

# Certification & Accomplishment



**O**ur focus is always on working to the highest standards of customer service, quality, and innovation. We're proud that this has been recognized with a range of industry Certifications and Accomplishments.

**H A D E S S**  
Secure Agile Development

## Customers

- **7ASecurity(Penetration Testing)**  
<https://7asecurity.com/>
- **AbanTether(Red Team, Application Security)**  
<https://abantether.com/>
- **Mofid Securities (Application Security)**  
<https://emofid.com/>

## Publications

- **Practical Application Security**  
<https://leanpub.com/practicalappsec>

## Certifications

- **eLearnSecurity Certified Penetration Tester eXtreme (eCPTXv2)**  
[320a9f14-1d12-4385-aae1-021a8a0c8965](https://www.elearnsecurity.com/certification/320a9f14-1d12-4385-aae1-021a8a0c8965)
- **Certified Red Team Professional (CRTP)**  
[30253302](https://www.redteam.io/certification/30253302)
- **Security Aware**  
<https://portal.securecodewarrior.com/#/stats/6050e0b01613e70091adcadb>
- **API Security Architect**  
75232225
- **Certification of Complete LPIC2**  
numberfd3ett3129nfujwrobx1
- **Certification of Complete LPIC3-303**  
2019-4037
- **Certification of Complete Openstack Administrator**  
2018-2968
- **Certification of Complete MTCNA**  
numberxb081kzv5wckb5vasnqo
- **Certification of Complete CEH v10**  
20190425ECC-01-9967
- **Certification of Complete SEC542**  
20190425SANS-02-8973
- **Certification of Complete SEC642**  
20190420SANS-03-8966
- **Certification of Complete CHFI v9**  
20200220ECC-02-9894
- **Certification of Complete FOR500**

- 20200220SANS-FOR500-01-98
- **Certification of Complete FOR572**  
20200220SANS-05-9893
- **Certification of Complete FOR600**  
20200220SANS-08-9683
- **Certification of Complete FOR610**  
20200221SANS-07-9895
- **Certification of Complete GMOB**
- **Certification of Complete Cryptography Fundamentals**  
C-75631f5bcb-413d9a3
- **Certification of Complete CCNA**  
C-75631f5bcb-8c7f89
- **Certification of Complete MCSA**  
C-75631f5bcb-6638a9
- **NSE 2 Network Security Associate**  
5cfbdf2f58f13e4a27016b865915aeb392180d39

## Awards

- **CVE 2019-017070**
- **CVE 2019-017071**
- **CVE 2019-017072**
- **Google [Hof](#)**
  - Due to the mentioned vulnerability, the attacker will be able to bypass the CORS security feature of the system and execute its JavaScript commands on the client.
- **Apple [Hof](#)**
  - Due to the mentioned vulnerability, the attacker will be able to view the information and settings on the server side of the system.
  - This vulnerability occurred in the management control and system error and the attacker only viewed the system configuration information by entering the vulnerable endpoint address.
- **Twitter [Hof](#)**
  - Due to the mentioned vulnerability, the attacker will be able to remove the users of this system.
  - This vulnerability occurred in the access control layer of the system and the attacker was able to delete the user's profile simply by knowing the user's user code.
- **Dell [Hof](#)**
  - Due to the mentioned vulnerability, the attacker will be able to inject and execute his JavaScript commands by bypassing the security controllers in the search section of the store.
  - This vulnerability has occurred in the store search section due to the lack of proper sanitize of the user input.

- **Mail.ru**
  - Due to the mentioned vulnerability, the attacker will be able to execute his commands on the victim browser by loading a file infected with JavaScript commands.
  - This vulnerability occurs in the File Upload module of the system and the attacker will be able to change the format of the sent file and inject JavaScript commands with the Intercept file upload request.
- **Zabbix 5 RCE**
  - Due to the mentioned vulnerability, the attacker will be able to forge his commands by the system administrator due to the lack of CSRF Token in the command execution module by the agents, and as a result, receive the possibility of remote command execution from the Zabbix server.
  - This vulnerability occurred in the access management layer at the form level and due to the lack of a unique code per user or CSRF Token, the attacker was able to forge the user side request.
- **Portswigger [HoF](#)**
  - Win flag-winning contests and web-based security challenges in more than 15 different security categories
  - Ranked 16<sup>th</sup> (RezaDuty as an expert) out of four thousand participants.
- **Hackthebox Top 10 [HoF](#)**
- **Datastax Hof**
  - Due to the mentioned vulnerability, the attacker will be able to receive all user transactions just by knowing their user code.
  - The vulnerability occurred in the access level management layer of the system and the attacker could view the victim by sending the user's user code to the vulnerable endpoint.
- **Barracuda Hof**
  - Due to the mentioned vulnerability, the attacker will be able to view all system users as well as all system certificates.
  - This vulnerability occurred in the access control management layer and the user input was not sanitized properly and the attacker could view the certificates and users of the system by sending a query to the vulnerable endpoint.
- **WordPress Plugin**
  - Registration and detection of SQL Injection, XSS vulnerabilities with CVE2020-17070-17071-17072 IDs from Client Dash, LIQUID SPEECH, Contact Form Widget plugins belonging to WordPress with more than 2,000 active installations in the world
- **Phpmyadmin v5.0.2 – Self-XSS**
- **Moodle v3.8.2 – Local Command Injection**
- **Phpbb v4.1.1 – Local SQLi**
- **Rocket.chat**



## About HADESS


HADESS is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the cyber threat.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionizing the way in which organizations think about cyber security.

**For more information from HADESS, please contact:**

- [marketing@hadess.io](mailto:marketing@hadess.io)
- +98217787338



**O**ur focus is always on working to the highest standards of customer service, quality, and innovation. We're proud that this has been recognized with a range of industry Certifications and Accomplishments.