Information Disclosure at PayPal and Xoom (PayPal Acquisition) via Simple Google Dork - 1,000 USD

YoKo Kho Follow
Sep 23 · 8 min read

بسم الله الرحمن الرحيم

> *(This is a 2017 article that has been released at my personal blog).*

. . .

I. ABSTRACT

We can't deny if one of the biggest dream for everyone that has so many contents at their site is to be indexed at top search engine in the world. In reality, we should realize that even the search engine could help us to "promote" our contents to public, the search engine itself could "betrayed" the site owner to leakage the information if those site owners doesn't setup the blocking rules properly.

This kind of mindset was coming out with a good fact by the research that has been conducted by Ateeq Khan. At November 2013, he has shown the interesting vulnerability (Critical Information Disclosure) that exist at Microsoft Yammer product by using the main function of the search engine. With the "leakage" of token that has been indexed "accidentally" by search engine, then the Attacker at that time could use those information to login to the related account.

As we could see from the two side of function from search engine, in this simple paper, we also would like to talk about the same vulnerability (that Ateeq Khan found on 2013) at another big company, which is PayPal. The problem exists when PayPal and Xoom (PayPal Acquisition) didn't setup the blocking rules properly to prevent the search engine to index the list of

emails and few lists of transaction purpose that used by their users at their application. By using the simple dork (at Google or other), then we could easily enumerate those information.

. . .

II. INTRODUCTION

In its implementation, PayPal has configuring the users' transaction to be send via GET Method of the secure HTTP transmission. Please kindly note, **there is nothing wrong with the method**. With so many customer that doing so many transaction around the world, then the possibility of search engine to index the site is become higher if the site doesn't setup the blocking rules properly.

Commonly, the blocking rules could be setup easily by write some "disallow" rules at robots.txt file.

Figure 1 Common Blocking Rules — via Robots.txt

As seen from the sample structure above, that rules will be very effective for preventing the search engine to index the content inside those directories. But when everything was process in the URL just like PayPal do, then it will become another point of view.

Figure 2 Sample of Decoded Request at One of Transaction at PayPal

As we could see from the sample picture above, without the proper setup of the search engine blocking, then the Attacker could try to enumerate the list of information at via search engine.

Please kindly note: (as far as my understanding) commonly, for preventing the search engine to index this type of request, the developer should use the **noindex** meta tag in the page. Google at its documentation has telling the other way to prevent the search engine to index this kind of method.

Figure 3 Block search indexing with 'noindex'

Also HubSpot from one of their article has telling the two effective ways to preventing the search engine to index our content that could be sensitive or not useful.

. . .

2.1. PayPal's Transaction Parameter at HTTP Request

When user would like to send some some money to other account, then normally PayPal will send several requests to server with GET method such as: recipient, onboardData, sendMoney, currencyCode, payment_type, sendMoneyText, or intent.

For example, here is the list of the complete request that send by a user when they would like to send a money:

```
(GET Method): https://www.paypal.com/signin/?
country.x=US&locale.x=en-
US&returnUri=https://www.paypal.com/myaccount/transfer/send/external?
recipient=
```

```
(victim_email_address)&amount=1000.00&currencyCode=USD&payment_type=G
ift&onboardData={"intent":"sendMoney","recipient":"
(victim_email_address)","currency":"$","amount":"1000.00","redirect_u
rl":"https://www.paypal.com/myaccount/transfer/send/external?
recipient=
(victim_email_address)&amount=1000.00&currencyCode=USD&payment_type=G
ift","flow":"p2p","country":"US","locale":"en-
US","sendMoneyText":"Custom message, for example is sending a money
to victim_email_address”}
```

Table 1 Sample of the Complete Request

As stated earlier, with the used of all parameters, then we could try to enumerate the transaction that ever been made by registered user.

. . .

2.2. Xoom’s Issue Related Information Disclosure

This one is a little different with PayPal. At the time when we do a research with this kind of tricks, we don’t get any information except the email address. At the first time, we have thought if that information will not be considered as vulnerability in the PayPal point of view. But when we find out if Xoom has implementing the unique method to prevent the user

enumeration at their portal, then we decided to report this issue to PayPal too (and yes, they acknowledged the report as a valid issue).

. . .

2.2.1. Xoom's User Enumeration Prevention Concept

When we try to register our account at Xoom for the first time, Xoom will proceed the registration normally and send the verification request to the related users. But the unique things happen when the user/attacker try to **register the exist account at application**, then Xoom still **process the registration normally** just like the process of registration when the user doesn't exist at the system.

At the other side, Xoom send the warning email to the registered account that was used by the Attacker to register again.

For a simple explanation, in other words, registered or not, Xoom still process the registration normally without showing the error if the account is exist already. But at the backend, Xoom has different way to differentiate between the registered or unregister account.

Figure 4 Registering with the Registered Email Account — Protecting the Enumeration

So by learning this flow, then **if we could enumerate the user ID**, then **it will be a flaw**.

. . .

2.2.2. Xoom's Referrer Parameter

One of the biggest question that came to our mind is how we could enumerate the list of users at Xoom. Finally, the answer come with the show of referrer feature.

Referrer is one of the feature that generally used by public company to increasing the used of its service. In usual situation, this referrer link always provided with the interesting promotion that could be used by the receiver. In the reality, Xoom also has this unique feature (found at: https://www.xoom.com/xoom-refer-a-friend-program) that could be used by their registered user to get the "$20 Amazon eGift card" for every first transfer of new user that has a value of $400 or more (transaction fee excluded).

And just like the things that we described earlier, the missing blocking rules protection at this feature could allow the Attacker to enumerate the list of registered users at the search engine.

. . .

III. SUMMARY OF ISSUE

As it has been described before, the security problem in this report is related way to enumerating some of information (information disclosure) via search engine. The problem exists because PayPal didn't implement the proper blocking rules yet.

. . .

IV. PROOF OF CONCEPT

The proof of concept related this one is very extremely easy. We just need a simple Google Dork to find out the list of some information that ever exist when the service was used by its user.

. . .

4.1. Enumerating the List of Email Address at Xoom

The proof of concept related this one is very extremely easy. We just need a simple Google Dork to find out the list of registered users (at Xoom) that ever used this service. And here are the lists of Google Dork that could be used to find out the registered users:

```
· site:xoom.com inurl:'@gmail.com'
· site:xoom.com inurl:'@yahoo.com'
· site:xoom.com inurl:'@hotmail.com'
· site:xoom.com inurl:'@msn.com'
· site:xoom.com inurl:'e=' 'refer'
· site:xoom.com inurl:'tellapal.id'
```

Please kindly note:

- we could change the @yahoo.com, etc to other domain that has an email service.
- Also, the list of information disclosure could be detected by other feature too, such as send-money (not only at the referrer feature).

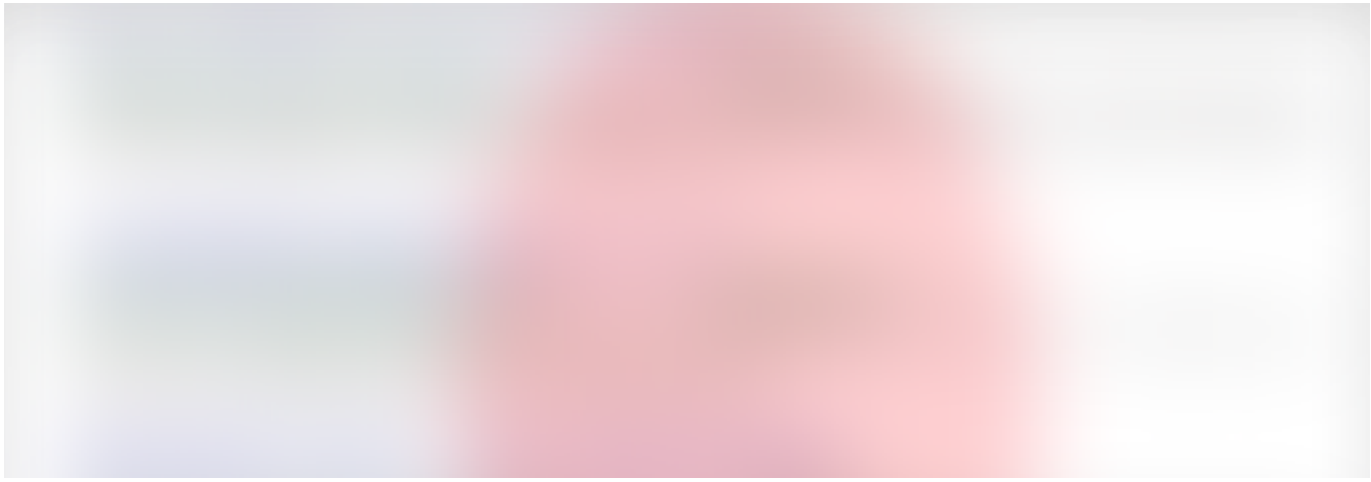


Figure 5 Information Disclosure via Search Engine — Referrer Feature

Figure 6 Information Disclosure via Search Engine — Send Money Feature

. . .

4.2. Enumerating the List of Some Information at PayPal

Just like the previous one, here are the lists of Google Dork that could be used to find out some of information:

```
· site:paypal.com inurl:'payment_type='
· site:paypal.com inurl:intent
· site:paypal.com inurl:'sendMoneyText'
· site:paypal.com inurl:'recipient='
· site:paypal.com inurl:currencyCode=
· site:paypal.com inurl:onboardData=
· site:paypal.com inurl:sendMoney
· site:paypal.com inurl:item_name
· site:paypal.com inurl:counterparty
```

Figure 7 Information Disclosure at PayPal — sendMoneyText Parameter

Figure 8 Information Disclosure at PayPal — payerView Parameter

Figure 9 Information Disclosure at PayPal — em Parameter

And in another situation, we could find out the valid customer invoice that accidentally post on public area (internet):

Figure 10 Sample of Valid Customer Invoice

. . .

V. RECOMMENDATION

The detail explanation has been explained by Google to preventing this issue to be happened. As an information, this detail could be found at the article of "Block search indexing with 'noindex'".

. . .

VI. ADDITIONAL INFORMATION

For completing the explanation, we upload the unlisted video at Youtube for both of scenario:

6.1. Information Disclosure at PayPal: https://youtu.be/N4owd36BNJY

6.2. Information Disclosure at Xoom: https://youtu.be/1cwwcFeJge8

. . .

VII. LESSON LEARNED

7.1. From the case of Xoom: always try to find a way to triggering your finding into the valid one by looking its procedure or flow of the application. Even in some case this one is not a valid security issue, then its worth to try (especially if no point will be reduced even the issue isn't valid).

7.2. And yes, one of the very useful lesson to be learned is please spare our time to read any research that conduct by another researcher. As an information, this research was inspired by the research that conducted by Ateeq Khan related the Critical Information Disclosure that exist at Microsoft Yammer product.

The detail could be found at: https://www.vulnerability-lab.com/get_content.php?id=1003

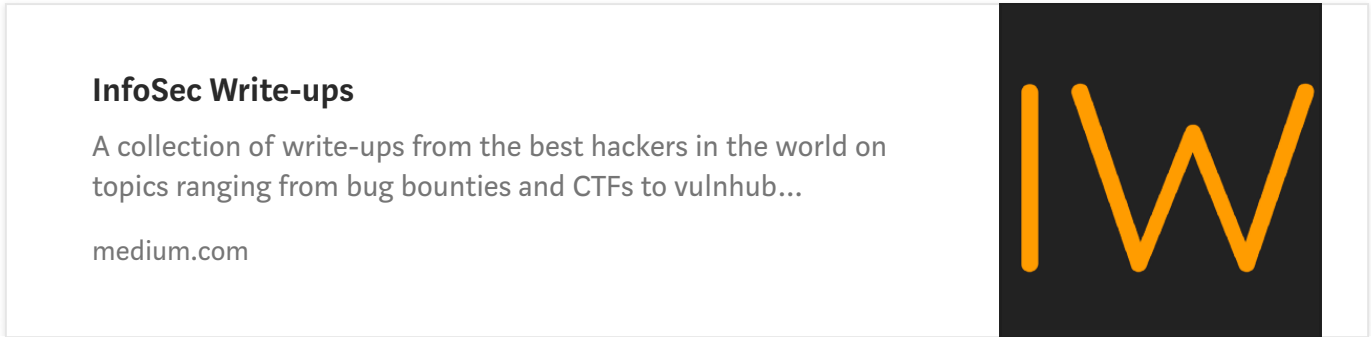
. . .

VIII. ADDITIONAL NOTE

- The **initial bounty** was sent on: July 13th, 2017 (Xoom Domain) and August 25th, 2017 (PayPal Domain)—with total of 500 USD.
- The **final bounty** was sent on: August 25th, 2017 (Xoom Domain) and December 6th, 2017 (PayPal Domain)—with total of 500 USD again.

. . .

Follow Infosec Write-ups for more such awesome write-ups.



153 claps

WRITTEN BY

YoKo Kho

Follow

Bug Hunter | OSCP | One of 2018 BugCrowd MVP | https://twitter.com/YoKoAcc | https://bugcrowd.com/YokoKho

InfoSec Write-ups

Follow

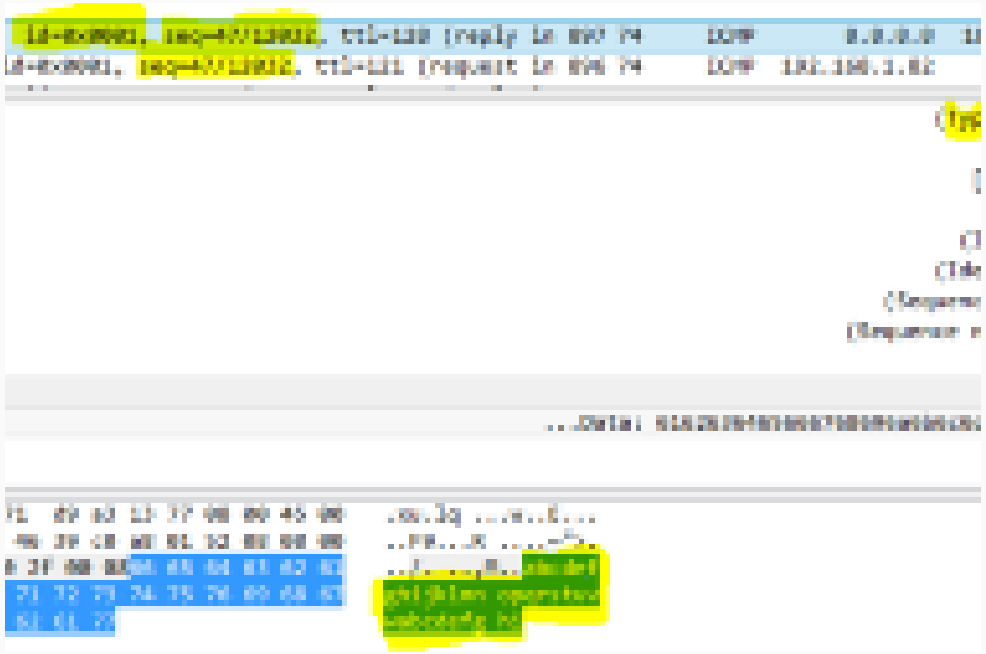
A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Powered by Hackrew

Write the first response

More From Medium

More from InfoSec Write-ups

Ping Power — ICMP Tunnel



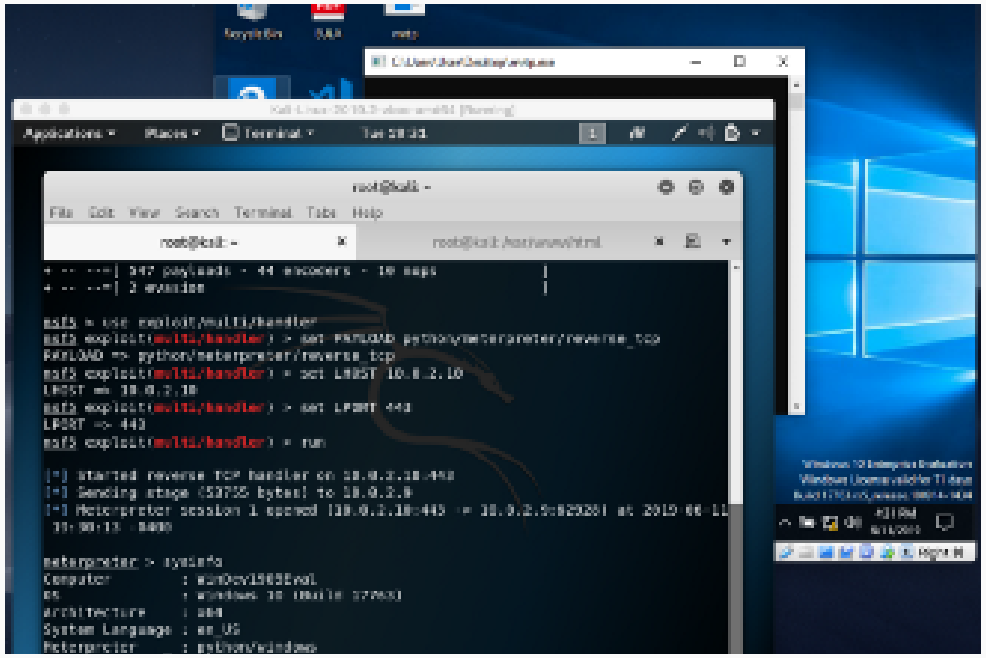
Nir Chako in InfoSec Write-ups
Dec 17, 2018 · 8 min read

1.1K

More from InfoSec Write-ups

Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups
Aug 16 · 16 min read ★



More from InfoSec Write-ups

Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups
Jun 11 · 6 min read ★