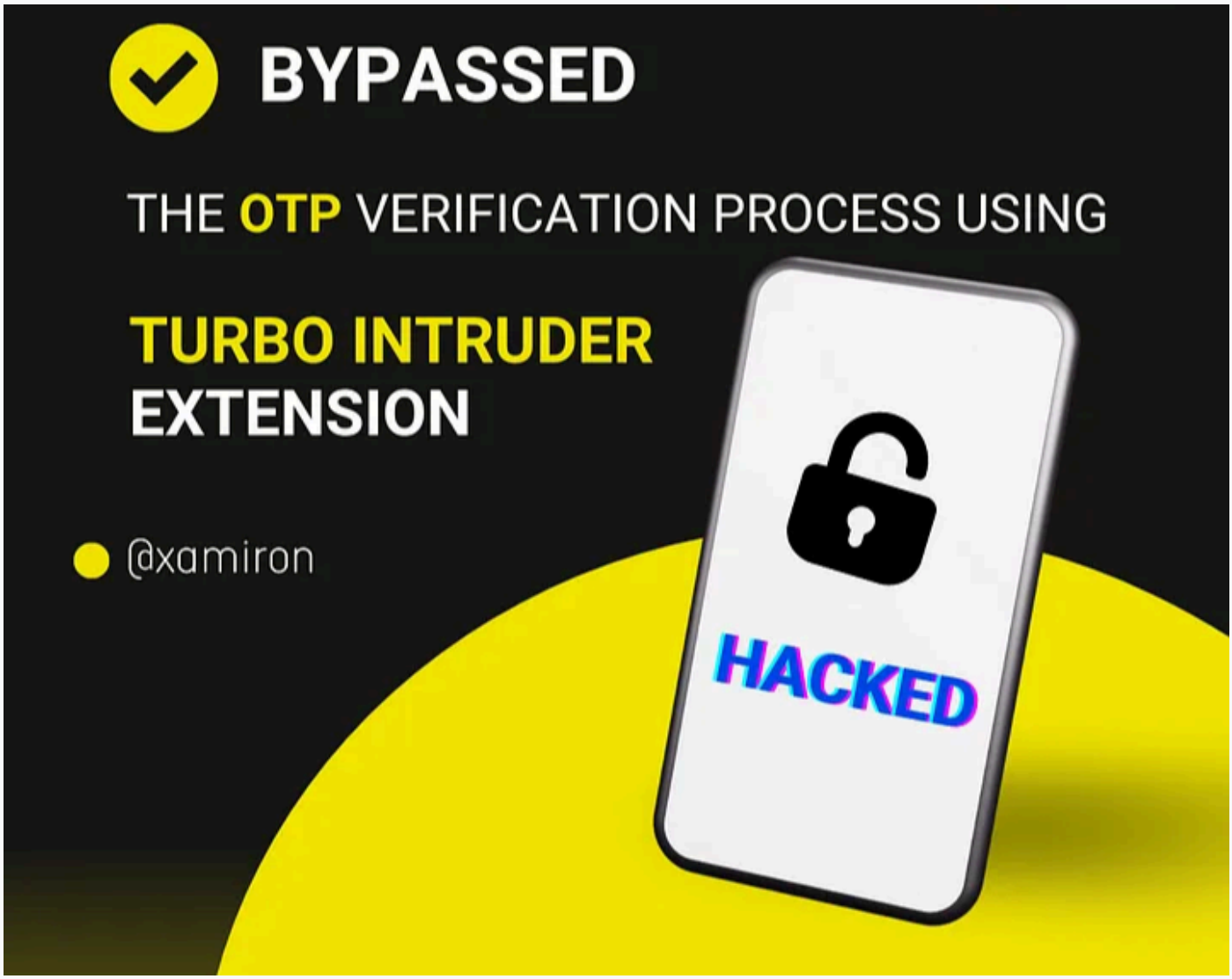
CYBER SECURITY

Bypassed the OTP verification process using “Turbo Intruder” Extension.

Sabuj Modak Samiron 22 Dec 2024 1 234 0 Share



Today, in this article, we will explore methods and techniques that have been used to bypass OTP.

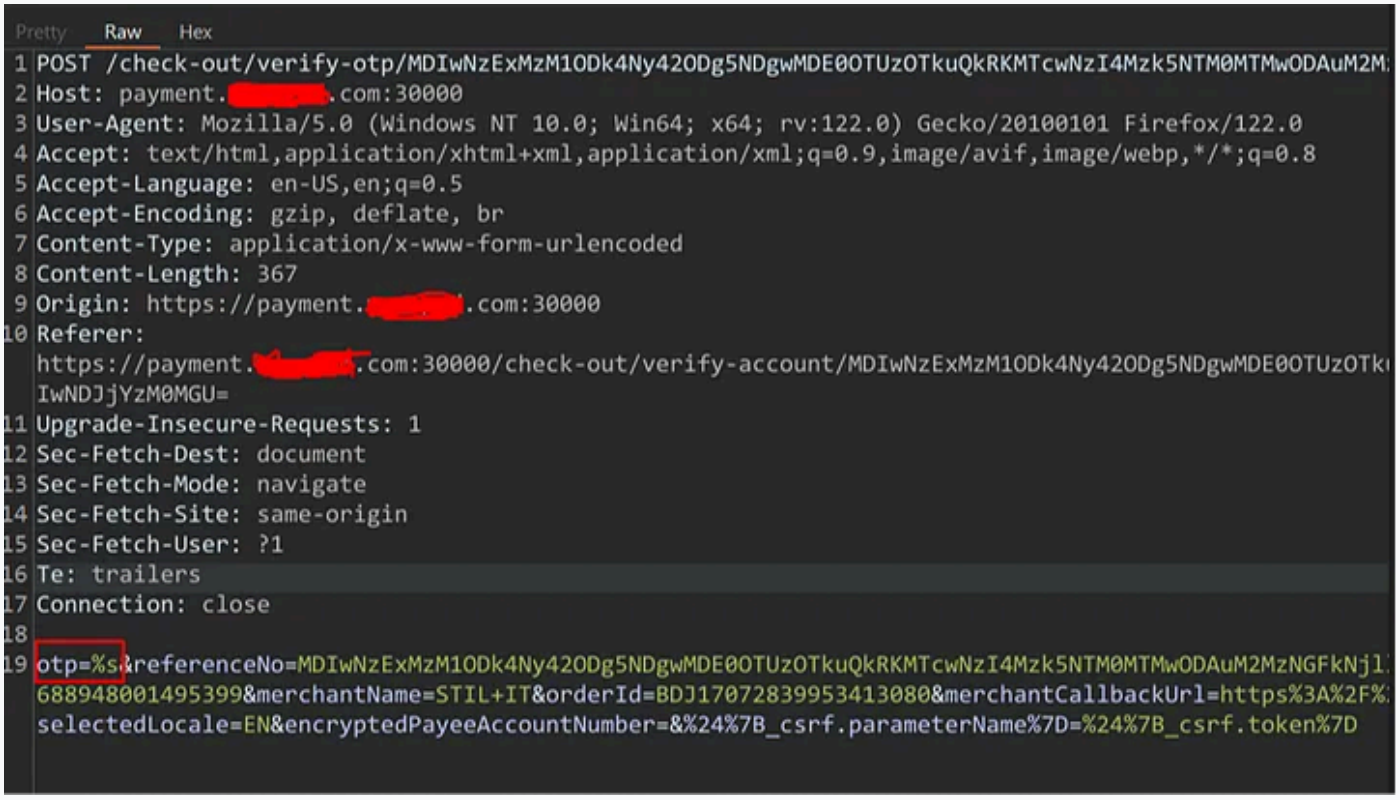
Step 01:

- You have to know OTP length: The length of the OTP affects the number of possible combinations. For example, a 6-digit OTP has 1,000,000 possible combinations (from 000000 to 999999). Knowing the length helps the attacker understand the complexity and the number of attempts required to guess the OTP.
- You have to know OTP validity time: OTPs are typically valid for a short period, often ranging from 30 seconds to a few minutes. Knowing the exact validity period helps the attacker time their attempts more effectively, ensuring they use the OTP within its active window.

helps the attacker plan their strategy to avoid detection and lockout.

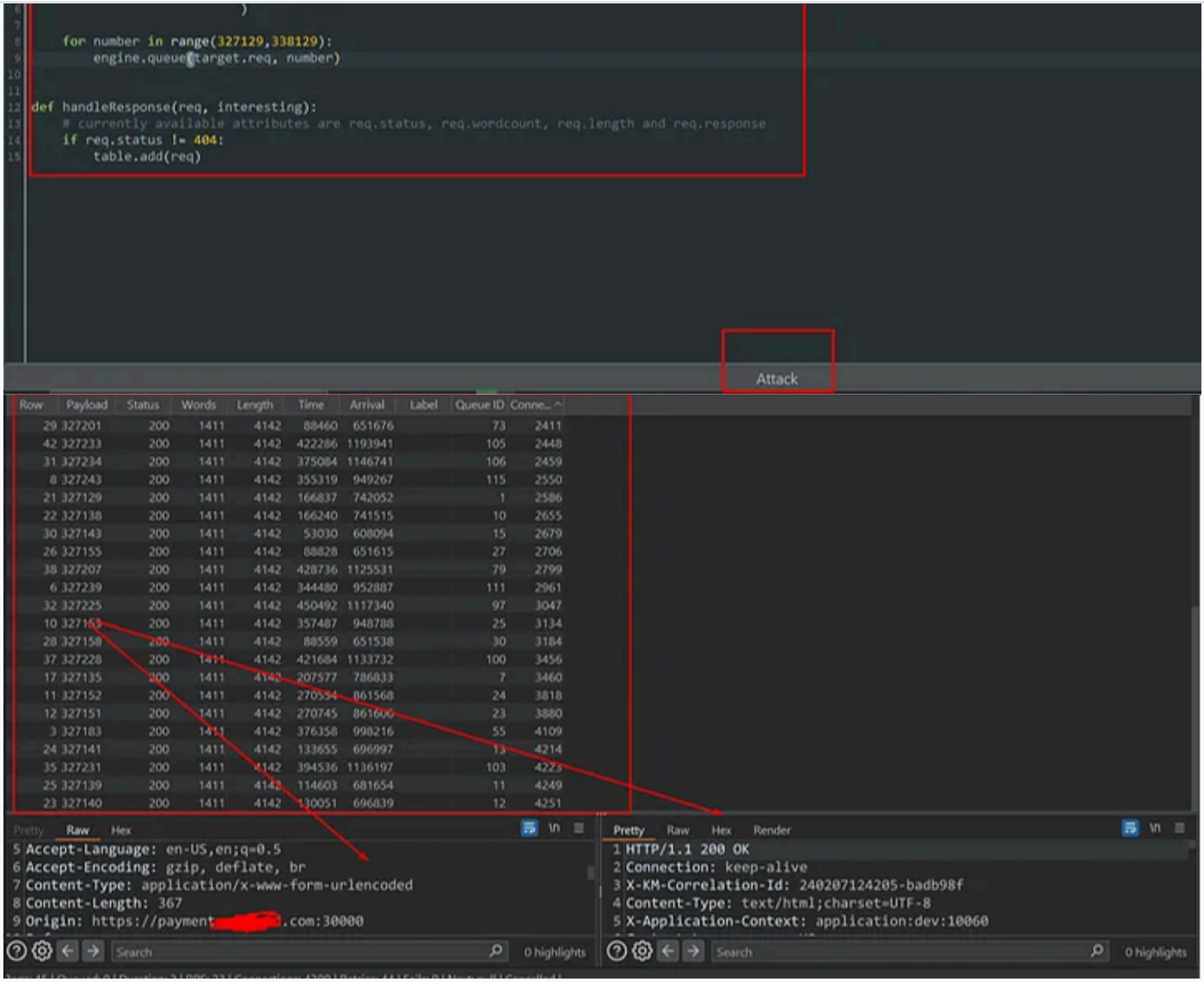
Step 02:
Capture the Payment Request:

- Open Burp Suite and start the proxy listener.
- Perform the payment action on your web application. This could be filling out a payment form and submitting it.
- Burp Suite will intercept the request. You can view this in the “Proxy” tab under the “HTTP history” section.
- Send the Request to Turbo Intruder:
- Right-click on the captured payment request in the HTTP history.
- Select Extensions > Turbo Intruder > Send to Turbo Intruder.
- Before sending the request to Turbo Intruder, you entered the incorrect OTP.
- Replace otp=328129 to otp=%s:



Step 03:
Write python script and start attack:

```
def queueRequests(target, wordlists):
engine = RequestEngine(endpoint=target.endpoint,
concurrentConnections=5000,
requestsPerConnection=10000,
pipeline=False
)
for number in range(327129,338129):
engine.queue(target.req, number)
def handleResponse(req, interesting):
if req.status != 404:
table.add(req)
```



To check the status code, length, arrival time, and other parameters.

cyber security | security testing | software testing

Share your thoughts Or Start discussion

Related Blogs

CYBER SECURITY 0 0 267

Ultimate Guide to Security Testing for Web Applications: Protect Your Site from...

Security Testing has become a critical component of web application development

Nishi Khan
25 Nov 2024

CYBER SECURITY 0 0 44

Enhancing Software Security Testing with Generative AI

In today's digital landscape, where software applications are central to virtu

Anwarul
18 Nov 2024

Popular Tags

sqa testing qa software testing qabrains testing tool automationtesting softwaretesting mobiletesting selenium

View All

Popular Post

Can a Software Tester Become a Game Tester? Here's What You Need t...

As the gaming industry continues to grow, fueled by innovations in virtual reali

Understanding Java Object-Oriented Programming (OOP) Concepts

Java is a powerful and widely used programming language known for its versatilit

Essential Bugs to Check for in Game Testing: A Guide for Beginners

Game testing is crucial to ensure a smooth, engaging, and bug-free experience fo

Popular Discussion

01 Top Software Testing Interview Questions and Expert Tips from QA Leaders

02 AI tools for QA engineer

03 What is SQL?

04 Appium, WebDriver

05 What are the most effective strategies you've found for balancing speed and...

View All

QA Brains

QA Brains is the ultimate QA community to exchange knowledge, seek advice, and engage in discussions that enhance Quality Assurance testers' skills and expertise in software testing.

QA Topics

Web Testing

Interview Questions

Game Testing

See more →

Quick Links

Discussion

About Us

Terms & Conditions

Privacy Policy

Follow Us