

Forum:[Hack Forums](#)

Thread: [Best and Worst Bug Bounty Experiences?](#)

onlineuser | D3RFER - October 21, 2025, 5:25 pm

About six months ago I found an information-disclosure issue at a big company, but it wasn't serious enough for their hall of fame.

6 months later, I decided to give it another try.

Today I spent six hours scanning subdomains and looking them through.

(1007 subdomains) and found two issues.

IDOR and a client-side authorization bypass by disabling JavaScript in my browser.

I was SO close to an SQL injection but couldn't get it, so I stopped. I decided to relax and watch YouTube, before sleeping.

The first ad that played was from the same company I'd been testing. Yup, felt like salt in the wound.

Palestine - October 21, 2025, 5:47 pm

(Oct 21, 2025 05:25 PM)onlineuser | D3RFER Wrote: [\[CITE\]](#) About six months ago I found an information-disclosure issue at a big company, but it wasn't serious enough for their hall of fame.

6 months later, I decided to give it another try.

Today I spent six hours scanning subdomains and looking them through.

(1007 subdomains) and found two issues.

IDOR and a client-side authorization bypass by disabling JavaScript in my browser.

I was SO close to an SQL injection but couldn't get it, so I stopped. I decided to relax and watch YouTube, before sleeping.

The first ad that played was from the same company I'd been testing. Yup, felt like salt in the wound.

You could make a great career out of doing that for major companies. I know they'd pay a fortune for that kind of work. You should definitely look into it, if I was skilled enough in this field I'd definitely do it.

Jinu - October 21, 2025, 6:40 pm

Damn, that ad at the end is peak irony. Nice persistence. 1007 subdomains is patience of a saint.

PacketPilot - October 21, 2025, 8:25 pm

Best part's when your report gets validated fast. Worst is when they ghost you for months.

onlineuser | D3RFER - October 22, 2025, 4:47 am

(Oct 21, 2025 05:47 PM)Palestine Wrote: [\[CITE\]](#) You could make a great career out of doing that for major companies. I know they'd pay a fortune for that kind of work. You should definitely look into it, if I was skilled enough in this field I'd definitely do it.

Indeed that is very true. I already do this kind of work for multiple companies. But I do not making living of it, I believe there's easier ways to make money tbh.

(Oct 21, 2025 06:40 PM)Jinu Wrote: [\[CITE\]](#) Damn, that ad at the end is peak irony. Nice persistence. 1007 subdomains is patience of a saint.

Thanks. Yeah it took some patience, but basically you scale down from 1,000 subdomains to few hundreds pretty quick.

Using whatever subdomain finder you prefer & afterwards doing live check with httpx. What comes afterwards is the real hunting. When you have to manually look through them all for possible vulnerabilities & dig for possible subdomain takeovers.

Not to long ago, I actually managed to do a subdomain takeover buying an expired LTD & settings up a certificate.

(Oct 21, 2025 08:25 PM)PacketPilot Wrote: [\[CITE\]](#) Best part's when your report gets validated fast. Worst is when they ghost you for months.

Either that or worst part is a duplicate.

Palestine - October 22, 2025, 6:50 am

(Oct 22, 2025 04:47 AM)onlineuser | D3RFER Wrote: [\[CITE\]](#) Indeed that is very true. I already do this kind of work for multiple companies. But I do not making living of it, I believe there's easier ways to make money tbh.

Thanks. Yeah it took some patience, but basically you scale down from 1,000 subdomains to few hundreds pretty quick.

Using whatever subdomain finder you prefer & afterwards doing live check with httpx. What comes afterwards is the real hunting. When you have to manually look through them all for possible vulnerabilities & dig for possible subdomain takeovers.

Not to long ago, I actually managed to do a subdomain takeover buying an expired LTD & settings up a certificate.

Either that or worst part is a duplicate.

Oh yeah if you have better/easier way to make money then keep doing you. Atleast you have a side hustle and even a back up gig incase you need something to fall back on.

sharn - October 26, 2025, 4:42 am

Best is when the team responds in hours.

Being ignored feels terrible.