CYBER PUBLIC SCHOOL

OTP and CAPTCHA Bypass Methods

https://cyberpublicschool.com/

What is OTP?

A One Time Password or OTP is a string of characters or numbers automatically generated to be used for one single login attempt. One Time Passwords will minimize the risk of fraudulent login attempts and thus the risk of stolen data. An OTP is more secure than a static password, especially a user-created password, which can be weak and reused across multiple accounts.

The OTP feature prevents some forms of identity theft by making sure that a captured username/password pair cannot be used a second time. Typically, the user's login name stays the same, and the one-time password changes with each login. One-time passwords (aka One-time passcodes) are a form of strong authentication, providing much better protection to eBanking, corporate networks, and other systems containing sensitive data.

One Time Password Examples

One Time Password as SMS Message

Originally, most OTPs were sent as SMS messages. Once the user has begun his login attempt, filling in his username and the correct password, an SMS OTP is sent to the mobile number connected to his account. The user then enters this code shown on this phone in the login screen, completing the authentication process.

One Time Password as Voice Message

An alternative to a One Time Password via SMS is Voice. With Voice, the spoken password is received as a phone call on the user's mobile. The password will not be stored on the user's phone and Voice allows you to reach users with limited sight. You can also implement Voice as a back-up in case your SMS is not delivered.

One Time Password as Push Notification

The Two-factor Authentication process using One Time Passwords via Push is similar to SMS OTP. In the login procedure to your online environment, an automated generated code is sent as a push notification to your App in the user’s phone. Then the user has to copy that code to the login screen to verify his identity. This does mean you’ll need a dedicated app.

How a one-time password works

In OTP-based authentication methods, the user's OTP app and the authentication server rely on shared secrets.

Values for one-time passwords are generated using the following factors in conjunction with one another:

- HMAC, or Hash-based Message Authentication Code, algorithm.
- A moving factor, such as time-based information -- e.g., a time-based OTP (TOTP) -- or an event counter that tracks the number of authorization attempts -- e.g., HMAC-based OTP (HOTPs).

The OTP values have minute or second timestamps for greater security. The one-time password can be delivered to a user through several channels, including an SMS-based text message, an email or a dedicated application on the endpoint.

Industries that Benefit from One Time Passwords

- Banking and finance
- Government
- Defence
- Consumer electronics
- Commercial security
- Travel and immigration
- Healthcare

What is CAPTCHA

CAPTCHA stands for the Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are tools you can use to differentiate between real users and automated users, such as bots. CAPTCHAs provide challenges that are difficult for computers to perform but relatively easy for humans. For example, identifying stretched letters or numbers, or clicking in a specific area.

What are CAPTCHAs Used for

CAPTCHAs are used by any website that wishes to restrict usage by bots. Specific uses include:

- **Maintaining poll accuracy**—CAPTCHAs can prevent poll skewing by ensuring that each vote is entered by a human. Although this does not limit the overall number of votes that can be made, it makes the time required for each vote longer, discouraging multiple votes.
- **Limiting registration for services**—services can use CAPTCHAs to prevent bots from spamming registration systems to create fake accounts. Restricting account creation prevents waste of a service's resources and reduces opportunities for fraud.
- **Preventing ticket inflation**—ticketing systems can use CAPTCHA to limit scalpers from purchasing large numbers of tickets for resale. It can also be used to prevent false registrations to free events.
- **Preventing false comments**—CAPTCHAs can prevent bots from spamming message boards, contact forms, or review sites. The extra step required by a CAPTCHA can also play a role in reducing online harassment through inconvenience.

How Does CAPTCHA Work

CAPTCHAs work by providing information to a user for interpretation. Traditional CAPTCHAs provided distorted or overlapping letters and numbers that a user then has to submit via a form field. The distortion of the letters made it difficult for bots to interpret the text and prevented access until the characters were verified.

This CAPTCHA type relies on a human's ability to generalize and recognize novel patterns based on variable past experience. In contrast, bots can often only follow set patterns or input randomized characters. This limitation makes it unlikely that bots will correctly guess the right combination.

Since CAPTCHA was introduced, bots that use machine learning have been developed. These bots are better able to identify traditional CAPTCHAs with algorithms trained in pattern recognition. Due to this development, newer CAPTCHA methods are based on more complex tests. For example, reCAPTCHA requires clicking in a specific area and waiting until a timer runs out.

OTP Bypass Methodologies

1. Social engineering

Social engineering represents a non-technical strategy where an attacker manipulates a victim into unintentionally revealing crucial information, such as a secret code. In cases where the attacker already possesses the victim's username and password, they might call or message the victim, spinning a convincing tale that persuades them to disclose their OTP code.

In other scenarios, the attacker may already have sufficient details about the victim needed to contact the targeted service's customer support desk posing as them. The criminal can impersonate the user, claiming their account is locked or there is an issue with their authentication application. If they are successful, the attacker can gain one-time access to the victim's account or, if they are particularly fortunate, reset and change the user's password entirely.

2. Abusing OAuth

OAuth protocol permits apps and services to retrieve user information on a restricted scale without the need to reveal the user's password. For instance, to log into an application, you might grant partial access to your Twitter or Facebook account. As such, the chosen application receives some degree of account authority; however, it does not retain any information associated with the user's passwords.

In a tactic known as Consent Phishing, a cybercriminal masquerades as a valid application with OAuth authorization and dispatches an access request. If the victim approves this access request, the attacker can act at will within the granted scope of access.

3. Brute-force attack

Some attackers opt for a brute-force method, mainly when dealing with outdated or inadequately protected hardware. For instance, some older OTP key fobs only have four digits, making them substantially easier to crack.

A deterrent for hackers is the fact that the one-time codes generated by these key fobs have a limited validity period (typically 30 to 60 seconds). Consequently, attackers have a narrow window of opportunity to sift through the potential codes before they are refreshed.

4. Leveraging pre-generated tokens

Certain platforms offer users the option to generate OTP codes in advance. Take, for instance, Google's account security settings which allow you to download a list of backup codes intended for future use. This feature is typically utilized in scenarios where the authentication device is lost or inaccessible. However, should this list or even just one of the backup codes fall into the wrong hands, the attacker would have unimpeded access to the account, despite the active OTP.

5. Session hijacking

Session hijacking (or cookie theft) can allow attackers to access an account without requiring any knowledge of OTP codes or even passwords. When users visit a website, they do not need to input their password every time due to a session cookie stored in the browser. This cookie carries user information, maintains authentication, and tracks all activity within the session. As long as the user does not manually log out, these session cookies persist in the browser. Therefore, a potential attacker can manipulate this cookie to gain access to the user's account.

Cybercriminals use several methods to hijack accounts, including cross-site scripting attacks, malware deployment, etc. Moreover, crooks may use special rogue frameworks to execute man-in-the-middle (MITM) attacks. Utilizing such frameworks, the attacker sends a phishing link to the user, which reroutes them to the login page of a legitimate website, albeit through a malicious proxy. When a user logs into their account using OTP, hackers intercept their login credentials and the authentication code.

6. SIM swapping

A SIM swap attack involves a situation where perpetrators manage to obtain total control over the victim's mobile number. Criminals might gather a set of basic user data and impersonate the user at the cell phone service provider's store to obtain a new SIM card. Additionally, SIM swapping could occur through spy apps installed on the target's phone.

Gaining control over a user's phone number means the hacker can intercept one-time codes delivered via SMS. Given that this is the most commonly used OTP method, an attacker can potentially breach all of the victim's vital accounts sequentially and gain complete access to essential data.

7. Clickjacking

Clickjacking is a devious technique where an attacker tricks a user into unknowingly turning off their OTP protection. Using an infected device or rogue website, the attacker overlays an invisible iframe containing the OTP disabled interface with a harmless-looking button. When the unsuspecting user clicks on the harmless element, they are interacting with the hidden iframe, consequently disabling their OTP.

Impact of OTP Bypass

Common implications of OTP bypass are:

- Escalate privileges, move on to additional pages, or create an admin session in the HTTP request.
- Download harmful firmware and change system settings.
- View, copy, delete, alter, or overwrite important data.
- Compromise a system admin account, gaining full control of the application and access to the infrastructure.

Mitigation measures for OTP bypass

Best practices for mitigating the threat of authentication bypass attacks include:

- Keeping up-to-date with updates to systems, applications, software, and networks.
- Encrypting all session IDs and cookies.
- Using antivirus protection.
- Ensuring that authentication policies are robust and leak-proof.
- Avoid exposure of authentication protocol in a client-side browser script. Also, validating user input on the server side.
- Avoiding the use of external SQL interpreters.

CAPTCHA Bypass Techniques

1. Missing Server-Side Validation of the Captcha Field

- Some applications send Captcha Parameters on the client side but they do not validate this on the server side.
- Simply, Remove the "Captcha" parameters and see if the request is processed successfully.
- If yes, you can now use this request to perform your brute-force or rate limiting attempts.

2. Missing Captcha Field Integrity Checks

- There are multiple scenarios around this one, this happens when the application validates whether the captcha parameters are present but not the "value".
- Simply, send an empty captcha parameter and see if the request works successfully.
- Change some specific characters of the captcha parameter and see if it possible to bypass the restriction. This usually happens when only string length is validated at the server-side.

3. HTTP Verb Manipulation

- If a request with POST method is using the Captcha, try changing the verb(method) from POST to GET and remove the captcha parameter.
- Often this bypasses the restrictions if the validation on the server-side are not in place.

4. Content Type Conversion

Change the content type from one type to another say from JSON to Plain Text and remove the captcha parameters to see if the request works successfully.

5. Reuseable Captcha

- Just repeat the request using the same Captcha key multiple times and see if that works.
- Capture the Request in Burp Proxy and send it to Intruder. Hold the request in Proxy Tool don't let it go.
- Run the Intruder and observed that same captcha can be reused any no. of time until you drop off the original request from proxy.

6. Using HTTP Request Headers

Using Headers such as X-Forwarded-For, X-Original-IP, etc. you can try to bypass the Captcha in some cases.

Impact of CPTCHA Bypass

1. Increased spam

Without an effective CAPTCHA "gatekeeper," you can expect spam comments that advertise everything from malicious services to other websites. If your website is set to approve comments first, they won't appear to the general public. However, you'll be drowned by dozens or even hundreds of irrelevant comments on the backend.

2. Invalid analytics data

Bots will skew the traffic on your web page and render your analytic data useless. If hackers figure out a way to get past your CAPTCHA, you may notice a spike in traffic with zero conversions or find that users are abandoning their carts, and you won't be able to figure out why.

3. Insecure shopping checkout

If you own an eCommerce website, a bypassed CAPTCHA means that hackers can now access user accounts, make purchases with stolen cards, and even access other sensitive areas of your website.

4. Database access

If you don't have CAPTCHA set up for your website login, then you might want to consider adding it. Bots can be used to access poorly secured user accounts and perform account takeovers. They can also access your online databases and even perform other forms of content-based fraud on your site.

5. Fewer web resources

With access to your website, bots will bombard your website, submitting connection requests and taking up finite resources. That means that legitimate users will have slowed or even non-existent access to your website, which can be damaging to your business.

Mitigation measures for CAPTCHA Bypass

Some Prevention techniques of CAPTCHA Bypassing are:

1. IP Blacklisting

It is utilized to help ensure against each of the three sorts of CAPTCHA assaults, as it targets obstructing any IP address that creates suspiciously enormous volumes of traffic to a site. A site proprietor actualizes this as it would explicitly target assailants of their website. Lamentably, this shield conveys with it the hazard of blocking authentic clients who happen to share an open IP address with an assailant, are utilizing an intermediary server, or who are using an undermined machine. An IP removing administration is accessible from many webs facilitating providers8. Notwithstanding, if this alternative can't from a facilitating supplier or no facilitating supplier is included, at that point, this defence is generally mind-boggling to execute. This is because its execution would require a method for checking the source IP addresses of visits to a site just as giving server-side code to square exceptionally dynamic IP addresses (for example, by designing the Linux local firewall, IP tables).

2. Site Keys

This shield forestalls a CAPTCHA from being shown on a site other than the one proposed along these lines moderating human misuse assaults. This defence is probably not going to influence authentic clients of a place in any capacity; all things considered, structured distinctly to forestall the showcase of a CAPTCHA on an unapproved location. When a key is given to the site proprietor, executing it might be as necessary as including a couple of lines of code.

3. Response Time Monitoring

This defence ensures against bots that completely solve CAPTCHAs altogether quicker than people. As needs are, it safeguards against CAPTCHA-explaining assaults. It may be executed with the CAPTCHA supplier if observing is confined to the time required to solve the riddle. On the other hand, if the site proprietor runs the project, for example, in the structure of JavaScript downloaded to the program, it could screen the time required to finish construction and illuminate the CAPTCHA. Much the same as the past protect, a client may be contrarily influenced if utilizing an auto-fill program, as it may finish a structure quicker than a client would. One of the manners in which this protection can be executed is using customer-side scripting to compute the time slipped by from

the minute information is recognized. The pace of CAPTCHA structure fruition can be determined from the contrasts between timestamps of observed occasions.

4. Switching between CAPTCHAs

This shield decreases the achievement odds of bots modified to fathom explicit CAPTCHAs. It must be executed by a site proprietor, as it would ordinarily include conveying CAPTCHAs from a scope of suppliers. It may influence ease of use as the client experience. Actualizing this project is expected to be very intricate, as it would require programming a site to naturally switch between CAPTCHAs as manage various sorts of reactions relying upon the CAPTCHA supplier. It hampers the client experience very much.

5. Device Fingerprinting

This protects a similar manner as IP boycotting. In any case, it has the preferred position of recognizing explicit gadgets paying little mind to regardless of whether they utilize changing IP locations, or they share IP addresses with other kind gadgets. Be that as it may, it is or maybe progressively muddled to actualize as it requires the distinguishing proof of gadget fingerprints by gathering a scope of data about the customer stage, commonly including the OS and internet browser. Gadget fingerprinting can be actualized by the site proprietor or redistributed to a gadget fingerprinting administration supplier Real clients may be influenced on the off chance that they were erroneously recognized as bots and accordingly obstructed from collaborating with the site or tested with more CAPTCHA puzzles.

6. Brand Customization

This shield will caution clueless clients that they are being tricked into unravelling a CAPTCHA puzzle of another site. This defence must be actualized if the CAPTCHA supplier gives a customization choice to the site proprietor. The expansion of a web logo, and maybe a little measure of caution content, is probably not going to have a critically antagonistic impact on clients. Since this is reliant on the CAPTCHA supplier, actualizing it would not usually require a site proprietor to do any more than finding a way to show the modified CAPTCHA.

Contact us.

https://lnkd.in/dUYHqXmT

https://cyberpublicschool.com/

https://www.instagram.com/cyberpublicschool/

https://www.youtube.com/@cyberpublicschool.com

Email:- Anandh@cyberpublicschool.com

Phone no: - +91 9631750498 (IND)

+91 7304708634 (IND)

Our Successful OSCP Students