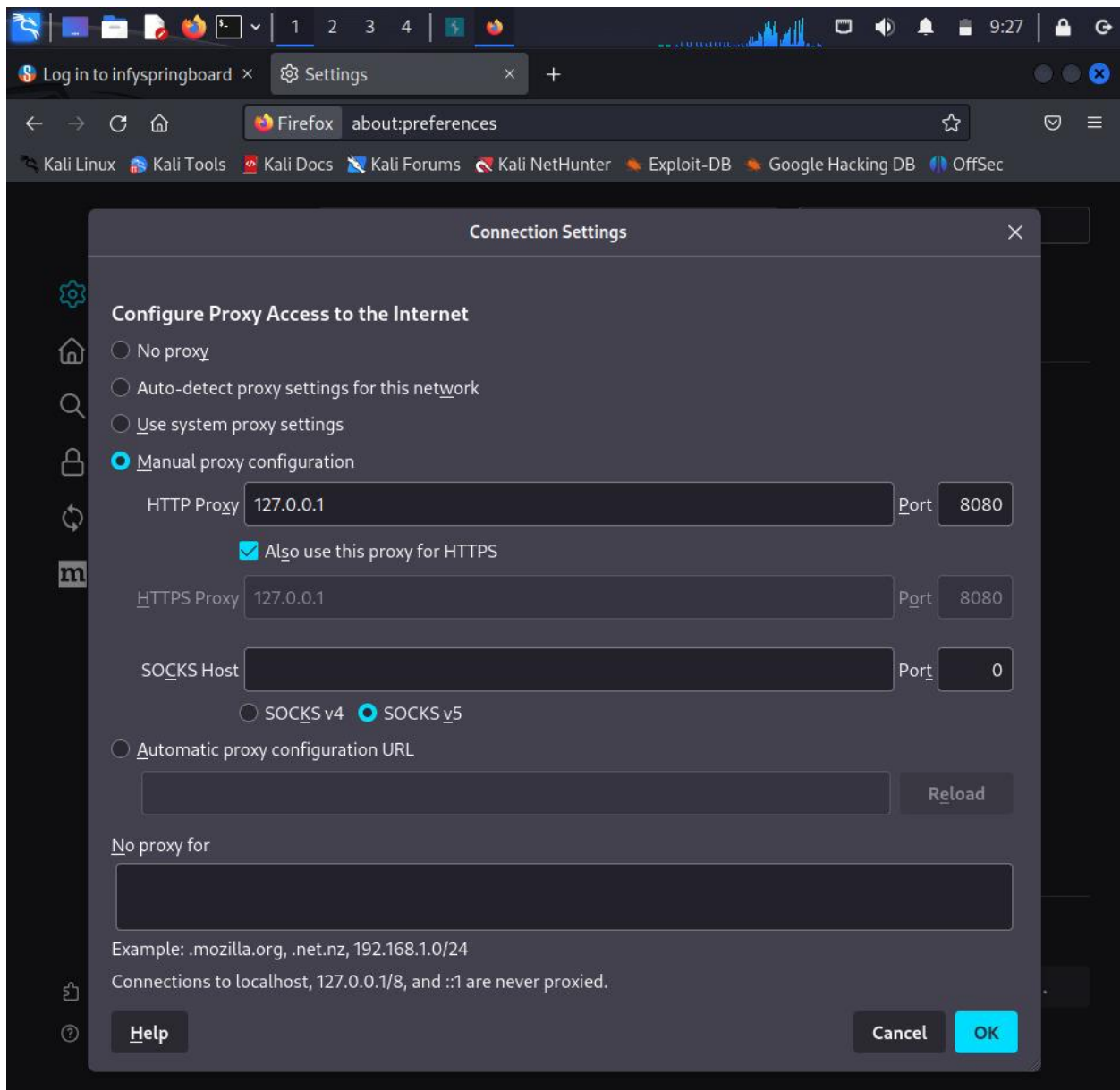


# Report on Web Application Server Hacking

## 1. Configuring of Brup Suites in the Firefox Browser: -

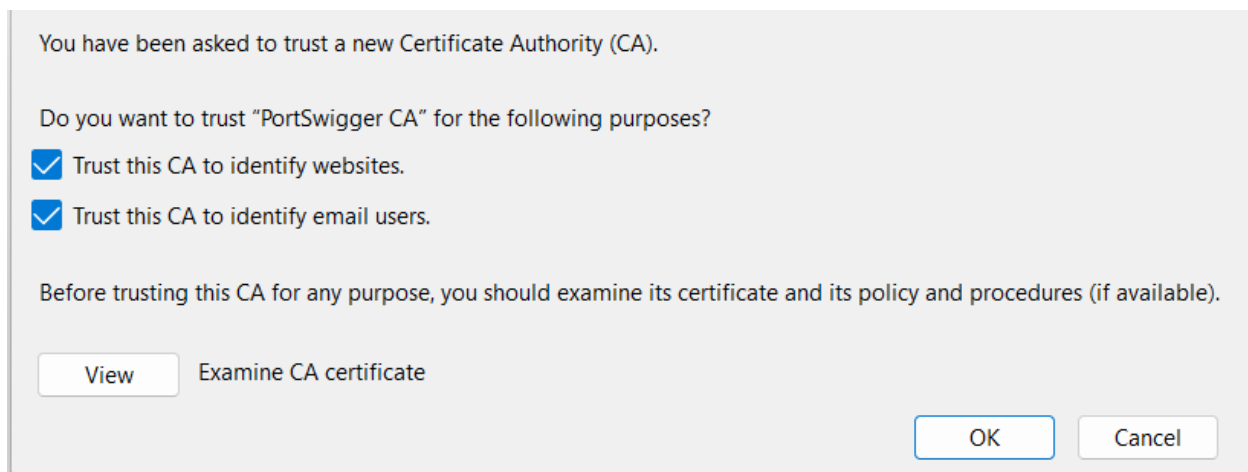
- Open Brup suits Application in Kali and make sure that it is running in localhost at Port number 8080.
- Go to Firefox setting, open Network setting and set Proxy server as 127.0.0.1 is IP address and port number is 8080.
- Enable the check of use this proxy to all HTTPS requests.



**Fig. Configuring the Brup suits Proxy in Firefox browser**

## 2. Adding of CA certificate into the Firefox Browser: -

- To download the CA certificate type 127.0.0.1:8080 in the search box and download it from there.
- Next, we need to add it into the Firefox browser.
- To add it into Firefox, Open Firefox setting then goto Privacy & Security, Scroll down and click on view certificates, then click on import certificate then select the downloaded certificate and make on all the check boxes.



**Fig. Adding of CA certificate into the Firefox browser**

### 3. Gathering of Information using Brup suits: -

- To get the User's Credentials like User-id and Password, we can find them into the POST type of HTTP method in the Brup Suits target.

#### 1)Website name: -

<https://infyspringboard.onwingspan.com/web/en/login>

The screenshot displays the Burp Suite interface. On the left, the Site map shows a list of domains, with <https://infyspringboard.onwingspan.com> highlighted. The main panel shows a list of HTTP requests. The selected request is a POST to `/auth/realms/infyspringboard.onwingspan.com/2Fweb%2Fen%2Flogin&groups=C0001%3A1`. The Request tab is active, showing the raw request body. The Inspector panel on the right shows the decoded request body, which contains the username and password.

Host	Method	URL	Params	Status code	Length	MIME type
https://infyspringboard.o...	GET	/api-gw/wn-apis/public/i...		200	1955	JSON
https://infyspringboard.o...	POST	/api-gw/wn-apis/public/i...	✓	200	1032	JSON
https://infyspringboard.o...	POST	/auth/realms/infyspringb...	✓	200	10464	HTML
https://infyspringboard.o...	GET	/auth/realms/infyspringb...	✓	200	10994	HTML
https://infyspringboard.o...	GET	/auth/resources/qg9q9/lo...		200	2130	XML
https://infyspringboard.o...	GET	/auth/resources/qg9q9/lo...		200	1220	script
https://infyspringboard.o...	GET	/auth/resources/qg9q9/lo...		200	4774	script
https://infyspringboard.o...	GET	/web/assets/authoring/cs...		200	59358	script
https://infyspringboard.o...	GET	/web/assets/icons/fb-wh...		200	4260	XML
https://infyspringboard.o...	GET	/web/assets/icons/qooql...		200	4452	XML

**Request**

```
Yfp-m0UqTtPriJEquzwMID/WzCvEQ; UptanonConsent=
isGpcEnabled=0&datestamp=Mon+Aug+28+2023+09%3A20%
3A56+GMT-0400+(Eastern+Daylight+Time)&version=202
308.1.0&browserGpcFlag=0&isIABGlobal=false&hosts=
&landingPath=https%3A%2F%2Finfyspringboard.onwing
span.com%2Fweb%2Fen%2Flogin&groups=C0001%3A1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 207
10 Origin: null
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16 Te: trailers
17
18 country_phone_code=%2B91&email-placeholder-text=
Enter+your+registered+email+id&
phone-placeholder-text=
Enter+your+registered+10+digit+mobile+number&
username=abdc%40gmail.com&password=Abcd%401234&
credentialId=
```

**Inspector**

Selection: 46 (0x2e)

**Selected text**

```
username=abdc%40gmail.com&password=
Abcd%401234
```

**Decoded from:** URL encoding

```
username=abdc@gmail.com&password=
Abcd1234
```

Request attributes: 2  
Request query parameters: 4  
Request body parameters: 6  
Request cookies: 4  
Request headers: 21  
Response headers: 17

**Fig. Information gathered which was entered by the user into the web page during the Log-in**

## 2)Website name: -

<https://www.tcsion.com/dotcom/TCSSMB/Login/login.html>

The screenshot displays the Burp Suite interface. The 'History' tab is active, showing a list of intercepted HTTP requests. The selected request is a POST to `/SMBPortal/Login` with a status code of 302. The 'Request' tab is expanded, showing the raw HTTP request details. The 'Inspector' tab on the right shows the selected text: `accountname=atoz%40gmail.com&password=Atoz%401576`.

Host	Method	URL	Params	Status code	Length	MIME type
https://www.tcsion.com	GET	/iONjsLib/js/jquery-3.6.0...		200	90150	script
https://www.tcsion.com	GET	/iONjsLib/js/jquery-3.6.0...		200	90150	script
https://www.tcsion.com	GET	/iONjsLib/js/jquery-migr...		200	19088	script
https://www.tcsion.com	POST	/SMBPortal/Login		302	1323	
https://www.tcsion.com	GET	/ConsentManagement/js/...				
https://www.tcsion.com	GET	/ConsentManagement/js/...				
https://www.tcsion.com	GET	/ConsentManagement/js/...				
https://www.tcsion.com	GET	/PasswordPolicy/forget_p...				
https://www.tcsion.com	GET	/PasswordPolicy/forget_p...				
https://www.tcsion.com	GET	/SMBPortal/FaceUnlock				

```
1 POST /SMBPortal/Login HTTP/1.1
2 Host: www.tcsion.com
3 Cookie: ifc@#13_9517=true; iocc@#13_9517=true
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 88
10 Origin: https://www.tcsion.com
11 Referer: https://www.tcsion.com/SelfServices/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 accountname=atoz%40gmail.com&password=Atoz%401576&loginType=5&remember_Me=0&device=login
```

**Inspector**

Selection: 49 (0x31)

**Selected text**

```
accountname=atoz%40gmail.com&password=Atoz%401576
```

**Decoded from:** URL encoding

```
accountname=atoz@gmail.com&password=Atoz@1576
```

**Request attributes:** 2

**Request body parameters:** 5

**Request cookies:** 2

**Request headers:** 17

**Response headers:** 20

## 3)Website name: -

<https://erp.gokuluniversity.ac.in>

The screenshot displays the Burp Suite Community Edition v2023.4.3 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar contains buttons for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, and Settings. The 'Target' tab is active, showing a site map on the left with a list of URLs, including <https://erp.gokuluniversity.ac.in>. The main panel shows a table of HTTP history with columns for Method, URL, Params, Status code, Length, MIME type, and Title. A POST request to `/Account/LoginAuthentication` is highlighted. Below the table, the 'Request' tab is selected, showing the raw request details. The request is a POST to `/Account/LoginAuthentication` with a `Cookie` containing `ASP.NET_SessionId=bcumt50mfxcgj4aimkhnn2425;` and a `__RequestVerificationToken=nYKghIXrRbFNpqCRQpBCAoKMwPmM1ZcussX4DToXiVnsDW-EmHXpMF6MiAyVJCY10RhEsT51Zq_D1DG5w4Uq07owotZvBRpkSSKN4aZPFtk1`. The request body contains the parameters `UserName=Atoz%40gmail.com&Password=Atox%401546`. The 'Inspector' panel on the right shows the selected text `UserName=Atoz%40gmail.com&Password=Atox%401546` and the decoded text `UserName=Atoz@gmail.com&Password=Atox@1546`.

Method	URL	Params	Status code	Length	MIME type	Title
GET	/		200	17716	HTML	Login
POST	/Account/LoginAuthentication		200	386	JSON	
GET	/Content/img/login-page...		200	17766	HTML	remotely
GET	/Scripts/Vendors/jquery.n...		200	3742	script	
GET	/Scripts/js/jquery-1.10.2...		200	93467	script	
GET	/Account/CheckWebLogin					
GET	/Account/CheckWebLogin...					
GET	/Account/GetQRCodeIma...					
GET	/Account/LoginAuthentic...					
GET	/Account/WebLogin					

```
1 POST /Account/LoginAuthentication HTTP/2
2 Host: erp.gokuluniversity.ac.in
3 Cookie: ASP.NET_SessionId=
  bcumt50mfxcgj4aimkhnn2425;
  __RequestVerificationToken=
  nYKghIXrRbFNpqCRQpBCAoKMwPmM1ZcussX4DToXiVnsDW-Em
  HXpMF6MiAyVJCY10RhEsT51Zq_D1DG5w4Uq07owotZvBRpkSS
  KN4aZPFtk1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded;
  charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 46
11 Origin: https://erp.gokuluniversity.ac.in
12 Referer: https://erp.gokuluniversity.ac.in/
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17
18 UserName=Atoz%40gmail.com&Password=Atox%401546
```

Inspector

Selection: 46 (0x2e)

Selected text

UserName=Atoz%40gmail.com&Password=Atox%401546

Decoded from: URL encoding

UserName=Atoz@gmail.com&Password=Atox@1546

Request attributes: 2

Request body parameters: 2

Request cookies: 2

Request headers: 19

Response headers: 10