediately. Attackers now have a window, from days to years, to search for systems or applications where the known vulnerability is still in place.

WHY IS IT BAD?

Because it’s public information, attackers have a recommended path to exploit and organizations have little excuse for leaving the path open.

10

INSUFFICIENT LOGGING & MONITORING

Insufficient monitoring allows attackers to work unnoticed

INSUFFICIENT LOGGING & MONITORING

WHAT IS IT?

If you're not looking for attackers or suspicious activities, you're not going to find them.

HOW DOES IT WORK?

Software and systems have monitoring abilities so organizations can see logins, transactions, traffic, and more. By monitoring for suspicious activity, such as failed logins, organizations can potentially see and stop suspicious activity.

WHY IS IT BAD?

Attackers rely on the lack of monitoring to exploit vulnerabilities before they're detected. Without monitoring and the logging to look back to see what happened, attackers can cause damage now and in the future.

MAKE THE INTERNET SAFER

References

- www.owasp.org
- www.hackerone.com

THANKS!

Any questions?