

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'. A 'Popular now' section lists various programs like 'Goldman Sachs', 'Bitrix', 'Marriott Bug Bounty', and 'Grab'. Each program card includes details such as 'Bug Bounty Program', 'Triaged by HackerOne, Retesting, Collaboration', 'Domain', 'Status', and a reward amount (e.g., 'Up to \$22k (+1.5 more)') with a progress indicator. A 'Collaboration Opportunities' section is visible at the bottom.

Intigriti

The screenshot shows the Intigriti platform interface. It features a header with the text 'Have a nice day hunting, primitheus'. Below the header is a search bar and a list of programs. Each program card displays the program name, a reward amount (e.g., '\$50 - \$15k'), and a progress indicator. The interface is clean and modern, with a focus on program details and search functionality.

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 All ▾

- 0 🛡️ By [waxx](#) to [Epic Games](#) \$2,000.00 closed 5 hrs ago
- 25 🛡️ By [nehuelm_to](#) to [Epic Games](#) \$100,000.00 bounty awarded 7 days ago
- 0 🛡️ 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) [application/javascript] 519104
2 Date: Sun, 26 Jun 2022 13:05:46 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 X-Frame-Options: DENY
5 X-XSS-Protection: 1; mode=block
6 Content-Security-Policy: default-src 'self';
7
8 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
9
10 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
11 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
12
13 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
14 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
15 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
16 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
17 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
18 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
19 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
20 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
21 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
22 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
23 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
24 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
25 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
26 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
27 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
28 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
29 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
30 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
31 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
32 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
33 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
34 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
35 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
36 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
37 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
38 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
39 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
40 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
41 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
42 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
43 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
44 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
45 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
46 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
47 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
48 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
49 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
50 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
51 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
52 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
53 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
54 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
55 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
56 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
57 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
58 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
59 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
60 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
61 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
62 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
63 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
64 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
65 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
66 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
67 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
68 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
69 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
70 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
71 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
72 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
73 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
74 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
75 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
76 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
77 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
78 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
79 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
80 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
81 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
82 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
83 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
84 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
85 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
86 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
87 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
88 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
89 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
90 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
91 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
92 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
93 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
94 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
95 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
96 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
97 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
98 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
99 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]
100 [Content-Security-Policy Report: https://www.w3.org/TR/2015/REC-CSP-1.1/#report-uri]

```

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



Any Questions?



www.shefesh.com
Thanks for coming!

