



DIS10.5

Data and Information security | Council of India

DIS10.5: TOP 20 Critical Web Application Vulnerability Certification(DWAV20 Standards)

DWAV20: Web Application Security Standards



What is DIS ?



DIS is the Globally trusted Brand in Information security and Ethical Hacking Training in world. **DIS Consultants** include group of Advanced Security Researchers from round the world who are real world Masters in Information Security. **DIS** is Providing Training via Live Classroom, Virtual Training Labs, Workshops, Webinars, Corporate Training's, and Training's via **DIS** Certified Training Centers (**Authorized Training Partners**).

DIS'S Digital Badge Program



DWAV20

TOP 20 Critical Web Application Vulnerability
Certification(DWAV20 Standards)

**Web Application Vulnerability
Certification(DWAV20 Standards)**

DIS10.5: TOP 20 Critical Web Application Vulnerability Certification(DWAV20 Standards)

DIS10.5 WEB APP SECURITY (DIS Top 20 Critical Web Application Vulnerabilities) course will help candidate get deep information about web applications security process. Web applications security includes various vulnerabilities like Sql Injection, Php Injection,XSS,CSRF, Indirect object reference and many more. This course will help student to get instant job in the Cyber Security.(25 Credits towards DIS10 Diploma)



Course Content

DWAV20

TOP 20 Critical Web Application Vulnerability
Certification(DWAV20 Standards)

- DWAV20.1 : SQL Injections Flaws**
- DWAV20.2 : Cross Site Scripting Flaw**
- DWAV20.3 : Source Code Disclosure Flaw**
- DWAV20.4 : OS Command Injection Flaw**
- DWAV20.5 : Broken Authentication and Session Management**
- DWAV20.6 : File Upload Vulnerability (Dangerous File Upload)**
- DWAV20.7 : CSRF – Cross Site Request Forgery**
- DWAV20.8 : Sensitive Data Exposure**
- DWAV20.9 : Insecure Direct Object Reference**
- DWAV20.10 : Local file Inclusion and Remote File Inclusion(LFI and RFI attack)**
- DWAV20.11 : Directory Traversal Attack**
- DWAV20.12 : Insecure Transport Level Communication**
- DWAV20.13 : Information Exposure Through an Error Message**
- DWAV20.14 : Invalid URL Redirection Flaw**
- DWAV20.15 : Hard-coded Credentials in Static Code**
- DWAV20.16 : Security Mis-Configuration**
- DWAV20.17 : Missing Authorization and Authentication for Critical Functions**
- DWAV20.18 : Session Fixation**
- DWAV20.19 : Weak Data Encryption**
- DWAV20.20 : Information Leakage**

GET CERTIFIED



TEACHING



LEARN

Who can Attend This Training ?

1. Students/Individuals
2. College going Students
3. Industry Expert
4. Network Specialist
5. Army/Navy Officials
6. Intelligence Agencies(Forensics Analyst)
7. College Faculties
8. Government and Corporate IT Managers
9. CEO/CTO and Higher Management Personals.
10. Security Tester who need to find network based vulnerabilities and re-mediate them.
11. Penetration Testers
12. Ethical Hackers
13. RED OR BLUE team Members
14. Computer geeks who wants deep knowledge about Computer Forensics

What Will You Get in DIS10.5 ?



- 1.** ALL Virtual Machines and Virtual Environment for Students who attend trainings.
- 2.** DVD with tools , Videos , Practice Tests , Virtual Labs.
- 3.** Audio and Video Tutorials which will help in doing practical sessions at your study desk also.
- 4.** Written Test Voucher Code
- 5.** Online Test Voucher Code

DIS10.5: Exam Details



Training Mode : Online Web Challenge

Course Duration : 60-80 Hours(Instructor-Led Training) 2 Hours /8 Hours /4 Hours Per Day

Exam Code : DIS10.5

Exam Duration: 60 Hours (Lab Challenge)

Exam Fee : 300 USD (Written + Lab Challenge) **Credits**: 25 Credits (Towards DIS10:Diploma in Information Security)

DIS Trainings and Exam's are only available at *Authorized Training Centers

Hands-on Training



- DWAV20.1 : SQL Injections Flaws : Manual and Automated using Havij, SQLMAP**
- DWAV20.2 : Cross Site Scripting Flaw : Manual and Tool Based : Using Burp Suite**
- DWAV20.3 : Source Code Disclosure Flaw : Manual Process and File Including**
- DWAV20.4 : OS Command Injection Flaw: On DVWA and Metasploitable Linux**
- DWAV20.5 : Broken Authentication and Session Management : DVWA, Samurai OS**
- DWAV20.6 : File Upload Vulnerability (Dangerous File Upload) Live Practical Based Example**
- DWAV20.7 : CSRF – Cross Site Request Forgery**
- DWAV20.8 : Sensitive Data Exposure : Live WebSite**
- DWAV20.9 : Insecure Direct Object Reference: Instructor Special**
- DWAV20.10 : Local file Inclusion and Remote File Inclusion(LFI and RFI attack): BURP SUITE**
- DWAV20.11 : Directory Traversal Attack. Manually Traversing Directories on a Web Site**
- DWAV20.12 : Insecure Transport Level Communication: Weak SSL Version Detection**
- DWAV20.13 : Information Exposure Through an Error Message**
- DWAV20.14 : Invalid URL Redirection Flaw**
- DWAV20.15 : Hard-coded Credentials in Static Code Live Example**
- DWAV20.16 : Security Mis-Configuration**
- DWAV20.17 : Missing Authorization and Authentication for Critical Functions**
- DWAV20.18 : Session Fixation : Practical Based**
- DWAV20.19 : Weak Data Encryption**
- DWAV20.20 : Information Leakage**

TOP 20 Critical Web Application Vulnerability Certification(DWAV20 Standards) DIS10.5 FAQs

What is DWAV20?

It is an International Standard Vulnerabilities which can occur in any web application. DWAV20 are categorized based on previous year vulnerability occurrence Database from various international vulnerability Database Research Organization.

What I will learn in this Web Application Attack Course?

In this Training and Certification one will be able to detect various vulnerabilities some of them like sql injection, command injection, file upload vulnerabilities, LFI, RFI, Authentication bypass, session related attacks, weak crypto detection in a web Application.

Who will teach this Course?

This course is taught to you by industry professionals and is designed by industry well known security consultants from round the world. Course is been taught by well experienced DIS Certified Trainers only.

How it's different from other certifications Vendors in market?

This course is completely practical based approach it is not just slide based trainings or big huge books based. This is completely a new practical full time approach for people who wants to get into security domain. This is the most advanced security certification trainings in the world.

Workshop Trainings / Corporate Trainings Placement Partners

CompTIA

Justdial
India's No.1 local search engine

HDFC BANK

DIS10



Microsoft
Partner Network



CISCO
Cisco Select Certified Partner

Hackinn
Technologies

IT Kanpur presents
TECHKRITI '14
6th-9th March



DELL
REGISTERED PARTNER
ID: 2724997904

redhat



جامعہ ملیہ اسلامیہ
جامیہ میللیا اسلامیہ

Jamia Millia Islamia
A Central University

ORACLE

DELL
REGISTERED PARTNER
ID: 2724997904

HACK
MANTHAN



AMITY
UNIVERSITY
—GURGAON—

CompTIA
AUTHORIZED PARTNER
GOLD



TrainingKart.in
New Art of Education

ignou
THE PEOPLE'S UNIVERSITY



TATA
COMMUNICATIONS

AVANZAR



BEST TRAINING
2013-14
PARTNER
Computer Council &
Society of INDIA



IGNUS 2013
click here to verify us..



Ministry of Corporate Affairs
Government of India



جامعہ ملیہ اسلامیہ
جامیہ میللیا اسلامیہ

Jamia Millia Islamia
A Central University

MCA21
Service Transformation

DIS10.5

Author Statement



Web Application Testing focus on core areas of Web Application Programming flaws due to which a malicious Hacker could breach the complete security of the System.

DIS Consultants(Content Contributor)
– Mr Pardeep Kumar, DIS Content Contributor

Web Application Penetration Tester

How do I Pay for this Course ?



**NEFT/RTGS/ Cash/Cheque/Demand Draft
Deposit to:**

Acc. Name: "Bytecode Cyber Security Pvt Ltd"

Account No : 003705018009

Branch : Preet Vihar, Delhi

IFSC Code : ICIC0000037

Swift Code : ICICNBBCTS



Now You Hold



Diploma in Information Security

GET CERTIFIED





Thank You

Call Us at 011-45671678

Mobile : +918130535445

Email: enquiry@bytecode.in

Address: Bytecode Cyber Security PVT LTD E-61, 3rd floor, Near Heera sweets, Laxmi Nagar, Delhi-110092

Landmark : Metro pillar no 46

website: www.bytecode.in

website: www.bytec0de.com

INDIA | USA | Nigeria | Dubai |

Australia | UAE | Germany