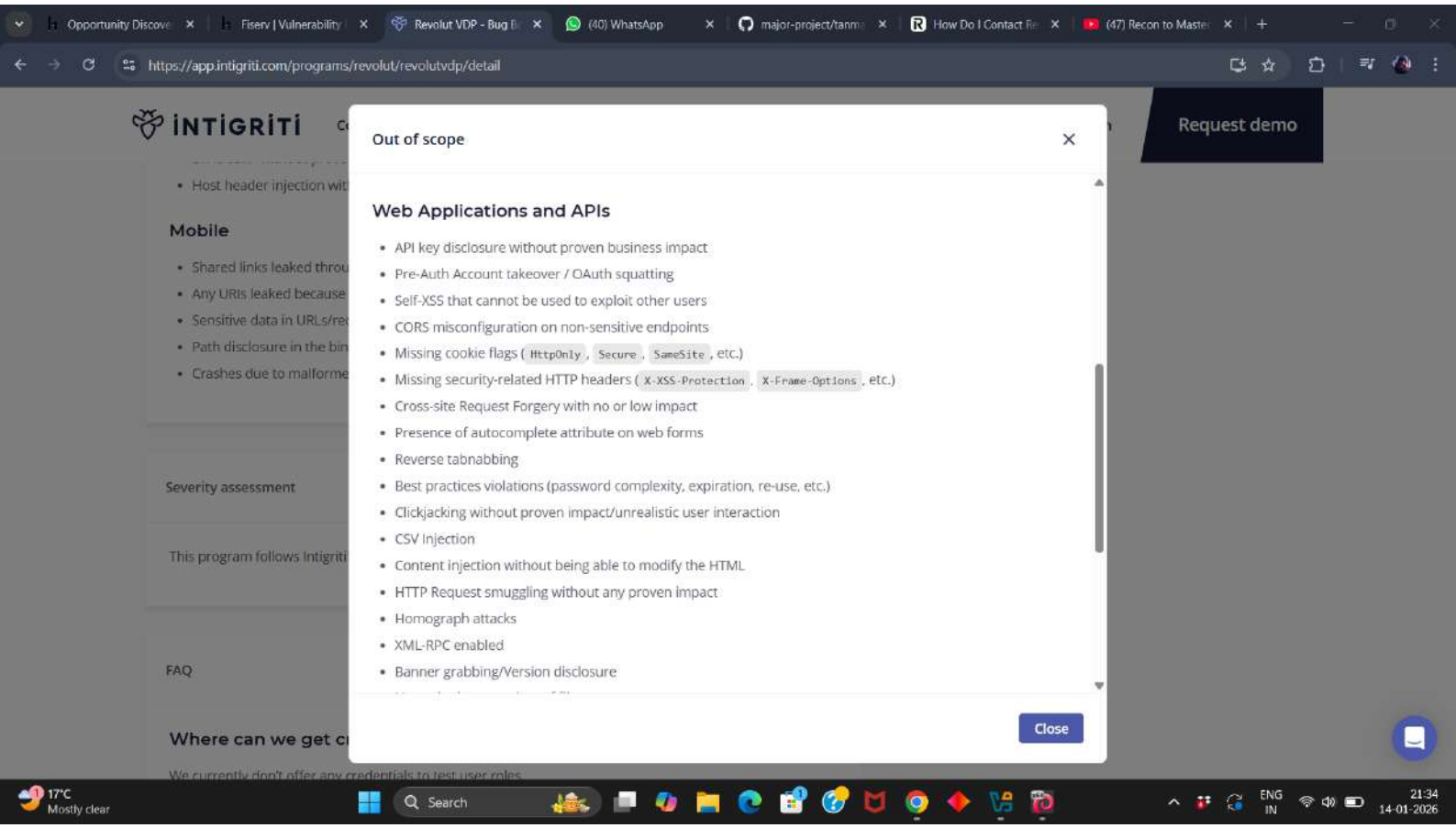
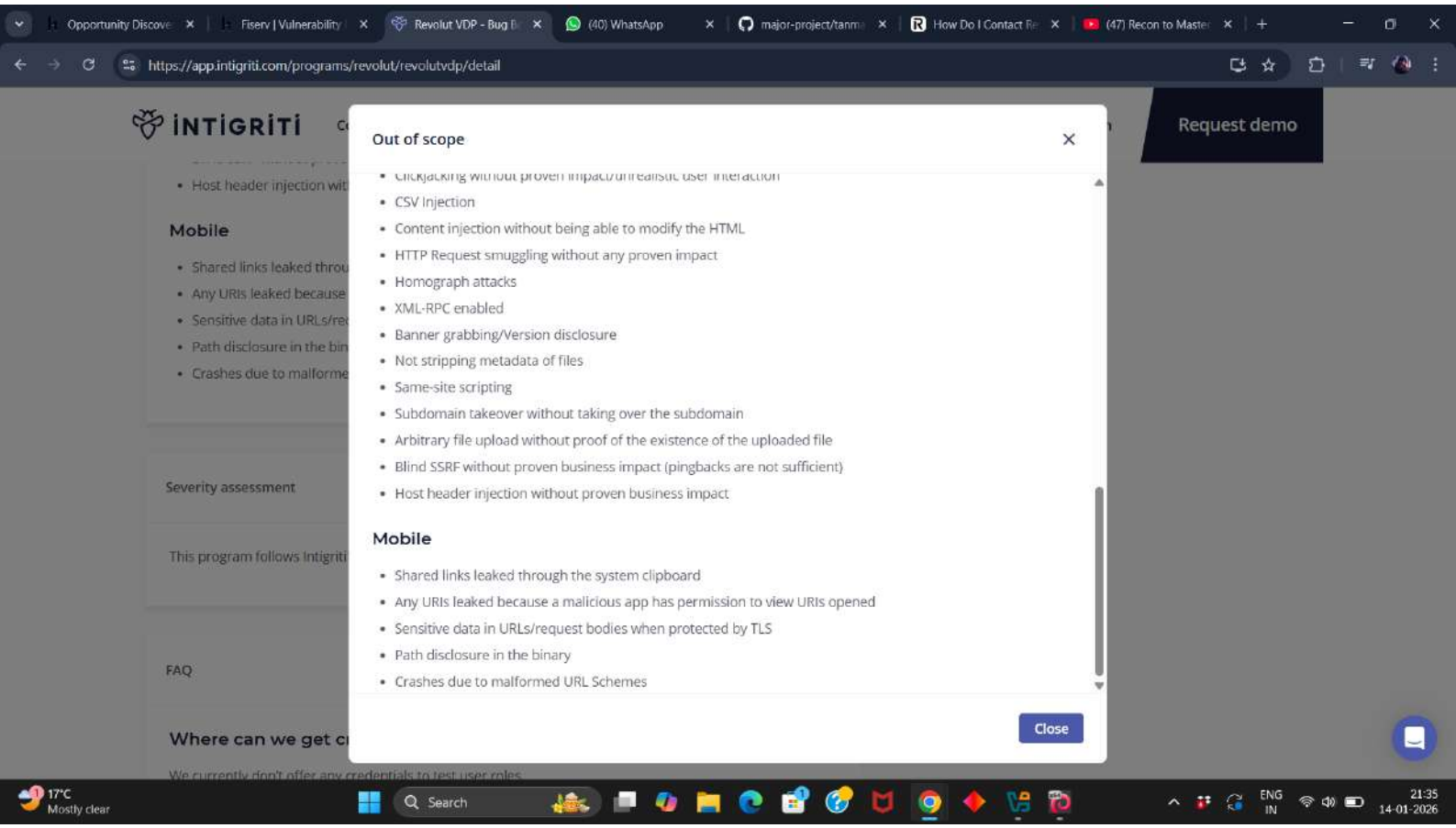
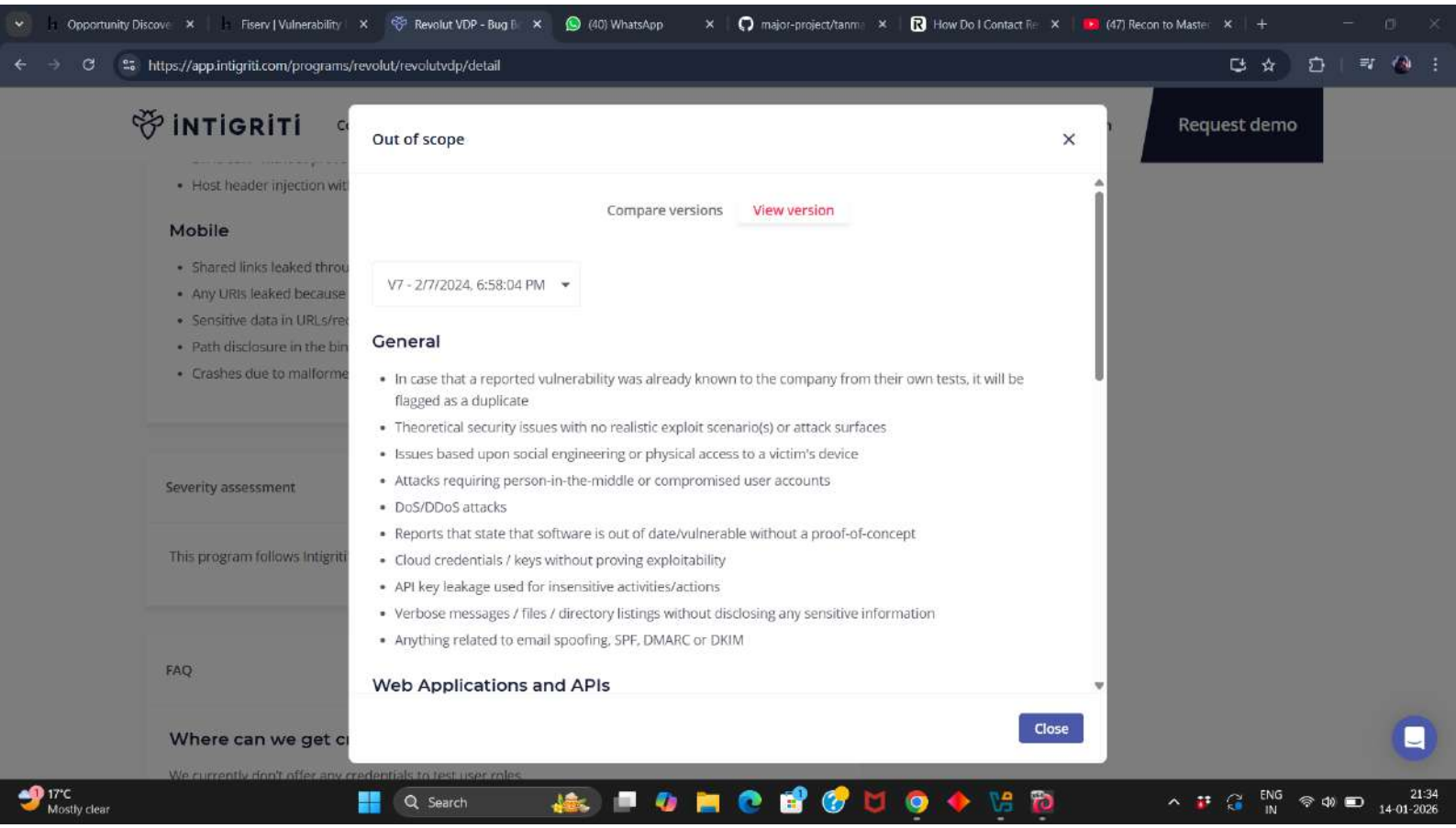

Opportunity Discove
Fiserv | Vulnerability
Revolut VDP - Bug B
(40) WhatsApp
major-project/tanma
How Do I Contact Re
(47) Recon to Master
https://app.intigriti.com/programs/revolut/revolutvdp/detail
INTIGRITI
Request demo
Out of scope
Web Applications and APIs
API key disclosure without proven business impact
Pre-Auth Account takeover / OAuth squatting
Self-XSS that cannot be used to exploit other users
CORS misconfiguration on non-sensitive endpoints
Missing cookie flags (HttpOnly , Secure , SameSite , etc.)
Missing security-related HTTP headers (X-XSS-Protection , X-Frame-Options , etc.)
Cross-site Request Forgery with no or low impact
Presence of autocomplete attribute on web forms
Reverse tabnabbing
Best practices violations (password complexity, expiration, re-use, etc.)
Clickjacking without proven impact/unrealistic user interaction
CSV Injection
Content injection without being able to modify the HTML
HTTP Request smuggling without any proven impact
Homograph attacks
XML-RPC enabled
Banner grabbing/Version disclosure
Close
Mobile
Severity assessment
FAQ
Where can we get c
We currently don't offer any credentials to test user roles
17°C
Mostly clear
Search
ENG
IN
21:34
14-01-2026


Opportunity Discove
Fiserv | Vulnerability
Revolut VDP - Bug B
(40) WhatsApp
major-project/tanm
How Do I Contact Re
(47) Recon to Master
https://app.intigriti.com/programs/revolut/revolutvdp/detail
INTIGRITI
Request demo
Out of scope
Clickjacking without proven impact/unrealistic user interaction
CSV Injection
Content injection without being able to modify the HTML
HTTP Request smuggling without any proven impact
Homograph attacks
XML-RPC enabled
Banner grabbing/Version disclosure
Not stripping metadata of files
Same-site scripting
Subdomain takeover without taking over the subdomain
Arbitrary file upload without proof of the existence of the uploaded file
Blind SSRF without proven business impact (pingbacks are not sufficient)
Host header injection without proven business impact
Mobile
Shared links leaked through the system clipboard
Any URIs leaked because a malicious app has permission to view URIs opened
Sensitive data in URLs/request bodies when protected by TLS
Path disclosure in the binary
Crashes due to malformed URL Schemes
Close
Host header injection wit
Mobile
Shared links leaked throu
Any URIs leaked because
Sensitive data in URLs/re
Path disclosure in the bin
Crashes due to malforme
Severity assessment
This program follows Intigriti
FAQ
Where can we get c
We currently don't offer any credentials to test user roles
17°C
Mostly clear
Search
ENG
IN
21:35
14-01-2026


Opportunity Discove
Fiserv | Vulnerability
Revolut VDP - Bug B
(40) WhatsApp
major-project/tanma
How Do I Contact Re
(47) Recon to Master
https://app.intigriti.com/programs/revolut/revolutvdp/detail
INTIGRITI
Request demo
Out of scope
Compare versions
View version
V7 - 2/7/2024, 6:58:04 PM
General
In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
Theoretical security issues with no realistic exploit scenario(s) or attack surfaces
Issues based upon social engineering or physical access to a victim's device
Attacks requiring person-in-the-middle or compromised user accounts
DoS/DDoS attacks
Reports that state that software is out of date/vulnerable without a proof-of-concept
Cloud credentials / keys without proving exploitability
API key leakage used for insensitive activities/actions
Verbose messages / files / directory listings without disclosing any sensitive information
Anything related to email spoofing, SPF, DMARC or DKIM
Web Applications and APIs
Close
Host header injection wit
Mobile
Shared links leaked throu
Any URIs leaked because
Sensitive data in URLs/re
Path disclosure in the bin
Crashes due to malforme
Severity assessment
This program follows Intigriti
FAQ
Where can we get c
We currently don't offer any credentials to test user roles
17°C
Mostly clear
Search
ENG
IN
21:34
14-01-2026