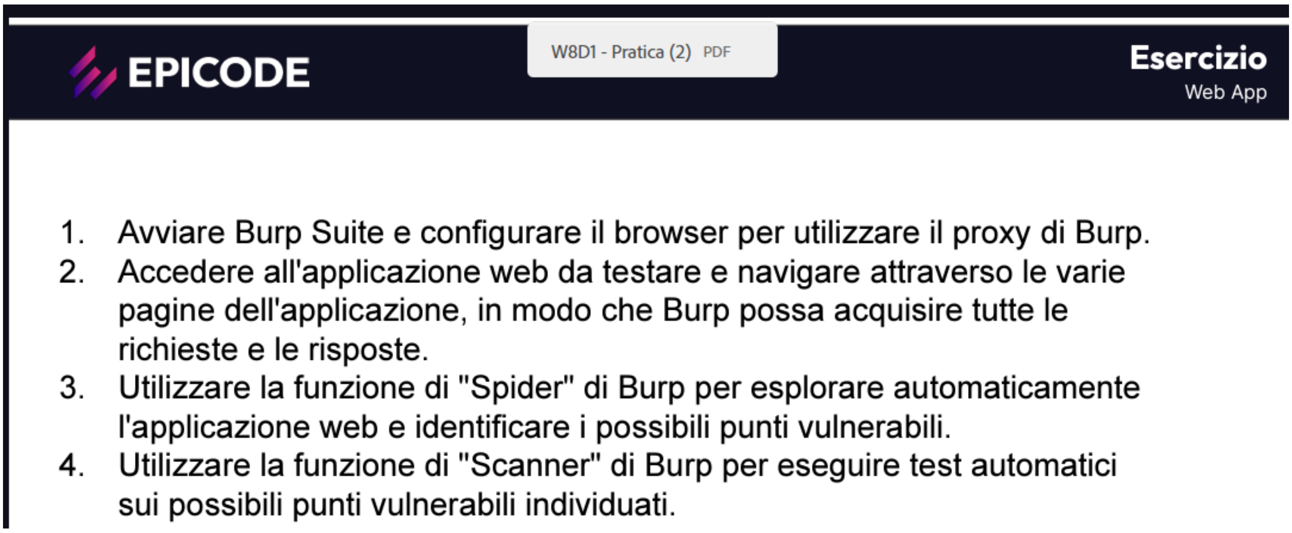
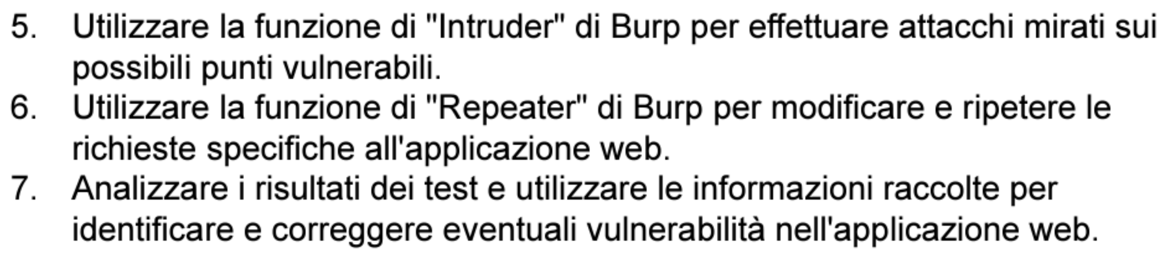
Traccia:



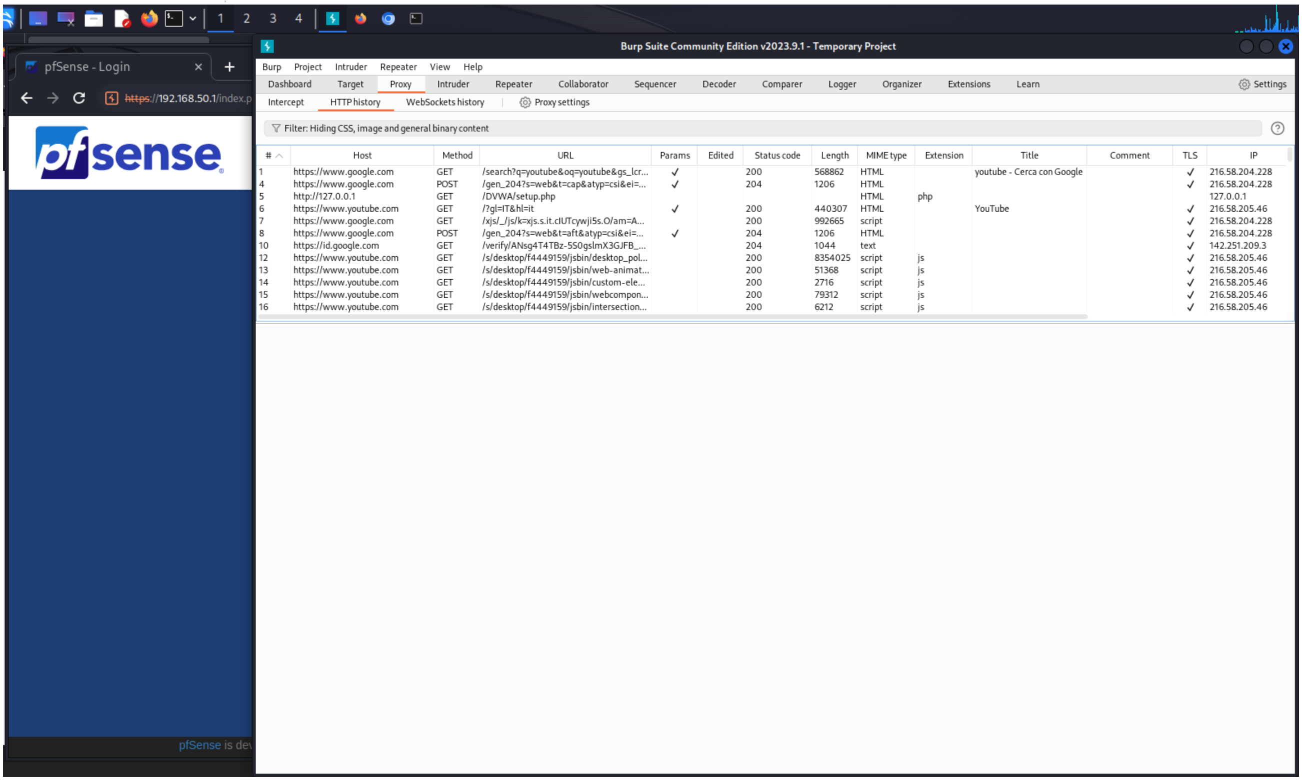
1. Avviare Burp Suite e configurare il browser per utilizzare il proxy di Burp.
2. Accedere all'applicazione web da testare e navigare attraverso le varie pagine dell'applicazione, in modo che Burp possa acquisire tutte le richieste e le risposte.
3. Utilizzare la funzione di "Spider" di Burp per esplorare automaticamente l'applicazione web e identificare i possibili punti vulnerabili.
4. Utilizzare la funzione di "Scanner" di Burp per eseguire test automatici sui possibili punti vulnerabili individuati.



5. Utilizzare la funzione di "Intruder" di Burp per effettuare attacchi mirati sui possibili punti vulnerabili.
6. Utilizzare la funzione di "Repeater" di Burp per modificare e ripetere le richieste specifiche all'applicazione web.
7. Analizzare i risultati dei test e utilizzare le informazioni raccolte per identificare e correggere eventuali vulnerabilità nell'applicazione web.

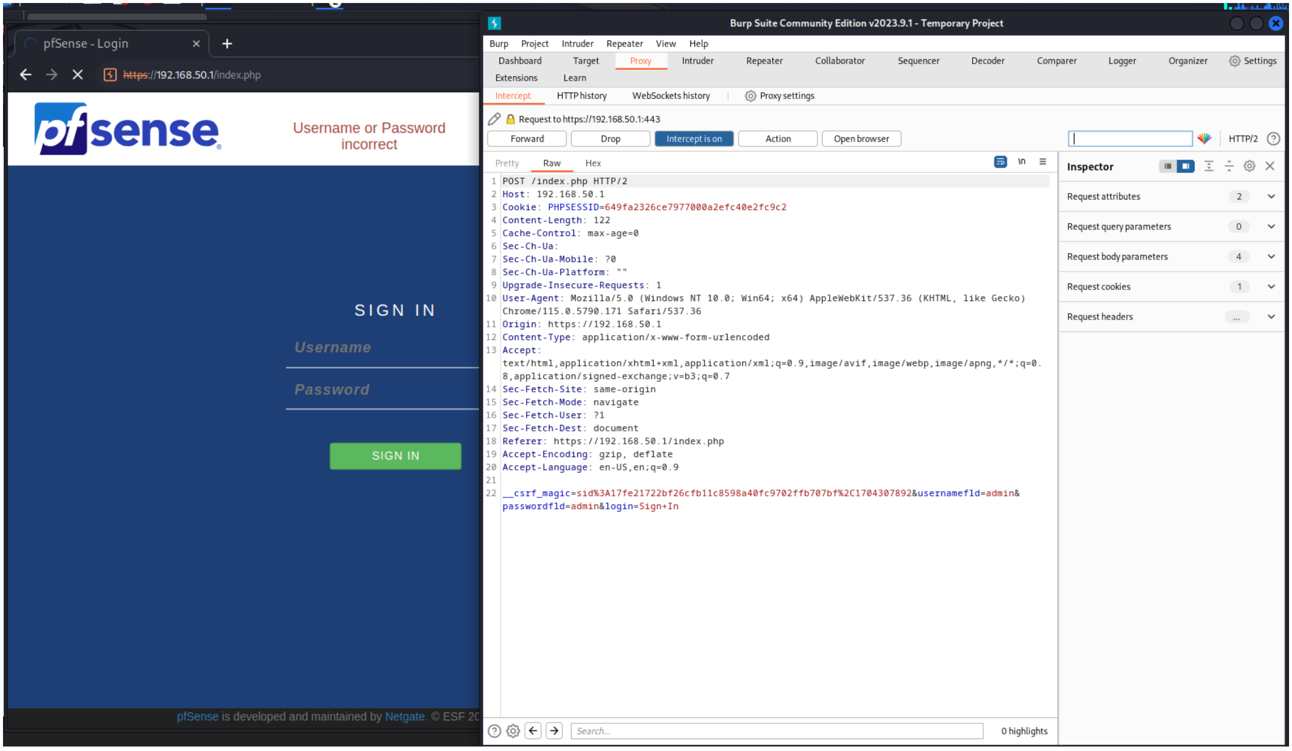
Soluzione:

1 e 2) Accesso alla pagina di login di Pfsense e acquisite le richieste e le risposte (vedi screen in allegato)


pfSense - Login
https://192.168.50.1/index.p
pfsense
pfSense is dev
Burp Suite Community Edition v2023.9.1 - 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 Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1	https://www.google.com	GET	/search?q=youtube&oq=youtube&gs_lcr...	✓		200	568862	HTML		youtube - Cerca con Google		✓	216.58.204.228
4	https://www.google.com	POST	/gen_204?s=web&t=cap&atyp=csi&ei=...	✓		204	1206	HTML				✓	216.58.204.228
5	http://127.0.0.1	GET	/DVWA/setup.php					HTML	php				127.0.0.1
6	https://www.youtube.com	GET	/?gl=IT&hl=it	✓		200	440307	HTML		YouTube		✓	216.58.205.46
7	https://www.google.com	GET	/xjs/_/js/k=xjs.s.it.cIUTcywji5s.O/am=A...			200	992665	script				✓	216.58.204.228
8	https://www.google.com	POST	/gen_204?s=web&t=aft&atyp=csi&ei=...	✓		204	1206	HTML				✓	216.58.204.228
10	https://id.google.com	GET	/verify/ANsg4T4TBz-5S0gslmX3GJFB_...			204	1044	text				✓	142.251.209.3
12	https://www.youtube.com	GET	/s/desktop/f4449159/jsbin/desktop_pol...			200	8354025	script	js			✓	216.58.205.46
13	https://www.youtube.com	GET	/s/desktop/f4449159/jsbin/web-animat...			200	51368	script	js			✓	216.58.205.46
14	https://www.youtube.com	GET	/s/desktop/f4449159/jsbin/custom-ele...			200	2716	script	js			✓	216.58.205.46
15	https://www.youtube.com	GET	/s/desktop/f4449159/jsbin/webcompon...			200	79312	script	js			✓	216.58.205.46
16	https://www.youtube.com	GET	/s/desktop/f4449159/jsbin/intersection...			200	6212	script	js			✓	216.58.205.46


pfSense - Login
https://192.168.50.1/index.php
pfsense
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 20
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
HTTP/2
Pretty Raw Hex
Inspector
Search...
0 highlights

Username or Password incorrect

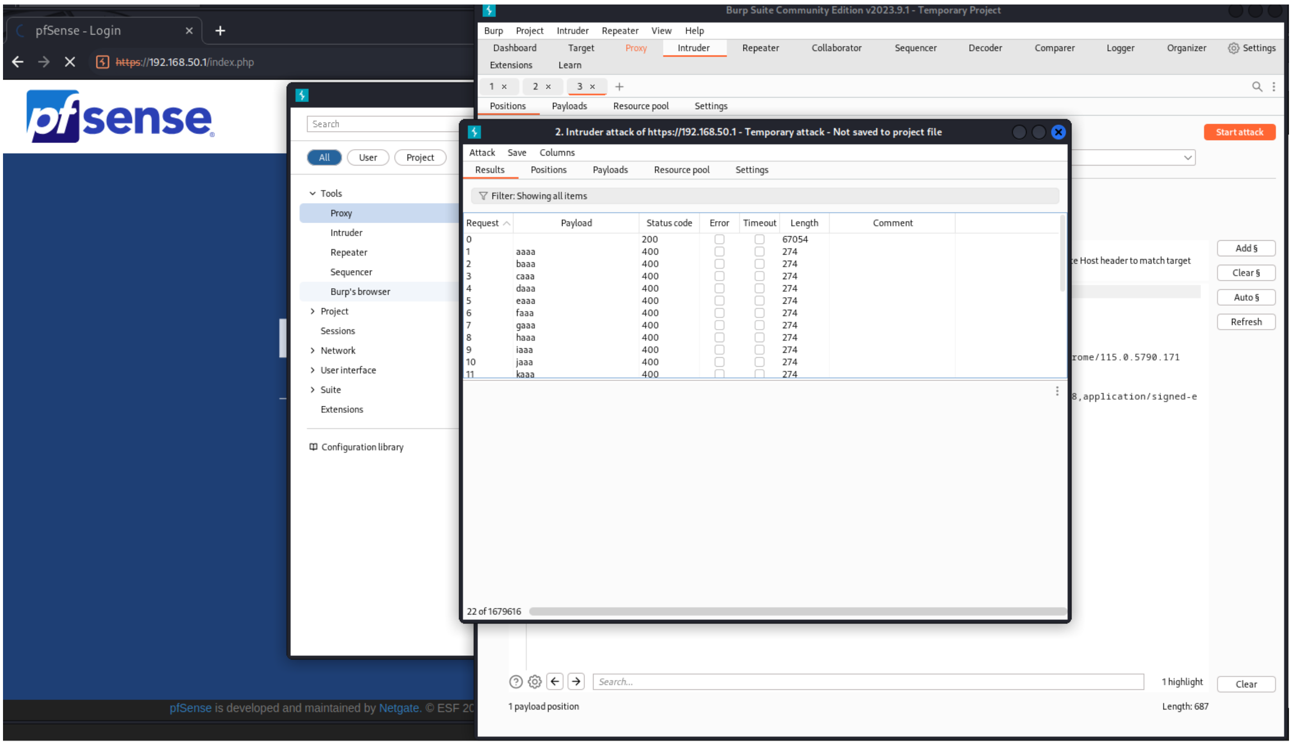
Request to https://192.168.50.1:443

```
POST /index.php HTTP/2
Host: 192.168.50.1
Cookie: PHPSESSID=649fa2326ce7977000a2efc40e2fc9c2
Content-Length: 122
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
Origin: https://192.168.50.1
Content-Type: application/x-www-form-urlencoded
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://192.168.50.1/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

__csrf_magic=sid%3A17fe21722bf26cfb11c8598a40fc9702ffb707bf%2C1704307892&usernamefld=admin&
passwordfld=admin&login=Sign+In
```

Request attributes	2
Request query parameters	0
Request body parameters	4
Request cookies	1
Request headers	...

3 e 5) Esecuzione delle varie tipologie di attacco



Burp Suite Community Edition v2023.9.1 - Temporary Project

2. Intruder attack of https://192.168.50.1 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	67054	
1	aaaa	400	□	□	274	
2	baaa	400	□	□	274	
3	caaa	400	□	□	274	
4	daaa	400	□	□	274	
5	eaaa	400	□	□	274	
6	faaa	400	□	□	274	
7	gaaa	400	□	□	274	
8	haaa	400	□	□	274	
9	iaaa	400	□	□	274	
10	jaaa	400	□	□	274	
11	kaaa	400	□	□	274	

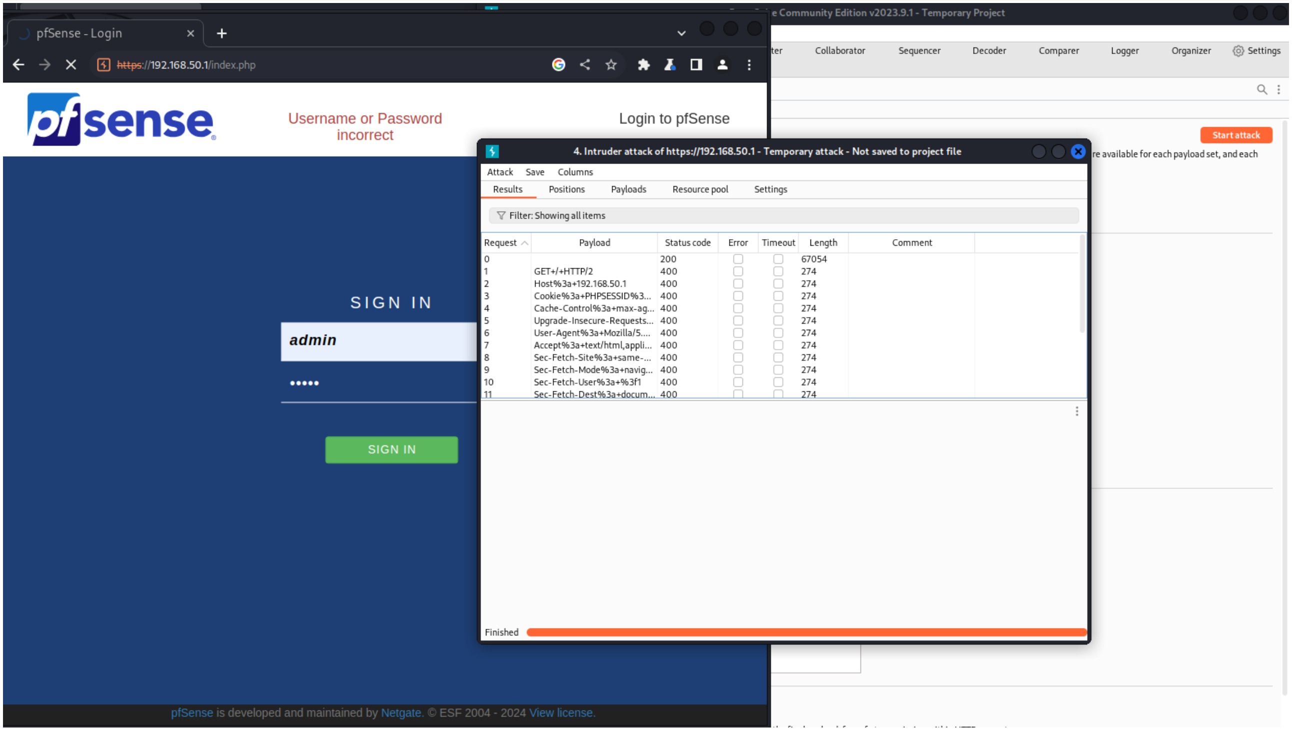
22 of 1679616

1 payload position

1 highlight

Length: 687

pfSense is developed and maintained by Netgate. © ESF 20



4. Intruder attack of https://192.168.50.1 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	67054	
1	GET+/+HTTP/2	400	□	□	274	
2	Host%3a+192.168.50.1	400	□	□	274	
3	Cookie%3a+PHPSESSID%3...	400	□	□	274	
4	Cache-Control%3a+max-ag...	400	□	□	274	
5	Upgrade-Insecure-Requests...	400	□	□	274	
6	User-Agent%3a+Mozilla/5....	400	□	□	274	
7	Accept%3a+text/html,appli...	400	□	□	274	
8	Sec-Fetch-Site%3a+same-...	400	□	□	274	
9	Sec-Fetch-Mode%3a+navig...	400	□	□	274	
10	Sec-Fetch-User%3a+%3f1	400	□	□	274	
11	Sec-Fetch-Dest%3a+docum...	400	□	□	274	

Finished

Username or Password incorrect

Login to pfSense

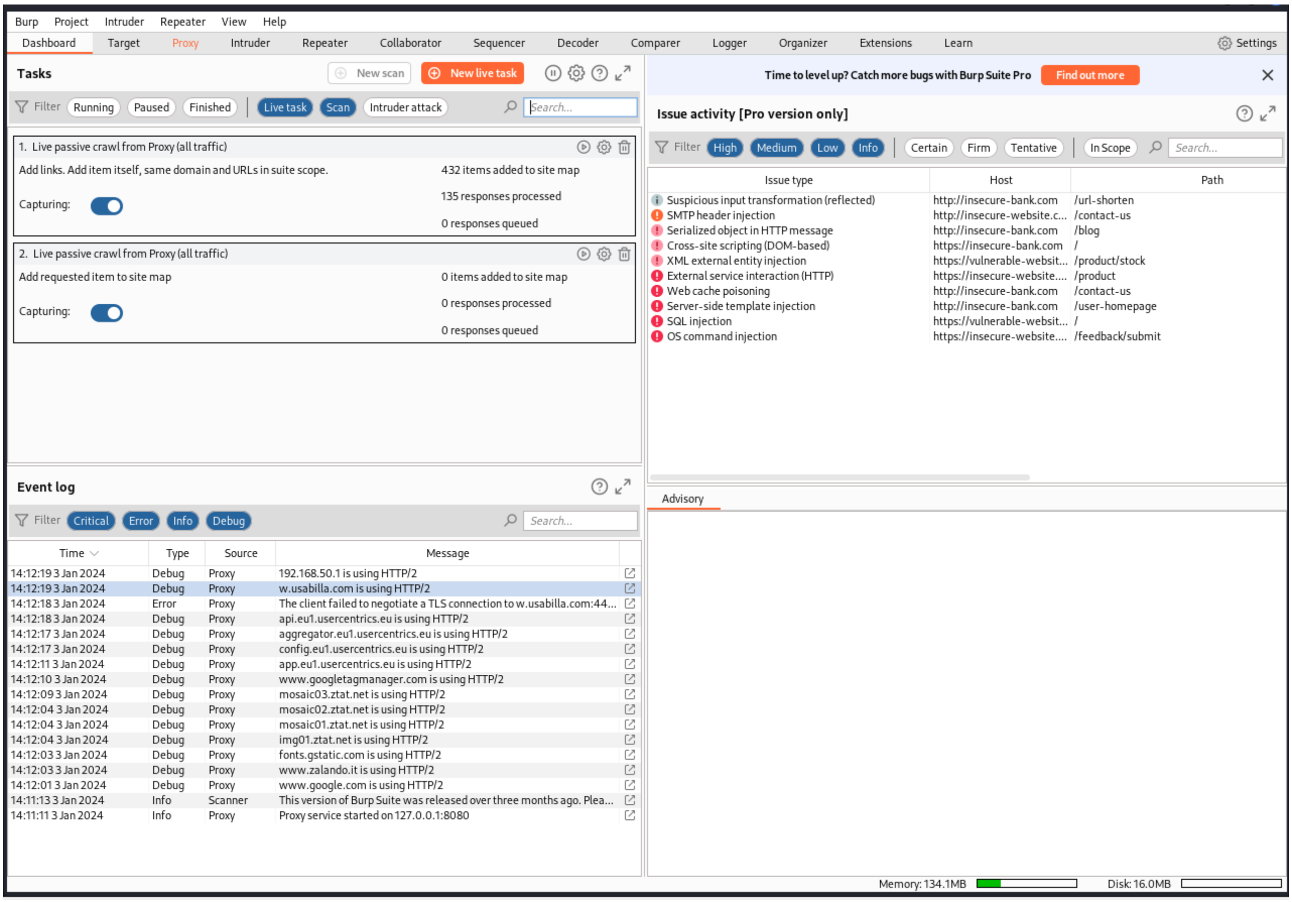
SIGN IN

admin

•••••

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

4) Utilizzo della funzione scanner



1. Live passive crawl from Proxy (all traffic)

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

432 items added to site map

135 responses processed

0 responses queued

Capturing: ●

2. Live passive crawl from Proxy (all traffic)

Add requested item to site map

0 items added to site map

0 responses processed

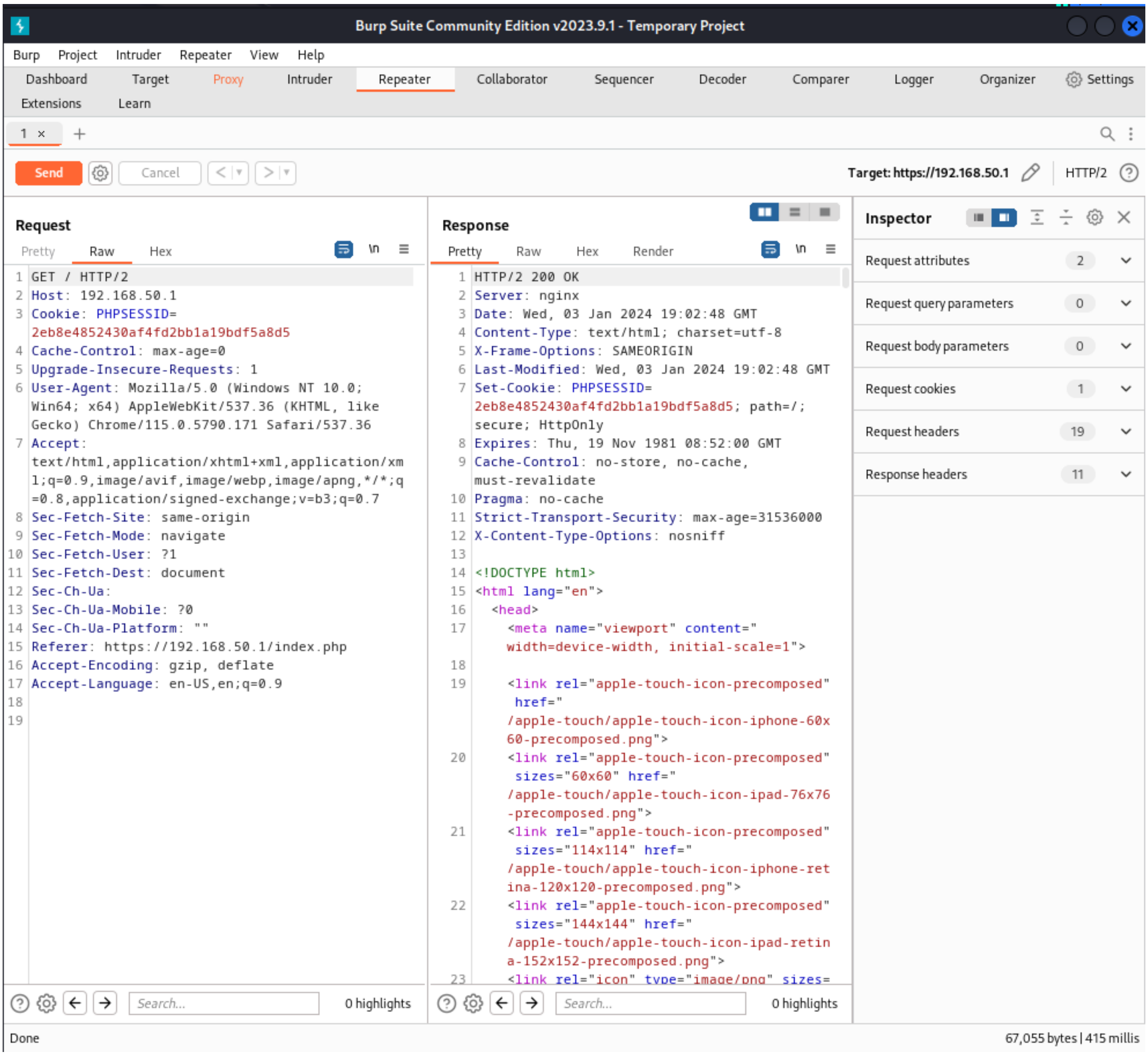
0 responses queued

Capturing: ●

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Time	Type	Source	Message
14:12:19 3 Jan 2024	Debug	Proxy	192.168.50.1 is using HTTP/2
14:12:19 3 Jan 2024	Debug	Proxy	w.usabilla.com is using HTTP/2
14:12:18 3 Jan 2024	Error	Proxy	The client failed to negotiate a TLS connection to w.usabilla.com:44...
14:12:18 3 Jan 2024	Debug	Proxy	api.eu1.usercentrics.eu is using HTTP/2
14:12:17 3 Jan 2024	Debug	Proxy	aggregator.eu1.usercentrics.eu is using HTTP/2
14:12:17 3 Jan 2024	Debug	Proxy	config.eu1.usercentrics.eu is using HTTP/2
14:12:11 3 Jan 2024	Debug	Proxy	app.eu1.usercentrics.eu is using HTTP/2
14:12:10 3 Jan 2024	Debug	Proxy	www.googletagmanager.com is using HTTP/2
14:12:09 3 Jan 2024	Debug	Proxy	mosaic03.ztat.net is using HTTP/2
14:12:04 3 Jan 2024	Debug	Proxy	mosaic02.ztat.net is using HTTP/2
14:12:04 3 Jan 2024	Debug	Proxy	mosaic01.ztat.net is using HTTP/2
14:12:04 3 Jan 2024	Debug	Proxy	img01.ztat.net is using HTTP/2
14:12:03 3 Jan 2024	Debug	Proxy	fonts.gstatic.com is using HTTP/2
14:12:03 3 Jan 2024	Debug	Proxy	www.zalando.it is using HTTP/2
14:12:01 3 Jan 2024	Debug	Proxy	www.google.com is using HTTP/2
14:11:13 3 Jan 2024	Info	Scanner	This version of Burp Suite was released over three months ago. Plea...
14:11:11 3 Jan 2024	Info	Proxy	Proxy service started on 127.0.0.1:8080

6) Utilizzo della funzione repeater per modificare richieste specifiche all’applicazione web

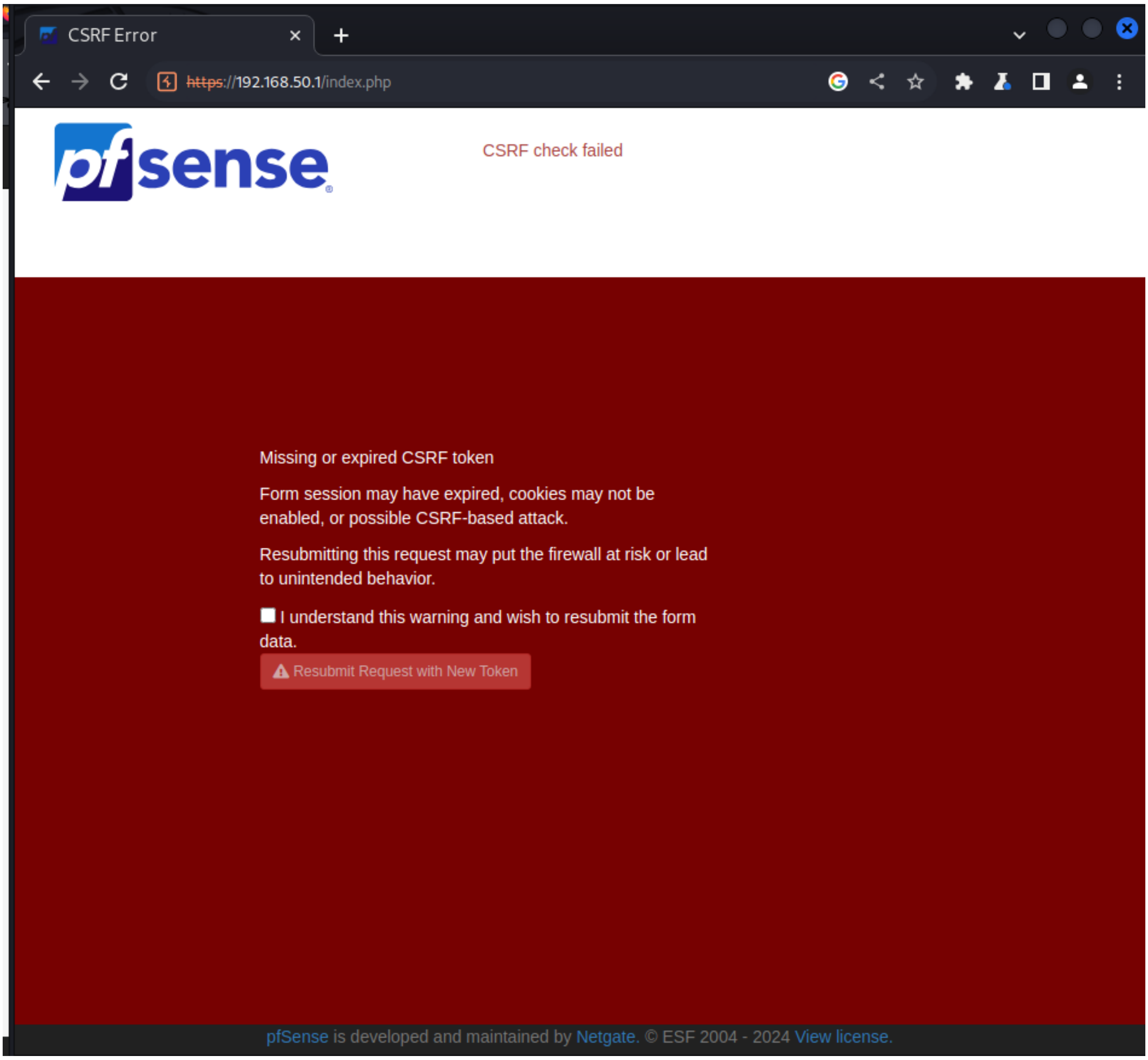

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
1 ×
Send
Cancel
Target: https://192.168.50.1
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 19
Response headers 11
Search...
0 highlights
Search...
0 highlights
Done
67,055 bytes | 415 millis

```
GET / HTTP/2
Host: 192.168.50.1
Cookie: PHPSESSID=
2eb8e4852430af4fd2bb1a19bdf5a8d5
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Referer: https://192.168.50.1/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Server: nginx
Date: Wed, 03 Jan 2024 19:02:48 GMT
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Last-Modified: Wed, 03 Jan 2024 19:02:48 GMT
Set-Cookie: PHPSESSID=
2eb8e4852430af4fd2bb1a19bdf5a8d5; path=/;
secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta name="viewport" content="
    width=device-width, initial-scale=1">

    <link rel="apple-touch-icon-precomposed"
     href="
    /apple-touch/apple-touch-icon-iphone-60x
    60-precomposed.png">
    <link rel="apple-touch-icon-precomposed"
     sizes="60x60" href="
    /apple-touch/apple-touch-icon-ipad-76x76
    -precomposed.png">
    <link rel="apple-touch-icon-precomposed"
     sizes="114x114" href="
    /apple-touch/apple-touch-icon-iphone-ret
    ina-120x120-precomposed.png">
    <link rel="apple-touch-icon-precomposed"
     sizes="144x144" href="
    /apple-touch/apple-touch-icon-ipad-retin
    a-152x152-precomposed.png">
    <link rel="icon" type="image/png" sizes=
```



CSRF Error
https://192.168.50.1/index.php

CSRF check failed

Missing or expired CSRF token

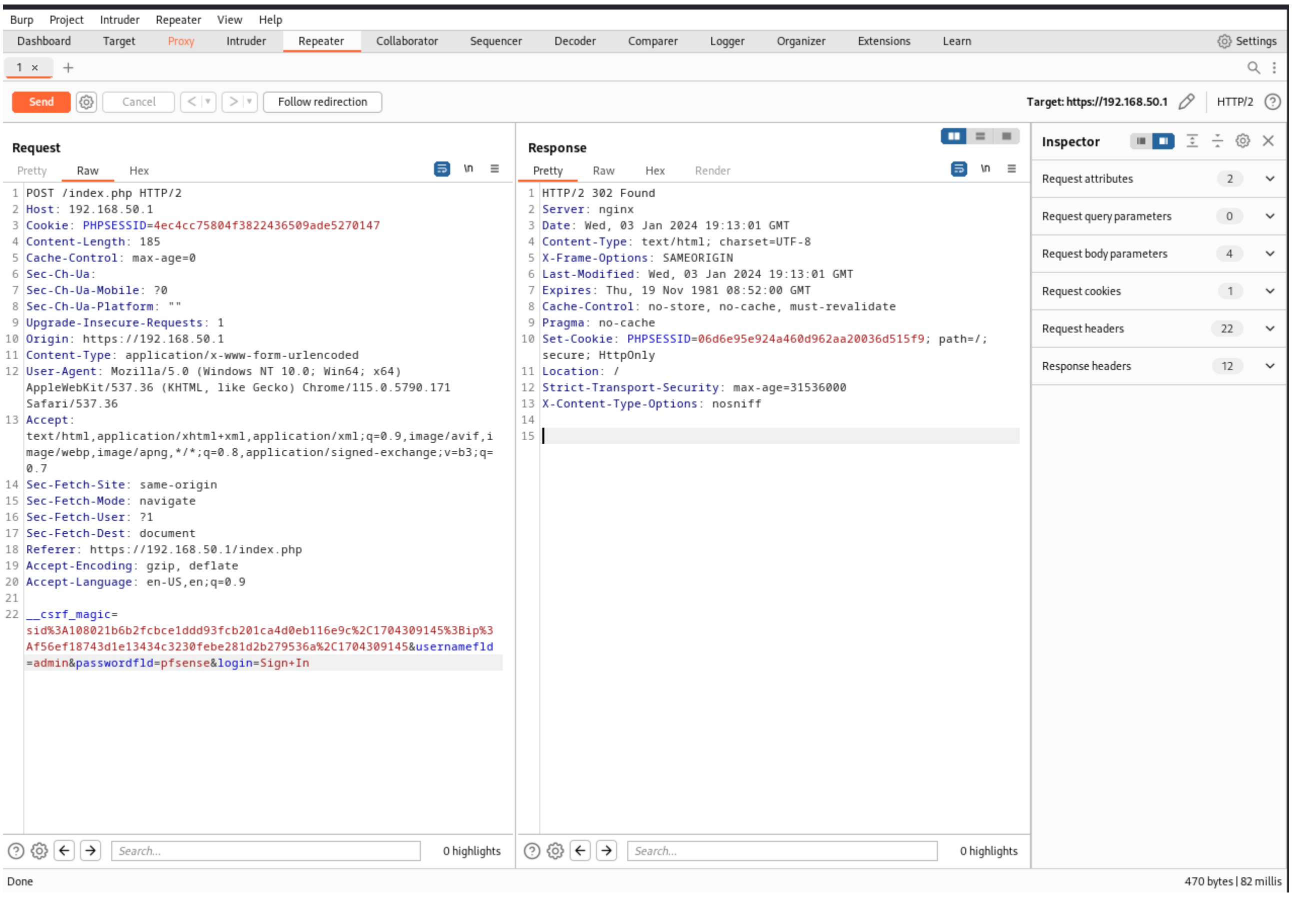
Form session may have expired, cookies may not be enabled, or possible CSRF-based attack.

Resubmitting this request may put the firewall at risk or lead to unintended behavior.

□ I understand this warning and wish to resubmit the form data.

Resubmit Request with New Token

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.



```
POST /index.php HTTP/2
Host: 192.168.50.1
Cookie: PHPSESSID=4ec4cc75804f3822436509ade5270147
Content-Length: 185
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://192.168.50.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://192.168.50.1/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

__csrf_magic=
sid%3A108021b6b2fcbce1ddd93fcb201ca4d0eb116e9c%2C1704309145%3Bip%3
Af56ef18743d1e13434c3230febe281d2b279536a%2C1704309145&usernamefld
=admin&passwordfld=pfsense&login=Sign+In
```

```
HTTP/2 302 Found
Server: nginx
Date: Wed, 03 Jan 2024 19:13:01 GMT
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Last-Modified: Wed, 03 Jan 2024 19:13:01 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=06d6e95e924a460d962aa20036d515f9; path=/;
secure; HttpOnly
Location: /
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff

```