

Forum:[Hack Forums](#)

Thread: [\\$300 in 15 minutes](#)

Mr. Corleone - January 2, 2023, 4:42 am

Found an open redirect in Epicgames.

I tried escalating the severity by trying a few things like chaining it to the oauth redirect, but they secured that tightly since that's a common thing to look for nowadays.

I find it funny how the most active programs still have low hanging fruit. Just gotta approach it from a different angle.

siddy357 - January 2, 2023, 4:48 am

I understood nothing from above. Can you rinse and repeat the same thing again then good for you for finding a bug

Molegrips - January 2, 2023, 5:21 am

Well done, was this relatively hard to do? or was it all with free tools?

Mr. Corleone - January 2, 2023, 3:03 pm

(Jan 2, 2023 05:48 AM)siddy357 Wrote: [\[CITE\]](#) I understood nothing from above. Can you rinse and repeat the same thing again then good for you for finding a bug

My bad, I didn't explain it in a way that everyone would understand.

I can't really rinse and repeat the same bug in this manner, since every website is different.

(Jan 2, 2023 06:21 AM)Molegrips Wrote: [\[CITE\]](#) Well done, was this relatively hard to do? or was it all with free tools?

This bug was very easy. Done with free tools.

Even if you have no background in IT, open-redirects are easy to understand within 2 minutes.

Duke190 - January 2, 2023, 3:17 pm

I wish I could understand the nonsense.

ailo - January 2, 2023, 3:20 pm

well done im trying to get into this as well seems lucrative.

Mr. Corleone - January 2, 2023, 3:37 pm

(Jan 2, 2023 04:20 PM)ailo Wrote: [\[CITE\]](#) well done im trying to get into this as well seems lucrative. Don't.

Most low hanging fruits are easily found by others already.
Thousands of people automating scripts and such to find them.

It takes too much time to learn and actually finding bugs.

The people who you see getting 10k+ bugs usually spend months just reading code from a single application and understand how it works inside out, to the point they understand it better than the developers in many cases.

Unless you're really fanatic about it or already have a lot of programming/web security experience, don't bother.

PhireTalker - January 3, 2023, 8:56 am

I have to agree, the learning curve to bug hunting has you constantly learning the process without actually hunting for bugs. By the time you actually know how to hunt for bugs, there's an uphill battle to keep learning for the most current bugs since the bugs you learned about has already been found.

web0m - January 4, 2023, 10:05 am

Nice one, really surprising that you were able to find something that simple.
Also, a lot of these programs open redirects are excluded.

The chances of you finding an open redirect that potentially thousands of people already looked for, and they also pay for open redirects, are super slim.

You should buy a lotto coupon

ihysmhf - January 4, 2023, 5:58 pm

Well done lmao. Way over my head but well done.

Mr. Corleone - January 5, 2023, 6:19 am

(Jan 4, 2023 11:05 AM)t0xi Wrote: [\[CITE\]](#) Nice one, really surprising that you were able to find something that simple.

Also, a lot of these programs open redirects are excluded.

The chances of you finding an open redirect that potentially thousands of people already looked for, and they also pay for open redirects, are super slim.

You should buy a lotto coupon

I found the unvalidated redirect on an out of scope domain.
Chained it to a validated redirect on an in-scope domain.

Hence why no one found it before me. But indeed, open redirects are extremely rare on a program of this size.

web0m - January 5, 2023, 6:20 am

(Jan 5, 2023 07:19 AM)Mr. Corleone Wrote: [\[CITE\]](#) I found the unvalidated redirect on an out of scope domain.

Chained it to a validated redirect on an in-scope domain.

Hence why no one found it before me. But indeed, open redirects are extremely rare on a program of this size.

Impressive that they still would pay you, when it's out of scope.
Nice find anyways!

The Pact - January 6, 2023, 10:22 pm

(Jan 2, 2023 04:03 PM)Mr. Corleone Wrote: [\[CITE\]](#) My bad, I didn't explain it in a way that everyone would understand.

I can't really rinse and repeat the same bug in this manner, since every website is different.

This bug was very easy. Done with free tools.

Even if you have no background in IT, open-redirects are easy to understand within 2 minutes.

So was this like White Hat. So Epic Games offers a bounty if you find a bug? Please excuse my ignorance if I'm getting it all wrong.

Mr. Corleone - January 7, 2023, 4:09 am

(Jan 6, 2023 11:22 PM)The Pact Wrote: [\[CITE\]](#) So was this like White Hat. So Epic Games offers a bounty if you find a bug? Please excuse my ignorance if I'm getting it all wrong.

Yup! That's exactly right. You're allowed to test epic games in-scope assets.

It's okay, not many people heard of bug bounties outside the IT-world.

The Pact - January 7, 2023, 4:26 am

(Jan 7, 2023 05:09 AM)Mr. Corleone Wrote: [\[CITE\]](#) Yup! That's exactly right. You're allowed to test epic games in-scope assets.

It's okay, not many people heard of bug bounties outside the IT-world.

HaHa I'm not and have never been in IT at all so I expect to be dumb around here but I guess I figured it out from being on HF long enough.

sammig - January 9, 2023, 2:42 pm

NoW seriously i ready bout this ewhores. Your rent the eprson and they have little Toy

CPA AND VIEWS

The Pact - January 9, 2023, 7:03 pm

(Jan 9, 2023 03:42 PM)sammig Wrote: [\[CITE\]](#) NoW seriously i ready bout this ewhores. Your rent the eprson and they have little Toy

CPA AND VIEWS

This isn't a thread about ewhores at all. Don't talk nonsense. Go read the help documents!

cicadamikoto - January 9, 2023, 10:07 pm

What's your enumeration methodology?

I once got \$10k in 25 seconds on a code review on a private bounty. Unbounded printf everywhere in a C codebase. Hilarious stuff.

Black Swan - January 15, 2023, 11:02 pm

Epic! Nice find any tips to finding stuff like this?

Mr. Corleone - January 16, 2023, 2:38 am

(Jan 16, 2023 12:02 AM)CodingY Wrote: [\[CITE\]](#) Epic! Nice find any tips to finding stuff like this? Yes.

If you find a redirection that's protected (i.e. you can redirect to 'trusted' wensites), then find an open redirect on these 'trusted' websites, even if they are out of scope.

If you can chain an out of scope to the in-scope domain to make it work, they'll most likely pay you.

I say most likely because some companies might not pay you for it.

But in general, big companies like epicgames will pay you.

Black Swan - January 16, 2023, 10:12 am

(Jan 16, 2023 03:38 AM)Mr. Corleone Wrote: [\[CITE\]](#) Yes.

If you find a redirection that's protected (i.e. you can redirect to 'trusted' wensites),

then find an open redirect on these 'trusted' websites, even if they are out of scope.

If you can chain an out of scope to the in-scope domain to make it work, they'll most likely pay you.

I say most likely because some companies might not pay you for it.

But in general, big companies like epicgames will pay you.

Thanks for the advice; for sure would probably only work with big companies, as smaller fish don't usually want to pay out on that type of thing. Were you using any automated tools to find endpoints, or was it just a huh, this looks insecure moment?

Mr. Corleone - January 16, 2023, 4:49 pm

(Jan 16, 2023 11:12 AM)CodingY Wrote: [\[CITE\]](#) Thanks for the advice; for sure would probably only work with big companies, as smaller fish don't usually want to pay out on that type of thing. Were you using any automated tools to find endpoints, or was it just a huh, this looks insecure moment?

Manually browsing with Burpsuite on.

In burpsuite i literally searched for 'redirect_to' 'returnUrl' etc.

incomeFor500 - March 1, 2023, 4:09 am

(Jan 2, 2023 05:42 AM)Mr. Corleone Wrote: [\[CITE\]](#)

Found an open redirect in Epicgames.

I tried escalating the severity by trying a few things like chaining it to the oauth redirect, but they secured that tightly since

that's a common thing to look for nowadays.

I find it funny how the most active programs still have low hanging fruit. Just gotta aproach it from a different angle.

I can respect this bro unlike most of these virtual pimps on here lmao

xaphy12 - March 26, 2023, 12:54 pm

Well done, was this relatively hard to do? or was it all with free tools?