INDUSFACE™

UNDERSTANDING OWASP TOP 10 & WEB APPLICATION SECURITY

www.apptrana.indusface.com

This paper is written for readers who would like to understand Web Application Security through the lens of OWASP, learn about the common vulnerabilities as per OWASP and their security implication. The paper also talks about the security counter measures that AppTrana customers can avail to ensure they are protected from attacks against these vulnerabilities.

Web Application Security Basics & Why Is It Important

Web Application Security focuses on securing the web applications, web services and websites. It is different from information security in the sense that it focuses particularly on the vulnerabilities on the application code that is exposed to end users and available publically over the internet through http (80) or https (443) communication channels.

2016 was the record year of data breaches and there was a 40% increase from 2015 according to Identity Threat Resource center, most of the data breaches were because of the vulnerabilities in the web application layer. From the looks of it 2017 is no different. And most of these breaches were due to exploits of the vulnerabilities present in the application layer. As one can imagine, cost of these attacks is very high and at times insurmountable. Biggest risk of such attacks is the reputation risk. Customers would lose trust in the brand and it will be a PR nightmare. For example, In a survey it was found out that 87% of companies would not do business with a company which has faced a breach of credit/debit card details.

Generally, these attacks are sophisticated and targeted attacks aimed at gaining access to critical resources/data or to deny access to critical data/resources.

Most of the commonly used attacks are SQL injection, cross site scripting, denial of service, leakage, disclosure attacks.

Why do these hacks happen in spite huge investments by organization on security?

In spite of continuous focus on security by organizations, theses breaches continue to happen because of lack of understanding of application security and/or lack of adequate tools to protect them. Most organizations do not have the expertise or the resources to spend time understanding their web application risk posture and how they can protect them. But hackers do! Hackers are generally well equipped to study the security posture of the application, find the weakest link and exploit them through sophisticated attack.

To build the best defense for your application, it is paramount to understand the risk posture of your application and OWASP Top 10 is ideal place to start covering your bases. In the rest of the paper, we will be discussing about OWASP Top 10 vulnerabilities, how attackers can exploit them and what AppTrana can do to protect against attacks exploiting these vulnerabilities.

What Is OWSAP and OWASP Top 10

Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Their mission is to make software security visible, so that individuals and organizations are able to make informed decisions. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security. They publish a ranking of the 10 most-critical web application security flaws, which are known as the OWASP Top 10.

The OWASP Top 10 represents a broad consensus of the most-critical web application security flaws. It's a widely accepted methodology for evaluating web application security and build mitigation strategies for websites and web-based applications. It outlines the top 10 areas where web applications are susceptible to attacks, and where common vulnerabilities are found in such workloads.

Last OWASP Top 10 was released on 2013 and new RC1 candidate was released on 2017. Final version is expected by Nov 2017.

About AppTrana and How It Is Different

AppTrana is a complete security as a service solution which helps you identify vulnerabilities in your application and protect against them immediately through virtual patching at WAF layer.

General cloud security solutions, takes a cookie cutter approach when it comes to WAF. They provide default set of rules that can be applied and then ask website owners to create/tweak the rules to meet their application need. The problem with this approach is

- With just default rules and no knowledge of vulnerability, the security is weak.
- Default rules will create false positives and tweaking it is time consuming
- Creating own custom rules are complex and requires expertise.

Due to these reasons over time, WAF solution becomes ineffective as organizations do not have time and expertise to maintain the rules.

We at AppTrana approach the problem differently. We believe, security of the application is best handled by experts and our experts fine-tune the rules based on the application need to avoid false positives and ensure that your application remain secure round the clock. Our integrated solution of scanner and WAF helps, you detect the vulnerabilities in your site and protect them immediately through custom made rules which assures zero false positive

Let's dig deeper into OWASP Top 10 vulnerabilities and its protection through AppTrana.

OWASP TOP 10 Vulnerability

In April 2017, OWASP released new set of OWASP Top 10. This was a RC candidate which is not yet finalized. Final version will be released by Nov 2017. As per the April release, the top vulnerabilities that organizations should be worried about are

A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Broken Access Control (NEW)

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Insufficient Attack Protection (NEW)

A8 Cross-Site Request Forgery (CSRF)

A9 Using Components with Known Vulnerabilities

A10 Under protected APIs (NEW)

With AppTrana, you will be able to detect if your application is vulnerable in any of these areas and also ensure you are protected from any exploits immediately.

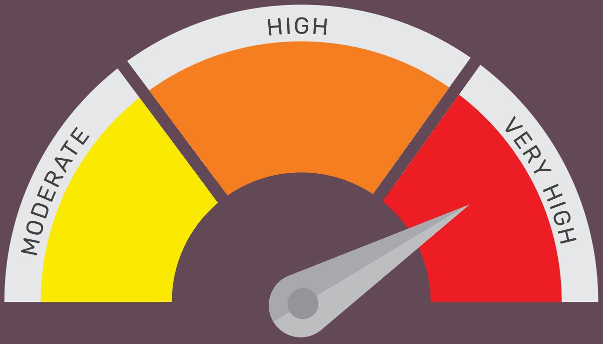
A1 Injection

What is it

Imagine a hacker coming to your account login page and entering a string of code. The command gets accepted and allows them to login without even a valid account or password. This is an injection attack. and SQL Injection is the most common attack in this category.

Websites that do not filter inputs and accept everything a user enters, are at a huge risk. Hackers can use commands to enter through this weakness and access server files. Injection attacks can happen from any input field, including the comments section.

Impact



What are the risks

Think of the infinite possibilities when hackers have a direct way of interacting with your server. They can steal data, change it, delete it, deny access, and much more. In fact, injection attacks are responsible for some of the major data breaches last year.

How can Apptrana help

AppTrana with its advance and premium scans can help you detect all the vulnerabilities. Premium scans are only available as part of our premium offering where our experts to manual grey box pen-testing to identify vulnerabilities in your site.

When it comes to protection AppTrana takes a multi-prong approach. It provides certain set of advance rules created by experts which we feel is error free and won't have any false positives most of the workloads.

Apart from it, there are rules which are experiential in nature which may cause false positives, these rules will be monitored by our experts and moved to block mode after fine-tuning. This is available only as part of the premium plan.

Also, our experts can create custom rules on request based on the application when any specific vulnerabilities are found which is not protected by the prewritten rules.

The complete competency matrix of AppTrana when it comes to Injection is as follows

OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A1 Injection						
	Test for SQL Injection	Yes	Yes	Yes	Yes	Yes
	Test for LDAP Injection	Yes	Yes			Yes
	Test for ORM Injection	Yes		Yes	Yes	
	Test for XML Injection	Yes				Yes
	Test for SSI Injection	Yes		Yes	Yes	Yes
	Test for XPath Injection	Yes	Yes	Yes	Yes	Yes
	Test for IMAP/SMTP Injection	Yes				Partial*
	Test for Code Injection	Yes	Yes	Yes	Yes	Yes
	Test for Command Injection	Yes	Yes	Yes	Yes	Yes
	Test for Buffer Overflow	On Request				

*Vulnerabilities are application specific and capability of virtual patching through custom rules is limited. Custom rules will be created by experts on request if vulnerability is detected. This will reduce the risk exposure but will not eliminate it.

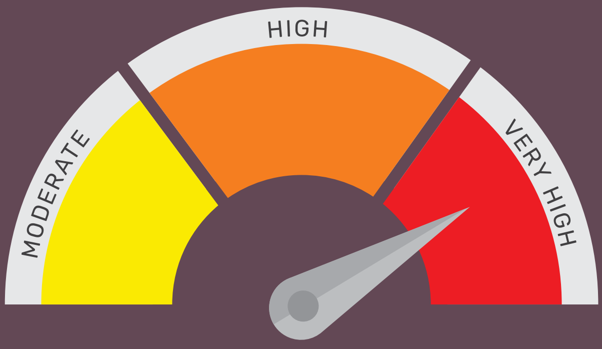
Note that buffer overflow checks are only done on request after customer approval.

A2 Broken Authentication & Session Management

What is it

“Incorrect Password” error messages are a classic example of this type of vulnerability. If a hacker tries a random combination of Username-Password and an error message tells them that the password is incorrect, he knows that at least the username is correct. A brute force attacker now knows that an account exists and he only needs the right password. There are dozens of automated tools from the dark web that can try millions of password combinations for a hacker. Improper sessions management is also a severe risk. Think of an online bank account that keeps you logged in even after closing the browser.

Impact



What are the risks

Such vulnerabilities allow attackers to earn complete account access. In severe cases, hackers have stolen database records and sold them on the underground black market.

How can Apptrana help

Since these vulnerabilities are application specific, automated scans have limited scope but all the vulnerabilities can be detected through AppTrana’s premium scans.

When it comes to protection, Session management and authentication vulnerability leads to unauthorized access and it becomes hard for WAF layer to distinguish between valid request which are properly authenticated and requests which uses stolen identity. In such cases AppTrana takes a reactive approach and helps you block requests once you know that there has been a compromise. You could choose to blacklist certain identities or if you know the token, you can request a custom rule to block access for the token temporarily or permanently.

Apart from that some of the vulnerabilities can be completely or partially patched through custom rules. You can request the rule, if the scanner finds any of these vulnerabilities on your site.

The complete competency matrix of AppTrana when it comes to broken authentication & session management is as follows

OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A2 Broken Authentication and Session Management						
	Test Role Definitions	Yes		Proper role definition must be done on application. Out of scope of WAF		
	Test User Registration Process	Yes		Registration process can only be improved in Application. WAF can be used to block on identity. Preventing malicious users registering multiple times		
	Test Account Provisioning Process	Yes		Process improvements needed. Out of scope of WAF		
	Test for Account Enumeration and Guessable User Account	Yes				Partial*
	Test for Weak or unenforced username policy	Yes				Yes
	Test for Credentials Transported over an Encrypted Channel	Yes	Yes	Encryption should be enforced at application. Out of scope of WAF		
	Test for default credentials	Yes		Strong password enforcement should happen at code level. Out of scope of WAF		
	Test for Weak lock out mechanism	Yes				Yes
	Test for Bypassing Authentication Schema	Yes		Strong authentication enforcement should happen at code level. Out of scope of WAF		
	Test for Vulnerable Remember Password	Yes				
	Test for Browser cache weakness	Yes				
	Test for Weak password policy	Yes				
	Test for Weak security question/answer	Yes				
	Test for weak password change or reset functionalities	Yes				
	Test for Weaker authentication in alternative channel	Yes				
	Test for Bypassing Authorization Schema	Yes				
	Test for Privilege escalation	Yes				Partial*
	Test for Session Management Schema	Yes				Partial*
	Test for cookies attributes	Yes	Yes			Yes
	Test for Session Fixation	Yes				Partial*
	Test for Exposed Session Variables	Yes	Yes			Partial*
	Test for logout functionality	Yes		Can be fixed only at the code level. Out of scope of WAF		
	Test Session Timeout	Yes				
	Test for Session puzzling	Yes				

*Vulnerabilities are application specific and capability of virtual patching through custom rules is limited. Custom rules will be created by experts on request if vulnerability is detected. This will reduce the risk exposure but will not eliminate it.

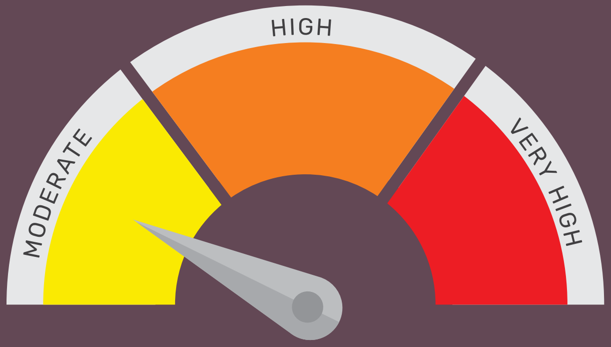
A3 Cross-Site Scripting (XSS)

What is it

An attacker can inject malicious scripts into trusted websites and use this code to hijack browser sessions from users to initiate a man-in-the-middle attack.

The attacker can send anything to your server now while simultaneously redirecting users to dark parts of the web without them knowing about it. Such attacks can trouble your customers and business equally.

Impact



What are the risks

Hackers can deface your website, inject malware, phishing links and hijack user accounts.

How can Apptrana help

Both the Automated scans and Premium scans of AppTrana can detect these vulnerabilities and they can be readily blocked by Advanced, premium rules which AppTrana provide.

In case of application specific vulnerability which is not covered by the pre-written rules, you can request a custom rule which will be written by our experts.

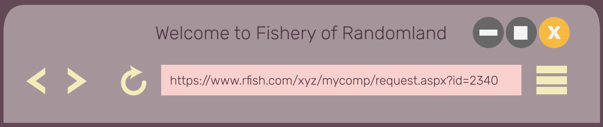
The complete competency matrix of AppTrana when it comes to Cross-Site Scripting (XSS) is as follows

OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A3 Cross-Site Scripting (XSS)						
	Test for Reflected Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for Stored Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for DOM-based Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for JavaScript Execution	Yes		Yes	Yes	Yes
	Test for HTML Injection	Yes	Yes	Yes	Yes	Yes
	Test for Cross site flashing	Yes		Yes	Yes	Yes
	XSS Filter Evasion Cheat Sheet	Yes	Yes	Yes	Yes	Yes

A4 Broken Access Control

What is it

In the latest version of OWASP Top 10, A4 represents two vulnerabilities from the previous list (2003 A4 & A7) combined into one. In the latest version of OWASP Top 10, A4 represents two vulnerabilities from the previous list (2003 A4 & A7) combined into one.

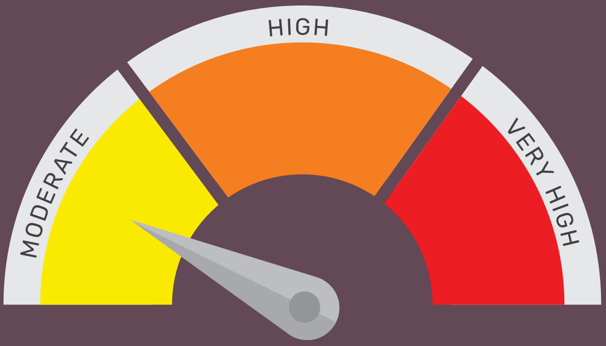

Welcome to Fishery of Randomland

https://www.rfish.com/xyz/mycomp/request.aspx?id=2340

Now if you change the digits '2340' to another set of digits allows you to view the account of another user, it's a huge opportunity for hackers.

The threat also arises when non-privileged users have access to admin privileges. After all, a junior-level developer should not be able to gain admin access to the server. Unfortunately, most companies do not bother ensuring that only authorized accounts access privileged information.

Impact



What are the risks

Such vulnerabilities lead to loss of data, ghost account creation and admin account hijacking.

How can Apptrana help

Both the Automated scans and Premium scans of AppTrana cover for this vulnerability and they can be readily blocked by Advanced, premium rules which AppTrana provide.

In case of application specific vulnerability which is not covered by the pre-written rules, you can request a custom rule which will be written by our experts.

The complete competency matrix of AppTrana when it comes to Broken Access Control is as follows

OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A4 Broken Access Control						
	Test Directory traversal/file include	Yes	Yes	Yes	Yes	Yes
	Test for Insecure Direct Object References	Yes	Yes			Partial*
	Test for Local File Inclusion	Yes	Yes	Yes	Yes	Yes
	Test for Remote File Inclusion	Yes		Yes	Yes	Yes
	Test for Bypassing Authorization Schema	Yes		Authorization process can only be improved in Application. WAF can be used to block on identity, preventing malicious users gaining access to unauthorized resources		
	Test for Bypassing Authentication Schema	Yes				

*Vulnerabilities are application specific and capability of virtual patching through custom rules is limited. Custom rules will be created by experts on request if vulnerability is detected. This will reduce the risk exposure but will not eliminate it.

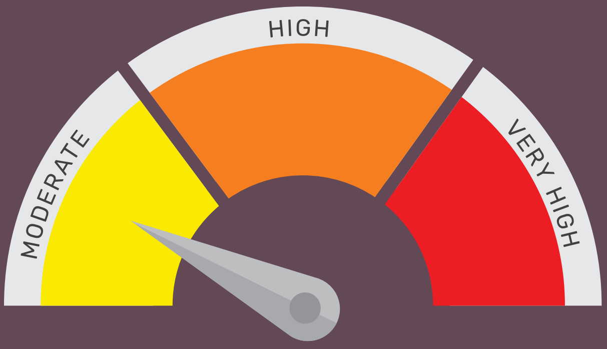
A5 Security Misconfiguration

What is it

Old sample apps, expired yet active features, default system passwords... hackers love all the additional information they can get. This vulnerability is about all of these loopholes.

Attackers look for small issues, combine them, and try to make something big out of them. They use default accounts, unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system

Impact



What are the risks

A5 can lead to complete loss of data through alteration, deletion and theft. Recovery is costly and highly unreliable, especially if the data gets encrypted.

How can Apptrana help

Since these vulnerabilities are regarding server configurations and at infra level, WAF can be used for mitigation purpose for most cases. Custom rule can be written to avoid some issues like banner grapping to find server info and the like, but in most cases the patching must be done only at application. If the pattern of exploit is known based on the vulnerability, then custom rules can be written to block them.

AppTrana's premium scan and automated scan will find most of this type of vulnerability

The complete competency matrix of AppTrana when it comes to Security Misconfiguration is as follows

OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A5 Security Misconfiguration						
	Fingerprint Web Server	Yes	Yes			Yes
	Fingerprint Web Application Framework	Yes	Yes			Yes
	Fingerprint Web Application	Yes	Yes			Yes
	Test Network/Infrastructure Configuration	Yes		Can be fixed only at Infra level. Out of Scope of WAF		
	Test Application Platform Configuration	Yes		Can be fixed only at Infra level. Out of Scope of WAF		
	Test File Extensions Handling for Sensitive Information	Yes				Partially*
	Review Old, Backup and Unreferenced Files for Sensitive Information	Yes				Partially*
	Enumerate Infrastructure and Application Admin Interfaces	Yes	Yes			Partially*
	Test HTTP Methods	Yes	Yes	Yes	Yes	Yes
	Test RIA cross domain policy	Yes	Yes	NA		Partially*
	Test for Error Code	Yes	Yes			Yes
	Test for Stack Traces	Yes	Yes			Yes

*Vulnerabilities are application specific and capability of virtual patching through custom rules is limited. Custom rules will be created by experts on request if vulnerability is detected. This will reduce the risk exposure but will not eliminate it.

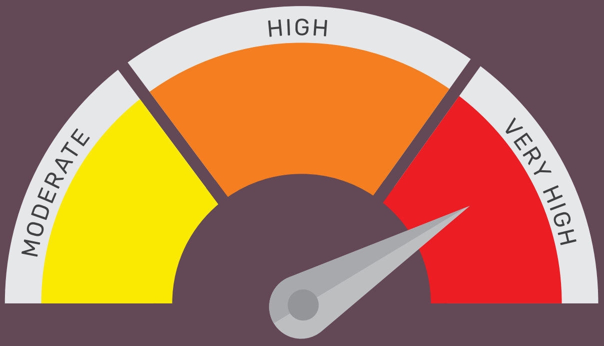
A6 Sensative Data Exposure

What is it

If somehow your application is breached, how easy is it for hackers to find the data that they want?

Consider database files, backups, financial transaction details, employment history and every piece of internal and external information. Don't store sensitive data unnecessarily and Discard it as soon as possible. If you have something, keep it encrypted.

Impact



What are the risks

Consider everything that comes with the loss of sensitive data. Loss of passwords, credit card information, addresses and bank statements bring serious repercussions in real-world scenarios.

How can Apptrana help

AppTrana can be effectively used to detect the vulnerability. Both Automated and Premium scans have test cases which will help find the vulnerability but since the vulnerability is around strong encryption, it is outside the scope of WAF and it is best to fix the vulnerability in the application itself.

The complete competency matrix of AppTrana when it comes to Sensative Data Exposure is as follows

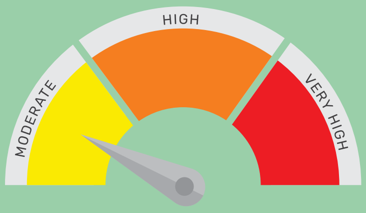
OWASP Top 10 Vul 2017	Tests Recommended by OWASP	Detection Coverage		Protection Coverager		
		Premium Scans	Automated Scans	Advance Rules	Premium Rules	Custom Rules
A6 Sensative Data Exposure						
	Test for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection	Yes	Yes	Stronger Encryption can be enforced only in Application level. Out of scope of WAF. WAF can be used to block users based on identity, so that malicious users do not take advantage of vulnerability		
	Test for Padding Oracle	Yes	Yes			
	Test for Sensitive information sent via unencrypted channels	Yes	Yes			
	Test HTTP Strict Transport Security	Yes				
	Test for Credentials Transported over an Encrypted Channel	Yes	Yes			

A7 Insufficient Attack Protection (New)

What is it

This newest addition to this year's OWASP 10 asks a powerful question; Does your application detect and respond to both manual and automated attacks? Can it patch itself to ward off attackers in real-time? Your applications and APIs might be sanitizing inputs or rejecting wrong passwords, but can they reject automated inputs? If there is a critical vulnerability discovered, how soon can you patch it?

Impact



What are the risks

Attackers can use automated tools to send botnet and find out types of vulnerabilities in an application. Successful attempts lead to Injection and XSS exploits.

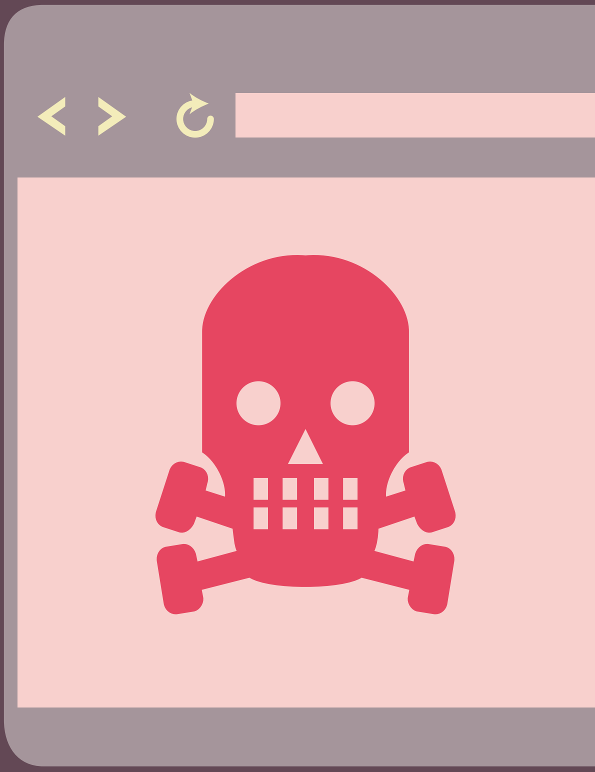
How can AppTrana help

Since AppTrana has inbuilt WAF, this vulnerability is not applicable. You will be able to react to new attacks quickly. Custom rules can be written by experts and deployed quickly without any trouble.

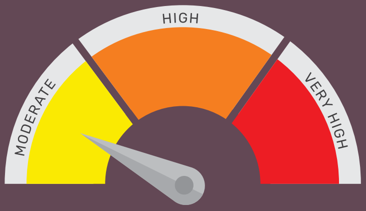
A8 Cross-Site Request Forgery (CSRF)

What is it

A compromised browser session is hijacked by a hacker to run rogue commands in a web application using CSRF. With a little help from phishing techniques (email or chat links), hackers trick users into changing email addresses, wiring money, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.



Impact



What are the risks

Rogue requests, fraudulent purchases, and money transfers - you will never be sure if it's a genuine request and customers will gradually lose trust in your website and brand.

How can AppTrana help

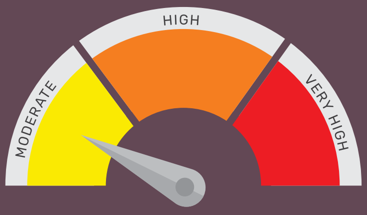
CSRF attacks are application specific and scope of automated scans are limited. These vulnerabilities can be discovered through AppTrana's premium scan. For protection, our security experts will be able to write customized rules to patch these vulnerabilities virtually depending on application need.

A9 Using Components with Known Vulnerabilities

What is it

Unknown chunks of code breed mysterious vulnerabilities. Developers use open source projects and often they don't even know what code library it came from where and with what vulnerability. Such components can weaken any application.

Impact



What are the risks

Unknown application codes bring unknown risks. XSS, injection risks, and business logic loopholes are just some of the examples. Such vulnerabilities might cause data breach, access control, defacement, and theft.

How can AppTrana help

This again being vulnerabilities on application logic, these vulnerabilities can be discovered through AppTrana's premium scan.

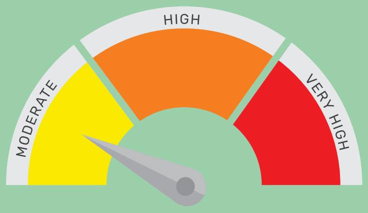
For protection, our security experts will be able to write customized rules to patch these vulnerabilities virtually depending on application need in certain cases. They can avoid banner grabbing and prevent exploit but will not be exhaustive.

A10 Underprotected APIs (New)

What is it

Most browser web applications are written in JavaScript and use APIs to get data but these APIs often contain numerous vulnerabilities. Attackers can reverse engineer the code or monitor the communication between browser and API with a tool to find vulnerabilities and to exploit them. Moreover, the architecture of most APIs is so complex that they require continuous automated testing and thorough penetration testing to find deep-seeded vulnerabilities.

Impact



What are the risks

The compromise risks everything an exploited API accesses. This type of attack can be used to steal information, send phishing emails, delete data, and so forth.

How can AppTrana help

Again, a business logic vulnerability this could only be identified readily through AppTrana's premium scan. Our security experts will be able to write customized rules to patch these vulnerabilities virtually depending on application need in certain cases.

Hope you have enough knowledge about Web Application Security and OWASP Top 10 vulnerabilities and are convinced that you should act now.!

Start securing your application for free. Try out our free trial by Clicking here.

Trust you have enough knowledge about Web Application Security and OWASP Top 10 vulnerabilities and are convinced that you should act now.

Start securing your applications for free.
Try out our free trial

Request a Free Trial of AppTrana

About Indusface

Indusface is an award-winning application security leader protecting 900+ customers across 17 countries. Our security products have been mentioned in the Gartner Magic Quadrants for Application Security Testing and Web Application Firewall, and have won all major startup awards in the last 12 months. Indusface TAS is available On-premise, As A Service and through the AWS Marketplace.

VADODARA BENGALURU MUMBAI NEW DELHI SAN FRANCISCO