Fairbets.co

Web Application Vulnerability Assessment and Penetration Testing Report

Business Confidential

Test Start Date : 6/4/2022
Test End Date: 7/4/2022

Retest V1.0 Start Date: 29/6/2022
Retest V1.0 End Date: 30/6/2022

Retest V1.1 Start Date: 17/9/2022
Retest V1.1 End Date: 17/9/2022

Project Target : fairbets.co

Scope

In this report, the penetration tester has showcased what vulnerabilities are being performed and found. The vulnerabilities in the report are what I've successfully encountered till now and when a new vulnerability is found , I'll update the new vulnerabilities in this report.

Confidentiality Statement

This document is the exclusive property of Fairbets.co and Pentester . This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Fairbets.co and Pentester.

Pentester may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Pentester prioritized the assessment to identify the weakest security controls an attacker would exploit. Pentester recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

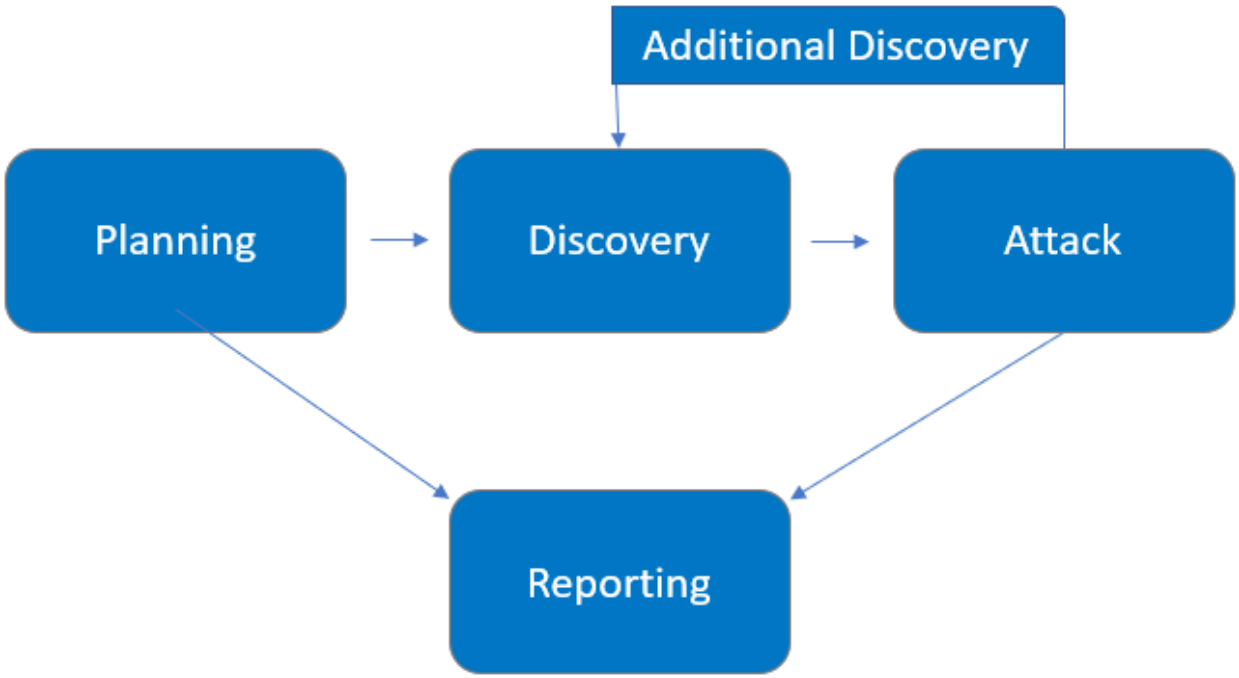
Name	Title	Contact Information
Fairbets.co		
Fairbets.co	Fairbets.co	N/A
Pentester		
Pentester	Penetration Tester	N/A

Assessment Overview

From MAY 2022, Fairbets.co engaged Pentester to evaluate the security posture of its infrastructure "fairbets.co" compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge.Pentester, a testing engineer, attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external Paths to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impacts.

Severity	CVSS V3 Score Range	Definition
Critical	9.0 - 10	Exploitation is straightforward and usually results in Path-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0 - 8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0 - 6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1 - 3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	fairbets.co

Executive Summary

Pentester evaluated fairbets.co external security posture through an external network penetration test from May 6th 2022 till May 7th 2022 . By leveraging a series of attacks, Pentester found critical-level vulnerabilities that allowed full internal network access to the Fairbets.co internal services. It is highly recommended that Fairbets.co address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Vulnerabilities found

Sr.No.	Vulnerability List	Status
1	Security Headers Missing	Not Fixed
2	SPF/DMARC Authentication	Not Fixed
3	Weak Password Implementation	Fixed
4	Parameter tampering (Minus Withdraw)	Fixed
5	No Captcha Implementation	Fixed (no need)
6	Broken Authentication (Multi Logins)	Fixed
7	No Input Validation	Fixed

8	Lower Nginx Version	Not Fixed
9	Lower Angular Version	Not Fixed
10	No max withdraw note (functional flaw)	Fixed
11	Parameter Tampering (on deposit)	Fixed
12	No WAF	Not Fixed
13	No Load Balancer	Not Fixed
14	No Rate Limit Mass OTP	Fixed
15	Missing Cookie Attributes	Not Fixed
16	UI Issues	Fixed
17	Parameter tampering The Deposit Limit	Not Fixed
18	Request Manipulation In Bank Detail	Not Fixed

Penetration Test Findings

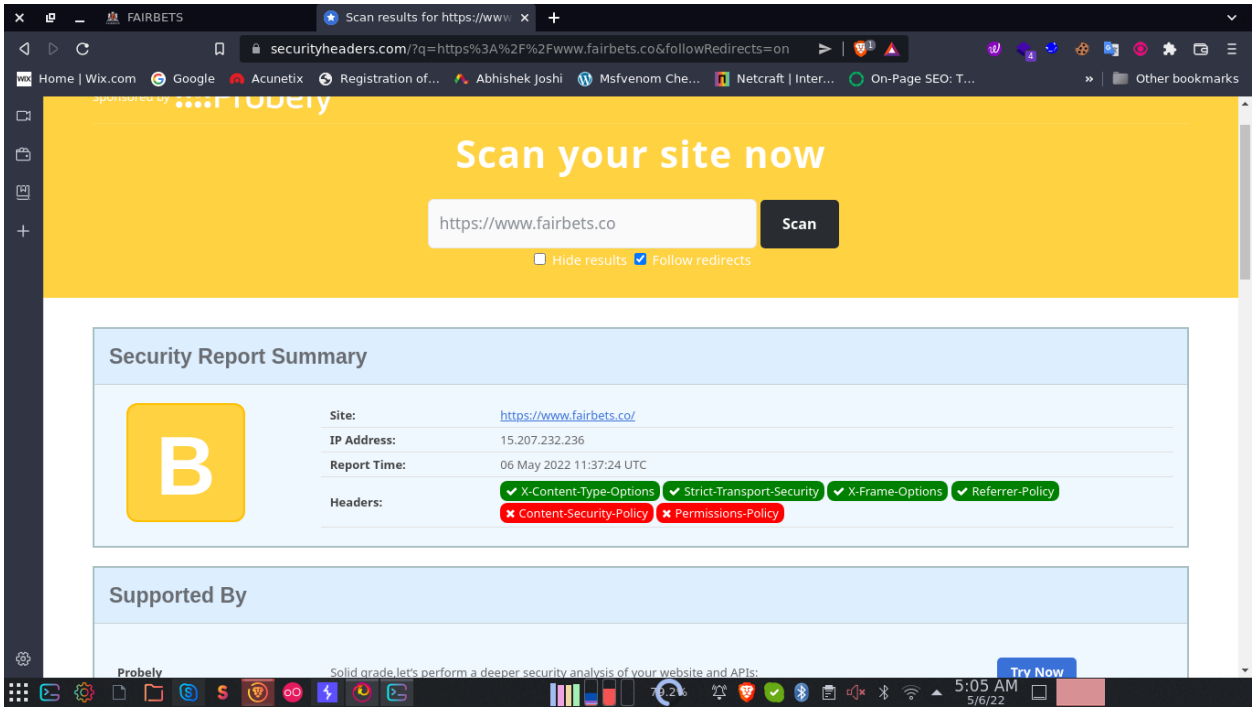
❖ Security Headers Missing

Severity	Critical
Description	● Strict-Transport-Security - Communication over a plain HTTP connection is not encrypted, making the transferred data accessible to network-level eavesdroppers. The Strict-Transport-Security header informs the browser that it should never load the site using HTTP and use HTTPS instead. Once it's set, the browser will use HTTPS instead of HTTP to access the domain without a redirect for a duration defined in the header. ● Content-Security-Policy - Introduced in November 2012, Content Security Policy presents an extra layer of security against multiple vulnerabilities such as XSS, Clickjacking, Protocol Downgrading and Frame Injection. It appears that CSP will become the most significant tool for client side security in the near future, since it provides a substitute for security headers, such as X-Frame-Options and *X-XSS-Protection*, that aren't enabled by default. ● X-Frame-Options - The X-Frame-Options Header is a security header suggested by Microsoft to avoid the UI Redressing attacks that began with Clickjacking in 2009. It's supported by all major browsers. UI Redressing attacks are based on loading web pages inside an iframe and overlaying them with other UI elements. There are various types of UI Redressing, such as hijacking keystrokes or extraction of content, each with its own advantages for attackers.

	• X-Content-Type-Options - This HTTP header is typically used to control the MIME Type Sniffing function in web browsers. MIME Type Sniffing is a content evaluation function used by browsers when the content type is not specified. Basically, if the *Content-Type* header is blank or missing, the browser 'sniffs' the content and attempts to display the source in the most appropriate way. However, if used in conjunction with an upload functionality, this sniffing process can pose some risks, so developers should be really careful how to use this header. • Referrer-Policy - Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites. • Permissions-Policy - Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.
Impact	Attackers can do malicious activity and perform critical vulnerabilities like sql injection, xss injection, clickjacking, etc. You'll need to implement/apply all the headers.
Path	https://www.fairbets.co/
Severity	**Medium**
References	https://securityheaders.com/?q=http%3A%2F%2F198.251.74.193%2F&followRedirects=on

Exploitation Proof of Concept

That’s not all. Expired or invalid certificates are highly threatening to your secure connections. Your website's reputation will also be damaged if your users are confronted with such easily preventable problems.



Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	recommends to apply all the headers

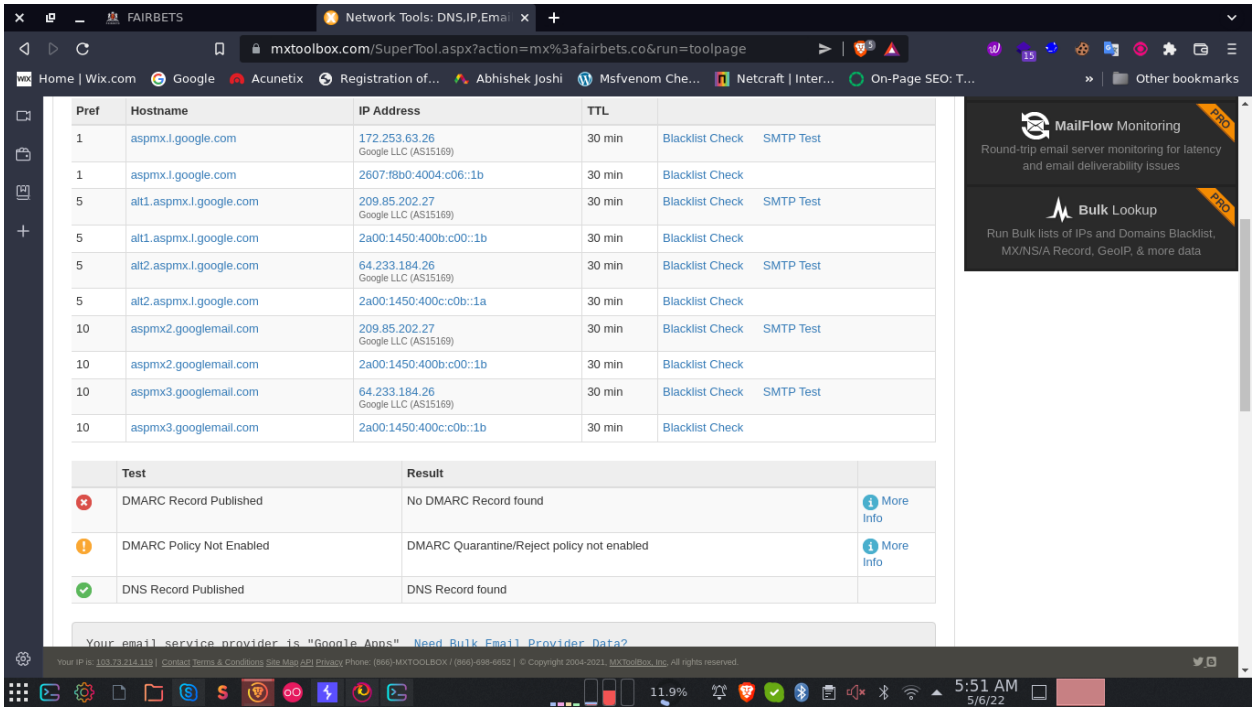
❖ SPF/DMARC Authentication

Severity	High
Description	Attackers can send spam messages and phishing sites or any payment method sites to steal critical and financial credentials with the use of your website domain. The Sender Policy Framework (SPF) is an email authentication technique that is used to prevent spammers from sending messages on behalf of your domain. With SPF, an organization can publish authorized mail servers. Together with the DMARC related information, this gives the receiver (or receiving systems) information on how trustworthy the origin of an email is. SPF is, just like DMARC, an email authentication technique that uses DNS (Domain Name Service). This gives you, as an email sender, the ability to specify which email servers are permitted to send an email on behalf of your domain.
Impact	Mail messages are sent by an attacker as spam messages asking for information to steal users' data. Attackers can also send a clone website to input information called a phishing attack.
Path	https://www.fairbets.co
severity	**Low**
References	https://geekflare.com/fix-email-spoofing-missing-spf-record-vulnerability/

Exploitation Proof of Concept

In this scenario, an attacker can send fake mails to anyone with the use of your domain. Can possibly perform malicious activity and demand money.

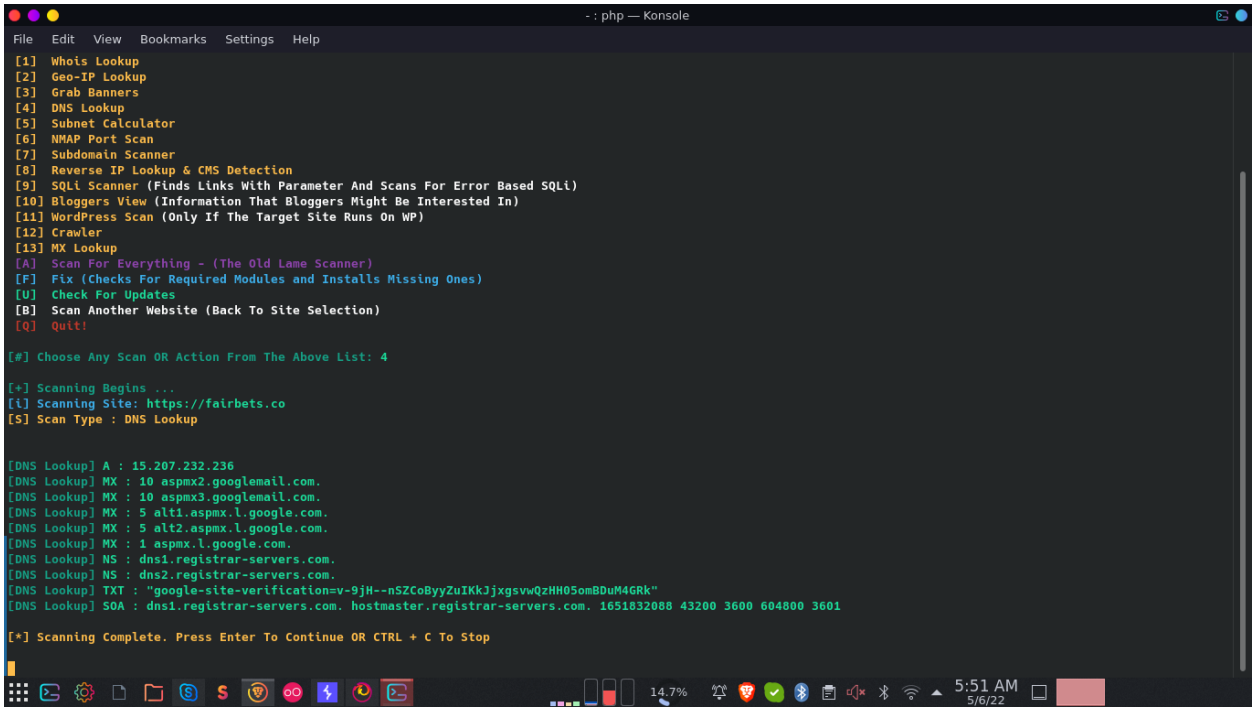
No dmarc policy enables

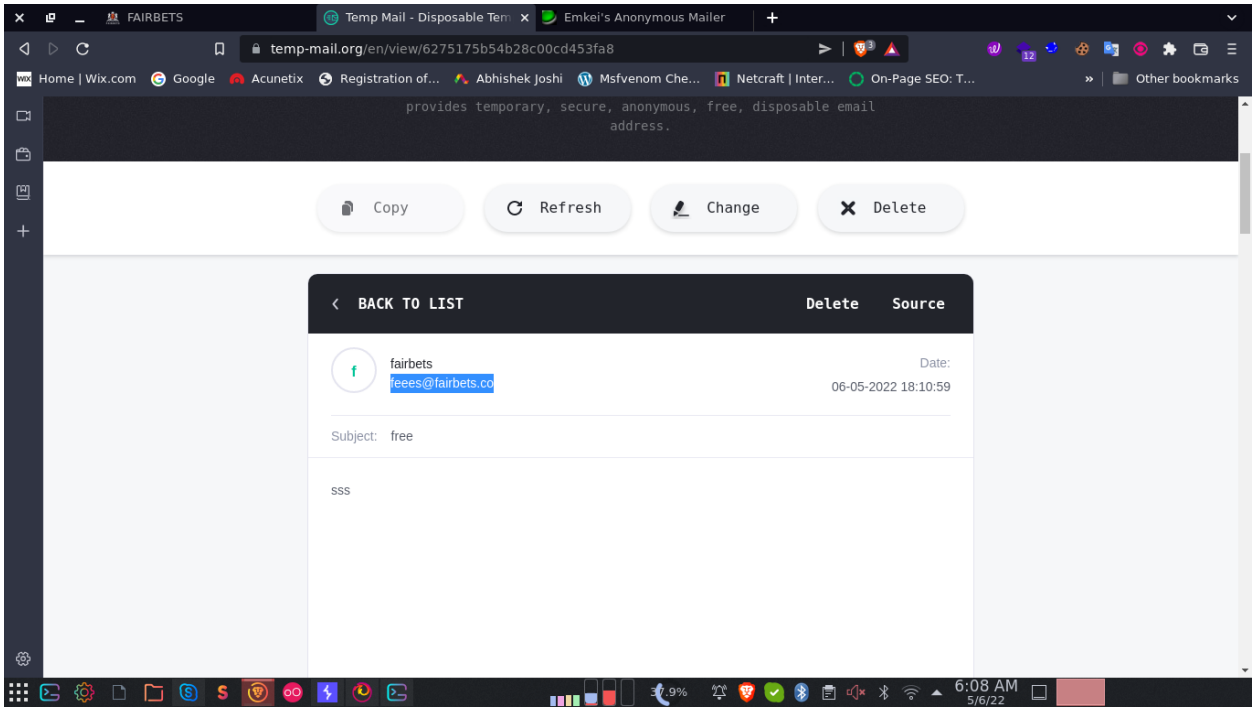


Pref	Hostname	IP Address	TTL	
1	aspmx.l.google.com	172.253.63.26 Google LLC (AS15169)	30 min	Blacklist Check SMTP Test
1	aspmx.l.google.com	2607:f8b0:4004:c06::1b	30 min	Blacklist Check
5	alt1.aspmx.l.google.com	209.85.202.27 Google LLC (AS15169)	30 min	Blacklist Check SMTP Test
5	alt1.aspmx.l.google.com	2a00:1450:400b:c00::1b	30 min	Blacklist Check
5	alt2.aspmx.l.google.com	64.233.184.26 Google LLC (AS15169)	30 min	Blacklist Check SMTP Test
5	alt2.aspmx.l.google.com	2a00:1450:400c:c0b::1a	30 min	Blacklist Check
10	aspmx2.googlemail.com	209.85.202.27 Google LLC (AS15169)	30 min	Blacklist Check SMTP Test
10	aspmx2.googlemail.com	2a00:1450:400b:c00::1b	30 min	Blacklist Check
10	aspmx3.googlemail.com	64.233.184.26 Google LLC (AS15169)	30 min	Blacklist Check SMTP Test
10	aspmx3.googlemail.com	2a00:1450:400c:c0b::1b	30 min	Blacklist Check

	Test	Result	
✖	DMARC Record Published	No DMARC Record found	More Info
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✔	DNS Record Published	DNS Record found	

No SPF TXT was present





Remediation

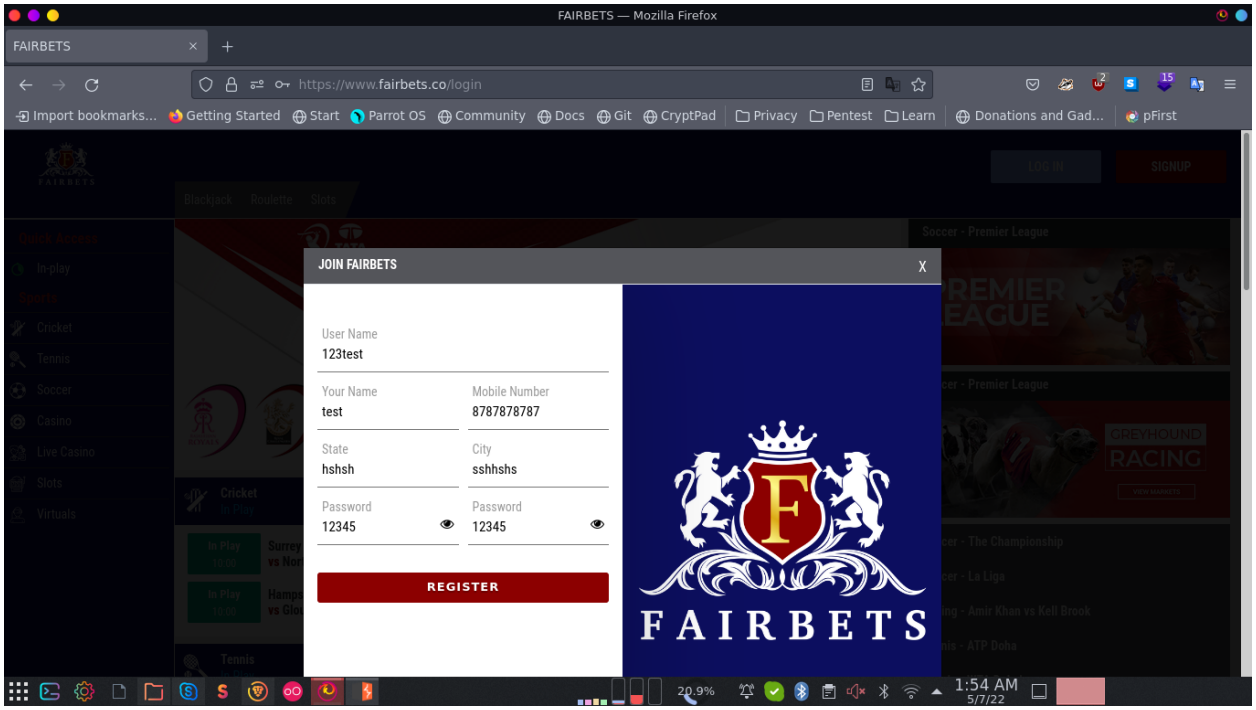
Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends to 1. apply SPF txt record 2. apply proper Sender Policy Framework mechanism on SPF txt otherwise it is still going to be vulnerable

❖ Weak Password Implementation

Severity	High
Description	Authentication mechanisms often rely on a memorized secret (also known as a password) to provide an assertion of identity for a user of a system. It is therefore important that this password be of sufficient complexity and impractical for an adversary to guess. The specific requirements around how complex a password needs to be depends on the type of system being protected. Selecting the correct password requirements and enforcing them through implementation are critical to the overall success of the authentication mechanism.
Impact	An attacker could easily guess user passwords and gain access to user accounts.
Path	https://fairbets.co
severity	Low
References	https://www.acunetix.com/vulnerabilities/web/weak-password/

Exploitation Proof of Concept

An attacker could deny service to legitimate system users by launching a brute force attack on the password recovery mechanism using user ids of legitimate users.



Remediation

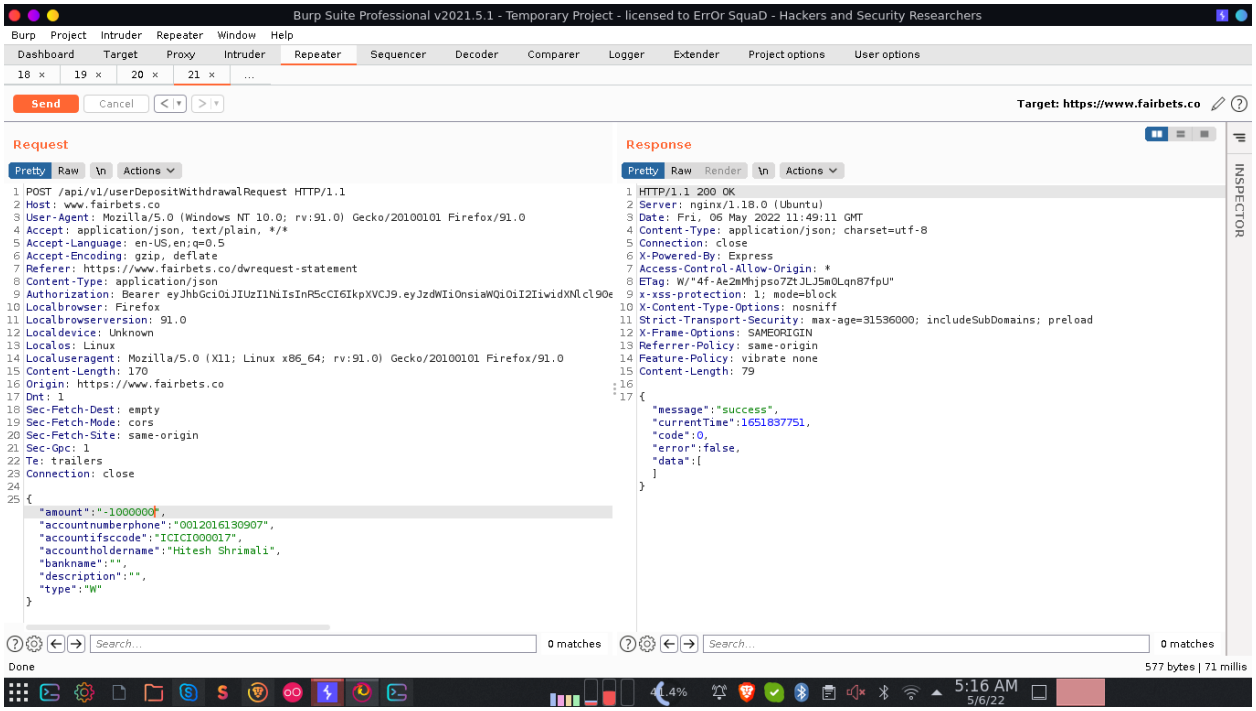
Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that 1. Consider implementing a password complexity meter to inform users when a chosen password meets the required attributes. a. Enforcement of a minimum and maximum length b. Restrictions against password reuse c. Restrictions against using common passwords d. Restrictions against using contextual string in the password (e.g., user id, app name) 2. Consider a second authentication factor beyond the password, which prevents the password from being a single point of failure.

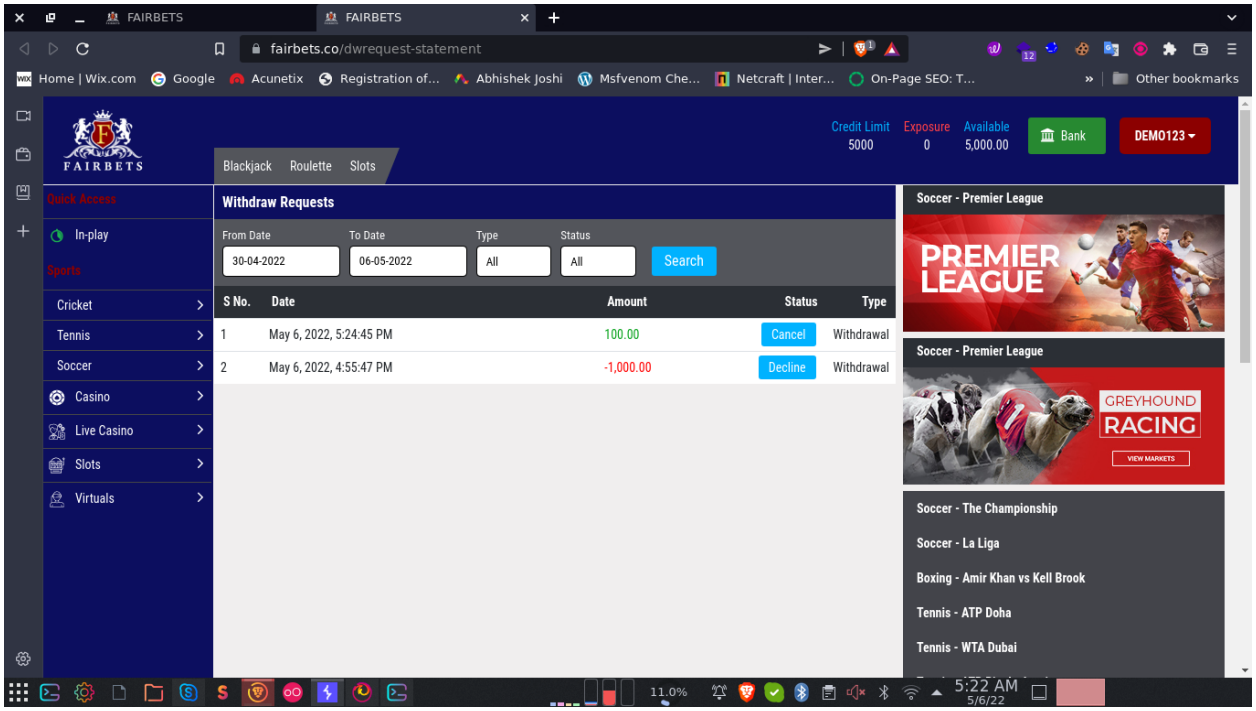
❖ Parameter Tampering (Minus Withdraw)

Severity	Medium
Description	The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools likes Webscarab and Paros proxy are mostly used.
Impact	An attacker can change the value and do malicious activity
Path	https://fairbets.co/api/v1/UserDepositWithdrawRequest
severity	**Critical**
References	https://owasp.org/www-community/attacks/Web_Parameter_Tampering

Exploitation Proof of Concept

In fairbets withdraw not working no wallet balance deducted when withdraw but after that functionality work attacker put a withdraw in minus and then the wallet should be in plus of the successfully ad 1lkh minus withdraw then they got 1lkh in wallet and they play the games and tends to business loss


Burp Suite Professional v2021.5.1 - Temporary Project - licensed to ErrOr SquaD - Hackers and Security Researchers
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: https://www.fairbets.co
Request
Pretty Raw \n Actions
POST /api/v1/userDepositWithdrawalRequest HTTP/1.1
Host: www.fairbets.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.fairbets.co/dwrequest-statement
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOnsiaWQiOiI2IiwidXNlcl90e
Localbrowser: Firefox
Localbrowserversion: 91.0
Localdevice: Unknown
Localos: Linux
Localuseragent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Content-Length: 170
Origin: https://www.fairbets.co
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Sec-Gpc: 1
Te: trailers
Connection: close
{
"amount":"-1000000",
"accountnumberphone":"0012016130907",
"accountifsccode":"ICICI000017",
"accountholdername":"Hitesh Shrimali",
"bankname":"",
"description":"",
"type":"W"
}
Response
Pretty Raw Render \n Actions
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 06 May 2022 11:49:11 GMT
Content-Type: application/json; charset=utf-8
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"4f-Ae2mMhjpso7ZtJLJ5mOLqn87fpU"
x-xss-protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Feature-Policy: vibrate none
Content-Length: 79
{
"message":"success",
"currentTime":1651837751,
"code":0,
"error":false,
"data":[
]
}
INSPECTOR
Search... 0 matches
Done
577 bytes | 71 millis
5:16 AM
5/6/22


FAIRBETS
fairbets.co/dwrequest-statement
Home | Wix.com Google Acunetix Registration of... Abhishek Joshi Msfvenom Che... Netcraft | Inter... On-Page SEO: T... Other bookmarks
FAIRBETS
Blackjack Roulette Slots
Credit Limit 5000
Exposure 0
Available 5,000.00
Bank
DEMO123
Quick Access
In-play
Sports
Cricket
Tennis
Soccer
Casino
Live Casino
Slots
Virtuals
Withdraw Requests
From Date 30-04-2022
To Date 06-05-2022
Type All
Status All
Search
S No. Date Amount Status Type
1 May 6, 2022, 5:24:45 PM 100.00 Cancel Withdrawal
2 May 6, 2022, 4:55:47 PM -1,000.00 Decline Withdrawal
Soccer - Premier League
PREMIER LEAGUE
Soccer - Premier League
GREYHOUND RACING
VIEW MARKETS
Soccer - The Championship
Soccer - La Liga
Boxing - Amir Khan vs Kell Brook
Tennis - ATP Doha
Tennis - WTA Dubai
5:22 AM
5/6/22

Remediation

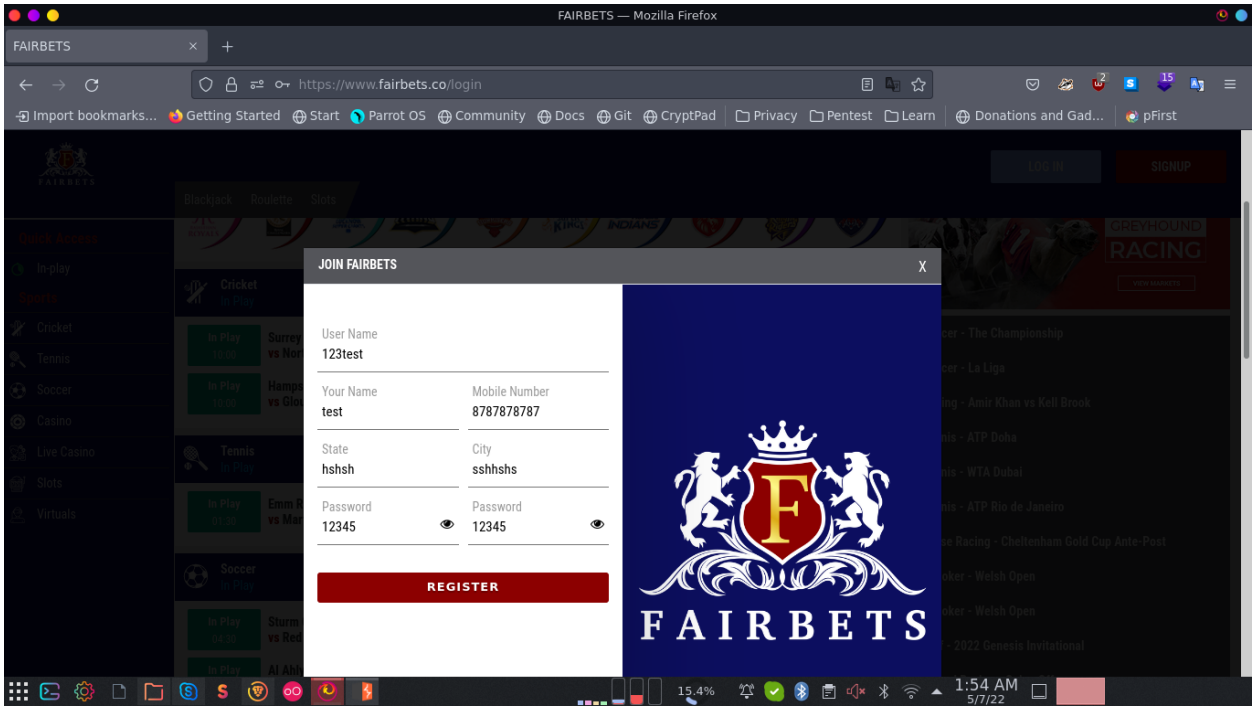
Target	https://www.fairbets.co
Vector	Parameter tampering
Recommendation	Pentester recommends that - Amount not should be submitted in minus

❖ No Captcha

Severity	High
Description	Captcha is very important because it prevents from intercept .CAPTCHA is an acronym for “Computer Automated Public Turing test to tell Computers and Humans apart”. It is used to determine whether or not the user is human.
Impact	An attacker could perform any manipulation,password attacks,any session or cookie related attacks
Path	https://fairbets.co
severity	Low
References	https://hackerone.com/reports/6697

Exploitation Proof of Concept

Without captcha attacker can do many malicious activities captcha prevent form interception



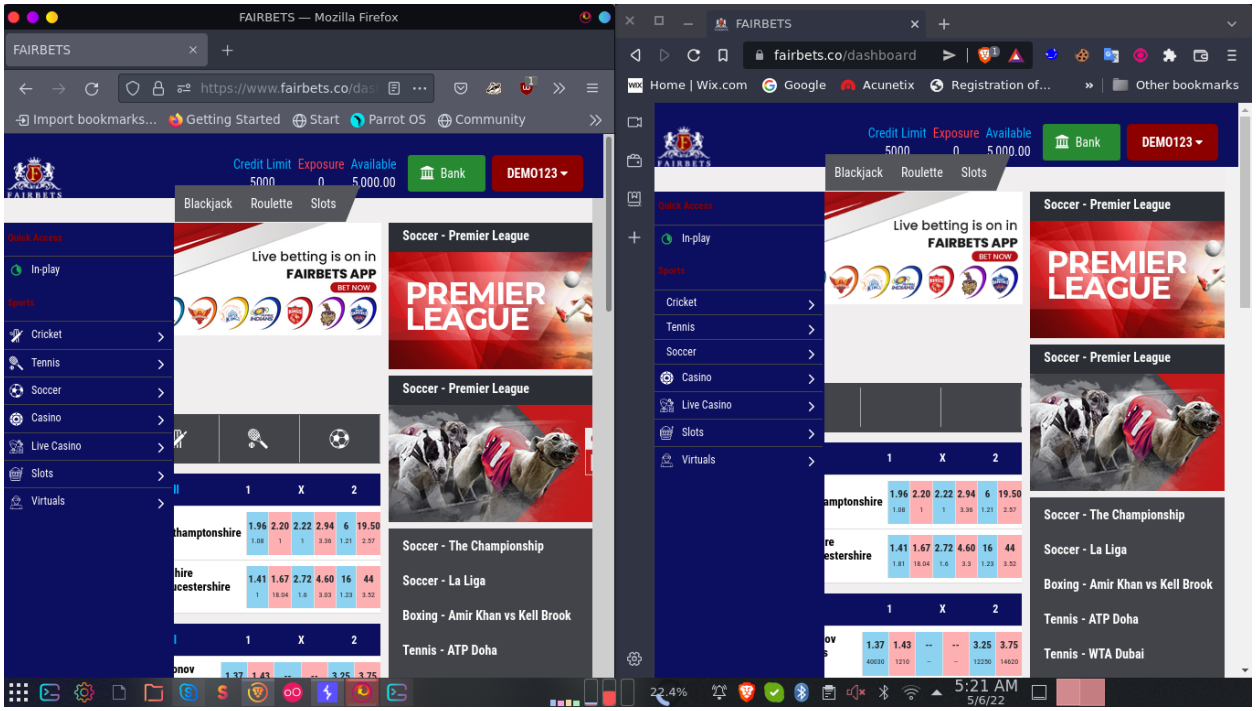
Remediation

Target	https://fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Apply best captcha for security

❖ Broken authentication (multi logins)

Severity	High
Description	Broken authentication active account only for one device
Impact	Multi logins
Path	https://fairbets.co
Severity	**Medium**
References	https://auth0.com/blog/what-is-broken-authentication/

Exploitation Proof of Concept



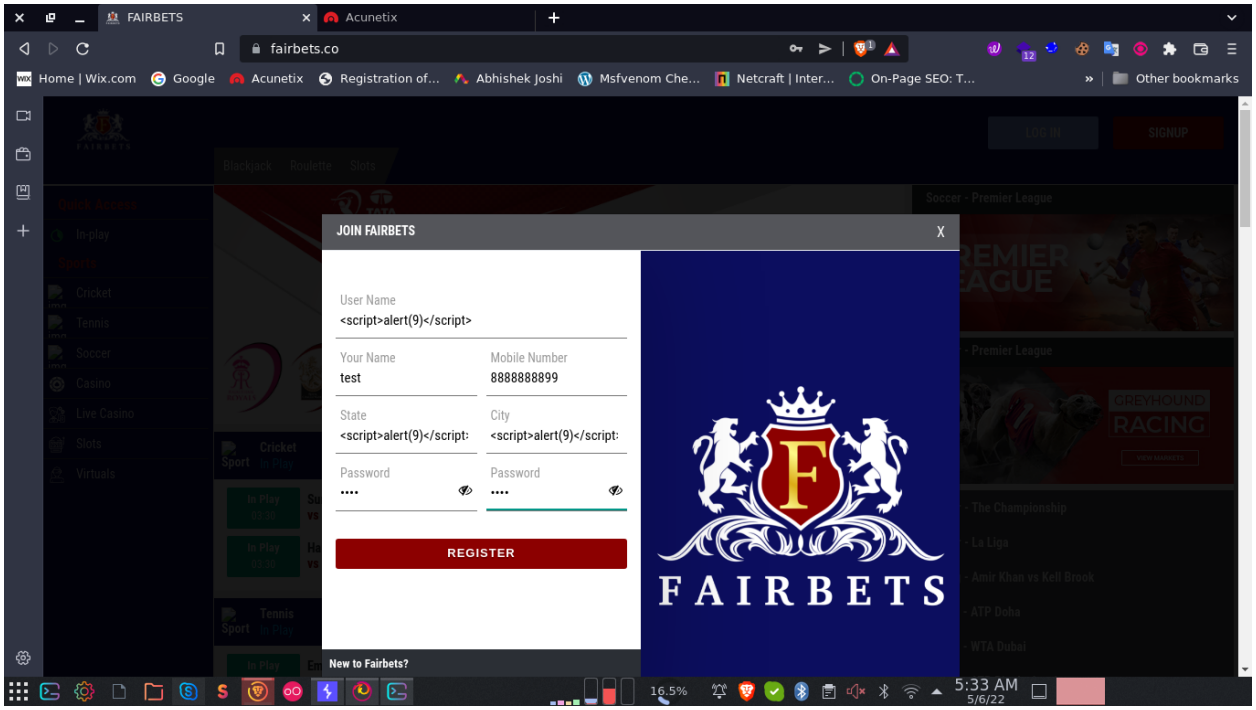
Remediation

Target	https://www.fairbets.co
Vector	Broken Authentication
Recommendation	Pentester Recommends that • Apply session expiration

❖ No Input Validation

Severity	Medium
Description	Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.
Impact	Attacker can do malicious activity using exploitation development such as XSS,SQL..injecting malicious scripts in input parameters
Path	https://www.fairbets.co
Severity	**Medium**
References	https://cwe.mitre.org/data/definitions/20.html

Exploitation Proof of Concept



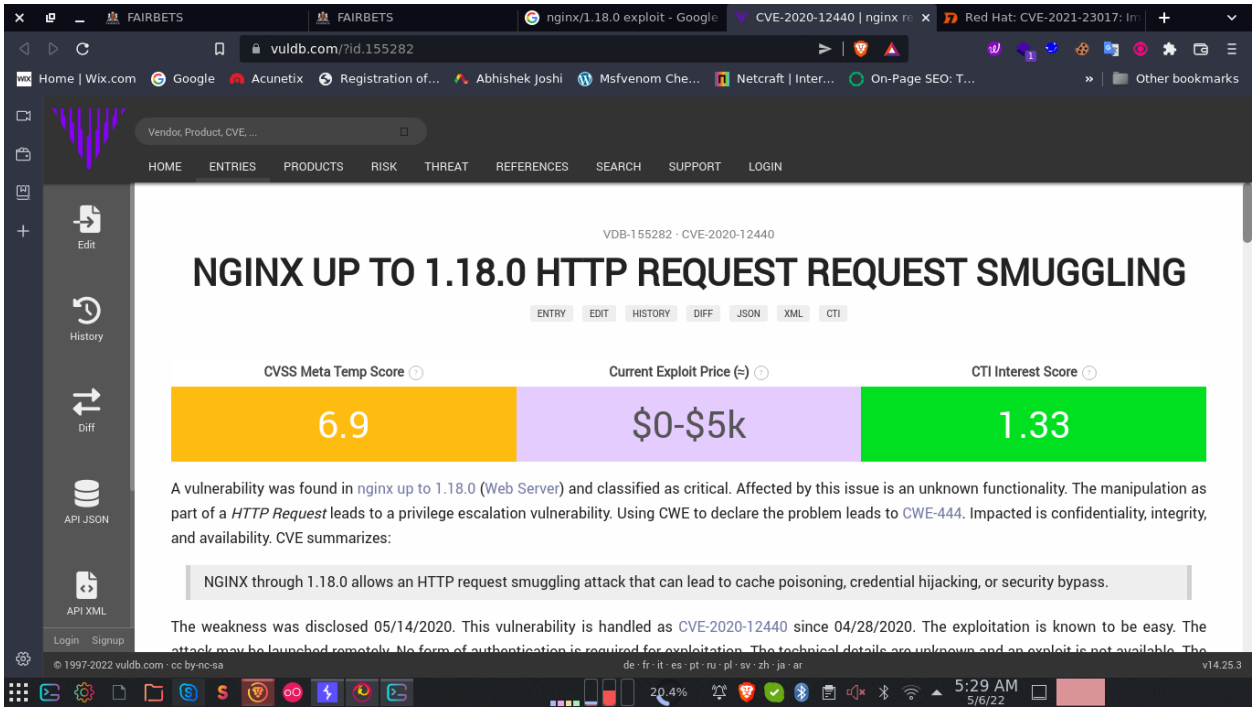
Remediation

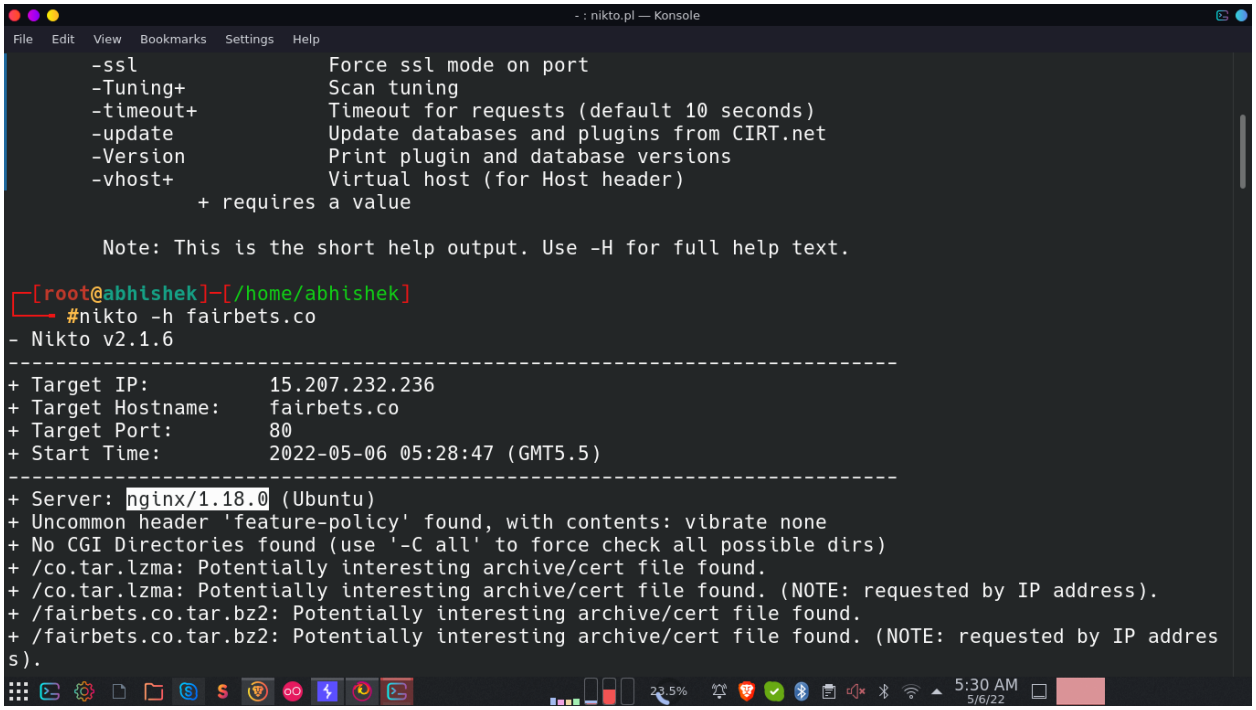
Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Implement the input validation

❖ Lower nginx version

Severity	Medium
Description	Many vulnerability will exist because of lower version
Impact	Hacker can identify the vulnerability related to that weakness and plan to exploitation
Path	https://www.fairbets.co
Severity	**Medium**
References	https://snyk.io/test/docker/nginx%3A1.18.0

Exploitation Proof of Concept





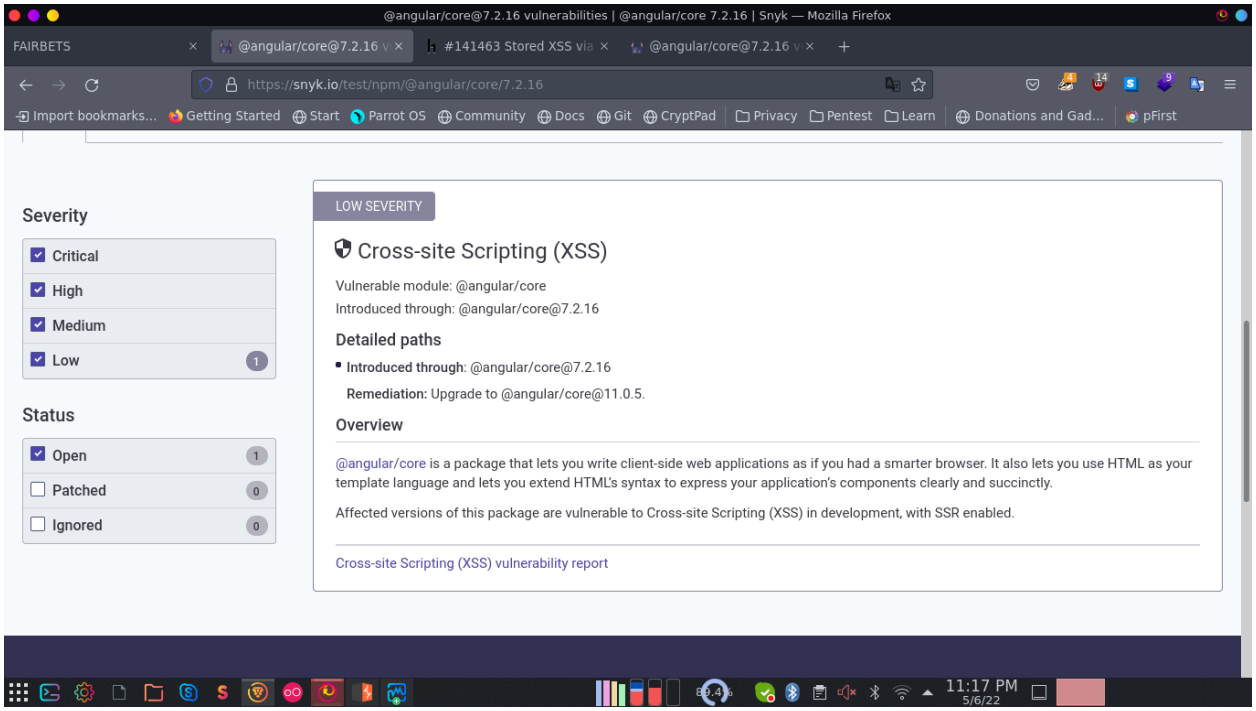
Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Update each and every software,firmware and frameworks

❖ Lower angular version

Severity	Medium
Description	Many vulnerability will exist because of lower version
Impact	Hacker can identify the vulnerability related to that weakness and plan to exploitation
Path	https://www.fairbets.co
Severity	**Medium**
References	https://snyk.io/test/npm/@angular/core/7.2.16

Exploitation Proof of Concept



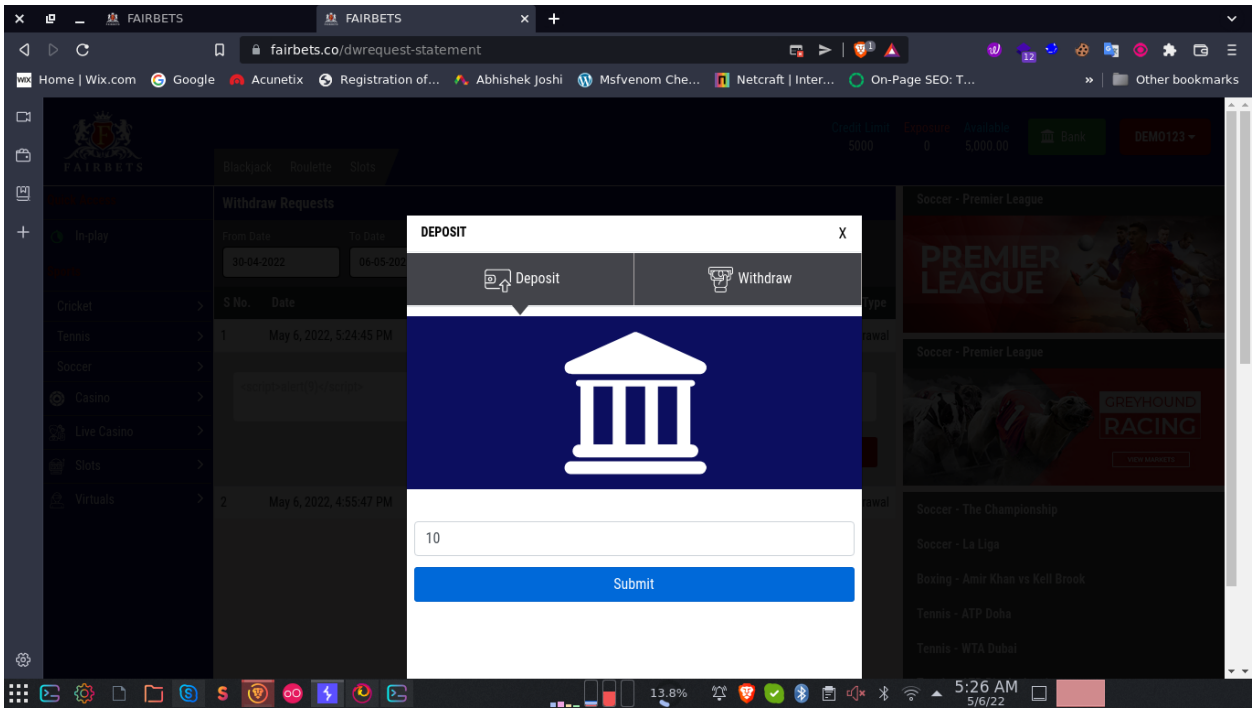
Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	APentester recommends that ● Update each and every software,firmware and frameworks

❖ No Max or Min Withdraw Note (Logic Flaw)

Severity	Medium
Description	Logic Flaw
Impact	N/A
Path	https://www.fairbets.co
References	N/A

Exploitation Proof of Concept



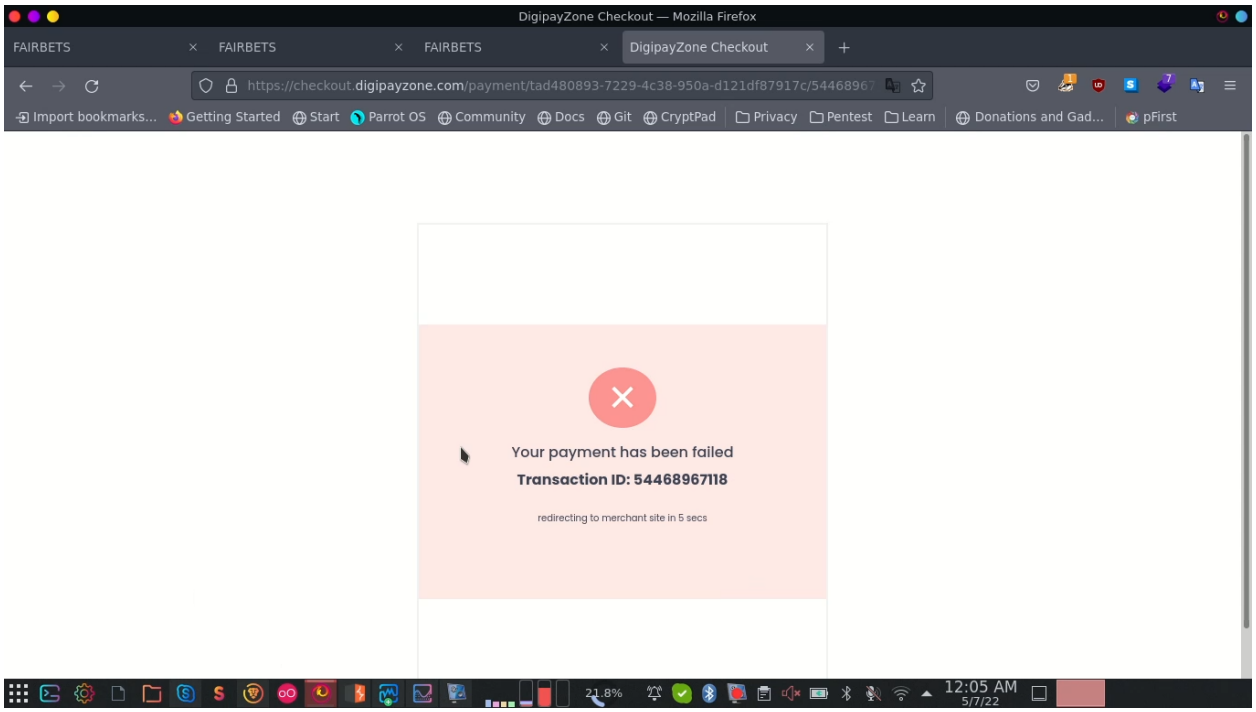
Remediation

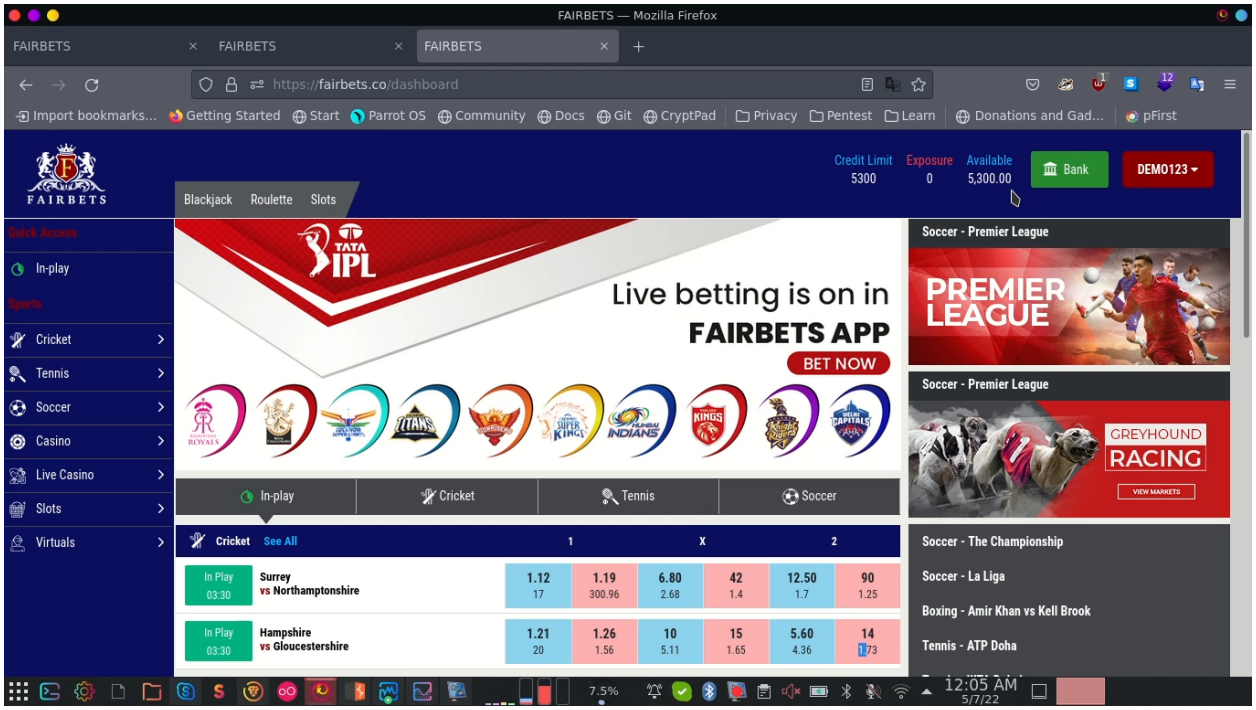
Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that ● Max or min note should be enable

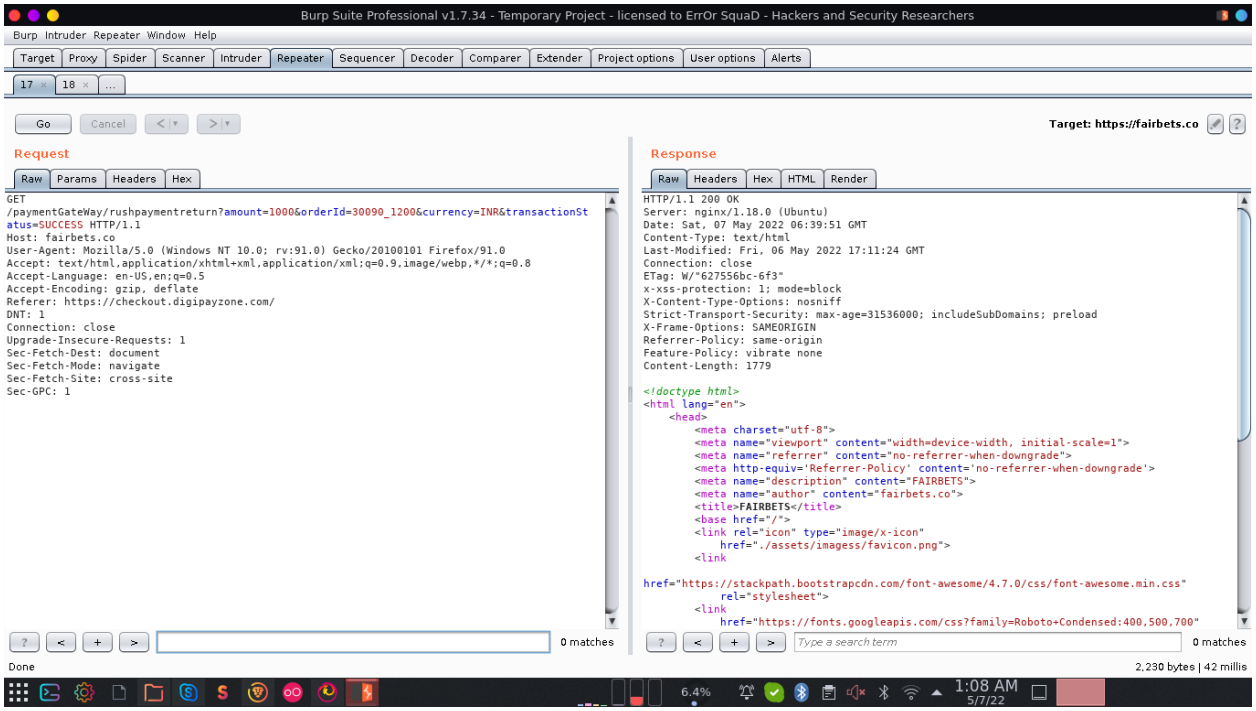
❖ Parameter Tampering (on Deposit)

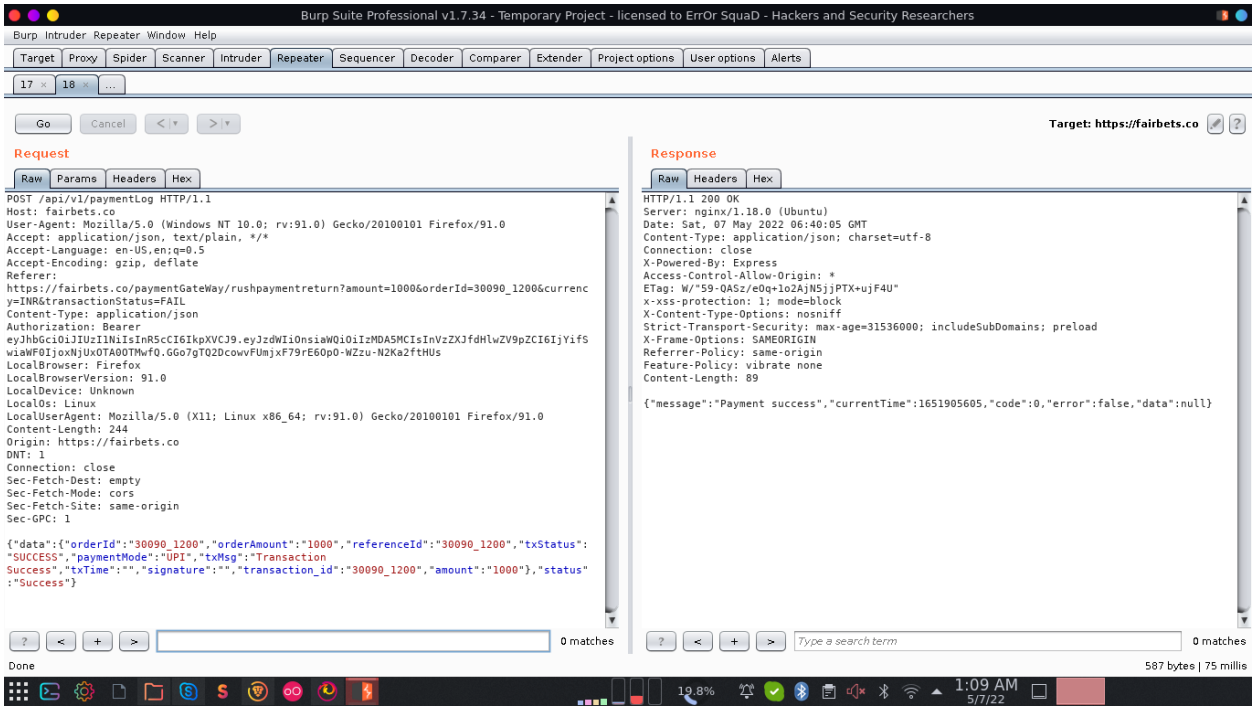
Severity	Medium
Description	The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools likes Webscarab and Paros proxy are mostly used.
Impact	An attacker can change the value and do malicious activity
Path	https://fairbets.co
Severity	**Critical**
References	https://owasp.org/www-community/attacks/Web_Parameter_Tampering

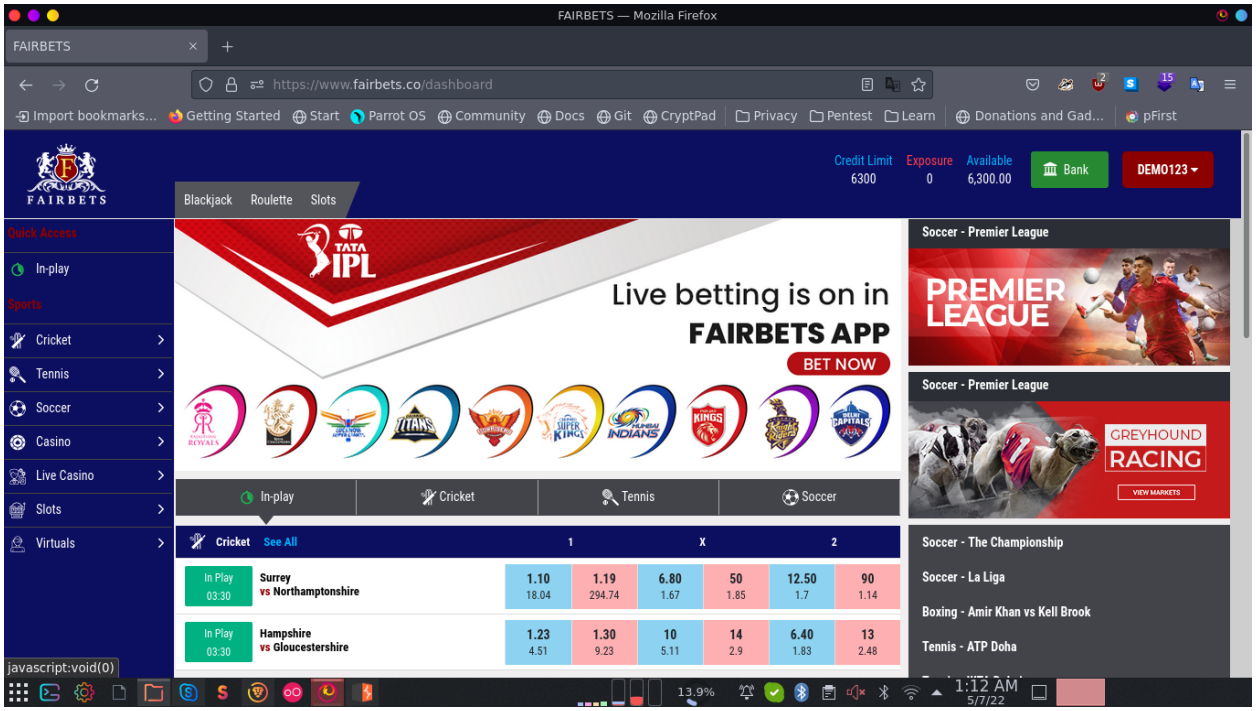
Exploitation Proof of Concept




FAIRBETS — Mozilla Firefox
FAIRBETS
https://fairbets.co/dashboard
Blackjack
Roulette
Slots
Credit Limit
5300
Exposure
0
Available
5,300.00
Bank
DEMO123
Quick Access
In-play
Sports
Cricket
Tennis
Soccer
Casino
Live Casino
Slots
Virtuals
TATA IPL
Live betting is on in
FAIRBETS APP
BET NOW
Soccer - Premier League
PREMIER LEAGUE
Soccer - Premier League
GREYHOUND RACING
VIEW MARKETS
In-play
Cricket
Tennis
Soccer
Cricket See All
1
X
2
In Play 03:30
Surrey vs Northamptonshire
1.12 17
1.19 300.96
6.80 2.68
42 1.4
12.50 1.7
90 1.25
In Play 03:30
Hampshire vs Gloucestershire
1.21 20
1.26 1.56
10 5.11
15 1.65
5.60 4.36
14 3.73
Soccer - The Championship
Soccer - La Liga
Boxing - Amir Khan vs Kell Brook
Tennis - ATP Doha
12:05 AM
5/7/22


Burp Suite Professional v1.7.34 - Temporary Project - licensed to ErrOr SquaD - Hackers and Security Researchers
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: https://fairbets.co
Request
Raw Params Headers Hex
GET /paymentGateWay/rushpaymentreturn?amount=1000&orderId=30090_1200&currency=INR&transactionStatus=SUCCESS HTTP/1.1
Host: fairbets.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
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
Referer: https://checkout.digipayzone.com/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-GPC: 1
0 matches
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 07 May 2022 06:39:51 GMT
Content-Type: text/html
Last-Modified: Fri, 06 May 2022 17:11:24 GMT
Connection: close
ETag: W/"627556bc-6f3"
x-xss-protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Feature-Policy: vibrate none
Content-Length: 1779
<!doctype html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="referrer" content="no-referrer-when-downgrade">
<meta http-equiv='Referrer-Policy' content='no-referrer-when-downgrade'>
<meta name="description" content="FAIRBETS">
<meta name="author" content="fairbets.co">
<title>FAIRBETS</title>
<base href="/">
<link rel="icon" type="image/x-icon" href="./assets/imagess/favicon.png">
<link
href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet">
<link
href="https://fonts.googleapis.com/css?family=Roboto+Condensed:400,500,700"
Type a search term
0 matches
Done
2,230 bytes | 42 millis
1:08 AM
5/7/22


Burp Suite Professional v1.7.34 - Temporary Project - licensed to ErrOr SquaD - Hackers and Security Researchers
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: https://fairbets.co
Request
Raw Params Headers Hex
POST /api/v1/paymentLog HTTP/1.1
Host: fairbets.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://fairbets.co/paymentGateWay/rushpaymentreturn?amount=1000&orderId=30090_1200&currency=INR&transactionStatus=FAIL
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOnsiaWQiOiIzMDA5MCIsInVzZXJfdHlwZV9pZCI6IjYifSwiaWF0IjoxNjUxOTA0OTMwfQ.GGo7gTQ2DcowvFUmjxF79rE6Op0-WZzu-N2Ka2ftHUs
LocalBrowser: Firefox
LocalBrowserVersion: 91.0
LocalDevice: Unknown
LocalOs: Linux
LocalUserAgent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Content-Length: 244
Origin: https://fairbets.co
DNT: 1
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Sec-GPC: 1
{"data":{"orderId":"30090_1200","orderAmount":"1000","referenceId":"30090_1200","txStatus":"SUCCESS","paymentMode":"UPI","txMsg":"Transaction Success","txTime":"","signature":"","transaction_id":"30090_1200","amount":"1000"},"status":"Success"}
Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 07 May 2022 06:40:05 GMT
Content-Type: application/json; charset=utf-8
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"59-QASz/eOq+1o2AjN5jjPTX+ujF4U"
x-xss-protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Feature-Policy: vibrate none
Content-Length: 89
{"message":"Payment success","currentTime":1651905605,"code":0,"error":false,"data":null}
0 matches
Type a search term
0 matches
Done
587 bytes | 75 millis
19.8%
1:09 AM
5/7/22


FAIRBETS — Mozilla Firefox
FAIRBETS
https://www.fairbets.co/dashboard
Import bookmarks... Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations and Gad... pFirst
FAIRBETS
Blackjack Roulette Slots
Credit Limit 6300
Exposure 0
Available 6,300.00
Bank
DEMO123
Quick Access
In-play
Sports
Cricket
Tennis
Soccer
Casino
Live Casino
Slots
Virtuals
TATA IPL
Live betting is on in
FAIRBETS APP
BET NOW
Soccer - Premier League
PREMIER LEAGUE
Soccer - Premier League
GREYHOUND RACING
VIEW MARKETS
In-play
Cricket
Tennis
Soccer
Cricket See All
1
X
2
In Play 03:30
Surrey vs Northamptonshire
1.10 18.04
1.19 294.74
6.80 1.67
50 1.85
12.50 1.7
90 1.14
In Play 03:30
Hampshire vs Gloucestershire
1.23 4.51
1.30 9.23
10 5.11
14 2.9
6.40 1.83
13 2.48
Soccer - The Championship
Soccer - La Liga
Boxing - Amir Khan vs Kell Brook
Tennis - ATP Doha
javascript:void(0)
13.9%
1:12 AM
5/7/22

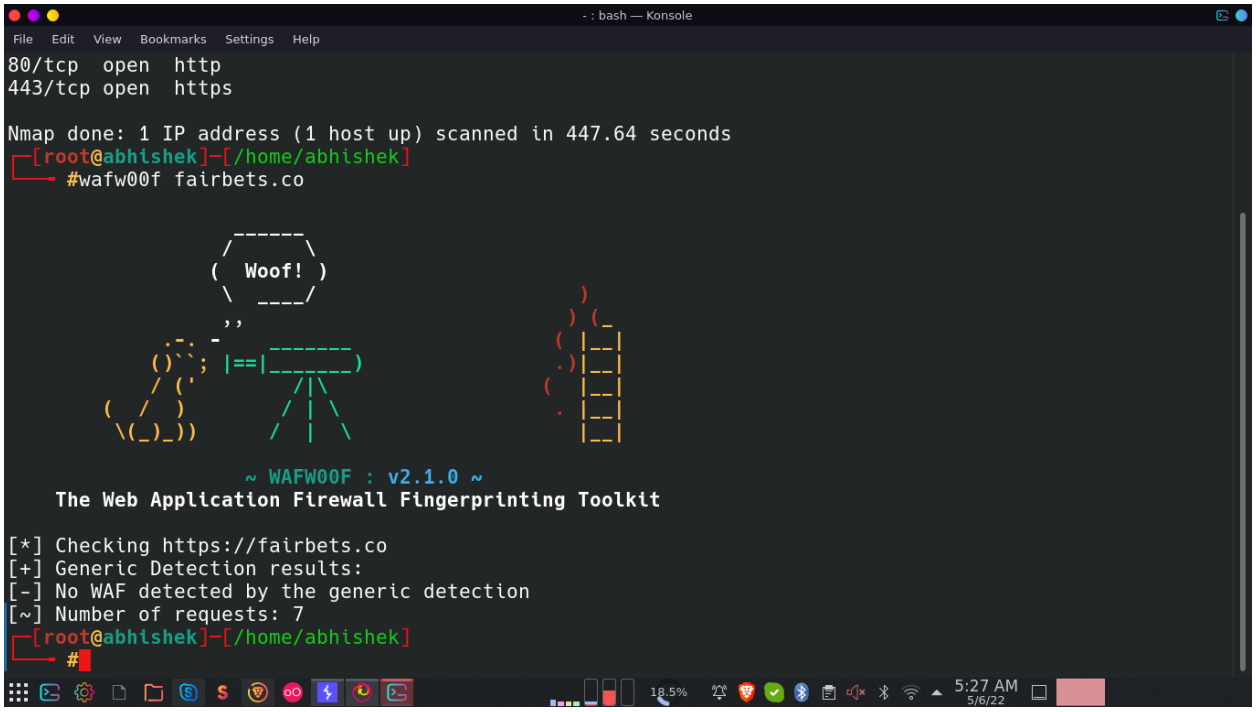
Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that ● Order_ID and transaction ID should Unique ● After the transaction failed or pending so they cannot be success same order_ID or transaction ID

❖ No WAF

Severity	Medium
Description	Web application firewall is very good option to add another security layer waf prevent from many attack like xss,sql,session attack etc
Impact	An attacker can attack sql,xss,session attack and so on if there is no waf configure
Path	https://www.fairbets.co
Severity	**Medium**
References	https://beaglesecurity.com/blog/article/secure-web-application-firewall-configuration.html#:~:text=A%20web%20application%20firewall%20or,web%20application%20and%20the%20internet.

Exploitation Proof of Concept



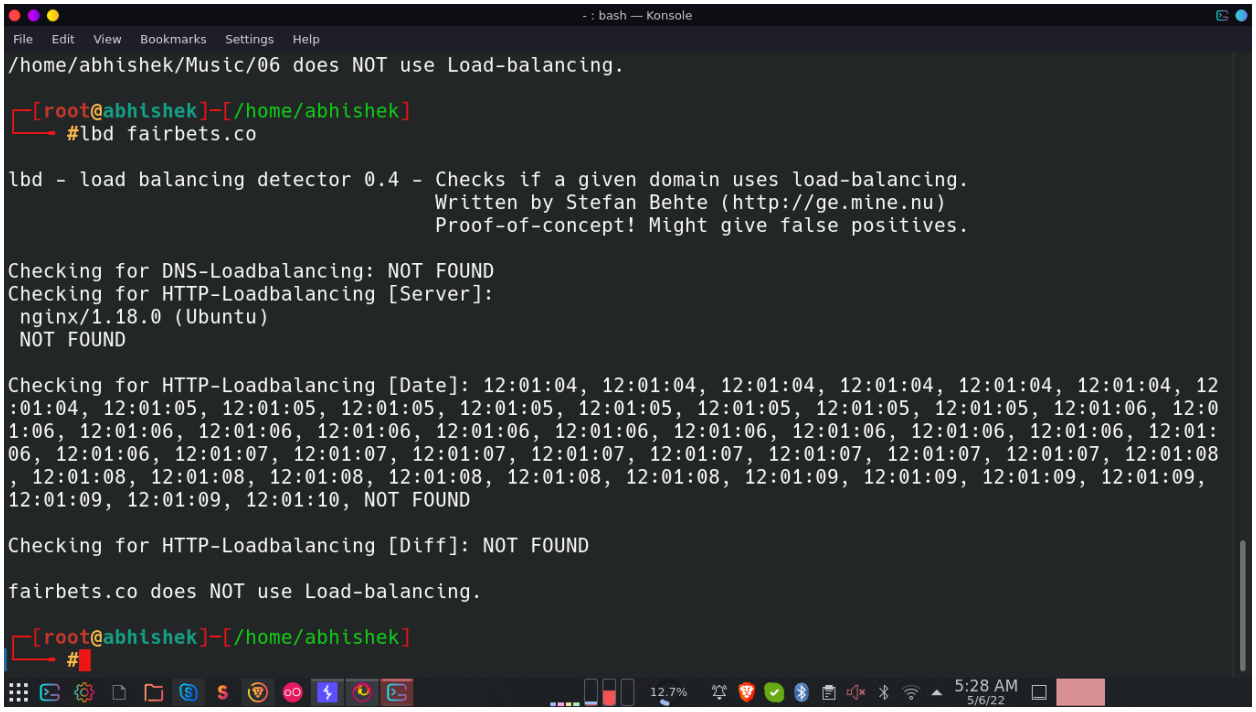
Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that ● Apply waf and all the security configuration

❖ Load balancer

Severity	Medium
Description	Load balancer is help for balancing the load and website should be stable if website have more traffic
Impact	Attacker can do dos or ddos attack if the load balancer was not implemented
Path	https://www.fairbets.co
Severity	**Medium**
References	https://medium.com/@itIsMadhavan/what-is-load-balancer-and-how-it-works-f7796a230034

Exploitation Proof of Concept



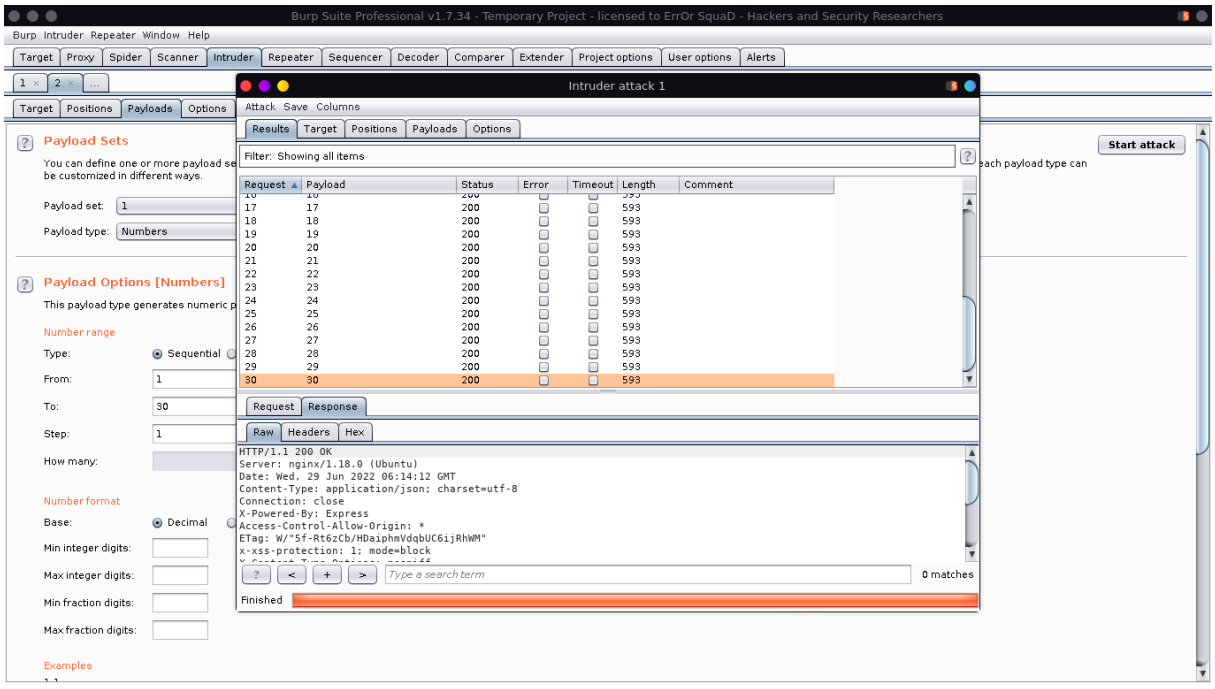
Remediation

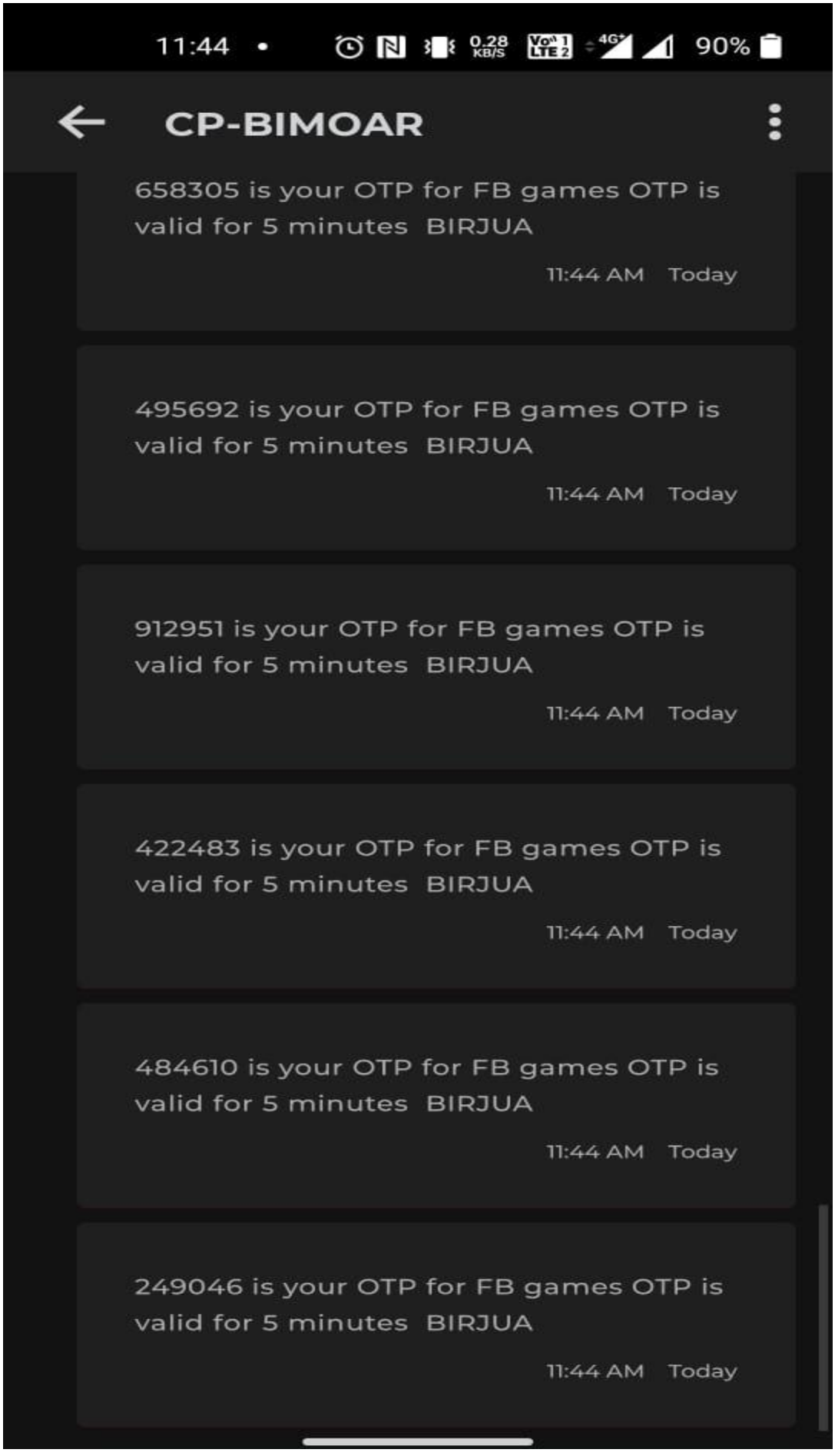
Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that ● Implement the load balancer

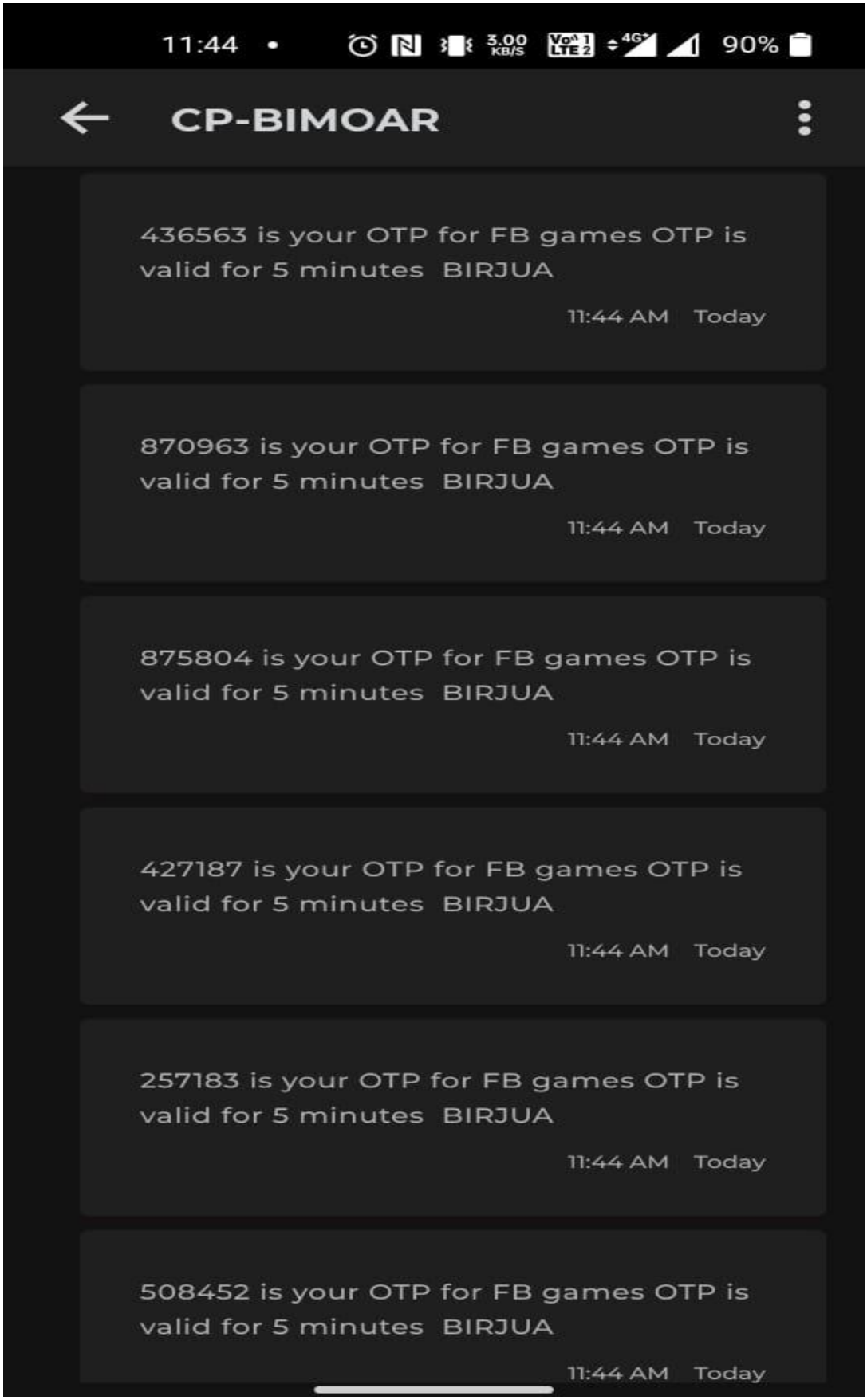
No rate limit on OTP (Dos attack)(Critical)

Description:	attacker can send multiple otp to the user account and also loss of business of organization
Impact:	Attacker can loss your business also blackmail the user
Files:	fairbets.co
Severity	**High**
References:	https://wpforms.com/simple-tricks-to-eliminate-spam-user-registration/

Exploitation Proof of Concept
penetration tester gathered this vulnerability from Manual testing using testing tools with proper path and parameters.




11:44 •
0.28 KB/S
90%
CP-BIMOAR
658305 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
495692 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
912951 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
422483 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
484610 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
249046 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today


11:44
90%
CP-BIMOAR
436563 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
870963 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
875804 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
427187 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
257183 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today
508452 is your OTP for FB games OTP is valid for 5 minutes BIRJUA
11:44 AM Today

Remediation:

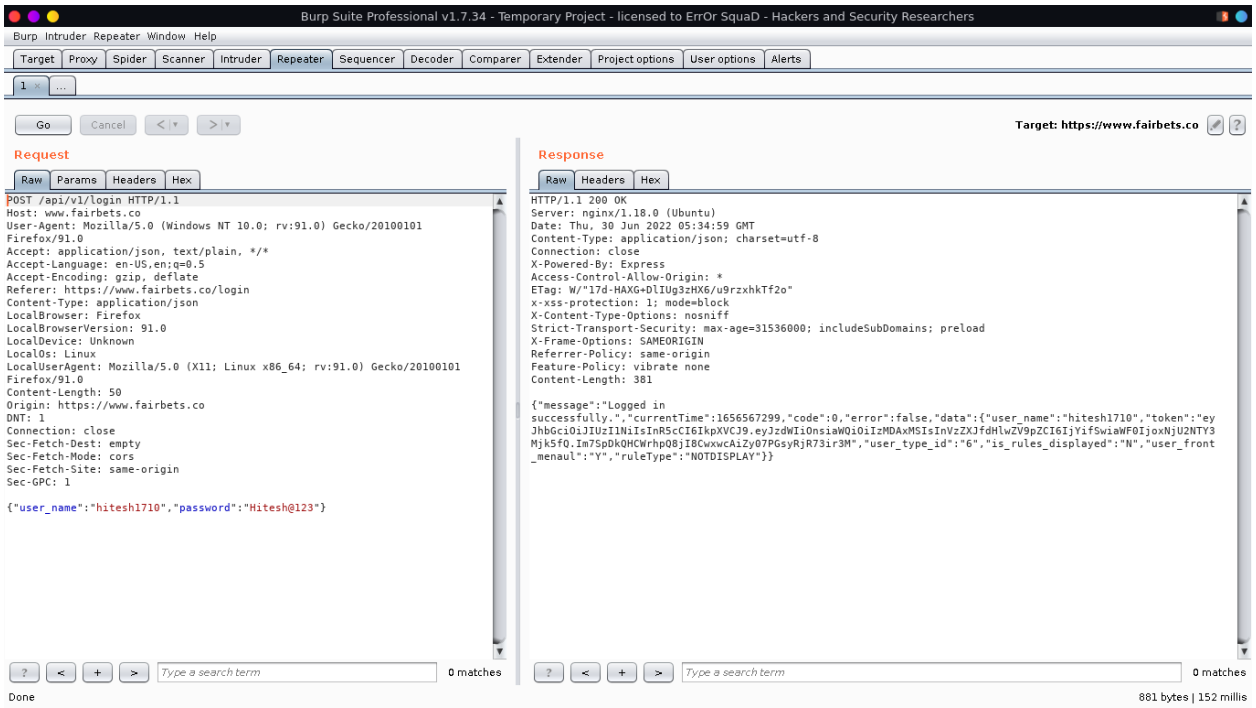
Who:	fairbets.co
Vector:	no rate limit
Action:	penetration tester recommends that SattaMatka: -set the limitations

❖ Missing Cookie Attributes

Severity	Medium
Description	Web Cookies (herein referred to as cookies) are often a key attack vector for malicious users (typically targeting other users) and the application should always take due diligence to protect cookies. HTTP is a stateless protocol, meaning that it doesn't hold any reference to requests being sent by the same user. In order to fix this issue, sessions were created and appended to HTTP requests. Browsers, as discussed in testing browser storage, contain a multitude of storage mechanisms. In that section of the guide, each is discussed thoroughly.
Impact	The most used session storage mechanism in browsers is cookie storage. Cookies can be set by the server, by including a `Set-Cookie` header in the HTTP response or via JavaScript. Cookies can be used for a multitude of reasons, such as: ● session management ● personalization ● tracking In order to secure cookie data, the industry has developed means to help lock down these cookies and limit their attack surface. Over time cookies have become a preferred storage mechanism for web applications, as they allow great flexibility in use and protection.
Path	https://www.fairbets.co

Severity	Medium
References	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes

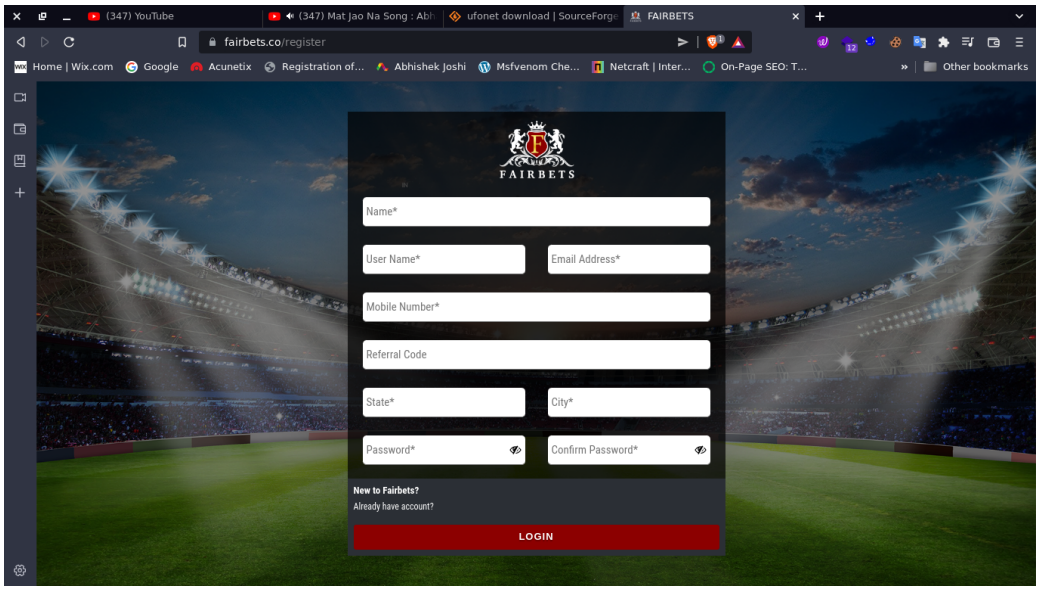
Exploitation Proof of Concept



Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Implement all cookie attributes - path - httponly -secure -domain -expire

❖ UI ISSUES

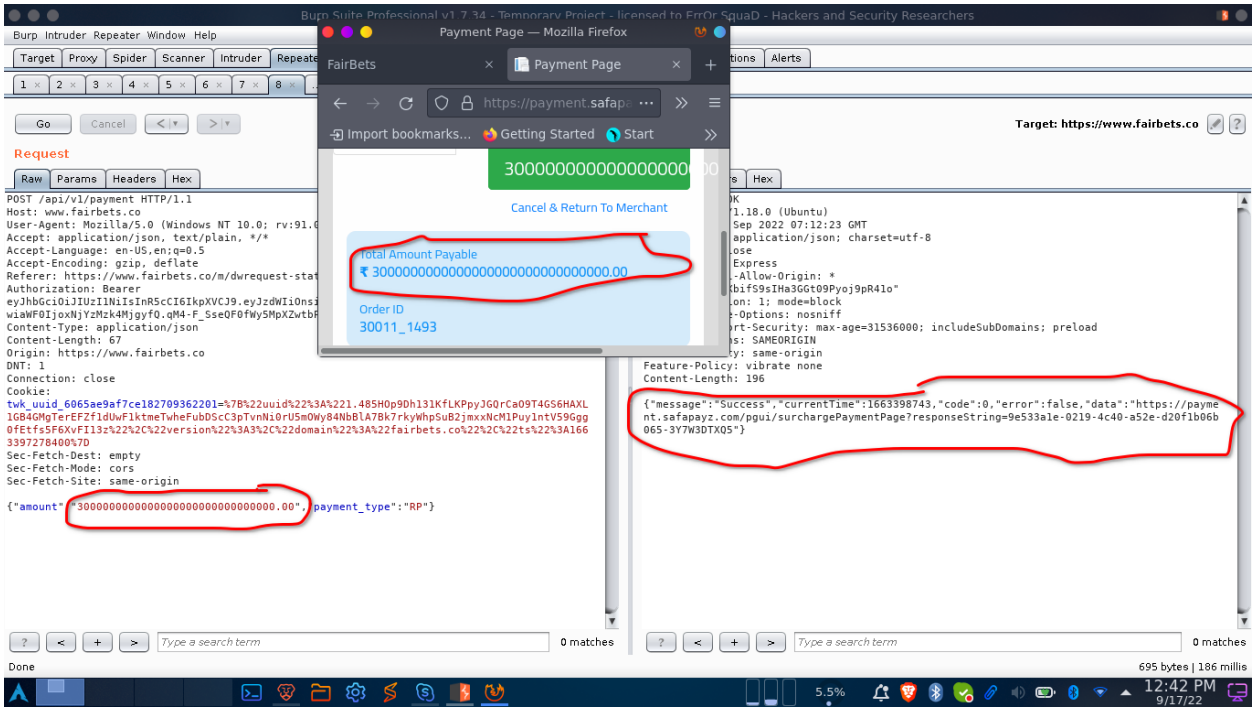


Check the ui issue of other laptop it was not comfortable

❖ Parameter tampering The Deposit Limit

Severity	Medium
Description	The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. This attack can be performed by a malicious user who wants to exploit the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack. In both cases, tools likes Webscarab and Paros proxy are mostly used.
Impact	Attacker can add the more value than max withdraw limit it might be attacker can white the black money also create business loss
Path	https://www.fairbets.co
Severity	**Critical**
References	https://owasp.org/www-community/attacks/Web_Parameter_Tampering

Exploitation Proof of Concept



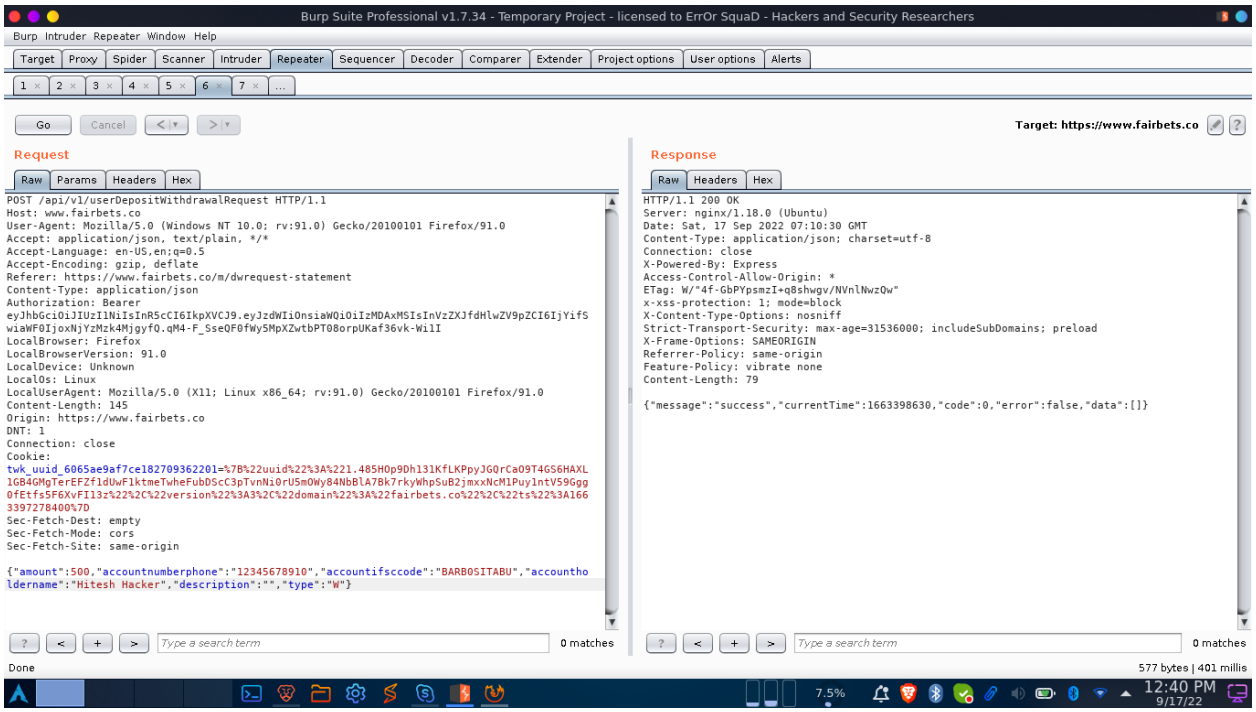
Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Attacker should not allow to change value • Check greater than and less than and equals parameter in code

❖ Request Manipulation In Bank Detail

Severity	**Medium**
Description	• Demonstrate the ability to capture HTTP data as it is communicated between your browser and the server it is communicating with. • Demonstrate the ability to modify this captured traffic before sending it to destination web servers.
Impact	Modify the request and easily change the detail in this scenario attack will change bank detail after they do kyc and submit bank detail
Path	https://www.fairbets.co
Severity	**Critical**
References	https://medium.com/nerd-for-tech/how-to-manipulate-web-requests-ea5cf1c80a90

Exploitation Proof of Concept



Remediation

Target	https://www.fairbets.co
Vector	Local
Recommendation	Pentester recommends that • Attacker should not modify the request and target