Beginning of the game

Round 1

Zihao Zeng

R3:http://eopgame.herokuapp.com/?s=SBsCNAv5PnpM2CMt&c=1&m=c1a675cb129e44f51b269c5871908e095dd58a19

When data flows from web server to the database , there is no encryption for log , which means attackers can easily read the information without any efforts .

RQ:http://eopgame.herokuapp.com/?s=SBsCNAv5PnpM2CMt&c=2&m=cae699b81f89c849f090c233ebce289ef4189131

There is no log from identity server to LDAP registry Hive which means we don’t know what happen in this process , thus attackers can claim anything they want .

IK:http://eopgame.herokuapp.com/?s=SBsCNAv5PnpM2CMt&c=3&m=f93bd5bbfa81bbc3b2b43835f9fea1cf44d0ba09

Scott Berry

Repudiation (Q):
http://eopgame.herokuapp.com/?s=QCnzjCf7pz5CODHV&c=1&m=b9b02dad6136f3e4cdee5064320bae3de32fe71e

There is no digital signing in the web server, leaving this system without verification of which users made changes. So rather than the attacker trying to claim an attack didn’t happen, the attacker shows that there is no way to prove that it was them who did the attack.

Spoofing (9):
http://eopgame.herokuapp.com/?s=QCnzjCf7pz5CODHV&c=2&m=153a0be386ab6daeef15b442e204e731b3d319c3

The Identity Server allows new password setting without knowledge of the original password and is thus vulnerable to attackers spoofing with accounts that were accessed without knowledge of password (i.e. using a key).

Spoofing (3):
http://eopgame.herokuapp.com/?s=QCnzjCf7pz5CODHV&c=3&m=141a400490bf861fb0b643f7c35fa10c03580e28

The Web Server is vulnerable to DDOS attacks, meaning that it allows endless attempts of requests without any threshold. So an attacker could iteratively try every password in attempts to log in until an eventual success. The load could also be too much for the system to bear without rate limiting.