

Ethical Student Hackers

Bug Bounties



The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.
- Relevant UK Law: <https://www.legislation.gov.uk/ukpga/1990/18/contents>



Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at <https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>



What are Bug Bounties?



Basic Flow

Pick a
Program

Find a
Bug

Write a
Report

Submit

Get
Rewarded

And stay in scope the whole time



A lot of companies, most of them you use on a daily have these bug bounty programs.



...And so on



Platforms

Hackerone

The screenshot shows the Hackerone 'Opportunity Discovery' interface. At the top, it says 'We have 428 opportunities for you'. Below this is a search bar with filters for 'Program type', 'Asset type', and 'Industry'. The main content area is titled 'Campaigns & top-paying opportunities' and displays a grid of four featured programs:

- Goldman Sachs:** Bug Bounty Program, Triaged by HackerOne, Collaboration. Ends in 14 days. Up to \$22k (+1.5 more). 319 assets, 156 bugs, 100% success rate.
- Bitrix:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Gold Standard. Ends in 23 days. Up to \$30k (+2 more). 140 assets, 80 bugs, 97% success rate.
- Marriott Bug Bounty:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 9 days. Up to \$12k (+1.25 more). 184 assets, 106 bugs, 99% success rate.
- Grab:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 7 days. \$50 - \$15k. 740 assets, 256 bugs, 94% success rate.

Below these are 'Collaboration Opportunities' including Conkabo, Iron Fish, SIX Group, and Ero.

Intigriti

The screenshot shows the Intigriti platform interface. At the top, it says 'Have a nice day hunting, primitheus'. Below this is a search bar and a list of programs:

- 100001 - 100008:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- ADD-100017 - ADD-100019:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100018:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100019:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100020:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100021:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100022:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100023:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100024:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100025:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100026:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100027:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100028:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100029:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100030:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100031:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100032:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100033:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100034:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100035:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100036:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100037:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100038:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100039:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100040:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100041:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100042:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100043:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100044:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100045:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100046:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100047:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100048:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100049:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.
- AD-100050:** Bug Bounty Program, Triaged by HackerOne, Retesting, Collaboration. Ends in 14 days. \$50 - \$1.5k.

Among a selection of other platforms such as Bugcrowd



Example of A Bounty

- Lists the Assets such as Domains, Executable, Android APKs etc.
- Reports are split into severity of the bug.
- You can see the “Hacktivity” tab which displays the most recent bug reports. Sometimes they will disclose what was submitted, most of the time they won’t (for obvious reasons)

Epic Games Bug Bounty Program

Triaged by [HackerOne](#), [Retesting](#), [Collaboration](#)

Domain 56 Executable 8
OtherAsset 2 Wildcard 2
iosAppStore 2 AndroidApk 1

\$200 - \$15k

🐞 1k 👤 311 🟢 95%

[See details](#)

Rewards

Low Medium High Critical

\$200 - \$500 \$1,000 - \$3,000 \$5,000 - \$10,000 \$10,000 - \$15,000

Reports are awarded based on severity as determined by the CVSS v3.0 scoring system. The tables above represent the maximum bounty for each severity. The bounty table for in-scope assets is further defined below:

Min/Max	Critical (CVSS 9.0 - 10.0)	High (CVSS 7.0 - 8.9)	Medium (CVSS 4.0 - 6.9)	Low (CVSS 0.0 - 3.9)
Minimum	\$10,000	\$5,000	\$1,000	\$200
Maximum	\$15,000	\$10,000	\$3,000	\$500

All assets running vBulletin, Salesforce, AnswerHub, or other third party services fall under the bounty table which is further defined below:

Min/Max	Critical (CVSS 9.0 - 10.0)	High (CVSS 7.0 - 8.9)	Medium (CVSS 4.0 - 6.9)	Low (CVSS 0.0 - 3.9)
Minimum	\$2,000	\$1,000	\$500	\$200
Maximum	\$5,000	\$2,000	\$1,000	\$500

Game/executable related findings, such as in game bugs, cheats, and exploits will be validated on a case-by-case basis. If your submission is already detected by our anti-cheat systems then it is unlikely to be awarded a bounty

Hacktivity

By [waxx](#) to Epic Games \$2,000.00 closed 5 hrs ago

By [nahuelm_to](#) to Epic Games \$100,000.00 bounty awarded 7 days ago

By [snorthax](#) to Epic Games closed 5 hrs ago



Misconceptions and Mistakes

“There are millions of hackers and they’re all more skilled than me, I’ll never find a bug.”
“These companies are so big, they would’ve plugged up any easy vulnerabilities to find.”

Going for the money

Money is great, but never go for the money.

Build up your skills. Learn and understand the

The vulnerabilities, develop a workflow that works for you.

If you make money that’s just a plus.



SCOPE!

- The important thing we have is consent! And we want to keep it.
- As long as you stay in scope, you're safe. Stepping out of scope, even with good intentions, you're just breaking the law.
- Example of the scope of Eero <https://hackerone.com/eero?type=team>



Finding a Bug

Reconnaissance

In this stage, you're finding assets or points of exploitation such as subdomains, parameters or queries. You want to know where you're exploiting, but also, you're wanting to take a deeper look into the actual product you're trying to exploit. Understanding how it works is essential.

Finding an Exploit

Know you're exploits <https://owasp.org/www-project-top-ten/> try to stay specific.

Escalation

If you can escalate the bug you have found, wonderful! But stay in the scope. If not then explain how this bug might lead to an escalated problem in your report.



You've Found a Bug

- Write a detailed report.

Your report is the most important thing in this process. You want your report to be very easy to follow and allow anyone reading it to be able to reproduce the bug you have found. And if you want to be rewarded, you must explain the severity and significance of what you have found.

You want to convince them that what you have found is a problem and it is worth fixing.

Doesn't necessarily have to be a long report.



Example



Abdelrhman Badr <mb.abdelrhman@gmail.com>
to admin ▾

Thu, Jun 30, 2022, 7:50 AM ☆ ↶ ⋮

Good Morning,

Parameter "ReturnUrl" is vulnerable to CRLF, allowing an attacker to inject their own headers in a server response.

An example is shown below.

```
1 HTTP/1.1 200 OK [application/javascript]
2 Date: Wed, 29 Jun 2022 12:00:00 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-Frame-Options: DENY
5 X-XSS-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 Content-Type: text/javascript
8 Expires: Wed, 29 Jun 2022 12:00:00 GMT
9 Cache-Control: no-cache, no-store, must-revalidate
10 Pragma: no-cache
11 Expires: Wed, 29 Jun 2022 12:00:00 GMT
12 Content-Type: text/javascript
13 Expires: Wed, 29 Jun 2022 12:00:00 GMT
14 Content-Type: text/javascript
15 Expires: Wed, 29 Jun 2022 12:00:00 GMT
16 Content-Type: text/javascript
17 Expires: Wed, 29 Jun 2022 12:00:00 GMT
18 Content-Type: text/javascript
19 Expires: Wed, 29 Jun 2022 12:00:00 GMT
20 Content-Type: text/javascript
21 Expires: Wed, 29 Jun 2022 12:00:00 GMT
22 Content-Type: text/javascript
23 Expires: Wed, 29 Jun 2022 12:00:00 GMT
24 Content-Type: text/javascript
25 Expires: Wed, 29 Jun 2022 12:00:00 GMT
26 Content-Type: text/javascript
27 Expires: Wed, 29 Jun 2022 12:00:00 GMT
28 Content-Type: text/javascript
29 Expires: Wed, 29 Jun 2022 12:00:00 GMT
30 Content-Type: text/javascript
31 Expires: Wed, 29 Jun 2022 12:00:00 GMT
32 Content-Type: text/javascript
33 Expires: Wed, 29 Jun 2022 12:00:00 GMT
34 Content-Type: text/javascript
35 Expires: Wed, 29 Jun 2022 12:00:00 GMT
36 Content-Type: text/javascript
37 Expires: Wed, 29 Jun 2022 12:00:00 GMT
38 Content-Type: text/javascript
39 Expires: Wed, 29 Jun 2022 12:00:00 GMT
40 Content-Type: text/javascript
41 Expires: Wed, 29 Jun 2022 12:00:00 GMT
42 Content-Type: text/javascript
43 Expires: Wed, 29 Jun 2022 12:00:00 GMT
44 Content-Type: text/javascript
45 Expires: Wed, 29 Jun 2022 12:00:00 GMT
46 Content-Type: text/javascript
47 Expires: Wed, 29 Jun 2022 12:00:00 GMT
48 Content-Type: text/javascript
49 Expires: Wed, 29 Jun 2022 12:00:00 GMT
50 Content-Type: text/javascript
51 Expires: Wed, 29 Jun 2022 12:00:00 GMT
52 Content-Type: text/javascript
53 Expires: Wed, 29 Jun 2022 12:00:00 GMT
54 Content-Type: text/javascript
55 Expires: Wed, 29 Jun 2022 12:00:00 GMT
56 Content-Type: text/javascript
57 Expires: Wed, 29 Jun 2022 12:00:00 GMT
58 Content-Type: text/javascript
59 Expires: Wed, 29 Jun 2022 12:00:00 GMT
60 Content-Type: text/javascript
61 Expires: Wed, 29 Jun 2022 12:00:00 GMT
62 Content-Type: text/javascript
63 Expires: Wed, 29 Jun 2022 12:00:00 GMT
64 Content-Type: text/javascript
65 Expires: Wed, 29 Jun 2022 12:00:00 GMT
66 Content-Type: text/javascript
67 Expires: Wed, 29 Jun 2022 12:00:00 GMT
68 Content-Type: text/javascript
69 Expires: Wed, 29 Jun 2022 12:00:00 GMT
70 Content-Type: text/javascript
71 Expires: Wed, 29 Jun 2022 12:00:00 GMT
72 Content-Type: text/javascript
73 Expires: Wed, 29 Jun 2022 12:00:00 GMT
74 Content-Type: text/javascript
75 Expires: Wed, 29 Jun 2022 12:00:00 GMT
76 Content-Type: text/javascript
77 Expires: Wed, 29 Jun 2022 12:00:00 GMT
78 Content-Type: text/javascript
79 Expires: Wed, 29 Jun 2022 12:00:00 GMT
80 Content-Type: text/javascript
81 Expires: Wed, 29 Jun 2022 12:00:00 GMT
82 Content-Type: text/javascript
83 Expires: Wed, 29 Jun 2022 12:00:00 GMT
84 Content-Type: text/javascript
85 Expires: Wed, 29 Jun 2022 12:00:00 GMT
86 Content-Type: text/javascript
87 Expires: Wed, 29 Jun 2022 12:00:00 GMT
88 Content-Type: text/javascript
89 Expires: Wed, 29 Jun 2022 12:00:00 GMT
90 Content-Type: text/javascript
91 Expires: Wed, 29 Jun 2022 12:00:00 GMT
92 Content-Type: text/javascript
93 Expires: Wed, 29 Jun 2022 12:00:00 GMT
94 Content-Type: text/javascript
95 Expires: Wed, 29 Jun 2022 12:00:00 GMT
96 Content-Type: text/javascript
97 Expires: Wed, 29 Jun 2022 12:00:00 GMT
98 Content-Type: text/javascript
99 Expires: Wed, 29 Jun 2022 12:00:00 GMT
100 Content-Type: text/javascript
```

The filter on returnUrl is bypassed by using "%E5%98%8A".

Kind Regards,
Abdelrhman



CraigDave <admin@craigdave.co.uk>
to me ▾

Thu, Jun 30, 2022, 1:36 PM ☆ ↶ ⋮

Hi Abdelrhman,

Every day's a school day :)
Many thanks for exposing that one for us. We have a patch in test now that will be going live tonight unless something unforeseen occurs.
I'll drop you a note when it's live and if you could give it a poke for us to double check that would be very much appreciated.

We don't have an official bug-bounty scheme but if there's anything that takes your fancy on our merch store (a hoody and a mug for example) then please let us know and we'll sort that out for you.
<https://shop.craigdave.org/product-category/merchandise>

Alternatively we can offer you an equivalent value in amazon vouchers if you prefer.

Many thanks,
Mark



Tools & Resources

- <https://github.com/tomnomnom/assetfinder> Great for Recon.
- <https://portswigger.net/burp> BurpSuite is your best friend for testing on domains.
- Time! Learning and testing could take up a lot of time so don't be discouraged if you feel like you'll never find a bug. You'll eventually find something because there are infinitely many bugs out there.

- <https://hackerone.com> Most popular bug bounty platform & Great CTFs to get you started.
- <https://owasp.org/> Learn about most common vulnerabilities and their uses.
- <https://www.youtube.com/@STOKfredrik> STÖK – Informative Guides (quit but still great)
- <https://www.youtube.com/@NahamSec> NahamSec – Informative Guides
- <https://www.youtube.com/@LiveOverflow> LiveOverflow – Deep dives into reports and vulnerabilities.



Make Your Account

https://hackerone.com/sign_up



Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Guest talk on BGP Hijacking by Simon Clayton
Mitchell from Node4

Any Questions?



www.shefesh.com
Thanks for coming!

