Top 10 use cases for reCAPTCHA Enterprise to defend against OWASP Web-Automated Attacks

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Google Cloud

Introduction

How you can use reCAPTCHA Enterprise to protect your websites from some of OWASP's most challenging web-automated attacks.

The threat landscape is changing as more businesses require that their customers have user accounts and login credentials to make purchases. According to a report by the Akrose Lab, about 73% of fraud and abuse cases were logins, and 19% of fraud and abuse were account registrations[1].

Fraudsters know that if they can take over a legitimate customer's account and blend in with normal customer traffic patterns, they can commit a wide variety of fraudulent activities and damage your business' brand and bottom line.

In the OWASP Automated Threat Handbook Web Applications Version 1.2, the handbook describes several threats that can target your web applications as a result of malicious web automation. In our handbook, we explore what we believe to be the top ten OWASP threats and how our solution, reCAPTCHA Enterprise, can help protect your business.

reCAPTCHA Enterprise helps protect your website from fraudulent activity, spam, and abuse. It was inspired by reCAPTCHA, a product that has been defending millions of websites for over a decade. reCAPTCHA Enterprise is a frictionless fraud detection service that can be installed on any web page. It was designed with the enterprise in mind and provides security teams several features, such as extra granular scores, reason codes for high-risk scores, and the ability to tune the risk analysis engine to your site's specific needs.

In the upcoming pages, we'll explore these OWASP-selected threats: account creation, carding, card cracking, cashing out, credential stuffing, denial of inventory, scalping, skewing, spamming, and token cracking. We'll define these threats and explain how they work and the tactics and techniques reCAPTCHA Enterprise used to stop them.

[1] Arkose Lab Fraud & Abuse report Q4 2019

All OWASP definitions, industries impacted, personnel impacted, what types of data are misused, how it works, and possible signs information in this report are courtesy of OWASP Automated Threat Handbook Web Applications Version 1.2. You can find the report here.

Account Creation

OWASP definition: Create multiple accounts for subsequent misuse.

Industries impacted:

- Education
- Entertainment
- Financial
- Retail
- Social Networking

Personnel impacted: Application owner

What types of data is misused: Authentication credentials and other business data

How it works: Bulk account creation, and sometimes profile population, uses the application's account sign-up processes. The accounts are subsequently misused for generating content spam, laundering cash and goods, spreading malware, affecting reputation, causing mischief, and skewing Search Engine Optimisation (SEO), reviews and surveys.

reCAPTCHA Enterprise engineering team's analysis: This attack is when a bad actor makes fake accounts to perform abuse such as fake posts, phishing, and money laundering. reCAPTCHA Enterprise uses an adaptive risk analysis engine to keep automated software from engaging in abusive activities on your site. With technology that has helped defend millions of websites for over a decade, reCAPTCHA Enterprise is built to help mitigate fraudulent online activity for your enterprise.

Possible signs for account creation:

- Higher than average account creation rate
- Accounts with incomplete information relative to the typical account holders
- Accounts created, but are not used immediately
- Accounts created with disproportionate use

Google Cloud

Carding

OWASP definition: Multiple payment authorization attempts used to verify the validity of bulk stolen payment card data.

Industries impacted:

- Entertainment
- Retail

Personnel impacted:

- End users
- Application owner
- Third parties

What type of data is misused: Payment cardholder data

How it works: Credit and/or debit card data are tested against a merchant's payment processes to identify valid card details. The quality of stolen data is often unknown, and carding is used to identify good data of higher value. Payment cardholder data may have been stolen from another application, stolen from a different payment channel, or acquired from a criminal marketplace.

reCAPTCHA Enterprise engineering team's analysis: We recommend adding reCAPTCHA Enterprise to your website for every single payment event. Examples of this include new and/or infrequent customers, smaller checkout baskets, or users that appear to have skipped directly to payment. With reCAPTCHA Enterprise running, you'll receive a score based on interactions with your websites, with 1.0 being a likely good interaction and 0.0 being a likely abusive action, so you can take action against carding.

Possible signs of carding:

- Elevated basket abandonment
- Reduced average basket price
- Higher proportion of failed payment authorizations
- Disproportionate use of the payment step
- Increased charge backs
- Multiple failed payment authorizations from the same user and/or IP address and/or user agent and/or session and/or device ID/fingerprint

Google Cloud

Card Cracking

OWASP definition: Identify missing start/expiry dates and security codes for stolen payment card data by trying different values.

Industries impacted: Retail

Personnel impacted:
- Many end users
- Application owner
- Third parties

What types of data are misused: Payment cardholder data

How it works: Brute force attacks go after the application payment card processes to identify the missing values for start date and card validation code (CVC).

reCAPTCHA Enterprise engineering team's analysis: Fraudsters often use automated tools to verify stolen credit cards before they're either sold or used. reCAPTCHA uses machine learning to recognize the patterns of legitimate and fraudulent transactions in order to detect this type of abuse. In doing so, it can reduce the transaction costs of such abuse as well as preventing larger scale attacks resulting from the use of stolen payment mechanisms. This is done through behavioral analysis that uses site-specific training and models. reCAPTCHA Enterprise will detect malicious requests and give you actionable insights to help protect your enterprise. reCAPTCHA Enterprise returns a score based on interactions with your websites, with 1.0 being a likely good interaction and 0.0 being a likely abusive action.

reCAPTCHA Enterprise uses machine learning to recognize the patterns of legitimate and fraudulent transactions.

Possible signs of card cracking:

- Elevated basket abandonment
- Higher proportion of failed payment authorisations
- Disproportionate use of the payment step
- Reduced average basket price
- Increased chargebacks

Cashing Out

OWASP definition: Buy goods or obtain cash utilising validated stolen payment card or other user account data.

Industries impacted:
- Entertainment
- Financial
- Government

Personnel impacted:
- Many users
- Application owner
- Third parties

What types of data are misused:
- Authentication credentials
- Payment cardholder sets
- Other financial data

How it works: Bots obtain currency or higher-value merchandise via the application using stolen, previously validated payment cards, or other account login credentials. Cashing Out sometimes may be undertaken in conjunction with product return fraud. For financial transactions, this is usually a transfer of funds to a mule's account. The refunding of payments via non-financial applications (e.g. tax refunds, claims payment) is also included in Cashing Out.

reCAPTCHA Enterprise engineering team's analysis: Cybercriminals attack a financial institution or payment processor by installing malware and exploiting network access in order to acquire customer debit or card account information. This not only costs your business time and money, but it also provides an avenue for organized crime to use their credit card databases on your site. reCAPTCHA Enterprise returns a score based on interactions with your websites, with 1.0 being a likely good interaction and 0.0 being a likely abusive action. This way you know if your site is a target for cashing out and can stop bots and other automated attacks while approving valid users for payment.

Possible signs of cashing out:

- Increased chargebacks
- Increased usage of interlinked accounts
- Increased demand for higher-value goods or services
- Same or similar accounts for both "buyer" and "seller" in sites that facilitate consumer-to-consumer (C2C) commerce
- Increased demand for a single supplier's goods or services

Credential Stuffing

OWASP definition: Mass login attempts used to verify the validity of stolen username/password pairs.

Industries impacted:

- Entertainment
- Financial
- Government
- Retail
- Social Networking

Personnel impacted:

- Many end users
- Application owner

What type of data is misused: Authentication credentials

How it works: Bots list authentication credentials stolen from elsewhere and are tested against the application's authentication mechanisms to identify whether users have re-used the same login credentials. The stolen usernames (often email addresses) and password pairs could have been sourced directly from another application by the attacker, purchased in a criminal marketplace, or obtained from publicly available breach data dumps.

reCAPTCHA Enterprise engineering team's analysis: Credential stuffing has become one of the most commonly used attack vectors. The use of credential stuffing has spiked due to the availability of usernames and passwords from a wide range of successful breaches and the ease of scripting the attacks. The stolen user data used in these attacks is readily available. The information is often posted and sold online.

Poor password hygiene is the main reason why this attack method is so successful. The most common username is your email address. Remembering unique passwords for every website is too much for most end users to handle. This leads them to using the same password for every site. Once one site is compromised, it's only a matter of time before a successful login will be realized by an attack using credential stuffing.

reCAPTCHA Enterprise is able to successfully detect and stop credential stuffing attacks by recognizing the bot behavior and introducing bot friction. This friction can alert to an attack and responses can be employed to defeat the attempt while letting valid users through the website.

Resources that are impacted:

- IP enabled door bells
- Home video surveillance systems
- eCommerce systems

Denial of Inventory

OWASP definition: Deplete goods or services stock without ever completing the purchase or committing to the transaction.

Industries impacted:

- Education
- Entertainment
- Financial
- Government
- Health
- Retail
- Technology

Personnel impacted:

- Few individual users
- Application owner
- Society

How it works: Selection and holding of items from a limited inventory or stock, but which are never actually bought, or paid for, or confirmed, such that other users are unable to buy/ pay/confirm the items themselves. Denial of Inventory is most commonly thought of as taking ecommerce items out of circulation by adding many of them to a cart/basket. The attacker never actually proceeds to checkout to buy them but contributes to a possible stock-out condition. A variation of this automated threat event is making reservations and/or click-and-collect without payment. Denial of Inventory reduces the availability of goods or services.

reCAPTCHA Enterprise engineering team's analysis: reCAPTCHA Enterprise works by using advanced risk analysis strategies to distinguish legitimate inventory purchases from fake ones. It provides security teams with several features, including extra granular risk scores, reason codes for high-risk scores, and the ability to tune the risk analysis engine to your site's specific needs. For example, any action can have a fraud risk score attached to it which can inform your team of suspicious activity and help you combat denial of inventory attacks.

Possible signs of denial of inventory:

- Inventory balances reduce quickly
- Increased stock held in baskets or reservations
- Elevated basket abandonment
- Reduced use of payment step
- Increasing complaints from users being unable to obtain goods/services

Scalping

OWASP definition: Obtain limited-availability and/or preferred goods/services by unfair methods.

Industries impacted:

- Entertainment
- Financial
- Retail

Personnel impacted:

- Many users
- Application owner

How it works: Acquisition of goods or services using the application in a manner that a normal user would be unable to undertake manually. Although Scalping may include monitoring availability of the goods or services, and then rapid action to beat normal users to obtain these, Scalping is not a "last minute" action. This is because Scalping includes the additional concept of limited availability of sought-after goods or services, and is most well known in the ticketing business where the tickets acquired are then resold later at a profit by the scalpers/touts.

reCAPTCHA Enterprise engineering team's analysis: reCAPTCHA Enterprise is a frictionless fraud detection service that leverages our experience from more than a decade of defending the internet and data for our network of four million sites. It can be installed on any web page at the point of action—such as the purchase page—to help detect and prevent fraud. Meanwhile, legitimate users will be able to make purchases or view pages and fake users will be blocked.

Possible signs of scalping:

- High peaks of traffic for certain limited-availability goods or services
- Increased circulation of limited goods reselling on secondary market

Skewing

OWASP definition: Repeated link clicks, page requests or form submissions intended to alter some metric.

Industries impacted:

- Education
- Entertainment
- Financial
- Government
- Health
- Retail
- Technology
- Social Networking

Personnel impacted:

- Few individuals users
- Many users
- Application owner
- Third parties
- Society

What types of data are common misused:

- Other personal data
- Other business data
- Public information

Description: Automated repeated clicking or requesting or submitting content, affecting application-based metrics such as counts and measures of frequency and/or rate. The metric or measurement may be visible to users or hidden. Metrics may affect individuals as well as the application owner, e.g. user reputation, influence others, gain fame, or undermine someone else's reputation.

reCAPTCHA engineering team's analysis: reCAPTCHA Enterprise uses an adaptive risk analysis engine to keep automated software from engaging in abusive activities on your site. With technology that has helped defend millions of websites for over a decade, reCAPTCHA Enterprise is built to help mitigate fraudulent online activity for your enterprise.

Possible signs of skewing:

- Decreased click/impression to outcome ratio
- Unexpected or unexplained changes to a metric
- Metric significantly different to accepted sector norms
- Increased costs/awards that are determined from an application metric or metrics

Spamming

OWASP definition: Malicious or questionable information addition that appears in public or private content, databases or user messages.

Applicable sectors:

- Entertainment
- Retail
- Social networking

Personnel impacted:

- Few individual users
- Many users
- Application owner
- Third parties
- Society

What types of data are misused:

- Other business data
- Public information

How it works: Malicious content can include malware, IFRAME distribution, photographs & videos, advertisements, referrer spam and tracking/ surveillance code. The content might be less overtly malicious but be an attempt to cause mischief, undertake search engine optimisation (SEO) or to dilute/hide other posts. The mass abuse of broken form-to-email and form-to-SMS functions to send messages to unintended recipients is not included in this threat event, or any other in this ontology, since those are considered to be the exploitation of implementation flaws alone.

reCAPTCHA Enterprise engineering team's analysis: reCAPTCHA Enterprise uses an adaptive risk analysis engine to keep malicious software from engaging in abusive activities on your site. With technology that has helped defend millions of websites for over a decade, reCAPTCHA Enterprise is built to help mitigate fraudulent online activity for your enterprise.

Possible signs of spamming:

- Increase in the rejection rate of user-generated content by moderation processes
- Higher rate of complaints from users about spam content
- High appearance of typically fraudulent keyword in user-generated content High hyperlink density
- Inclusion of hyperlinks to web hosts that redirect, or with low reputation, or that host malicious content directly
- Requests from source IP addresses, devices, fingerprints that appear on spam lists

Token Cracking / Coupon Fraud

OWASP definition: Mass enumeration of coupon numbers, voucher codes, discount tokens, etc.

Impacted industries:

- Entertainment
- Financial
- Retail

Personnel impacted: Application owner

What type of data is misused: Other business data

Description: Identification of valid token codes providing some form of user benefit within the application. The benefit may be a cash alternative, a non-cash credit, a discount, or an opportunity such as access to a limited offer.

reCAPTCHA Enterprise engineering team's analysis: The reCAPTCHA Enterprise service helps you detect abusive traffic on your website without any user friction. Using a score-based detection system, you can rest assured that your countermeasures rely on detailed data about online activity in order to stop bots and other automated attacks while letting valid users in.

Possible signs of token cracking:

- Multiple failed token attempts from the same user and/or IP address and/or User Agent and/or device ID/fingerprint
- High number of failed token attempts