

Project Category: Data Breach Assessment & Testing

Project Name	Carding Attack Prevention and AWS Buckets assessments
Client Name	One of our recurring client (Client Location is USA)
Industry	E-commerce
Challenges (Work)	One of our US location clients reached out to us because they face sudden random orders and transaction disputes and chargebacks from the payment gateway provider. They're running an E-commerce Shop backed by AWS cloud and Amazon related technologies. However data is managed at AWS but the store is custom designed.
Type	Cloud Security, Penetration Testing, Red Teaming, Data Breach Assessment and Anti Hacking Security
Project Duration	25 Days
Outcome	We immediately investigated the cause and found that the client's customer's credit card data was stolen and appeared on the dark web. So our cyber lawyers and forensic experts are working and removing the data and asking clients to temporarily postpone their business. So they agreed and we

immediately informed the local cyber police authority and explained to them. So they're starting to investigate. Now the problem is that one of the private AWS buckets is public and visible and accessible to anyone. And all data is stored into that. So the intruder accessed and committed this crime. We implemented a data breach resistance mechanism and installed SIEM. Now the client feels relaxed.