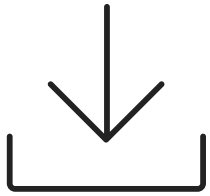
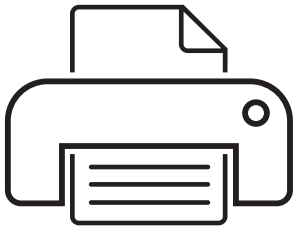
OWASP TOP 10 2017

Flashcard Guide on The 10 Most Critical Web Security Risks of 2017
One of the most effective security awareness training tools for your company.

With just 5 easy steps, you're ready to begin:



Step 1: Download



Step 2: File > Print

Step 3: Print 2-Sided

Step 4: Trim cards around edge

Step 5: Get learning!

hackerone

OWASP TOP 10 2017

A Flash Card Reference Guide to the
10 Most Critical Web Security Risks of 2017

hackerone

OWASP TOP 10 2017

1

INJECTION

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

hackerone

OWASP TOP 10 2017

2

BROKEN AUTHENTICATION

Incorrectly implemented
authentication and session
management functions

hackerone

OWASP TOP 10 2017

3

SENSITIVE DATA EXPOSURE

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

hackerone

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.

FUN FACTS

SQL injection was leveraged in the infamous Sony Pictures hack of 2014, when suspected North Korean operatives gained access to confidential data. According to US-CERT, the attackers used a Server Message Block Worm Tool to install several malicious components, including a backdoor and other destructive tools.

hackerone

LET'S MAKE THE INTERNET SAFER, TOGETHER.

There's no such thing as perfectly secure software. All software has vulnerabilities, and it's up to us to find and fix those vulnerabilities as quickly and efficiently as possible to mitigate the risk of exploitation.

The Open Web Application Security Project, is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

One of those projects, The OWASP Top Ten, provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The OWASP team recently released the 2017 revised and updated version of the ten most critical web application security risks and so we've created these flash cards for you, your friends, and your colleagues (especially product and engineering) to test your knowledge and learn more about these important issues.

Company-wide security awareness is a powerful way to improve the overall security of your organization. So adorn your waiting rooms, cubicles, and snack rooms with these flash cards for easy learning and remembrance.

Sincerely,
HackerOne

ABOUT HACKERONE

More than 1,000 organizations, including The U.S. Department of Defense, General Motors, Lufthansa and Starbucks trust HackerOne to find critical software vulnerabilities before criminals can exploit them. HackerOne customers have resolved more than 57,000 vulnerabilities and awarded more than $22M in bug bounties. To learn more, visit **www.hackerone.com**.

hackerone

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.

FUN FACTS

Wireless routers offer notoriously weak data protections. Researchers recently found that the cryptography protecting WPA2, the industry standard, exposes data and allows it to be read or manipulated as it's wirelessly transferred.

hackerone

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.

FUN FACTS

The simplest examples of this vulnerability are either storing user credentials without encryption or allowing them to be easily guessed. Other examples include using session IDs in the URL and enabling unreasonably long session timeouts.

hackerone

OWASP TOP 10 2017

4

XML ETERNAL ENTITIES

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

hackerone

OWASP TOP 10 2017

5

BROKEN ACCESS CONTROL

Improper enforcement of what authenticated users are allowed to do

hackerone

OWASP TOP 10 2017

6

SECURITY MISCONFIGURATION

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

hackerone

OWASP TOP 10 2017

7

CROSS-SITE SCRIPTING (XSS)

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

hackerone

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.

FUN FACTS

A web meeting platform, Fuze, enabled meeting access via a simple URL ending with an incrementing seven-digit number. Using any number provided access to replays of the corresponding meeting. Since the URLs were unprotected, the content was then indexed by – and searchable through – popular search engines.

hackerone

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.

FUN FACTS

The classic "billion laughs" attack exploits XXE by defining 10 elements that refer to each other, quickly exceeding any available memory and disrupting entire services.

hackerone

CROSS-SITE SCRIPTING (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.

FUN FACTS

XSS exploits have been reported for more than 20 years, and have impacted Twitter, Facebook, YouTube, and many, many others. It's showing no signs of waining, however, as both Adobe and WordPress patched XSS vulnerabilities as recently as November 2017.

hackerone

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.

FUN FACTS

The infamous Mirai botnet of 2016 relied on unchanged default credentials (such as a login of "admin" and a password of "1234") of just over 60 specific IoT devices. When exploited, it eventually infected nearly 400,000 units of just those 60 unprotected devices.

hackerone

OWASP TOP 10 2017

8

INSECURE DESERIALIZATION

Receipt of hostile serialized objects resulting in remote code execution

hackerone

OWASP TOP 10 2017

9

USING COMPONENTS WITH KNOWN VULNERABILITIES

Finding and exploiting already-known vulnerabilities before they are fixed

hackerone

OWASP TOP 10 2017

10

INSUFFICIENT LOGGING & MONITORING

Insufficient monitoring allows attackers to work unnoticed

hackerone

START UNCOVERING CRITICAL VULNERABILITIES TODAY

More security teams use HackerOne to manage vulnerability disclosure and bug bounty programs than any other platform.

GM · Lufthansa · European Commission · airbnb · Square · LendingClub · Google Play · New Relic · Nintendo · Adobe · coinbase · YAHOO! · slack · yelp

WWW.HACKERONE.COM / SALES@HACKERONE.COM / +1 (415) 891-0777

hackerone

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.

FUN FACTS

The former CEO of Equifax, while testifying to Congress regarding their infamous 2017 breach, blamed it on someone in IT, stating "The human error was that the individual who's responsible for communicating in the organization to apply the patch, did not."

hackerone

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.

FUN FACTS

During 2015 and 2016, insecure deserialization was found in so many Java applications, including one at PayPal, the wave of vulnerabilities was dubbed the "Java Deserialization Apocalypse".

hackerone

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.

FUN FACTS

Logging isn't just important for identifying attacks in progress; it can assist with the forensic analysis after an attack has succeeded.

hackerone