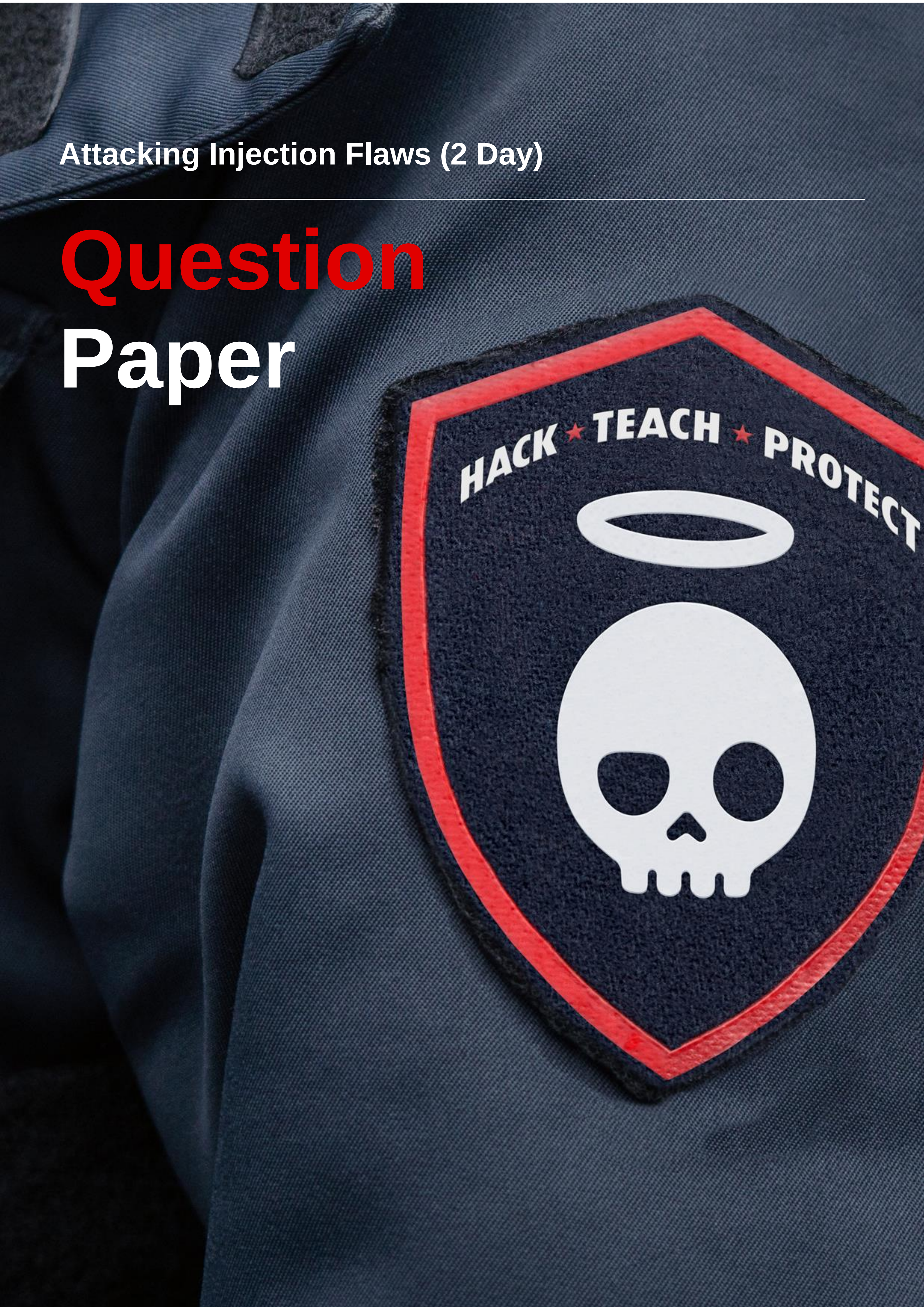
Attacking Injection Flaws (2 Day)

Question Paper



Contents

Module: XML External Entity (XXE) Attacks

XML External Entity (XXE)

Challenge URL: http://hc.webhacklab.com/

- **Identify and exploit XXE to extract the contents of the file "/etc/passwd".**

Advanced XXE Exploitation over OOB

Challenge URL: http://hc.webhacklab.com/

- **Identify and exploit blind XXE over OOB channels on the API v2 to extract the contents of the file "/etc/passwd" from the host.**

XXE through SAML

Challenge URL: http://topup.webhacklab.com/saml/SAML.aspx

- **Exploit SAML XML to perform XXE attack and extract the contents of the file "c:/windows/win.ini" from the host.**

XXE in File Parsing

Challenge URL: http://shop.webhacklab.com/career.php

- **Upload a file having "docx" type to perform an XXE attack and extract the contents of the file "/etc/passwd" from the host.**

XXE via XInclude

Challenge URL: http://hc.webhacklab.com/HealthCheckV3

- **Identify and exploit XXE attack and extract the contents of the file "/etc/passwd" from the host.**

Module: SQL Injection Masterclass

Second Order SQL Injection

Challenge URL: http://topup.webhacklab.com/Account/SecurityQuestion

- **Identify a Second order injection using your account.**
- **Exploit the injection to extract the name of the user running the service.**

SQLi Through Crypto - OOB

Challenge URL: http://topup.webhacklab.com/Shop/Order

- **Identify a data encryption endpoint using your registered account.**
- **Utilize the knowledge of encryption endpoint to confirm SQL injection using an OOB channel.**

SQL Injection to Reverse Shell

Challenge URL: http://topup.webhacklab.com/api/voucher

- **Continue with previous exercise to obtain a reverse shell on the DB host using Metasploit and native Windows tools (powershell, certutil, cscript etc.).**

Second-order SQL Injection on Joomla

Challenge URL: http://cms.webhacklab.com:81/administrator/index.php

- **Identify and exploit second order SQL Injection point in Joomla Instance**
- **Fetch the databases from database server**

Advance SQLMAP Usage with eval option

Challenge URL: http://topup.webhacklab.com/api/Product/GetProduct?pid=&sig=

- **Identify SQL Injection point**
- **Fetch the databases from the database server**

Data Exfiltration over DNS via SQLi

Challenge URL: http://topup.webhacklab.com/Account/SecurityQuestion

- **Exploit the injection vulnerability to exfiltrate the output of command “ipconfig” over DNS channel.**

SQLi via File Metadata

Challenge URL: http://reimbursement.webhacklab.com/Expense/Add

- **Identify and Exploit SQL Injection via File Metadata properties to retrieve current database user and database name.**

GraphQL Exploitation

Challenge URL: http://expense.webhacklab.com:3000/viewexpense

- **Exploit SQL injection in one of the GraphQL endpoints and retrieve admin credentials.**
- **Use Introspection to extract the PII (Salary) of the ‘userX@webhacklab.com’.**
- **Using GraphQL mutation, view expenses of all the users.**

Module: Remote Code Execution (RCE)

PHP Object Injection

Challenge URL: http://shop.webhacklab.com/help.php

- **Exploit a PHP object injection instance to access “/etc/passwd” file from the server.**

PHP Deserialization Attack

Challenge URL: http://slim.webhacklab.com:8081

- **Identify and exploit the PHP Deserialization vulnerability.**
- **Get a reverse shell and extract the system information such as username, OS type from the server.**

Java Deserialization Attack - Binary

Challenge URL: http://mblog.webhacklab.com/login

- **Identify and inject a payload into the serialised data to make the host send DNS requests to an external host.**
- **Get a reverse shell and extract the system information such as usernames, OS type from the server and also read "/etc/passwd" file.**

Tricky Java Deserialization Attack - Binary

Challenge URL: http://mblog.webhacklab.com/login

- **Identify and inject a payload into the serialised data to make the host send DNS requests to an external host.**
- **Get a reverse shell and extract the system information such as usernames, OS type from the server and also read "/etc/passwd" file.**

Java Deserialization Attack - XML

Challenge URL: http://mblog.webhacklab.com/api/add/microblog

- **Identify the request to inject XML serialised data and inject a payload into it to make the host send ping requests to an external host.**
- **Get a reverse shell and extract the system information such as username, OS type from the server and also read "/etc/passwd" file.**

Jackson JSON Deserialization Attack

Challenge URL: http://mblog.webhacklab.com/mblog/api/add/microblog

- **Get a reverse shell and extract the system information such as username, OS type from the server and also read "/etc/passwd" file.**

.NET Serialization Attack

Challenge URL: http://admin.webhacklab.com

- **Identify and exploit the .Net Deserialization vulnerability to make the host send HTTP requests to an external host.**
- **Get a reverse shell and extract the system information such as username, OS type from the server and read "win.ini" file.**

Python Serialization Attack

Challenge URL: http://reimbursement.webhacklab.com/Support/AddTicket

- **Identify and exploit the Python Deserialization vulnerability to make the host send DNS requests to an external host.**
- **Get a reverse shell and extract the system information such as username, OS type from the server and read "/etc/passwd" file.**

Plex Python Deserialization

Challenge URL: http://plex.webhacklab.com:32400

- **Perform RCE using python deserialization vulnerability.**

Ruby/ERB Template Injection

Challenge URL: http://shop.webhacklab.com/referral.php

- **Identify the template engine and exploit it to extract the content of the file "/etc/passwd"**

Server-side Template Injection in YouTrack

Challenge URL: http://192.168.200.20:8888

- **Identify the template engine and exploit it to extract the output of "id" command**

Leverage Git misconfiguration to ViewState RCE

Challenge URL: http://books.webhacklab.com/.git

- **Leverage Git misconfiguration to extract the Machine Key.**
- **Exploit ViewState to perform Remote Code Execution (RCE)**

Module: Server Side Request Forgery (SSRF)

SSRF To Check Open Ports and Fetch File

Challenge URL: http://shop.webhacklab.com/products.php

- **Utilizing SSRF extract the contents of the internal file "/etc/passwd".**
- **Identify the ports open on the host "http://192.168.200.10/".**

SSRF via PDF Generation

Challenge URL: http://topup.webhacklab.com/Account/Profile

- **Utilise PDF export injection to confirm SSRF using OOB channel.**
- **Retrieve the content of the internal file “win.ini”:**

SSRF Filter Bypass

Challenge URL: http://52.86.173.194/index.php

- **Access the server-status page of the application.**

AWS - SSRF Exploitation - Elastic Beanstalk

Challenge URL: http://cloud.webhacklab.com/view_pospdocument.php?doc= {}

- **Identify and exploit SSRF vulnerability to gain access to S3 buckets and download the source of the application hosted on AWS cloud.**
- **Upload a web shell via Continuous Deployment (CD) pipeline.**

Module: Miscellaneous Injections

SAML Authorization Bypass

Challenge URL: http://topup.webhacklab.com/saml/SAML.aspx

- **Login as user "not-a-john@webhacklab.com".**
- **Decode the SAML data into XML format.**
- **Exploit SAML XML to login as user "john@webhacklab.com".**

Log4Shell

Challenge URL: http://mblognew.webhacklab.com/login

- **Identify Log4Shell vulnerability and inject a payload to make the host send DNS requests to an external host.**
- **Get a reverse shell and extract system information such as usernames, OS type from the server.**

Host Header Validation Bypass

Challenge URL: http://topup.webhacklab.com/Account/ForgotPassword

- **Bypass host header validation to perform header poisoning for your account.**
- **Capture the password reset token.**
- **Change the password of the account using the captured token.**

HTTP Parameter Pollution (HPP)

Challenge URL: http://misc.webhacklab.com:5984/_utils/

- **Create a new user (userX) with "admin" role in the CouchDB instance.**