

Forum:[Hack Forums](#)

Thread: [Found Sql injection in a online casino](#)

21redallday12 - January 14, 2014, 9:36 pm

So just thought i would share this sql injection technique.

MY AIM WAS TO SEE IF I COULD, AND TO REPORT IT IN HOPE FOR A REWARD.

I decided find a vulnerability in a online casino[A major player in uk], So i started off by finding out how online casino's are regulated, and it turns out that they are regulated by the gambling commision. On there website [www.gamblingcommission.gov.uk/?] there is a list of every single LEGAL gambling sites. Next i looked for one that used older software, and gernrally older software.

I found 3 sutible targets, next i manually scanned the websites for vulnerability's didn't find much apart from a few sensitive directories & XSS. [Tested cookies,refferers, user-agents the whole shabang(english term)]

So i decided to download the casino program, which is an .exe executable. I am not very familiar with decompiling/reverse engineering, but my first attempt was to try and decompile the code so i can find out what is going on server side. Did not work, i assume it was written in a lower level langauge. I have decompiled/revesed .net and flash files before, and i thought it was possible to decompile, obviously not. (decompiling is not my area)

Next, bridged my to laptops together and started listening on wireshark on one laptop, whilst i installed the program on the other(due to OS complications one laptops windows, the other ubuntu)

I was watching the the packets/requests whilst it was installing (Mainly looking for HTTP GET/POST data), and sure enough the requests started to flow. At first it was simply grabing images from the server EG -

```
GET /sensitive-directory/images/casino.jpg HTTP /1.1
GET /sensitive-directory/images/logo.jpg HTTP /1.1
etc
```

Then i noticed one requests, which was to a script , which contianed a GET parameter named something like user_id=879888

```
GET /sensitive-directory/command.asp?user_id=241241&rando=4342424&type=new HTTP /1.1
```

(another thing i forgot to mention, the casino.exe program has its one user-agent, so if you tried it directly from your browser without tampering your useragent it would simply not work, i think it replied with an odder http response code)

Next, i opened up firefox + local proxy chaged my request to the same user-agent as the program eg FakeCansionName Version 1.35[]. Tested the parameter with the single quote and open sesimi. Microsoft SQL Sever Syntax error/ or unclosed quote, carn't remember.

Then i did a quick few tests eg AND 1=1, 1=0, Sleep delay etc, ; sleep -- . and its vulnerable!
--BTESU :

PS for anybody trying to find vulnerabilities on servers using this technique, I would probably stick to testing HTTP if your new to this. You might get confused with the encrypted APP-DATA, etc.

The APP-DATA using a very strong encryption and you will need the private key to decrypt. HTTP is obviously unencrypted so its easy to test, even for amateurs.

I have found a similar vulnerability, in a flash program before by downloading the flash file, decompiling [which is very very simple], then look for GET/POST and other sensitive information.

If you find any .net apps, then you can actually decompile and properly understand the code rather than going blind like i did.

Just thought i would share this with you as i don't see these kind of unorthodox methods on here.

PS my spellings a mess its late and i can't be bothered to be grammatically correct :)
[I have reported the vulnerability, and thats why i am posting it openly]

I'm not a white hat, and i'm not a black hat, hats just don't suite me.

21redallday12

on-silo - January 14, 2014, 11:58 pm

(Jan 14, 2014 10:36 PM)21redallday12 Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#) So just thought i would share this sql injection technique.

MY AIM WAS TO SEE IF I COULD, AND TO REPORT IT IN HOPE FOR A REWARD.

I decided find a vulnerability in a online casino[A major player in uk], So i started off by finding out how online casino's are regulated, and it turns out that they are regulated by the gambling commission. On there website [\[www.gamblingcommission.gov.uk/?\]](http://www.gamblingcommission.gov.uk/) there is a list of every single LEGAL gambling sites. Next i looked for one that used older software, and generally older software.

I found 3 suitable targets, next i manually scanned the websites for vulnerabilities didn't find much apart from a few sensitive directories & XSS. [Tested cookies, referers, user-agents the whole shabang(english term)]

So i decided to download the casino program, which is an .exe executable. I am not very familiar with decompiling/reverse engineering, but my first attempt was to try and decompile the code so i can find out what is going on server side. Did not work, i assume it was written in a lower level language. I have decompiled/reversed .net and flash files before, and i thought it was possible to decompile, obviously not. (decompiling is not my area)

Next, bridged my two laptops together and started listening on Wireshark on one laptop, whilst i installed the program on the other(due to OS complications one laptop windows, the other ubuntu)

I was watching the the packets/requests whilst it was installing (Mainly looking for HTTP GET/POST data), and sure enough the requests started to flow. At first it was simply grabbing images from the server EG -

```
GET /sensitive-directory/images/casino.jpg HTTP /1.1
GET /sensitive-directory/images/logo.jpg HTTP /1.1
etc
```

Then i noticed one request, which was to a script, which contained a GET parameter named something like user_id=879888

GET /sensitive-directory/command.asp?user_id=241241&rando=4342424&type=new HTTP /1.1

(another thing i forgot to mention, the casino.exe program has its one user-agent, so if you tried it directly from your browser without tampering your useragent it would simply not work, i think it replied with an odder http response code)

Next, i opened up firefox + local proxy chaged my request to the same user-agent as the program eg FakeCansionName Version 1.35[]. Tested the parameter with the single quote and open sesimi. Microsoft SQL Sever Syntax error/ or unclosed quote, carn't remember.

Then i did a quick few tests eg AND 1=1, 1=0, Sleep delay etc, ; sleep -- . and its vulnerable! --BTESU :

PS for anybody trying to find vulnerablites on servers using this techinque, I would probably stick to testing HTTP if your new to this. You might get confisude with the encrypyted APP-DATA, etc. The APP-DATA using a very stong encryption and you will need the private key to decrypt. HTTP is obvously unencrypted so its easy to test, even for amauters.

I have found a similar vulnerablity, in a flash program before by downloaded the flash file, decompiling [which is very very simple], then look for GET/POST and other sensitive infromation.

If you find any .net apps, then you can acctually decompile and properly understand the code rather then going blind like i did.

Just thought i would share this with you as i don't see these kind of unotherdox methods on here.

PS my spellings a mess its, late and a carn't be botherd to be grammaticaly correct :)
[I have reported the vulnerablity, and thats why i am posting it openly]

I'm not a white hat, and i'm not a black hat, hat's just don't suite me.

21redallday12

I wish people did well worded and understandable write-ups like this more often, kudos

g0han - January 14, 2014, 11:59 pm

On my phone so that's a lot of text to read, I'll read on my computer later :L

Grim - January 15, 2014, 12:00 am

very nice man! very few HQ people like this on here

21redallday12 - January 15, 2014, 12:24 am

(Jan 15, 2014 12:58 AM)cryotic Wrote: [\[CITE\]](#) I wish people did well worded and understandable write-ups like this more often, kudos
Thanks bro.

(Jan 15, 2014 01:00 AM)Preditor Wrote: [\[CITE\]](#) very nice man! very few HQ people like this on here
Thanks, good to hear nice feedback.

rDNix - January 15, 2014, 12:32 am

Awesome this is how you work when you put target on your mind .. am really like how you are thinking , thank you .

Avocado - January 15, 2014, 3:35 am

I like these sorts of posts in this section, breath of fresh of here. Thank you, an interesting read for sure.

Jack Daniels™ - January 15, 2014, 3:39 am

I'd love to learn stuff like this.. How did you first learn? Pretty interesting to read too.

21redallday12 - January 31, 2014, 7:04 pm

(Jan 15, 2014 01:32 AM)rDNix Wrote: [\[CITE\]](#) Awesome this is how you work when you put target on your mind .. am really like how you are thinking , thank you .

Thanks, i really appreciate it.

(Jan 15, 2014 04:35 AM)Avocado Wrote: [\[CITE\]](#) I like these sorts of posts in this section, breath of fresh of here. Thank you, an interesting read for sure.

Thanks, i enjoy adding different concepts to this section.

(Jan 15, 2014 04:39 AM)Omegle Wrote: [\[CITE\]](#) I'd love to learn stuff like this.. How did you first learn? Pretty interesting to read too.

I think its quite simple and logical, when you think about it. I was writing a program in python and then wondered how to connect to a database when i realised application connect to dbs.

Thanks again

-- -- ---

By the way this method works against flash aswell, decompiling flash/swf is very very simple then just look for get/post variables etc.

aksh1008 - September 25, 2019, 10:33 pm

dm me we can work together

karsina - September 26, 2019, 4:32 am

from 2014 bro :D

i think too late

Big Cash Spender - September 26, 2019, 6:46 am

(Sep 25, 2019 10:33 PM)aksh1008 Wrote: [\[CITE\]](#) dm me we can work together
Gravedigger!

0x3043 - September 26, 2019, 7:17 am

It is a 5 year old post dude, gravedigging af !!