RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HT-W02**

Pain in the Apps — Three Attack Scenarios Attackers Are Using to PWN SaaS

Matt Radolec

Senior Director of Incident Response and Cloud Operations
Varonis

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

Is SaaS safe or Is there pain in these Apps?

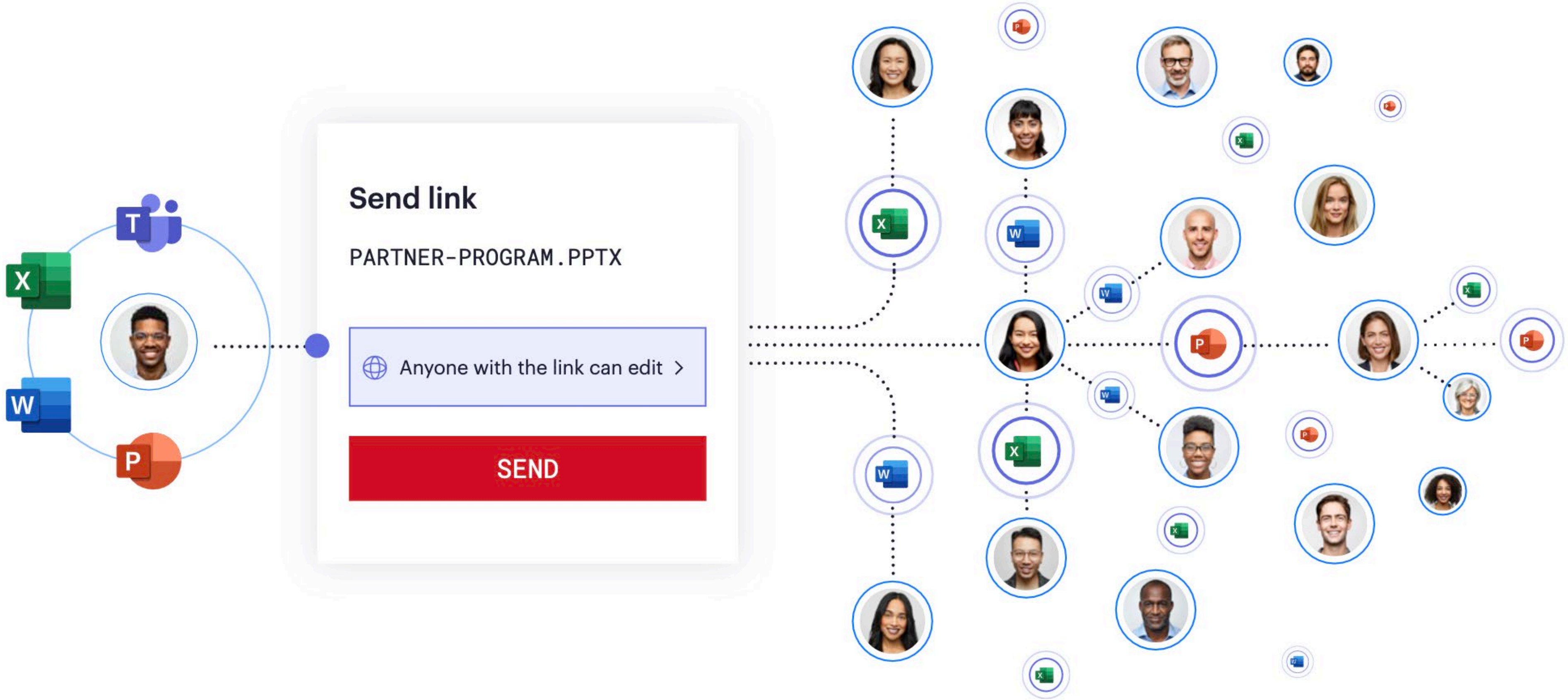
Let’s talk about SaaS.

Box	Google Drive	Amazon S3	AWS	Nutanix Files	Nasuni	NetApp	Dell EMC
Salesforce	GitHub	Slack	Jira	Ctera	Cohesity	Panzura	HPE
Windows File Shares	SharePoint	Exchange Server	UNIX/Linux	SharePoint Online	OneDrive	Exchange Online	Teams

What makes data more important and valuable than ever?

Collaboration.
If we can’t share it, we can’t realize its value.

SaaS apps make collaboration easy.

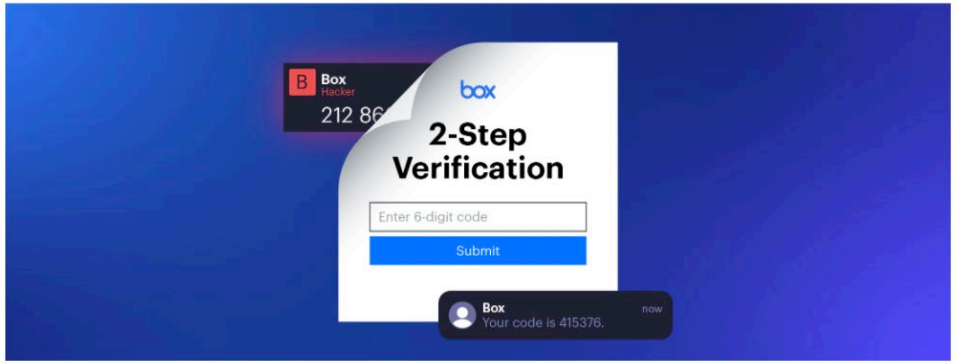


Securing SaaS is getting harder.

- **44 percent** of SaaS privileges are **misconfigured.**
- **75 percent** of external contractor accounts **remain active after they leave.**
- **15 percent** of employees transfer business-critical data to their **personal cloud accounts.**

Source: Varonis 2021 SaaS Risk Report (data from actual SaaS environments, *not* surveys).

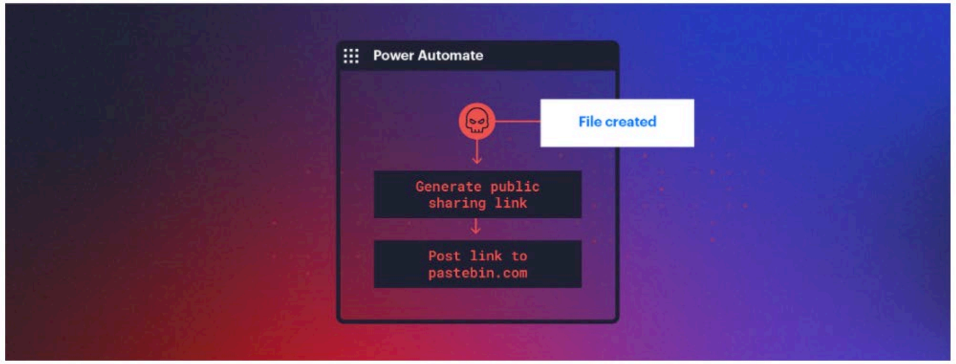
Threat actors are attacking SaaS (and so is Varonis Threat Labs).



THREAT RESEARCH | JANUARY 18, 2022

Mixed Messages: Busting Box's MFA Methods

By Tal Peleg



THREAT RESEARCH | FEBRUARY 2, 2022

Using Power Automate for Covert Data Exfiltration in Microsoft 365

By Eric Saraga

RSA Conference2022

Pain in the App #1 – SSO Imposter

RSAConference2022

What do you do if one of your SSO/IAM admins was an imposter?

5 questions to discuss during the simulation:

- What can I find out today?
- How quickly can I find it?
- What am I missing?
- How could I have detected it?
- How could I have minimized the blast radius before this event?

Attack Flow

okta
Get admin access to any connected application

box
Backdoor access to customer contracts folder

Google Workspace
Downloads full users list
Exfiltrate sensitive HR files

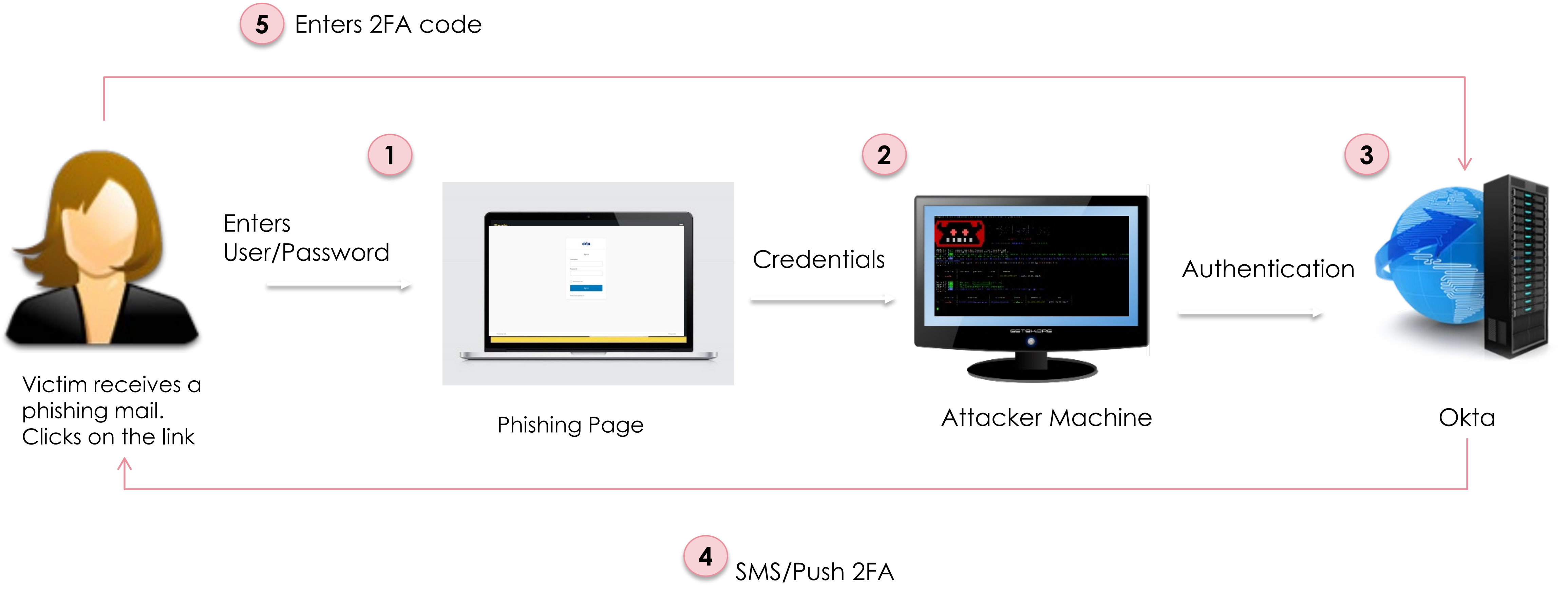
Phishing Mail

okta
Impersonation to other users using SSO

Google Workspace
Extracting users list using admin panel
Sharing sensitive data stored on My Drive with external

box
Share customers contracts using a public custom URL

Advanced Phishing: Bypassing MFA



Phase 1 – Initial Foothold - Okta

- Attack -
  - Using advanced phishing, attacker bypasses MFA
  - Attacker impersonates to other users by taking advantage of default SSO settings of Okta.
- Detections to Consider
  - Activity from new Geo Location
  - Suspicious IP activity
  - Direct assignment of Okta application

Phase 2 – Impersonation + Data Exfiltration on Google Workspace

- Attack -
  - Using the Google Workspace admin Jerome has, the attacker exports the users list of the organization
  - Attacker impersonate to desired executive and sharing sensitive data from it's My Drive with external.
- Detections to Consider
  - User list export
  - Direct assignment of Okta application

Phase 3 – Impersonation + Data Exfiltration on Box

- Attack -
  - Attacker finds out the Box super admin mail using Jerome's Box user.
  - Attacker impersonates to Box's super admin user and shares sensitive data using a custom URL.
- Detections to Consider
  - Sharing of Sensitive Content
  - Box File Shared Publicly via Custom URL

Is SaaS safe or Is there pain in these Apps?

RSAConference2022

Pain in the App #2 – Cross-Cloud Hacking: Stealing Salesforce Data via GitHub & Slack

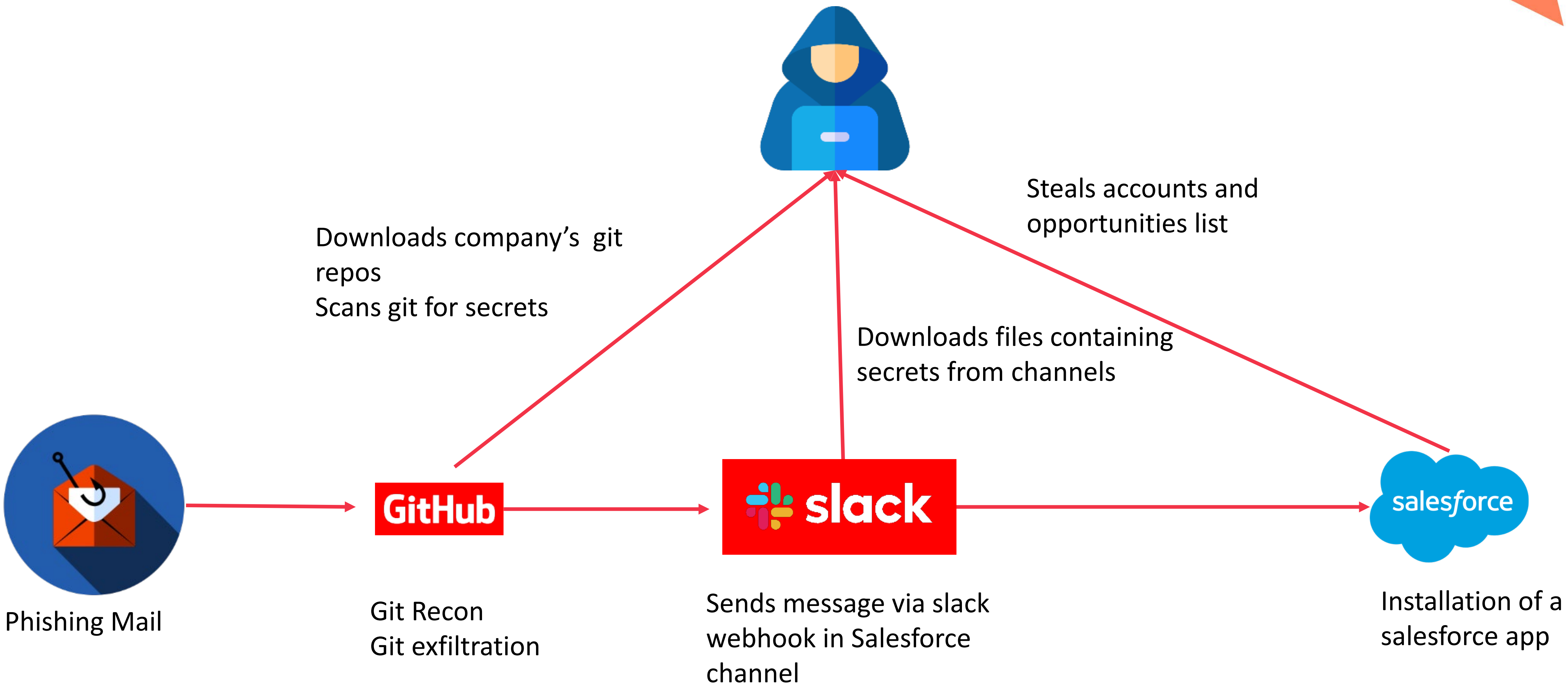
RSAConference2022

How would you identify lateral movement in SaaS and SalesForce data exfiltration?

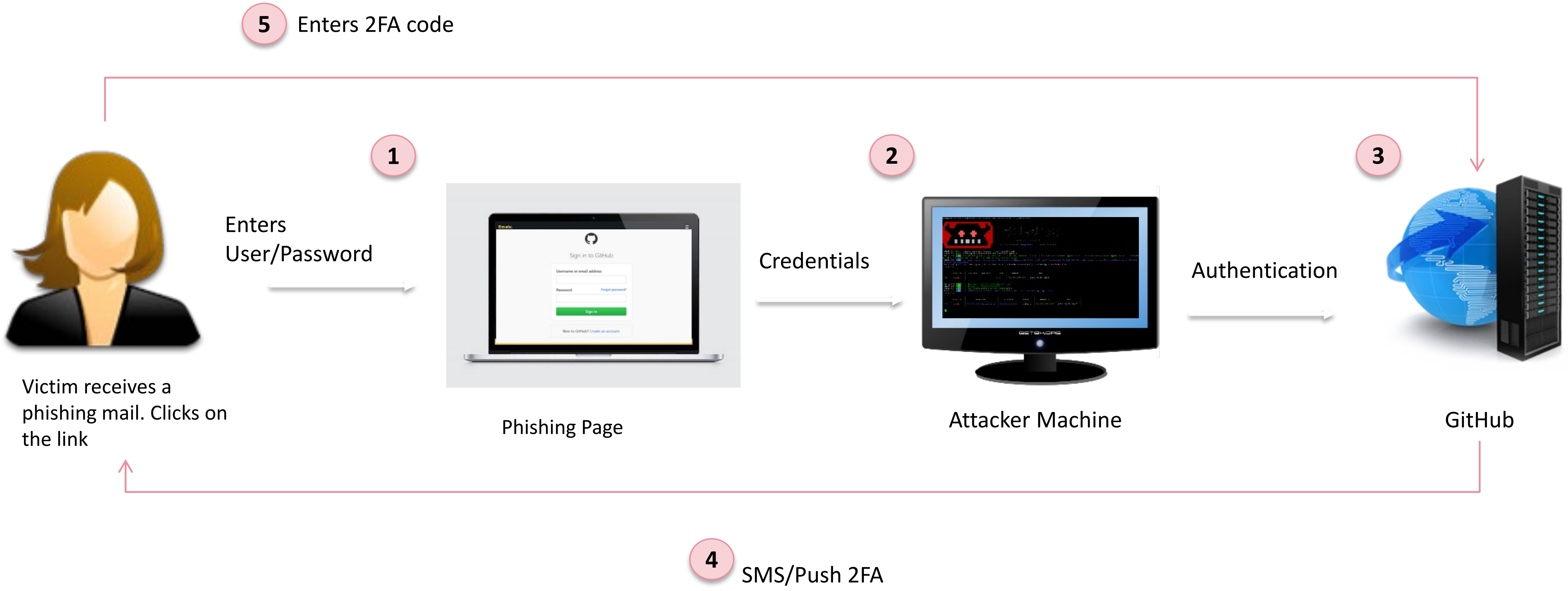
5 questions to discuss during the simulation:

- What can I find out today?
- How quickly can I find it?
- What am I missing?
- How could I have detected it?
- How could I have minimized the blast radius before this event?

Attack Flow


Downloads company's git repos
Scans git for secrets
Steals accounts and opportunities list
Downloads files containing secrets from channels
GitHub
slack
salesforce
Phishing Mail
Git Recon
Git exfiltration
Sends message via slack webhook in Salesforce channel
Installation of a salesforce app

Advanced Phishing: Bypassing MFA



Phase 1 – Initial Foothold GitHub

- Attack -
  - Using advanced phishing, attacker bypasses MFA
  - Attacker users hijacked session to download Git repo code
- Detections to Consider
  - Activity from new Geo Location
  - Suspicious IP activity

Phase 2 – Lateral movement to Slack

- Attack -
  - Using the stolen credentials, attacker logs in to Slack
  - Attacker scans slack channels and downloads secrets
- Detections to Consider
  - Activity from new Geo Location
  - Suspicious IP activity
  - Access/Use of Key Files in Slack
  - Abnormal File Downloads from Slack

Phase 3 – Lateral movement and exfiltration from Salesforce

- Attack -
  - Using Slack webhook attacker sends a message in a SF admin channel, Lures SF admin to install a SF app
  - Performs privilege escalation and persistency by creating a backdoor SF user
  - Exfiltrates SF data
- Detections to Consider
  - Activity from new Geo Location
  - Suspicious IP activity
  - Authorization/Installation of New Salesforce Application
  - Abnormal Access to Salesforce records

RSAConference2022

Is SaaS safe or Is there pain in these Apps?

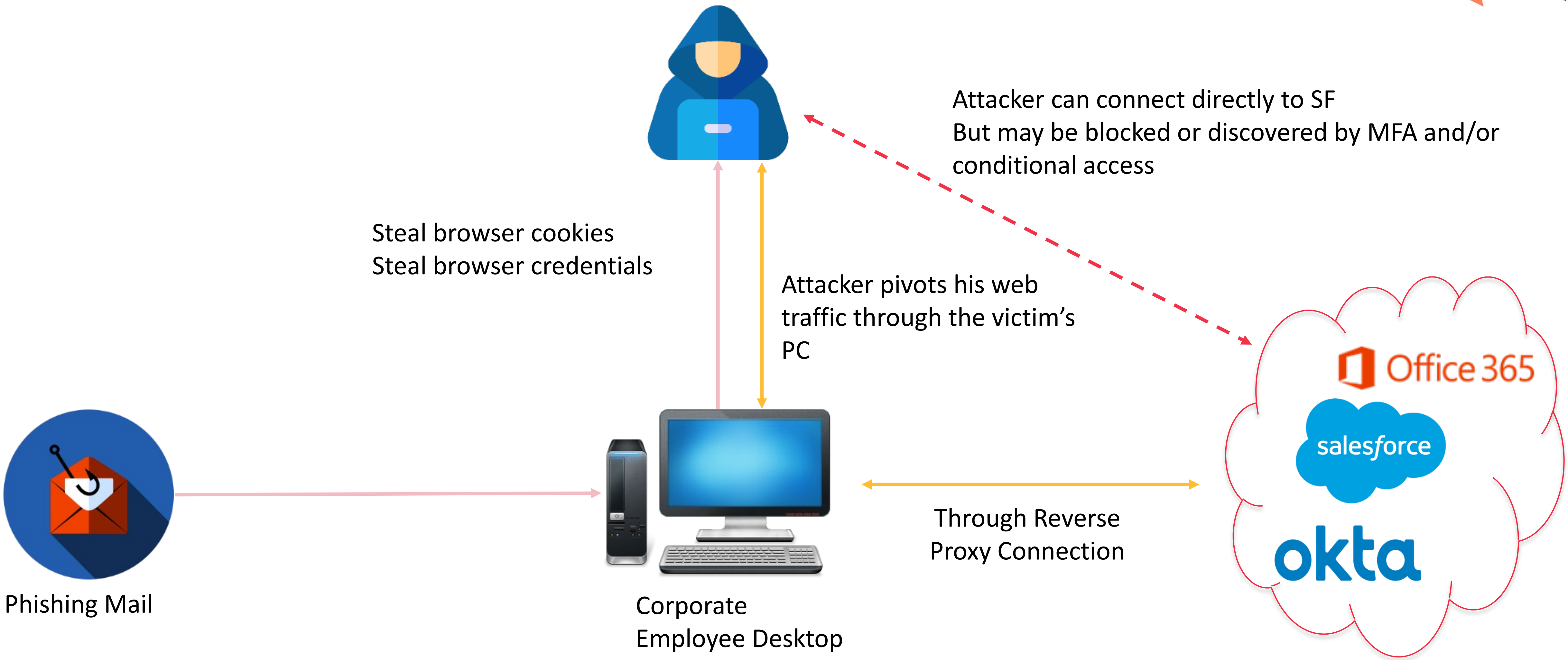
RSA Conference2022

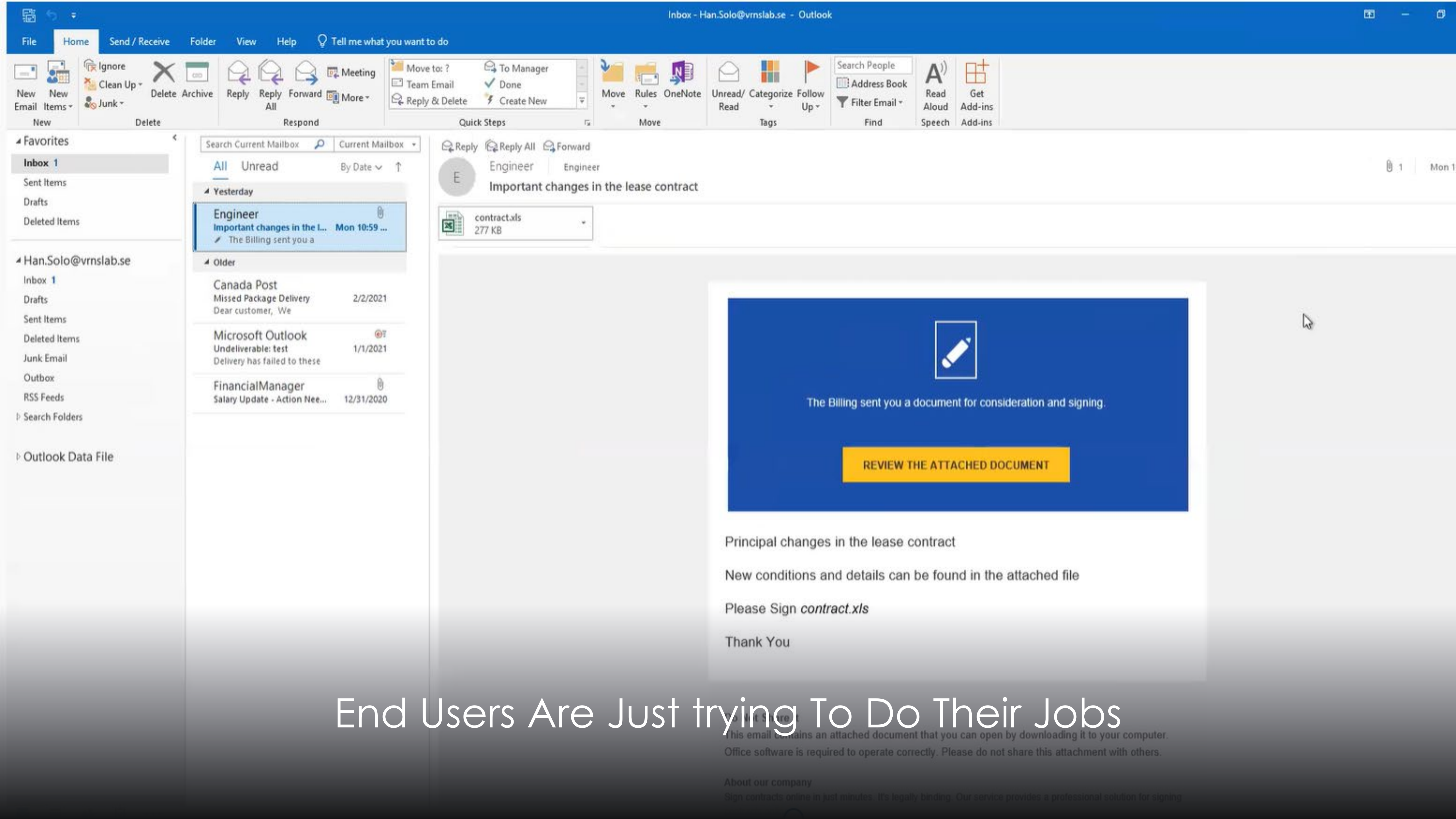
Pain in the App #3 – Those cookies will go straight to your SaaS

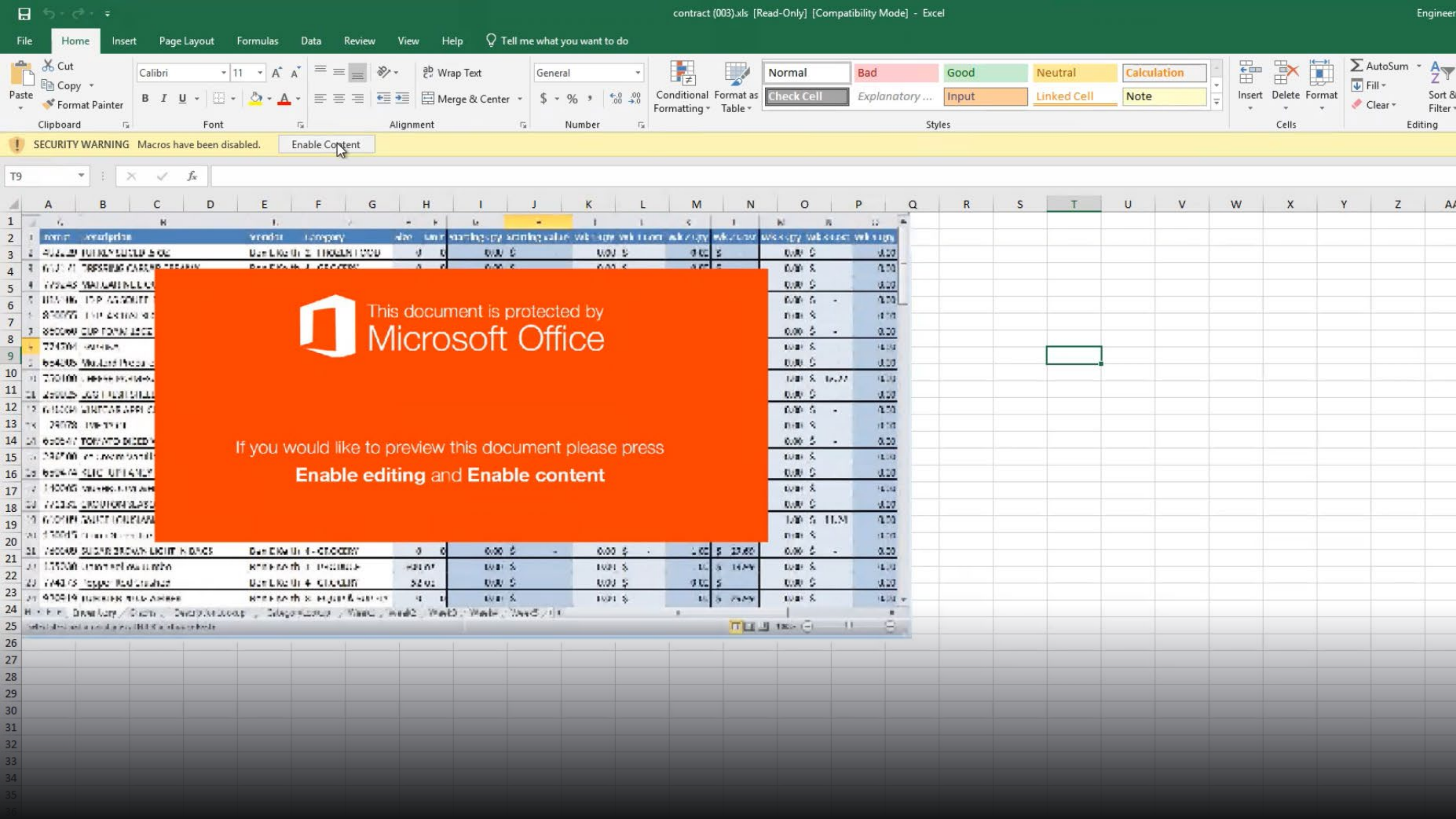
RSAConference2022

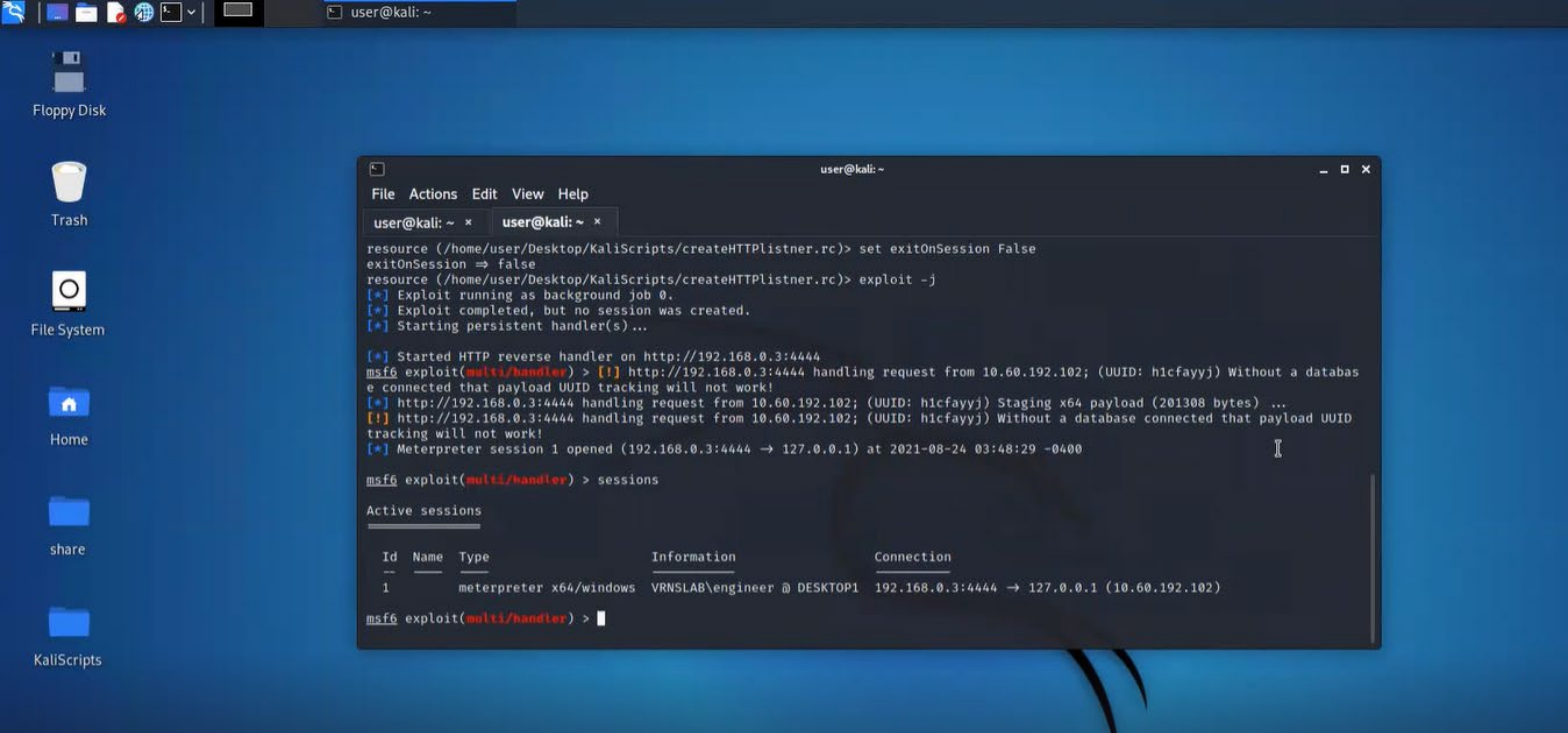
How do you protect your cookies and monitor your SaaS Apps?

Attack Flow

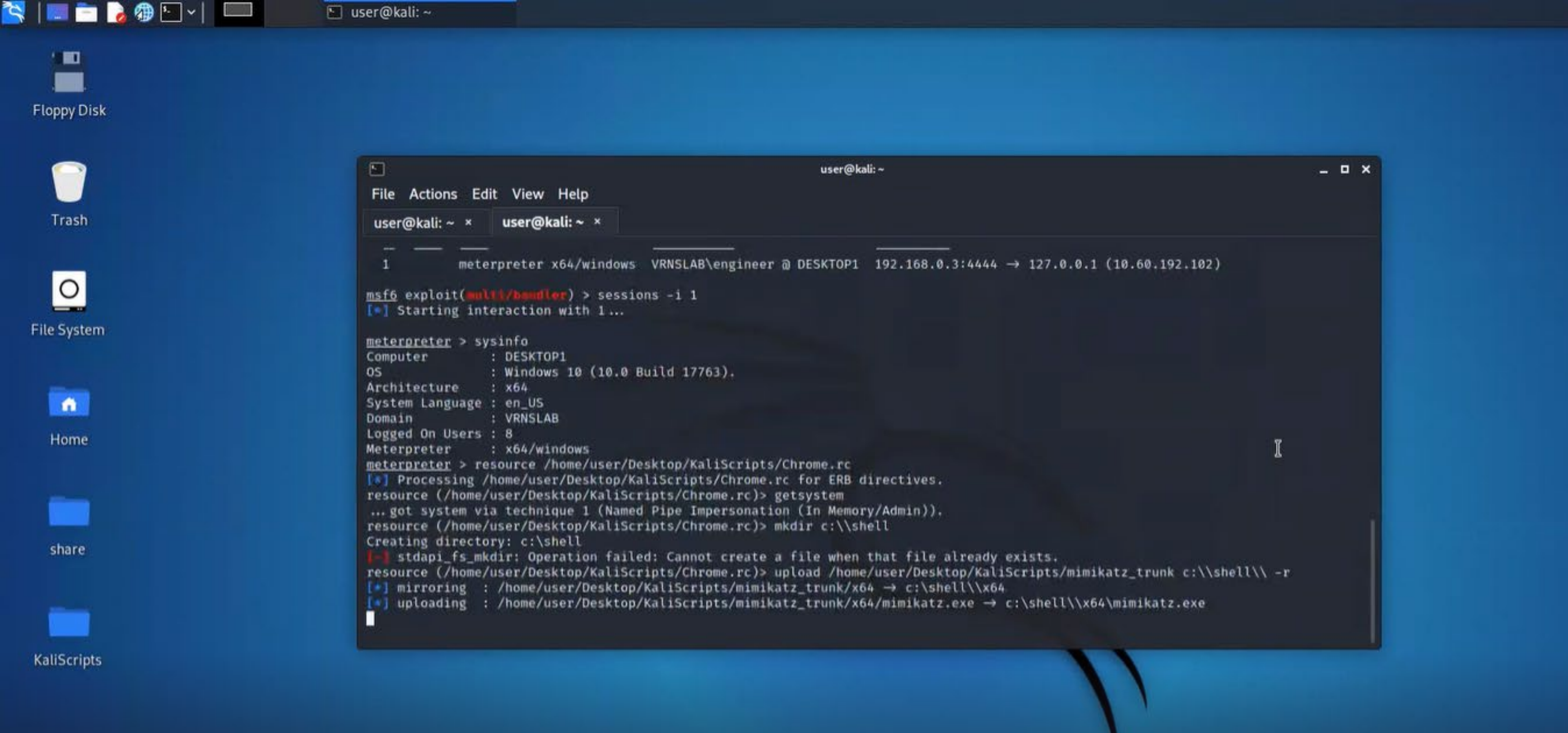

Attacker can connect directly to SF
But may be blocked or discovered by MFA and/or conditional access
Steal browser cookies
Steal browser credentials
Attacker pivots his web traffic through the victim's PC
Office 365
salesforce
okta
Through Reverse Proxy Connection
Phishing Mail
Corporate Employee Desktop


Inbox - Han.Solo@vrnslab.se - Outlook
Engineer
Important changes in the lease contract
contract.xls
277 KB
The Billing sent you a document for consideration and signing.
REVIEW THE ATTACHED DOCUMENT
Principal changes in the lease contract
New conditions and details can be found in the attached file
Please Sign contract.xls
Thank You
Canada Post
Missed Package Delivery
Microsoft Outlook
Undeliverable: test
FinancialManager
Salary Update - Action Nee...
End Users Are Just trying To Do Their Jobs

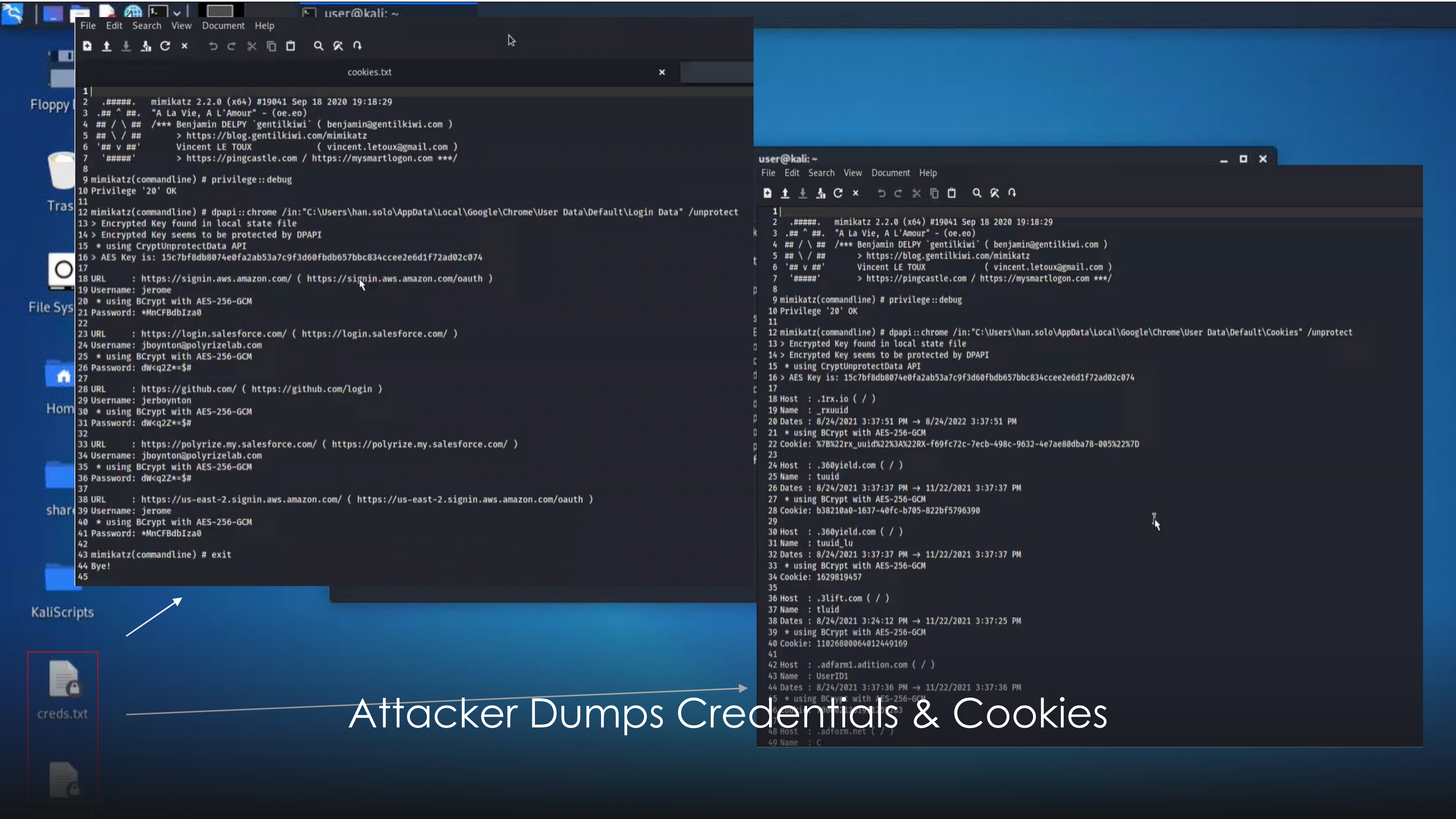

contract (003).xls [Read-Only] [Compatibility Mode] - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me what you want to do
SECURITY WARNING Macros have been disabled.
Enable Content
This document is protected by
Microsoft Office
If you would like to preview this document please press
Enable editing and Enable content



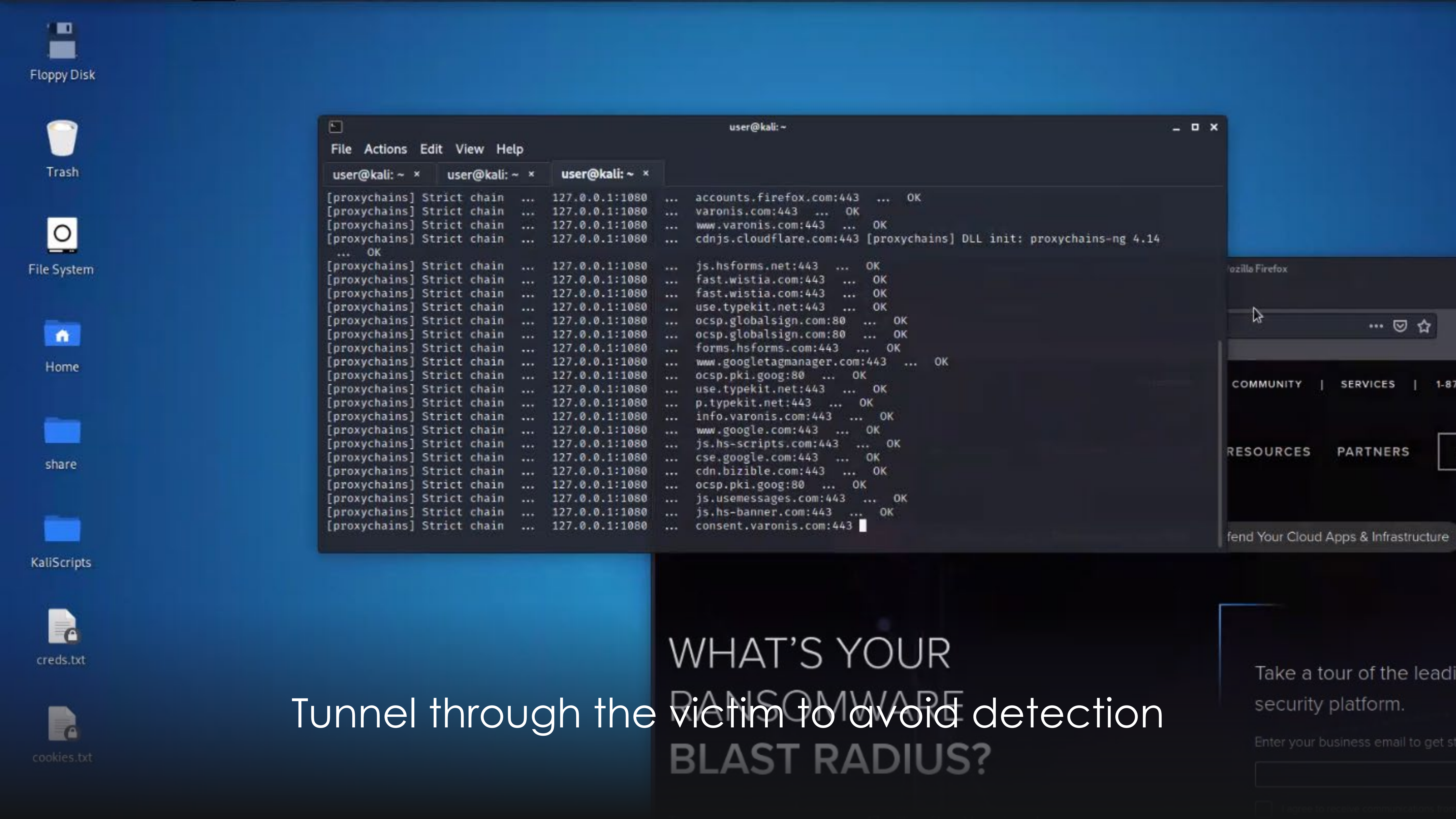
What the Hacker Sees



Browser Gives them the Keys to Your SaaS Kingdom



Attacker Dumps Credentials & Cookies


Floppy Disk
Trash
File System
Home
share
KaliScripts
creds.txt
cookies.txt
user@kali: ~
File Actions Edit View Help
user@kali: ~
user@kali: ~
user@kali: ~
[proxychains] Strict chain ... 127.0.0.1:1080 ... accounts.firefox.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cdnjs.cloudflare.com:443 [proxychains] DLL init: proxychains-ng 4.14
... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hsforms.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... fast.wistia.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... fast.wistia.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... use.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.globalsign.com:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.globalsign.com:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... forms.hsforms.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.googletagmanager.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.pki.goog:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... use.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... p.typekit.net:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... info.varonis.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... www.google.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hs-scripts.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cse.google.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... cdn.bizible.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... ocsp.pki.goog:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.usemessages.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... js.hs-banner.com:443 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... consent.varonis.com:443
COMMUNITY | SERVICES
RESOURCES PARTNERS
WHAT'S YOUR
BLAST RADIUS?
Take a tour of the leadi
security platform.
Tunnel through the victim to avoid detection

Average vs Advanced Attackers

Average Hacker Joe

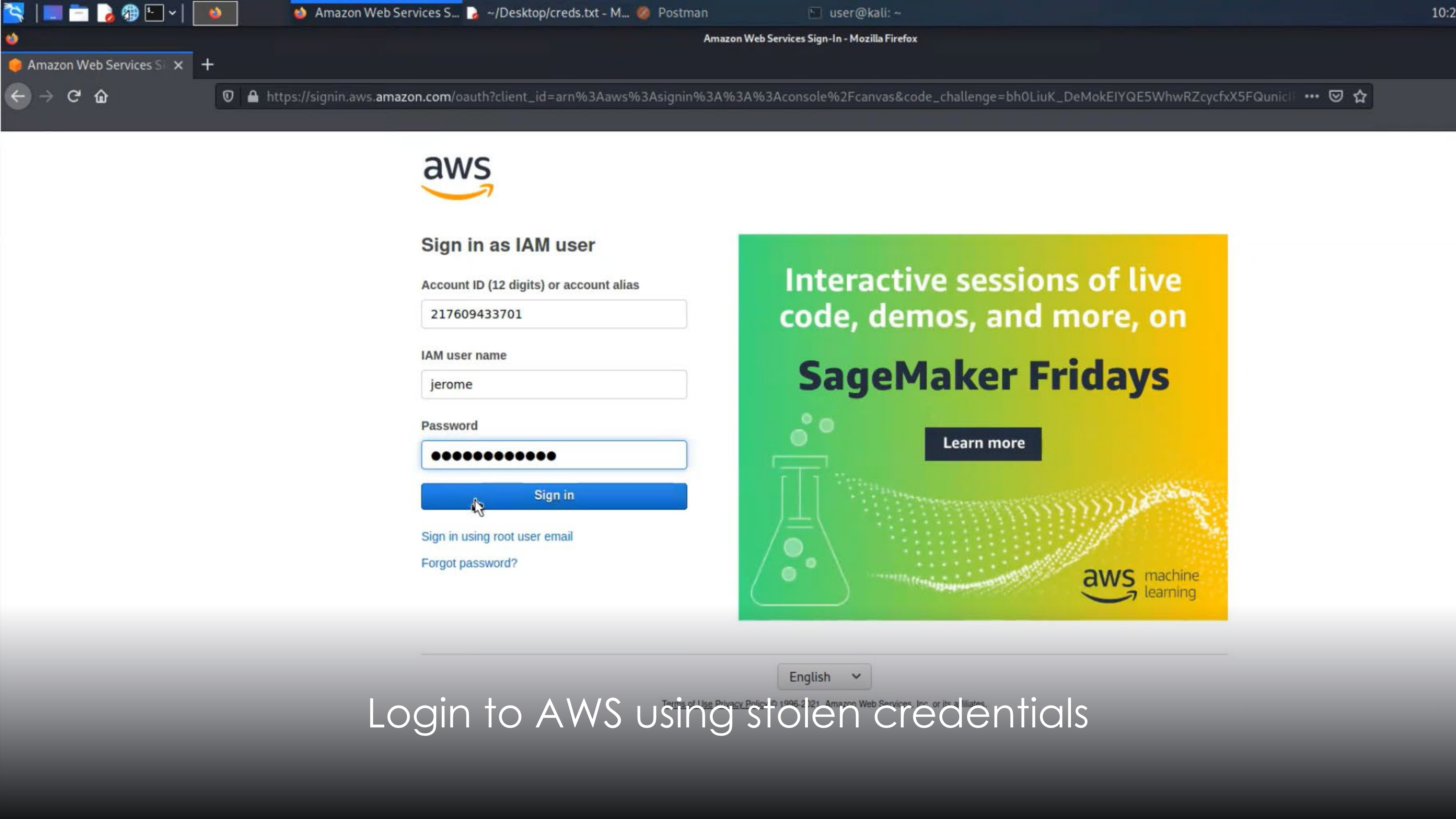
- Average Attacker
  - Compromises Endpoint
  - Pulls down Creds and Cookies
  - Takes them offline to attacker machine
  - Logs in using compromised creds from that machine
- Results
  - Alerts trigger around Geo location
  - Suspicious IP Sources
  - Potentially blocked by conditional access settings

Sophisticated Hacker Snir

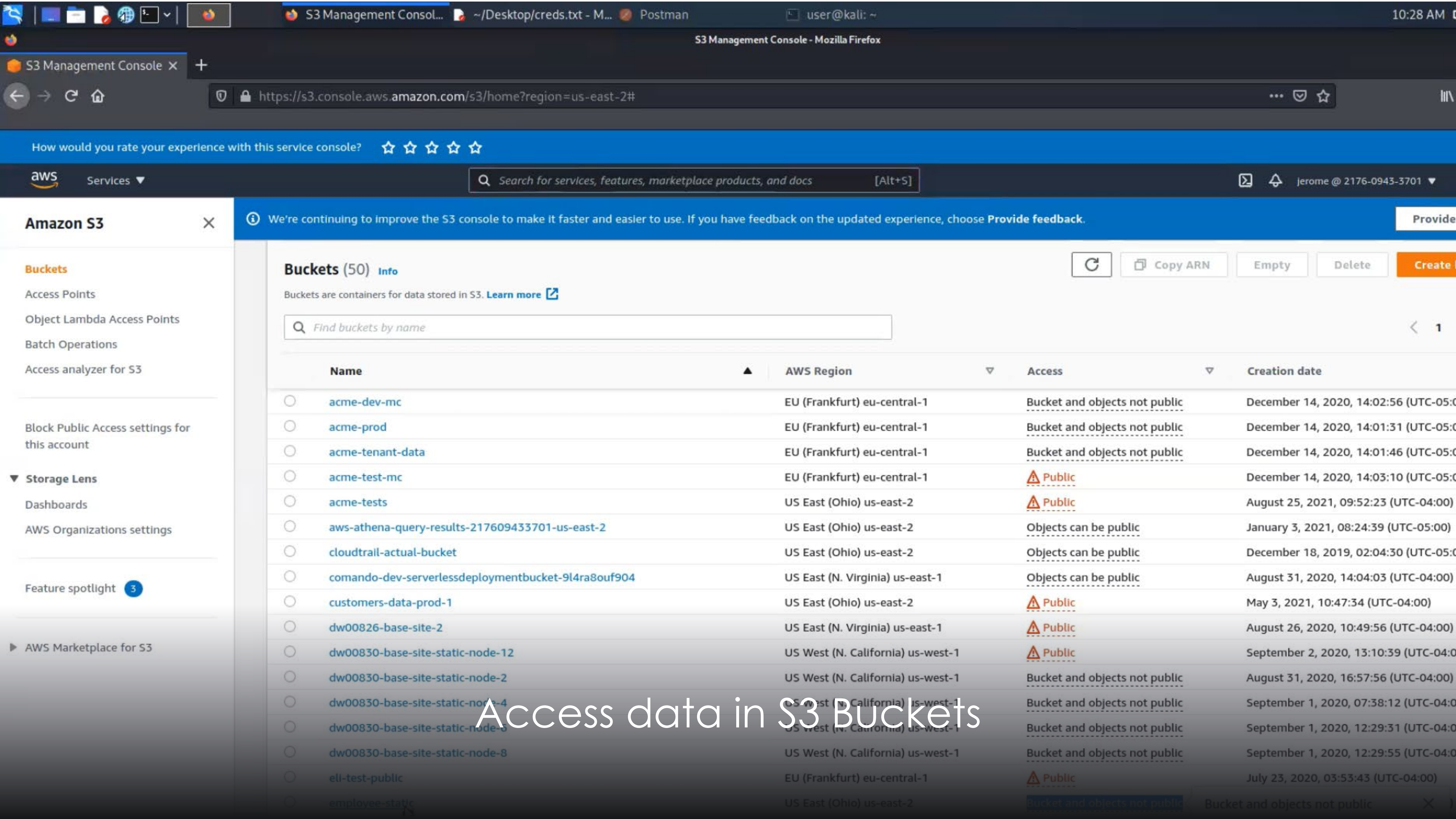
- Advanced Attacker
  - Compromises Endpoint
  - Pulls down Creds and Cookies
  - Route all web traffic through compromised machine using proxy
  - Access Cloud Applications through proxy using compromised creds
- Results
  - No change in geolocation or IP source
  - Not blocked by conditional access

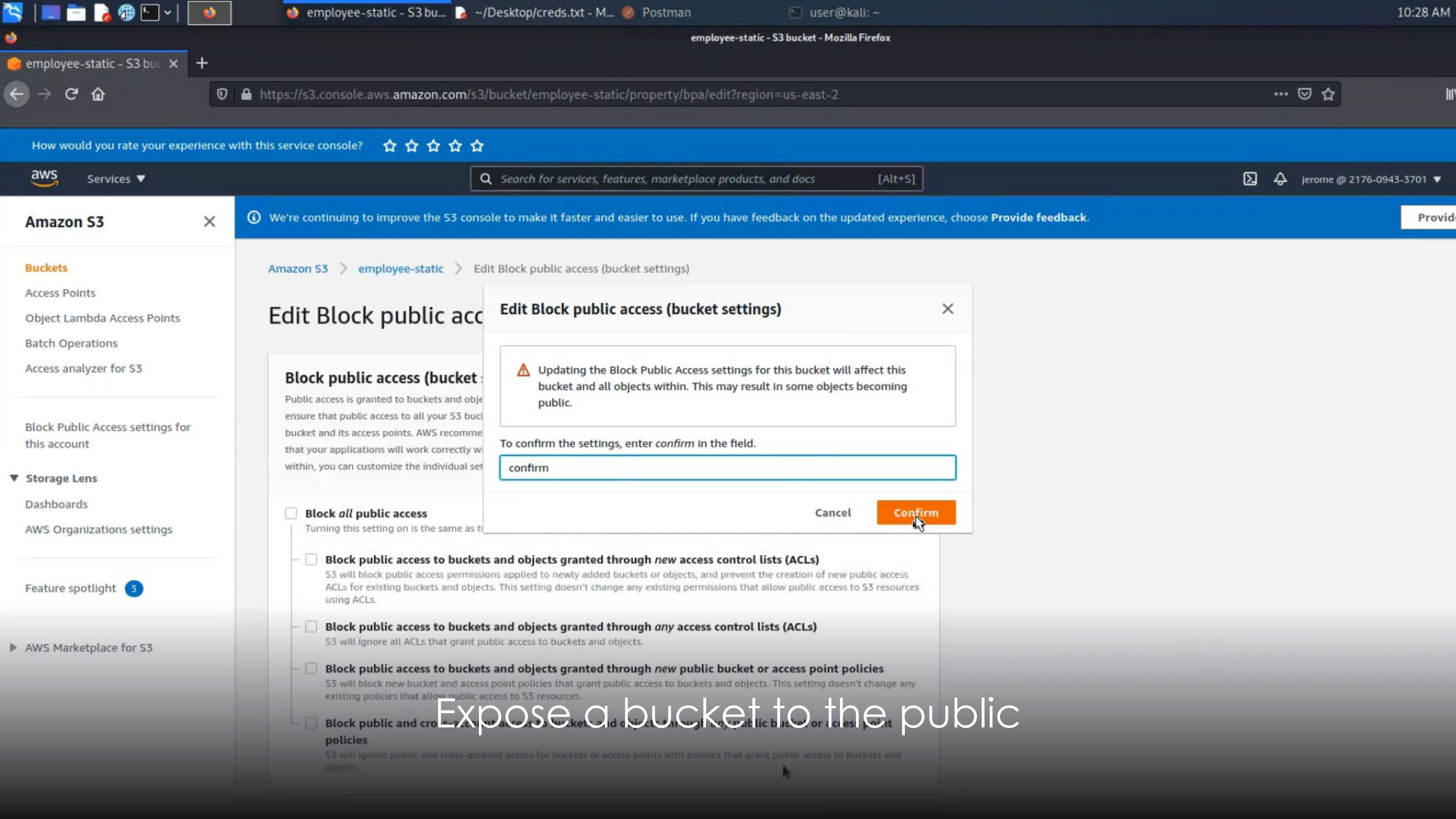
Phase 1 – Initial Foothold on User Machine

- Attack -
  - Establishing command and control of end user computer
  - Scrape all cookies and credentials
  - Proxy traffic through the compromised device to avoid detection or abnormal geo activity
- Detections to Consider
  - C2 Beacon
  - Dumping of Cookies/Credentials on Endpoints
  - New Proxy installed/configured on endpoint

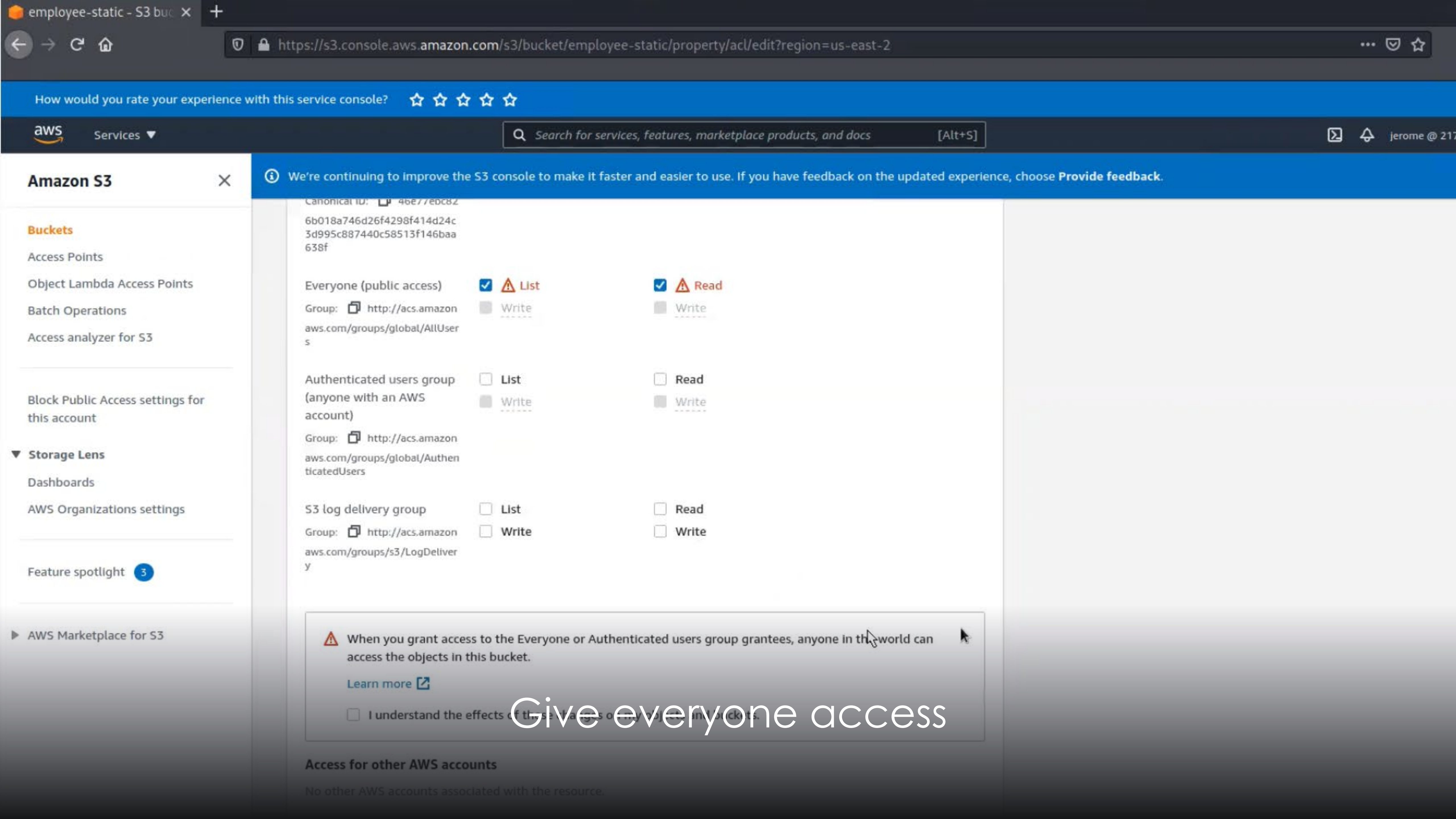


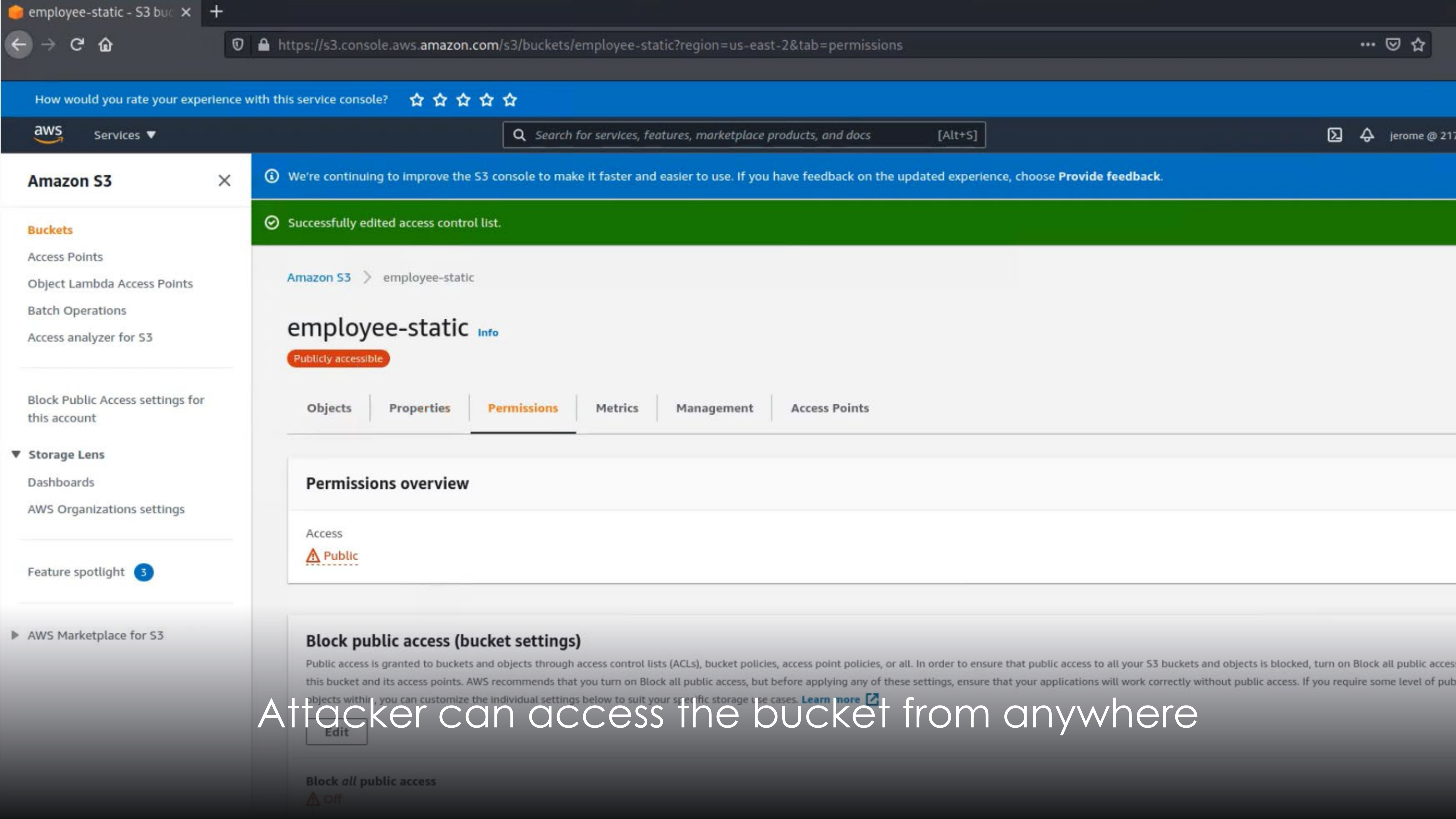
Login to AWS using stolen credentials


S3 Management Console - Mozilla Firefox
https://s3.console.aws.amazon.com/s3/home?region=us-east-2#
How would you rate your experience with this service console?
Services
Search for services, features, marketplace products, and docs [Alt+S]
jerome @ 2176-0943-3701
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
Buckets (50) Info
Copy ARN
Empty
Delete
Buckets are containers for data stored in S3. Learn more
Find buckets by name
Name
AWS Region
Access
Creation date
acme-dev-mc EU (Frankfurt) eu-central-1 Bucket and objects not public December 14, 2020, 14:02:56
acme-prod EU (Frankfurt) eu-central-1 Bucket and objects not public December 14, 2020, 14:01:31
acme-tenant-data EU (Frankfurt) eu-central-1 Bucket and objects not public December 14, 2020, 14:01:46
acme-test-mc EU (Frankfurt) eu-central-1 Public December 14, 2020, 14:03:10
acme-tests US East (Ohio) us-east-2 Public August 25, 2021, 09:52:23 (UTC-04:00)
aws-athena-query-results-217609433701-us-east-2 US East (Ohio) us-east-2 Objects can be public January 3, 2021, 08:24:39 (UTC-05:00)
cloudtrail-actual-bucket US East (Ohio) us-east-2 Objects can be public December 18, 2019, 02:04:30
comando-dev-serverlessdeploymentbucket-9l4ra8ouf904 US East (N. Virginia) us-east-1 Objects can be public August 31, 2020, 14:04:03 (UTC-04:00)
customers-data-prod-1 US East (Ohio) us-east-2 Public May 3, 2021, 10:47:34 (UTC-04:00)
dw00826-base-site-2 US East (N. Virginia) us-east-1 Public August 26, 2020, 10:49:56 (UTC-04:00)
dw00830-base-site-static-node-12 US West (N. California) us-west-1 Public September 2, 2020, 13:10:39
dw00830-base-site-static-node-2 US West (N. California) us-west-1 Bucket and objects not public August 31, 2020, 16:57:56 (UTC-04:00)
Bucket and objects not public September 1, 2020, 07:38:12
Bucket and objects not public September 1, 2020, 12:29:31
dw00830-base-site-static-node-8 US West (N. California) us-west-1 Bucket and objects not public September 1, 2020, 12:29:55
eli-test-public EU (Frankfurt) eu-central-1 Public July 23, 2020, 03:53:43 (UTC-04:00)
Access data in S3 Buckets



Expose a bucket to the public

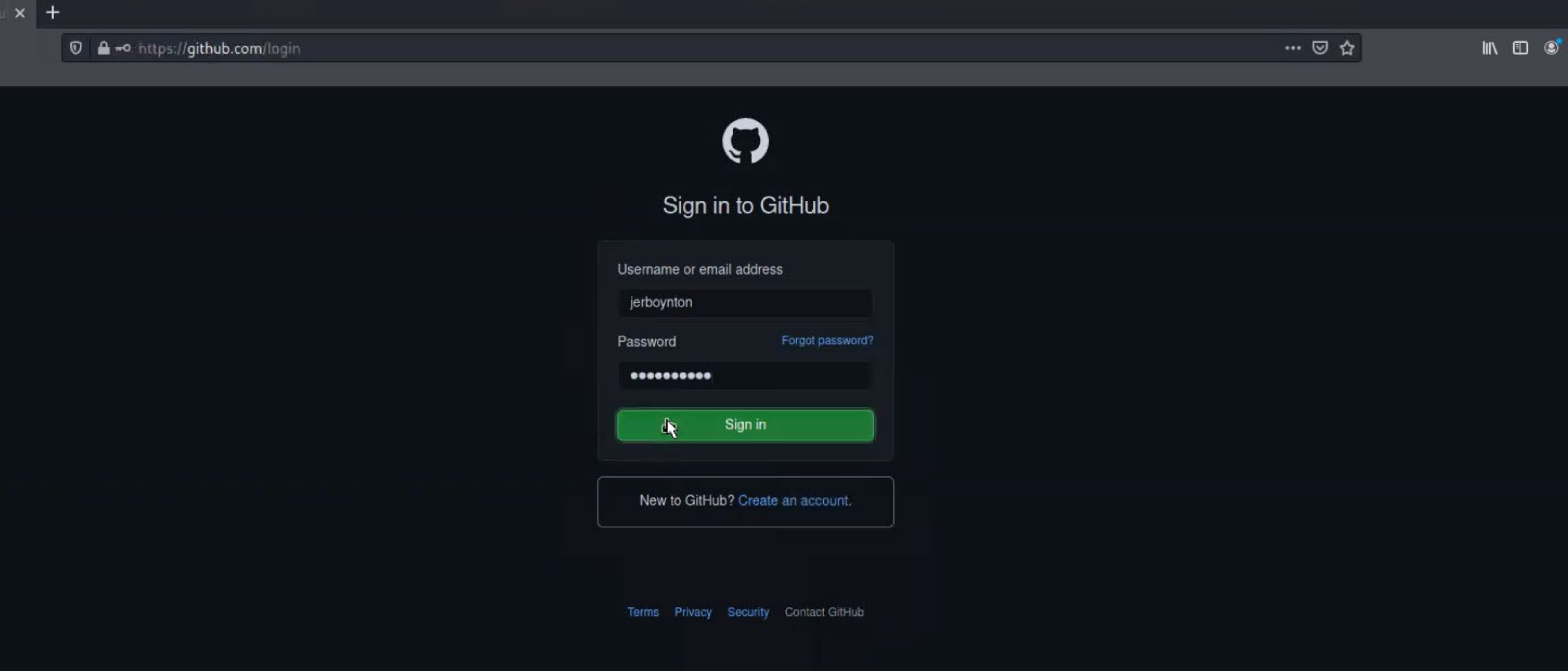

employee-static - S3 buc
https://s3.console.aws.amazon.com/s3/bucket/employee-static/property/acl/edit?region=us-east-2
How would you rate your experience with this service console?
aws
Services
Search for services, features, marketplace products, and docs
[Alt+S]
jerome @ 21
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
6b018a746d26f4298f414d24c
3d995c887440c58513f146baa
638f
Everyone (public access)
Group: http://acs.amazon
aws.com/groups/global/AllUser
s
List
Write
Read
Write
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazon
aws.com/groups/global/Authen
ticatedUsers
List
Write
Read
Write
S3 log delivery group
Group: http://acs.amazon
aws.com/groups/s3/LogDeliver
y
List
Write
Read
Write
When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.
Learn more
I understand the effects
Access for other AWS accounts
Give everyone access



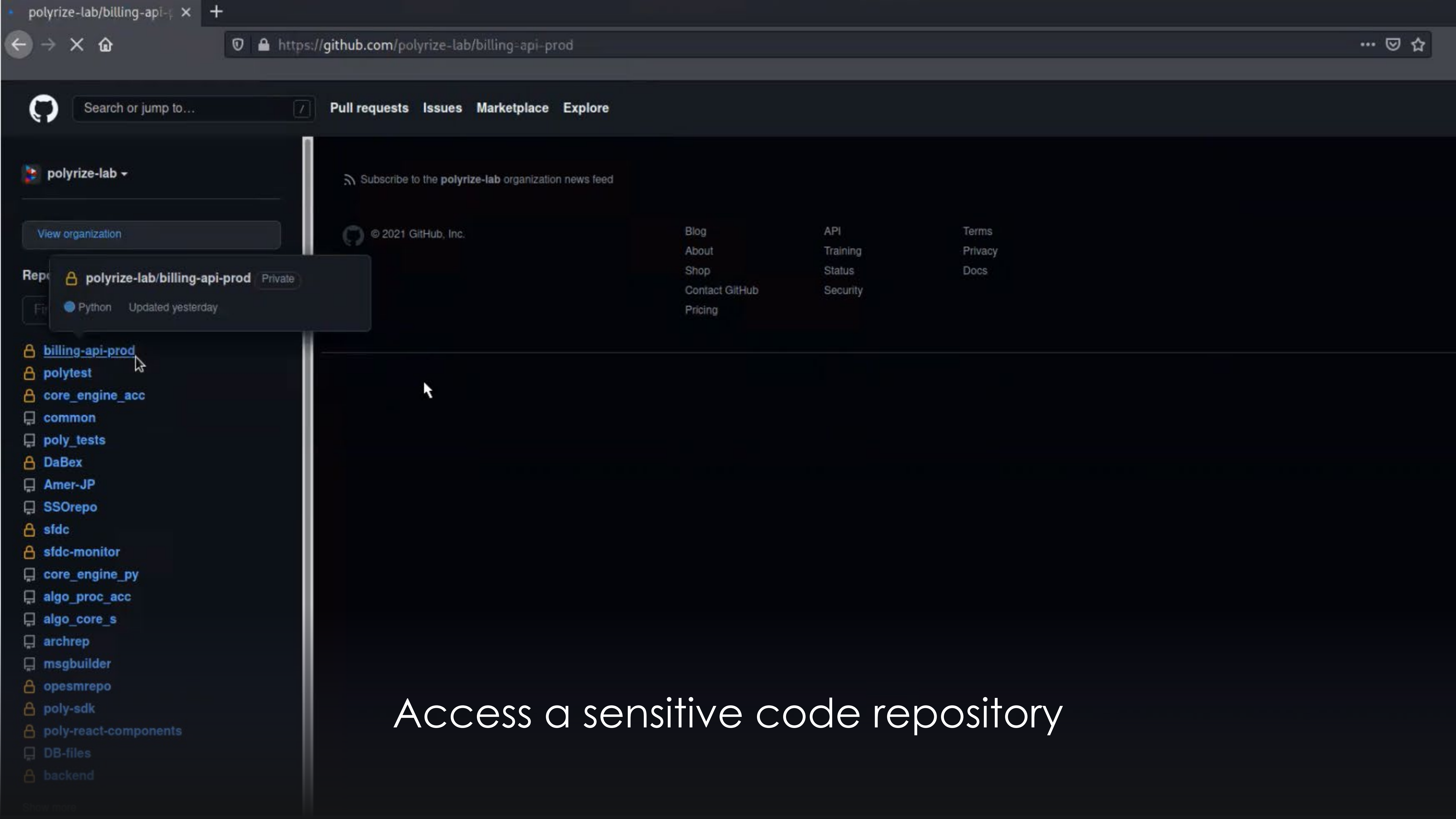
Attacker can access the bucket from anywhere

Phase 2 – AWS S3 Bucket Theft

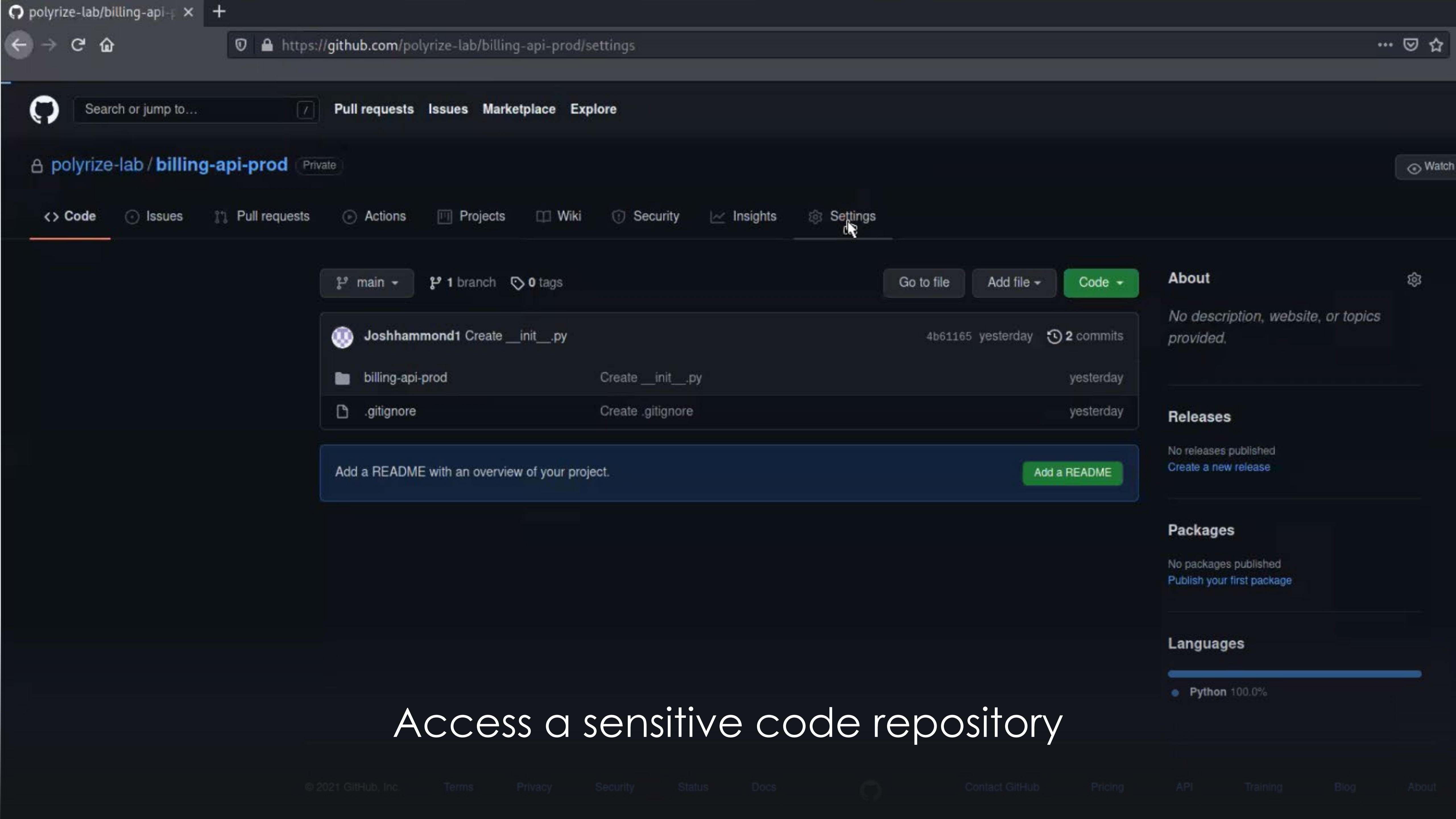
- Attack -
  - Use stolen cookie to impersonate AWS Admin
  - Set Private Bucket to Public
  - Download Publicly exposed data
- Detections to Consider
  - S3 Bucket set Public
  - Abnormal Access / Download of S3 Objects



Access GitHub with stolen credentials



Access a sensitive code repository



Access a sensitive code repository

https://github.com/polyrize-lab/billing-api-prod/settings

Archives

When creating source code archives, you can choose to include files stored using Git LFS in the archive.

- [ ] **Include Git LFS objects in archives**
  Git LFS usage in archives is billed at the same rate as

GitHub Pages

Pages settings now has its own dedicated tab! Ch

Danger Zone

Change repository visibility
This repository is currently private.

Change visibility

Transfer ownership
Transfer this repository to another user or to an org

Transfer

Archive this repository
Mark this repository as archived and read-only.

Archive this repository

Delete this repository
Once you delete a repository, there is no going back. Please be certain.

Delete this repository

Change repository visibility

Warning: this is a potentially destructive action.

Make public
Make this repository visible to anyone.

- The code will be visible to everyone who can visit https://github.com
- Anyone can fork your repository.
- Your changes will be published as activity.

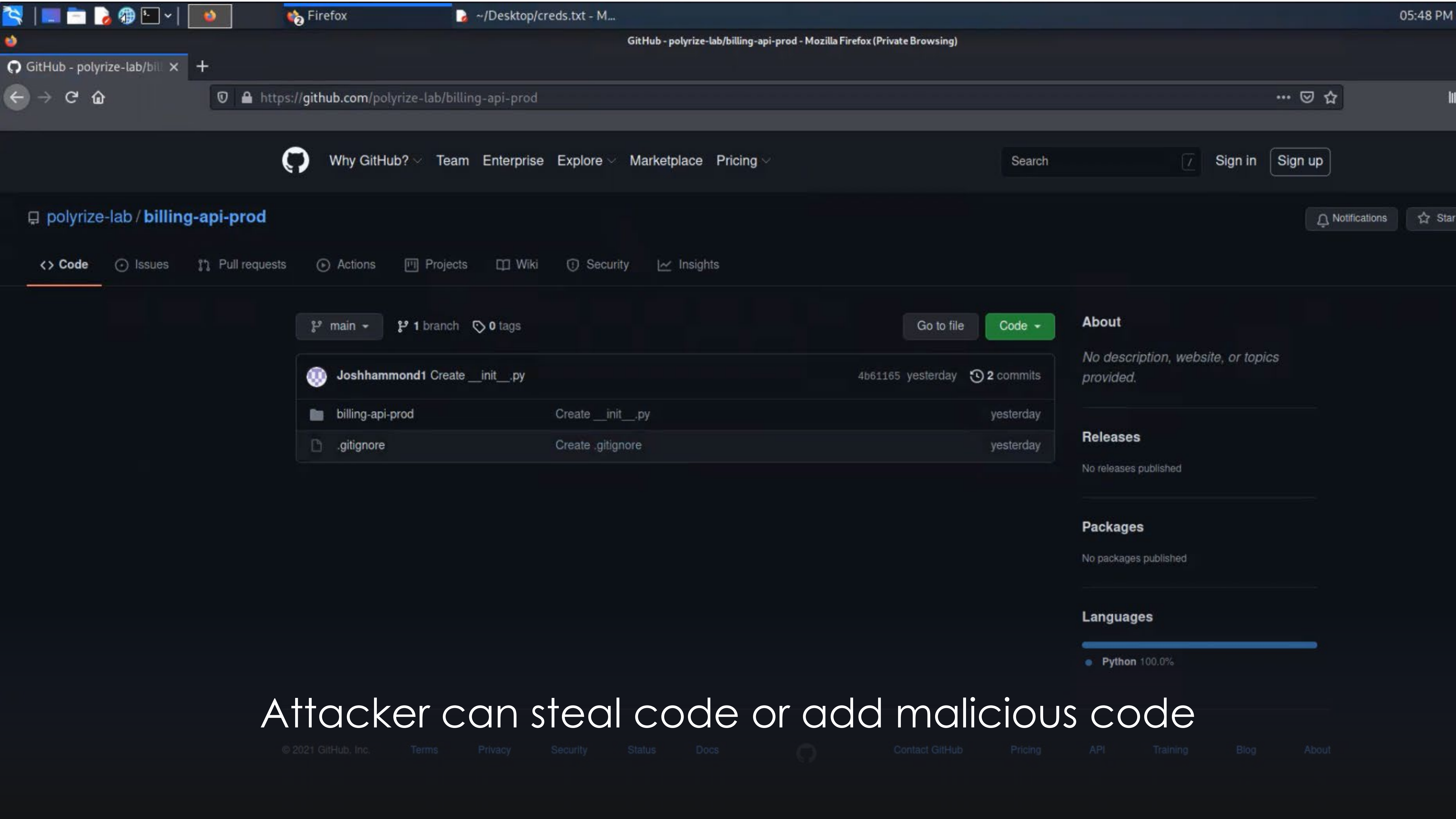
Make private
This repository is currently private.

Please type **polyrize-lab/billing-api-prod** to confirm.

polyrize-lab/billing-api-prod

I understand, change repository visibility.

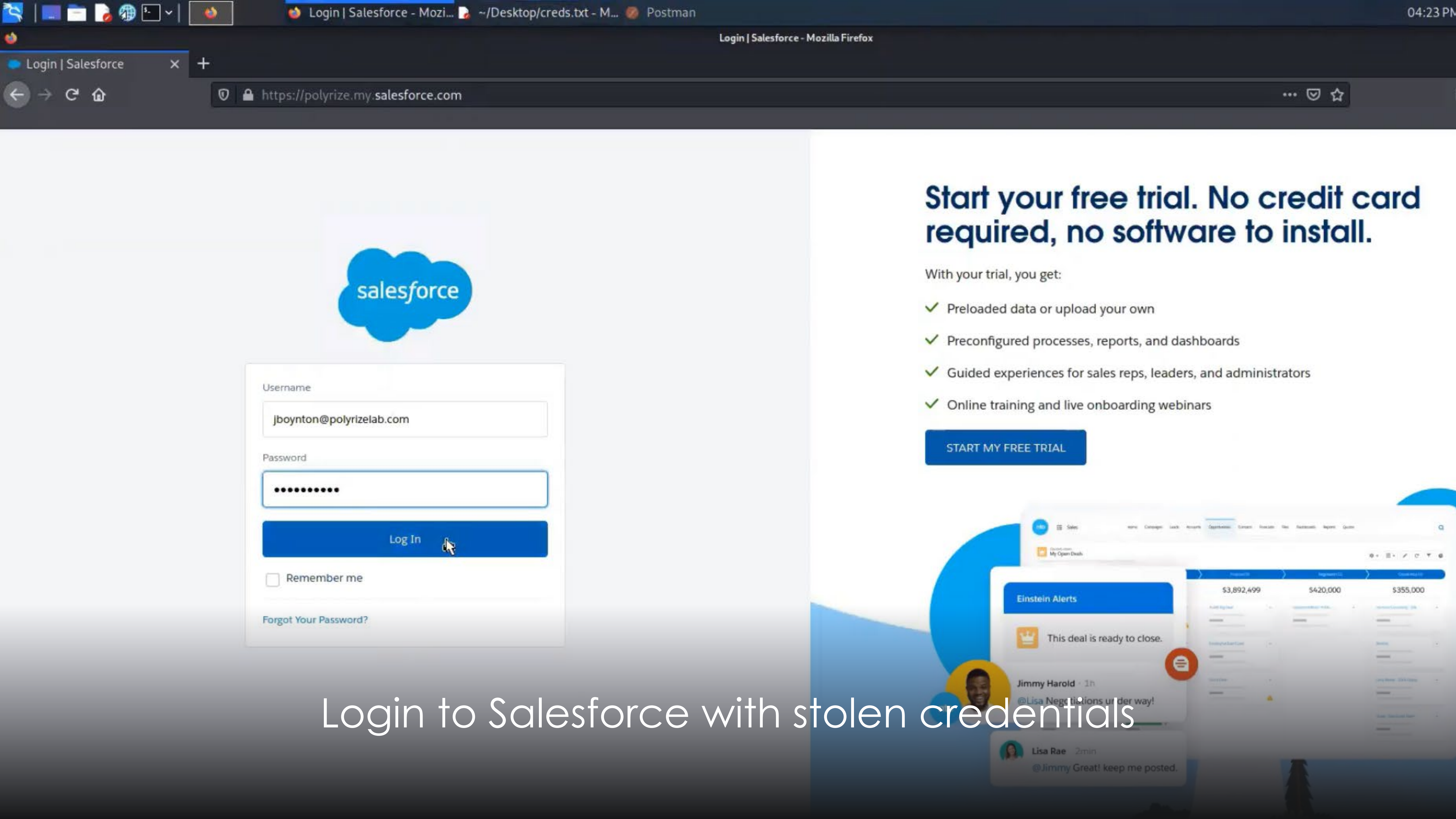
Make the repository public

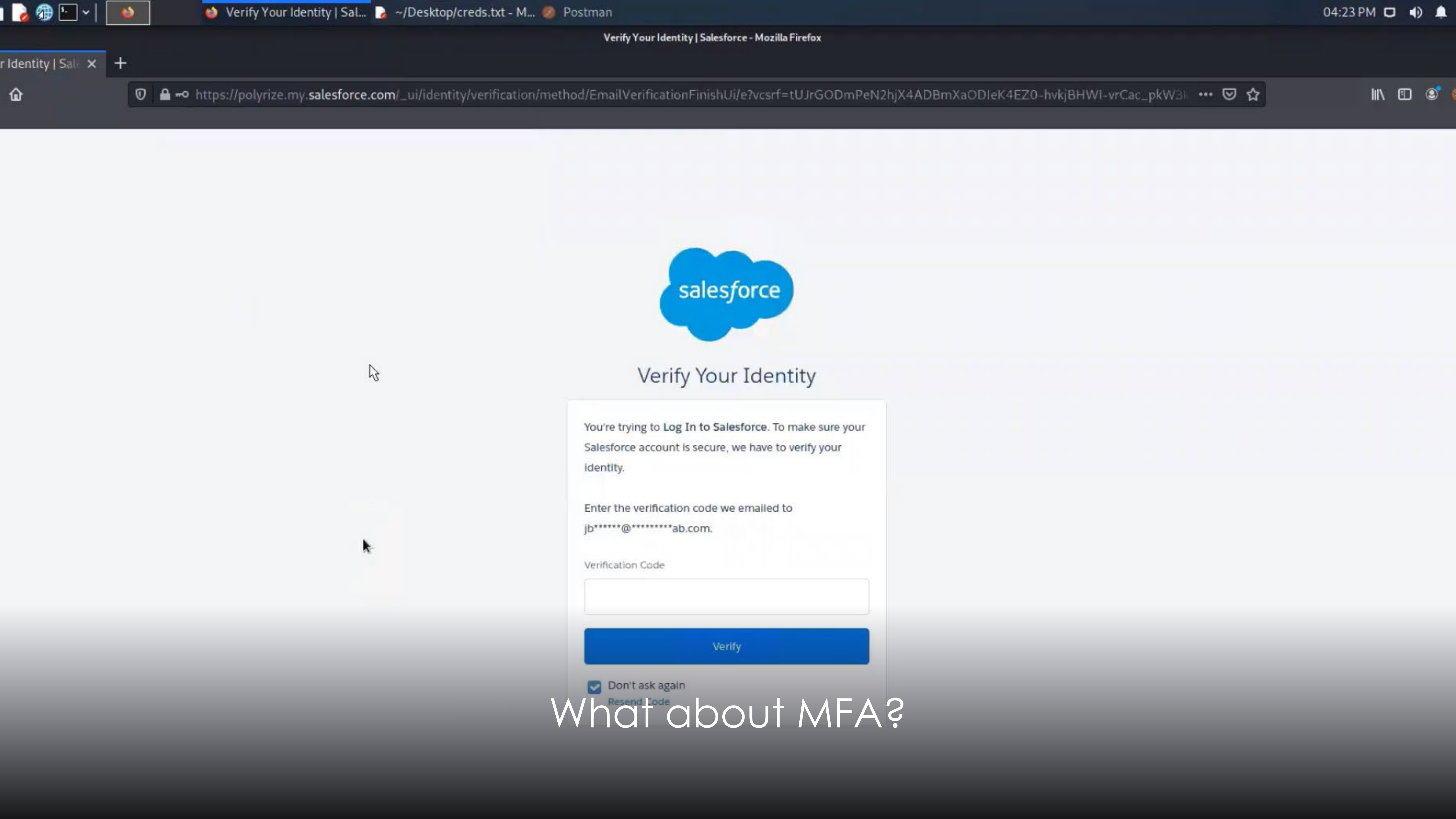


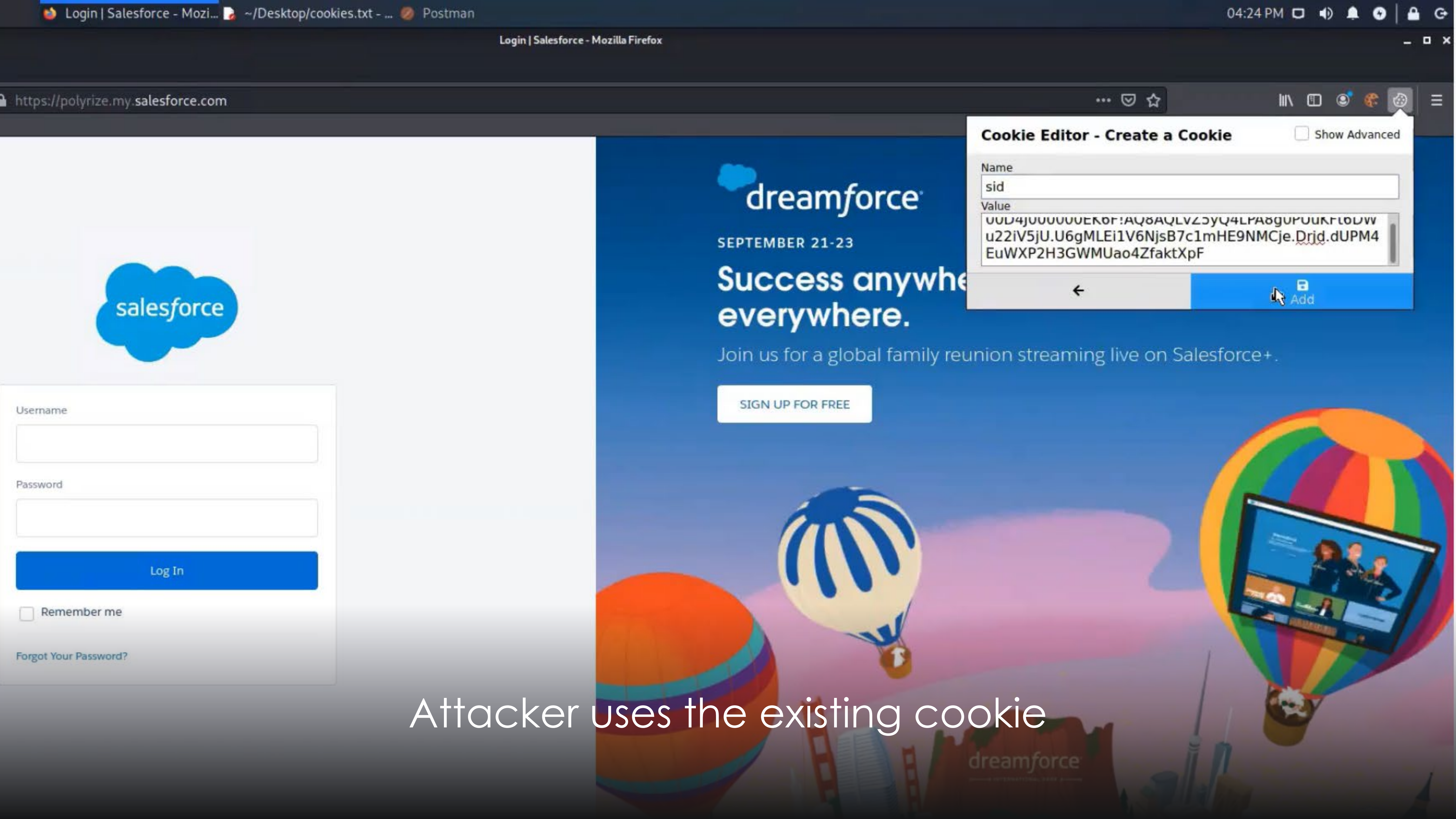
Attacker can steal code or add malicious code

Phase 3 – GitHub Repo Theft

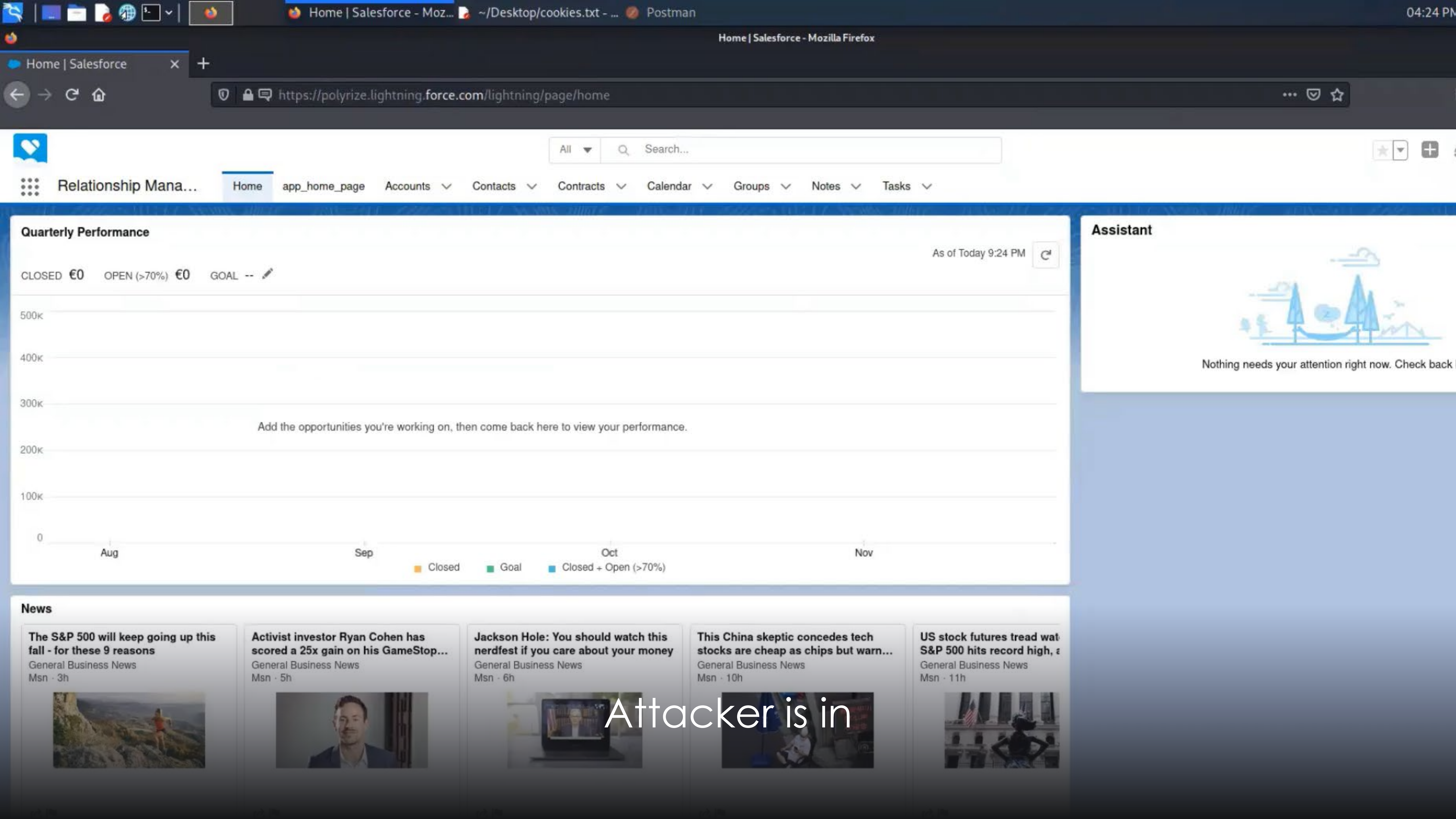
- Attack -
  - Use stolen cookie to impersonate GitHub
  - Set Private repo to Public
  - Download Publicly exposed data
- Detections to Consider
  - Repo set Public

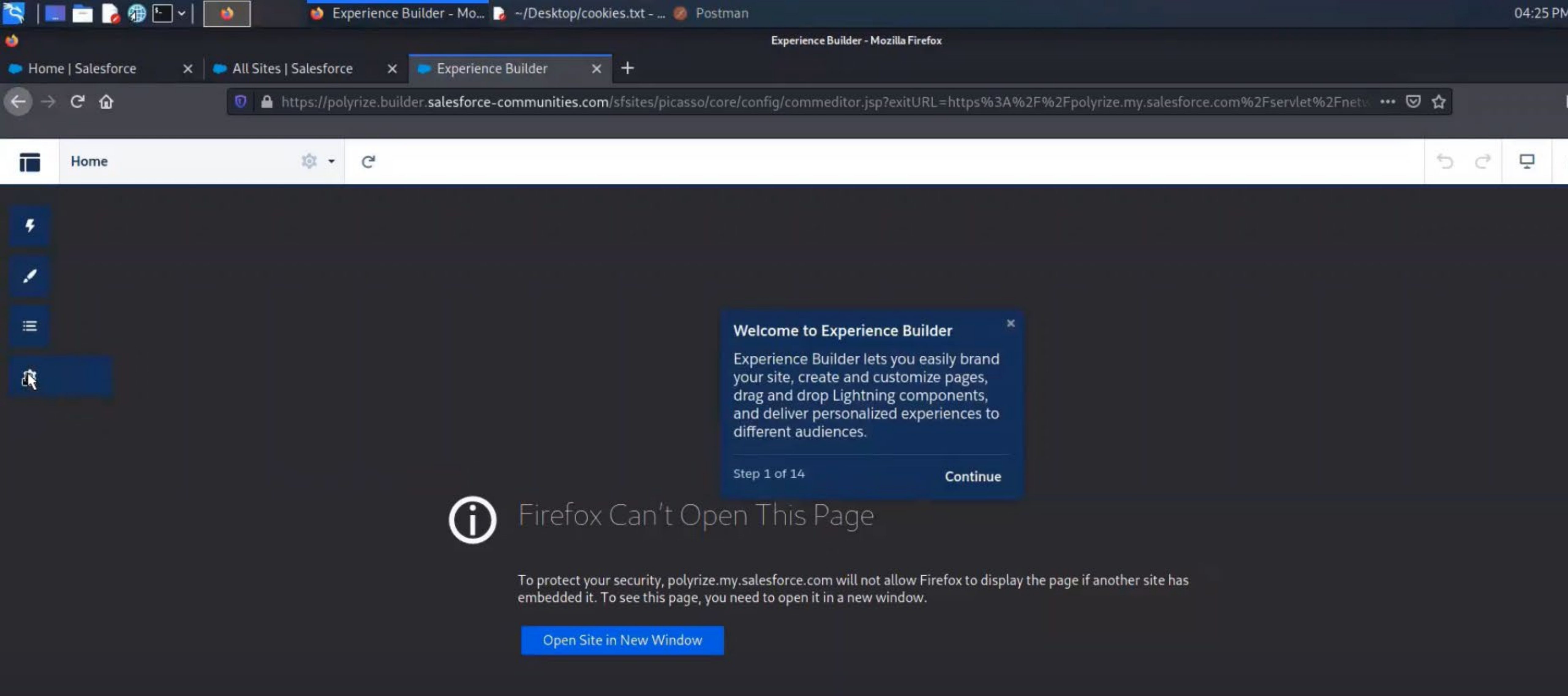

Login | Salesforce - Mozi...
~/Desktop/creds.txt - M...
Postman
04:23 PM
Login | Salesforce - Mozilla Firefox
Login | Salesforce
https://polyrize.my.salesforce.com
salesforce
Username
jboynton@polyrizelab.com
Password
Log In
Remember me
Forgot Your Password?
Start your free trial. No credit card required, no software to install.
With your trial, you get:
Preloaded data or upload your own
Preconfigured processes, reports, and dashboards
Guided experiences for sales reps, leaders, and administrators
Online training and live onboarding webinars
START MY FREE TRIAL
Einstein Alerts
This deal is ready to close.
$3,892,499
$420,000
$355,000
Jimmy Harold
Lisa Rae
@Jimmy Great! keep me posted.
Login to Salesforce with stolen credentials


Verify Your Identity | Sal...
~/Desktop/creds.txt - M...
Postman
04:23 PM
Verify Your Identity | Salesforce - Mozilla Firefox
https://polyrize.my.salesforce.com/_ui/identity/verification/method/EmailVerificationFinishUi/e?vcsrf=tUJrGODmPeN2hjX4ADBmXaODIeK4EZ0-hvkjBHWI-vrCac_pkW3
salesforce
Verify Your Identity
You're trying to Log In to Salesforce. To make sure your Salesforce account is secure, we have to verify your identity.
Enter the verification code we emailed to jb******@*********ab.com.
Verification Code
Verify
Don't ask again
Resend Code
What about MFA?

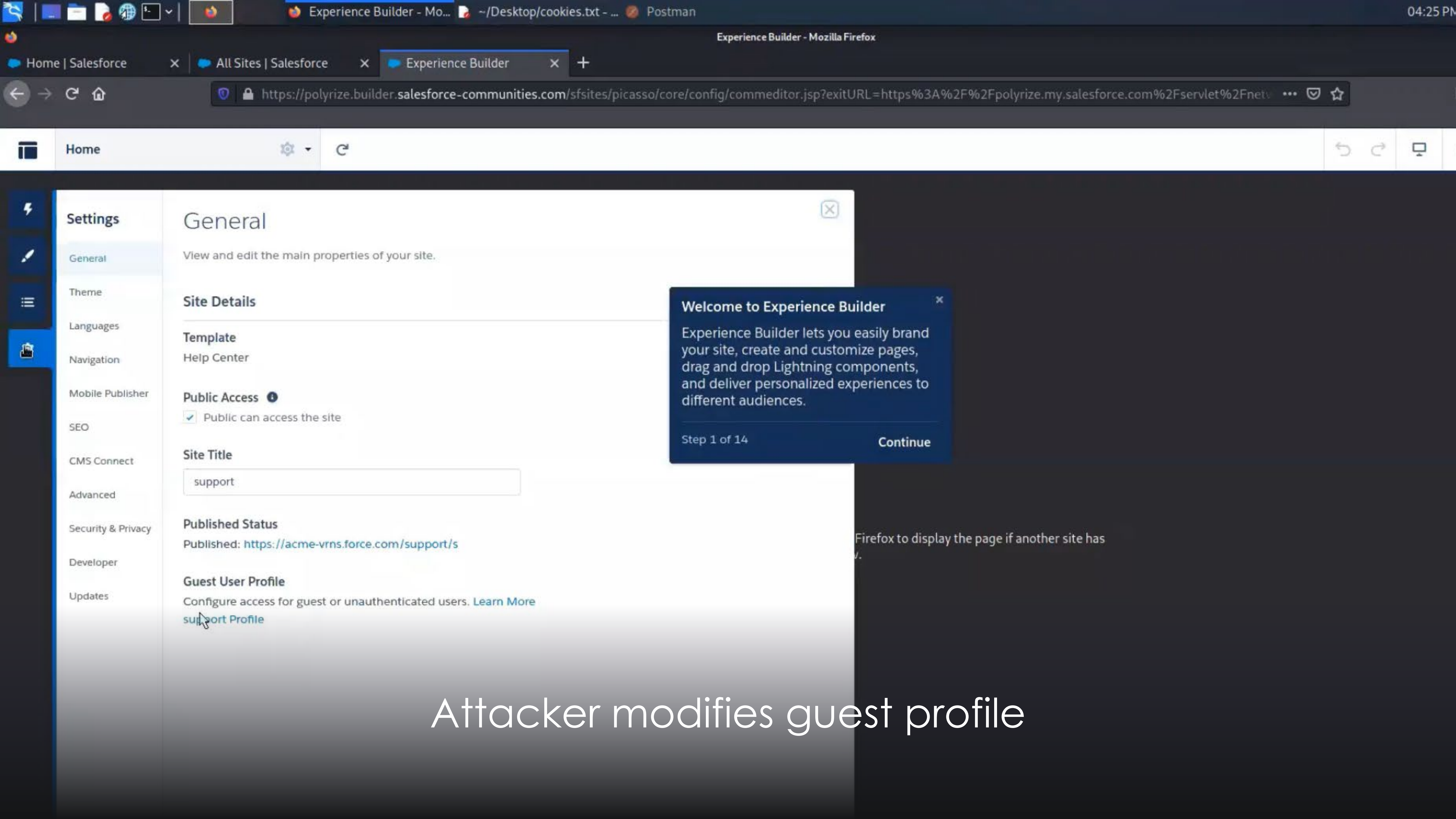


Attacker uses the existing cookie

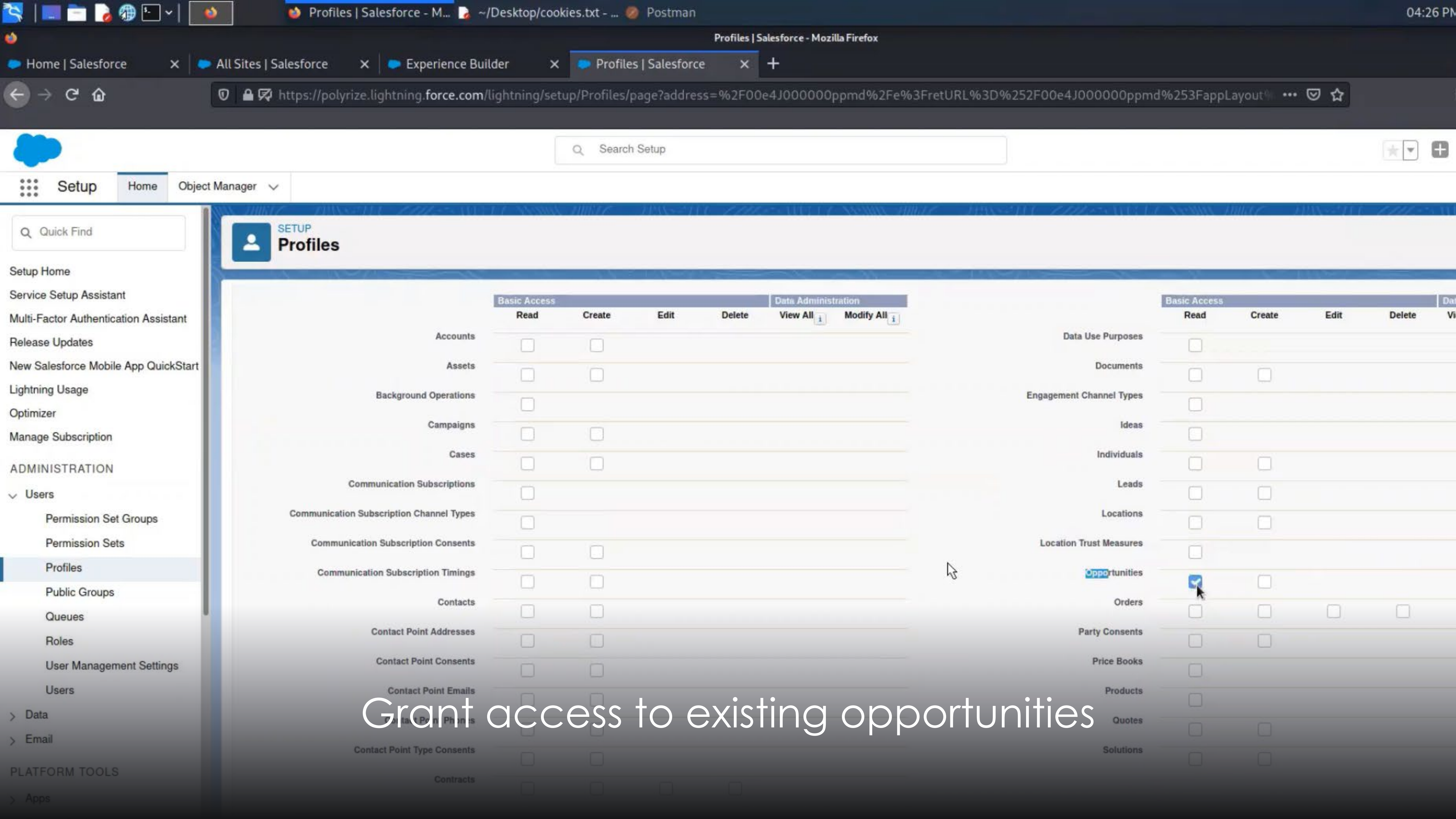

Home | Salesforce - Moz...
~/Desktop/cookies.txt - ...
Postman
04:24 PM
Home | Salesforce - Mozilla Firefox
Home | Salesforce
https://polyrize.lightning.force.com/lightning/page/home
All
Search...
Relationship Mana...
Home
app_home_page
Accounts
Contacts
Contracts
Calendar
Groups
Notes
Tasks
Quarterly Performance
As of Today 9:24 PM
CLOSED €0
OPEN (>70%) €0
GOAL --
500K
400K
300K
200K
100K
0
Add the opportunities you're working on, then come back here to view your performance.
Aug
Sep
Oct
Nov
Closed
Goal
Closed + Open (>70%)
Assistant
Nothing needs your attention right now. Check back
News
The S&P 500 will keep going up this fall - for these 9 reasons
General Business News
Msn · 3h
Activist investor Ryan Cohen has scored a 25x gain on his GameStop...
General Business News
Msn · 5h
Jackson Hole: You should watch this nerdfest if you care about your money
General Business News
Msn · 6h
This China skeptic concedes tech stocks are cheap as chips but warn...
General Business News
Msn · 10h
General Business News
Msn · 11h
Attacker is in

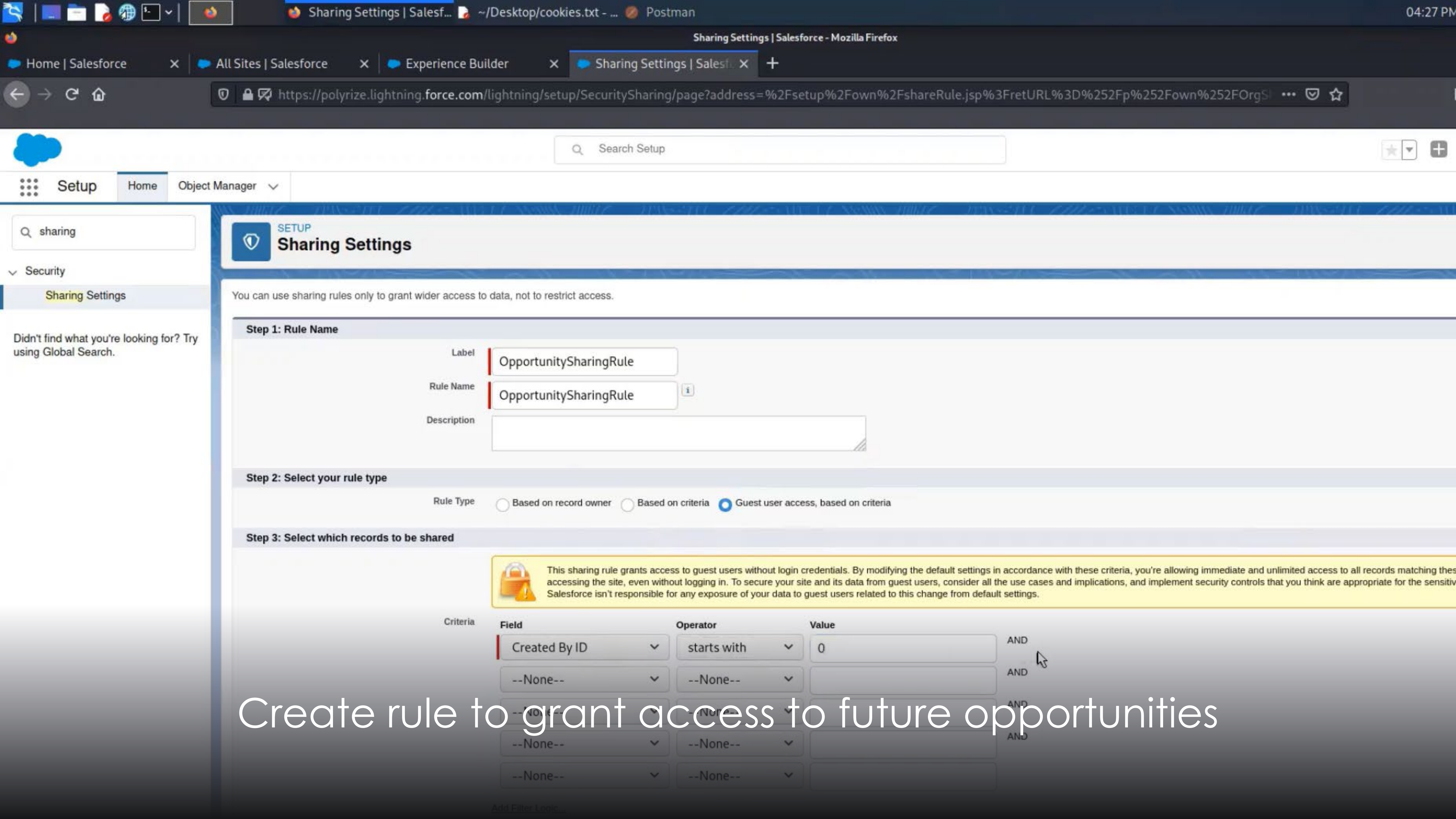


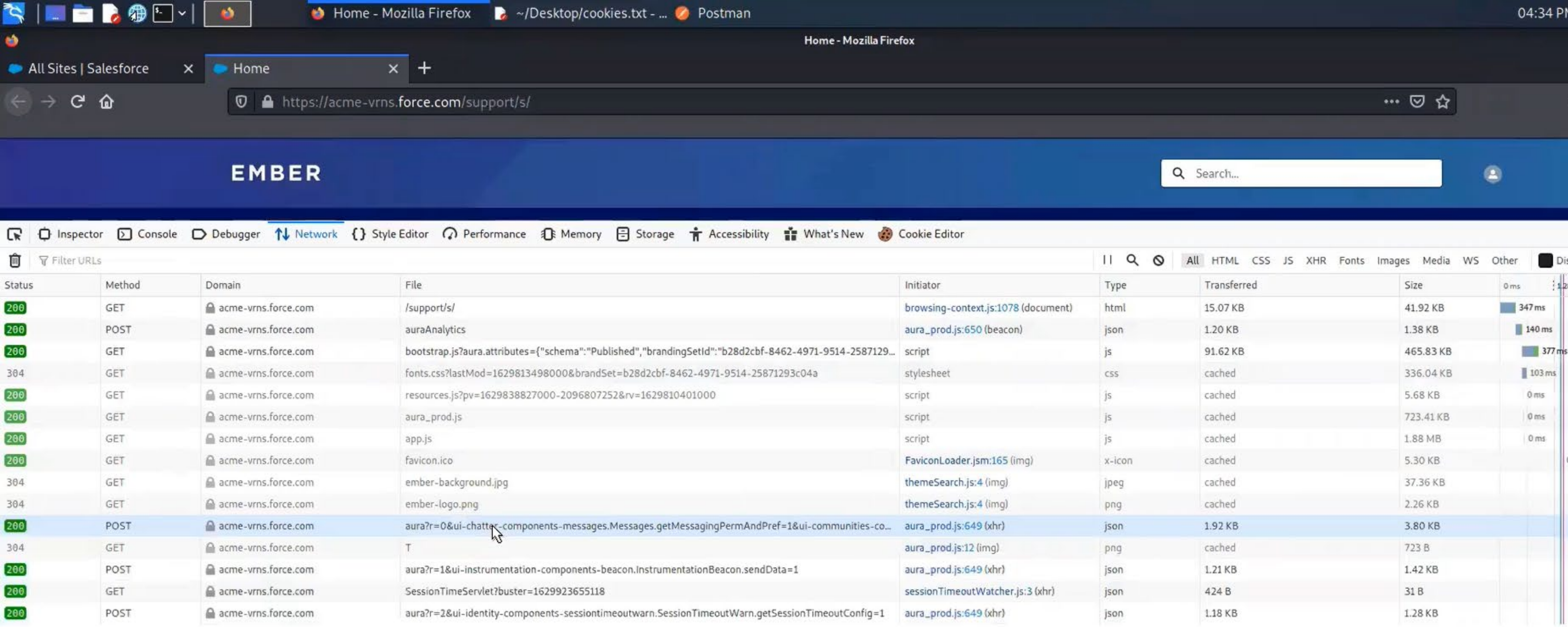
SF guest profile can't access data



Attacker modifies guest profile

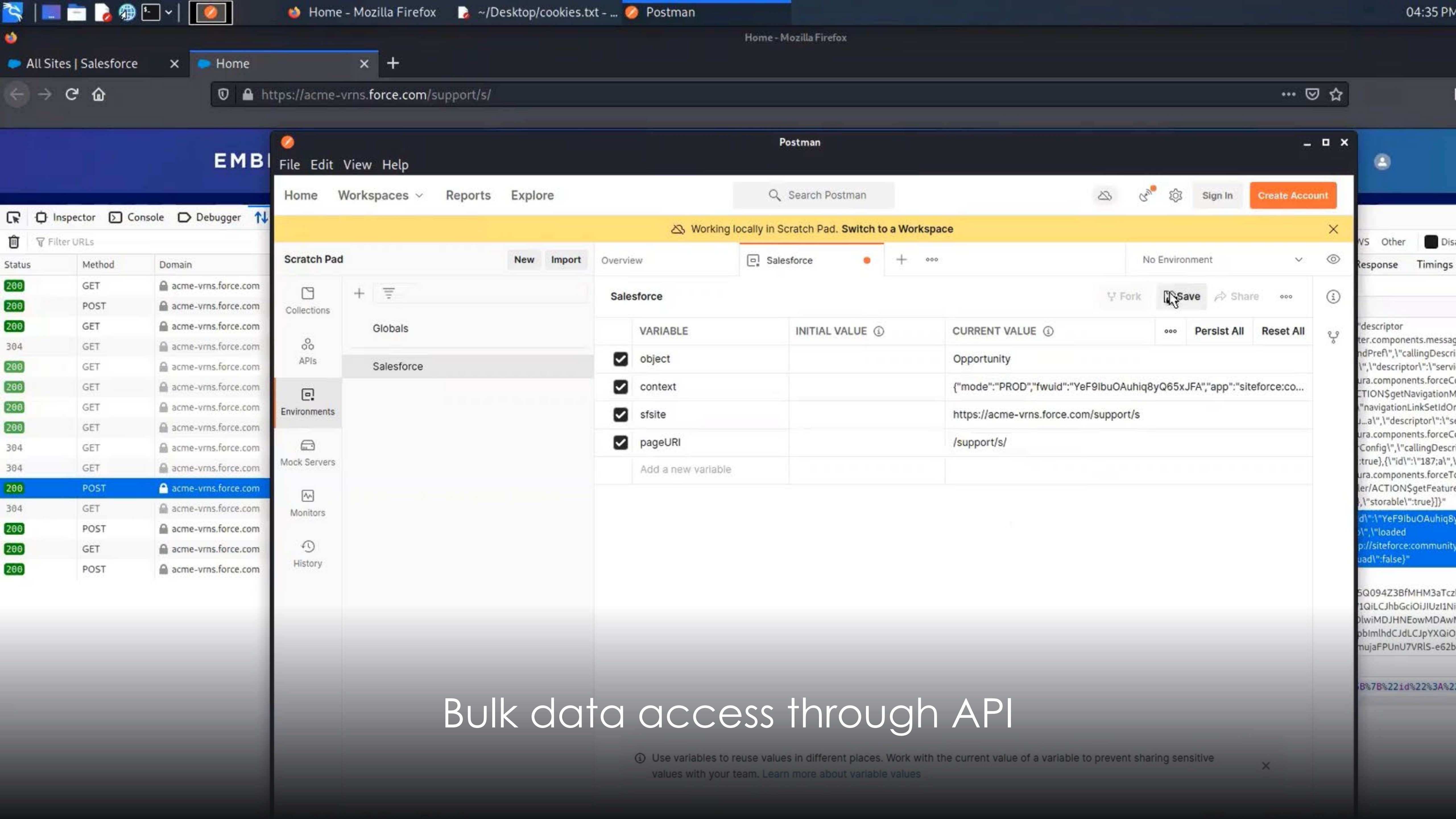

Profiles | Salesforce - Mozilla Firefox
Home | Salesforce
All Sites | Salesforce
Experience Builder
Profiles | Salesforce
https://polyrize.lightning.force.com/lightning/setup/Profiles/page?address=%2F00e4J000000ppmd%2Fe%3FretURL%3D%252F00e4J000000ppmd%253FappLayout
Search Setup
Setup
Home
Object Manager
Quick Find
Setup Home
Service Setup Assistant
Multi-Factor Authentication Assistant
Release Updates
New Salesforce Mobile App QuickStart
Lightning Usage
Optimizer
Manage Subscription
ADMINISTRATION
Users
Permission Set Groups
Permission Sets
Profiles
Public Groups
Queues
Roles
User Management Settings
Users
Data
Email
PLATFORM TOOLS
SETUP
Profiles
Basic Access
Data Administration
Read
Create
Edit
Delete
View All
Modify All
Accounts
Assets
Background Operations
Campaigns
Cases
Communication Subscriptions
Communication Subscription Channel Types
Communication Subscription Consents
Communication Subscription Timings
Contacts
Contact Point Addresses
Contact Point Consents
Contact Point Emails
Contact Point Type Consents
Contracts
Data Use Purposes
Documents
Engagement Channel Types
Ideas
Individuals
Leads
Locations
Location Trust Measures
Opportunities
Orders
Party Consents
Price Books
Products
Quotes
Solutions
Grant access to existing opportunities


Sharing Settings | Salesf...
~/Desktop/cookies.txt - ...
Postman
04:27 PM
Sharing Settings | Salesforce - Mozilla Firefox
Home | Salesforce
All Sites | Salesforce
Experience Builder
Sharing Settings | Salesf...
https://polyrize.lightning.force.com/lightning/setup/SecuritySharing/page?address=%2Fsetup%2Fown%2FshareRule.jsp%3FretURL%3D%252Fp%252Fown%252FOrgS
Search Setup
Setup
Home
Object Manager
sharing
Security
Sharing Settings
Didn't find what you're looking for? Try using Global Search.
SETUP
Sharing Settings
You can use sharing rules only to grant wider access to data, not to restrict access.
Step 1: Rule Name
Label
OpportunitySharingRule
Rule Name
OpportunitySharingRule
Description
Step 2: Select your rule type
Rule Type
Based on record owner
Based on criteria
Guest user access, based on criteria
Step 3: Select which records to be shared
This sharing rule grants access to guest users without login credentials. By modifying the default settings in accordance with these criteria, you're allowing immediate and unlimited access to all records matching thes
accessing the site, even without logging in. To secure your site and its data from guest users, consider all the use cases and implications, and implement security controls that you think are appropriate for the sensitiv
Salesforce isn't responsible for any exposure of your data to guest users related to this change from default settings.
Criteria
Field
Operator
Value
Created By ID
starts with
0
AND
--None--
--None--
AND
AND
--None--
--None--
AND
--None--
--None--
Create rule to grant access to future opportunities

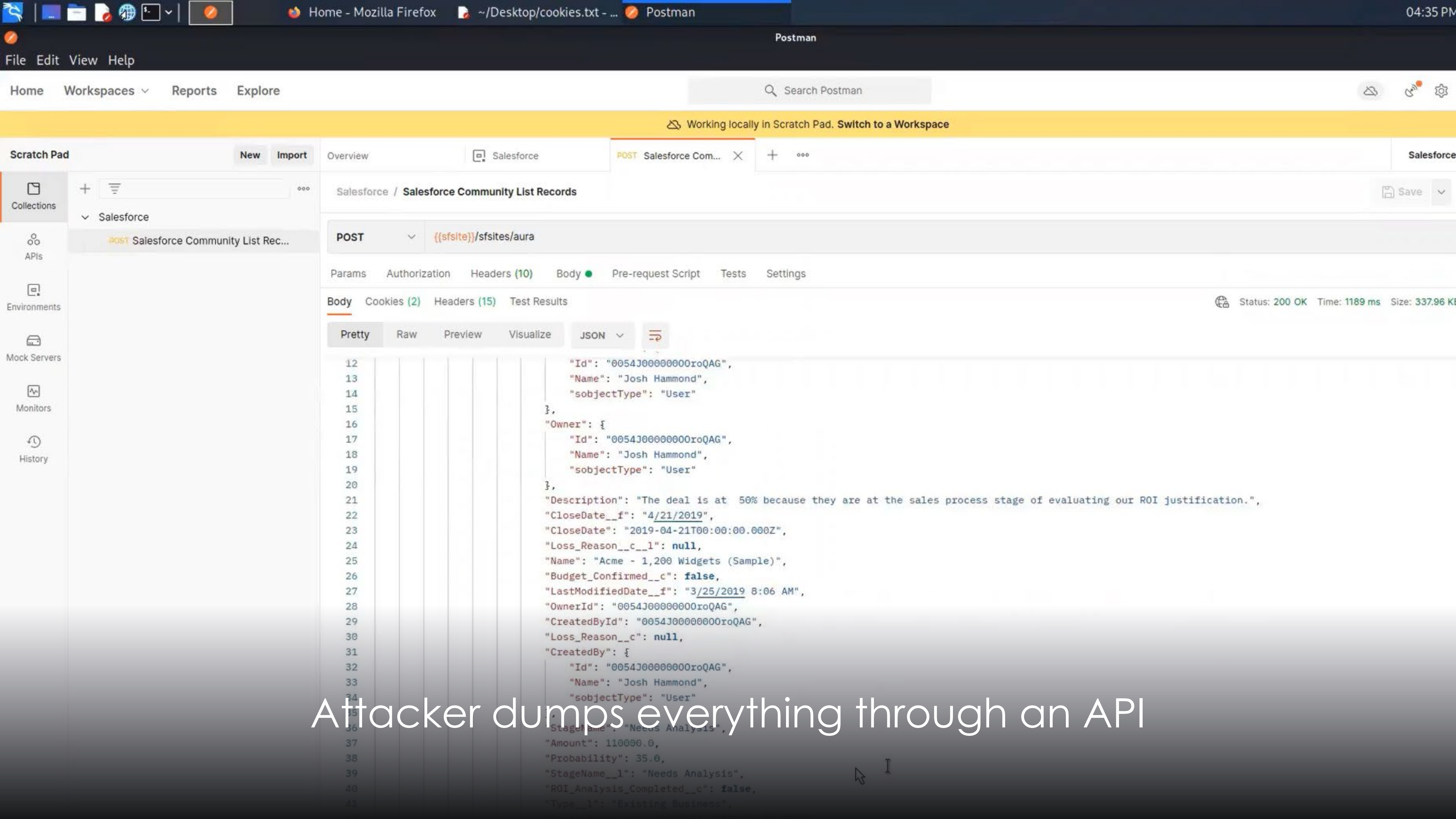


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	acme-vrns.force.com	/support/s/	browsing-context.js:1078 (document)	html	15.07 KB	41.92 KB
200	POST	acme-vrns.force.com	auraAnalytics	aura_prod.js:650 (beacon)	json	1.20 KB	1.38 KB
200	GET	acme-vrns.force.com	bootstrap.js?aura.attributes={"schema":"Published","brandingSetId":"b28d2cbf-8462-4971-9514-2587129...	script	js	91.62 KB	465.83 KB
304	GET	acme-vrns.force.com	fonts.css?lastMod=1629813498000&brandSet=b28d2cbf-8462-4971-9514-25871293c04a	stylesheet	css	cached	336.04 KB
200	GET	acme-vrns.force.com	resources.js?pv=1629838827000-2096807252&rv=1629810401000	script	js	cached	5.68 KB
200	GET	acme-vrns.force.com	aura_prod.js	script	js	cached	723.41 KB
200	GET	acme-vrns.force.com	app.js	script	js	cached	1.88 MB
200	GET	acme-vrns.force.com	favicon.ico	FaviconLoader.jsm:165 (img)	x-icon	cached	5.30 KB
304	GET	acme-vrns.force.com	ember-background.jpg	themeSearch.js:4 (img)	jpeg	cached	37.36 KB
304	GET	acme-vrns.force.com	ember-logo.png	themeSearch.js:4 (img)	png	cached	2.26 KB
200	POST	acme-vrns.force.com	aura?r=0&ui-chatter-components-messages.Messages.getMessagingPermAndPref=1&ui-communities-co...	aura_prod.js:649 (xhr)	json	1.92 KB	3.80 KB
304	GET	acme-vrns.force.com	T	aura_prod.js:12 (img)	png	cached	723 B
200	POST	acme-vrns.force.com	aura?r=1&ui-instrumentation-components-beacon.InstrumentationBeacon.sendData=1	aura_prod.js:649 (xhr)	json	1.21 KB	1.42 KB
200	GET	acme-vrns.force.com	SessionTimeServlet?buster=1629923655118	sessionTimeoutWatcher.js:3 (xhr)	json	424 B	31 B
200	POST	acme-vrns.force.com	aura?r=2&ui-identity-components-sessiontimeoutwarn.SessionTimeoutWarn.getSessionTimeoutConfig=1	aura_prod.js:649 (xhr)	json	1.18 KB	1.28 KB

Guest profile can access everything



Bulk data access through API



Attacker dumps everything through an API

Phase 4 – Salesforce Exfil

- Attack -
  - Attacker modifies guest user profile
    - Grants access to opportunities
    - Grants API access to guest accounts
  - Steals opportunity data via API
- Detections to Consider
  - Modifications to guest user profile
  - Modifications to opportunities object permissions
  - API Access added to profile

How to apply what you've learned today

- Next week you should:
  - Create an inventory of your sanctioned SaaS apps
  - Check what telemetry & logs you have from each vendor
- Next month you should:
  - Audit org-wide configuration settings
  - Hunt down and kill unnecessary global access (e.g., "Anyone links")
- Within six months you should:
  - Define data security policies for each SaaS app
  - Trigger alerts on policy violations and abnormal behavior

Feeling Overwhelmed?

- Stop by the Booth
- Visit Varonis.com
- Stick around!