

HUNT LIKE A RAT

root@hackxpert:~\$

Bug bounty field card · The XSS Rat methodology · Authorized testing only

THE MINDSET — 8 RULES

1 PoC or GTFO

No impact, no report.

3 Out-think, don't out-race

Chase the leftovers.

5 Impact is king

Always ask 'so what?'

7 VDP is the training ground

Build a process first.

2 Know your enemy

Map for days, not hours.

4 Every tool lies

Confirm by hand.

6 Barriers are friends

Friction thins competition.

8 GDPR multiplier (EU)

PII access raises severity.

THE FOUR-PHASE METHOD

1 RECON

subs · alive · JS · dorking

> 2 EXPLORE

every role · poisoned signup

> 3 BURP

param reqs · hidden endpoints

> 4 TEST + CHAIN

vuln classes → chain → report

Recon is NOT hacking — it only finds where to hack.

PARAM → HYPOTHESIS

url= feed= webhook=

file= page= path=

id= user_id= invoice=

redirect= next= goto=

q= search= comment=

cmd= exec= ping=

XML/DOCX/SVG upload

SSRF

LFI/RFI

IDOR

Open redirect

XSS/SSTI/SQLi

Cmd injection

XXE

POISONED REGISTRATION

Seed EVERY field from minute one:

```
<img src=x onerror=
```

```
alert(document.domain)>${{7*7}}${{7*7}}
```

Fires later in: admin panels, PDFs, emails, backend logs.
Pair with a blind-XSS callback host.

PAYLOAD & TEST QUICK REFERENCE

Detection probes — confirm every hit by hand before you report.

XSS

Probe with `document.domain` (proves origin), not `alert(1)`.

```
<img src=x onerror=alert(document.domain)> <svg onload=alert(1)>
```

Stored / Reflected / DOM / Blind. Check 404/403/500 pages & Referer header.

SSTI

Seed math probes; the result fingerprints the engine (often RCE).

```
{{7*7}}=49 Jinja/Twig   ${7*7} Freemarker   <%= 7*7 %> ERB   *{7*7} Spring
```

SQL INJECTION

Inject body, cookies, and headers. Start with a quote; watch error/diff/timing.

```
' ' OR 1=1-- ' AND SLEEP(5)-- {"$gt":""} (NoSQL)
```

Confirm by hand, then `sqlmap --batch`. Test second-order too.

IDOR / BROKEN ACCESS CONTROL (the Rat's specialty)

A+B same role (horizontal) - admin+user (vertical) - two tenants (isolation).

Do action as A, replay with B's session, swap id/GUID/slug. Can B read/edit?

GUID amplification: an unguessable ID is only safe if it is never disclosed.

SSRF -> METADATA -> RCE

Any server-side URL fetch: `url=` `feed=` `webhook=` `image=`

```
http://169.254.169.254/latest/meta-data/iam/security-credentials/
```

Leak IAM creds, then S3/EC2. One of the highest-impact chains.

REPORT TEMPLATE

Title [Severity] - Summary (2-3 lines) - Steps (numbered, exact values) -

Impact (name data/accounts + GDPR on EU) - PoC (screenshot/recording) - Fix.