HTTP’s Basic Authentication: A Story

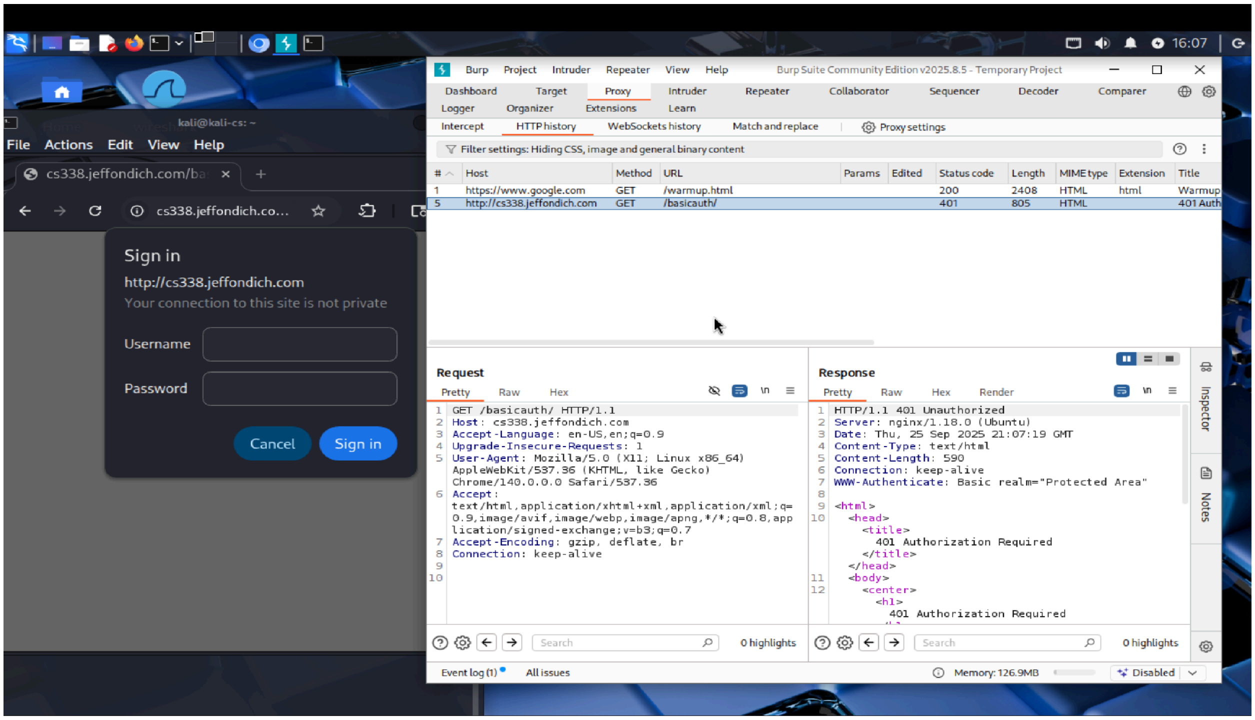
Beshir Said

To explore the details and limitations of Basic Authentication, I used BurpSuite Community Edition inside the Kali Linux. Essentially, BurpSuite is a software tool used for analyzing security and discovering the ins and outs of HTTP requests and responses.

I first loaded Jeff’s nginx server http://cs338.jeffondich.com/basicauth/ without signing in. The initial request inside the HTTP history came back with 401 Authorization Required message with the Authorization header of WWW-Authenticate: Basic realm = “Protected Area” (Figures 1-2). The Authorization header is the part of the HTTP request that carries the clients credentials to the server, so the server can verify the clients identity.

Once I entered the username and password, the browser resent the request with a Base64-encoded string. I decoded the Base64 string inside the terminal and received this output: cs338:password (Figure 5). This confirmed that Basic Authentication simply encodes the credentials and does not encrypt them. After this, the server responded with a HTTP/1.1 200 OK and gave me the contents of the secret directory (Figure 4). The curl command confirmed the same interaction, showing the earlier 401 message and later the successful 200 response (Figure 3).

This experiment shows how HTTP Basic Authentication works but at the same time how it is insecure. The flow from 401 Unauthorized to the Authorization Header to 200 OK shows how the browser and server interact. However, the credentials are only Base64-encoded and anyone monitoring the plaintext HTTP traffic can recover them on a network like Wireshark. I think for this reason, one should try to use stronger authentication methods and also note that Basic Authentication should always be used over HTTPS. Unlike HTTP, HTTPS wraps the content inside TLS/SSL encryption, meaning intruders cannot read the requests, responses, or headers.


Burp Suite Community Edition v2025.8.5 - Temporary Project
Proxy
HTTP history
Filter settings: Hiding CSS, image and general binary content
Sign in
http://cs338.jeffondich.com
Your connection to this site is not private
Username
Password
Cancel
Sign in

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	https://www.google.com	GET	/warmup.html			200	2408	HTML	html	Warmup
5	http://cs338.jeffondich.com	GET	/basicauth/			401	805	HTML		401 Auth

Request

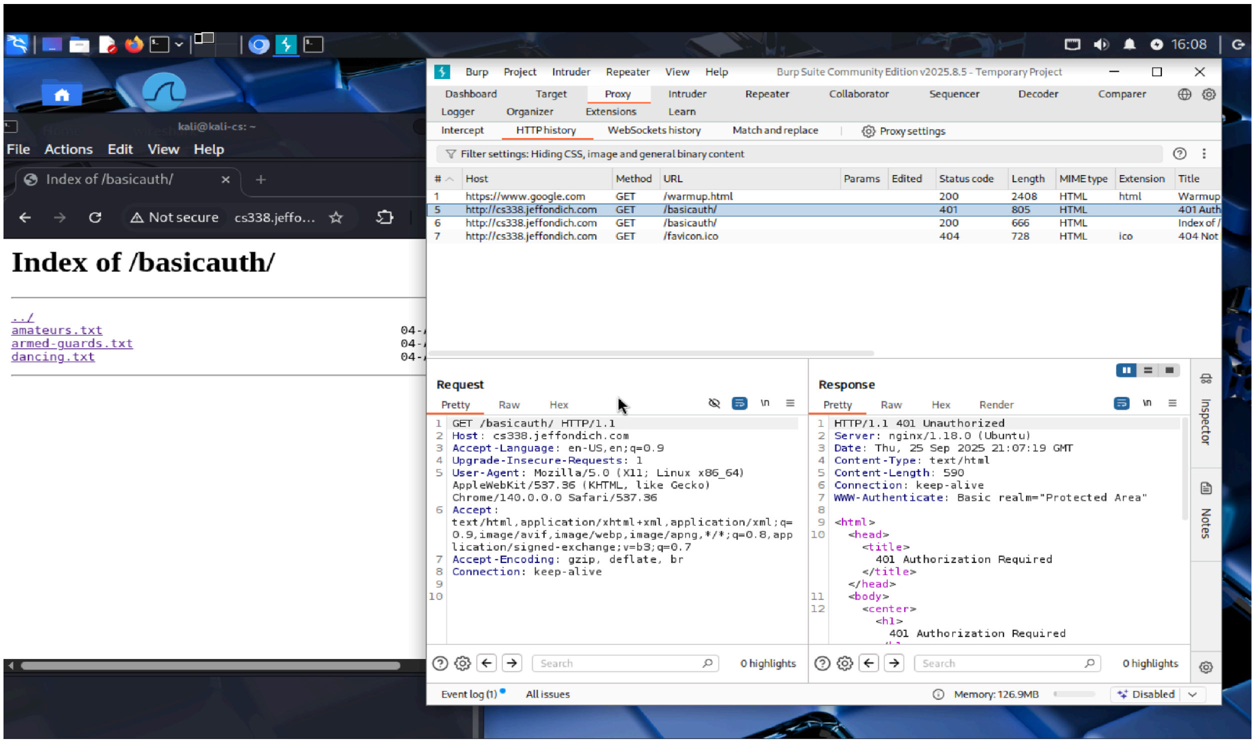
```
GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Sep 2025 21:07:19 GMT
Content-Type: text/html
Content-Length: 590
Connection: keep-alive
WWW-Authenticate: Basic realm="Protected Area"

<html>
  <head>
    <title>
      401 Authorization Required
    </title>
  </head>
  <body>
    <center>
      <h1>
        401 Authorization Required
```

Figure 1: 401 Authorization Required before signing in


Burp Suite Community Edition v2025.8.5 - Temporary Project
Proxy
HTTP history
Filter settings: Hiding CSS, image and general binary content
Index of /basicauth/
Not secure

Index of /basicauth/

```
../
amateurs.txt                                       04-
armed-guards.txt                                   04-
dancing.txt                                        04-
```

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	https://www.google.com	GET	/warmup.html			200	2408	HTML	html	Warmup
5	http://cs338.jeffondich.com	GET	/basicauth/			401	805	HTML		401 Auth
6	http://cs338.jeffondich.com	GET	/basicauth/			200	666	HTML		Index of /
7	http://cs338.jeffondich.com	GET	/favicon.ico			404	728	HTML	ico	404 Not

Request

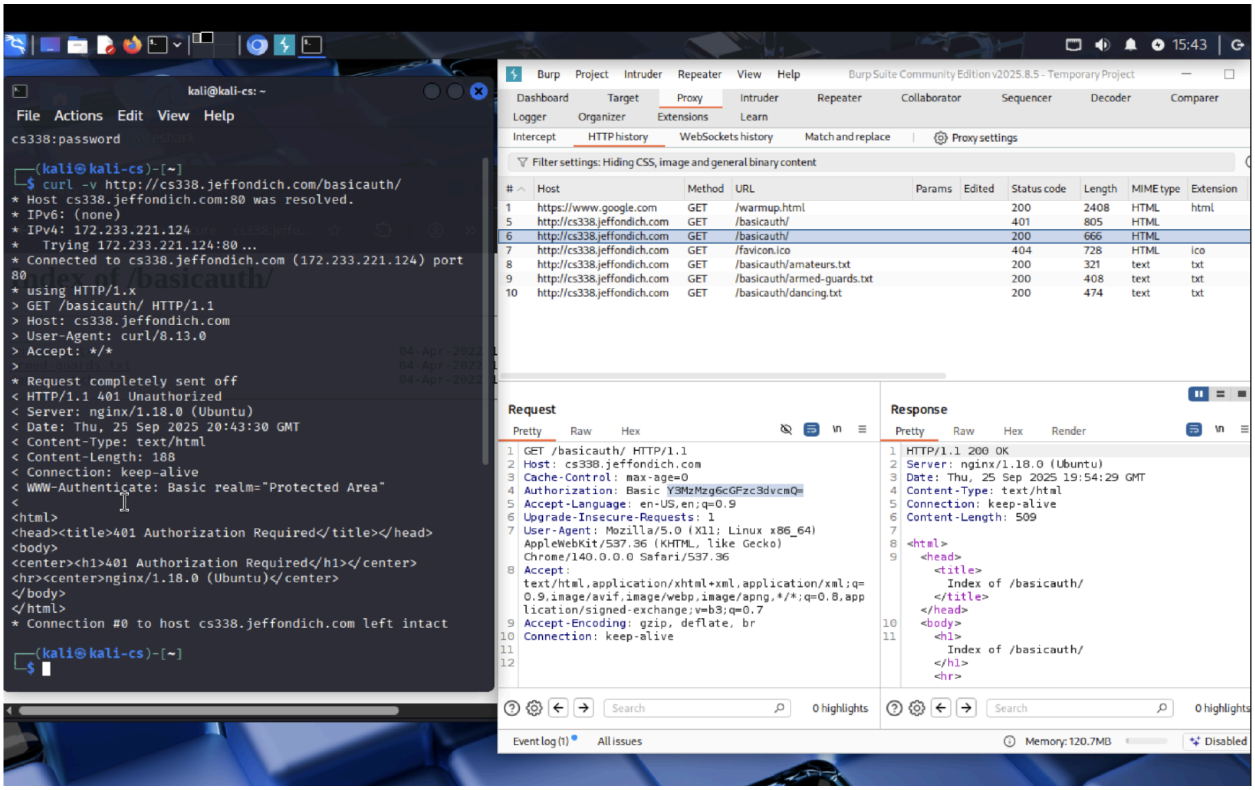
```
GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Sep 2025 21:07:19 GMT
Content-Type: text/html
Content-Length: 590
Connection: keep-alive
WWW-Authenticate: Basic realm="Protected Area"

<html>
  <head>
    <title>
      401 Authorization Required
    </title>
  </head>
  <body>
    <center>
      <h1>
        401 Authorization Required
```

Figure 2: 401 Unauthorized with WWW-Authenticate Basic realm = “Protected Area”



```
cs338:password

┌──(kali㉿kali-cs)-[~]
└─$ curl -v http://cs338.jeffondich.com/basicauth/
* Host cs338.jeffondich.com:80 was resolved.
* IPv6: (none)
* IPv4: 172.233.221.124
*   Trying 172.233.221.124:80 ...
* Connected to cs338.jeffondich.com (172.233.221.124) port
80
* using HTTP/1.x
> GET /basicauth/ HTTP/1.1
> Host: cs338.jeffondich.com
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 401 Unauthorized
< Server: nginx/1.18.0 (Ubuntu)
< Date: Thu, 25 Sep 2025 20:43:30 GMT
< Content-Type: text/html
< Content-Length: 188
< Connection: keep-alive
< WWW-Authenticate: Basic realm="Protected Area"
<
<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
* Connection #0 to host cs338.jeffondich.com left intact

┌──(kali㉿kali-cs)-[~]
└─$
```

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
1	https://www.google.com	GET	/warmup.html			200	2408	HTML	html
5	http://cs338.jeffondich.com	GET	/basicauth/			401	805	HTML	
6	http://cs338.jeffondich.com	GET	/basicauth/			200	666	HTML	
7	http://cs338.jeffondich.com	GET	/favicon.ico			404	728	HTML	ico
8	http://cs338.jeffondich.com	GET	/basicauth/amateurs.txt			200	321	text	txt
9	http://cs338.jeffondich.com	GET	/basicauth/armed-guards.txt			200	408	text	txt
10	http://cs338.jeffondich.com	GET	/basicauth/dancing.txt			200	474	text	txt

Request

```
GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Cache-Control: max-age=0
Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=
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/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

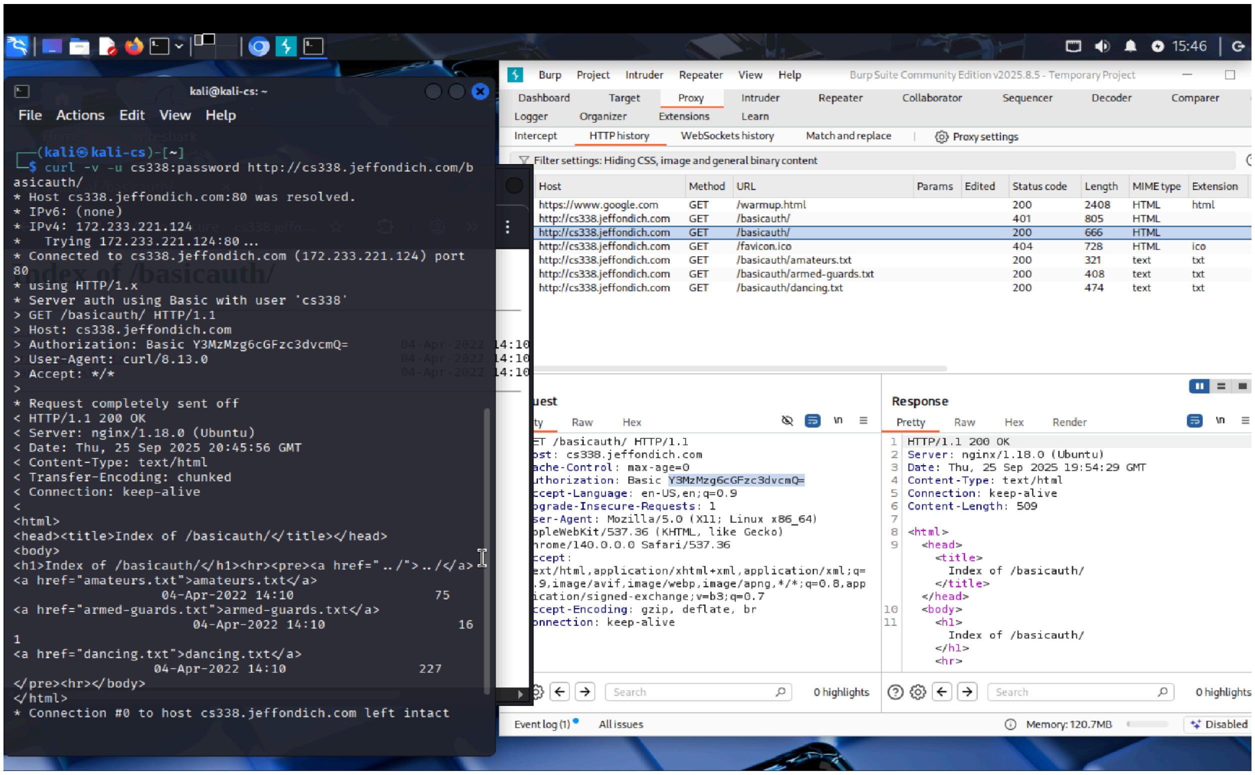
Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Sep 2025 19:54:29 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 509

<html>
  <head>
    <title>
      Index of /basicauth/
    </title>
  </head>
  <body>
    <h1>
      Index of /basicauth/
    </h1>
    <hr>
```

15:43
kali@kali-cs: ~
File Actions Edit View Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Pretty Raw Hex
Pretty Raw Hex Render
Search
0 highlights
Event log (1)
All issues
Memory: 120.7MB
Disabled

Figure 3: curl output confirming the 401



```
┌──(kali㉿kali-cs)-[~]
└─$ curl -v -u cs338:password http://cs338.jeffondich.com/b
asicauth/
* Host cs338.jeffondich.com:80 was resolved.
* IPv6: (none)
* IPv4: 172.233.221.124
*   Trying 172.233.221.124:80 ...
* Connected to cs338.jeffondich.com (172.233.221.124) port
80
* using HTTP/1.x
* Server auth using Basic with user 'cs338'
> GET /basicauth/ HTTP/1.1
> Host: cs338.jeffondich.com
> Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Thu, 25 Sep 2025 20:45:56 GMT
< Content-Type: text/html
< Transfer-Encoding: chunked
< Connection: keep-alive
<
<html>
<head><title>Index of /basicauth/</title></head>
<body>
<h1>Index of /basicauth/</h1><hr><pre><a href="../">../</a>
<a href="amateurs.txt">amateurs.txt</a>
                   04-Apr-2022 14:10                  75
<a href="armed-guards.txt">armed-guards.txt</a>
                       04-Apr-2022 14:10                  16
1
<a href="dancing.txt">dancing.txt</a>
                  04-Apr-2022 14:10                  227
</pre><hr></body>
</html>
* Connection #0 to host cs338.jeffondich.com left intact
```

Filter settings: Hiding CSS, image and general binary content

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
https://www.google.com	GET	/warmup.html			200	2408	HTML	html
http://cs338.jeffondich.com	GET	/basicauth/			401	805	HTML	
http://cs338.jeffondich.com	GET	/basicauth/			200	666	HTML	
http://cs338.jeffondich.com	GET	/favicon.ico			404	728	HTML	ico
http://cs338.jeffondich.com	GET	/basicauth/amateurs.txt			200	321	text	txt
http://cs338.jeffondich.com	GET	/basicauth/armed-guards.txt			200	408	text	txt
http://cs338.jeffondich.com	GET	/basicauth/dancing.txt			200	474	text	txt

uest

```
ET /basicauth/ HTTP/1.1
ost: cs338.jeffondich.com
ache-Control: max-age=0
uthorization: Basic Y3MzMzg6cGFzc3dvcmQ=
ccept-Language: en-US,en;q=0.9
pgrade-Insecure-Requests: 1
ser-Agent: Mozilla/5.0 (X11; Linux x86_64)
opleWebKit/537.36 (KHTML, like Gecko)
hrome/140.0.0.0 Safari/537.36
ccept:
ext/html,application/xhtml+xml,application/xml;q=
.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
ication/signed-exchange;v=b3;q=0.7
ccept-Encoding: gzip, deflate, br
onnection: keep-alive
```

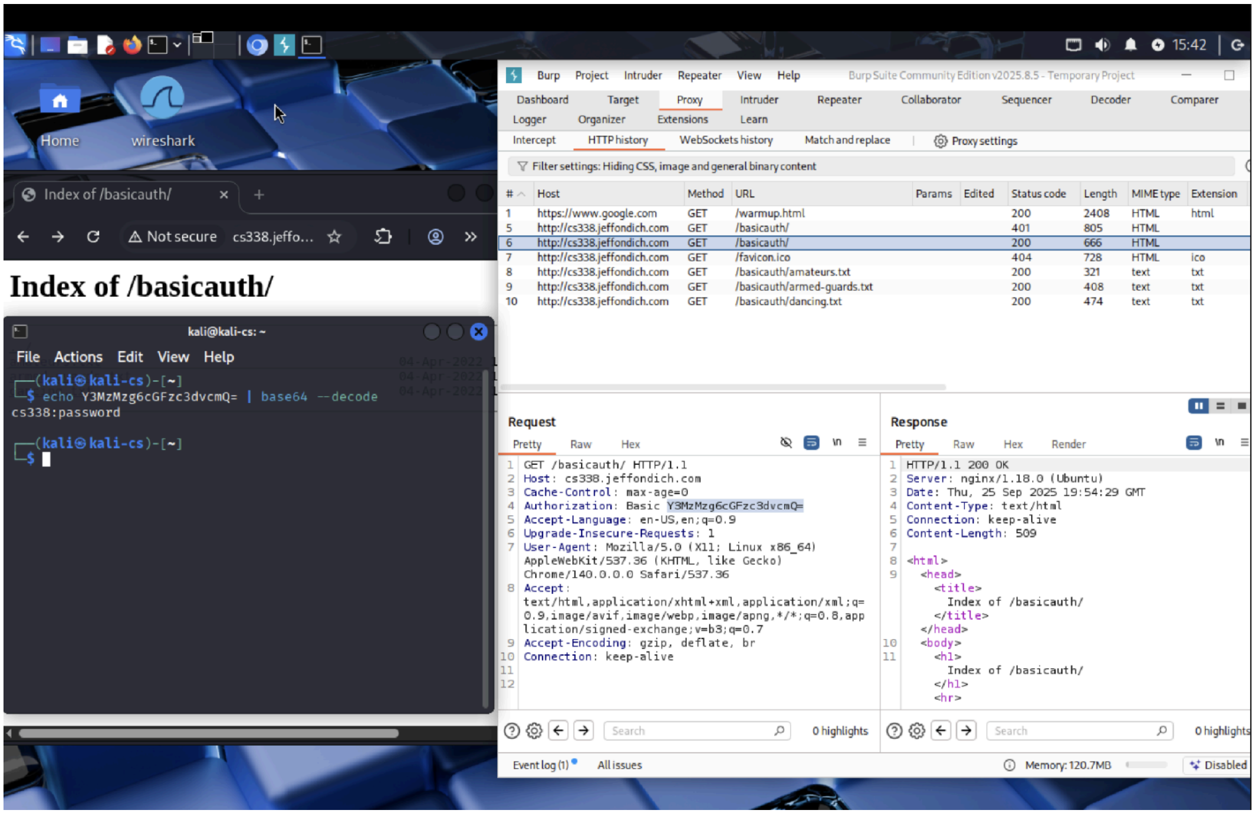
Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Sep 2025 19:54:29 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 509

<html>
  <head>
    <title>
      Index of /basicauth/
    </title>
  </head>
  <body>
    <h1>
      Index of /basicauth/
    </h1>
    <hr>
```

15:46
kali@kali-cs: ~
File Actions Edit View Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
ty Raw Hex
Pretty Raw Hex Render
Search
0 highlights
Event log (1)
All issues
Memory: 120.7MB
Disabled

Figure 4: Successful Authorized request with 200 OK with content listing



Index of /basicauth/

```
┌──(kali㉿kali-cs)-[~]
└─$ echo Y3MzMzg6cGFzc3dvcmQ= | base64 --decode
cs338:password

┌──(kali㉿kali-cs)-[~]
└─$ 
```

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
1	https://www.google.com	GET	/warmup.html			200	2408	HTML	html
5	http://cs338.jeffondich.com	GET	/basicauth/			401	805	HTML	
6	http://cs338.jeffondich.com	GET	/basicauth/			200	666	HTML	
7	http://cs338.jeffondich.com	GET	/favicon.ico			404	728	HTML	ico
8	http://cs338.jeffondich.com	GET	/basicauth/amateurs.txt			200	321	text	txt
9	http://cs338.jeffondich.com	GET	/basicauth/armed-guards.txt			200	408	text	txt
10	http://cs338.jeffondich.com	GET	/basicauth/dancing.txt			200	474	text	txt

```
GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Cache-Control: max-age=0
Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=
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/140.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Sep 2025 19:54:29 GMT
Content-Type: text/html
Connection: keep-alive
Content-Length: 509

<html>
  <head>
    <title>
      Index of /basicauth/
    </title>
  </head>
  <body>
    <h1>
      Index of /basicauth/
    </h1>
    <hr>
```

Figure 5: Request containing Authorization Basic Header and base64 decoding